Bitdefender®

TOTAL SECURITY 2018

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Bitdefender Total Security 2018
Руководство пользователя

Дата публикации 20.02.2018

Правовое положение

Bitdefender

Содержание

Об этом руководстве

1. Цель и целевая аудитория

Ваша подписка Bitdefender Total Security 2018 может защитить до 10 различных ПК, Mac, iOS и Android смартфонов и планшетов. Управление устройствами выполняется через учетную запись Bitdefender

Руководство оказывает помощь в настройке продуктов Вашей Подписки: Bitdefender Total Security, Bitdefender Antivirus for Mac, Bitdefender Mobile Security for iOS и Bitdefender Mobile Security & Antivirus для устройств Android

Получить сведения о настройке Bitdefenderна различных устройствах

2. Как использовать руководство

Данное руководство предназначено для продуктов, включенных в Bitdefender Total Security 2018:

- «Total Security для ПК» (p. 1)

  Получить сведения о применении продукта на ноутбуках и компьютерах под управлением Windows.

- «Антивирус для Mac» (p. 235)

  Получить сведения о применении продукта на устройстве Mac

- « Мобильная безопасность для iOS» (p. 272)

  Получить сведения о применении продукта на смартфонах и планшетах

- «Mobile Security для Android» (p. 284)

  Получить сведения о применении продукта на смартфонах и планшетах

- «Свяжитесь с нами» (p. 329)

  Поиск информации в случае возникновения проблем.

TOTAL SECURITY ДЛЯ ПК

1. УСТАНОВКА

1.1. Подготовка к установке

Перед установкой Bitdefender Total Security 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. 2).
- 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.
- Отключите или удалите брандмауэр, который может быть запущен на компьютере. Одновременный запуск двух брандмауэров может повлиять на их работу и вызвать серьезные проблемы с системой. Во время установки брандмауэр 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.

1.2. Системные требования

Вы можете установить Bitdefender Total Security 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.

Замечание

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.

Минимальные системные требования

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

Рекомендуемые системные требования

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

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
- Skype 6.3 более новые версии
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 и выше

1.3. 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 подписка охватывает более чем один компьютер, повторите процесс установки и активации продукта, с той же учетной записью, на каждом компьютере. Вам нужно использовать аккаунт, который содержит активную подписку на ваш Bitdefender.

Установка из Bitdefender Central

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

Для скачивания Bitdefender Total Security из Bitdefender Central необходимо:

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.
3. В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.
4. Выберите одну из двух доступных опций:

   - **Загрузка**

     Нажмите на кнопку и сохраните установочный файл.

   - **На другое устройство**

Выберите **Windows**, чтобы скачать Bitdefender и затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.

5. 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 Total Security инсталляционный пакет постоянно обновляется.

Замечание

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 Total Security.

Шаг 1 - Bitdefender установка

На экране установки Bitdefender нажмите кнопку **Установить** для запуска процесса установки Bitdefender.

Три дополнительные задачи могут быть выполнены во время этого шага:

- Ознакомьтесь с Соглашением о Подписке перед тем как запустить установку. Соглашение о Подписке содержит условия и положения, в соответствии с которыми используется Bitdefender Total Security

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

- Не выключайте опцию **Отправить анонимные отчеты**. 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.

Шаг 2 - Ход выполнения установки

Дождитесь завершения установки. Отображаются подробные сведения о ходе выполнения.

Выполняется проверка критических областей системы на наличие вирусов, 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. 100)

Шаг 3 - Установка завершена

Ваш Bitdefender продукт успешно установлен.

Отображается сводная информация по установке. Если во время установки обнаружены и удалены вредоносные программы, 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 Total Security интерфейс.

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.

Замечание

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 Total Security.

Шаг 1 - Bitdefender Установка

На экране установки Bitdefender нажмите кнопку **Установить** для запуска процесса установки Bitdefender.

Три дополнительные задачи могут быть выполнены во время этого шага:

- Ознакомьтесь с Соглашением о Подписке перед тем как запустить установку. Соглашение о Подписке содержит условия и положения, в соответствии с которыми используется Bitdefender Total Security

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

- Не выключайте опцию **Отправить анонимные отчеты**. 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.

Шаг 2 - Ход выполнения установки

Дождитесь завершения установки. Отображаются подробные сведения о ходе выполнения.

Критические области вашей системе проверяются на наличие вирусов и Bitdefender службы запускаются. 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. 100)

Шаг 3 - Установка завершена

Отображается сводная информация по установке. Если во время установки обнаружены и удалены вредоносные программы, 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 дополнительной информации перейдите к «*Bitdefender Central*» (p. 39).

Выполните действия, соответствующие текущей ситуации.

Я хочу создать учетную запись Bitdefender

Введите необходимую информацию в соответствующих полях, а затем нажмите **СОЗДАТЬ АККАУНТ**.

Информация, которую вы предоставите, останется конфиденциальной.

Пароль должен содержать не менее 8 символов и содержать цифру.

Прочитайте Условия предоставления услуг Bitdefender, прежде чем двигаться дальше.

Замечание

После создания учетной записи Вы можете использовать имеющийся адрес электронной почты и пароль для входа в учетную записьhttps://central.bitdefender.com

У меня уже есть учетная запись Bitdefender

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

Нажмите **Войти** чтобы продолжить.
Если Вы забыли пароль учетной записи или просто хотите сбросить уже имеющийся, нажмите ссылку **Забыли пароль**. Введите адрес вашей электронной почты, затем нажмите кнопку**ЗАБЫЛИ ПАРОЛЬ** Проверьте электронную почту учетной записи и следуйте приведенным инструкциям для установки нового пароля Вашей учетной записи Bitdefender

Замечание

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.

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

Шаг 5 - Активация вашего продукта

Замечание
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**.

     Замечание
     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 Total Security интерфейс.

2. НАЧАЛО РАБОТЫ

2.1. Основы

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

Приложение использует технологию Фотон для повышения скорости и производительности антивирусного процесса сканирования. 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. 162).

Можете отслеживать пароли и учетные данные, сохранив их в «*Защита ваших учетных данных при помощи Менеджер паролей*» (p. 155) Хранилище. Используя один мастер-пароль Вы можете защитить персональные данные от злоумышленников, которые могут попытаться вывести Ваши денежные средства.

«*Защита веб-камеры*» (p. 144)отвлекает ненадежные приложения от доступа к видеокамере, тем самым избегая любых попыток взлома. С учетом выбора пользователей Bitdefender доступ к популярным приложениям на веб-камеру будет разрешен или заблокирован.

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. 141)

Ваши личные файлы, хранящиеся локально, такие как документы, фотографии или видеоматериалы, а также те, которые хранятся на облаке,остаются под надежной защитой от самого опасного сегодня вредоносного ПО, а именно, вируса-вымогателя. Информацию о том, как перенести личные файлы в хранилище см.«*Безопасные файлы*» (p. 147)

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. 192).

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 дополнительной информации перейдите 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 Total Security и управлять своими подписками и устройствами, войдите в вашу учетную запись Bitdefender. Для получения дополнительной информации перейдите к «*Bitdefender Central*» (p. 39).

В разделе «*Советы*» (p. 52) вы найдете пошаговые инструкции о том, как выполнять общие задачи. Если у вас возникли проблемы при использовании Bitdefender, проверьте раздел «Решение общих вопросов.» (p. 200) для возможного решения наиболее распространенных проблем.

Откройте окно Bitdefender.

Выполните следующую процедуру, чтобы войти в главный интерфейс Bitdefender Total Security:

- В **Windows 7**:
  1. Нажмите **Пуск** и перейдите в **Все программы**.
  2. Нажмите **Bitdefender 2018**.

3. Нажмите **Bitdefender Total Security** или дважды нажмите на Bitdefender иконку системном трее.

- 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 системном трее.

- 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 системном трее.

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

Устранение неисправностей

Bitdefender использует Систему слежения в целях обнаружения проблем, которые могут отразиться на безопасности Вашего компьютера и личных данных и сообщает Вам о них. По умолчанию он будет контролировать только те группы проблем, которые считает особенно серьезными. Тем не менее, Вы можете настроить его по своему усмотрению, выбрав отдельные виды проблем, о которых желаете получать уведомления.

К обнаруженным проблемам относится отключение важных параметров настроек защиты и другие условия, представляющие угрозу безопасности. Они сгруппированы в две категории:

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

Изменение цвета значка Bitdefender в system tray свидетельствует о наличии проблем:

Критические проблемы влияют на безопасность системы. Они требуют немедленного вмешательства и решения.

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

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

Когда Вы откроете Bitdefender интерфейс Статус Защиты области, на верхней панели инструментов будет отмечено какого рода проблемы воздействуют на систему.

Мастер проблем безопасности

Чтобы устранить обнаруженные проблемы, следуйте инструкциям мастера **Security Issues**.

1. Для того чтобы запустить мастер, сделайте следующее:
   - Правой кнопкой мыши щелкните по значку Bitdefender в Системный трей и выберите **Просмотр проблем безопасности**.
   - Откройте окно Bitdefender interface и щелкните внутри области Состояния Безопасности на верхней панели инструментов.
2. Вы можете видеть проблемы, подвергающие риску безопасность вашего компьютера и данных. Выбрано устранение всех текущих проблем.

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

   Для проблемы будет установлен статус **Отложить**, и система не будет предпринимать никаких действий по ее исправлению.
3. Для устранения выбранных проблем, нажмите **Устранить**. Некоторые проблемы незамедлительно будут устранены. Устранить остальные вам поможет мастер.

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

- **Отключенные параметров настройки безопасности.** Такие проблемы устраняются незамедлительно путем включения соответствующих параметров безопасности.
- **Профилактические задачи безопасности, которые необходимо выполнить.** При устранении таких проблем мастер поможет вам успешно завершить задачу.

Настройка отслеживания состояния

Bitdefender может сообщить вам, когда проблемы обнаруживаются при эксплуатации следующих программных компонентов:

- Антивирус
- Брандмауэр (Firewall)
- Обновления
- Защита Браузера

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

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **РАСШИРЕННЫЙ**
3. Нажмите ссылку **Настройка уведомлений о состоянии**.
4. С помощью переключателей можно включить или отключить Уведомление о статусе в соответствии с потребностями.

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 произведено обновление, были ли обнаружены вредоносные программы или неисправности на вашем компьютере и

т.д. Кроме того, при необходимости можно предпринять дополнительные действия или изменить операции, которые выполнил Bitdefender.

Чтобы получить доступ к журналу Уведомлений, нажмите иконку на левой панели инструментов Bitdefender interface. Каждый раз, когда происходит критическое событие, счетчик отмечает его на иконке.

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.

Автопилот

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

Когда режим "Автопилот" включен, Bitdefender применяет оптимальную конфигурацию безопасности и принимает за вас все решения, связанные с защитой. Это означает, что всплывающие окна и уведомления не будут отображаться и вам не потребуется настраивать никакие параметры.

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

- Антивирусная защита, реализуемая с помощью резидентного и непрерывного сканирования.
- Защита брандмауэра.
- Защита в Интернете.
- Автоматические обновления.

Чтобы включить или выключить Автопилот, нажмите переключатель **АВТОПИЛОТ** на верхней панели Bitdefender интерфейс.

Пока режим "Автопилот" остается включенным, значок Bitdefender в области уведомления будет иметь вид .

Важно

Если режим "Автопилот" включен, то изменение функций, которыми он управляет, приведет к их отключению .

Чтобы просмотреть историю действий, выполняемых Bitdefender во время работы Автопилота, откройте окно Уведомления.

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 Кино
: 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.

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
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, щелкните соответствующий переключатель вкл / выкл. Только один профиль можно активировать за один раз.

Для получения более подробной информации о Профилях, пожалуйста, обратитесь*«Профили»* (p. 192)

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 на  иконку в нижнем левом углу Bitdefender interface.
2. В окне **Общие** включите **Параноидальный режим**, используя соответствующий переключатель.
3. Введите пароль в двух полях и затем нажмите **ОК**. 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 на  иконку в нижнем левом углу Bitdefender interface.
2. В окне **ОБЩИЕ** отключите защиту паролем, щелкнув соответствующий переключатель.
3. Введите пароль и затем нажмите **ОК**

Замечание

Для того, чтобы изменить пароль доступа к продукту, нажмите **Поменять пароль**. Введите текущий пароль и нажмите *ОК*. В новом окне, которое появится введите новый пароль, который вы хотите использовать, чтобы ограничить доступ к вашим Bitdefender параметрам.

Анонимные отчеты об использовании

По умолчанию Bitdefender отправляет отчеты, содержащие информацию по использованию вами серверов Bitdefender. Эта информация поможет нам усовершенствовать продукт и предложить в будущем более широкие возможности. Учтите, эти отчеты не содержат конфиденциальных данных, таких как, например, ваше имя, IP-адрес. Также они не могут быть использованы в каких-либо коммерческих целях.

В случае, если вы хотите прекратить отправку анонимных отчетов об использовании:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **РАСШИРЕННЫЙ**
3. Нажмите соответствующий переключатель.

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 на иконку в нижнем левом углу Bitdefender interface.
2. В окне **ОБЩИЕ**, выберите соответствующий переключатель вкл/выкл.

Опция специальные предложения и уведомления о продуктах включена по умолчанию.

2.2. Интерфейс Bitdefender

Bitdefender Total Security 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 **ДАЛЕЕ**, чтобы продолжить выполнение руководства, или **Пропустить**, чтобы закрыть мастер.

Значок Bitdefender в system tray icon позволяет в любой момент времени просмотреть состояние продукта и предоставляет доступ к основным задачам.

Окно Главное окно позволяет управлять поведением продукта с помощью Автопилот, предоставляет доступ к важной информации о продукте и позволяет выполнять общие задачи. С левой боковой панели Вы можете получить доступ к учетной записи Bitdefender акаунт и

Bitdefender разделы для подробной настройки и расширения административных задач.

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

Значок системный трей

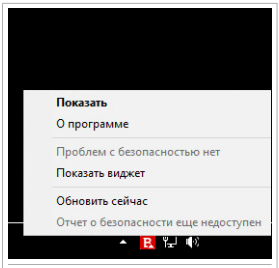
Чтобы быстрее управлять всем продуктом, в системном трее можно использовать значок Bitdefender .

Замечание

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.



Иконка Трея

- **Показать** - открытие главного окна Bitdefender.
- **О программе** - открывает окно, где можно просмотреть информацию о Bitdefender и о том, где искать помощь в случае непредвиденных обстоятельств.
- **Просмотр проблем безопасности** -помогает удалить текущие уязвимости системы безопасности. Если опция недоступна, значит проблем, требующих решения, нет. Для получения дополнительной информации перейдите к «Устранение неисправностей» (p. 14).
- **Скрыть / Показать Виджет Безопасности** - включает / отключает Виджет Безопасности.
- **Обновить сейчас** - запускает немедленное обновление. Состояние обновления можно увидеть на панели "Обновления" в главном Bitdefender окне.
- **Показать отчет о безопасности** - открывает окно, где Вы можете видеть еженедельный статус и рекомендации для вашей системы. Вы можете следовать рекомендациям по улучшению безопасности Вашей системы.

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

Критические проблемы влияют на безопасность вашей системы. Они требуют немедленного вмешательства и должны быть исправлены как можно скорее.
Некритические проблемы влияют на безопасность системы. Их следует проверить и исправить в ближайшее время.
Задействована функция Автопилот в Bitdefender.

Если Bitdefender не работает, значок в области уведомления отображается на сером фоне: . 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.

Главное окно

Главное окно Bitdefender позволяет выполнять типичные задачи, быстро устранять проблемы безопасности, просматривать информацию о работе продукта и получать доступ к панелям, из которых Вы настраиваете параметры продукта. Вам требуется всего несколько раз нажать мышью.

Окно разделено на четыре основные области:

Область состояния
: Здесь вы можете проверить состояние безопасности Вашего компьютера, запустить обновление и настроить Автопилот.

Левая боковая панель инструментов
: Это меню позволяет получать доступ и управлять Bitdefender учетная запись вместе с онлайн-функциями вашего продукта или переключаться между тремя основными разделами продукта. Отсюда Вы можете также получить доступ к Уведомления, к еженедельному Отчет о безопасности, Общим настройкам и области Помощь & Поддержка.

Кнопки действий и доступ к области функций
: Здесь вы можете запускать различные задачи, чтобы сохранить защиту вашей системы и работать с оптимальной скоростью. Кроме того, можно получить доступ к функциям Bitdefender для настройки продукта самостоятельно.

Нижняя панель
: Здесь вы можете легко установить Bitdefender на другие устройства, при условии, что Ваша подписка имеет достаточно доступных слотов.

Область состояния

Область состояния содержит следующие элементы:

- **Состояние Безопасности** на левой стороне области, информирует о наличии каких-либо проблем, влияющих на безопасность Вашего компьютера и помогает исправить их.

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

- **Область выделена зеленым цветом.** Проблемы отсутствуют. Ваш компьютер и данные защищены.
- **Область выделена желтым цветом.** Некритические проблемы влияют на безопасность системы. Их следует проверить и исправить в ближайшее время.
- **Область выделена красным цветом.** Критические проблемы влияют на безопасность системы. Эти проблемы следует разрешить незамедлительно.

Щелкнув в любом месте области состояния безопасности, можно получить доступ к мастеру, который поможет легко удалить все угрозы с компьютера. Для получения дополнительной информации перейдите к «Устранение неисправностей» (p. 14).

- **АВТОПИЛОТ** позволяет осуществлять оптимальную защиту и пользоваться полностью тихой безопасностью. Для получения дополнительной информации перейдите к «Автопилот» (p. 17).
- **ОБНОВИТЬ СЕЙЧАС** позволяет запускать обновление продукта, когда Вы хотите убедиться в том, имеются ли у Вас последние сигнатуры вредоносных программ. Для получения дополнительной информации перейдите к «*Поддержка Bitdefender в обновленном состоянии*» (p. 46).
- **Активный Профиль** отображает текущий профиль, включенный в продукте Bitdefender. Для получения дополнительной информации перейдите к «*Профили*» (p. 192).

Левая боковая панель инструментов

Наводящие значки доступны на левой боковой панели, предоставляют доступ к учетной записи Bitdefender, разделам продукта, отчету о деятельности, уведомлениям, общим настройкам и поддержке.

Имена значков видны, щелкнув☰ значок, как показано ниже:

- **Защита**. Кнопки действия **Быстрое Сканирование** и **Сканирование Уязвимостей** будут видны в левом нижнем углу интерфейса Bitdefender. Также видна информация о заблокированных приложениях, обнаруженных угрозах и атаках. Щелкните **ПРОСМОТР ФУНКЦИЙ** для доступа к области конфигурации.

- **Приватность**. Кнопки быстрых действий **Безопасный платеж** и **Родительский контроль** становятся видимыми в левом нижнем углу интерфейса Bitdefender. Кроме того, отображается информация об обнаруженных кошельках и хранилищах файлов. Щелкните **ПРОСМОТР ФУНКЦИЙ** для доступа к области конфигурации.

- **Инструменты**. Кнопки быстрых действий **Оптимизация в один клик** и **Оптимизация запуска** становятся видимыми в левом нижнем углу интерфейса Bitdefender. Кроме того, отображается информация об оптимизированном пространстве и функция **Очистка диска** может быть запущена для создания места для новых данных путем стирания больших файлов и папок, которые вы не используете больше. Кроме того, доступна функция Анти-вора.

- **Действия**. Отсюда вы можете просматривать активность вашего продукта в течение последних 30 дней и получить доступ к отчету о безопасности, который генерируется каждые семь дней.

- **Уведомления**. Отсюда вы получаете доступ к сгенерированным уведомлениям.

- **Аккаунт** Подробности об аккаунте Bitdefender и доступные к использованию подписки. Перейдите в аккаунт Bitdefender чтобы проверить подписки и выполнять задачи по обеспечению безопасности на устройствах, которыми вы управляете.

- **Параметры**. Отсюда Вы можете получить доступ к общим настройкам.

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

Кнопки действий и доступ к области функций

С помощью кнопки быстрого действия вы можете быстро запускать важные задачи. Кнопки действий становятся видимыми в левом нижнем углу интерфейса Bitdefender при выборе одного из трех разделов: **Безопасность**, **Приватность** или **Инструменты** с левой боковой панели.

В зависимости от выбранного раздела, кнопки действий, видимые в этой области, могут быть:

- **Быстрое Сканирование**. Запустите быстрое сканирование чтобы убедиться, что компьютер очищен от вредоносных программ.
- **Сканирование Уязвимостей**. Проверьте компьютер на наличие уязвимостей, чтобы убедиться, что все установленные приложения, вместе с операционной системой, обновляются и должным образом функционируют.
- **Безопасный платеж**. Откройте Bitdefender Safepay™, чтобы защитить ваши конфиденциальные данные во время онлайн-транзакций.
- **VPN**. Откройте Bitdefender VPN, чтобы добавить дополнительный уровень защиты при подключении к Интернету
- **Оптимизация в один клик**. Освобождение места на диске, исправление ошибок реестра и защита Ваших персональных данных, путем удаления файлов, которые больше не нужны, одним нажатием кнопки.
- **Оптимизация загрузки**. Уменьшите время загрузки системы, исключив ненужные приложения из загрузки при запуске.

Нижняя панель

Чтобы начать защиту дополнительных устройств:

1. Нажмите ссылку **УСТАНОВИТЬ НА ДРУГОЕ УСТРОЙСТВО** .

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

2. В появившемся окне выберите нужную операционную систему и нажмите **ПРОДОЛЖИТЬ** .

3. Введите адрес электронной почты, на который следует отправить ссылку для загрузки установки выбранной платформы.

В зависимости от вашего выбора будут установлены следующие продукты Bitdefender:

- Bitdefender Total Securityна устройствах на базе Windows.
- Bitdefender Антивирус для Mac на устройствах на базе macOS.
- Bitdefender Мобильная безопасность & антивирус на устройствах на базе Android.
- Bitdefender Мобильная безопасность на устройствах на базе iOS.

- Bitdefender Родительский Контроль на macOS, iOS и устройствах на базе Android.

Разделы Bitdefender

Продукт Bitdefender поставляется с тремя разделами, разделенными на полезные функции, которые помогут вам оставаться защищенными во время работы, веб-серфинга или совершения онлайн-платежей, улучшить скорость системы и многое другое.

Всякий раз, когда вы хотите получить доступ к функциям для конкретного раздела или для начала настройки продукта, перейдите к следующим значкам, расположенным на левой боковой панели Bitdefender интерфейс:

- Защита
- Приватность
- Инструменты

Защита

В разделе Защита вы можете настроить Расширенные настройки безопасности, управлять друзьями и спамерами, просматривать и редактировать настройки сетевого подключения, настраивать безопасные файлы и функции веб-защиты, проверять и устранять потенциальные уязвимости системы и оценивать Безопасность беспроводных сетей, к которым вы подключаетесь.

Функции, которыми вы можете управлять в разделе Защита:

АНТИВИРУС

Антивирусная защита — это основа вашей безопасности. Bitdefender обеспечивает защиту в реальном времени и по запросу от всех типов вредоносного ПО, включая вирусы, трояны, шпионские, рекламные программы 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. 92).

ВЕБ-ЗАЩИТА

Веб-защита помогает вам оставаться защищенным от фишинг-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 «*Веб-защита*» (p. 118).

БРАНДМАУЭР

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

Дополнительные сведения о конфигурации брандмауэра см. в «*Брандмауэр (Firewall)*» (p. 130).

АКТИВНЫЙ КОНТРОЛЬ УГРОЗ

Активный Контроль Угроз эффективно защищает вашу систему от вредоносных программ, таких как вымогателей, шпионских программ и троянов, анализируя поведение всех установленных приложений. Подозрительные процессы идентифицируются и, при необходимости, блокируются.

Для получения дополнительной информации о том, как защитить вашу систему от вредоносного ПО, пожалуйста, обратитесь в«*АКТИВНЫЙ КОНТРОЛЬ УГРОЗ*» (p. 116).

АНТИСПАМ

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

Для получения более подробной информации о защите от спама, пожалуйста, обратитесь «*Антиспам*» (p. 120).

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 **Советник Безопасности Wi-Fi**, чтобы просмотреть список беспроводных сетей, к которым вы подключаетесь, вместе с оценкой репутации каждого из них и действиями, которые вы можете предпринять, чтобы оставаться в безопасности от потенциальных ищеек .

Для получения более подробной информации о настройке защиты от уязвимостей, пожалуйста, обратитесь в «*Уязвимости*» (p. 136).

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. «*Безопасные файлы*» (p. 147).

Приватность

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. 162).

ШИФРОВАНИЕ ФАЙЛОВ

Создание зашифрованных, защищенных паролем логических дисков (или хранилища) на вашем компьютере, где можно безопасно хранить ваши конфиденциальные и секретные документы.

Для получения более подробной информации о том, как создать в зашифрованном виде, защищенные паролем логические диски (или хранилища) на вашем компьютере, пожалуйста, обратитесь «*Шифрование файла*» (p. 150).

ЗАЩИТА ВЕБ-КАМЕРЫ

BitdefenderЗащита веб-камеры обеспечивает безопасность веб-камеры, блокируя доступ к ненадежным приложениям.

Для получения дополнительной информации о том, как защитить веб-камеру от нежелательного доступа, обратитесь в«*Защита веб-камеры*» (p. 144).

МЕНЕДЖЕР ПАРОЛЕЙ

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

Дополнительные сведения о настройке Менеджер Паролей см. «*Защита ваших учетных данных при помощи Менеджер паролей*» (p. 155).

БЕЗОПАСНЫЙ ПЛАТЕЖ

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

Нажмите **Безопасный платеж** из интерфейса Bitdefender, чтобы начать онлайн-транзакцию в безопасной среде.

Для получения более подробной информации о Bitdefender Safepay™, пожалуйста, обратитесь «*Безопасный платеж - безопасность для онлайн-транзакций*» (p. 165).

РОДИТЕЛЬСКИЙ КОНТРОЛЬ

Родительский контроль Bitdefender позволяет контролировать действия Вашего ребенка на компьютере. В случае ненадлежащего содержания (контента), вы можете ограничить его доступ к сети Интернет или к определенным приложениям.

Нажмите **Настроить**, на панели Родительский контроль, чтобы приступить к настройке устройств ваших детей и контролировать их действия, где бы вы не находились.

Дополнительную информацию по настройке родительского контроля см. в «*Родительский контроль*» (p. 171).

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. 170).

Инструменты

В разделе Инструменты можно улучшить скорость работы системы и управлять вашими устройствами.

Настройка системы

Bitdefender Total Security не только обеспечивает защиту, но также помогает поддерживать компьютер в работоспособном состоянии.

В функции Настройка вы можете получить доступ к ряду полезных инструментов:

- Оптимизация в один клик
- Оптимизация загрузки
- Очистка диска

Дополнительные сведения об инструментах оптимизации производительности см. в «*Инструменты*» (p. 189).

Анти-вор

Bitdefender Анти-вор защищает ваш компьютер и данные от кражи или потери. В случае такого события, это позволяет удаленно найти или заблокировать компьютер. Вы также можете стереть все данные, находящиеся в вашей системе.

Bitdefender Анти-вор предлагает следующие возможности:

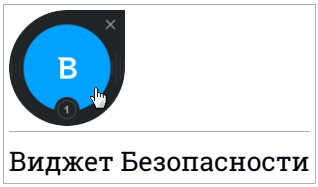
- Удаленный поиск
- Удаленная блокировка
- Удаленное стирание
- Удаленное Оповещение

Для получения более подробной информации о том, как вы можете защитить вашу систему от "плохих" рук, пожалуйста, обратитесь «*Устройство Анти-вор* » (p. 185).

Виджет Безопасности

Виджет безопасности является быстрым и простым способом для контроля и управления Bitdefender Total Security. 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 дополнительной информации, пожалуйста, перейдите «Уведомления» (p. 16).

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.

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 системного трея:

1. Правой кнопкой мыши щелкните по значку Bitdefender в системный трей.
2. Нажмите **Виджет безопасности** в появившемся контекстном меню.

- Из интерфейса Bitdefender:

1. Нажмите на  иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ОБЩИЕ**.
3. Нажмите на соответствующий переключатель **Отобразить Виджет безопасности**, чтобы включить виджет.

Виджет безопасности Bitdefender по умолчанию отключен.

Действие

Окно Действия отображает информацию о действиях, предпринятых Bitdefender на устройстве в течение последних 30 дней. Здесь вы можете проверить какие были заблокированы приложения, угрозы и атаки в этот период, и были ли попытки атак вирусов-вымогателей.

Кроме того, Вы можете открыть панель Bitdefender Central действия, нажав на соответствующую ссылку.

Нажав на соответствующую ссылку можно также получить Отчет о безопасности, который предоставляет еженедельную сводку для вашего продукта и различные советы по улучшению защиты системы. Эти подсказки необходимы для управления общей защитой и позволяют вам легко посмотреть решения, которые вы можете принять для вашей системы.

Отчет обычно генерируется один раз в неделю и содержит необходимую информацию о действиях вашего продукта, чтобы вы могли быстро понять, что произошло за этот период.

Информация, представленная на Отчете безопасности делится на три категории:

- Область **Защита** - вид информации, связанной с защитой Вашей системы.
  - **Сканированные файлы**

Позволяет просмотреть файлы, сканированные Bitdefender за неделю. Вы можете просмотреть такие сведения, как количество проверенных файлов и количество файлов, очищенных Bitdefender.

Дополнительная информация по антивирусной защите представлена в «*Антивирусная защита*» (p. 92).

- **Отсканированные веб-страницы**

  Позволяет проверить количество веб-страниц, сканированных и блокированных Bitdefender. Для того, чтобы личная информация не разглашалась во время загрузки, Bitdefender обеспечивает безопасность вашего веб-трафика.

  Для получения более подробной информации о Веб-защите, пожалуйста, обратитесь «*Веб-защита*» (p. 118).

- **Уязвимости**

  Позволяет легко выявить и устранить уязвимости в системе для того, чтобы максимально защитить Ваш компьютер от вредоносных программ и хакеров.

  Для получения более подробной информации о сканировании уязвимостей, пожалуйста, обратитесь «*Уязвимости*» (p. 136).

- **Хронология событий**

  Позволяет получить общее представление обо всех процессах сканирования и проблемах, зафиксированных Bitdefender в течение недели. События разделяются по дням.

  Дополнительные сведения о подробном журнале событий, касающихся действий на компьютере, см. «Уведомления» (p. 16).

- Область **Приватность** - показывает информацию, связанную с приватностью вашей системы.

  - **Хранилище файлов**

    Позволяет просматривать, сколько файлов защищено от нежелательного доступа.

    Чтобы найти более подробную информацию о том, как создать в зашифрованном виде, защищенные паролем логические диски (или хранилища) на вашем компьютере, пожалуйста, обратитесь «*Шифрование файла*» (p. 150).

- Раздел **Оптимизация** - просматривает информацию, связанную с очищенным пространством, количеством оптимизированных приложений и сколько батареи компьютера вы сохранили с помощью профиля Battery Mode.
  - **Очищенное пространство**

    Позволяет просматривать, сколько мест было очищено в процессе оптимизации системы. Bitdefender использует Настройку, чтобы помочь улучшить скорость системы.

    Для получения более подробной информации о Настройке, пожалуйста, обратитесь «*Инструменты*» (p. 189).
  - **Экономия батареи**

    Позволяет видеть, сколько батареи вы сохранили в то время как система работала используя профиль Режим батареи.

    Для получения более подробной информации о профиле Режим батареи, пожалуйста, обратитесь «Профиль Режим работы от батарей» (p. 198).
  - **Оптимизированные приложения**

    Позволяет увидеть количество приложений, используемых в Профилях.

    Для получения дополнительной информации о Профилях, пожалуйста, обратитесь к «*Профили*» (p. 192).

Проверка Отчета о безопасности

Отчет по безопасности использует систему отслеживания проблем для обнаружения и оповещения о событиях, которые могут повлиять на безопасность компьютера и данных. К обнаруженным проблемам относится отключение важных параметров настроек защиты и другие условия, представляющие угрозу безопасности. С помощью отчета можно настраивать определенные компоненты Bitdefender или предпринимать профилактические действия для защиты компьютера и личных данных.

Чтобы проверить отчет по безопасности:

1. Доступ к отчету:
   - Нажмите на  иконку в нижнем левом углу Bitdefender interface.

Нажмите ссылку **Отчет безопасности**, расположенную в нижнем правом углу окна Отчет о действиях.

- Правой кнопкой мыши щелкните по значку Bitdefender в области уведомления и выберите **Показать отчет безопасности**.
- После того, как отчет будет готов, появится всплывающее окно с уведомлением. Нажмите **Показать** для доступа к отчету о действиях.

  Откроется веб-страница в вашем веб-браузере, где вы сможете посмотреть отчет.

2. В верхней части окна отобразиться информация об общем состоянии системы безопасности.
3. Проверьте наши рекомендации в нижней части страницы.

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

- **Область выделена зеленым цветом.** Проблемы отсутствуют. Ваш компьютер и данные защищены.
- **Желтая зона.** Некритические угрозы безопасности системы. Их следует проверить и исправить в ближайшее время.
- **Область выделена красным цветом.** Критические проблемы влияют на безопасность системы. Эти проблемы следует разрешить незамедлительно.

Включение / отключение уведомлений о состоянии системы безопасности.

Включение / отключение уведомлений о состоянии системы безопасности:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. В окне **ОБЩИЕ**, выберите соответствующий переключатель вкл/выкл.

   Уведомление Отчета о состоянии системы безопасности всплывает по умолчанию.

2.3. Bitdefender Central

Bitdefender Central это веб-платформа, на которой у Вы имеете доступ к онлайн-функциям и услугам, а также можете удаленно выполнять важные задачи на устройствах, на которых установлен Bitdefender. Вы можете войти в учетную запись Bitdefender с любого компьютера или мобильного устройства, подключенного к сети Интернет, перейдя https://central.bitdefender.com. 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 Total Security
  - Антивирус Bitdefender для Mac
  - Bitdefender Мобильная безопасность & Антивирус для Android
  - Bitdefender Мобильная безопасность для iOS
  - Bitdefender Родительский контроль
- Управление и обновление своей Bitdefender подпиской.
- Добавлять новые устройства к сети и управлять ими, где бы вы не находились.
- Защитите сетевые устройства и их данные от кражи или потери с Анти-вор.
- Настройте Родительский контроль для учетных записей Ваших детей, и контролируйте их действия, где бы Вы не находились.
- Получите доступ к отчету Действия, чтобы просмотреть статус Вашей текущей подписки и устройств, добавленных в Вашу сеть, и в случае необходимости дистанционно повысить производительность Ваших устройств на базе Windows.

Доступ к Bitdefender Central

Есть несколько способов доступа к Bitdefender Central. В зависимости от задачи, которую вы хотите выполнить, вы можете использовать любую из следующих возможностей:

- Из интерфейса Bitdefender:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **Перейти 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 в Интернет.
  2. Перейти к: https://central.bitdefender.com.
  3. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.

Мои подписки

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

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.

Замечание

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

Добавить новое устройство

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

1. Войдите в ваш Bitdefender Central.

2. Выберите **Мои устройства** на панели справа.
3. В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.
4. Выберите одну из двух доступных опций:

   - **Загрузка**

     Нажмите на кнопку и сохраните установочный файл.

   - **На другое устройство**

     Выберите **Windows**, чтобы скачать Bitdefender и затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.

5. Подождите окончания загрузки, затем запустите программу установки.

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.

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 **АКТИВИРОВАТЬ КОД**, чтобы продолжить.

Подписка активирована. Перейдите в панель **Мои устройства** и выберите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**, чтобы установить продукт на одном из Ваших устройств.

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**.

В случае если Автопилот выключен, вы можете включить его, нажав переключатель. Нажмите **СОХРАНИТЬ** чтобы применить изменения.

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:

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. 100) и «Запуск быстрого сканирования» (p. 100).

- **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 более подробной информации об этой функции, пожалуйста, обратитесь «*Уязвимости*» (p. 136).

Действие

Область Действия в Bitdefender Central доступна только для пользователей подписки Bitdefender Family Pack 2018 или Bitdefender Total Security 2018, связанную с их учетными записями. Его роль заключается в том, чтобы сообщать о защите Bitdefender подключенных устройств, в течение последних семи дней, и показывать сведения о включенной подписке.

После доступа к окну **ДЕЙСТВИЯ** доступны следующие карточки:

- **Защита**. Здесь Вы можете просмотреть информацию о файлах, приложениях и URL-адресах, которые были заблокированы из-за подозрительного поведения. Ознакомится с возникшими проблемами можно в представленных графиках, отображающих собранные данные, разделенные по дням и количеству обнаруженных угроз. Также Вы можете переместить указатель мыши на отображаемые данные, чтобы узнать количество обнаруженных угроз.

  В нижней части карты можно заметить название устройства с наибольшим количеством угроз.

- **Настройка** Здесь вы можете оптимизировать производительность устройств Windows, на которых установлена программа Bitdefender

Total Security. функция Оптимизация запуска Bitdefender отображает информацию о работающих приложениях во время запуска системы и позволяет управлять их поведением на этом этапе. В зависимости от решений, принятых сообществом, применив команду **Отложить**, будут отображены только три верхних устройства. Нажмите **Применить**, чтобы внести предлагаемые изменения на выбранное устройство.

Чтобы увидеть другие Bitdefender пользовательские решения,нажмите ссылку, отображающую количество обнаруженных приложений и сэкономленное время Отображена информация о времени загрузки системы, приложений и оптимизированном времени. Выберите **Отложить все** , если хотите остановить их при запуске. Дополнительные сведения о функции Bitdefender Оптимизации запуска см.«Оптимизация времени загрузки ПК» (p. 190).

Замечание

Если на Ваших устройствах Windows не установлена защита Bitdefender, карта **Настройки** не содержит никакой информации.

- **Подписка** Здесь Вы можете узнать, сколько устройств охватывает Ваша подписка и на сколько устройств установлена защита Bitdefender. Для установки Bitdefender на другие устройства, нажмите кнопку **УСТАНОВИТЬ** в желаемой операционной системе и выполните необходимые шаги.

  Имя используемой подписки отображается вместе с цветной точкой:

  - Фиолетовый - ваша подписка активна.
  - Красный - срок действия Вашей подписки истекает. Для продолжения защиты устройств рекомендуется как можно скорее обновить его.

  Нажмите ссылку **Подробнее**, чтобы перейти на страницу **Подписки** , где можно просмотреть подробную информацию о Вашей активной подписке.

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.

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.

2.4. Поддержка Bitdefender в обновленном состоянии

Каждый день обнаруживаются новые вредоносные программы. Именно поэтому очень важно обновлять Bitdefender, чтобы получить последние сигнатуры вредоносных программ.

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. 85).
- При низкой скорости подключения к Интернету во время загрузки обновлений могут возникать ошибки. Инструкции по устранению таких ошибок см. в *«Обновление Bitdefender при низкой скорости подключения к Интернету»* (p. 211).
- Если вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять Bitdefender по запросу. Для получения дополнительной информации перейдите к «Выполнение обновления» (p. 48).

Проверьте, установлены ли последние обновления Bitdefender

Чтобы проверить время последнего обновления вашего Bitdefender, посмотрите **Состояние безопасности**, на левой стороне панели раздела Состояние.

Для получения дополнительной информации о последних обновлениях, просмотрите события обновления:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
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.

Выполнение обновления

Для выполнения обновления требуется подключение к Интернету.

Для того, чтобы запустить обновление, выполните одно из следующих действий:

- Откройте интерфейс Bitdefender и нажмите ссылку **ОБНОВИТЬ СЕЙЧАС** расположенную под статусом вашей программы.
- Правый клик на Bitdefender иконку в системный трей 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:

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.
3. Нажмите иконку желаемой карточки устройства, затем выберите **Обновить**.

Включение и отключение автоматического обновления

Чтобы включить или выключить автоматическое обновление:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ОБНОВИТЬ**.
3. Нажмите 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.

Внимание

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.

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 на  иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ОБНОВИТЬ** 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 местоположение

В Bitdefender настроено получение обновлений с серверов обновлений Bitdefender в Интернете. Обновления доступны на веб-сайте, при открытии которого автоматически происходит перенаправление на ближайший сервер обновлений Bitdefender в вашем регионе.

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

Можно вернуться к общему местоположению обновления Интернета, щелкнув **ПО УМОЛЧАНИЮ**.

Обновить правила обработки

Предусмотрено три способа загрузки и установки обновлений:

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

Для завершения установки некоторых обновлений требуется перезагрузка. По умолчанию если обновление требует 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, чтобы система выдавала запрос, когда обновление требует перезагрузки, отключите параметр **Postpone reboot**, нажав на соответствующий переключатель.

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 инициировать 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.

Замечание

Обновления, включая новые функции и усовершенствования, будут доставлены только пользователям, у которых установлен Bitdefender 2017.

3. СОВЕТЫ

3.1. Установка

3.1.1. 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 ссылку **УСТАНОВИТЬ НА ДРУГОЕ УСТРОЙСТВО** в нижнем правом углу интерфейса Bitdefender.

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

2. В появившемся окне выберите нужную операционную систему и нажмите **ПРОДОЛЖИТЬ** .

3. Введите адрес электронной почты, на который следует отправить ссылку для загрузки установки выбранной платформы.

4. Запустите Bitdefender продукт, который вы скачали. Дождитесь завершения процесса установки и затем закройте окно.

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

3.1.2. 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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
  5. Щелкните **УДАЛИТЬ**.
  6. Для завершения процесса необходимо перезагрузить компьютер.

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

3.1.3. 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.

Замечание
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 **Мои устройства** на панели справа.
3. В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.
4. Выберите одну из двух доступных опций:
   - **Загрузка**

     Нажмите на кнопку и сохраните установочный файл.
   - **На другое устройство**

     Выберите **Windows**, чтобы скачать Bitdefender и затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.
5. Запустите Bitdefender продукт, который вы скачали.

3.1.4. 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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
     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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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 **Мои устройства** на панели справа.
   b. В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.

c. Выберите одну из двух доступных опций:

- **Загрузка**

  Нажмите на кнопку и сохраните установочный файл.

- **На другое устройство**

  Выберите **Windows**, чтобы скачать Bitdefender и затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.

4. Запустите Bitdefender продукт, который вы скачали.

Замечание
Эта процедура переустановки навсегда удалит настроенные параметры.

3.1.5. 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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
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.

Замечание
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 **Мои устройства** на панели справа.
     c. В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.
     d. Выберите одну из двух доступных опций:
        - **Загрузка**

          Нажмите на кнопку и сохраните установочный файл.
        - **На другое устройство**

          Выберите **Windows**, чтобы скачать Bitdefender и затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.
  2. Запустите Bitdefender продукт, который вы скачали.

  Для получения дополнительной информации о процессе установки Bitdefender, пожалуйста, обратитесь к «*Установка продукта Bitdefender*» (p. 4).

3.1.6. Как перейти к последней версии Bitdefender?

Начиная с Bitdefender 2018, обновление до новейшей версии возможно без выполнения процедуры ручного удаления и повторной установки. 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 используется версия 2017, можно выполнить обновление 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.

3.2. Подписки

3.2.1. 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 Total Security, есть два возможных варианта:

- Вы обновили предыдущую версию Bitdefender на новую:

  1. После завершения обновления до Bitdefender Total Security 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 Total Security.
4. Нажмите на иконку в нижнем левом углу Bitdefender interface.
5. Нажмите ссылку **Активировать код**.

   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.

3.3. Bitdefender Central

3.3.1. 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 на иконку в нижнем левом углу Bitdefender interface.

2. Нажмите кнопку **ПОМЕНЯТЬ УЧЕТНУЮ ЗАПИСЬ**, чтобы изменить учетную запись, связанную с компьютером.
3. Введите адрес электронной почты и пароль Вашей учетной записи в соответствующие поля, затем нажмите **ВОЙТИ**.

Замечание
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. 330).

3.3.2. 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**.

3.3.3. 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 на иконку в нижнем левом углу Bitdefender interface.
  2. Нажмите кнопку **ПЕРЕКЛЮЧИТЬ УЧЕТНУЮ ЗАПИСЬ**.

     Появится новое окно.

3. Нажмите на ссылку **Забыл пароль**.
4. Введите адрес электронной почты, используемый для создания учетной записи Bitdefender, а затем нажмите кнопку **ЗАБЫЛИ 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 кнопку **СБРОС ПАРОЛЯ**.

- Из вашего веб-браузера:
  1. Перейти к: https://central.bitdefender.com.
  2. Нажмите на ссылку **Забыл пароль**.
  3. Введите адрес Вашей электронной почты, затем нажмите кнопку**ЗАБЫЛИ 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.

3.3.4. 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

3.4. Сканирование с Bitdefender

3.4.1. 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.

3.4.2. Как выполнить сканирование системы?

Чтобы выполнить полную проверку системы:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Системное сканирование**.
4. 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 дополнительной информации перейдите к «Мастер антивирусного сканирования» (p. 105).

3.4.3. 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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.
4. 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 **Создать новую задачу**.
5. Включить переключатель **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

3.4.4. 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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.
4. Нажмите **Новая задача сканирования**. В вкладке **Основное**введите имя для сканирования и выберите сканируемые местоположения.
5. 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.
6. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.
7. Используйте соответствующий переключатель, если требуется задать расписание для задачи сканирования.
8. Нажмите **Начать сканирование** и следуйте инструкциям мастера сканирования чтобы выполнить проверку. На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).
9. При желании можно быстро перезапустить предыдущее пользовательское сканирование, щелкнув соответствующую запись в доступном списке.

3.4.5. Как исключить папку из сканирования?

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

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

- У вас имеется большая папка в системе, в которой хранятся фильмы и музыка.

- У вас имеется большой архив в системе, в котором хранятся различные данные.
- У вас имеется папка для установки разных типов программного обеспечения и приложений в целях тестирования. В результате сканирования папки некоторые данные могут быть потеряны.

Чтобы добавить папку в список исключений:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Выберите вкладку **ИСКЛЮЧЕНИЯ**.
5. Нажмите **Список файлов и папок, исключенных из сканирования** из соответствующего меню, а затем кнопку **ДОБАВИТЬ**.
6. Нажмите **Обзор** , выберите папку, которую Вы хотите исключить из сканирования, а затем выберите тип сканирования, из которого она должна быть исключена.
7. Нажмите **Добавить** чтобы сохранить изменения и закрыть окно.

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

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

1. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Нажмите на иконку в нижнем левом углу Bitdefender interface.
   b. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
   c. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
   d. В окне **ЩИТ** нажмите переключатель ВКЛ/ВЫКЛ.

      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. Инструкции для этой процедуры см. в «*Как отобразить скрытые объекты в Windows?*» (p. 87).
3. Восстановление файла из области карантина:
   a. Нажмите на иконку в нижнем левом углу Bitdefender interface.
   b. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
   c. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
   d. Выберите вкладку **Карантин**.
   e. Выберите файл и затем нажмите **ВОССТАНОВИТЬ**.
4. Добавьте файл в список исключений. Инструкции для этой процедуры см. в «*Как исключить папку из сканирования?*» (p. 65).
5. Включить антивирусную защиту Bitdefender в режиме реального времени.
6. Свяжитесь с нашей службой поддержки, и мы удалим сигнатуру обнаружения. Инструкции для этой процедуры см. в «*Обращение за помощью*» (p. 330).

3.4.7. Как проверить, какие вирусы обнаружил 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 на иконку в нижнем левом углу Bitdefender interface.

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

   Здесь можно просмотреть все события сканирования на вирусы, включая угрозы, обнаруженные при резидентном сканировании, 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 **ПРОСМОТРЕТЬ ЖУРНАЛ**.

3.5. Родительский контроль

3.5.1. Как защитить детей от интернет-угроз?

Bitdefender Родительский контроль позволяет ограничивать доступ к Интернету и конкретным приложениям, не позволяя детям просматривать неуместный контент, когда вас нет рядом.

Чтобы настроить Родительский контроль:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **Родительский контроль**, выберите **Настроить**.

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

4. Будет открыта информационная панель "Родительского контроля". Здесь вы можете проверять и управлять параметрами Родительского контроля.
5. Нажмите **ДОБАВИТЬ ПРОФИЛЬ** на правой стороне окна **МОИ ДЕТИ**.
6. Укажите конкретную информацию в соответствующих полях, например: имя и дата рождения. Чтобы добавить фотографию профиля, нажмите ссылку **Выбрать файл** . Для продолжения нажмите **ДАЛЕЕ**

Основываясь на стандартах развития детей, установки даты рождения ребенка автоматически загружает настройки для поиска в Интернете, которые считаются подходящими для его возрастной категории.

7. Если на устройстве вашего ребенка уже установлен Bitdefender Total Security, выберите его устройство из списка доступных, а затем выберите учетную запись, которую вы хотите контролировать. Нажмите **СОХРАНИТЬ**.

   Если Ваш ребенок использует Android или iOS устройства и Bitdefenderприложение Родительский Контроль не установлено, нажмите кнопку **Добавить устройство**. Если Ваш ребенок использует устройство Mac и приложение Bitdefender Антивирус для Mac не установлено, нажмите ту же кнопку. Выберите операционную систему, которую хотите установить, и нажмите **ДАЛЕЕ**, чтобы продолжить.

8. Введите адрес электронной почты на которую мы отправим ссылку на скачивание, чтобы установить в Bitdefender приложение, затем нажмите **ОТПРАВИТЬ ССЫЛКУ ДЛЯ УСТАНОВКИ**.

Проверьте действия своих детей и измените настройки Родительского контроля с помощью учетной записи Bitdefender с любого компьютера или мобильного устройства, подключенного к Интернету.

Важно

На устройствах под управлением Windows необходимо загрузить и установить Bitdefender Total Security, включенный в вашу подсылку.
На устройствах на базе MacOS необходимо загрузить и установить продукт Bitdefender Антивирус для Mac.
На устройствах Android и iOS необходимо загрузить и установить приложение Bitdefender Родительский Контроль.

3.5.2. Как заблокировать доступ моего ребенка к веб-сайту?

Bitdefender Родительский контроль позволяет контролировать и блокировать доступ к веб-сайтам Ваших детей через Ваше устройство.

Чтобы заблокировать доступ к веб-сайту, вы должны добавить его в Список исключений, а именно:

1. Перейти к: https://central.bitdefender.com.

2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
3. Нажмите **Родительский контроль** для доступа к панели управления.
4. Выберите профиль своего ребенка в окне **МОИ ДЕТИ**.
5. Выберите на вкладке **ВЕБ-САЙТЫ**.
6. Нажмите кнопку **УПРАВЛЕНИЕ**.
7. Введите веб-страницу, которую вы хотите заблокировать, в соответствующем поле.
8. Выберите **Разрешить** или **Заблокировать**.
9. Нажмите **ЗАВЕРШИТЬ**, чтобы сохранить изменения.

Замечание
Ограничения могут быть установлены только для устройств на базе Android и Windows.

3.5.3. Как запретить игру?

Bitdefender Родительский контроль позволяет контролировать содержимое, доступное вашему ребенку при пользовании компьютером.

Чтобы заблокировать доступ к игре:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
3. Нажмите **Родительский контроль** для доступа к панели управления.
4. Выберите профиль своего ребенка в окне **МОИ ДЕТИ**.
5. Выберите вкладку **Приложения**.

   Отобразится список с карточками. Карточки представляют собой приложения, которые использует ваш ребенок.
6. Выберите карточку с тем приложением, которое хотите запретить для ребенка.

   Появится символ галочка, который означает, что ваш ребенок не сможет использовать данное приложение.

3.5.4. Как предотвратить контактирование ребенка с недоверенными лицами?

Bitdefender Родительский контроль предоставляет Вам возможность блокировать телефонные звонки с неизвестных телефонных номеров или от друзей из списка телефонов вашего ребенка.

Чтобы заблокировать определенный контакт на устройстве Android, на котором установлено приложение Bitdefender Родительский Контроль:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
3. Нажмите **Родительский контроль** для доступа к панели управления.
4. Выберите профиль ребенка, на котором вы хотите установить ограничения.
5. Выберите вкладку **Телефонные контакты** .

   Отобразится список с карточками. Карточки отобразят контакты с телефона вашего ребенка.
6. Выберите карточку с номером телефона, который хотите заблокировать.

   Появиться символ галочка, который означает, что ваш ребенок не сможет использовать выбранный номер телефона.

Чтобы заблокировать определенный контакт на устройстве Android, на котором установлено приложение Bitdefender Родительский Контроль:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
3. Нажмите **Родительский контроль** для доступа к панели управления.
4. Выберите профиль ребенка, на котором вы хотите установить ограничения.
5. Нажмите ссылку **Установить Родительский Контроль на устройстве** на желаемой карточке.

6. Нажмите **ДОБАВИТЬ УСТРОЙСТВО** в появившемся окне.
7. Опция **BitdefenderРодительский контроль для Android** выбрана по умолчанию. Нажмите **ДАЛЕЕ**, чтобы продолжить, затем установите приложение на желаемое устройство.
8. Выберите вкладку **Телефонные контакты** .

   Отобразится список с карточками. Карточки отобразят контакты со смартфона Вашего ребенка.
9. Выберите карточку с номером телефона, который хотите заблокировать.

   Появиться символ галочка, который означает, что ваш ребенок не сможет использовать выбранный номер телефона.

Чтобы заблокировать неизвестные номера телефонов, включите переключатель **ЗАБЛОКИРОВАТЬ НЕИЗВЕСТНЫЕ НОМЕРА**.

Замечание
Ограничения на телефонные звонки могут быть установлены только для устройств Android, добавленных в профиль Вашего ребенка.

3.5.5. Как обозначить местоположение как безопасное или небезопасное для ребенка?

Bitdefender Родительский контроль позволяет вам обозначить безопасное или небезопасное местоположение для ребенка.

Чтобы установить местоположение:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
3. Нажмите **Родительский контроль** для доступа к панели управления.
4. Выберите профиль своего ребенка в окне **МОИ ДЕТИ**.
5. Выберите вкладку **Местоположение ребенка**
6. Нажмите **Устройства** в рамке, которая находится у вас в окне **Местоположение ребенка**.
7. Нажмите **ВЫБРАТЬ УСТРОЙСТВА**, а затем выберите устройство, которое вы хотите настроить.

8. В окне **Области**, нажмите кнопку **ДОБАВИТЬ ОБЛАСТЬ**.
9. Выберите тип местоположения **БЕЗОПАСНОЕ** или **ОГРАНИЧЕННОЕ**.
10. Введите допустимое имя для области, в которой ваш ребенок может находиться.
11. Установите диапазон, который должен применяться для мониторинга из ползунка **Радиус**.
12. Нажмите **ДОБАВИТЬ ОБЛАСТЬ**, чтобы сохранить ваши настройки.

Всякий раз, когда вы хотите установить ограниченное место в качестве безопасного, или безопасное место, как ограниченное, щелкните его, а затем выберите **РЕДАКТИРОВАТЬ ОБЛАСТЬ**. В зависимости от изменения, которое требуется сделать, выберите параметр**БЕЗОПАСНЫЙ** или **ОГРАНИЧЕННЫЙ**, а затем нажмите **Обновление области**.

3.5.6. Как заблокировать доступ моего ребенка к назначенным устройствам в учебные дни?

Bitdefender Родительский Контроль позволяет ограничить доступ Вашего ребенка к заданным устройствам в часы посещения школы и до того времени,когда домашняя работа должна быть выполнена.

Чтобы установить ограничения:

1. Войдите в панель Родительский контроль из Bitdefender Central.
2. В окне **МОИ ДЕТИ** выберите профиль ребенка, для которого Вы хотите установить ограничения.
3. Выберите вкладку **Расписание времени** .
4. В области **ДНЕВНОЙ ЛИМИТ** нажмите **ОСОБЫЙ**.
5. Установите флажок **Лимит времени в учебные дни**.
6. Выберите в сетке периоды, в течение которых доступ в Интернет будет заблокирован.

Замечание

Ограничения могут быть установлены только для устройств на базе Android и Windows.

3.5.7. Как заблокировать доступ моего ребенка к назначенным устройствам во время школьных вечеров?

Bitdefender Родительский Контроль позволяет ограничить доступ ребенка к назначенным устройствам во время школьных вечеров.

Чтобы установить ограничения:

1. Войдите в панель Родительский контроль из Bitdefender Central.
2. В окне **МОИ ДЕТИ** выберите профиль ребенка, для которого Вы хотите установить ограничения.
3. Выберите вкладку **Расписание времени** .
4. В области **Время сна** установите флажок **Школьный вечер**.
5. Используйте клавиши со стрелками вверх и вниз из соответствующих счетчиков, чтобы установить временные интервалы, в течение которых доступ должен быть заблокирован.

Замечание
Ограничения могут быть установлены только для устройств на базе Android и Windows.

3.5.8. Как заблокировать доступ моего ребенка к заданным устройствам в выходные дни?

BitdefenderРодительский Контроль позволяет ограничить доступ Вашего ребенка к заданным устройствам в выходные дни и ночи.

Чтобы установить ограничения:

1. Войдите в панель Родительский контроль из Bitdefender Central.
2. В окне **МОИ ДЕТИ** выберите профиль ребенка, для которого Вы хотите установить ограничения.
3. Выберите вкладку **Расписание времени** .
4. В области **ВРЕМЯ СНА** установите флажок **Выходные ночи**.
5. Используйте клавиши со стрелками вверх и вниз из соответствующих счетчиков, чтобы установить временные интервалы, в течение которых доступ должен быть заблокирован.

6. В области **ЛИМИТ ДНЕВНОГО ВРЕМЕНИ** имеются следующие опции:
   - **СОВОКУПНЫЙ**
     a. Установите флажок на **Лимит в выходные дни**.
     b. Перетащите слайдеры вдоль шкалы, чтобы установить разрешенное время для доступа к устройствам.
   - **ОСОБЫЙ**
     a. Установите флажок на **Лимит в выходные дни**.
     b. Выберите в сетке периоды, в течение которых доступ в Интернет будет заблокирован.

   Обратите внимание, что настройки **СОВОКУПНЫЙ** и **ОСОБЫЙ** несовместимы в работе.

Замечание
Ограничения могут быть установлены только для устройств на базе Android и Windows.

3.5.9. Как удалить профиль ребенка

Если вы хотите удалить существующий профиль вашего ребенка:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
3. Нажмите **Родительский контроль** для доступа к панели управления.
4. Нажмите иконку на профиле ребенка, который вы хотите удалить, а затем выберите **Удалить**.

3.6. Защита приватности

3.6.1. 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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку быстрого действия **Safepay**.
3. Нажмите кнопку для доступа к **Виртуальной клавиатуре**.

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

3.6.2. Что делать, если мое устройство было украдено?

Кражи мобильных устройств, смартфонов, планшетов или ноутбуков, являются основной проблемой,с которой сталкивалось большинство людей во всем мире.

Bitdefender Anti-Theft позволяет не только обнаружить и заблокировать украденное устройство, но и стереть все данные, чтобы ими не смогли воспользоваться злоумышленники.

Чтобы получить доступ к функции Анти-Вор из вашей учетной записи :

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.
3. В окне **МОИ УСТРОЙСТВА**, выберите необходимое устройство.
4. Нажмите **Анти-вор**.
5. Выберите функцию, которую вы хотите использовать:
   - **МЕСТОПОЛОЖЕНИЕ** - посмотреть местоположение вашего устройства на Google Maps.
   - **ТРЕВОГА** - отправить уведомление о тревоге на устройство.
   - **Замок** - блокируйте свой компьютер и установите числовой PIN-код для его разблокировки. В качестве альтернативы, включите

соответствующую опцию, чтобы позволить Bitdefender делать снимки человека, который пытается получить доступ к устройству.

- **Стереть** - удалить все данные с вашего компьютера.

  Важно
  После очистки устройства все возможности Анти-Вора перестанут функционировать.

- **Показать IP** - отображает последний IP-адрес выбранного устройства.

3.6.3. Как использовать хранилища файлов?

Хранилище файлов Bitdefender позволяет создавать на компьютере шифрованные логические диски, защищенные паролем (хранилища), в которых можно безопасно хранить важные конфиденциальные документы. Физически хранилище представляет собой файл с расширением BVD, расположенный на локальном жестком диске.

При создании хранилища файлов необходимо учесть два важных момента: размер хранилища и пароль. Размер 100 МБ по умолчанию, этого объема должно быть достаточно для ваших личных документов, файлов Excel и других подобных данных. Тем не менее, для хранения видеозаписей и других файлов большого размера может потребоваться дополнительное пространство.

Для безопасного хранения файлов и папок, содержащих личную и конфиденциальную информацию, в хранилищах файлов Bitdefender выполните следующие действия:

- **Создайте хранилище файлов и задайте для него надежный пароль.**

  Чтобы создать хранилище, щелкните правой кнопкой мыши по пустой области рабочего стола или по папке на вашем компьютере, выберите пункт **Bitdefender** > **Bitdefender Хранилище файлов** и выберите **Создать хранилище файлов**.

  Появится новое окно. Выполните следующие действия:

  1. Нажмите **Обзор**, выберите расположение хранилища и сохраните файл хранилища под желаемым именем.

2. Выберите букву диска из меню. Когда вы открываете Хранилище, виртуальный диск появляется в окне **Мой компьютер**.
3. Введите пароль хранилища в полях **Пароль** и **Подтвердить**.
4. Если вы хотите изменить стандартный размер (100 МБ) хранилища, введите нужное значение в поле **Размер хранилища(MB)**, используя клавиши стрелки.
5. Нажмите **Создать**.

> **Замечание**
> При открытии хранилища, виртуальный диск появится в окне **Мой компьютер**. Этот диск будет обозначен буквой, назначенной хранилищу.

- **Добавьте файлы или папки, которые следует сохранить в хранилище.**

  Чтобы добавить файл в хранилище, необходимо сначала открыть хранилище.

  1. Перейдите к BVD-файлу хранилища.
  2. Щелкните правой кнопкой мыши по файлу хранилища, наведите курсор на хранилище файлов Bitdefender и выберите **Открыть**.
  3. В появившемся окне введите пароль, выберите букву диска для его обозначения в хранилище и нажмите кнопку **OK**.

  Теперь операции на диске, соответствующем выбранному хранилищу файлов, можно выполнять, используя для этого проводник Windows, как и в случае с обычным диском. Чтобы добавить файл в открытое хранилище, можно также щелкнуть правой кнопкой мыши по хранилищу файлов Bitdefender и выбрать **Добавить в хранилище файлов**.

- **Хранилище должно быть всегда заблокировано.**

  Открывать хранилища рекомендуется только для доступа или управления их содержимым. Чтобы заблокировать хранилище, щелкните правой кнопкой мыши по соответствующему диску в разделе **Мой компьютер**, наведите курсор на **Bitdefender Хранилище файлов** и выберите **Заблокировать**.

- **Не удаляйте файл хранилища с расширением BVD.**

При удалении файла выполняется также удаление содержимого хранилища.

Дополнительные сведения о работе с хранилищами файлов, пожалуйста, см. в «*Шифрование файла*» (p. 150).

3.6.4. 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. Появится окно подтверждения. Нажмите **Да, УДАЛИТЬ**, чтобы запустить мастер Файлового шредера

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

3.6.5. Как защитить веб-камеру от взлома?

Вы можете настроить для вашего продукта Bitdefender разрешение или запрет доступа установленных приложений к веб-камере, выполнив следующие шаги:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **ЗАЩИТА ВЕБ-КАМЕРЫ** нажмите **Доступ к веб-камере**.

   Отобразится список приложений, запрашивающих доступ к камере.
4. Укажите приложение, которому Вы разрешаете или запрещаете доступ, затем нажмите на соответствующий переключатель.

   Чтобы просмотреть, что другие пользователи Bitdefender выбрали для данного приложения, нажмите значок . Вы будете получать уведомления каждый раз, когда одно из перечисленных приложений

блокируется пользователями Bitdefender, независимо от статуса Автопилота.

Чтобы вручную добавить приложения в этот список, нажмите ссылку **Добавить новое приложение в список** .

Замечание
Поскольку приложения Windows Store работают в едином процессе, каждый раз, когда доступ к одному из его приложений установлен на режиме «Разрешить» или «Блокировать», данное правило будет применяться ко всей системе. Примеры таких приложений:Internet Explorer и Microsoft Edge.

3.7. Инструменты оптимизации

3.7.1. Как повысить производительность системы?

Производительность системы зависит не только он конфигурации программно-аппаратного обеспечения (загрузка ЦП, использование памяти и пространства на диске). Быстродействие системы также зависит от конфигурации программного обеспечения и управления данными.

Следующие действия доступны в Bitdefender для повышения производительности и быстродействия системы:

- «*Оптимизация производительности системы с помощью одного клика*» (p. 80)
- «*Регулярно выполняйте сканирование системы*» (p. 81)

Оптимизация производительности системы с помощью одного клика

Опция Оптимизация в один клик экономит время, когда вы хотите улучшить производительность системы, быстро сканируя, обнаруживая и очищая бесполезные файлы.

Чтобы начать процесс Оптимизации в один клик:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку **Оптимизация в один клик**.

3. Позвольте Bitdefender найти файлы, которые могут быть удалены, а затем нажмите кнопку **ОПТИМИЗИРОВАТЬ**, чтобы завершить процесс.

Для получения более подробной информации о том, как можно улучшить скорость работы компьютера с помощью одного клика, пожалуйста, обратитесь «Оптимизация производительности системы в один клик» (p. 189).

Регулярно выполняйте сканирование системы

Вредоносное ПО может негативно повлиять на производительность системы и ее общее поведение.

Регулярно выполняйте сканирование системы (не реже одного раза в неделю).

Рекомендуется использовать полное сканирование системы, так как в этом случае выполняется проверка на все типы вирусных угроз безопасности системы, а также сканируются файлы в архивах.

Чтобы запустить Сканирование Системы:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Системное сканирование**.
4. Следуйте инструкциям мастера.

3.7.2. Как можно улучшить время запуска системы?

Ненужные приложения, которые замедляют время загрузки при запуске компьютера, можно отключить или отложить, таким образом, Оптимизация загрузки экономит время.

Чтобы использовать Оптимизацию загрузки:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку **Оптимизация загрузки**.
3. Выберите приложения, которые вы хотите отложить при запуске системы.

Для получения более подробной информации о том, как оптимизировать время загрузки вашего компьютера, пожалуйста, обратитесь «Оптимизация времени загрузки ПК» (p. 190).

3.8. Полезная информация

3.8.1. Как протестировать мою систему антивирусной защиты?

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

"Eicar test" позволяет вам проверить систему антивирусной защиты при помощи файла безопасности, разработанного для этой цели.

Чтобы проверить ваше антивирусное решение:

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 на странице, куда вы пытаетесь перейти, содержится EICAR-Test-File (не вирус).

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

   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. 330).

3.8.2. Как удалить Bitdefender?

Если вы хотите удалить Bitdefender Total Security:

- В **Windows 7**:

1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
2. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
  5. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
  6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Замечание
Эта процедура переустановки навсегда удалит настроенные параметры.

3.8.3. 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.

3.8.4. Как автоматически выключить компьютер после завершения сканирования?

Bitdefender предлагает несколько задач проверки, которые можно использовать, чтобы убедиться, что ваша система не заражена вредоносными программами. Сканирование всего компьютера может занять больше времени,в зависимости от вашей системы, аппаратной и программной конфигурации.

По этой причине Bitdefender позволяет вам настраивать Bitdefender и завершить работу вашей системы, как только закончится сканирование.

Рассмотрим этот пример: вы закончили работу за компьютером. Вы бы хотели проверить всю систему на вредоносные программы Bitdefender.

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

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.
4. В окне **Управление задачами сканирования**, нажмите **Новая пользовательская задача** введите имя сканирования и выберите места для сканирования.
5. Если вы хотите настроить дополнительный параметры сканирования, выберите вкладку **Расширенное**.
6. Выберите завершение работы компьютера после завершении сканирования, если угрозы не найдены.
7. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.
8. Нажмите кнопку **Начать сканирование** чтобы начать сканирование системы.

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 дополнительной информации перейдите к «Мастер антивирусного сканирования» (p. 105).

3.8.5. 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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **РАСШИРЕННЫЙ**
3. Включите использование прокси с помощью соответствующего переключателя.
4. Нажмите ссылку **Управление 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.

     Замечание
     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.

3.8.6. 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.

3.8.7. Как отобразить скрытые объекты в Windows?

Эти инструкции полезны для устранения вредоносного ПО в тех случаях, когда необходимо найти и удалить скрытые зараженные файлы.

Для отображения скрытых объектов в Windows выполните следующие действия:

1. Нажмите **Пуск** 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**.

3.8.8. 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 Total Security 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.

3.8.9. 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 вирусов, препятствующих нормальной загрузке Windows. В безопасном режиме могут работать только некоторые приложения, Windows загружает только основные драйвера и минимум компонентов операционной системы. Именно поэтому большинство вирусов неактивны при работе Windows в безопасном режиме и их можно легко удалить.

Запуск Windows в безопасном режиме:

- 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 **OK** 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 **OK**.
  3. Выберите вкладку **Загрузка**.
  4. В разделе **Параметры загрузки** поставьте флажок **Безопасная загрузка**.
  5. Выберите **Сеть** и затем **OK**.
  6. Выберите **OK** 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.

4. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

4.1. Антивирусная защита

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

- Проверка при доступе — предотвращение попадания в систему нового вредоносного ПО. К примеру, Bitdefender будет сканировать документ Word на наличие известных угроз при его открытии и сообщение электронной почты при его получении.

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

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

- Сканирование по запросу - позволяет обнаруживать и удалять вредоносное ПО, которое уже находится 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 дополнительной информации перейдите к «Автоматическое сканирование съемных носителей » (p. 109).

Если сканирование определенных файлов или типов файлов выполнять не требуется, опытные пользователи могут настроить исключения при сканировании. Для получения дополнительной информации перейдите к «Настройка исключений сканирования» (p. 112).

В случае обнаружения вируса или других вредоносных программ Bitdefender попытается автоматически удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция называется "лечение". Файлы, которые не удается вылечить, перемещаются в папку карантина во избежание распространения

вируса. Для получения дополнительной информации перейдите к «Управление файлами в карантине» (p. 115).

В случае заражения компьютера вирусом см. информацию в «Удаление вредоносного ПО из системы» (p. 223). Чтобы помочь вам очистить компьютер от вирусов, которые невозможно удалить из операционной системы Windows, Bitdefender предоставляет режим«Bitdefender Режим Восстановления (Rescue Environment в Windows 10)» (p. 224). Это доверенная среда, предназначенная, в частности, для удаления вредоносного ПО, которая позволяет загружать компьютер без запуска Windows. Когда компьютер запущен в Режиме Спасения (среда спасения в Windows 10), вредоносные программы Windows неактивны, что упрощает удаление.

Резидентное сканирование (защита в реальном времени)

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

Включение или отключение защиты в реальном времени

Для включения или выключения защиты в реальном времени от вредоносных программ:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. В окне **ЩИТ** нажмите переключатель ВКЛ/ВЫКЛ.
5. 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.

Внимание
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 вредоносного ПО.

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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. В окне **ЩИТ** нажмите в соответствующем меню **ПОКАЗАТЬ РАСШИРЕННЫЕ НАСТРОЙКИ**.

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

Информация о параметрах сканирования

Эти сведения могут быть полезными:

- Значение незнакомых терминов можно посмотреть в глоссарии. Также вы можете найти полезную информацию в Интернете.
- **Параметры сканирования для используемых файлов.** В Bitdefender можно настроить, чтобы выполнялось только сканирование всех файлов и приложений (файлов программ), вызываемых пользователем. Наиболее качественная защита обеспечивается посредством сканирования всех открываемых файлов, однако

сканирование только приложений обеспечивает оптимальную производительность системы.

По умолчанию локальные папки и общие сетевые ресурсы подвергаются проверке при доступе. Для улучшения производительности системы сетевые расположения можно исключить из сканирования при доступе.

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

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

- **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. Вредоносные программы могут скомпрометировать систему только в том случае, если зараженный файл будет извлечен из архива и выполнен; при этом защита в режиме реального времени должна быть отключена.

  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.

- **Сканирование электронной почты.** Чтобы предотвратить загрузку вредоносных программ на ваш компьютер, Bitdefender автоматически сканирует входящие и исходящие сообщения электронной почты.

Хотя это и не рекомендуется, вы можете отключить Антивирусное сканирование электронной почты для повышения производительности системы. 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 угроза, поскольку защита в режиме реального времени блокирует вредоносные программы при доступе (открытии, перемещении, копировании или выполнении) 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. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие 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. Назначение данной функции является улучшение обнаружения вирусов при запуске системы и времени загрузки вашей системы.

Действия, выполненные в отношении обнаруженных вредоносных программ

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

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.

2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. В окне **ЩИТ** нажмите в соответствующем меню **ПОКАЗАТЬ РАСШИРЕННЫЕ НАСТРОЙКИ**.

   Отобразится новая панель
5. Прокрутите вниз, пока не увидите опцию**Действия после завершения сканирования**.
6. 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.** Файлы, распознанные как зараженные вирусом, соответствуют вирусным сигнатурам в базе данных вирусных сигнатур Bitdefender. Bitdefender попытается автоматически удалить вредоносный код из зараженного файла и изменить структуру исходного файла. Эта операция называется "лечение".

  Файлы, которые не удается вылечить, перемещаются в папку карантина во избежание распространения вируса. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Для получения дополнительной информации перейдите к «Управление файлами в карантине» (p. 115).

  Важно

  В случае определенных типов вредоносных программ 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 в карантине автоматически отправляются в лабораторию Bitdefender, где они анализируются специалистами Bitdefender по вирусам. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

- **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 дополнительной информации перейдите к «Управление файлами в карантине» (p. 115).

Запретить доступ

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

Восстановление настроек по умолчанию

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

Восстановление настроек по умолчанию для защиты в режиме реального времени:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. В окне **ЩИТ** нажмите в соответствующем меню **ПОКАЗАТЬ РАСШИРЕННЫЕ НАСТРОЙКИ**.

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

Сканирование по запросу

Основная цель для Bitdefender заключается в том, чтобы сохранить ваш компьютер чистым от вирусов. Система защиты закрывает доступ для новых вирусов в ваш компьютер и сканирует все сообщения в электронной почте и новые файлы, которые были загружены или скопированы в вашу систему.

Однако есть вероятность того, что вирус проник в компьютер до установки Bitdefender. Поэтому полезно проверить ваш компьютер на наличие вирусов после установки программы Bitdefender. И это, безусловно, хорошая идея - часто сканировать компьютер на наличие вирусов.

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.

Сканирование файла или папки на предмет наличия вредоносных программ

Рекомендуется выполнять сканирование файлов и папок каждый раз при подозрении на заражение их вирусом. Щелкните правой кнопкой мыши 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).

Запуск быстрого сканирования

Функция быстрого сканирования использует технологию "облачного" сканирования для распознавания вредоносных программ, запущенных в системе. Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, в отличие от процесса стандартного антивирусного сканирования.

Для запуска быстрого сканирования:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Быстрое сканирование**.
4. Следуйте инструкциям мастера антивирусного сканирования для выполнения проверки. Bitdefender автоматически выполняет рекомендуемые действия в отношении обнаруженных файлов. Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

Более быстрый способ, нажмите значок на левой боковой панели интерфейс Bitdefender, а затем нажмите кнопку **Быстрое сканирование**.

Запуск проверки системы

Задача сканирования системы сканирует весь компьютер на наличие всех типов вредоносных программ, угрожающих его безопасности, таких как вирусы, шпионские программы, руткиты и другие.

Замечание

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 установлены последние обновления вирусных сигнатур для Bitdefender. Сканирование компьютера с использованием устаревшей базы данных сигнатур может помешать Bitdefender обнаруживать новые вредоносные программы, обнаруженные с момента последнего обновления. Для получения дополнительной информации перейдите к *«Поддержка Bitdefender в обновленном состоянии» (p. 46)*.
- Закройте все открытые программы.

Чтобы выполнить сканирование отдельных папок на компьютере или настроить параметры сканирования, создайте и запустите пользовательское сканирование. Для получения дополнительной информации перейдите к «Настройка пользовательского сканирования» (p. 101).

Чтобы запустить сканирование системы:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Системное сканирование**.
4. Следуйте инструкциям мастера антивирусного сканирования для выполнения проверки. Bitdefender автоматически выполняет рекомендуемые действия в отношении обнаруженных файлов. Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

Настройка пользовательского сканирования

Чтобы подробно настроить пользовательское сканирование и затем запустить его:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.

4. Нажмите кнопку **Новая пользовательская задача**. В вкладке **Основное**введите имя для сканирования и выберите сканируемые местоположения.
5. 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 системный трей .** Сворачивает окно сканирования в системный трей. Дважды щелкните значок Bitdefender, чтобы открыть его.
      - Задать действие, выполняемое при отсутствии обнаруженных угроз.

   c. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.
6. 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
7. Нажмите **Начало сканирования** и следуйте инструкциям мастера антивирусного сканирования, чтобы выполнить проверку. Процедура

сканирования может занять некоторое время, в зависимости от выбранных путей сканирования. На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).

8. 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 программные файлы) значительно более уязвимы для вирусных атак, чем другие типы файлов. В эту категорию включены следующие расширения файлов: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Параметры сканирования архивов .** Архивы, содержащие зараженные файлы, не представляют собой непосредственной угрозы безопасности системы. Вредоносные программы могут скомпрометировать систему только в том случае, если зараженный

файл будет извлечен из архива и выполнен; при этом защита в режиме реального времени должна быть отключена. Тем не менее, рекомендуется использовать этот параметр для обнаружения и удаления всех вирусов, даже тех, которые не представляют собой непосредственной угрозы системе.

Замечание

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

- **Сканирование загрузочных секторов.** Bitdefender можно настроить для сканирования загрузочных секторов жесткого диска. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
- **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 общее быстродействие системы с минимальными потерями в безопасности.
- **Пропускать коммерческие клавиатурные шпионы.** Выберите этот параметр, если вы установили и используете на компьютере коммерческие программы клавиатурных шпионов. Коммерческие клавиатурные шпионы — это законные программы мониторинга компьютеров, базовой функцией которых является запись текста, вводимого с клавиатуры.
- **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.

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.

Замечание

Если Мастер сканирования не отображается, сканирование может быть настроено на запуск в фоновом режиме. Найдите значок состояния сканирования в системном трее. 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 их 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).

Замечание

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

Зараженные объекты отображаются в группах в зависимости от вредоносной программы, 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.** Файлы, распознанные как зараженные вирусом, соответствуют вирусным сигнатурам в базе данных вирусных сигнатур Bitdefender. Bitdefender попытается автоматически удалить вредоносный код из зараженного файла

и изменить структуру исходного файла. Эта операция называется "лечение".

Файлы, которые не удается вылечить, перемещаются в папку карантина во избежание распространения вируса. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Для получения дополнительной информации перейдите к «Управление файлами в карантине» (p. 115).

Важно

В случае определенных типов вредоносных программ 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 в карантине автоматически отправляются в лабораторию Bitdefender, где они анализируются специалистами Bitdefender по вирусам. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

- **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. Дополнительные сведения и инструкции по удалению вредоносных программ вручную см. в «Удаление вредоносного ПО из системы» (p. 223).

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 на иконку в нижнем левом углу Bitdefender interface.
2. На вкладке **ВСЕ**, выберите уведомления относительно последнего сканирования.

   Здесь можно просмотреть все события сканирования на вирусы, включая угрозы, обнаруженные при резидентном сканировании, 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 **ПРОСМОТР ЖУРНАЛА**.

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 вирусами и другими вредоносными программами.

Обнаруженные устройства относятся к одной из следующих категорий:

- CD/DVD
- Запоминающие устройства USB, 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.

Как это работает?

При обнаружении съемного носителя Bitdefender запускает операцию его сканирования на вирусы в фоновом режиме (если функция автоматического сканирования для этого типа устройств включена). Значок сканирования Bitdefender появится в системном трее. Вы можете щелкнуть этот значок, чтобы открыть окно сканирования и просмотреть ход сканирования.

Если режим "Автопилот" включен, процесс сканирования не будет отвлекать вас. Сканирование будет регистрироваться, и информация о нем будет доступна в окне Уведомления.

Если режим "Автопилот" отключен:

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

   Замечание
   Обратите внимание 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.

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

Следующая информация может оказаться вам полезной:

- Соблюдайте осторожность при использовании зараженных CD/DVD, так как удалить вредоносное ПО с дисков невозможно (носители доступны только для чтения). Убедитесь, что защита в реальном времени включена, чтобы предотвратить распространение вредоносных программ в системе. Рекомендуется скопировать любые ценные данные с диска в систему, а затем утилизировать диск.

- В некоторых случаях Bitdefender не может удалить вредоносные программы 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).

  Инструкции по обработке вредоносного ПО см. в «Удаление вредоносного ПО из системы» (p. 223)

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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Выберите вкладку **Диски и устройства**.

Опции сканирования предварительно настроены для достижения наилучших результатов обнаружения. При обнаружении зараженных файлов, Bitdefender попытается вылечить (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.

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **РАСШИРЕННЫЙ**
3. Нажмите соответствующий переключатель.

Настройка исключений сканирования

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

Вы можете настроить исключения, которые будут применяться только для резидентного сканирования или сканирования по запросу либо в обоих случаях. Объекты, исключенные из проверки при доступе, не будут сканироваться, независимо от того, доступны ли они вам или приложению.

Замечание

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**.

Исключение файлов или папок из сканирования

Чтобы исключить файлы или папки из сканирования:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Выберите вкладку **ИСКЛЮЧЕНИЯ**.

5. Нажмите **список файлов и папок, исключенных из сканирования** из соответствующего меню. В открывшемся окне можно управлять файлами и папками, исключенными из сканирования.
6. Добавьте исключения, выполнив следующие действия:
   a. Нажмите кнопку **ДОБАВИТЬ**.
   b. Нажмите **Обзор**, выберите файл или папку, которые требуется исключить из сканирования, а затем нажмите **ОК** 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**.

Исключение расширений файлов из сканирования

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

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

Исключение расширений файлов из сканирования:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Выберите вкладку **ИСКЛЮЧЕНИЯ**.

5. Нажмите **Список расширений, исключенных из сканирования** аккордеонного меню. В открывшемся окне сканирования можно управлять расширениями файлов, исключенными из сканирования.
6. Добавьте исключения, выполнив следующие действия:
   a. Нажмите кнопку **ДОБАВИТЬ**.
   b. Введите расширения, которые требуется исключить из сканирования, разделив их точкой с запятой (;). Пример:

      txt;avi;jpg

   c. По умолчанию все файлы с заданными расширениями исключаются из сканирования в режиме реального времени и сканирования по запросу. Чтобы изменить время применения исключения, выберите один из других параметров.
   d. Нажмите **Добавить**.

Управление исключениями сканирования

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

Управление исключениями сканирования:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Выберите вкладку **ИСКЛЮЧЕНИЯ**.
5. Используйте опции в **Списке файлов и папок, исключенных из сканирования** аккордеонного меню для управления исключениями сканирования.
6. Для того, чтобы удалить или изменить исключения сканирования, нажмите на одну из доступных ссылок. Выполните следующие действия:
   - Чтобы удалить запись из списка, выделите ее и нажмите кнопку **УДАЛИТЬ**.
   - Чтобы отредактировать запись из таблицы, дважды щелкните ее (или выделите ее) и нажмите**РЕДАКТИРОВАТЬ**. Появится новое

окно, в котором можно изменить расширение или путь, который необходимо исключить, а также тип сканирования, из которого требуется исключить их, при необходимости. Внесите необходимые изменения и нажмите **Изменить**.

Управление файлами в карантине

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

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

Кроме того, Bitdefender сканирует файлы, помещенные в карантин после каждого обновления сигнатур вредоносных программ. Вылеченные файлы автоматически возвращаются на свое место.

Чтобы проверить и управлять файлами на карантине:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Выберите вкладку **Карантин**.
5. Bitdefender автоматически управляет файлами в карантине в соответствии с настройками параметров карантина по умолчанию. Вы можете изменить настройки параметров карантина в соответствии со своими потребностями, однако это делать не рекомендуется.

   Повторно сканировать карантин после обновления определений вирусов

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

Отправка подозрительных файлов на карантин для дальнейшего анализа

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

Удалять содержимое старше {30} дней

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

6. Для удаления файлов, помещенных в карантин, выделите их и нажмите кнопку **УДАЛИТЬ**. Для восстановления файла из папки карантина в исходную папку необходимо выбрать файл и нажать **ВОССТАНОВИТЬ**.

4.2. 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 непрерывно отслеживает приложения, работающие на компьютере, на предмет вредоносных действий. Для всех вышеперечисленных действий присваивается определенный балл и для каждого процесса подсчитывается общий рейтинг.

В качестве меры безопасности Вы будете получать уведомления каждый раз, когда обнаружена и заблокирована атака программы-вымогателя, даже если задействована функция автопилота.

Включение и выключение Активный Контроль Угроз:

Чтобы включить или выключить Активный Контроль Угроз:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

3. На панели **Активный Контроль Угроз** щелкните переключатель ВКЛ/ВЫКЛ.

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

Проверка обнаруженных вирусов-вымогателей

Для проверки обнаруженных атак вирусов-вымогателей:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **АКТИВНЫЙ КОНТРОЛЬ УГРОЗ** щелкните **Защита от вымогателей**.
4. В окне с описанием функции «Активный Контроль Угроз» 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.

Проверка обнаруженных подозрительных приложений

Для проверки обнаруженных атак вирусов-вымогателей:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **Активный Контроль Угроз** щелкните **Защита от угроз**.
4. В окне с описанием функции «Активный Контроль Угроз» нажмите **ОК** .

   Отображаются приложения, которые были обнаружены в качестве угроз и заблокированы в последние 90 дней. Чтобы найти информацию о приложении, пути вредоносного процесса или результат успешного лечения, просто нажмите на нее.

Добавить исключения процесса

Вы можете настроить правила исключения для доверенных приложений, чтобы активный вирусный контроль не блокировал их, когда они выполняют операции с признаками вредоносного поведения. Активный Контроль Угроз продолжит мониторинг исключенных приложений.

Чтобы начать добавлять процессы в список исключений Активного контроля угроз:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом нижнем углу панели **Активный Контроль Угроз**.
4. В окне **Белый список** нажмите **Добавить приложения в белый список** .
5. Найдите и выберите приложение, которое хотите исключить, затем нажмите **ОК** .

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

4.3. Веб-защита

Bitdefender Веб-защита обеспечивает безопасный просмотр, предупреждая вас о потенциальных вредоносных веб-страницах.

Bitdefender обеспечивает веб-защиту в режиме реального времени для:

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

Чтобы настроить параметры Веб-защиты:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

3. Нажмите ⚙ в правом нижнем углу **ВЕБ-ЗАЩИТА** панели

Нажмите на переключатели, чтобы включить или отключить:

- Сканирование HTTP-трафика блокирует вредоносные программы, поступающие из Интернета, включая загрузку с диска.
- 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
- Сканирование SSL.

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

Можно создать список веб-сайтов, для которых сканирование Bitdefender Антифишинг выполняться не будет. 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 веб-защиты, предоставляемой Bitdefender:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **ВЕБ-ЗАЩИТА** нажмите **Белый список**.
4. В текстовом поле **Добавить URL** введите имя веб-сайта, которое вы хотите добавить в белый список, затем 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.

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.**

4.4. Антиспам

Термином "спам" обозначаются нежелательные сообщения электронной почты Спам является растущей проблемой, как для отдельных лиц так и для организаций. Это ненужная информация, вы не захотите, чтобы ваши дети увидели ее. Она может "украсть" у вас много времени, и вы не можете остановить людей, отправивших ее. Следующая лучшая вещь, это, очевидно, прекратить его получать. К сожалению, спам приходит в широком диапазоне форм и размеров.

Антиспам Bitdefender использует передовые технологические достижения и соответствующие стандарты для отсеивания спама фильтром еще до того, как он попадает в ваш почтовый ящик. Для получения дополнительной информации перейдите к «Антиспам» (р. 121).

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

Замечание

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

Спам, обнаруженный Bitdefender, помечается префиксом [спам] в теме письма. Bitdefender автоматически перемещает спам в особую папку, такую как:

- В Microsoft Outlook спам перемещается в папку **Спам**, находящуюся в папке **Удаленные**. Папка **Спам** создается, когда электронное письмо помечено как спам.
- В Mozilla Thunderbird спам перемещается в папку **Спам**, находящуюся в папке **Удаленные**. Папка **Спам** создается, когда электронное письмо помечено как спам.

Если вы используете другие почтовые программы, вам надо создать правило, перемещающее письма, помеченные Bitdefender как [спам], в пользовательскую карантинную папку. Если папки «Удалить элементы» и «Корзина» удалены, папка «Спам» также будет удалена. Однако новая папка спама будет создана, как только электронное письмо будет помечено как спам.

Антиспам

Антиспам-фильтры

Bitdefender Защита Антиспам включает в себя облачную защиту и несколько других фильтров различного назначения, таких как Список друзей, Список спамеров и Фильтр кодировки, при помощи которых обеспечивается защита вашего почтового ящика от спама. .

Список друзей / Список спамеров

Большинство людей регулярно общаются с группой людей или даже получают сообщения от компаний или организаций, наравне с одним

и тем же доменом. Используя **список друзей или спамеров**, вы можете легко классифицировать, от каких людей вы хотите получать электронную почту (друзья) независимо от того, что содержит сообщение; или от людей, которых вы не хотите ничего получать (спамеры).

Замечание

Рекомендуется добавлять имена и адреса электронной почты ваших друзей в **Список друзей**. Bitdefender не блокирует письма от людей из этого списка, значит, чем больше друзей занесено в список, тем больше вероятность, что Вы получите ожидаемое сообщение.

Фильтр символов

Многие спам сообщения записываются в кириллице и/или азиатских кодировках. Фильтр кодировки определяет подобные сообщения и отмечает их как SPAM.

Работа параметра Антиспам

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

Каждое сообщение, полученное из Интернета, сначала проверяется на наличие адресата в Списке друзей и Списке спамеров. Если адрес отправителя найден в Списке друзей, сообщение перемещается непосредственно в папку **Входящие**.

В противном случае сообщение будет проверено с помощью фильтра Список спамеров на наличие данного электронного адреса в его списке. Если адресат найден в списке, такие письма помечаются как СПАМ и перемещаются в папку **Спам**.

Также с помощью Фильтра символов отсеиваются письма, написанные Кириллицей или иероглифами. Если адресат найден в списке, такие письма помечаются как СПАМ и перемещаются в папку **Спам**.

Замечание

Письма категории "ОТКРОВЕННОГО ХАРАКТЕРА" Bitdefender считает СПАМОМ

Поддерживаемые почтовые клиенты и протоколы

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

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 и выше

Включение и отключение защиты антиспама

Защита от спама включается по умолчанию.

Чтобы включить или отключить функцию антиспама:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИСПАМ** нажмите переключатель ВКЛ/ВЫКЛ.

Использование панели инструментов антиспама в окне почтового клиента

В верхней части вашей почтовой программы вы можете заметить панель Антиспама. Панель инструментов анти-спам позволяет управлять защитой от спама непосредственно из почтового клиента. Вы можете легко поправить Bitdefender, если он принял легальное письмо за СПАМ.

Важно

Bitdefender интегрируется в наиболее часто используемые почтовые клиенты с помощью простой в использовании антиспам-панели инструментов. С полным списком системных требований можно ознакомиться в разделе «Поддерживаемые почтовые клиенты и протоколы» (p. 123).

Ниже приводится описание каждой кнопки панели инструментов Bitdefender:

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

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

Важно
Кнопка **Not Spam** становится активной, когда вы выделяете письмо, помеченное программой Bitdefender как СПАМ (обычно эти письма помещаются в папку **Спам**).

Добавить спамера: добавление отправителя выбранного письма в список спамеров. Необходимо нажать **ОК** для подтверждения. Почтовые сообщения, полученные с адресов из списка спамеров, автоматически помечаются как [spam].
Добавить друга: добавление отправителя выбранного письма в список друзей. Необходимо нажать **ОК** для подтверждения. Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.
Спамеры — открытие **Списка спамеров**, содержащего адреса, с которых Вы не хотите получать сообщения, независимо от их содержания. Для получения дополнительной информации перейдите к «Настройка Списка Спамеров» (р. 127).
Друзья — открытие **Списка друзей**, содержащего адреса, с которых Вы всегда хотите получать сообщения независимо от их содержания. Для получения дополнительной информации перейдите к «Настройка Списка Друзей» (р. 126).

Отображение обнаружения ошибок

Если Вы используете поддерживаемую почтовую службу, Вы можете легко корректировать фильтр антиспама, указывая, какие письма не следует помечать как [спам]. Это поможет повысить эффективность фильтра антиспама. Следуйте инструкции:

1. Откройте ваш почтовый клиент.

2. Перейдите в папку нежелательной почты, куда помещаются спам-сообщения.
3. Выберите легитимные сообщения, ошибочно помеченные Bitdefender как [спам].
4. Нажмите кнопку **Добавить друга** на панели управления Bitdefender антиспама для добавления отправителя в список друзей. Необходимо нажать **OK** для подтверждения. Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.
5. Нажмите кнопку **Не спам** на панели инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента). Письмо будет перемещено в папку "Входящие".

Обозначение необнаруженных сообщений спама

При использовании поддерживаемого почтового клиента можно легко указать, какие сообщения электронной почты должны были быть обнаружены как нежелательные. Это поможет повысить эффективность фильтра антиспама. Следуйте инструкции:

1. Откройте ваш почтовый клиент.
2. Перейти к папке "Входящие".
3. Выберите необнаруженные спам-сообщения.
4. Нажмите кнопку **Является спамом** на панели Bitdefender инструментов анти-спама(обычно находится в верхней части окна почтового клиента). Они незамедлительно будут помечены как [spam] и перенесены в папку нежелательной почты.

Настройка параметров панели инструментов

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

Здесь доступны следующие варианты:

- **Пометить спам-сообщения как "Прочитанные"** - письма спама автоматически отмечаются как прочитанные, чтобы они не отвлекали пользователей при поступлении.

- Вы можете выбрать, будут или нет отображаться окна подтверждения при нажатии на **Добавить спамера** и **Добавить друга** кнопки на панели инструментов защиты от спама.

  Окна подтверждения позволяют предотвращать случайное добавление отправителей электронной почты в списки друзей и спамеров

Настройка Списка Друзей

Список друзей — это список всех адресов электронной почты, с которых вы всегда хотите получать сообщения, независимо от их содержания. Сообщения от друзей не помечаются как Спам, даже если их содержание соответствует определению Спама.

Замечание

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

Настройка и управление списком друзей:

- Если используется Microsoft Outlook или Thunderbird, нажмите кнопку **Друзья** на панели инструментов Bitdefender.
- В качестве альтернативы:
  1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
  2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
  3. На панели **АНТИСПАМ**, выберите **Управление друзьями**.

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

Чтобы добавить адреса электронной почты с определенного домена, выберите параметр **Имя домена**, введите имя домена и нажмите **Добавить**. Имя домена должно иметь следующий вид:

- @domain.com и *domain.com — все письма, приходящие с domain.com, попадут в Вашу папку **Входящие** независимо от содержания;
- domain - все письма, приходящие с domain (независимо от доменного суффикса) будут помечены как СПАМ;
- com- се письма с доменным суффиксом com будут помечены как СПАМ.

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

Чтобы удалить элемент из списка, нажмите соответствующую ссылку **Удалить**. Чтобы удалить все записи из списка, нажмите кнопку **Очистить список**.

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

Для загрузки сохраненного ранее списка друзей нажмите кнопку **Загрузить** и откройте соответствующий .bwl файл. Чтобы сбросить содержимое существующего списка при загрузке ранее сохраненного списка, выберите **Перезапустить текущий список**.

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

Настройка Списка Спамеров

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

Настройка и управление списком спамеров:

- Если вы используете Microsoft Outlook или Thunderbird нажмите кнопку **Спамеры** на Bitdefender панели инструментов антиспама интегрированную в ваш почтовый клиент.
- В качестве альтернативы:
  1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
  2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
  3. На панели **АНТИСПАМ**, выберите **Управление друзьями**.

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

Чтобы добавить адреса электронной почты с определенного домена, выберите параметр **Имя домена**, введите имя домена и нажмите **Добавить**. Имя домена должно иметь следующий вид:

- @domain.com и domain.com- все письма, приходящие с domain.com, попадут в Вашу папку **Входящие** независимо от содержания;
- domain - все письма, приходящие с domain (независимо от доменного суффикса) будут помечены как СПАМ;
- com- се письма с доменным суффиксом com будут помечены как СПАМ.

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

Внимание

На добавляйте домены легальных онлайн e-mail сервисов (таких как Yahoo, Gmail, Hotmail и другие) в список Спаммеров. Иначе, любое сообщение полученное от пользователя такого сервиса будет определено как спам. Например, если вы добавите yahoo.com в список спамеров, все сообщения электронной почты, приходящие от адресов yahoo.com, будут помечены как [spam].

Чтобы удалить элемент из списка, нажмите соответствующую ссылку **Удалить**. Чтобы удалить все записи из списка, нажмите кнопку **Очистить список**.

Список друзей можно сохранить в файл, чтобы его можно было использовать на другом компьютере или после переустановки продукта. Для сохранения списка спамеров нажмите кнопку **Сохранить** и сохраните список в желаемое место. Расширение файла будет .bwl.

Для загрузки сохраненного ранее списка спамеров нажмите кнопку **Загрузить** и откройте соответствующий .bwl файл. Чтобы сбросить содержимое существующего списка при загрузке ранее сохраненного списка, выберите **Перезапустить текущий список**.

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

Настройка локальных фильтров антиспама

Как описано в «Антиспам» (p. 121), для распознавания спама Bitdefender использует комбинацию из нескольких различных фильтров антиспама.

Фильтры антиспама предварительно настроены в целях обеспечения эффективной защиты.

Важно

В зависимости от того, получаете ли Вы легитимные сообщения электронной почты, созданные с использованием символов кириллицы или иероглифов, следует включить или отключить параметр, автоматически блокирующий прием таких сообщений В локализованных версиях программы, в которых используются такие шрифты, соответствующая настройка отключена (например, в русской или китайской версии).

Чтобы настроить локальные фильтры антиспама:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу модуля **АНТИСПАМ**.
4. Нажмите соответствующий переключатель.

Если вы используете Microsoft Outlook или Thunderbird, то вы можете настроить локальные фильтры антиспама непосредственно из почтового клиента. Нажмите кнопку **Настройки** на панели антиспама Bitdefender (как правило, находится в верхней части окна почтового клиента) и затем вкладку **Антиспам-фильтры**.

Настройка параметров в облаке

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

Функция защита в облаке работает всегда, пока Bitdefender Антиспам работает.

Примеры законных сообщений и спама можно отправить в облако Bitdefender при обнаружении ошибок и пропущенных сообщениях спама Это позволит повысить точность распознавания спама Bitdefender.

Настройте отправку образцов сообщений электронной почты в облако Bitdefender, выбрав нужные параметры, выполнив следующие действия:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.

2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом верхнем углу модуля **АНТИСПАМ**.
4. В окне **НАСТРОЙКИ** выберите нужные параметры.

Если вы используете Microsoft Outlook или Thunderbird, то вы можете настроить функцию обнаружения в облаке непосредственно из почтового клиента. Нажмите кнопку **Настройки** на панели инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента) и перейдите на вкладку **Настройки Облака**.

4.5. Брандмауэр (Firewall)

Брандмауэр защищает компьютер от входящих и исходящих несанкционированных попыток подключения, как в локальных сетях так и в Интернете. Фактически он выполняет функции охранника на входе: отслеживает попытки подключения и определяет, какие подключения следует разрешить, а какие требуется заблокировать.

Брандмауэр Bitdefender использует набор правил для фильтрации данных, передаваемых в вашу систему и из нее.

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

В качестве меры безопасности Вы будете получать уведомления каждый раз, когда потенциально вредоносное приложение блокируется при доступе к Интернету, даже если задействована функция автопилота.

Bitdefender автоматически присваивает тип сети для каждого сетевого соединения. В зависимости от типа сети, брандмауэр установлен на соответствующем уровне для каждого соединения.

Дополнительную информацию о настройках брандмауэра для каждого типа сети и процедуре изменения настроек сети см. в «Управление параметрами соединения» (p. 134).

Включение или отключение защиты брандмауэра

Чтобы включить или отключить защиту файервола:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.

2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **Файрвол** нажмите переключатель ВКЛ/ВЫКЛ.

Внимание

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

Правила управления приложениями

Для просмотра и управления правилами фаервола, контроля доступа приложений к сетевым ресурсам и Интернету, выполните следующие действия:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **Файрвол** выберите **Доступ к приложениям** .
4. В окне с описанием функции брандмауэра нажмите **ОК** .

Вы можете увидеть последние 15 программ (процессов), которые прошли через Bitdefender Файрвол и интернет-сеть, к которой Вы подключены. Чтобы просмотреть правила, созданные для конкретного приложения, просто нажмите на него, а затем нажмите ссылку **Просмотр правил приложения** . Откроется окно **ПРАВИЛА** .

Для каждого правила отображается следующая информация:

- **СЕТЬ** - типы процессов и сетевых адаптеров (Дом / Офис,Публичная или Все), к которым применяется правило. Правила автоматически создаются для фильтрации доступа к сети и Интернету через любой адаптер. По умолчанию, правила применяются к любой сети. Можно вручную создать правила или изменить существующие правила для фильтрации сети приложения или доступа к Интернету через конкретный адаптер (например, Беспроводной сетевой адаптер).
- **ПРОТОКОЛ** — IP-протокол, к которому применяется правило. По умолчанию, правила применяются к любому протоколу.
- **ТРАФИК** - правило применяется в обоих направлениях, входящем и исходящем.

- **ПОРТЫ** - протокол ПОРТ, к которому применяется правило. По умолчанию, правила применяются к любому протоколу.
- **IP**-Интернет-протокол (IP) правило применяется к. По умолчанию правила применяются к любому IP-адресу.
- **ДОСТУП** - разрешает или запрещает приложению доступ к сети или Интернету в указанных обстоятельствах.

Чтобы изменить или удалить правила для выбранного приложения, щелкните значок ... .

- **Изменить правило** - открывает окно, в котором Вы можете редактировать текущее правило.
- **Удалить правило** - Вы можете удалить текущий набор правил для выбранного приложения.

Добавить правило приложения

Чтобы добавить правило приложения:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **Файрвол**
4. Нажмите ссылку **Добавить правило** в верхней части окна **ПРАВИЛА** .

В окне **НАСТРОЙКИ** Вы можете применить следующие изменения:

- **Применить это правило для всех приложений.** Включите этот параметр, чтобы применять это правило для всех приложений.
- **Путь программы.** Нажмите **Обзор** и выберите приложение, к которому вы хотите применить правило.
- **Разрешение.** Выберите одно из доступных разрешений:

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

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

- **Тип сети.** Выберите тип сети, для которого будет назначено правило. Чтобы изменить тип, откройте раскрывающееся меню **Тип сети** и выберите один из доступных типов в списке.

Тип сети	Описание
Любая сеть	Разрешение всего трафика между Вашим компьютером и другими компьютерами независимо от типа сети
Домашняя/Офис	Разрешение всего трафика между вашим компьютером и компьютерами в локальной сети.
Публичная	Весь трафик фильтруется.

- **Протокол.** Выберите из меню IP-протокол, к которому будет применяться правило.
  - Если вы хотите, чтобы правило применялось ко всем протоколам, выберите **Любой**.
  - Если вы хотите применить правило к TCP, выберите **TCP**.
  - Если вы хотите применить правило к UDP, выберите **UDP**.
  - Если вы хотите применить правило к ICMP, выберите **ICMP** .
  - Если вы хотите, чтобы правило применялось к IGMP, выберите **IGMP** .
  - Если вы хотите, чтобы правило применялось к определенному протоколу, введите номер, присвоенный протоколу, который вы хотите отфильтровать, в пустом поле редактирования.

> **Замечание**
>
> Диапазоны IP-адресов выделяются Администрацией адресного пространства Интернет (IANA). Полный список выделенных IP-адресов можно найти на странице http://www.iana.org/assignments/protocol-numbers.

- **Направление.** Выберите из меню направление трафика, к которому будет применяться правило.

Направление	Описание
Исходящий	Правило будет применяться только к исходящему трафику.
Входящий	Правило применяется только ко входящему трафику.
Оба	Правило будет применяется и к входящему, и к исходящему трафику.

В окне **РАСШИРЕННЫЙ** вы можете настроить следующие параметры:

- **Пользовательский локальный адрес.** Укажите локальный IP-адрес и порт, к которому будет применяться правило.
- **Пользовательский удаленный адрес.** Укажите удаленный IP-адрес и порт, к которому будет применяться правило.

Чтобы удалить текущий набор правил и восстановить установленные по умолчанию, нажмите ссылку **Сбросить правила** в верхней части окна **ПРАВИЛА** .

Управление параметрами соединения

Если вы подключаетесь к Интернету с помощью Wi-Fi или Ethernet адаптера, вы можете настроить, какие параметры должны быть применены для безопасной навигации. Варианты, которые вы можете выбрать из:

- **Динамичный** - тип сети будет автоматически установлен на основе профиля подключенной сети, дома / офиса или общего доступа В этом случае будут применяться только правила брандмауэра для определенного типа сети или те, которые определены для применения ко всем сетевым типам.
- **Дом/ Офис** - тип сети всегда будет Дом/ Офис, несмотря на профиль подключенной сети. В этом случае будут применяться только правила брандмауэра для дома/офиса или те, которые определены для применения ко всем сетевым типам.

- **Публичная** - тип сети всегда будет общедоступным, несмотря на профиль подключенной сети. В этом случае применяются только правила брандмауэра для Публичной сети или те, которые определены для применения ко всем типам сети.

Чтобы настроить сетевые адаптеры:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **Файрвол**
4. Выберите вкладку **ТИП СЕТИ**.
5. Выберите настройки, которые Вы хотите применить при подключении к следующим адаптерам:
   - Wi-Fi
   - Ethernet

Настройка дополнительных параметров

Конфигурация дополнительных настроек фаервола:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **Файрвол**
4. Выберите вкладку **НАСТРОЙКИ**.

Можно настроить следующие параметры:

- **Блокировать сканирование портов** — обнаружение и блокирование попыток сканирования открытых портов.

  Сканирование портов часто используется хакерами для обнаружения открытых портов на вашем компьютере. Они могут проникнуть в ваш компьютер, если найдут уязвимый или менее защищенный порт.

- **Параноидальный режим** - предупреждения отображаются каждый раз, когда приложение пытается подключиться к Интернету Выберите **Разрешить** или **Заблокировать**. Когда включен Параноидальный режим, функции Автопилот и Профили автоматически выключаются.

Параноидальный режим можно использовать одновременно с **Режим работы батареи**.

- **Скрытый режим** - параметр, определяющий возможность быть обнаруженным другими компьютерами. Нажмите **Изменить скрытые подключения** , чтобы выбрать, когда ваше устройство должно или не должно быть видимым для других компьютеров.
- **Поведение приложения по умолчанию** - разрешитьBitdefender применять автоматические настройки к приложениям без определенных правил. Нажмите **Настроить приложения** , чтобы выбрать, следует ли применять автоматические настройки или нет.
  - Автоматический доступ к приложениям будет разрешен или запрещен на основе автоматического брандмауэра и пользовательских правил.
  - Разрешить- приложения, которые не имеют определенного правила брандмауэра, будут автоматически разрешены.
  - Блокировать - приложения, которые не имеют определенного правила брандмауэра, будут автоматически заблокированы.

4.6. 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.

Сканирование системы на наличие уязвимостей

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

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку действия **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 @).

- **Слабые 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.

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 на иконку в нижнем левом углу Bitdefender interface.
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 **ВКЛЮЧИТЬ**.
   - 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 **ПОМЕНЯТЬ ПАРОЛЬ**, чтобы принудительно 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 **ИСПРАВИТЬ**, чтобы отключить ее.
   - Если на маршрутизаторе, который вы настроили, установлен ненадежный пароль, нажмите **ИЗМЕНИТЬ ПАРОЛЬ**, чтобы получить доступ к интерфейсу, где вы можете установить надежный пароль.
   - Если сеть, к которой вы подключены, имеет уязвимости, которые могут подвергнуть вашу систему риску, нажмите **ИЗМЕНЕНИЕ НАСТРОЕК WIFI** .

Для настройки параметров мониторинга уязвимостей:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **УЯЗВИМОСТИ** нажмите переключатель ВКЛ/ВЫКЛ.

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

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

Критические обновления Windows

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

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.

Слабые 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 @).

Автозапуск носителя

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

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

Уведомления Советника Wi-Fi безопасности

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.

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

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

Включение/отключение уведомлений Wi-Fi Советника безопасности

Чтобы включить или выключить уведомления Советника Безопасности:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **УЯЗВИМОСТИ**
4. В окне **НАСТРОЙКИ** нажмите соответствующий переключатель ВКЛ/ВЫКЛ.

Настройка домашней сети Wi-Fi

Для того, чтобы приступить к настройке домашней сети:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **УЯЗВИМОСТИ** нажмите **Wi-Fi Советник Безопасности** .
4. На вкладке **Домашний wi-fi** нажмите кнопку **Выбрать домашний wi-fi**.

   Будет отображен список беспроводных сетей, к которым вы подключались ранее.
5. 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**.

Публичные Wi-Fi

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

- Активный Контроль Угроз включен
- Фаервол Bitdefender включен и следующие настройки применяются для беспроводного адаптера:
  - Режим "Невидимки" - включен
  - Тип сети - Публичная

- Включены следующие настройки Веб-защиты:
  - Сканировать SSL
  - Защита от мошенничества
  - Защита от фишинга
- Кнопка, открывающая Bitdefender Safepay™, доступна. В этом случае по умолчанию включена защита HotSpot для незащищенных сетей.

Проверка информации о сетях Wi-Fi

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

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **УЯЗВИМОСТИ** нажмите **Wi-Fi Советник Безопасности** .
4. В зависимости от информации, которую вам необходимо получить, выберите одну из двух вкладок: **ДомашнийWi-Fi** или **Общедоступный Wi-Fi**.
5. 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.

4.7. Защита веб-камеры

Тот факт, что хакеры могут захватить вашу веб-камеру, чтобы шпионить за вами -это больше не новинка. И такие решения для ее защиты, как отмена привилегий приложения, отключение встроенной камеры не практичны. Чтобы предотвратить дальнейшие попытки получить доступ к Вашей конфиденциальности, Bitdefender Защита веб-камеры постоянно отслеживает приложения, которые пытаются получить доступ к Вашей камере, и блокирует те, которые не указаны как надежные.

В качестве меры безопасности Вы будете получать уведомления каждый раз, когда обнаружена и заблокирована атака программы-вымогателя, даже если задействована функция автопилота.

Включение и выключение Защиты веб-камеры

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **ЗАЩИТА ВЕБ-КАМЕРЫ** нажмите переключатель ВКЛ/ВЫКЛ.

Настройка защиты веб-камеры

Вы можете настроить, какие правила следует применять, когда приложение попытается получить доступ к камере, выполнив следующие действия:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу **ЗАЩИТА ВЕБ-КАМЕРЫ**

Правила блокирования приложений

- **Блокировать весь доступ к веб-камере** - никакому приложению не разрешается получать доступ к Вашей веб-камере.
- **Блокировать доступ браузеров к веб-камере** - ни один веб-браузер, кроме Internet Explorer и Microsoft Edge, не получит доступ к Веб-камере. В связи с тем, что приложения Windows Store запускается в одном процессе, Internet Explorer и Microsoft Edge не могут быть обнаружены Bitdefender в качестве веб-браузеров и поэтому исключены из этого параметра
- **Установка доступа к веб-камерам приложения на основе выбора пользователей Bitdefender** - если большинство пользователей Bitdefender считают популярное приложение безопасным, тогда его доступ к веб-камере будет автоматически установлен на Разрешить. Если популярное приложение считается опасным для многих, то его доступ будет автоматически заблокирован.

Вы будете проинформированы каждый раз, когда одно из установленных приложений будет отмечено как заблокированное большинством пользователей Bitdefender, даже если задействована функция автопилота.

Уведомления

- **Уведомлять, когда разрешенные приложения подключаются к веб-камере** - Вы получите уведомление всякий раз, когда разрешенное приложение будет получать доступ к веб-камере, даже если включена функция автопилота.

Добавление приложений в Список защиты веб-камеры

Приложения, которые пытаются подключиться к веб-камере, автоматически обнаруживаются и в зависимости от их поведения и выбора сообщества, их доступ разрешен или запрещен. Однако Вы можете вручную вручную настроить, какие действия следует предпринять, выполнив следующие шаги:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **ЗАЩИТА ВЕБ-КАМЕРЫ** нажмите **Доступ к веб-камере**.
4. В окне с описанием функции защиты веб-камеры щелкните ссылку **Начать добавление приложений в список доступа к веб-камерам** .
5. Перейдите в EXE-файл, который хотите добавить в список, и нажмите **ОК** .
6. Щелкните переключатель доступ разрешен/доступ заблокирован.

   Чтобы просмотреть, что другие пользователи Bitdefender выбрали для данного приложения, нажмите значок .

Чтобы добавить дополнительные приложения, нажмите ссылку **Добавить новое приложение в список** .

В этом окне появятся приложения, которые будут запрашивать доступ к вашей камере вместе со временем последнего действия.

Вы будете получать уведомления каждый раз, когда одно из разрешенных приложений блокируется пользователями Bitdefender, независимо от статуса автопилота.

Замечание

Поскольку приложения Windows Store работают в едином процессе, каждый раз, когда доступ к одному из его приложений установлен на режиме «Разрешить» или «Блокировать», данное правило будет применяться ко всей системе. Примеры таких приложений:Internet Explorer и Microsoft Edge.

4.8. Безопасные файлы

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, или посещение зараженных веб-сайтов, и установки вредоносных приложений, не давая пользователю знать, что происходит в его системе.

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 приложения во время запуска.

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

Замечание

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.

Включение или выключение Безопасных Файлов

Чтобы включить или отключить функцию Безопасные Файлы:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите переключатель ВКЛ/ВЫКЛ.

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

Замечание
Функция Безопасные файлы включена по умолчанию.

Защита личных файлов от атак вымогателей

Если вы хотите хранить личные файлы под защитой:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Защищенные папки**.
4. В окне с описанием функции «Безопасные файлы» нажмите кнопку **ЗАЩИТИТЬ БОЛЬШЕ ПАПОК**.
5. Выберите папку, которую Вы хотите защитить и нажмите **OK** .

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

Папки «Фотографии», «Видео», «Музыка», «Рабочий стол» и «Загрузки» защищены от 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.

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

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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Доступ к приложениям**.
4. В списке указаны приложения, которые запросили изменить файлы в ваших защищенных папках. Нажмите "Разрешить" и выберите приложение, в безопасности которого вы уверены.

В том же окне Вы можете отключить защиту от программы-вымогателя для определенных приложений, щелкнув переключатель «Блок».

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

Защита при загрузке системы

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

Чтобы отключить Защиту при загрузке:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите значок в нижнем правом углу модуля **БЕЗОПАСНЫЕ ФАЙЛЫ**
4. Нажмите переключатель ВКЛ/ВЫКЛ.

Замечание
Приложения, добавленные к исключениям, будут также сканироваться и соответственно обрабатываться.

4.9. Шифрование файла

Шифрование файлов Bitdefender позволяет создавать на вашем компьютере зашифрованные и защищенные паролем логические диски (или хранилища), где вы можете безопасно хранить свои конфиденциальные и важные документы. Доступ к данным, хранящимся в этих хранилищах, могут получать пользователи, которые знают пароль.

Пароль позволяет открывать и хранить данные, а также закрывать хранилище, обеспечивая их безопасность. Пока хранилище открыто, вы можете добавлять новые файлы, получать доступ к текущим файлам или изменять их.

Физически хранилище представляет собой расположенный на локальном жестком диске файл с расширением .bvd. Хотя физические файлы, которые представляют собой диски хранилища, можно открывать из различных операционных систем (таких как Linux), информация, хранящаяся на них, не может быть прочитана, так как она зашифрована.

Управление хранилищами файлов может осуществляться из окна Bitdefender или с помощью контекстного меню Windows и логических дисков, связанных с хранилищем.

Управление хранилищем файлов

Для управления хранилищем файлов из Bitdefender, нажмите значок на левой боковой панели Bitdefender интерфейс.

Существующие хранилища файлов появятся в модуле **Хранилище файлов**.

Создание файловых хранилищ

Создать новое Хранилище:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

3. На панели **ШИФРОВАНИЕ ФАЙЛОВ** выберите **Создать хранилище файлов**.
4. Укажите имя и расположение файла хранилища.
   - Введите имя файла хранилища в соответствующем поле.
   - Нажмите **Обзор**, выберите расположение хранилища и сохраните файл хранилища под желаемым именем.
5. Выберите букву диска из соответствующего меню. Когда вы открываете Хранилище, виртуальный диск появляется в окне Мой компьютер.
6. Если вы хотите изменить стандартный размер (100 МБ) хранилища, введите нужное значение в поле **Размер хранилища(MB)**, используя клавиши стрелки.
7. Введите новый пароль хранилища в полях **Пароль** и **Подтвердить пароль**. Пароль должен быть не менее 8 символов. Любой пользователь, пытающийся открыть хранилище и получить доступ к его файлам, должен предоставить пароль.
8. Нажмите **Создать**.

Bitdefender немедленно проинформирует вас о результате операции. Если произошла ошибка, используйте сообщение об ошибке для устранения неполадок.

Чтобы быстро создать новое защищенное хранилище, щелкните правой кнопкой мыши на рабочем столе или в папке на вашем компьютере, выберите пункт **Bitdefender** > **Bitdefender Хранилище файлов** и выберите **Создать хранилище файлов**.

Замечание

Это может оказаться удобным - хранить все хранилища файлов в одном и том же месте. Таким образом, вы сможете быстрее их найти.

Импорт хранилища файлов

Чтобы импортировать хранилище файлов, хранящихся локально:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **Шифрование файлов** выберите **Импорт хранилища файлов**.

4. Найдите местоположение хранилища и выберите его (файл db).
5. Нажмите **Открыть**.

Открытие хранилище файлов

Для работы с файлами, расположенными в хранилище, необходимо открыть хранилище. При открытии хранилища, виртуальный диск появится в окне Мой компьютер. Этот диск будет обозначен буквой, назначенной хранилищу.

Чтобы открыть хранилище:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.

   Существующие хранилища файлов появятся в модуле **Хранилище файлов**.
2. Нажмите ссылку **Просмотр хранилищ**, а затем выберите хранилище, которое вы хотите открыть.
3. Нажмите на кнопку **Разблокировать**, а затем введите нужный пароль.
4. Нажмите **ОК**, а затем кнопку **Открыть**, чтобы открыть хранилище.

Bitdefender немедленно проинформирует вас о результате операции. Если произошла ошибка, используйте сообщение об ошибке для устранения ошибки.

Чтобы быстрее открыть защищенное хранилище, найдите на своем компьютере файл .bvd, представляющий хранилище, которое вы хотите открыть. Щелкните правой кнопкой на файле хранилища на вашем компьютере, укажите на **Bitdefender File Хранилище** и выберите **Открыть**. Введите пароль и нажмите **ОК**.

Добавление файлов в хранилища

Прежде чем добавлять файлы и папки в хранилище, необходимо сначала его открыть.

Чтобы добавить новые файлы в хранилище:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите в правом нижнем углу панели **ШИФРОВАНИЕ ФАЙЛА**

4. В окне **МОИ ХРАНИЛИЩА**, выберите хранилище, которое вы хотите открыть.
5. Нажмите на кнопку **Разблокировать**, а затем введите нужный пароль.
6. Нажмите кнопку **Открыть**, чтобы открыть хранилище.
7. Добавляйте файлы или папки, как вы обычно делаете в ОС Windows (например, вы можете использовать традиционный метод копировать-вставить).

Для быстрого добавления файлов в защищенное хранилище, щелкните правой кнопкой мыши файл или папку, которую вы хотите скопировать в хранилище, выберите пункт **Bitdefender Хранилище файлов** и нажмите **Добавить файл в хранилище**.

- Если открыто только одно хранилище, файл или папка будут скопированы в это хранилище.
- Если открыто несколько хранилищ, вам будет предложено выбрать куда скопировать элемент. Выберете в меню соответствующий диск и нажмите **ОК** чтобы скопировать элемент.

Блокировка хранилищ

Когда вы закончите работать с хранилищем файлов, вам нужно будет заблокировать его, чтобы защитить свои данные. Блокируя хранилище, соответствующий виртуальный диск исчезает с "Мой компьютер". Следовательно, доступ к данным, хранящимся в хранилище, полностью блокируется.

Чтобы заблокировать хранилище:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. В области **хранилище файлов** нажмите **Просмотр хранилищ** .
3. В окне **Мои хранилища** выберите хранилище, которое нужно заблокировать.
4. Нажмите кнопку **Заблокировать**.

Bitdefender немедленно проинформирует вас о результате операции. Если произошла ошибка, используйте сообщение об ошибке для устранения неполадок.

Чтобы быстро заблокировать защищенное хранилище, щелкните правой кнопкой мыши на файле .bvd, представляющего хранилище, выберите пункт **Bitdefender Хранилище файлов** и нажмите кнопку **Заблокировать**.

Удаление файлов из хранилищ

Чтобы удалить файлы или папки из хранилища, необходимо открыть хранилище. Чтобы удалить файлы или папки из хранилища:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите в правом нижнем углу панели **ШИФРОВАНИЕ ФАЙЛА**
4. В окне **Мои хранилища**, выберите хранилище, из которого вы хотите удалить файлы.
5. Нажмите кнопку **Разблокировать**, в случае если оно заблокировано.
6. Нажмите кнопку **Открыть**.

   Удалите файлы так, как вы обычно делаете это в Windows (например, щелкните правой кнопкой мыши по файлу, который хотите удалить, и выберите **Удалить**).

Изменение пароля хранилища

Пароль защищает содержимое хранилища от несанкционированного доступа. Только пользователи, знающие пароль, могут открыть хранилище и получить доступ к документам и данным, хранящимся в нем.

Хранилище должно быть заблокировано, прежде чем можно будет изменить пароль. Чтобы изменить пароль хранилища:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите в правом нижнем углу панели **ШИФРОВАНИЕ ФАЙЛА**
4. В окне **Мои хранилища**, выберите хранилище, в котором вы хотите изменить пароль.
5. Нажмите кнопку **Настройки**.

6. Введите текущий пароль хранилища в поле **Старый пароль**.
7. Введите новый пароль хранилища в полях **Новый пароль** и **Подтвердить новый пароль**.

> **Замечание**
> Пароль должен быть не менее 8 символов. Для того, чтобы пароль был сильным, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, #, $ или @).

Bitdefender немедленно проинформирует вас о результате операции. Если произошла ошибка, используйте сообщение об ошибке для устранения неполадок.

Для того, чтобы быстро сменить пароль защищенного хранилища, найдите на своем компьютере файл .bvd, представляющий это хранилище. Щелкните правой кнопкой на файле, укажите на **Хранилище файлов Bitdefender** и выберите **Изменить пароль хранилища**.

4.10. Защита ваших учетных данных при помощи 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, компонент 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 к приложениям
- Пароли к сетям Wi-Fi

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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **КОШЕЛЕК** нажмите **Создать новый Кошелек**.
4. Нажмите кнопку **Создать новый** .
5. 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.

6. Нажмите **Продолжить**.
7. На этом шаге вы можете выбрать хранение информации в облаке. Если вы выберите Да, банковская информация будет храниться локально на вашем устройстве. Выберите нужный вариант, а затем нажмите **Продолжить**.
8. Выберите веб-браузер, из которого вы хотите импортировать учетные данные.
9. Нажмите **Завершить**.

Импортировать существующую базу данных

Чтобы импортировать базу данных кошелька, хранящуюся локально:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **КОШЕЛЕК** нажмите **Создать новый Кошелек**.
4. Нажмите кнопку **От целевой**.
5. Перейдите к местоположению на устройстве, где требуется сохранить базу данных кошелька, а затем выберите имя для него.
6. Нажмите **Открыть**.
7. Укажите имя Вашего Кошелька и введите пароль, заданный при первоначальной установке.
8. Нажмите **Импорт**.
9. Выберите программы, из которых требуется импортировать учетные данные Кошелька, а затем кнопку **Завершить**.

Экспорт базы данных Кошелька

Чтобы экспортировать базу данных Кошелька:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **КОШЕЛЕК** нажмите **Мои кошельки**.

4. Нажмите на значок ⋮ желаемого кошелька, затем выберите **Экспорт**.
5. Выполните поиск местоположения базы данных кошелька и выберите ее (файл. db).
6. Нажмите **Сохранить**.

Замечание
Кошелек должен быть открыт для того, чтобы опция **Экспорт** была доступна.
Если кошелек, который нужно экспортировать, заблокирован, нажмите кнопку **АКТИВИРОВАТЬ КОШЕЛЕК**, затем введите пароль, заданный первоначально.

Синхронизация ваших Кошельков в облаке

Чтобы включить или выключить синхронизацию бумажника с облаком:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **КОШЕЛЕК** нажмите **Мои кошельки**.
4. Нажмите значок ⋮ желаемого кошелька, затем выберите **Настройки**.
5. Выберите нужную опцию в появившемся окне, а затем нажмите **Сохранить**.

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

Управление учетными данными Кошелька

Для управления вашими паролями:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

3. В области **КОШЕЛЕК** нажмите **Мои кошельки**.
4. Выберите нужную базу данных кошелька из окна **МОИ КОШЕЛЬКИ**, затем нажмите кнопку **АКТИВИРОВАТЬ КОШЕЛЕК**.
5. Введите мастер-пароль, а затем нажмите кнопку **ОК**.

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

- Личные
- Веб-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**.

Включение и отключение защиты Менеджера паролей

Чтобы включить или отключить защиту Менеджера Паролей:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **КОШЕЛЕК** нажмите переключатель ВКЛ/ВЫКЛ.

Управление настройками Менеджера паролей

Чтобы детально настроить мастер-пароль:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.

2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок ⚙ в нижнем правом углу панели **Кошелек**.
4. Выберите вкладку **ПАРАМЕТРЫ БЕЗОПАСНОСТИ**.

Доступны следующие опции:

- **Спрашивать мастер-пароль при включении компьютера** - при доступе к компьютеру 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.
- **Автоматически блокировать Кошелек, когда я оставляю компьютер без присмотра** - Вам будет предложено ввести мастер-пароль, когда вы вернетесь к компьютеру 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 на 👁 иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок ⚙ в нижнем правом углу панели **Кошелек**.
4. Выберите вкладку **ПЛАГИНЫ**.

   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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **Кошелек**.
4. Выберите вкладку **ПАРАМЕТРЫ АВТОЗАПОЛНЕНИЯ**.
5. Настройте следующие опции:
   - **Настройка способа защиты учетных данных кошелька**:
     - **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-сайты - открывает подменю со всеми логинами веб-сайтов хранящихся в Кошельке. Нажмите **Добавить веб-сайт**, 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.

4.11. 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.

Замечание

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.

Установка VPN

Приложение VPN можно установить из интерфейса Bitdefender следующим образом:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **VPN** нажмите **Включить VPN**.
4. В окне с описанием приложения VPN прочитайте **Лицензионное соглашение**, затем нажмите **ВКЛЮЧИТЬ Bitdefender VPN**.

   Подождите несколько минут, пока файлы загрузятся и установятся

Замечание

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.

Открытие VPN

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

- Из системного трея

1. Щелкните правой кнопкой мыши значок в системном трее, затем нажмите **Показать**.

- Из интерфейса Bitdefender:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку действия **VPN**.

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. 165).

Чтобы подключиться или отключиться, просто нажмите на статус, отображаемый в верхней части экрана, или щелкните значок панели задач правой кнопкой мыши. Значок в системном трее 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.
- **Поддержка** - обратитесь в службу поддержки клиентов, если Вам необходима помощь в настройке продукта.
- **Информация** - отображение информации об установленной версии.

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 Total Security 2018, это значит,что Вы можете пользоваться ее возможностями, независимо от Вашей антивирусной подписки. В случае истечения срока действия подписки Bitdefender Premium VPN при активной Bitdefender Total Security 2018, Вы вернетесь к бесплатной версии.

4.12. 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 дополнительной информации перейдите к «*Защита ваших учетных данных при помощи Менеджер паролей*» (p. 155).

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 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™.

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 на  иконку в нижнем левом углу Bitdefender interface.
  2. Нажмите кнопку быстрого действия **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.

Замечание

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  .

Замечание
Для переключения между режимами рабочего стола Windows и Bitdefender Safepay™, нажмите клавиши **Alt+Tab** или нажмите кнопку **Свернуть**.

Настройка параметров

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

- В разделе **Общие настройки** вы можете настроить следующее:

  Поведение Bitdefender Safepay™

  Выберите действие при входе на сайт Интернет-магазина или Интернет-банкинга через ваш обычный веб-браузер:
  - Автоматически открывать веб-сайты в Безопасном платеже.
  - Предлагать мне использовать Безопасный платеж.
  - Не предлагать мне использовать Безопасный платеж.

  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.

- В разделе **Расширенные настройки** доступны следующие опции:

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.

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.

   Замечание
   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.

4.13. Защита данных

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. Появится окно подтверждения. Нажмите **Да, УДАЛИТЬ**, чтобы запустить мастер Файлового шредера 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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **ЗАЩИТА ДАННЫХ** выберите **Файловый шредер**.
4. 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

4.14. Родительский контроль

Функция Родительского Контроля позволяет управлять доступом к Интернету и конкретным приложениям для каждого устройства, на котором установлена эта функция. После того, как вы настроили Родительский контроль, вы можете легко узнать, что ваш ребенок делает на используемом устройстве и где он находился за последние 24 часа. Кроме того, чтобы помочь вам лучше знать о действиях ребенка, приложение предлагает статистику его действий и интересов.

Для этого потребуется только компьютер с доступом в Интернет и веб-браузер.

Можно настроить в Родительском контроле блокировку:

- неприемлемых веб-страниц.

- приложений, например, игры, чаты, программы обмена файлами и другие.
- блокировать определенные контакты, чтобы не позволять им связываться по телефону с вашим ребенком.

Проверьте действия своих детей и измените настройки Родительского контроля с помощью учетной записи Bitdefender с любого компьютера или мобильного устройства, подключенного к Интернету.

Доступ к Родительскому контролю - Мои дети

После того, как будет выполнен вход к разделу Родительский контроль, откроется окно **МОИ ДЕТИ**. Здесь можно просматривать и редактировать все профили, созданные для ваших детей. Профили отображаются в виде карточек профиля, что позволяет быстро управлять ими и проверять их состояние.

Как только профиль будет создан, можно приступить к более детальной настройке для контроля и управления доступом к сети Интернет и к определенным приложениям для ваших детей.

Вы можете получить доступ к параметрам Родительского контроля из учетной записи Bitdefender Central на любом компьютере или мобильном устройстве, подключенном к Интернету.

Войдите в вашу учетную запись Bitdefender:

- На любом устройстве с доступом в Интернет:
  1. Войдите в ваш Bitdefender Central.
  2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
  3. Выберите функцию **Родительский Контроль** .
  4. В появившемся окне **МОИ ДЕТИ** вы можете управлять и настраивать профили родительского контроля для любого устройства.
- Из интерфейса Bitdefender:
  1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
  2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
  3. На панели **Родительский контроль**, выберите **Настроить**.

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

4. Выберите функцию **Родительский Контроль** .
5. В появившемся окне **МОИ ДЕТИ** вы можете управлять и настраивать профили родительского контроля для любого устройства.

Замечание
Необходимо войти в систему с учетными данными администратора. Только пользователи с правами администратора (системные администраторы) могут получить доступ к настройкам Родительского контроля.

Добавление профиля вашего ребенка

Для запуска мониторинга действий Вашего ребенка, необходимо настроить профиль и установить агент Bitdefender Родительский контроль на используемых устройствах.

Чтобы добавить профиль ребенка в Родительский контроль:

1. Войдите в панель Родительский контроль из Bitdefender Central.
2. Нажмите **ДОБАВИТЬ ПРОФИЛЬ** на правой стороне окна **МОИ ДЕТИ**.
3. Укажите конкретную информацию в соответствующих полях, например: имя и дата рождения. Чтобы добавить фотографию профиля, нажмите ссылку **Выбрать файл** . Для продолжения нажмите **ДАЛЕЕ**

   Основываясь на стандартах развития детей, установки даты рождения ребенка автоматически загружает настройки для поиска в Интернете, которые считаются подходящими для его возрастной категории.
4. Если на устройстве вашего ребенка уже установлен Bitdefender Total Security, выберите его устройство из списка доступных, а затем выберите учетную запись, которую вы хотите контролировать. Нажмите **СОХРАНИТЬ**.

   Если Ваш ребенок использует Android или iOS устройства и Bitdefenderприложение Родительский Контроль не установлено, нажмите кнопку **Добавить устройство**. Если Ваш ребенок использует устройство Mac и приложение Bitdefender Антивирус для Mac не

установлено, нажмите ту же кнопку. Выберите операционную систему, которую хотите установить, и нажмите **ДАЛЕЕ**, чтобы продолжить.

5. Введите адрес электронной почты на которую мы отправим ссылку на скачивание, чтобы установить в Bitdefender приложение, затем нажмите **ОТПРАВИТЬ ССЫЛКУ ДЛЯ УСТАНОВКИ**.

Важно

На устройствах под управлением Windows необходимо загрузить и установить Bitdefender Total Security, включенный в вашу подсылку.
На устройствах на базе MacOS необходимо загрузить и установить продукт Bitdefender Антивирус для Mac.
На устройствах Android и iOS необходимо загрузить и установить приложение Bitdefender Родительский Контроль.

Присвоение нескольких устройств одному профилю

Вы можете назначить несколько устройств одному и тому же профилю, чтобы применить те же ограничения:

1. Войдите в ваш Bitdefender Central.
2. Выберите функцию Родительский Контроль .
3. Нажмите значок ⋮ на нужной карточке профиля и выберите **Устройства** .
4. Выберите из списка доступные устройства, к которым вы хотите присвоить профиль.

   Если Ваш ребенок использует Android или iOS устройства и Bitdefenderприложение Родительский Контроль не установлено, нажмите кнопку **Добавить устройство**. Если Ваш ребенок использует устройство Mac и приложение Bitdefender Антивирус для Mac не установлено, нажмите ту же кнопку. Выберите операционную систему, которую хотите установить, и нажмите **ДАЛЕЕ**, чтобы продолжить.

   Введите адрес электронной почты на которую мы отправим ссылку на скачивание, чтобы установить в Bitdefender приложение, затем нажмите **ОТПРАВИТЬ ССЫЛКУ ДЛЯ УСТАНОВКИ**.
5. После завершения процесса установки на новом устройстве, выберите его из списка, чтобы применить профиль.

6. Выберите **СОХРАНИТЬ**.

Связать Родительский контроль с Bitdefender Central

Чтобы отслеживать онлайн-действия ребенка на Android и iOS, Вы должны соединить свое устройство с его учетной записи Bitdefender, выполнив вход в учетную запись из приложения.

Чтобы связать ваше устройство с учетной записью Bitdefender:

- На **Android**:

  1. Выберите кнопку, которая появится в электронном письме, отправленного с нашего сервера. Вы будете перенаправлены в Google Play Store.

     Если вы не перешли из учетной запись Bitdefender по ссылке для загрузки, перейдите в Google Play и выполните поиск приложения Bitdefender Родительский контроль.

  2. Нажмите **УСТАНОВИТЬ** в окне Bitdefender Родительский контроль, затем нажмите **ПРИНЯТЬ**, если вас попросят принять разрешения. Bitdefender необходимы разрешения, чтобы информировать о действиях Вашего ребенка, если они не будут приняты - приложение не установится.

  3. Откройте приложение Родительского контроля.

  4. Прочитайте **Соглашение о подписке** , затем нажмите **ПРОДОЛЖИТЬ** .

  5. Войдите в учетную запись Bitdefender или выполните вход, используя аккаунт Google.

     Если у Вас нет учетной записи Bitdefender, можете создать ее, используя соответствующую опцию.

  6. Нажмите **ПЕРЕЙТИ К НАСТРОЙКАМ**, для перехода на экран, на котором можно включить опцию «Специальные возможности» для приложения. Следуйте инструкциям на экране, чтобы корректно настроить приложение.

  7. Нажмите **ПЕРЕЙТИ К НАСТРОЙКАМ**, для перехода на экран, на котором можно включить опцию «Специальные возможности» для

приложения. Следуйте инструкциям на экране, чтобы корректно настроить приложение.

8. Нажмите **ПЕРЕЙТИ К НАСТРОЙКАМ**для перехода на экран, на котором можно включить параметр «Активировать права администратора устройства» для приложения. Следуйте инструкциям на экране, чтобы корректно настроить приложение.

   Это не позволит ребенку удалить приложение Родительский Контроль.

9. Нажмите **ГОТОВО**, для завершения процесса установки.

> **Замечание**
> На устройствах Android 4. 4 и более поздних версиях для отслеживания SMS-сообщений ребенка в Bitdefender необходимо изменить установленные настройки приложения Android Messages. Выберите **Да** в появившемся диалоговом окне после нажатия **ГОТОВО** в приложении.

- На **iOS**:

1. Выберите кнопку, которая появится в электронном письме, отправленного с нашего сервера, затем установите приложение.
2. Откройте приложение Родительского контроля.
3. Отображается мастер установки, содержащий подробную информацию о характеристиках программы. Для продолжения нажмите **Далее**
4. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
5. Разрешите доступ к местонахождению устройства, чтобы Bitdefender обнаружил его.
6. Разрешите приложению отправлять уведомления.
7. Свяжите устройство с профилем Вашего ребенка.

Мониторинг действий ребенка

Bitdefender помогает отслеживать онлайн-действия детей.

Таким образом, вы всегда сможете узнать, какие сайты они посещали, какие приложения использовали или какие действия были заблокированы Родительским контролем.

В зависимости от ваших настроек, отчеты могут содержать подробную информацию для каждого события, например:

- Состояние события.
- Важность уведомления.
- Имя устройства.
- Дата и время события.

Для контроля Интернет-трафика, доступа к приложениям или действиям ребенка в сети Facebook, выполните следующие действия:

1. Войдите в панель Родительский контроль из Bitdefender Central.
2. Выберите нужную карточку устройства.

   В окне **Действие** можно просматривать интересующую Вас информацию. Или выберите ссылку **Просмотр текущего действия** на карточке контролируемого устройства для перехода в окно **Действия**

Конфигурация Общих настроек

Если включен Режим Родительского Контроля, журнал действий детей ведется по умолчанию.

Для получения уведомлений по электронной почте:

1. Войдите в панель Родительский контроль из Bitdefender Central.
2. Выберите вкладку **Настройки** в верхнем правом углу.
3. Включите соответствующую опцию для получения отчетов о действиях.
4. Введите адрес электронной почты, на который будут отправляться уведомления.
5. Получать следующее уведомления по электронной почте:
   - Заблокированные сайты
   - Заблокированные приложения

- Области ограниченного доступа
- Вызов, полученный от заблокированного номера телефона
- Удаление родительского контроля на приложении Facebook

6. Нажмите **СОХРАНИТЬ**.

Редактирование профиля

Чтобы редактировать существующий профиль:

1. Войдите в ваш Bitdefender Central.
2. Нажмите на панель **Родительский контроль**.
3. Нажмите ⋮ иконку на желаемой карточке профиля, а затем выберите **Редактировать**.
4. После настройки желаемых параметров, выберите **СОХРАНИТЬ**.

Удаление профиля

Чтобы удалить существующий профиль:

1. Войдите в ваш Bitdefender Central.
2. Нажмите на панель **Родительский контроль**.
3. Нажмите ⋮ иконку на карточке желаемого профиля, а затем выберите **Удалить**.
4. Подтвердите свой выбор.

Настройка профиля Родительского контроля

Чтобы начать мониторинг Вашего ребенка, необходимо связать профиль с устройством, на котором установлен агент Bitdefender Родительского контроля.

После добавления профиля вашего ребенка, вы можете настроить более подробные настройки для контроля и управления доступом к Интернету и к конкретным приложениям.

Для начала настройки профиля, выберите нужную карточку профиля из окна **МОИ ДЕТИ**

Щелкните вкладку, чтобы настроить соответствующую функцию Родительского контроля для устройства:

- Действия - отображение всех действий, местоположений и общение с друзьями, начиная текущего дня.
- Приложения - позволяет блокировать доступ к определенным приложениям, например, игры, мессенджеры, фильмы и т.д.
- Веб-сайты - позволяет фильтровать веб-навигацию.
- Контакты - здесь можно указать какие контакты из списка ребенка могут общаться с ним по телефону.
- Локация ребенка - здесь Вы можете установить безопасные местоположения или не являющиеся таковыми для Вашего ребенка.
- Соц.сети - позволяет блокировать доступ к социальным сетям.
- Расписание - позволяет заблокировать доступ к устройствам, указанным в профиле ребенка.

Действие

Активное окно предоставит Вам подробную информацию об активностях Ваших детей за последние 24 часа, как внутри, так и за пределами дома. Для просмотра действий за предыдущие дни нажмите значок календаря в верхнем левом углу окна.

В зависимости от действий, это окно может включать информацию о:

- **Местоположения** - здесь вы можете посмотреть места, которые ребенок посещал в течение дня.
- **Интересы** - здесь Вы можете просмотреть данные о том, какие категории веб-сайтов посещал Ваш ребенок. Нажмите на ссылку **Просмотр нежелательного контента**, чтобы разрешить или запретить доступ к определенным контентам.
- **Виртуальное общение** - здесь Вы можете просмотреть контакты, с которыми общался Ваш ребенок. Нажмите на ссылку **Управление контактами**, чтобы выбрать контакты, с которыми ваш ребенок должен оставаться на связи, а с которыми нет.
- **Приложения** - здесь вы можете увидеть приложения, которыми пользуется Ваш ребенок. Чтобы заблокировать или разрешить доступ

к определенным приложениям, щелкните ссылку **Обзор ограничений приложения**.

- **Действия за день** - здесь вы можете увидеть время, проведенное в Интернете со всех устройств, назначенных ребенку, и посещаемые места. Собранная информация, начиная с текущего дня.

Приложения

Окно приложения позволяет блокировать запуск приложений. Игры, медиа, мессенджеры, а также другие категории программного обеспечения и вредоносных программ могут быть заблокированы таким образом.

Функция может быть включена или отключена с помощью соответствующего переключателя.

Чтобы настроить управление приложениями для конкретной учетной записи пользователя:

1. Отобразится список с карточками. Карточки представляют собой приложения, которые использует ваш ребенок.
2. Выберите карточку с тем приложением, которое хотите запретить для ребенка.

   Появится символ галочка, который означает, что ваш ребенок не сможет использовать данное приложение.

Веб-сайты

Окно Веб-сайты поможет вам блокировать веб-сайты с нежелательным содержимым Сайты, принимающие видео, игры, мессенджеры, а также другие категории негативного содержания могут быть заблокированы таким образом.

Функция может быть включена или отключена с помощью соответствующего переключателя.

В зависимости от возраста, установленного для вашего ребенка, список Интересы включает выбранную категорию по умолчанию. Чтобы разрешить или запретить доступ к определенной категории, щелкните по ней.

Появляется символ галочка, которая означает, что ваш ребенок не сможет получить доступ к содержимому, связанному с конкретной категорией.

Разрешить или заблокировать доступ к веб-сайту

Чтобы разрешить или ограничить доступ к определенным веб-страницам, вы должны добавить их в список исключений, а именно:

1. Нажмите кнопку **УПРАВЛЕНИЕ**.
2. Введите веб-страницу, которую вы хотите заблокировать, в соответствующем поле.
3. Выберите **Разрешить** или **Заблокировать**.
4. Нажмите **ЗАВЕРШИТЬ**, чтобы сохранить изменения.

Замечание

Ограничения доступа к веб-сайтам могут быть установлены только для устройств Windows, Android и macOS, добавленных к профилю Вашего ребенка.

Телефонные контакты

Окно Телефонные контакты дает возможность указать, какие контакты из списка друзей Вашего ребенка могут или не могут общаться с ним по телефону.

Чтобы исключить конкретный телефонный номер из контактов, следует добавить к профилю Вашего ребенка устройство Android, которым он пользуется, выполнив следующие действия:

1. Выберите раздел **Родительский контроль** в Bitdefender Central.
2. Нажмите ссылку **Установить Родительский Контроль на устройстве** на желаемой карточке.
3. Нажмите **ДОБАВИТЬ УСТРОЙСТВО** в появившемся окне.
4. Опция **BitdefenderРодительский контроль для Android** выбрана по умолчанию. Для продолжения нажмите **ДАЛЕЕ**
5. Выберите профиль ребенка, на котором вы хотите установить ограничения.
6. Выберите вкладку **Телефонные контакты** .

Отобразится список с карточками. Карточки отобразят контакты со смартфона Вашего ребенка.

7. Выберите карточку с номером телефона, который хотите заблокировать.

   Появиться символ галочка, который означает, что ваш ребенок не сможет использовать выбранный номер телефона.

Чтобы заблокировать неизвестные номера телефонов, включите переключатель **ЗАБЛОКИРОВАТЬ НЕИЗВЕСТНЫЕ НОМЕРА**.

Замечание
Ограничения на телефонные звонки могут быть установлены только для устройств Android, добавленных в профиль Вашего ребенка.

Местонахождение ребенка

Посмотреть текущее местоположение вашего устройства на Google Maps. Местонахождение актуализируется каждые 5 секунд, так что вы сможете отследить все передвижения.

Точность расположения зависит от того, как Bitdefender определяет его:

- Если на устройстве включен GPS, местоположение устройства можно отследить с точностью до нескольких метров, пока оно находится в радиусе действия спутников GPS (т.е. не внутри здания).
- Если устройство в помещении, его местонахождение может быть определено с точностью до десятков метров, при условии, что включена функция Wi-Fi и есть доступные беспроводные сети в радиусе действия.
- Иначе, местонахождение будет определяться с использованием данных сети мобильной связи, которые могут предложить точность до нескольких сот метров.

Настройка местонахождения &Безопасная регистрация

Чтобы убедиться, что ваш ребенок находиться в "правильных" местах, вы можете составить список безопасных и небезопасных мест. Уведомление, подтверждающее безопасность ребенка будет появляться

каждый раз, когда он пересекает определенную область. Нажимая **Благополучное прибытие** , Вы получите уведомление из Вашей учетной записи Bitdefender о благополучном прибытии к месту назначения.

В том случае, если подтверждение от ребенка не поступило, Вы можете просмотреть историю его местонахождений в течение дня, проверив его профиль в своей учетной записи Bitdefender.

Чтобы настроить местоположение:

1. Нажмите **Устройства** в рамке, которая находится у вас в окне **Местоположение ребенка**.
2. Нажмите **ВЫБРАТЬ УСТРОЙСТВА**, а затем выберите устройство, которое вы хотите настроить.
3. В окне **Области**, нажмите кнопку **ДОБАВИТЬ ОБЛАСТЬ**.
4. Выберите тип местоположения **БЕЗОПАСНОЕ** или **ОГРАНИЧЕННОЕ**.
5. Введите действительное имя области, которую ребенок имеет или не имеет права посещать
6. Установите диапазон, который должен применяться для мониторинга из ползунка **Радиус**.
7. Нажмите **ДОБАВИТЬ ОБЛАСТЬ**, чтобы сохранить ваши настройки. Запрашивание информации о возможности передвижения детей в одиночку. Подтвердите Да или Нет.

Замечание

Трекер местоположения можно использовать для отслеживания устройств Android и iOS, на которых установлено приложение Bitdefender Родительский Контроль

Социальная сеть

При помощи функции родительского контроля отслеживается детская учетная запись на Facebook и подготавливаются отчеты об основных действиях ребенка.

Эти онлайн-действия проверяются и, если возникает угроза безопасности приватности ваших детей, Вы будете предупреждены.

Мониторинг элементов онлайн-аккаунта включает в себя:

- Информация об аккаунте

- Понравившиеся страницы
- Загруженные фото

Чтобы настроить защиту Facebook для определенной учетной записи пользователя, введите адрес электронной почты отслеживаемой детской учетной записи и нажмите **ОТПРАВИТЬ**.

Сообщите ребенку о ваших намерениях и попросите его нажать на ссылку активации **ЗАЩИТИТЬ АККАУНТ**, которую он получил в своей электронной почте.

Чтобы получить доступ к отслеживаемой учетной записи Facebook, нажмите ссылку **Просмотреть на Facebook**.

Чтобы остановить наблюдение за учетной записью, используйте кнопку сверху **РАЗЪЕДИНИТЬ УЧЕТНУЮ ЗАПИСЬ**.

Чтобы получить предупреждение по электронной почте об удалении приложения Родительский Контроль на устройстве ребенка, установите соответствующий флажок.

Расписание

Окно Расписание- позволяет заблокировать доступ к устройствам, установленным Вами в профиле ребенка. Ограничения можно установить в любые дни и время только для устройств на базе Android и Windows.

Чтобы начать настройку временных ограничений в ночное время:

1. В области **ВРЕМЯ СНА** установите флажок **Школьный вечери Выходной вечер**
2. Нажмите значок ⊗ в соответствующем поле, затем пользуясь клавишами со стрелками вверх и вниз, установите интервалы времени, в течение которых доступ должен быть заблокирован.

Чтобы начать настройку временных ограничений в течение дня:

1. В области **ЛИМИТ ДНЕВНОГО ВРЕМЕНИ** имеются следующие опции:
   - **СОВОКУПНЫЙ**
     a. Установите флажки на **Лимит времени в учебные дни** и **Лимит времени в выходные**.

b. Перетащите слайдеры вдоль шкалы, чтобы установить разрешенное время для доступа к устройствам.

- **ОСОБЫЙ**

a. Установите флажки на **Лимит времени в учебные дни** и **Лимит времени в выходные**.

b. Выберите в сетке периоды, в течение которых доступ в Интернет будет заблокирован.

Замечание
Настройки **СОВОКУПНЫЕ** и **ОСОБЫЙ** предназначены для работы отдельно друг от друга.

4.15. Устройство Анти-вор

Кража ноутбука является серьезной проблемой, которая может затронуть отдельных лиц и организации. Потеря данных может причинить более значительный ущерб (как финансовый, так и эмоциональный), чем потеря самого оборудования.

Тем не менее, люди принимают необходимые меры, чтобы обезопасить свои важные личные, деловые и финансовые данные в случае кражи или потери.

Bitdefender Анти-вор поможет вам лучше подготовиться к такому событию, позволяя удаленно найти или заблокировать ноутбук и даже стереть на нем все данные, если вы когда-либо расстанетесь с ноутбуком против вашей воли.

Для использования функции Анти-вор необходимо соблюдение следующих условий:

- Команды могут быть посланы только из учетной записи Bitdefender.
- Для получения команд ноутбук должен быть подключен к Интернету.

Функция Анти-вор работает следующим образом:

Местоположение

Посмотреть местоположение вашего устройства на Google Maps.

Точность расположения зависит от того, как Bitdefender определяет его. Местоположение определяется с точностью до десятков метров

если Wi-Fi включен на вашем ноутбуке и в радиусе действия есть беспроводные сети.

Если компьютер подключен к проводной локальной сети без доступных сетей Wi-Fi, то местоположение будет определяться на основании IP-адреса, которое является менее точным.

Тревога
Отправить удаленное оповещение о тревоге на устройство.

Эта функция доступна только на мобильных устройствах.

Заблокировать
Заблокируйте ваш ноутбук и установите 4-значный PIN-код для его разблокировки. Когда вы посылаете команду **Заблокировать**, система перезагружается и вход в Windows возможен только после ввода установленного PIN-кода.

Если вы хотите чтобы Bitdefender сфотографировал того человека, который пытается получить доступ к вашему ноутбуку, установите соответствующий флажок. Фотографии делаются с помощью фронтальной камеры и отображаются вместе со значением времени в панели Анти-вор. Будут сохранены только две последние фотографии.

Это действие доступно только для ноутбуков, у которых есть фронтальная камера.

Стереть данные
Удаление всех данных из вашей системы. Когда вы посылаете команду **Стереть**, ноутбук перезагружается и данные во всех разделах жесткого диска стираются.

Показать IP
Отображение последнего IP-адреса для выбранного устройства. Нажмите **ПОКАЗАТЬ IP**, чтобы сделать IP-адрес видимым.

Анти-вор активируется после установки и может быть доступен только через учетную запись Bitdefender с любого устройства, подключенного к Интернету, в любом месте.

Использование функций Анти-вор

Чтобы получить доступ к функциям Анти-вор, используйте одну из следующих возможностей:

- Из интерфейса Bitdefender:
  1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
  2. Нажмите кнопку **Анти-вор**.
  3. В открывшемся окне Bitdefender Central, нажмите на нужную карточку устройства, а затем выберите **Анти-вор**.
- На любом устройстве с доступом в Интернет:
  1. Откройте веб-браузер и перейдите: https://central.bitdefender.com.
  2. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
  3. Выберите **Мои устройства** на панели справа.
  4. Нажмите требуемую карточку устройства, затем выберите **Анти-вор**.
  5. Выберите функцию, которую вы хотите использовать:

     Показать IP - отобразить последний IP-адрес устройства.
     Местоположение - посмотреть местоположение вашего устройства на Google Maps.

     ТРЕВОГА - отправить уведомление о тревоге на устройство.

     Lock - заблокировать ноутбук и установить PIN-код для его разблокировки.

     Стереть - удалить все данные с вашего ноутбука.

     Важно
     После очистки устройства все возможности Анти-Вора перестанут функционировать.

4.16. USB иммунизация

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 использоваться вредоносными программами для автоматического запуска и проникнуть в ваш компьютер от перезаписываемых носителей, таких как USB флэш-диски и карты памяти, подключенные через устройства чтения карт памяти. В последние годы были созданы многочисленные атаки, основанные на автозапуске.

С помощью USB иммунизации вы можете предотвратить выполнение вредоносного кода на флэш-накопителях форматов NTFS, FAT32 или FAT. После того как USB-устройство будет иммунизированно, вредоносные программы больше не смогут настраивать его для запуска определенного приложения, когда устройство подключено 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**.

> **Замечание**
> Если накопитель уже был иммунизирован, то вместо опции Иммунизация появится сообщение **Устройство USB, защищено от вредоносного программного обеспечения на основе автозапуска**.

Для того, чтобы предохранить ваш компьютер от запуска вредоносных программ с неиммунизированных USB-устройств, отключите функцию автоматического автозапуска. Для получения дополнительной информации перейдите к «Использование автоматического мониторинга уязвимостей» (p. 138).

5. ОПТИМИЗАЦИЯ СИСТЕМЫ

5.1. Инструменты

Bitdefender поставляется с разделом Инструменты, который оказывает помощь в поддержке целостности системы. Предлагаемые инструменты помогут улучшить показатели работы Вашей системы, а также организовать эффективное использование свободного места на жестких дисках.

Bitdefender предоставляет следующие инструменты настройки ПК:

- Оптимизация в один клик анализирует и улучшает скорость вашей системы, выполняя несколько задач одним нажатием кнопки.
- Оптимизация загрузки снижает время запуска системы путем остановки загрузки ненужных приложений, когда ПК загружается.
- Очистка диска определяет самые большие файлы и папки, которые не использовались в течение длительного времени.

Оптимизация производительности системы в один клик

Такие проблемы, как ошибки жестких дисков, оставшиеся файлы реестра и история браузера, могут замедлять работу компьютера. Все они теперь могут быть исправлены одним нажатием кнопки.

OneClick Optimizer позволяет выявлять и удалять ненужные файлы запустив несколько задач очистки одновременно.

Чтобы начать процесс Оптимизации в один клик:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку **Оптимизация в один клик**.
   a. **Анализ**

      Подождите, пока Bitdefender завершит проверку уязвимостей.

      - Очистка диска - идентифицирует большие файлы и папки, которые вы больше не используете.
      - Очистка реестра - идентифицирует недействительные или устаревшие ссылки в реестре Windows.

- Приватная очистка - идентифицирует временные файлы Интернета, cookies, кэш браузера и историю.

Отображается количество найденных проблем. Нажмите ссылку **Подробнее**, чтобы ознакомиться с ними, прежде чем продолжить процесс очистки. Нажмите **ОПТИМИЗИРОВАТЬ** для продолжения.

b. **Оптимизация**

Подождите пока Bitdefender закончит оптимизацию системы.

c. **Проблемы**

Здесь можно просмотреть результаты операции.

Если вы хотите получить полную информацию о процессе оптимизации, нажмите кнопку **ПОСМОТРЕТЬ ПОДРОБНЫЙ ОТЧЕТ**.

Оптимизация времени загрузки ПК

Долгий запуск системы является реальной проблемой из-за приложений, которые установлены для запуска со стартом системы, без необходимости. Ожидание даже нескольких минут загрузки системы может повлиять на вашу работу.

Окно Оптимизация загрузки отображает запущенные во время загрузки приложения позволяет управлять их поведением на этом этапе.

Чтобы начать процесс оптимизации:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку **Оптимизация загрузки**.

a. **Выберите приложения**

Вы можете увидеть список приложений, работающих при запуске системы. Выберите те, что вы хотите отключить или отложить при запуске.

b. **Выбор сообщества**

Посмотрите, что делают другие пользователи Bitdefender с приложением, которое вы выбрали.

c. **Время загрузки системы**

Используйте ползунок в верхней части окна, чтобы увидеть время, необходимое для загрузки системы и выбранные приложений для запуска.

Для получения сведений о времени запуска системы и приложений требуется перезапуск системы.

d. **Статус автозагрузки**

- **Включить.** Выберите эту опцию, если вы хотите чтобы приложение запускалось при запуске системы. Эта опция включена по умолчанию.
- **Отложить.** Выберите эту опцию, чтобы отложить программу от старта при запуске системы. Это означает, что выбранные приложения запустятся с пяти-минутной задержкой, после входа пользователей в систему. Функция **Отложить** предопределена и не может быть настроена пользователем.
- **Выключить.** Выберите эту опцию, чтобы запретить программе старт при запуске системы.

e. **Результаты**

Отображаются такие сведения, как предполагаемое время загрузки системы после задержки или отключения программ.

Для просмотра всей этой информации может потребоваться перезапуск системы.

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

Замечание

В случае, если срок действия вашей подписки истек или вы решили удалить Bitdefender, программы будут восстановлены до параметров запуска по умолчанию.

Оптимизация диска

Ненужные файлы и папки, которые используют пространство на диске, могут привести к замедлению системы. Поэтому рекомендуется проводить регулярную очистку через равные промежутки времени для улучшения производительности системы.

Bitdefender Очистка диска позволяет освободить место на диске путем выявления больших файлов и папок, которые больше не используются.

Для запуска очистки вашей системы:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите кнопку быстрого действия **Очистка диска**.
3. Появится окно, отображающее сведения о том, что Очистка диска может сделать для вашей системы, чтобы освободить пространство для новых данных. Нажмите **ОК**

   a. **Диски и устройства**

      Вы можете просмотреть список доступных дисков. Кроме дисков Windows, внешние жесткие диски и USB-устройства сканируются и отображаются в списке. Нажмите **АНАЛИЗИРОВАТЬ ДИСК** в области диска, которую необходимо очистить.

   b. **Анализ диска**

      Выбранный диск анализируется. Подождите, пока Bitdefender закончит поиск больших файлов и папок.

   c. **Проблемы**

      Здесь вы можете просмотреть результат операции. В левой части окна используйте стрелку раскрывающегося списка **СОРТИРОВАТЬ ПО** чтобы выбрать, в каком порядке должны отображаться результаты, по размеру или по типу.

      Выберите файлы, которые хотите удалить и нажмите **ПОДТВЕРДИТЬ ВЫБОР** , чтобы начать процесс удаления.

      Подтвердите действие, нажав **УДАЛИТЬ**.

5.2. 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 Кино
- 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.
- Антиспам включен
- 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 Total Security устанавливается для автоматического выполнения следующих настроек программы:

- Активный Контроль Угроз включен
- Фаервол Bitdefender включен и следующие настройки применяются для беспроводного адаптера:

- Режим "Невидимки" - включен
- Тип сети - Публичная

- Включены следующие настройки Веб-защиты:
  - Сканировать SSL
  - Защита от мошенничества
  - Защита от фишинга

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
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 Bitdefender не вводится автоматически в профиль Работа при запуске определенного рабочего приложения, можно вручную добавить приложение в **Список приложений**.

Чтобы вручную добавить приложения в Список приложений в профиле Работа:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Работа.
4. В окне **ПРОФИЛЬ РАБОТА** нажмите ссылку **Список приложений**.
5. Нажмите **Добавить**, чтобы добавить новое приложение к **Списку приложений**.

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

Профиль Кино

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
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 плана питания для просмотра кино

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

Добавление видео-проигрывателей в список профиля Фильм вручную

Если Bitdefender автоматически не переходит в профиль Фильма при запуске определенного приложения видео-проигрывателя, можно вручную добавить приложение в список **Список проигрывателей**.

Чтобы вручную добавить видео-проигрываетли в список профиля Фильм:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Фильм.
4. В окне **ПРОФИЛЬ ФИЛЬМ** нажмите ссылку **Список плееров**.
5. Нажмите **Добавить**, чтобы добавить новое приложение к **Списку плееров**.

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

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 на иконку в нижнем левом углу Bitdefender interface.

2. Выберите вкладку **ПРОФИЛИ**.
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 Bitdefender автоматически не переходит в профиль Игра при запуске определенной игры или приложения, вы можете вручную добавить приложение в список **Список игр**.

Чтобы вручную добавить игры в Список игр в профиле Игра:

1. Нажмите на  иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Игра.
4. В окне **Профиль Игра** нажмите ссылку **Список игр**.
5. Нажмите **Добавить**, чтобы добавить новую игру в **Список игр**.

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

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
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**.

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
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.

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 на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ПРОФИЛИ**.
3. Прокрутите вниз, пока не увидите параметр оптимизации в режиме реального времени, затем используйте соответствующий переключатель, чтобы включить или выключить его.

6. УСТРАНЕНИЕ НЕПОЛАДОК

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. 200)
- «*Сканирование не начинается*» (p. 202)
- «*Не удается использовать приложение*» (p. 204)
- «*Что делать, если Bitdefender блокирует безопасный веб-сайт или онлайн приложение*» (p. 205)
- «*Что делать, если Bitdefender определяет безопасное приложение в качестве программы-вымогателя*» (p. 206)
- «*Обновление Bitdefender при низкой скорости подключения к Интернету*» (p. 211)
- «*Службы Bitdefender не отвечают*» (p. 212)
- «*Фильтр антиспама работает некорректно*» (p. 213)
- «*Функция "Автозаполнение" в Кошельке не работает*» (p. 218)
- «*Сбой удаления Bitdefender*» (p. 219)
- «*Моя система не загружается после установки Bitdefender*» (p. 220)

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. 330).

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.**

  Хотя Bitdefender выполняет поиск и удаление программ безопасности, обнаруженных во время установки, рекомендуется удалить остальные антивирусные программы заранее, перед установкой Bitdefender. Для получения дополнительной информации перейдите к *«Как удалить другие решения безопасности?»* (p. 88).

- **Не соблюдены минимальные системные требования для запуска Bitdefender.**

  Если компьютер не соответствует минимальным системным требованиям, это может стать причиной медленной работы системы, особенно при одновременной работе нескольких приложений. Для получения дополнительной информации перейдите к «Минимальные системные требования» (p. 3).

- **Вы установили приложение, которое не используете**.

  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**.

  Вредоносное ПО может 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 он сканирует все типы вредоносных программ, угрожающих безопасности вашей системы.

  Чтобы запустить Сканирование Системы:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Системное сканирование**.
4. Следуйте инструкциям мастера.

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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
    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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
    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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Замечание
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 дополнительной информации перейдите к «*Как удалить другие решения безопасности?*» (p. 88).
  2. Переустановите Bitdefender:
     - В **Windows 7**:
       a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
       b. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
       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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.

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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.

d. Нажмите **Удалить** снова, чтобы подтвердить выбор.

e. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.

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

Замечание

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. 330).

3. Не удается 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 в основе этой функции лежит система эвристического анализа, возможны случаи распознавания активным вирусным контролем легитимных приложений как вирусов.

При возникновении такой ситуации можно исключить соответствующее приложение из мониторинга активного вирусного контроля.

Чтобы добавить программу в список исключений:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите иконку в правом нижнем углу панели **Активный Контроль Угроз**.
4. В окне **Белый список** нажмите **Добавить приложения в белый список** .
5. 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. 330).

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 одной и той же страницы или приложения их можно добавить в белый список, чтобы они не проверялись Bitdefender, обеспечивая тем самым плавный просмотр веб-страниц.

Чтобы добавить веб-сайт в **Белый список**:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **ВЕБ-ЗАЩИТА** нажмите **Белый список**.
4. Укажите адрес заблокированного сайта или интернет-приложения в соответствующем поле и нажмите **Добавить**.
5. Нажмите **Сохранить**, чтобы сохранить изменения и закрыть окно.

Только веб-сайты и приложения, которым вы полностью доверяете должны быть добавлены в этот список. Они будут исключены из сканирования следующими категориями: вредоносные программы, фишинг и мошенничество.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 330).

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.

В случае, если такое приложение добавляется в список ненадежных приложений, но вы уверены, что его использование безопасно, выполните следующие действия:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Доступ к приложениям**.
4. В списке указаны приложения, которые запросили изменить файлы в ваших защищенных папках. Нажмите "Разрешить" и выберите приложение, в безопасности которого вы уверены.

6. Не удается подключиться к Интернету

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

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

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **Файрвол**
4. Выберите вкладку **Правила**.
5. Чтобы добавить правило для приложения, выберите ссылку **Добавить правило**.
6. Появится новое окно, где вы можете добавить информацию. Убедитесь, что выбрали все типы сетей доступными и в разделе **Разрешения** выберите **Разрешить**.

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

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 330).

7. Не удается получить доступ к устройству в сети

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

В этом случае рекомендуется настроить в Bitdefender возможность автоматически разрешать подключение к соответствующему устройству следующим образом:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Нажмите значок в нижнем правом углу панели **Файрвол**
4. Нажмите ссылку **Добавить правило** в верхней части окна **ПРАВИЛА** .
5. В окне **НАСТРОЙКИ** включите опцию **Применить это правило ко всем приложениям** .
6. Выберите вкладку **РАСШИРЕННЫЙ**
7. В поле **Удаленный адрес пользователя** введите IP адрес желаемого компьютера или принтера для использования в неограниченном доступе.

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

Проверьте другие возможные причины, такие как:

- Совместный доступ к файлу и принтеру на вашем компьютере может быть заблокирован брандмауэром, установленным на другом компьютере.
  - Если используется брандмауэр Windows, его можно настроить таким образом, чтобы разрешить доступ к файлам и принтерам:
    - В **Windows 7**:
      1. Нажмите **Пуск**, перейдите на вкладку **Панель управления** и выберите **Система и Безопасность**.

2. Перейдите к **Брандмауэр Windows** и затем нажмите **Разрешить программу через брандмауэр Windows**.
3. Отметьте флажок **Общий доступ к файлам и принтерам**.

- 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 кнопку **Система и безопасность**, перейдите **Брандмауэр Windows** и выберите **Разрешить приложение через брандмауэр Windows**.
3. Отметьте флажком **Общий доступ к файлам и принтеру** и затем нажмите **ОК**.

- В **Windows 10**:

1. Введите "Разрешить связь для программ через Брандмауер Windows" в поле поиска на панели задач и щелкните ее иконку.
2. Нажмите **Изменить настройки**.
3. В списке **Разрешенные приложения и функции** отметьте галочкой **Общий доступ к файлам и принтеру** и затем нажмите **ОК**.

- Если используется другой брандмауэр, обратитесь к его документации или файлу справки.

- Общие условия, которые могут предотвратить использование общего принтера или подключение к нему:
  - Для доступа к общему принтеру может потребоваться вход в учетную запись администратора Windows.
  - Разрешения устанавливаются на общий принтер, чтобы разрешить доступ только конкретному компьютеру и пользователям. Если используется общий доступ к принтеру, проверьте разрешения, установленные для принтера, чтобы узнать, разрешен ли пользователю другого компьютера доступ к принтеру. Если вы пытаетесь подключиться к общему принтеру, свяжитесь с пользователем другого компьютера для проверки того, есть ли у вас разрешение на подключение к принтеру.

- Принтер, подключенный к вашему компьютеру или к другому компьютеру, не является общим.
- Общий принтер не добавлен на компьютер.

> **Замечание**
> Чтобы научиться управлять принтерами (обеспечивать общий доступ к принтеру, устанавливать или удалять разрешения для принтера, подключаться к сетевому или к общему принтеру), перейдите к центру справки и поддержки Windows (в меню Пуск выберите команду **Справка и поддержка**).

- Доступ к сетевому принтеру для определенных компьютеров или пользователей может быть ограничен. Необходимо проверить у администратора сети наличие разрешений на подключение к этому принтеру.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 330).

8. Низкая скорость подключения к Интернету

Эта ситуация может возникать после установки Bitdefender. Проблема может быть вызвана ошибками конфигурации брандмауэра Bitdefender.

Чтобы устранить эту ситуацию:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **БРАНДМАУЭР** нажмите соответствующий переключатель ВКЛ/ВЫКЛ, чтобы отключить эту функцию.
4. Проверьте подключение к Интернету при отключенном брандмауэре Bitdefender.
   - Если подключение к Интернету все еще работает медленно, значит Bitdefender не является причиной этой неисправности. Необходимо связаться с поставщиком услуг Интернета и проверить работоспособность подключения на стороне поставщика.

     Если поставщик интернет-услуг подтверждает, что на его стороне неполадки с соединением отсутствуют, но проблема продолжает

возникать, обратитесь в Bitdefender в соответствии с инструкциями в разделе «*Обращение за помощью*» (p. 330).

- Если подключение к Интернету улучшилось после отключения брандмауэра Bitdefender:

  a. Нажмите на иконку в нижнем левом углу Bitdefender interface.

  b. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

  c. Нажмите значок в нижнем правом углу панели **Файрвол**

  d. Перейдите на вкладку **СЕТЕВЫЕ АДАПТЕРЫ** и установите подключение к Интернету в **Дом/Офис**.

  e. На вкладке **ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ** нажмите соответствующий переключатель, чтобы отключить **Блокировать порт сканирования сети** .

  В области **Скрытый режим** нажмите **Изменить скрытые подключения** . Включите Скрытый Режим для сетевого адаптера, к которому Вы подключены.

  f. Закройте Bitdefender, перезагрузите систему и проверьте скорость подключения к Интернету.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 330).

9. Обновление Bitdefender при низкой скорости подключения к Интернету

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

Для того, чтобы сохранить вашу систему в актуальном состоянии с новейшими вирусными сигнатурами Bitdefender:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Выберите вкладку **ОБНОВИТЬ**.
3. Рядом с **Обновление правил обработки**, выберите **Подсказать перед загрузкой** из выпадающего меню.

4. Вернитесь в главное окно и нажмите кнопку **Обновить** в интерфейсе Bitdefender.
5. Выберите только **Обновление сигнатур**, а затем нажмите кнопку **ОК**.
6. Bitdefender выполнит загрузку и установку только обновлений вирусных сигнатур.

10. 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 дополнительной информации перейдите к «*Как удалить другие решения безопасности?*» (p. 88).

Если ошибка продолжает возникать, свяжитесь с нашей службой поддержки, как описано в разделе «*Обращение за помощью*» (p. 330).

11. Фильтр антиспама работает некорректно

Эта статья поможет вам устранить следующие проблемы, связанные с операциями фильтрации антиспама Bitdefender:

- Количество легальных сообщений, помеченных как [spam].
- Многие спам-сообщения не помечены фильтром антиспама.
- Фильтр антиспама не распознает спам-сообщения.

11.1. Легальные сообщения помечены как [спам]

Легальные сообщения помечены как [spam] потому, что для антиспама Bitdefender они выглядят как спам. Обычно эту проблему можно решить путем адекватной настройки фильтра антиспама.

Bitdefender автоматически добавляет получателей Вашей почты в список друзей. Сообщения электронной почты, полученные из Списка друзей, считаются легитимными. Они не проверяются Антиспам Фильтром, и никогда не помечаются как [spam].

Автоматическая конфигурация списка друзей не предотвращает ошибки обнаружения, которые могут возникнуть в таких ситуациях:

- Вы получаете большое количество коммерческой почты в результате подписки на различных веб-сайтах. В данном случае решением будет добавить адреса электронной почты, с которых приходят данные сообщения, в список друзей.
- Значительная часть вашей легальной почты от людей, с которыми вы никогда не переписывались, например клиентов, потенциальных партнеров и других. В данном случае необходимы другие решения.

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

  Замечание

  Bitdefender интегрируется в наиболее часто используемые почтовые клиенты с помощью простой в использовании антиспам-панели инструментов. С полным списком системных требований можно ознакомиться в разделе «Поддерживаемые почтовые клиенты и протоколы» (p. 123).

Добавить контакты в список друзей

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

1. В почтовом клиенте выберите сообщение электронной почты от отправителя, которого требуется добавить в список друзей.
2. Нажмите кнопку **Добавить друга** на панели управления антиспама Bitdefender.
3. Вам будет предложено подтвердить добавление адресов в список друзей. Выберите **Не показывать это сообщение снова** и нажмите **ОК**.

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

Если вы используете другой почтовый клиент, вы можете добавлять контакты в список друзей из интерфейса Bitdefender. Следуйте инструкции:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **АНТИСПАМ**, выберите **Управление друзьями**.

   Появится окно конфигурации.
4. Введите адрес электронной почты, с которого Вы хотите всегда получать письма, и нажмите **Добавить**. Можно добавить любое необходимое количество адресов электронной почты.
5. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.

Показать ошибки обнаружения

Если Вы используете поддерживаемую почтовую службу, Вы можете легко корректировать фильтр антиспама, указывая, какие письма не следует помечать как [спам]. Это поможет повысить эффективность фильтра антиспама. Следуйте инструкции:

1. Откройте ваш почтовый клиент.
2. Перейдите в папку нежелательной почты, куда помещаются спам-сообщения.

3. Выберите легитимные сообщения, ошибочно помеченные Bitdefender как [спам].
4. Нажмите кнопку **Добавить друга** на панели управления Bitdefender антиспама для добавления отправителя в список друзей. Необходимо нажать **ОК** для подтверждения. Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.
5. Нажмите кнопку **Не спам** на панели инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента). Письмо будет перемещено в папку "Входящие".

11.2. Многие сообщения спама остаются необнаруженными

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

Попробуйте следующие решения:

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

   ### Замечание

   Bitdefender интегрируется в наиболее часто используемые почтовые клиенты с помощью простой в использовании антиспам-панели инструментов. С полным списком системных требований можно ознакомиться в разделе «Поддерживаемые почтовые клиенты и протоколы» (p. 123).

2. Добавить спамеров в Список спамеров. Почтовые сообщения, полученные с адресов из списка спамеров, автоматически помечаются как [spam].

Указать необнаруженные сообщения спама

При использовании поддерживаемого почтового клиента можно легко указать, какие сообщения электронной почты должны были быть обнаружены как нежелательные. Это поможет повысить эффективность фильтра антиспама. Следуйте инструкции:

1. Откройте ваш почтовый клиент.

2. Перейти к папке "Входящие".
3. Выберите необнаруженные спам-сообщения.
4. Нажмите кнопку **Является спамом** на панели Bitdefender инструментов анти-спама(обычно находится в верхней части окна почтового клиента). Они незамедлительно будут помечены как [spam] и перенесены в папку нежелательной почты.

Добавить спамеров в Список спамеров

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

1. Откройте ваш почтовый клиент.
2. Перейдите в папку нежелательной почты, куда помещаются спам-сообщения.
3. Выберите сообщения, помеченные Bitdefender как [спам].
4. Нажмите кнопку **Добавить спамера** на панели антиспама Bitdefender.
5. Вам будет предложено подтвердить добавление адресов в список спамеров. Выберите **Не показывать это сообщение снова** и нажмите **ОК**.

Если вы используете другой почтовый клиент, вы можете вручную добавлять спамеров в Список спамеров из интерфейса Bitdefender. Это удобнее делать после того, как Вы получили несколько спам-сообщений с одного и того же адреса электронной почты. Следуйте инструкции:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. На панели **АНТИСПАМ**, выберите **Управление друзьями**.

   Появится окно конфигурации.
4. Введите адрес электронной почты спамера и нажмите **Добавить**. Можно добавить любое необходимое количество адресов электронной почты.
5. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.

11.3. Фильтр антиспама не обнаруживает ни одно сообщение спама

Если нет спам-сообщений, помеченных как [spam], могут быть проблемы в работе антиспама Bitdefender. До устранения проблемы убедитесь, что она не вызвана одной из следующих причин:

- Защита антиспама может быть отключена. Чтобы проверить статус защиты от спама, нажмите значок на левой боковой панели Bitdefender, затем выберите ссылку **ПРОСМОТР ФУНКЦИЙ**. Нажмите на значок шестеренки на панели **АНТИСПАМ**, а затем посмотрите в верхней части окна, чтобы проверить включение функции.

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

- Антиспам защита Bitdefender доступна только для клиентов электронной почты, настроенной на прием сообщений электронной почты по протоколу POP3. Это значит:

  - Сообщения электронной почты, полученные через веб-службы электронной почты (например, Yahoo, Gmail, Hotmail или другой), не фильтруются Bitdefender на предмет спама.

  - Если Ваша почтовая служба настроена на получение сообщений электронной почты с использованием протоколов, отличных от протокола POP3 (например, IMAP4), антиспам Bitdefender не проверяет их на предмет спама.

  > **Замечание**
  >
  > POP3 является одним из наиболее широко используемых протоколов для загрузки сообщений электронной почты с почтового сервера. Если Вы не знаете, какой протокол использует Ваша почтовая служба для загрузки сообщений электронной почты, спросите того, кто настроил его.

- Bitdefender Total Security не сканирует трафик POP3 Lotus Notes.

Возможным решением может быть переустановка продукта. Однако вместо этого, вы можете обратиться за поддержкой в Bitdefender, как описано в разделе «*Обращение за помощью*» (p. 330).

12. 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 Wallet** и нажмите **Enable**.
- В **Mozilla Firefox:**
  1. Открыть Mozilla Firefox.
  2. Зайдите в раздел "Инструменты".
  3. Нажмите "Управление настройками".
  4. Нажмите "Расширение".
  5. Наведите указатель мыши на **Bitdefender Wallet** и нажмите **Enable**.
- В **Google Chrome:**
  1. Открыть Google Chrome.
  2. Перейдите в "Меню".
  3. Нажмите «Дополнительные инструменты».
  4. Нажмите "Расширение".
  5. Наведите указатель мыши на **Bitdefender Wallet** и нажмите **Enable**.

Замечание

Функция "Управление настройками" активируется после того, как вы перезагрузите ваш браузер.

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. 330).

13. 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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

14. 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. Инструкции для этой процедуры см. в *«Как перезагрузить компьютер в безопасном режиме?»* (p. 89).
  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.
       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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.

  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. Выберите **Bitdefender Total Security** и нажмите **Деинсталлировать**.

  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. Инструкции для этой процедуры см. в *«Как перезагрузить компьютер в безопасном режиме?»* (p. 89).

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. Инструкции для этой процедуры см. в «*Как перезагрузить компьютер в безопасном режиме?*» (p. 89).
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. 330).

Удаление вредоносного ПО из системы

Вредоносные программы могут влиять на работу системы различными способами. Работа Bitdefender зависит от типа атаки вредоносного ПО. Вследствие того, что поведение вирусов часто изменяется, определить единый шаблон их поведения и действий довольно сложно.

В отдельных случаях Bitdefender не удается автоматически удалить вирусы из системы. В таких случаях требуется вмешательство пользователя.

- «Bitdefender Режим Восстановления (Rescue Environment в Windows 10)» (p. 224)
- «Действия в случае обнаружения Bitdefender вирусов на компьютере» (p. 228)
- «Как удалить вирус из архива?» (p. 230)
- «Как очистить от вирусов архив электронной почты?» (p. 231)
- «Что делать, если имеются подозрения в том, что файл является опасным?» (p. 232)
- «Что представляют собой защищенные паролями файлы в журнале сканирования?» (p. 232)
- «Поиск пропущенных элементов в журнале сканирования» (p. 233)
- «Поиск файлов с избыточным сжатием в журнале сканирования.» (p. 233)

- «Почему Bitdefender автоматически удалил зараженный файл?» (p. 234)

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. 330).

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 Total Security 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, если Вы подозреваете, что угроза вредоносного ПО 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 на иконку в нижнем левом углу Bitdefender interface.

2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Режим Восстановления**.
4. Нажмите **ДА** в окне подтверждения, которое появляется 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.

Замечание
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 на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Режим Восстановления**.
4. Нажмите **ДА** в окне подтверждения, которое появляется для перезагрузки компьютера.
5. 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.
6. 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.

> **Замечание**
> 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. 224).

Запуск системы в Rescue Environment в Windows 10

Вход в Rescue Environment возможен только с ВашегоBitdefender средства, как показано ниже:

1. Нажмите на иконку в нижнем левом углу Bitdefender interface.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.

3. В области **ANTIVIRUS** нажмите **Rescue Environment** .
4. 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. 225).
  2. Появится логотип Bitdefender, и начнется копирование антивирусных систем.
  3. Откроется окно приветствия. Нажмите **Продолжить**.
  4. Установка обновления вирусных сигнатур запущена.
  5. После завершения обновления появится окно "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.

     > **Замечание**
     > 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 будут обнаружены вредоносные программы, следуйте инструкциям для устранения угрозы.
  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. 226)
2. Процесс сканирования Bitdefender запускается автоматически, как только система загружается в Среде восстановления.
3. Дождитесь завершения процесса сканирования. Если будут обнаружены вредоносные программы, следуйте инструкциям для устранения угрозы.
4. Чтобы выйти из Среды, нажмите кнопку **ЗАКРЫТЬ** в окне с результатами сканирования.

Действия в случае обнаружения Bitdefender вирусов на компьютере

Обнаружить в компьютере вирус можно одним из следующих способов:

- Выполнено сканирование компьютера. Bitdefender обнаружил зараженные элементы.
- Оповещение о вирусе сообщает о блокировке Bitdefender одного или нескольких вирусов, проникших в компьютер.

В такой ситуации обновите Bitdefender и убедитесь, что установлены последние версии сигнатур вредоносного ПО, и запустите программу сканирования системы.

Как только процесс сканирования будет завершен, примените желаемую меру в отношении зараженного элемента (вылечить, удалить, переместить в карантин).

Внимание

Если вы считаете, что этот файл является частью операционной системы Windows, или сомневаетесь в том, что файл заражен вирусом, выполните следующие действия и как можно скорее свяжитесь со службой поддержки клиентов Bitdefender.

Если выбранное действие не может быть выполнено и в журнале сканирования отображаются сведения об обнаруженном вирусе, который невозможно удалить, необходимо удалить файл(ы) вручную:

Первый метод можно использовать в нормальном режиме:

1. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Нажмите на  иконку в нижнем левом углу Bitdefender interface.
   b. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
   c. Выберите  иконку в правом верхнем углу на панели **АНТИВИРУС**.
   d. В окне **ЩИТ** нажмите переключатель ВКЛ/ВЫКЛ.
2. Отображать скрытые объекты в Windows. Инструкции для этой процедуры см. в «*Как отобразить скрытые объекты в Windows?*» (p. 87).
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. Инструкции для этой процедуры см. в «*Как перезагрузить компьютер в безопасном режиме?*» (p. 89).
2. Отображать скрытые объекты в Windows. Инструкции для этой процедуры см. в «*Как отобразить скрытые объекты в Windows?*» (p. 87).
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. 330).

Как удалить вирус из архива?

Архив представляет собой файл или набор файлов, сжатых в специальном формате в целях уменьшения пространства на диске, требуемого для хранения файлов.

Некоторые из этих форматов являются открытыми, что дает Bitdefender возможность просканировать их изнутри и выполнить после этого соответствующие действия для их удаления.

Другие форматы архивов являются частично или полностью закрытыми. Bitdefender может только обнаруживать присутствие в них вирусов, не выполняя каких-либо дополнительных действий.

В тех случаях, когда Bitdefender выводит уведомление об обнаружении вируса в архиве, не предлагая доступных действий, это означает, что удаление вируса невозможно из-за ограничений, установленных для параметров разрешений архива.

Удалить вирус из архива можно следующим образом:

1. Определите архив, который включает в себя вирус посредством проверки системы.
2. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Нажмите на иконку в нижнем левом углу Bitdefender interface.
   b. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
   c. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
   d. В окне **ЩИТ** нажмите переключатель ВКЛ/ВЫКЛ.
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.

Замечание
Обратите внимание на то, что вирус, содержащийся в архиве, не представляет собой непосредственной угрозы системе, поскольку для заражения системы необходимо, чтобы вирус был распакован и исполнен.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 330).

Как очистить от вирусов архив электронной почты?

Bitdefender также может выполнять поиск вирусов в базах данных электронной почты и архивах электронной почты на диске.

В отдельных случаях требуется найти зараженное сообщение, используя данные отчета о сканирования, и удалить его вручную.

Удалить вирус из архива электронной почты можно следующим способом:

1. Сканирование базы данных электронной почты с помощью Bitdefender.
2. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Нажмите на иконку в нижнем левом углу Bitdefender interface.
   b. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
   c. Выберите иконку в правом верхнем углу на панели **АНТИВИРУС**.
   d. В окне **ЩИТ** нажмите переключатель ВКЛ/ВЫКЛ.
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. 330).

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. Инструкции для этой процедуры см. в *«Как выполнить сканирование системы?»* (p. 63).
2. Если при сканировании угрозы обнаружены не были, но у вас все еще имеются сомнения и вы хотите убедиться в безопасности определенного файла, свяжитесь с нашей службой поддержки.

   Инструкции для этой процедуры см. в *«Обращение за помощью»* (p. 330).

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.

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.

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.

Почему Bitdefender автоматически удалил зараженный файл?

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

В случае определенных типов вредоносных программ лечение невозможно, поскольку 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.

АНТИВИРУС ДЛЯ MAC

7. УСТАНОВКА И УДАЛЕНИЕ

В данной главе рассматриваются следующие темы:

- «*Системные требования*» (p. 236)
- «*Установка Bitdefender Antivirus for Mac*» (p. 236)
- «*Открытие Bitdefender Antivirus for Mac*» (p. 241)

7.1. Системные требования

Установка Bitdefender Antivirus for Mac возможна только на компьютерах Macintosh на базе Intel с OS X Mavericks (10. 9. 5), OS X Yosemite (10. 10. 5), OC X El Capitan (10. 11. 6), macOS Sierra (10. 12. 5 или новее), macOS High Sierra 10. 13.

Устройство Mac должно соответствовать следующим требованиям:

- Минимум 1 ГБ оперативной памяти
- Минимум 600 Мб свободного места на жестком диске

Для регистрации и обновления Bitdefender Antivirus for Mac необходимо подключение к Интернету.

Поиск номера версии macOS на компьютере Mac

Нажмите на значок Apple в верхнем левом углу экрана и выберите **Об устройстве Mac**. В появившемся окне отображается версия операционной системы и другая информация. Нажмите **Дополнительная информация** для получения подробной информации.

7.2. Установка Bitdefender Antivirus for Mac

Приложение Bitdefender Antivirus for Mac можно установить Bitdefender следующим образом:

1. Вход в систему с правами администратора.
2. Перейти к: https://central.bitdefender.com.
3. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
4. В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.

5. Выберите одну из двух доступных опций:
   - **Загрузка**

     Нажмите на кнопку и сохраните установочный файл.
   - **На другое устройство**

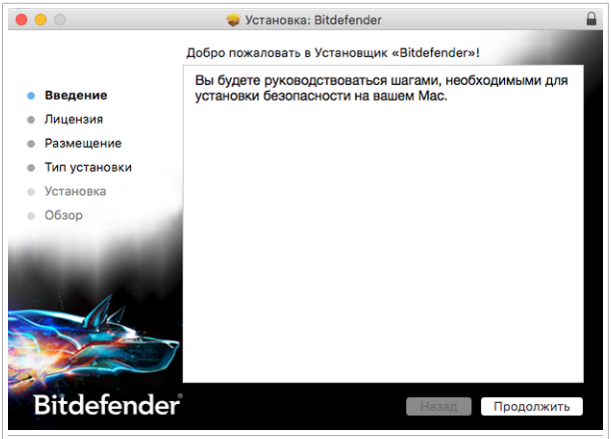
     Выберите **macOS** чтобы загрузить Bitdefender, затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.
6. Запустите Bitdefender продукт, который вы скачали.
7. Выполните процедуру установки

7.2.1. Процесс установки

Установить Bitdefender Antivirus for Mac:

1. Нажмите на загруженный файл Запустится установщик с сопутствующей информацией для дальнейшего процесса установки
2. Следуйте инструкциям мастера настройки.

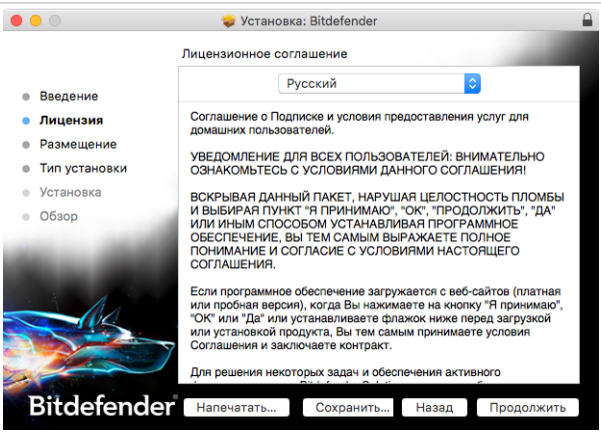
Шаг 1. Окно приветствия



Окно приветствия

Нажмите **Продолжить**.

Шаг 2 - Ознакомьтесь с Соглашением о Подписке



Соглашение о Подписке

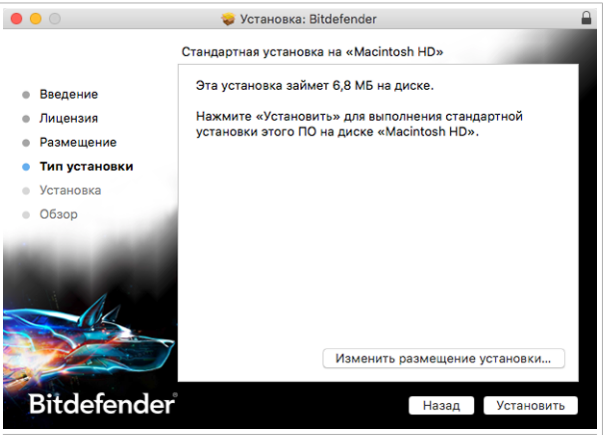
Данное Соглашение о Подписке является юридическим соглашением между Вами и Bitdefender об использовании Bitdefender Antivirus for Mac. Соглашение о Подписке можно сохранить или распечатать и ознакомиться с ним позже

Внимательно ознакомьтесь с Соглашением о Подписке. Для продолжения установки программы необходимо согласиться с условиями Соглашения. Нажмите **Продолжить**, затем нажмите **Согласен**.

Важно

Если Вы не согласны с этими условиями, нажмите **Продолжить**, затем нажмите **Не согласен** для отмены установки и выхода из программы.

Шаг 3. Запуск установки

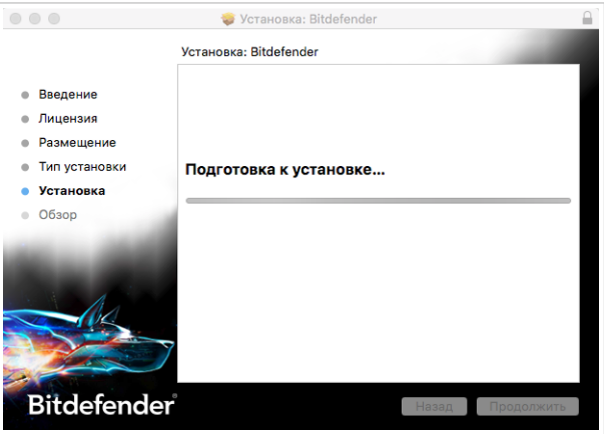


Запуск установки

Bitdefender Antivirus for Mac будет установлен на Macintosh HD/Library / Bitdefender. **Невозможно изменить путь установки**

Нажмите **Установить**, чтобы начать установку.

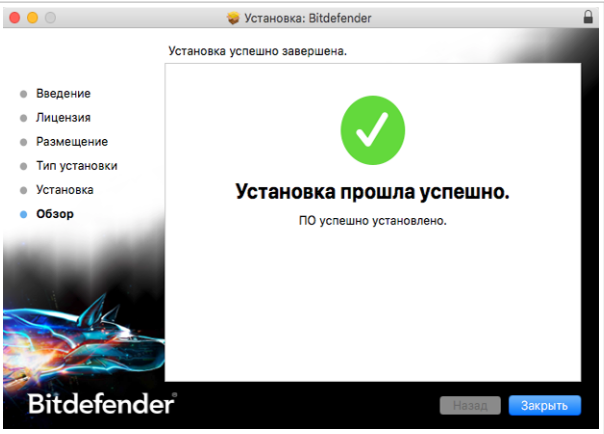
Шаг 4- Установка Bitdefender Antivirus for Mac



Установка Bitdefender Antivirus for Mac

Дождитесь окончания установки и нажмите **Продолжить**.

Шаг 5. Завершение



Готово

Нажмите **Закрыть** чтобы закрыть окно установщика программы.

Установка завершена.

Важно
В случае установки Bitdefender Antivirus for Mac на macOS High Sierra 10.13 или новую версию, появится уведомление **Блокировать систему** Данное уведомление информирует о том, что подключенные к Bitdefenderрасширения заблокированы и должны подключены вручную. Для продолжения нажмите **OK**. В появившемся окне Bitdefender Antivirus for Mac нажмите ссылку **Безопасность & Конфиденциальность**. Установите флажок Bitdefender в списке и нажмите **OK**. Перезагрузите Mac для завершения процесса установки.

При первичной установке Bitdefender Antivirus for Mac появятся мастер Защиты резервного копирования и мастер компонента Безопасные файлы Для получения подробной информации, обратитесь к «*Безопасные файлы*» (p. 258) и «*Резервное копирование*» (p. 247).

7.3. Открытие Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac невозможно удалить простым способом, путем перетаскивания значка из папки Приложения в корзину.

Чтобы удалить Bitdefender Antivirus for Mac, выполните следующие действия:

1. Откройте окно **Поиск**, перейдите в папку Приложения и выберите Утилиты.
2. Нажмите дважды на приложение Bitdefender Удаление чтобы открыть его
3. Нажмите **Удалить** и дождитесь завершения.
4. Нажмите **Закрыть** для завершения.

Важно
В случае необходимости можно обратиться в службу поддержки клиентов Bitdefender, как указано в «*Обращение за помощью*» (p. 330).

8. НАЧАЛО РАБОТЫ

В данной главе рассматриваются следующие темы:

8.1. О Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac - мощный антивирусный сканер обнаруживает и удаляет все типы вредоносных программ, в том числе:

- вирус-вымогатель
- рекламное ПО
- Вирусы
- Вредоносное ПО
- Трояны
- кейлоггеры
- черви

Приложение обнаруживает и удаляет вредоносные программы Mac, а также Windows, предотвращая случайное отправление зараженных файлов кому-либо.

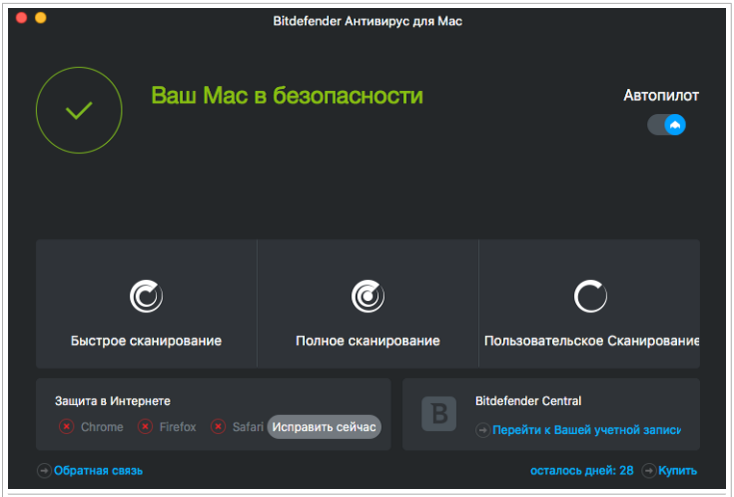
8.2. Открытие Bitdefender Antivirus for Mac

Несколько способов открыть Bitdefender Antivirus for Mac.

- Нажмите значок Bitdefender Antivirus for Mac на панели.
- Нажмите значок в строке меню и выберите **Открыть главное окно**
- Откройте окно Поиска, перейдите в Приложения и нажмите дважды на значок Bitdefender Antivirus for Mac.

8.3. Главное окно приложения

В главном окне приложения можно проверить состояние безопасности компьютера, запустить сканирование системы, защиту веб-браузера или войти в учетную запись Bitdefender.



Главное окно приложения

Опция **Автопилот**, расположенная в верхней правой части главного окна, непрерывно контролирует запущенные на компьютере приложения, выявляет вредоносные действия и предотвращает от вторжения угроз в Вашу систему.

В целях безопасности рекомендуется оставлять Автопилот в работающем режиме. Автоматическая защита от вредоносных программ невозможна при выключенном Автопилоте.

Строка состояния в верхней части окна информирует о состоянии безопасности системы. Если в Bitdefender Antivirus for Mac нет предупреждений об угрозах, строка состояния будет зеленой. Если обнаружена угроза безопасности, строка состояния поменяет цвет на желтый. Нажмите кнопку **Просмотр** для просмотра элементов, угрожающих безопасности системы. Для получения дополнительной информации о проблемах и способах их устранения см. «*Устранение угроз*» (p. 250).

В строке состояния доступны три кнопки сканирования устройства Mac:

- **Быстрое сканирование** выявляет наличие вредоносных программ в наиболее уязвимых местах системы (например, папки с документами, загруженные и временные файлы).

- **Полное Сканирование** проверяет всю систему на наличие вредоносного ПО. Также будут проверены все подключенные утилиты.
- **Выборочное сканирование** проверяет определенные файлы или папки на наличие вредоносных программ.

Для получения более подробной информации, обратитесь к «*Сканирование Mac*» (p. 246).

Помимо кнопок сканирования доступны дополнительные опции:

- **Веб-защита** фильтрует весь веб-трафик и блокирует любой вредоносный контент. Для получения более подробной информации, обратитесь к «*Веб-защита*» (p. 251).
- **Переход к Bitdefender учетной записи** - нажмите ссылку **Переход к учетной записи** в нижней правой части основного интерфейса для доступа к Вашей учетной записи Bitdefender. Для получения более подробной информации, обратитесь к «*Bitdefender Central*» (p. 263).
- **Количество оставшихся дней** - отображает оставшееся время до истечения срока действия подписки. По истечении срока действия перейдите по ссылке для продления подписки.
- **Купить** - переход на страницу Bitdefender для выбора доступных предложений и покупки подписки.
- **Обратная связь** - открывает по умолчанию новое окно в Вашей почтовой программе для связи с нашими специалистами.

8.4. Значок приложения Dock

Значок Bitdefender Antivirus for Mac появится в Dock сразу после входа в приложение. Значок в Dock - простой способ сканирования файлов и папок на наличие вредоносных программ. Перетащите файл или папку на значок Dock и сканирование начнется немедленно.

Значок Dock

9. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

В данной главе рассматриваются следующие темы:

9.1. Практические приемы

Для защиты системы от вредоносных программ и предотвращения заражения, следуйте следующим рекомендациям:

- Оставьте **Автопилот** в работающем режиме для сканирования Bitdefender Antivirus for Massистемных файлов
- Обновляйте Bitdefender Antivirus for Mac на включенном режиме **Автопилот** для обновления вирусных сигнатур
- Регулярно проверяйте предупреждения Bitdefender Antivirus for Mac об угрозах и устраняйте их. Для получения дополнительной информации перейдите к «*Устранение угроз*» (p. 250).
- Проверьте журнал событий, связанных с действиями Bitdefender Antivirus for Mac на Вашем компьютере Всякий раз при нарушении безопасности системы или данных в Bitdefender отчеты поступает новое предупреждение Для получения подробных сведений нажмите «*Журнал*» (p. 260).
- Также следует придерживаться следующих рекомендаций:
  - Сканируйте файлы, загружаемые из внешней памяти (USB, CD)
  - Файл DMG необходимо установить перед сканированием его содержимого

Легкий способ сканирования файла или папки - перетащить его в окно Bitdefender Antivirus for Mac или навести на значок Dock.

Других действий не требуется. Можно персонализировать параметры для Вашего удобства Для получения более подробной информации, обратитесь к «*Настройка свойств*» (p. 255).

9.2. Сканирование Mac

Функции **Автопилот** беспрерывно контролирует запущенные на компьютере приложения, распознает угрозы и предотвращает проникновение новых вредоносных программ в систему. Тем не менее, сканирование устройства Mac или определенных файлов можно проводить в любое удобное для Вас время.

Легкий способ сканирования файла или папки - перетащить его в окно Bitdefender Antivirus for Mac или навести на значок Dock. Появится мастер сканирования для оказания помощи в процессе сканирования

Также запустить сканирование можно следующим образом:

1. Открыть Bitdefender Antivirus for Mac.
2. Нажмите одну из трех кнопок сканирования, чтобы начать сканирование.
   - **Быстрое сканирование** выявляет наличие вредоносных программ в наиболее уязвимых местах системы (например, папки с документами, загруженные и временные файлы).
   - **Полное Сканирование** проверяет всю систему на наличие вредоносного ПО. Также будут проверены все подключенные утилиты.

Замечание

В зависимости от размера жесткого диска сканирование всей системы может занять некоторое время (до часа или даже больше). Для повышения производительности не рекомендуется запуск этой функции во время выполнения ресурсоемких задач (например, редактирование видео)
Можно отменить сканирование определенных файлов, добавив их в список Исключения в окне Параметры

- **Выборочное сканирование** проверяет определенные файлы или папки на наличие вредоносных программ.

9.3. Включение и выключение Автопилота

Для включения или отключения Автопилота, выполните одно из следующих действий:

- Откройте Bitdefender Antivirus for Mac и нажмите на переключатель, чтобы включить или выключить Автопилот.
- Нажмите на значок в строке меню и выберите **Отключить Автопилот**.

Внимание

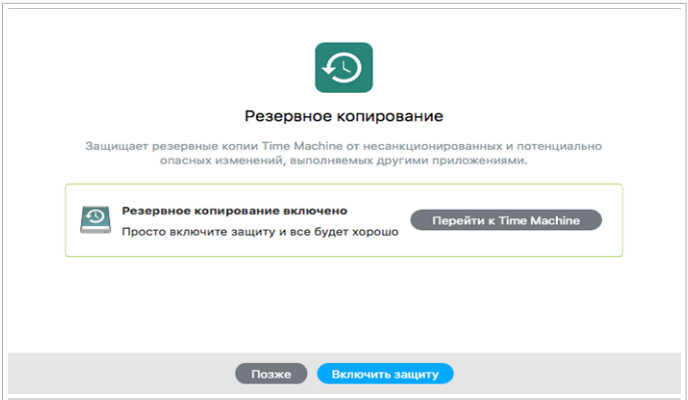
Не рекомендуется отключать Автопилот на длительное время Автоматическая защита от вредоносных программ невозможна при выключенном Автопилоте.

9.4. Резервное копирование

Bitdefender Защита Резервного Копирования обеспечивает дополнительный уровень безопасности резервного диска, а также его содержимого, блокируя доступ к любому внешнему источнику. В том случае, если файлы резервного копирования будут зашифрованы программой-вымогателем, Вы сможете безопасно восстановить их.

Мастер Защиты резервного копирования

Bitdefender мастер Резервного копирования появится сразу после установки Bitdefender Antivirus for Mac на устройство



Мастер Защиты резервного копирования

Необходимо выполнить настройки Резервного копирования до запуска Bitdefender защиты

Если функция Резервного копирования не подключена:

1. Нажмите кнопку **Переход к Резервному копированию**.

   Окно **Резервное копирование** появится в системных настройках

2. Активируйте эту функцию, а затем выберите место для хранения файлов резервных копий.

Для получения дополнительных сведений нажмите на ссылку мастера **Настройка Резервного копирования**

Для включения Bitdefender Защита резервного копирования:

1. Нажмите опцию **Включить защиту**

   Появится окно подтверждения.

2. Нажмите **Закрыть**.

Включение или выключение Защиты резервного копирования

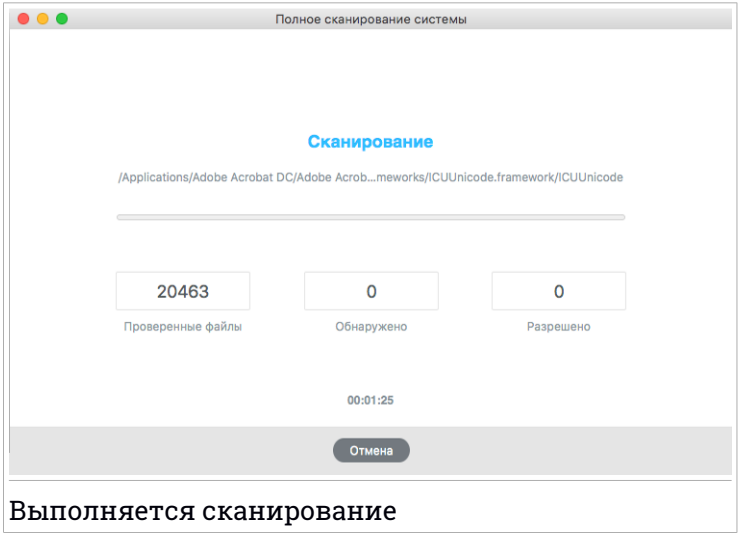
Включение или выключение Защиты резервного копирования

1. Открыть Bitdefender Antivirus for Mac.

2. В строке меню нажмите Bitdefender Antivirus for Mac и выберите **Настройки**.
3. Выберите вкладку **Protection**.
4. Установите или снимите флажок на **Резервное копирование**

9.5. Мастер сканирования

Всякий раз при запуске сканирования будет появляться мастер сканирования Bitdefender Antivirus for Mac



Выполняется сканирование

При каждом сканировании информация о выявленных и устраненных угрозах будет отображаться в режиме реального времени.

Дождитесь окончания сканирования Bitdefender Antivirus for Mac.

Замечание

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

9.6. Устранение угроз

Bitdefender Antivirus for Mac автоматически обнаруживает и предупреждает о проблемах, влияющих на безопасность системы и данных. Таким образом,можно легко устранять угрозы безопасности.

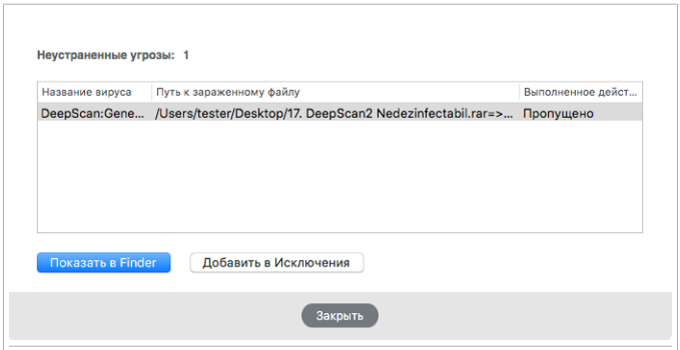
Устранение обнаруженных Bitdefender Antivirus for Mac угроз - это быстрый и легкий способ защиты системы и данных

Обнаруженные проблемы включают:

- **Автопилот** отключен и обновления, а также новые сигнатуры вредоносных программ не загрузились
- В системе обнаружены неустраненные угрозы.
- **Автопилот** отключен.

Чтобы проверить и исправить обнаруженные проблемы:

1. Открыть Bitdefender Antivirus for Mac.
2. Если в Bitdefender нет предупреждений об угрозах, строка состояния будет зеленой. Если обнаружена угроза безопасности, строка состояния поменяет цвет на желтый.
3. Просмотрите характеристики для получения дополнительных сведений.
4. После обнаружения проблемы нажмите кнопку **Просмотр проблем**, для получения сведений, касающихся безопасности системы Действия можно выполнять в появившемся окне.



Окно неустраненных угроз

Список неустраненных угроз обновляется после каждого сканирования системы.

Можно принять следующие меры в отношении неустраннных угроз:

- Показать в Finder. Выполните это действие, чтобы удалить вирусы вручную.
- Добавить в Исключения. Невозможно применить это действие к вредоносным программам, обнаруженных в архивах

9.7. Веб-защита

Bitdefender Antivirus for Mac использует расширение TrafficLight для безопасного просмотра веб-страниц. РасширениеTrafficLight перехватывает, обрабатывает и фильтрует весь веб-трафик, блокируя любой вредоносный контент.

Расширения функционируют и интегрируются со следующими веб-браузерами: Mozilla Firefox, Google Chrome и Safari.

Для защиты от всевозможных угроз, с которыми можно столкнуться при просмотре веб-страниц, доступен набор следующих функций:

- Расширенный Фильтр Угроз предотвращает доступ к веб-сайтам, подозреваемых в фишинге и распространении вредоносных программ.
- Анализатор Результатов Поиска предупреждает о подозрительных веб-сайтах в результатах поисковых запросов.
- Уведомления о шпионских программах - распознает и предупреждает о шпионских программах, обнаруженных на посещаемых веб-сайтах

Функция TrafficLight

Чтобы включить расширения TrafficLight, выполните следующие действия:

1. Открыть Bitdefender Antivirus for Mac.
2. Нажмите **Установить сейчас** для активации Веб-защиты
3. Bitdefender Antivirus for Mac распознает установленный веб-браузер Чтобы установить расширение TrafficLight в браузере, нажмите **Расширение**.
4. Вы будете перенаправлены к:

https://bitdefender.com/solutions/trafficlight.html

5. Выберите **Скачать бесплатно**.
6. Выполните следующие действия для установки расширения TrafficLight, соответствующего Вашему веб-браузеру.

Страница оповещения

В зависимости от того, как расширение TrafficLight классифицирует просматриваемую веб-страницу, в ее области отображается один из следующих значков:

 Эта страница безопасна для посещения. Можете продолжить работу

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

 Следует незамедлительно закрыть веб-страницу Также можно выбрать другой вариант:

- Перейдите на веб-страницу, нажав кнопку **Защитить снова**.
- Игнорируя предупреждение, перейдите на веб-страницу, нажав кнопку **Я осознаю риск. Перейти все равно.**

9.8. Обновления

Каждый день обнаруживаются новые вредоносные программы. Именно поэтому очень важно обновлять Bitdefender Antivirus for Mac, чтобы получить последние сигнатуры вредоносных программ.

Включите **Автопилот** для автоматического обновления вирусных сингатур 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 любая возможность возникновения уязвимости.

- Обновленный Bitdefender Antivirus for Mac обнаруживает новейшие угрозы и очищает зараженные файлы.

- Не обновленный Bitdefender Antivirus for Mac не способен обнаружить и удалить новейшую вредоносную программу, обнаруженную Bitdefender Labs.

9.8.1. Запрос обновления

Можно вручную запросить обновление в любое время

Чтобы проверить наличие обновлений и загрузить их, необходимо активное интернет-соединение

Запросить обновление вручную:

1. Открыть Bitdefender Antivirus for Mac.
2. Нажмите кнопку **Действия** в строке меню.
3. Выберите **Обновить базу данных вирусов**.

Также можно запросить обновление вручную, нажав CMD + U.

Процесс обновления и загруженные файлы доступны для просмотра

9.8.2. Загрузка обновлений через прокси-сервер

Bitdefender Antivirus for Mac обновляется только через прокси-серверы, не требующих аутентификации. Какие-либо настройки параметров программы не требуются.

Если вы подключаетесь к Интернету через прокси-сервер с аутентификацией, необходимо регулярно переключаться на прямое интернет-соединение, чтобы получать обновления сигнатур вредоносных программ.

9.8.3. Обновление предыдущей версии

Для улучшения функций и добавления новых, а также устранения неисправностей продукта, периодически запускаются обновления Эти обновления требуют перезагрузки системы, чтобы начать установку новых файлов. Если для обновления требуется перезагрузка компьютера, Bitdefender Antivirus for Mac по умолчанию продолжит работу с предыдущими файлами до перезагрузки системы. В этом случае процесс обновления не будет мешать работе пользователя.

Когда обновление продукта будет завершено, всплывающее окно сообщит Вам о перезапуске системы. В том случае, если Вы пропустите

это уведомление, Вы можете перезапустить систему вручную или нажать **Перезапуск для обновления**.

10. НАСТРОЙКА СВОЙСТВ

В данной главе рассматриваются следующие темы:

10.1. Доступ к настройкам

Чтобы открыть окно Параметры Bitdefender Antivirus for Mac:

1. Открыть Bitdefender Antivirus for Mac.
2. Сделайте следующее:
   - В строке меню нажмите Bitdefender Antivirus for Mac и выберите **Настройки**.
   - В строке меню нажмите значок и выберите **Настройки.**
   - Нажмите команду - запятая (,)

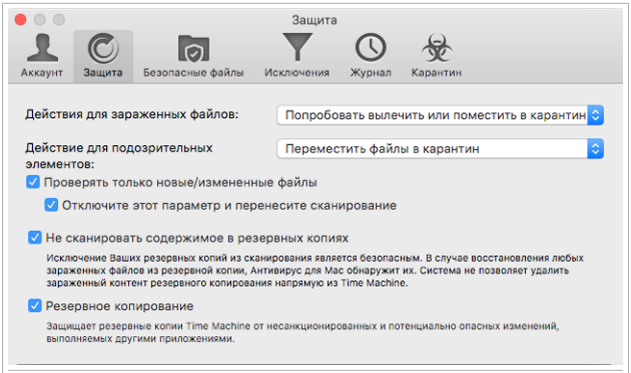
10.2. Информация об учетной записи

В информационном окне отображаются сведения о подписке и учетной записи Bitdefender.

Всякий раз при входе в систему под другой учетной записью Bitdefender, нажмите кнопку **Переключение аккаунта**, введите новый адрес электронной почты и пароль в приложении Bitdefender, затем нажмите **ВХОД**.

10.3. Настройки Безопасности

В окне настроек безопасности представлен общий метод сканирования Можно настроить действия, выполняемые для зараженных и подозрительных файлов, а также другие общие настройки

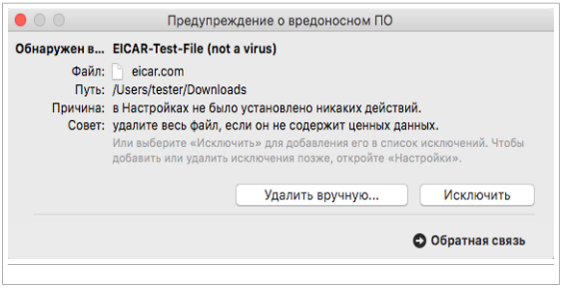


Настройки Безопасности

- **Действия для зараженных файлов.** В случае обнаружения вируса или других вредоносных программ Bitdefender Antivirus for Mac попытается автоматически удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция называется "лечение". Файлы, которые не удается вылечить, перемещаются в папку карантин карантина во избежание распространения вируса.

  Можно настроить приложение таким образом, чтобы к зараженным файлам не предпринималось никаких действий (не рекомендуется) Обнаруженные файлы только регистрируются

  Автопилот обеспечивает защиту от вредоносных программ, оказывая незначительное влияние на производительность системы. Если имеются неисправленные угрозы, Вы можете ознакомиться с ними и предпринять дальнейшие действия



- **Действие для подозрительных элементов:** Файлы помечены эвристическим анализом как подозрительные. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

  Подозрительные файлы перемещаются в карантин по умолчанию. Вирус, изолированный в карантинной зоне, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

  Можете игнорировать подозрительные файлы. Обнаруженные файлы только регистрируются

- **Сканирование только новых/измененных файлов.** Установите этот флажок, чтобы Bitdefender Antivirus for Mac проверял только те файлы, которые не были проверены ранее или были изменены с момента последнего сканирования.

  Можете не применять этот параметр, установив соответствующий флажок.

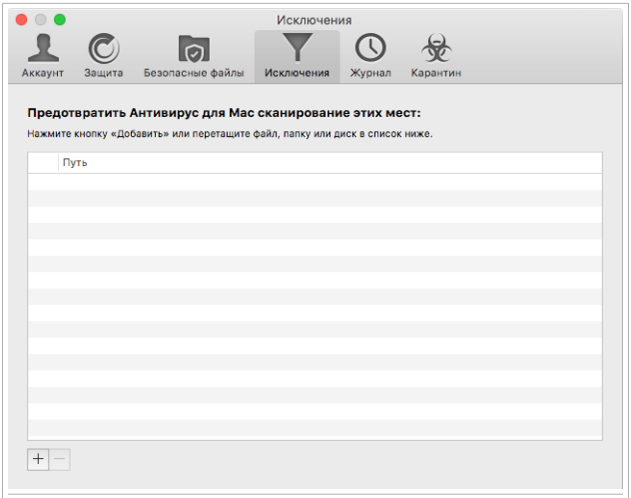
- **Не сканировать содержимое в резервных копиях.** Установите этот флажок для исключения файлов резервного копирования из сканирования. Если зараженные файлы будут восстановлены позднее, Bitdefender Antivirus for Mac автоматически обнаружит их и предпримет соответствующие действия.

- **Резервное копирование.** Установите этот флажок, чтобы защитить файлы, хранящиеся в Резервном копировании. В том случае, если файлы резервного копирования будут зашифрованы программой-вымогателем, Вы сможете безопасно восстановить их.

10.3.1. Исключения из сканирования

Можете установить Bitdefender Antivirus for Mac таким образом, чтобы определенные файлы и папки не сканировались Например, Вы можете исключить из сканирования:

- Файлы, ошибочно идентифицированые как зараженные (ложные срабатывания)
- Фалы, вызывающие ошибки сканирования
- Том резервного копирования



Исключения из сканирования

Список исключений содержит недопустимые пути сканирования.

Задать исключение сканирования можно двумя способами:

- Перетащите & файл, папку или том на список исключений и отпустите.
- Под списком исключений нажмите кнопку со знаком «плюс» (+) Затем выберите файл, папку или том для исключения из сканирования.

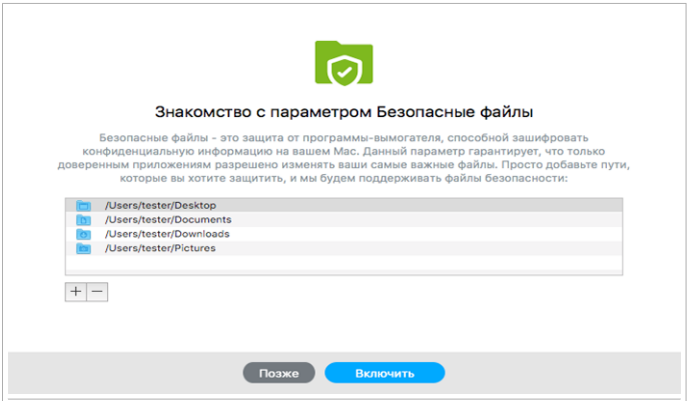
Чтобы удалить исключение из сканирования, выберите его из списка и нажмите кнопку со знаком «минус» (-), расположенную под списком исключений.

10.4. Безопасные файлы

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.

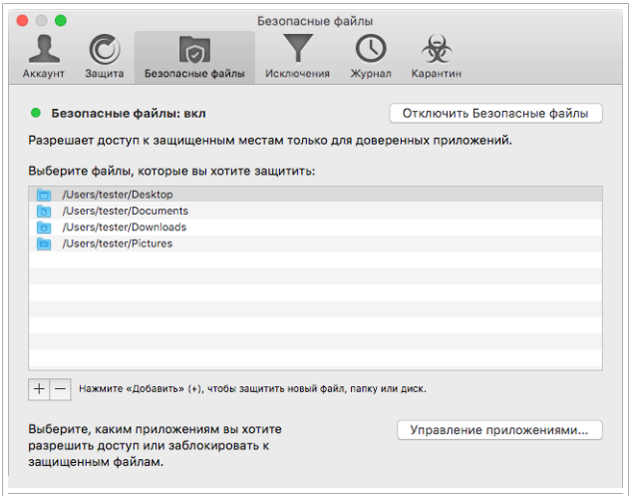
Bitdefender обеспечивает целостность системы, используя новейшие технологии. Защищает системные области от атак вымогателей, не влияя на производительность системы. Тем не менее, Вы также можете оградить такие личные файлы, как документы, фотографии или фильмы,

от доступа ненадежных приложений. При помощи Bitdefender Безопасные файлы можно перенести файлы в хранилище и установить в настройках приложения с правом внесения изменений.



Мастер Безопасных файлов

Мастер Bitdefender Безопасные файлы появится сразу после установки Bitdefender Antivirus for Mac на устройстве Macintosh. Выберите или добавьте новые местоположения, нуждающиеся в защите, затем нажмите **Включить Безопасные файлы**.



Безопасные файлы

Существует два способа добавления файлов в защищенную компьютерную среду:

- Перетащите & и отпустите файл, папку или том в окно Безопасные файлы.
- Нажмите кнопку со знаком «плюс» (+), расположенную под списком защищенных файлов. Затем выберите файл,папку или том, подлежащие защите в случае атаки вируса-вымогателя.

Вы будете получать уведомления каждый раз, когда неизвестное приложение с подозрительным поведением будет пытаться изменить добавленные файлы. Нажмите **Разрешить** или **Заблокировать**, чтобы добавить его в список Управление приложениями.

10.4.1. Управление приложениями

Те приложения, которые попытаются изменить или удалить защищенные файлы могут быть помечены как потенциально опасные и будут добавлены в список Заблокированных приложений. Если Вы уверены, что его поведение такого приложения является нормальным, Вы можете разблокировать его, нажав кнопку **Управление приложениями** и изменить его статус на «Разрешить».

Статус "разрешенных" приложений можно изменить на "заблокированные"

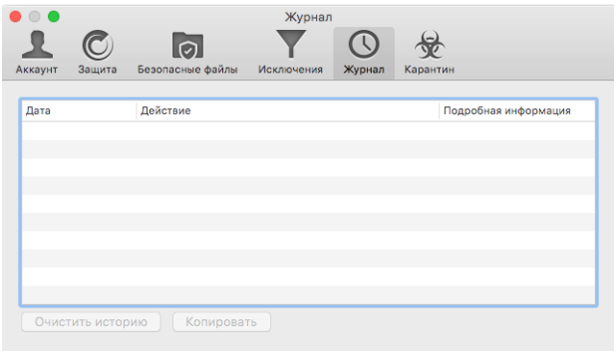
Перетащите или нажмите на знак плюс (+) чтобы добавить в список больше приложений.

10.5. Журнал

Bitdefender ведет подробный журнал событий, касающихся его автивности, которые он выполняет на вашем компьютере. Каждый раз, когда происходит событие, влияющие на безопасность системы или данных, в Bitdefender Antivirus for Mac История поступит новое сообщение.

События являются важным инструментом для мониторинга и управления защитой Bitdefender. Например, можно легко проверить результат обновления, если на компьютере было обнаружено вредоносное ПО, попытка доступа несанкционированного приложения к диску Резервного копирования и т.д.

Отображаются сведения о действиях продукта.



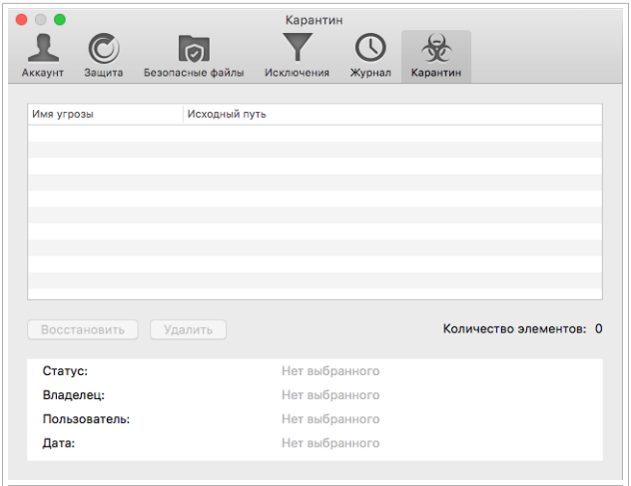
Журнал

Для удаления журнала истории нажмите кнопку **Очистить историю**

Нажав на кнопку **Копировать** можно скопировать эту информацию в буфер обмена.

10.6. Карантин

Bitdefender Antivirus for Mac изолирует зараженные или подозрительные файлы в безопасной области - карантине. Вирус, изолированный в карантинной зоне, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.



Элементы карантина

В разделе Карантин отображаются файлы, изолированные в данный момент в папке Карантин.

Чтобы удалить файл из карантина, выберите его и нажмите **Удалить**. Для восстановления файла из папки карантина в исходную папку необходимо выбрать файл и нажать **Restore**.

11. BITDEFENDER CENTRAL

В данной главе рассматриваются следующие темы:

- «*О Bitdefender Central*» (p. 263)
- «*Мои подписки*» (p. 264)
- «*Мои устройства*» (p. 265)

11.1. О Bitdefender Central

Bitdefender Central это веб-платформа, на которой у Вы имеете доступ к онлайн-функциям и услугам, а также можете удаленно выполнять важные задачи на устройствах, на которых установлен Bitdefender. Вы можете войти в учетную запись Bitdefender с любого компьютера или мобильного устройства, подключенного к сети Интернет, перейдя https://central.bitdefender.com. Если у вас есть доступ к нему, вы можете начать делать следующее:

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

11.2. Доступ к Bitdefender Central

Есть несколько способов доступа к Bitdefender Central. В зависимости от задачи, которую вы хотите выполнить, вы можете использовать любую из следующих возможностей:

- Из интерфейса Bitdefender Antivirus for Mac:

1. Нажмите ссылку **Переход к учетной записи** в нижней правой части экрана.

- Из вашего веб-браузера:
  1. Откройте веб-браузер на любом устройстве с доступом в Интернет.
  2. Перейти к: https://central.bitdefender.com.
  3. Войдите в свой аккаунт, используя адрес электронной почты и пароль.

11.3. Мои подписки

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

11.3.1. Активировать подписку

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

Если Вы приобрели код активации у наших реселлеров или получили его в подарок, можете добавить его к подписке Bitdefender .

Для активации подписки, используя код активации, выполните следующие действия:

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок , расположенный в верхнем левом углу окна, затем выберите **Мои Подписки**.
3. Нажмите кнопку**АКТИВИРОВАТЬ КОД**, затем введите код в соответствующем поле.
4. Нажмите **АКТИВИРОВАТЬ КОД**, чтобы продолжить.

Подписка активирована.

Чтобы начать установку продукта на устройства см. «*Установка Bitdefender Antivirus for Mac*» (p. 236).

11.3.2. Купить подписку

Подписку можно приобрести непосредственно из учетной записи Bitdefender, выполнив следующие действия:

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок , расположенный в верхнем левом углу окна, затем выберите **Мои Подписки**.
3. Нажмите ссылку **Купить сейчас**. Переход на веб-страницу, с которой можно совершить покупку.

Как только процесс завершится, подписка будет видна в нижнем правом углу основного интерфейса продукта.

11.4. Мои устройства

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

11.4.1. Настройка устройства

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: добавьте фотографию, адрес электронной почты, номер телефона и выберите дату рождения.
6. Нажмите **ДОБАВИТЬ** чтобы сохранить профиль.
7. Выберите нужного владельца из списка **Владелец устройства**, затем нажмите кнопку **НАЗНАЧИТЬ**.

11.4.2. Действия по восстановлению

Для удаленного обновления Bitdefender на устройстве:

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**.

Чтобы удаленно включить функцию автопилота:

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**. Нажмите на соответствующий переключатель для включения Автопилота.

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 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. Дополнительные сведения о процессах сканирования см. в «*Сканирование Mac*» (p. 246).

12. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

Каким образом можно ознакомиться с Bitdefender Antivirus for Mac до оформления заявки на подписку?

Как новый клиент Bitdefender Вы хотели бы ознакомиться с работой продукта до оформления покупки. Пробный период составляет 30 дней и Вы можете продолжить пользоваться установленным продуктом только в том случае, если оформите покупку подпискиBitdefender. Чтобы попробовать Bitdefender Antivirus for Mac необходимо:

1. Создать учетную запись Bitdefender, выполнив следующие действия:
   - Перейти к: https://central.bitdefender.com.
   - Введите необходимую информацию в соответствующих полях, затем нажмите **СОЗДАТЬ АККАУНТ**.

     Информация, которую вы предоставите, останется конфиденциальной.
2. Загрузить Bitdefender Antivirus for Mac следующим образом:
   - В окне **МОИ УСТРОЙСТВА** нажмите **УСТАНОВИТЬ ЛОКАЛЬНУЮ ЗАЩИТУ**.
   - Выберите одну из двух доступных опций:
     - **Загрузка**

       Нажмите на кнопку и сохраните установочный файл.
     - **На другое устройство**

       Выберите **macOS** чтобы загрузить Bitdefender, затем нажмите **ПРОДОЛЖИТЬ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ**.
   - Запустите Bitdefender продукт, который вы скачали.

У меня есть код активации. Как добавить его срок действия к моей подписке?

Если Вы приобрели код активации у наших реселлеров или получили его в подарок, можете добавить его к подписке Bitdefender .

Для активации подписки, используя код активации, выполните следующие действия:

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок , расположенный в верхнем левом углу окна, затем выберите **Мои Подписки**.
3. Нажмите кнопку**АКТИВИРОВАТЬ КОД**, затем введите код в соответствующем поле.
4. Нажмите еще раз кнопку **ACTIVATION CODE**.

Теперь расширение отображается в учетной записи Bitdefender и в нижней правой части экрана ВашегоBitdefender Antivirus for Mac.

Сканирование журнала выявило неустраненные элементы. Каким образом их удалить?

Этими элементами могут быть:

- архивы с ограниченным доступом (xar, rar и т.д.)

  Решение: используйте опцию **Раскрыть**, чтобы найти файл и вручную удалить его. Убедитесь, то корзина пуста.

- почтовые ящики с ограниченным доступом (Thunderbird и т.д.)

  Решение: используйте приложение для удаления записи, содержащей зараженный файл.

- Содержимое резервных копий

  Решение: Включите в настройках защиты опцию **Не сканировать содержимое резервных копий** или **Добавить в исключения** обнаруженные файлы.

  Если зараженные файлы будут восстановлены позднее, Bitdefender Antivirus for Mac автоматически обнаружит их и предпримет соответствующие действия.

> **Замечание**
> Ограниченный доступ к файлам означает, что файлы Bitdefender Antivirus for Mac можно только открывать, но не изменять.

Где можно просмотреть подробную информацию о действии продукта?

Bitdefender ведет журнал всех важных действий, изменений статусов и других важных действий. Чтобы получить доступ к этой информации, откройте окно Настройки Bitdefender Antivirus for Mac:

1. Открыть Bitdefender Antivirus for Mac.
2. Сделайте следующее:
   - В строке меню нажмите Bitdefender Antivirus for Mac и выберите **Настройки**.
   - В строке меню нажмите значок и выберите **Настройки.**
   - Нажмите команду - запятая (,)
3. Выберите вкладку **История**.

   Отображаются сведения о действиях продукта.

Возможно обновление Bitdefender Antivirus for Mac с использованием прокси-сервера?

Bitdefender Antivirus for Mac обновляется только через прокси-серверы, не требующих аутентификации. Какие-либо настройки параметров программы не требуются.

Если вы подключаетесь к Интернету через прокси-сервер с аутентификацией, необходимо регулярно переключаться на прямое интернет-соединение, чтобы получать обновления сигнатур вредоносных программ.

Как удалить Bitdefender Antivirus for Mac?

Чтобы удалить Bitdefender Antivirus for Mac, выполните следующие действия:

1. Откройте окно **Поиск**, перейдите в папку Приложения и выберите Утилиты.
2. Дважды нажмите приложение Bitdefender Удаление.
3. Для продолжения нажмите **Удалить**
4. Дождитесь завершения процесса, затем нажмите **Закрыть**

> **Важно**
> В случае необходимости можно обратиться в службу поддержки клиентов Bitdefender, как указано в «*Обращение за помощью*» (p. 330).

Как удалить расширения TrafficLight из моего веб-браузера?

- Чтобы удалить расширения TrafficLight из Mozilla Firefox, выполните следующие действия:
  1. Откройте браузер Mozilla Firefox.
  2. Перейдите в **Инструменты** и выберите **Дополнения**.
  3. Выберите **Расширения** в левой колонке.
  4. Выберите расширение и нажмите **Удалить**.
  5. Перезагрузите браузер для завершения процесса удаления.
- Чтобы удалить расширения TrafficLight из Google Chrome, выполните следующие действия:
  1. Откройте браузер Google Chrome.
  2. Нажмите  на панели инструментов браузера.
  3. Перейдите в **Инструменты** и выберите **Расширения**.
  4. Выберите расширение и нажмите **Удалить**.
  5. Нажмите **Удалить**, чтобы подтвердить процесс удаления.
- Чтобы удалить Bitdefender TrafficLight из Safari, выполните следующие действия:
  1. Откройте браузер Safari.
  2. Нажмите  на панели инструментов браузера и выберите **Настройки**.
  3. Перейдите на вкладку **Расширения** и найдите в списке **BitdefenderTrafficLight Safari**.
  4. Выберите расширение и нажмите **Удалить**.
  5. Нажмите **Удалить**, чтобы подтвердить процесс удаления.

МОБИЛЬНАЯ БЕЗОПАСНОСТЬ ДЛЯ IOS

13. ЧТО ТАКОЕ BITDEFENDER MOBILE SECURITY FOR IOS

Онлайн-операции, такие как оплата счетов, резервирование отелей или покупка товаров и услуг, удобны и не доставляют хлопот. Но так как многие из них происходят в Интернете, они сопряжены с высокими рисками и, если не соблюдать детали безопасности, личные данные могут быть взломаны. Что может быть более важным, чем защита хранящихся в онлайн-аккаунтах и на личном смартфоне данных?

Bitdefender Mobile Security for iOS позволяет:

- Проверять, произошла ли какая-либо утечка в ежедневно используемых онлайн-аккаунтах.
- Находить, блокировать и удалять данные с Вашего устройства в случае его потери или кражи

Bitdefender Mobile Security for iOS предоставляется для бесплатного использования и активируется с помощью Bitdefender account.

14. НАЧАЛО РАБОТЫ

Технические Требования

Bitdefender Mobile Security for iOS работает на любом устройстве под управлением iOS 10 и выше, для его стабильной работы и обнаружения утечки данных с Ваших аккаунтов необходимо стабильное подключение к интернету.

Установка Bitdefender Mobile Security for iOS

- **Из Bitdefender Central**
  - На iOS
    1. Перейти к: https://central.bitdefender.com.
    2. Войдите в ваш аккаунт Bitdefender.
    3. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
    4. Нажмите **УСТАНОВКА ЛОКАЛЬНОЙ ЗАЩИТЫ**.
    5. Выберите из списка Bitdefender Мобильная безопасность, затем нажмите **ПЕРЕЙТИ В APP STORE**
    6. Нажмите **INSTALL** на экране App Store.
  - На Windows, macOS, Android
    1. Перейти к: https://central.bitdefender.com.
    2. Войдите в ваш аккаунт Bitdefender.
    3. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
    4. Нажмите **УСТАНОВКА ЛОКАЛЬНОЙ ЗАЩИТЫ**.
    5. На Windows и macOS нажмите ссылку **На другом устройстве** .

       На Android нажмите **Хотите защитить другие устройства?** .
    6. Выбрать **iOS**.
    7. Выберите из списка **Bitdefender Mobile Security**, а затем нажмите **CONTINUE**.

8. Введите адрес электронной почты в соответствующем поле, а затем нажмите **SEND**.
9. Зайдите в учетную запись с устройства iOS, затем нажмите **ПРИОБРЕСТИ В AppStore** в письме, отправленном с нашего сервера.

   Вы переадресованы в **App Store** приложение.
10. Нажмите **INSTALL** на экране App Store.

- **Из App Store**

  Ищите Bitdefender Mobile Security for iOS для поиска и установки приложения.

Мастер

Мастер ввода, содержащий сведения о функциях продукта, отображается при первом открытии приложения. Нажмите **Get started** для продолжения.

Войдите в ваш аккаунт Bitdefender

Для работы Bitdefender Mobile Security for iOS необходимо связать устройство с Вашей учетной записью Bitdefender, выполнив вход в учетную запись из приложения. Когда мастер ввода будет заполнен, введите адрес электронной почты и пароль Вашей учетной записи Bitdefender, затем нажмите **Вход**. Если у Вас нет учетной записи, коснитесь соответствующей ссылки, чтобы создать ее.

Панель управления

Нажмите Bitdefender Mobile Security for iOS иконку в вашем списке приложений, чтобы открыть интерфейс приложения.

Чтобы получить доступ к необходимой информации, коснитесь соответствующего значка в нижней части экрана.

Приватность

Узнайте, была ли утечка Ваших учетных записей электронной почты или нет. Для получения дополнительной информации перейдите к «*Приватность*» (p. 277).

Анти-вор

Найти и заблокировать устройство для предотвращения утечки данных Для получения дополнительной информации перейдите к «*Анти-Вор Характеристики*» (p. 279).

Чтобы просмотреть дополнительные параметры, нажмите значок на Вашем устройстве на главном экране приложения. Появятся следующие параметры:

- Начало - возможен быстрый просмотр продукта.
- Обратная связь - запускает по умолчанию почтовую службу, с которой Вы можете отправить нам Ваши отзывы о приложении.
- App info - отображение информации об установленной версии.

15. ПРИВАТНОСТЬ

Bitdefender Account Privacy определяет, произошли ли какие-либо утечки данных в учетных записях, которые вы используете для он-лайн платежей, покупок или подписания в разных приложениях или на веб-сайтах. Данные, сохраненные в учетной записи, могут являться паролями, информацией о кредитной карте или банковского счета, и, если им не была надлежащим образом обеспечена защита, может произойти кража информации или вторжение в частную жизнь.

Статус конфиденциальности учетной записи отображается сразу после проверки.

Чтобы проверить утечку из какой-либо учетной записи, коснитесь **Сканировать утечки**.

Чтобы начать безопасное хранение личных данных:

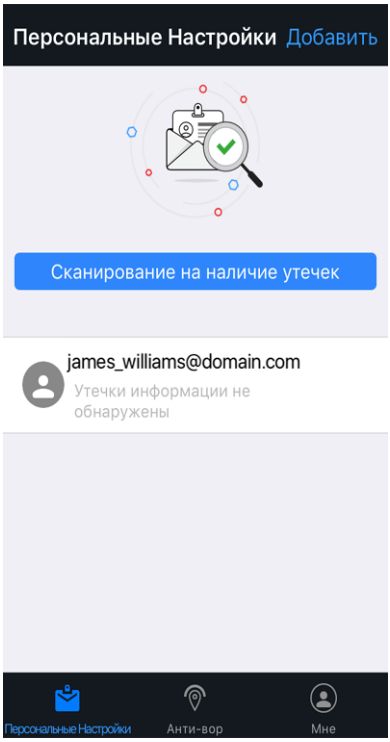
1. Нажмите значок  в нижней части экрана.
2. Нажмите **Добавить** в правом верхнем углу экрана.
3. Введите Ваш адрес электронной почты в соответствующее поле, затем нажмите **Далее**

   Bitdefender должен проверить эту учетную запись до отображения личной информации. Поэтому на указанный адрес электронной почты отправляется электронное письмо с кодом проверки.
4. Проверьте Ваш почтовый ящик и введите полученный код в области **Конфиденциальность аккаунта** Вашего приложения. Если Вы не можете найти письмо с подтверждением в папке «Входящие», проверьте папку «Спам».

   Отображается статус конфиденциальности проверенной учетной записи.

В случае обнаружения утечек в любом из Ваших аккаунтов, рекомендуем сменить пароль как можно скорее. Чтобы создать надежный и безопасный пароль, примите во внимание следующие советы:

- Сделайте его не менее восьми символов.
- Включите символы нижнего и верхнего регистра.
- Добавьте хотя бы одно число или символ, например, #, @,% или !.



Приватность

16. АНТИ-ВОР ХАРАКТЕРИСТИКИ

Bitdefender может помочь вам найти ваше устройство и предотвратить утечку личных данных.

Все, что вам нужно сделать, это активировать Анти-Вор на вашем устройстве и, при необходимости, зайти в **Bitdefender Central** с любого веб-браузера, из любого места.

Bitdefender Mobile Security for iOS предлагает следующие функции Анти-Вор:

Удаленное Местонахождение
Посмотреть текущее местоположение Вашего устройства на карте.

Точность расположения зависит от того, как Bitdefender определяет его:

- Если на устройстве включен GPS, местоположение устройства можно отследить с точностью до нескольких метров, пока оно находится в радиусе действия спутников GPS (т.е. не внутри здания).
- Если устройство в помещении, его местонахождение может быть определено с точностью до десятков метров, при условии, что включена функция Wi-Fi и есть доступные беспроводные сети в радиусе действия.
- Иначе, местонахождение будет определяться с использованием данных сети мобильной связи, которые могут предложить точность до нескольких сот метров.

Удаленная блокировка
Блокировать удаленно экран Вашего устройства.

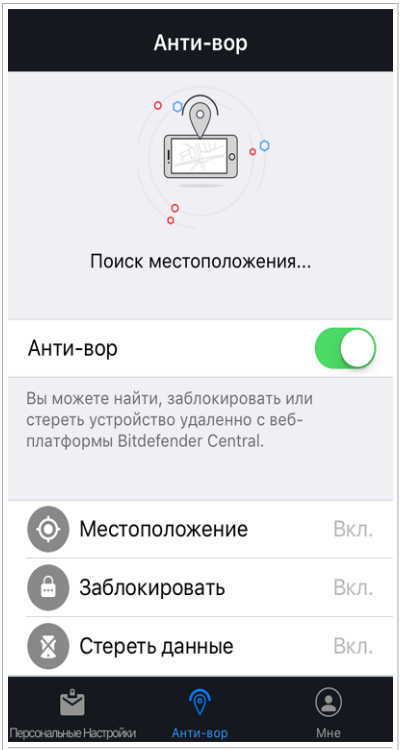
Удаленное стирание
Удаление всей персональной информации с утерянного устройства.

Активация Анти-Вор

Для включения функции Анти-вор выполните следующие действия:

1. Нажмите значок  в нижней части экрана.
2. Включите переключатель.

3. Нажмите **Разрешить** установить профиль MDM (Управление мобильными устройствами) чтобы Bitdefender продолжил процесс активации.
4. Введите PIN-код, установленный для защиты смартфона, чтобы разрешить Bitdefender установить файлы.
5. Предоставьте доступ к местоположению Вашего устройства, чтобы Bitdefender мог найти его в случае кражи или утери.



Анти-вор

Использование функций Анти-Вор из Bitdefender Central (Веб-Защита)

Чтобы получить доступ к функции Анти-Вор из вашей учетной записи Bitdefender:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в ваш аккаунт Bitdefender.
3. Нажмите значок ☰ в верхнем левом углу экрана, затем выберите **Мои устройства**.
4. Коснитесь нужной карты устройства, затем вкладку **АнтиВор**.
5. В нижнем части окна нажмите иконку ⋯, а затем кнопку соответствующую нужной функции:

   Locate - отображение местоположение Вашего устройства на картах.

   Заблокировать> - заблокируйте ваше устройство и установите PIN код для его разблокировки.

   Удалить - удалить все данные с вашего устройства.

   Важно
   После очистки устройства все возможности Анти-Вора перестанут функционировать.

17. АККАУНТ BITDEFENDER

Учетная запись Bitdefender необходима для активации Bitdefender Mobile Security for iOS. Для доступа к сетевым функциям и услугам продукта, удаленного выполнения важных задач на устройствах Bitdefender можно войти в свой аккаунт с любого компьютера или мобильного устройства, подключенного к Интернету, перейдя в https://central.bitdefender.com.

Мои устройства

Раздел **Мои устройства** в вашей учетной записи Bitdefender дает возможность устанавливать, управлять и осуществлять удаленные действия на любом устройстве, на котором установлен Bitdefender,при условии, что оно включен и подключено к Интернету. Карточки устройства отображают имя устройства, состояние защиты и риски безопасности, влияющие на защиту устройств.

Для простого распознавания и управления устройствами можно задать имя устройства и назначить или создать владельца для каждого из них:

1. Нажмите значок ☰ в верхнем левом углу экрана, затем выберите **Мои устройства**.

2. Нажмите на желаемую карту устройства, затем значок ⋮ в правом верхнем углу экрана. Доступны следующие опции:

   - **Settings** -здесь Вы можете изменить имя выбранного устройства.
   - **Профиль** - назначение профиля для выбранного устройства Нажмите **Добавить владельца**, затем заполните соответствующие поля, укажите имя, адрес электронной почты, номер телефона, дату рождения, а также изображение профиля.
   - **Удалить** -удаление профиля с назначенным устройством из учетной записи Bitdefender.

Редактирование данных учетной записи

Для входа в систему с другой учетной записью, изменения пароля или редактирования данных Вашего профиля непосредственно из приложения:

1. Нажмите значок в нижней части экрана.
2. Нажмите значок в верхней правой части экрана. Можно выполнить следующие действия:
   - **Редактировать профиль** - позволяет изменять информацию о Вашем профиле и учетной записи.
   - **Выход** - позволяет выйти из текущей учетной записи Bitdefender и войти в систему с другой.
   - **Изменить пароль** - позволяет сменить пароль, установленный для Вашей Bitdefender учетной записи .

MOBILE SECURITY ДЛЯ ANDROID

18. ЗАЩИТНЫЕ ФУНКЦИИ

Bitdefender Mobile Security & Antivirus защищает ваше Android устройство, используя защитные функции:

- Антивирусная проверка
- Приватность
- Интернет-защита
- VPN
- Анти-Вор, включает:
  - Удаленное Местонахождение
  - Удаленная блокировка устройства
  - Удаленное стирание данных устройства
  - Удаленный сигнал тревоги устройства
- Блокировка приложений
- Оценка безопасности
- Отчеты
- WearON

Вы можете использовать функции продукта в течении 14 дней, бесплатно. После истечения этого срока, вам необходимо приобрести полную версию, для защиты вашего мобильного устройства.

19. НАЧАЛО РАБОТЫ

Технические Требования

Bitdefender Mobile Security & Antivirus работает на любом устройстве под управлением Android 4.0 и выше. Активное подключение к Интернету требуется для сканирования вредоносного ПО в облаке.

Установка Bitdefender Mobile Security & Antivirus

- **Из Bitdefender Central**
  - На Android
    1. Перейти к: https://central.bitdefender.com.
    2. Войдите в ваш аккаунт Bitdefender.
    3. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
    4. Нажмите **УСТАНОВКА ЛОКАЛЬНОЙ ЗАЩИТЫ**.
    5. Выберите из списка **Bitdefender Мобильная безопасность**, а затем нажмите **Пройти на GOOGLE PLAY**.
    6. Нажмите **Установить** в окне Google Play.
  - На Windows, macOS, iOS
    1. Перейти к: https://central.bitdefender.com.
    2. Войдите в ваш аккаунт Bitdefender.
    3. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
    4. Нажмите **УСТАНОВКА ЛОКАЛЬНОЙ ЗАЩИТЫ**.
    5. На Windows и macOS нажмите ссылку **На другом устройстве** .

       На iOS нажмите **Хотите защитить другие устройства?** .
    6. Выберите **Android**.
    7. В списке выберите **Bitdefender Мобильная безопасность** , затем нажмите **ПРОДОЛЖИТЬ** .

8. Введите адрес электронной почты в соответствующем поле, затем нажмите **Отправить**.
9. Зайдите в учетную запись электронной почты с вашего устройства Android, а затем нажмите кнопку **Скачать с Google Play**.

   Вы переадресованы в **Google Play**.
10. Нажмите **Установить** в окне Google Play.

- **Из Google Play**

  Найдите Bitdefender Mobile Security & Antivirus, чтобы установить приложение.

  Или отсканируйте QR код:

Войдите в ваш аккаунт Bitdefender

Для использования Bitdefender Mobile Security & Antivirus, необходимо связать Ваше устройство с учетной записью Bitdefender, Facebook, Google или Microsoft, выполнив вход в учетную запись из приложения. При открытии приложения в первый раз, вам будет предложено войти в учетную запись.

Если вы установили Bitdefender Mobile Security & Antivirus с вашего Bitdefender аккаунта, то приложение будет пытаться автоматически войти в этот аккаунт.

Чтобы подключить ваше устройство к учетной записи Bitdefender:

1. Открыть Bitdefender Mobile Security & Antivirus.

2. Введите Ваш адрес электронной почты и пароль аккаунта Bitdefender в соответствующие поля. Если у Вас нет учетной записи Bitdefender и Вы хотите ее создать, выберите соответствующую ссылку.
3. Две дополнительные задачи могут быть выполнены во время этого шага:
   - Прежде чем приступать к установке, прочитайте **Соглашение о подписке** . Соглашение о Подписке содержит условия и положения, в соответствии с которыми используется Bitdefender Mobile Security & Antivirus
   - Держите включенной опцию **Помощь в улучшении путем автоматического отправления анонимной статистики**. 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.
4. Нажмите **Войти** .

Чтобы войти в систему с помощью учетной записи Facebook, Google или Microsoft, коснитесь службы, которую хотите использовать, в области **Или войти с помощью**. Вы будете перенаправлены на страницу входа в выбранной службе. Следуйте инструкциям, чтобы связать Вашу учетную запись с Bitdefender Mobile Security & Antivirus.

Замечание

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

Активация Bitdefender Mobile Security & Antivirus

Для использования защиты Bitdefender Mobile Security & Antivirus, вы должны зарегистрировать ваш продукт, используя лицензионный ключ или подписку, которые определяют, как долго вы можете использовать продукт. Как только срок истек, программа перестает выполнять свои функции защиты устройства.

Чтобы активировать Bitdefender Mobile Security & Antivirus:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Приложение отобразит информацию о текущем состоянии подписки.

   Нажмите **У МЕНЯ ЕСТЬ КОД**.
3. Введите код активации в соответствующее поле, а затем нажмите **Активировать**.

Чтобы продлить имеющуюся подписку:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Информация об аккаунте** из списка.
3. В разделе **Продлить подписку** введите код активации, а затем нажмите **Активировать**.

   В качестве альтернативы вы можете продлить свою текущую подписку, обратившись к перечисленным предложениям.

Панель управления

Нажмите Bitdefender Mobile Security & Antivirus иконку в вашем списке приложений, чтобы открыть интерфейс приложения.

Панель управления предоставляет информацию о состоянии безопасности вашего устройства и позволяет вам легко управлять всеми функциями защиты.

Когда процесс запущен или функция требует ввод данных, карточка с более подробной информацией и возможные действия отобразятся в панели управления.

Вы можете получить доступ к функциям Bitdefender Mobile Security & Antivirus и легко переходить от раздела к разделу с помощью кнопки **Меню**, которая находится в правом верхнем углу экрана:

Антивирусная проверка

Позволяет инициировать проверку по запросу, а также включение или отключение Проверки Хранилищ. Для получения дополнительной информации перейдите к *«Антивирусная проверка»* (p. 291).

Приватность

Проверяет, произошла ли утечка данных в ваших онлайн-аккаунтах. Для получения дополнительной информации перейдите к «*Приватность*» (p. 294).

Интернет-защита

Позволяет вам включать или отключать функцию Интернет Защиты. Для получения дополнительной информации перейдите к «*Интернет-защита*» (p. 296).

VPN

Шифрует интернет-связь, помогая поддерживать Вашу конфиденциальность независимо от того, к какой сети Вы подключены. Для получения дополнительной информации перейдите к «*VPN*» (p. 298).

Анти-вор

Позволяет вам включать или отключать функцию Анти-Вор, и настраивать параметры Анти-Вор. Для получения дополнительной информации перейдите к «*Анти-Вор Характеристики*» (p. 302).

Блокировка приложений

Позволяет защитить ваши установленные приложения, путем установки PIN кода. Для получения дополнительной информации перейдите к «*Блокировка приложений*» (p. 308).

Оценка безопасности

Предоставляет вам информацию о приложениях Android, установленных на вашем устройстве и действиях, которые они совершают в фоновом режиме. Для получения дополнительной информации перейдите к «*Оценка безопасности*» (p. 314).

Отчеты

Ведет журнал всех важных действий, изменений и других критических сообщений, связанных с активностью вашего устройства. Для получения дополнительной информации перейдите к «*Отчеты*» (p. 316).

WearON

Взаимодействует с вашими SmartWatch для нахождения вашего телефона, в случае его утери. Для получения дополнительной информации перейдите к «*WearON*» (p. 317).

20. АНТИВИРУСНАЯ ПРОВЕРКА

Bitdefender защищает ваше устройство и информацию от вредоносных приложений, используя сканирование при установке и по требованию.

Замечание
Убедитесь, что ваше устройство подключено к сети Интернет. Если ваше устройство не подключено к Интернету, процесс сканирования не начнет.

- **Сканирование при установке**

  Всякий раз, когда вы устанавливаете приложение, Bitdefender Mobile Security & Antivirus автоматически просканирует его, используя облачные технологии. Процесс сканирования будет запускаться каждый раз после обновления приложения.

  Этот тип сканирования использует функцию Автопилот. Автопилот - это интеллектуальный сканер, который сканирует и блокирует вирусы в устанавливаемых и обновляемых приложениях.

  Если приложение признано вредоносным, появится предупреждение и запрос на его удаление. Нажмите **Удалить** для перехода на экран удаления приложения.

- **Сканирование по запросу**

  Если вы хотите удостовериться, что приложения, установленные на вашем устройстве, безопасны для использования - вы можете начать сканирование по требованию.

  Чтобы начать сканирование по требованию, просто нажмите кнопку **Начать сканирование** из раздела Антивирусная проверка, который доступен на панели управления.

  В качестве альтернативы, вы можете запустить сканирование выполнив следующие действия:

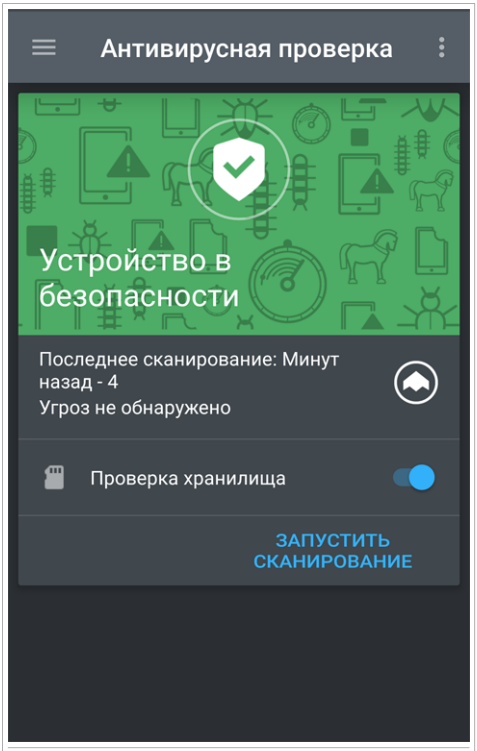
  1. Открыть Bitdefender Mobile Security & Antivirus.
  2. Нажмите кнопку **Меню** и выберите **Антивирусная проверка** из списка.
  3. Нажмите **Начать сканирование**.

Замечание

Дополнительные разрешения требуются на Android 6 для функции скрытого фото. После нажатия на кнопку **Начать сканирование** выберите **Разрешить** для следующих действий:

- Разрешить **Антивирус** совершать и управлять телефонными звонками?
- Разрешить **Антивирус** получать доступ к фотографиям, медиа, а также файлам на вашем устройстве?

Процесс сканирования будет отображен и вы сможете остановить его в любой момент.



Антивирусная Проверка

По умолчанию, Bitdefender Mobile Security & Antivirus будет сканировать внутреннюю память вашего устройства, в том числе

любую установленную SD-карту. В этом случае, любые опасное приложение, которые могут быть на карте могут быть обнаружены, прежде чем причинить вред.

Чтобы включить или выключить сканирование памяти:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Антивирусная проверка** из списка.
3. Нажмите на соответствующую кнопку.

Можно также включить или выключить сканирование памяти из области **Настройки**, нажав кнопку  , а затем соответствующий переключатель.

Если будут обнаружены вредоносные приложения, информация о них будет отображена и вы сможете удалить их нажав кнопку **Удалить**.

Плитка Malware Scanner отображает статус вашего устройства. Если ваше устройство безопасно, плитка будет зеленой. Когда устройство требует сканирование или нуждается в каких-либо действиях, которые требуется ввод, то плитка будет красной.

21. ПРИВАТНОСТЬ

Bitdefender Account Privacy определяет, произошли ли какие-либо утечки данных в учетных записях, которые вы используете для он-лайн платежей, покупок или подписания в разных приложениях или на веб-сайтах. Данные, сохраненные в учетной записи, могут являться паролями, информацией о кредитной карте или банковского счета, и, если им не была надлежащим образом обеспечена защита, может произойти кража информации или вторжение в частную жизнь.

Статус конфиденциальности учетной записи отображается сразу после проверки.

Автоматическое повторное сканирование устанавливается для запуска в фоновом режиме, но сканирование вручную может также выполняться ежедневно.

Уведомления будут отображаться каждый раз, когда будут обнаружены новые утечки, содержащие любые проверенные учетные записи электронной почты.

Чтобы начать безопасное хранение личных данных:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Конфиденциальность аккаунта** из списка.
3. Нажмите синий круг в правом нижнем углу экрана.
4. Введите Ваш адрес электронной почты в соответствующее поле, затем нажмите **ДАЛЕЕ**

   Bitdefender должен проверить эту учетную запись до отображения личной информации. Поэтому на указанный адрес электронной почты отправляется электронное письмо с кодом проверки.
5. Проверьте Ваш почтовый ящик и введите полученный код в области **Конфиденциальность аккаунта** Вашего приложения. Если Вы не можете найти письмо с подтверждением в папке «Входящие», проверьте папку «Спам».

   Отображается статус конфиденциальности проверенной учетной записи.

В случае обнаружения утечек в любом из Ваших аккаунтов, рекомендуем сменить пароль как можно скорее. Чтобы создать надежный и безопасный пароль, примите во внимание следующие советы:

- Сделайте его не менее восьми символов.
- Включите символы нижнего и верхнего регистра.
- Добавьте хотя бы одно число или символ, например, #, @,% или !.

22. ИНТЕРНЕТ-ЗАЩИТА

Веб-защита проверяет с помощью Bitdefender веб-страницы облачных сервисов с браузером Android по умолчанию, Google Chrome, Firefox, Opera, Opera Mini и Dolphin. Полный список поддерживаемых браузеров доступен в разделе Безопасные сети.

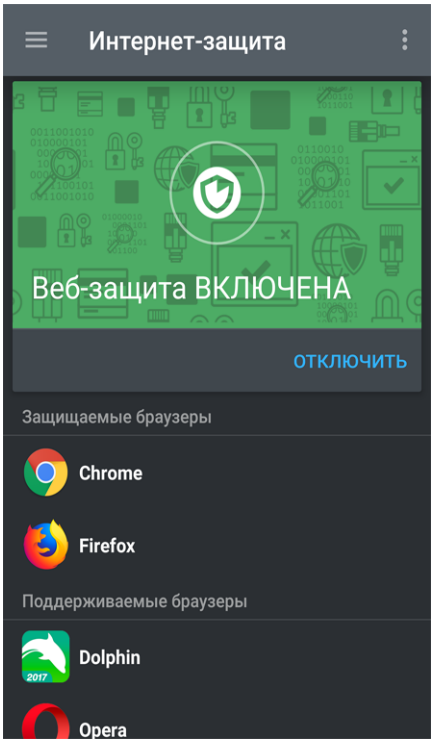
Если Ссылка указывает на мошеннический или фишинг сайт, или на вредоносный контент, например программы-шпионы или вирусы, веб-страница будет временно заблокирована и показано оповещение.

Вы можете выбрать действия для выполнения - игнорировать предупреждение и продолжить, либо вернутся на безопасную страницу.

Замечание

Дополнительные разрешения требуются на Android 6 для функции Web-Защиты.

Разрешите регистрацию как службы доступности и нажмите **Включить** при запросе. Нажмите **Антивирус**, включите переключатель, а затем подтвердите, что вы согласны с доступом к разрешениям вашего устройства.



Интернет-защита

23. VPN

С Bitdefender VPN Вы можете держать в безопасности Ваши личные данные каждый раз во время подключения к небезопасным беспроводным сетям, находясь в аэропортах, торговых центрах, кафе или отелях. Таким образом можно избежать определенные неприятные ситуации, например, кража личных данных или попытки хакеров открыть доступ IP-адреса Вашего устройства.

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.

Замечание

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.

Существует два способа включения и выключения Bitdefender VPN:

- Нажмите кнопку включения питания на карте VPN на панели управления.

  Отображается состояние Bitdefender VPN.

- Нажмите кнопку **Меню** и выберите **VPN** из списка.

  Нажмите **ПОДКЛЮЧИТЬ** каждый раз, если хотите оставаться защищенным во время подключения к незащищенным беспроводным сетям.

  Нажмите **ОТКЛЮЧИТЬ**, если хотите отключить соединение.

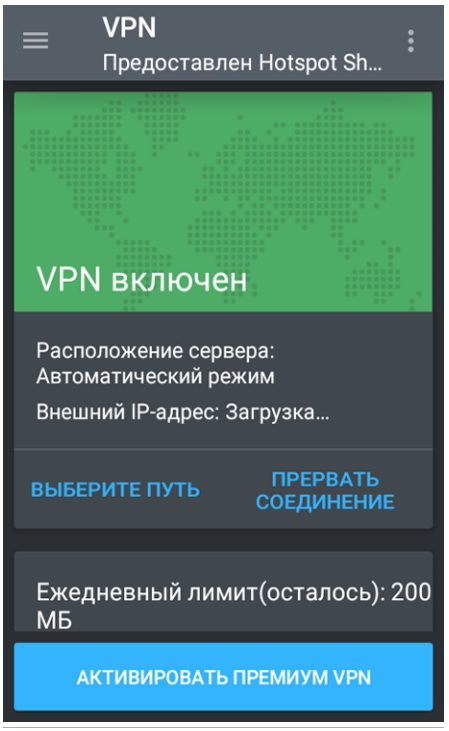
Замечание

При первом включении VPN Вы получите запрос на разрешение Bitdefender настроить VPN-соединение, контролирующее сетевой трафик. Нажмите **OK** для продолжения.

Значок появляется в строке состояния, если Bitdefender VPN активен.

Для экономии заряда батареи, рекомендуем отключить функцию VPN, если она Вам не нужна.

Если у Вас есть премиум-подписка и Вы хотите подключиться к серверу по своему желанию, нажмите **ВЫБРАТЬ МЕСТОПОЛОЖЕНИЕ** в функции VPN, затем выберите нужное местоположение. Дополнительные сведения о VPN подписках см. в «Подписки» (p. 300).



VPN

Нажмите **ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ** на карте VPN из панели мониторинга для получения доступа к функции, в которой можно:

- Просмотреть объем трафика, оставшегося из ежедневной квоты или обновить до версии премиум-класса - информация доступна в бесплатной версии VPN.
- Выбрать сервер, к которому хотите подключиться и посмотреть оставшееся время текущей подписки - информация доступна в версии Премиум VPN.

Настройки VPN

Нажмите кнопку  в меню функций VPN, затем выберите **Настройки** для дополнительной настройки VPN.

В VPN **Настройки** можно настроить следующие параметры:

- Быстрый доступ к VPN-уведомлению - в строке состояния появится уведомление, позволяющее быстро включить VPN.
- Уведомление при подключении к открытому WiFi - каждый раз при подключении к открытой сети Wi-Fi, Вы будете получать уведомления в строке состояния для использования VPN.
- Уведомление при доступе к банковскому сайту - каждый раз во время доступа к банковскому сайту, Вы будете получать уведомление в строке состояния об использовании VPN.

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 до версии Bitdefender Premium VPN в любое время, нажав кнопку **Включить Премиум VPN**, доступную на панели инструментов или в окне VPN.

Подписка Bitdefender Premium VPN не зависит от подписки Bitdefender Mobile Security & Antivirus, это значит,что Вы можете пользоваться ее возможностями, независимо от Вашей антивирусной подписки. Если истекает срок действия подписки Bitdefender Premium VPN при активной Bitdefender Mobile Security & Antivirus, Вы вернетесь к бесплатной версии.

24. АНТИ-ВОР ХАРАКТЕРИСТИКИ

Bitdefender может помочь вам найти ваше устройство и предотвратить утечку личных данных.

Все, что вам нужно сделать, это активировать Анти-Вор на вашем устройстве и, при необходимости, зайти в **Bitdefender Central** с любого веб-браузера, из любого места.

Даже если у вас нет доступа к сети Интернет, вы можете защитить ваше устройство путем отправления **СМС команд** с любого телефона на ваш смартфон в виде текстовых сообщений.

Bitdefender Mobile Security & Antivirus предлагает следующие функции Анти-Вор:

Удаленное Местонахождение

Посмотреть текущее местоположение вашего устройства на картах Google. Местонахождение актуализируется каждые 5 секунд, так что вы сможете отследить все передвижения.

Точность расположения зависит от того, как Bitdefender определяет его:

- Если на устройстве включен GPS, местоположение устройства можно отследить с точностью до нескольких метров, пока оно находится в радиусе действия спутников GPS (т.е. не внутри здания).
- Если устройство в помещении, его местонахождение может быть определено с точностью до десятков метров, при условии, что включена функция Wi-Fi и есть доступные беспроводные сети в радиусе действия.
- Иначе, местонахождение будет определяться с использованием данных сети мобильной связи, которые могут предложить точность до нескольких сот метров.

Показать IP

Отображение последнего IP-адреса для выбранного устройства. Нажмите **SHOW IP**, чтобы сделать его видимым.

Удаленное стирание

Удаление всей персональной информации с утерянного устройства.

Удаленная блокировка

Блокировка экрана вашего устройства и установка цифрового PIN кода для его разблокировки.

Тревожное оповещение (Сигнал)

Дистанционная отправка сообщения, которое будет отображаться на экране устройства или подача громкого звукового сигнала динамиками устройства.

При утере вашего устройства, вы можете дать информацию для возвращения устройства нашедшим, показывая сообщение на экране устройства.

Если вы не можете найти устройство и есть шанс, что оно находится не далеко от вас (например, где-то около дома или в офисе), что может быть лучше для его поисков, чем громкий звуковой сигнал? Звук будет воспроизведен даже если устройство в беззвучном режиме.

Активация Анти-Вор

Чтобы включить функции Анти-Вора, просто завершите процесс настройки Анти-Вор в плитке панели управления.

В качестве альтернативы, вы можете активировать Анти-Вор выполнив следующие действия:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Анти-вор** из списка.
3. Нажмите **Включить**.
4. Начнется следующая процедура, чтобы помочь вам активировать эту функцию:

Замечание

Дополнительные разрешения требуются на Android 6 для функции скрытого фото. Чтобы включить ее, выполните следующие действия:

- Нажмите **Активировать Анти-Вор**, а затем нажмите **Включить**.
- Дайте разрешения для следующих действий:
  a. Разрешить **Антивирус** отправлять и смотреть сообщения SMS?
  b. Разрешить **Антивирус** доступ к местоположению устройства?

c. Разрешить **Антивирус** доступ к вашим контактам?

a. **Предоставить Антивирусу права администратора**

Роль администратора важна для правильной работы модуля Анти-Вор и, следовательно, должна быть предоставлена для продолжения.

b. **Установка PIN-кода приложений**

Чтобы убедиться, что любые изменения, внесенные в настройки Анти-Вор, проделаны вами, должен быть установлен ПИН-код. При попытке изменить настройки Анти-Вор, для принятия изменений потребуется введение PIN кода. Кроме того, на устройствах, поддерживающих проверку подлинности отпечатков пальцев, вместо настроенного PIN-кода можно использовать подтверждение по отпечаткам пальцев.

Замечание
Такой же PIN используется Мастером блокировки приложений для защиты ваших установленных приложений.

c. **Активировать Быстрое фото**

Если кто-то попытается получить доступ к Вашим приложениям, опция Snap Photo, Bitdefender сделает снимок экрана. Для более подробной информации об этой функции, пожалуйста, обратитесь «Сделать фото» (p. 311).

d. **Введите доверенный номер для Анти-Вора**

Выберите вкладку **СМС КОНТРОЛЬ**, введите или выберите из списка контактов надежный номер телефона, затем нажмите **СОХРАНИТЬ НОМЕР**. Надежный номер должен содержать код страны и может являться как номером телефона кого-либо так и Вашим другим номером телефона.

При замене SIM карты в устройстве, Bitdefender Mobile Security & Antivirus автоматически посылает текстовое сообщение на доверенный номер, сообщая новый номер телефона утройства.

Таким образом, вы можете посылать СМС команды на ваш телефон, даже если SIM карта изменена и ее номер меняется.

Важно
Это не обязательный шаг, но рекомендуем установить доверенный номер во время первоначальной настройки. Команда Стереть работает только при отправке с доверенного номера.

Как только Анти-Вор функция активирована, Вы можете включить или выключить Веб и СМС Контроль по отдельности с экрана Анти-Вор, нажав соответствующие кнопки.

Использование функций Анти-Вор из Bitdefender Central (Веб-Защита)

Замечание
Все функции модуля Анти-Вор требуют, чтобы опция **Фоновые данные** была включена в настройках использования данных вашего устройства.

Чтобы получить доступ к функции Анти-Вор из вашей учетной записи Bitdefender:

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
3. В окне **Мои устройства** выберите требуемое устройство.
4. Выберите вкладку **Анти-Вор**.
5. В нижнем части окна нажмите иконку , а затем кнопку соответствующую нужной функции:

   Местоположение - посмотреть местоположение вашего устройства на Google Maps.

   Внимание - введите сообщение для отображения на экране вашего устройства и/или воспроизведения звукового сигнала тревоги устройством.

   Заблокировать> - заблокируйте ваше устройство и установите PIN код для его разблокировки.

   Удалить - удалить все данные с вашего устройства.

Важно
После очистки устройства все возможности Анти-Вора перестанут функционировать.

Показать IP - отображает последний IP-адрес выбранного устройства.

Использование функций Анти-Вор СМС командами (СМС Контроль)

После включения функции СМС команд, вы можете отправить следующие команды на ваш смартфон путем СМС с другого мобильного телефона:

- **LOCATE** - послать сообщение, содержащее местоположение устройства на номер, с которого была подана команда. Сообщение содержит ссылку на Google Maps, которая может быть открыта в браузере мобильного телефона.
- **SCREAM** - издать громкий сигнал на динамиках устройства.
- **LOCK** - заблокировать экран устройства с установленным PIN-кодом.
- **WIPE** - удалить всю информацию с устройства.

Важно
Команда Стереть работает только при отправке с доверенного номера.

- **CALLME** - набор телефонного номера, с которого была подана команда с включенным динамиком. Таким образом, вы сможете услышать у кого находится ваш телефон.
- **HELP** - отправить сообщение, содержащее все доступные команды на номер, с которого была подана команда.
- **SIM Change** - на установленный Вами надежный номер придет СМС с новым номером телефона после того, как только ваша СИМ-карта будет заменена новой. Чтобы настроить номер телефона Вашего друга, нажмите опцию **Надежный номер** . Введите его номер, включая код страны, или выберите его карточку из списка контактов.

Все SMS команды должны быть отправлены, используя следующий формат:

bd-<PIN код> <команда>

Замечание

Скобки обозначают переменные и не должны появляться в команде.

Например, если вы установили PIN код безопасности 123456 и вы хотите получить сообщение с местонахождением вашего телефона, отправьте следующее текстовое сообщение на свой номер телефона:

BD-123456 Установить местоположение

25. БЛОКИРОВКА ПРИЛОЖЕНИЙ

Установленные приложения, такие как электронные письма, фотографии или сообщения, могут содержать личные данные, к которым Вы хотели бы выборочно закрыть доступ.

Мастер блокировки приложений поможет блокировать нежелательный доступ к приложениям, установив PIN код для доступа. PIN код, который вы устанавливаете должен содержать минимум 4 символа (не больше 8) и потребуется каждый раз, когда вы хотите получить доступ к выбранному защищенному приложению.

Кроме того, на устройствах, поддерживающих проверку подлинности отпечатков пальцев, вместо настроенного PIN-кода можно использовать подтверждение по отпечаткам пальцев.

Активация Мастера блокировки приложений

Чтобы ограничить доступ к выбранным приложениям, настройте Блокировку приложений в плитке отображенной в панели управления после активации Анти-Вор.

В качестве альтернативы, вы можете активировать Блокировку приложений выполнив следующие действия:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Блокировка приложений** из списка.
3. Нажмите **Включить**, затем разрешите доступ к данным об использовании для Bitdefender, установив соответствующий флажок.

   Замечание
   Дополнительные разрешения требуются на Android 6 для функции скрытого фото.
   Чтобы включить ее, разрешите **Антивирус** снимать фотографии и записывать видео.

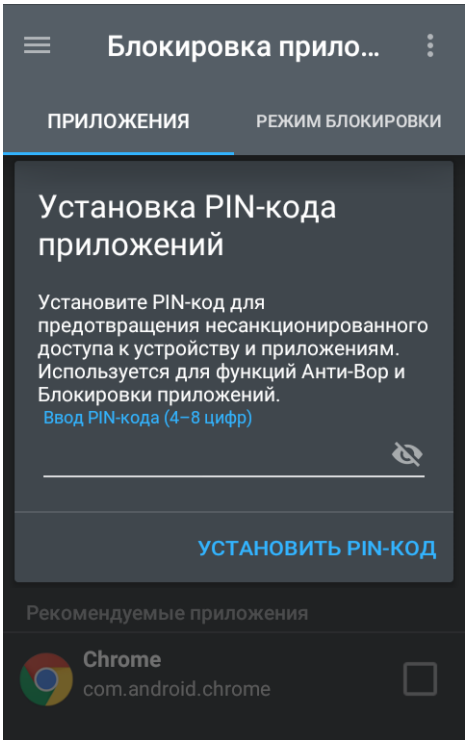
4. Вернитесь в приложение, настройте код доступа и нажмите **Установить PIN код**.

Замечание
Этот шаг доступен, только если вы ранее не настраивали PIN-код в Анти-Вор.

5. Включите опцию Быстрое фото, чтобы поймать любого злоумышленника, который попытается получить доступ к Вашим личным данным.
6. Выберите приложение, которое вы хотите защитить.

Используя неправильный PIN-код или отпечаток пальца пять раз подряд, активируется 30-секундный тайм-аут. Таким образом, любая попытка взлома защищенных приложений будет заблокирована.

Замечание
Такой же PIN код используется функцией Анти-Вор для местонахождения вашего устройства.



Блокировка приложений

Режим блокировки

Здесь можете выбрать, когда функция блокировки приложений должна защищать приложения, установленные на Вашем устройстве.

Вы можете выбрать один из следующих параметров:

- **Блокировать каждый раз** - PIN-код или отпечаток пальца, который Вы настроили, нужно будет использовать каждый раз для доступа к заблокированным приложениям.
- **Разблокировка до закрытия экрана** - доступ к Вашим приложениям будет действителен до тех пор, пока экран не отключится.
- **Разрешить быстрый выход** - Вы можете выйти и снова открыть разблокированные приложения в течение 30 секунд.

- **Активировать интеллектуальную разблокировку** - при включении и подключении к сети, установленной как надежная, другие настройки недоступны. Это означает, что при доступе к заблокированным приложениям не требуется подтверждение PIN-кода или отпечатка пальца.

Настройка Блокировки приложений

Нажмите кнопку  в меню функций Блокировка приложений, затем выберите **Настройки** для дополнительных настроек вашего Мастера блокировки приложений (Блокировка приложений).

В **Настройках** Мастера блокировки приложений вы можете сделать следующее:

- Активируйте Быстрое фото (Snap photo), если использованы три неудачные попытки разблокировки.
- Блокировка уведомлений о новых установленных приложениях.
- Смена вашего PIN кода.

Сделать фото

С Bitdefender Быстрое фото можно застать друзей или родственников в врасплох. Таким образом вы можете проучить любопытных, чтобы они не лазили по вашим личным файлам или приложениям, которые вы используете.

Эта функция работает просто: каждый раз, когда PIN-код или подтверждение отпечатка пальца, установленное для защиты ваших приложений, будут введены неверно три раза подряд, будет сделано фото используя, переднюю камеру устройства. Фотография сохраняется вместе с меткой о времени и причиной срабатывания, ее можно будет увидеть, когда Вы откроете Bitdefender Mobile Security & Antivirus и перейдете к функции Блокировка приложений.

Замечание

Эта функция доступна только для телефонов, имеющих переднюю (фронтальную) камеру.

Чтобы настроить функцию быстрое фото:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Блокировка приложений** из списка.
3. Нажмите  кнопку в меню функции Блокировка приложений и затем выберите **Настройки**.
4. Включите **Snap фото, когда сделано 3 неправильных попытки разблокировки** .

Фото будет сделано при вводе неправильного PIN-кода и будет отображаться в меню Блокировки приложений, которое можно просмотреть в полноэкранном режиме.

В качестве альтернативы, они могут быть просмотрены в вашей учетной записи Bitdefender:

1. Перейти к: https://central.bitdefender.com.
2. Войдите в свой аккаунт.
3. Нажмите значок  в верхнем левом углу экрана, затем выберите **Мои устройства**.
4. Выберите устройство из окна **Мои девайсы**, затем вкладку **Анти-Вор**.

   Будут отображены фото.

Будут сохранены только 3 последние фотографии.

Автоматическая разблокировка

Простым способом остановить работу функции Блокировка приложений о вводе ПИН-кода или подтверждения отпечатка пальца каждый раз когда вы обращаетесь к защищенным приложениям является активация Умная разблокировка.

С помощью Умная разблокировка Вы можете установить доверенные сети WiFi, которые обычно используете и при подключении к ним, функция блокировки для защищенных приложений будет отключена.

Чтобы активировать функцию Умная разблокировка:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Блокировка приложений** из списка.
3. Выберите вкладку **РЕЖИМ БЛОКИРОВКИ**, а затем нажмите на соответствующий переключатель.

Отображается беспроводная сеть, к которой Вы подключены.

Чтобы установить соединение WiFi, которое Вы сейчас используете,как надежное, нажмите значок  .

Замечание

Этот параметр доступен, только если функция Умная разблокировкавключена.

Всякий раз, когда вы измените свое мнение, отключите функцию и WiFi сети, которые вы установили в качестве доверенных будут рассматриваться как ненадежные.

26. ОЦЕНКА БЕЗОПАСНОСТИ

Советник Приватности опирается на информацию отчетов из облака и постоянно предлагает актуальную информацию о ваших Android приложениях.

Большинство приложений являются легальными, но есть также приложения, которые могут отслеживать ваше местоположение, получать доступ и передавать Вашу личную информацию. Советник Приватности предоставляет факты, но решение об использовании приложения принимаете Вы.

Используйте Советник Приватности для получения подробной информации о приложениях, которые:

- получают доступ к контактам вашей адресной книги и загружают данные в свое облако
- могут узнать ваши личные данные
- могут быть небрежными, посылая ваш пароль через Интернет и подвергая риску данные ваших аккаунтов
- могут использовать и загружать Уникальный идентификатор вашего устройства для анализа ваших активностей
- собирать аналитику для определения ваших активностей
- отслеживать ваше местонахождение
- показывать рекламные объявления
- могут стоить вам денег

Нажмите на значок фильтра для просмотра списка важнейшей информации.

Следующая информация доступна в этом списке:

- какие приложения являются вирусами
- какие приложения могут отправлять ваши идентификационные данные незнакомым людям
- какие приложения используют очень назойливую рекламу
- какие приложения могут отправлять ваши личные данные незнакомым людям

- какие приложения могут стоить вам денег
- какие приложения могут отправлять незашифрованные данные
- какие приложения отслеживают ваше местонахождение
- какие приложения имеют доступ к уязвимым данным

Оценка Безопасности

Вычислив Оценку Безопасности для каждого пользователя, Советник Приватности обеспечивает точный обзор уязвимостей, так что вы можете оценить и принять надлежащие меры для каждого установленного приложения. Следует принять меры, если оценка безопасности низкая.

Если вы сомневаетесь в разрешениях, требуемых конкретным приложением, попробуйте найти более подробную информацию о нем, прежде чем принять решение об использовании.

27. ОТЧЕТЫ

Отчеты содержат подробный журнал событий, касающихся активности сканирования вашего устройства.

Всякий раз, когда происходит что-то относящееся к безопасности вашего устройства, в Отчеты поступает новое сообщение.

Для доступа к разделу Отчеты:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Отчеты** из списка.

В окне Отчеты доступны следующие вкладки:

- **ЕЖЕНЕДЕЛЬНЫЕ ОТЧЕТЫ** - здесь доступ к просмотру информации о состоянии безопасности и о выполненных задач за текущую и предыдущую недели. Отчет текущей недели генерируется каждое воскресенье и вы получите уведомление, информирующее о том, что отчет доступен.

  Каждую неделю в этом разделе будет отображаться новая подсказка, поэтому регулярно проверяйте данный раздел, чтобы получить лучшее от приложения.

- **ЖУРНАЛ АКТИВНОСТИ** - здесь можно просмотреть подробную информацию о работе Bitdefender Mobile Security & Antivirus приложения с тех пор, когда он был установлен на Вашем Android-устройстве.

  Для удаления доступного журнала действий, нажмите  кнопку в верхнем правом углу экрана, а затем выберите очистить журнал активности **Очистить журнал активности**.

28. WEARON

С Bitdefender WearON ы можете легко найти свой смартфон, дед бы вы его не оставили - в конференц-зале офиса или под подушкой на диване. Устройство может быть найдено, даже если активирован беззвучный режим.

Держите эту функцию включенной, чтобы убедиться, что ваш смартфон у вас всегда под рукой.

Замечание
Функция работает с Android 4.3 и Android Wear.

Активация WearON

Для использования WearON, вам следует только подключить смарт-часы к приложению Bitdefender Mobile Security & Antivirus и активировать функцию с помощью следующей голосовой команды:

Start:<Where is my phone>

Bitdefender WearON есть две команды:

1. **Телефонный сигнал**

   С функцией Телефонный сигнал вы сможете быстро найти ваш смартфон всякий раз, когда вы отходите слишком далеко от него.

   Если ваши смарт часы с вами, они автоматически распознают приложение на вашем телефоне и завибрируют, если вы в более чем десяти метрах от вашего устройства.

   Для включения этой функции, откройте Bitdefender Mobile Security & Antivirus, выберите **Global Settings** в меню и выберите соответствующий переключатель в секции WearON.

2. **Сигнал тревоги**

   Поиск телефон никогда не было так легок. Всякий раз, когда вы забыли, где вы оставили свой телефон, используйте команду Сигнал на часах, чтобы ваш телефон подал сигнал.

29. BITDEFENDER CENTRAL

Bitdefender Central это веб-платформа, на которой у Вы имеете доступ к онлайн-функциям и услугам, а также можете удаленно выполнять важные задачи на устройствах, на которых установлен Bitdefender. Вы можете войти в учетную запись Bitdefender с любого компьютера или мобильного устройства, подключенного к сети Интернет, перейдя https://central.bitdefender.com. Если у вас есть доступ к нему, вы можете начать делать следующее:

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

Войдите в вашу учетную запись Bitdefender

Чтобы войти в учетную запись Bitdefender:

1. Откройте веб-браузер на любом устройстве с доступом в Интернет.
2. Перейти к: https://central.bitdefender.com.
3. Войдите в свой аккаунт, используя адрес электронной почты и пароль.

Мои устройства

Раздел **Мои устройства** в вашей учетной записи Bitdefender дает возможность устанавливать, управлять и осуществлять удаленные действия на любом устройстве, на котором установлен Bitdefender,при условии, что оно включен и подключено к Интернету. Карточки устройства отображают имя устройства, состояние защиты и риски безопасности, влияющие на защиту устройств.

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

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
3. Нажмите на желаемую карту устройства, затем значок в правом верхнем углу экрана.
4. Выберите **Настройки**.
5. Введите новое имя в поле **Имя устройства**, затем выберите **Сохранить**.

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

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
3. Нажмите на желаемую карту 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 **Присвоить**.

Для получения дополнительных возможностей удаленного управления и информации о вашем продукте Bitdefender на определенном устройстве, выберите нужную карту устройства.

После того, как вы выберете карту 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. Если возникнут проблемы, влияющие на устройство, нажмите стрелку раскрывающегося списка в верхней области состояния для получения подробной информации. Здесь можно вручную исправить проблемы, влияющие на безопасность устройств.

- **Защита**. Из этого окна вы можете удаленно запустить сканирование на вашем устройстве. Нажмите кнопку **SCAN**, чтобы начать процесс. Вы также можете проверить, когда на устройствах выполнялось последнее сканирование и просмотреть отчет последней проверки с наиболее важной информацией.
- **Anti-Theft** (Анти-вор). В случае, если вы потеряли устройство с включенной функцией Анти-Вор, вы можете найти его и удаленно выполнить определенные действия. Нажмите **LOCATE**, чтобы выяснить местоположение устройства. Последнее известное местоположение будет отображаться вместе с датой и временем. Для более подробной информации об этой функции, пожалуйста, обратитесь «*Анти-Вор Характеристики*» (p. 302).

Мои подписки

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

Проверка доступных подписок

Проверка доступных подписок:

1. Войдите в ваш Bitdefender Central.
2. Нажмите на иконку  в верхнем левом углу экрана, а затем выберите **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.

Добавить новое устройство

Если ваша подписка включает более одного устройства, вы можете добавить новое устройство и установить Bitdefender Mobile Security & Antivirus на нем, как описано в «Установка Bitdefender Mobile Security & Antivirus» (p. 286).

Продлить подписку

Если осталось менее 30 дней вашей подписки и вы отключили автоматическое продление, вы можете проделать это вручную, выполнив следующие действия:

1. Войдите в ваш Bitdefender Central.
2. Нажмите на иконку в верхнем левом углу экрана, а затем выберите **Мои подписки**.
3. Выбрать нужную карточку подписки.
4. Нажмите **ОБНОВЛЕНИЕ** чтобы продолжить.

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

30. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

Почему Bitdefender Mobile Security & Antivirus требует подключение к сети Интернет?

Приложение должно взаимодействовать с серверами Bitdefender, чтобы определять состояние безопасности приложений, которые он сканирует, и веб-страниц, которые вы посещаете, а также для получения команд из учетной записи Bitdefender, при использовании функции Анти-Вор.

Какие разрешения Bitdefender Mobile Security & Antivirus потребует?

- Доступ в Интернет -> используется для связи с облаком.
- Оценка статуса телефона и его идентификации -> используется для защиты устройства при подключении к Интернету и для получения информации, необходимой для создания уникального ID для связи с Bitdefender облаком.
- Чтение и запись закладок браузера -> модуль Интернет Защиты удаляет вредоносные сайты из истории посещенных страниц.
- Чтение данных журнала -> Bitdefender Mobile Security & Antivirus обнаруживает следы вредоносных программ в журналах Android.
- Чтение / написание СМС, контакты, данные аккаунта и внешнего хранилища -> Требуется для удаленного стирания данных.
- Местонахождение -> Требуется для удаленного местоположения.
- Требуется камера -> для получения фото.
- Используется хранилище ->, чтобы позволить антивредоносному сканеру проверять SD-карты.

Где я могу увидеть подробную информацию о деятельности приложения?

Bitdefender Mobile Security & Antivirus ведет журнал всех важных действий, изменений статусов и других важных действий. Чтобы получить доступ к этой информации откройте Bitdefender Mobile Security & Antivirus и нажмите кнопку **Menu**, а затем выберите **Reports** из списка.

Я забыл PIN код, который установил для защиты приложения. Что мне делать?

1. Войдите в ваш Bitdefender Central.

2. Нажмите значок в верхнем левом углу экрана, затем выберите **Мои устройства**.
3. Нажмите на желаемую карту устройства, затем значок в правом верхнем углу экрана.
4. Выберите **Настройки**.
5. Восстановить ПИН-код из области **PIN код приложения**.

Как Bitdefender Mobile Security & Antivirus повлияет на производительность моего устройства и работу батареи?

Мы постоянно следим, чтобы влияние было очень низким. Приложение работает только тогда, когда это необходимо - после установки приложения, при просмотре интерфейса приложения или если вы хотите провести проверку безопасности. Bitdefender Mobile Security & Antivirus прекращает работу, когда вы звоните своим приятелям, вводите сообщение или играете.

Как отключить функцию блокировки приложения?

Опция блокировки приложения не отключена, но Вы можете легко отключить ее, сняв флажки рядом с выбранными приложениями после проверки установленного Вами PIN-кода или отпечатка пальца.

Как установить другую беспроводную сеть как надежную?

Если хотите установить другую беспроводную сеть как надежную:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Блокировка приложений** из списка.
3. Выберите вкладку **РЕЖИМ БЛОКИРОВКИ** и затем значок.
4. Укажите Ваш PIN-код или отпечаток пальца для подтверждения Вашего выбора.
5. Нажмите значок рядом с сетью, которую хотите установить в качестве надежной.

Что Советник Безопасности расскажет о приложениях, устанавливаемых мной?

Советник Приватности сообщает о возможных действиях приложения на устройстве. Сообщит, если приложение может получить доступ к

личным данным, отправлять сообщения, подключаться к Интернету или выполнять любую другую функцию, которая может представлять угрозу для вашей безопасности.

Могу ли я удалить приложение, которое я считаю угрозой для моей личной информации?

Вы можете вручную удалить приложение, используя Советник Приватности. Для этого выберите нужное приложение, а затем нажмите кнопку **Удалить приложение**. Подтвердите свой выбор и дождитесь окончания процесса удаления.

Как отключить уведомления Советника Приватности?

Если вы хотите прекратить получение уведомлений от Советника Приватности:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Настройки** из списка.
3. Под разделом **Советник Приватности**, нажмите на соответствующий переключатель.

Как я могу остановить несанкционированный просмотр фотографий, сделанных на моих устройствах?

Для того, чтобы установить видимость фотографий, сделанных на устройствах:

1. Войдите в ваш Bitdefender Central.
2. Нажмите значок в верхней правой части экрана.
3. Нажмите **Моя учетная запись** в слайд-меню.
4. Щелкните на вкладке **Настройки**.
5. Отключите опцию **Показывать/не показывать снимки фотографий на ваших устройствах**

Как сохранить в безопасности интернет-магазины?

Интернет-магазин может быть небезопасным, если пренебрегать некоторыми деталями. Чтобы не стать жертвой мошенничества, рекомендуем следующее:

- Поддерживайте антивирус в актуальном (обновленном) состоянии.
- Проводите онлайн-платежи только с защитой покупателя.

- Используйте VPN при подключении к Интернету из общественных и незащищенных беспроводных сетей.
- Обратите внимание на пароли, назначенные Вашим учетным данным в Интернете. Они должны быть сильными, включая заглавные и строчные буквы, цифры и символы (@,!,%, # И т.д.).
- Убедитесь, информация отправляется через защищенные соединения. Расширение онлайн-сайта должно быть HTTPS://, а не HTTP://.

Когда я должен использовать VPN Bitdefender?

Вы должны быть осторожны при входе, загрузке или загрузке контента в Интернете. В целях обеспечения безопасности во время просмотра веб-страниц, рекомендуем использовать VPN Bitdefender, когда Вы:

- хотите подключиться к общедоступным беспроводным сетям
- хотите получить доступ к контенту, обычно ограниченному в определенных областях, независимо от того, находитесь ли Вы дома или за границей
- хотите сохранить Ваши личные данные были приватными (имена пользователей, пароли, информация о кредитной карте и т. д.)
- хотите скрыть Ваш IP-адрес

Будет ли Bitdefender VPN негативно влиять на срок службы батареи моего устройства?

Bitdefender VPN предназначен для защиты Ваших персональных данных, скрытия Вашего IP-адреса при подключении к незащищенным беспроводным сетям и доступа к ограниченному контенту в некоторых странах. Чтобы избежать ненужного потребления батареи устройством, рекомендуем использовать VPN только в необходимых случаях и отключать в автономном режиме.

Почему я сталкиваюсь со снижением скорости работы интернета при подключении к VPN Bitdefender?

Bitdefender VPN разработан для комфортного веб-серфинга, тем не менее, скорость Вашего подключение к сети или серверу может быть снижена. В таком случае, если нет необходимости в подключении к удаленному серверу, рекомендуем разрешить Bitdefender VPN автоматически находить и подключать устройство к ближайшему для Вашего местонахождения серверу.

Могу ли я изменить учетную запись Bitdefender, связанную с моим устройством?

Да, вы можете легко изменить учетную запись Bitdefender, связанную с вашим устройством, выполнив следующие действия:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Информация об аккаунте** из списка.
3. Нажмите **Выход**, а затем подтвердите свой выбор.
4. Нажмите **Использовать аккаунт Central** и наберите ваш новый адрес электронной почты и пароль Bitdefender.

Что такое Администратор Устройства?

Администратор Устройства - это функция Android, дающая Bitdefender Mobile Security & Antivirus разрешения, необходимые для выполнения определенных задач удаленно. Без этого разрешения, невозможна удаленная блокировка и функция стирания не сможет полностью удалить ваши данные. Если Вы хотите удалить приложение, убедитесь, что сняли разрешения перед попыткой удаления в **Настройки > Безопасность > Выбор администратора устройства**.

Для чего нужен доверенный номер?

Если ваш телефон попадает в руки тех, кто не имеет ни малейшего намерения вернуть его законному владельцу, вполне вероятно, что SIM карта будет быстро заменена. При замене SIM карты в устройстве, Bitdefender Mobile Security & Antivirus автоматически посылает текстовое сообщение на доверенный номер, сообщая новый номер телефона устройства. Таким образом, вы можете посылать СМС команды на ваш телефон, даже если SIM карта изменена и ее номер меняется. Это может быть телефон того, кого вы хорошо знаете и доверяете, или другой номер телефона, который вы используете.

Может ли доверенный номер быть изменен после его установки?

Чтобы установить другой доверенный номер:

1. Открыть Bitdefender Mobile Security & Antivirus.
2. Нажмите кнопку **Меню** и выберите **Настройки** из списка.
3. Под разделом **Анти-Вор** нажмите **Доверенный номер**.

Вам будет предложено ввести PIN код перед подтверждением измененного доверенного номера.

Сколько мне будет стоить отправка CMC команд?

CMC команды отправляются в виде стандартных текстовых сообщений, оплата взимается согласно тарифам вашего оператора сотовой связи. Bitdefender не взимает каких-либо дополнительных сборов.

Как исправить "No Google Token" ошибку, которая возникает при входе в Bitdefender Mobile Security & Antivirus.

Эта ошибка возникает, когда устройство не связано с аккаунтом Google, или устройство связано с учетной записью, но не может подключится к Google. Попробуйте одно их следующих решений:

- Перейдите в настройки Android > Приложения > Управление Приложениями > Bitdefender Mobile Security & Antivirus и нажмите **Очистить данные**. Затем попытайтесь войти снова.
- Убедитесь, что ваше устройство связано с аккаунтом Google.

  Для проверки, перейдите в Настройки > Аккаунты & синхронизируйте и посмотрите, есть ли Google в списке **Управление Аккаунтами**. Добавьте свой аккаунт, если он отсутствует в списке, перезагрузить устройство, а затем попытаться войти в Bitdefender Mobile Security & Antivirus.
- Перезагрузите устройство, затем попытайтесь войти снова.

На каких языках доступен Bitdefender Mobile Security & Antivirus?

Bitdefender Mobile Security & Antivirus в настоящее время доступен на следующих языках:

- Бразильский
- Голландский
- русский
- Французский
- Немецкий
- Греческий
- Итальянский
- Японский
- Корейский
- Польский
- Португальский

- Румынский
- Русский
- Испанский
- Тайский
- Турецкий
- Вьетнамский

Другие языки будут добавлены в будущих версиях. Для смены языка интерфейса Bitdefender Mobile Security & Antivirus, перейдите в настройки устройства **Язык & клавиатуры** и установите язык для устройства, который вы хотите использовать.

СВЯЖИТЕСЬ С НАМИ

31. ОБРАЩЕНИЕ ЗА ПОМОЩЬЮ

Bitdefender предоставляет своим потребителям быструю и надежную поддержу, 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. 200) 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 через интерфейс Bitdefender» (p. 330)
- «Свяжитесь с нами через онлайн-центр поддержки» (p. 331)

Свяжитесь с нами через интерфейс Bitdefender

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

Следуйте инструкции:

1. Нажмите на  иконку в нижнем левом углу Bitdefender interface.
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.
   - **Обратиться в службу поддержки**

     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. Продолжите выполнение последующих шагов.

   Подождите несколько минут, пока Bitdefender выполнит сбор сведений о продукте. Эта информация поможет нашим техническим специалистам найти эффективное решение вашей 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 **ОТПРАВИТЬ ЗАПРОС**.

   Подождите несколько минут, пока ваш запрос будет создан, и собранная информация будет отправлена в Отдел обслуживания клиентов Bitdefender.

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.

32. 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.

32.1. 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 по предотвращению заражения вирусами, управлению решениями Bitdefender с подробными разъяснениями, а также другая информация.

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

Центр поддержки Bitdefender доступен круглосуточно по адресу

https://www.bitdefender.com/support/consumer.html.

32.2. Форум техподдержки Bitdefender

Форум техподдержки Bitdefender предоставляет пользователям Bitdefender простой способ не только получить необходимую помощь, но и помочь другим.

В случае некорректной работы продукта Bitdefender (продукт не может удалить отдельные вирусы с компьютера) или возникновения вопросов относительно работы продукта вы можете опубликовать описание проблемы или свой вопрос на форуме.

Специалисты Службы технической поддержки Bitdefender отслеживают новые сообщения на форуме, что позволяет своевременно реагировать на все вопросы пользователей. На форуме также есть возможность получить ответ или узнать о способах решения проблемы от более опытных пользователей Bitdefender.

Перед публикацией своего сообщения о проблеме или вопроса, выполните поиск похожих или связанных тем 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.

32.3. 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 вирусах, текущих тенденциях развития систем безопасности и других событиях в отрасли компьютерной безопасности регулярно публикуются новые статьи.

Веб-страница HOTforSecurity: https://www.hotforsecurity.com.

33. 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.

33.1. 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 вирусов: virus_submission@bitdefender.com
Отправка спама: spam_submission@bitdefender.com
Жалобы: abuse@bitdefender.com
Сайт:http://www.bitdefender.ru

33.2. 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. Указывайте адрес электронной почты на английском языке, чтобы мы смогли своевременно обработать ваш вопрос.

33.3. 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
Сайт: https://www.bitdefender.es

Румыния

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
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
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

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.

E-mail

Электронная почта. Сервис, отправляющий сообщения на другие компьютеры через локальную или глобальную сеть.

IP-адрес

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

Photon

Технология Photon является инновационным решением Bitdefender, разработанным для того, чтобы свести к минимуму влияние на производительность антивирусной защиты. 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.

Браузер

Веб-браузер – приложение, которое находит и выводит на экран веб-страницы. 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.

Вирус

Программа или часть кода, которая загружается в ваш компьютер без вашего ведома и запускается без вашего участия. Многие вирусы также могут копировать себя. Все компьютерные вирусы создаются людьми. Очень легко написать простой вирус, который копирует себя снова и снова. Даже такой простой вирус очень опасен, так как он быстро использует всю свободную память и система зависает. Более опасные вирусы могут передавать себя по сети и прорываться через системы защиты.

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

Вирус, заражающий загрузочный сектор жесткого или гибкого диска. Попытка загрузиться с зараженной дискеты приводит к тому, что вирус активизируется в памяти. Каждый раз, когда вы загружаете систему с этого места, вирус 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)

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

Клавиатурные шпионы по сути не являются вредоносным ПО. Их можно использовать в законных целях, например для контроля за действиями сотрудников или детей. Однако все чаще они используются кибер-мошенниками 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

Компьютерный вирус, 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 проверки основан на использовании определенных сигнатур вирусов. Основное преимущество этого метода состоит в том, что его нельзя обмануть похожей на вирус программой, а, следовательно, не возникает ложное срабатывание.

Область уведомлений (System tray)

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.

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 программы 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

Вирус, изменяющий свою форму всякий раз, заражая новый файл. Поскольку у таких вирусов нет бинарной закономерности, их трудно обнаружить.

Порт

Компьютерный интерфейс, с помощью которого подключается внешнее устройство. У персональных компьютеров есть несколько видов портов. Внутри корпуса есть несколько портов для подключения дисководов, монитора и клавиатуры. Снаружи есть порты для подключения модемов, принтеров, мыши и других внешних устройств.

В сетях на базе протоколов TCP/IP и UDP, порт – это конечная точка логического подключения. Номер порта указывает на его тип. Например, порт номер 80 используется для HTTP трафика.

Постоянные угрозы повышенной сложности (Advanced persistent threat)

Advanced persistent threat (APT) использует уязвимости систем, чтобы украсть важную информацию для доставки ее к источнику. Большие группы, такие как организации, компании или правительства подвергаются атакам этой вредоносной программы.

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 вируса в сеть - через PDF файл или документ Office, которые выглядят безвредными, так что каждый пользователь может запустить данные файлы.

Почтовый клиент

Приложение, которое позволяет вам 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. Кроме того, программы-шпионы могут собирать информацию об адресах электронной почты, паролях и даже номерах кредитных карточек пользователей.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионов обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионов являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти 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, чаще всего, их используют как вредоносные программы либо для скрытия присутствия в системе. При совмещении с вредоносными программами руткиты представляют серьезную угрозу для целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

Сигнатура вируса

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

События (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. Обычно под спамом понимают незаконную рассылку электронных писем, часто коммерческого содержания.

Сценарий

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

Троян

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от обычных вирусов, вирус класса Троян не копирует себя, однако, он может быть не менее разрушительным. Вирусы трояны одни из наиболее опасных типов, обещающие избавить ваш компьютер от всех вирусов, но, на самом деле, загружают вирусы в 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.

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, сводящееся к отправке пользователю электронного письма якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации о пользователе и ее последующего присвоения в корыстных целях. В получаемом пользователем сообщении по электронной почте его с помощью ссылки приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные (например, пароли и номера банковского счета, кредитной карточки, карточки социального обеспечения). Однако, на самом деле, такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

Червь

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

Эвристический анализ (Heuristic)

Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными сигнатурами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может "обмануть" фильтр. Однако он может принять подозрительный код в обычных программах за вирус и вызвать так называемое «ложное срабатывание».

Элементы запуска

Все файлы, помещенные в эту папку будут открываться при запуске компьютера. Это могут быть, например, экран запуска, звуковой файл, проигрываемый при первом запуске компьютера, ежедневник с напоминаниями или другие приложения. Обычно в эту папку помещается не сам файл, а его ярлык.

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.