

# Bitdefender® ANTIVIRUS PLUS 2018



РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ



## Bitdefender Antivirus Plus 2018 Руководство пользователя

Дата публикации 19.02.2018

Авторские права © 2018 Bitdefender

### Правовое положение

Все права защищены. Никакая часть этой публикации не может быть воспроизведена или передана в любой форме или любыми средствами, электронными или механическими, включая фотокопирование, запись, использование средств хранения и поиска информации, без получения письменного разрешения уполномоченного представителя компании BitDefenderBitdefender. Использование цитат в обзорах разрешается только со ссылкой на цитируемый источник. Запрещено вносить какие-либо изменения в данный материал.

**Предупреждение и ограничение ответственности.** Данный программный продукт и документация к нему защищены авторским правом. Данный программный продукт и документация к нему защищены авторским правом. Информация в этом документе предоставляется «как есть», без гарантии. «» Хотя в ходе подготовки этого документа были приняты все меры предосторожности, авторы не несут никакой ответственности перед любым лицом или организацией в отношении каких-либо потерь или ущерба, причиненных или предположительно вызванных прямо или косвенно информацией, содержащейся в документе.

Данная книга содержит ссылки на сторонние веб-сайты, не находящиеся под контролем Bitdefender, поэтому Bitdefender не несет ответственности за их содержание. Переходя на сторонние сайты, указанные в документе, Вы делаете это на свой страх и риск. Bitdefender приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что Bitdefender берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

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



## Содержание

<b>Установка</b> .....	<b>1</b>
1. Подготовка к установке .....	2
2. Системные требования .....	3
2.1. Минимальные системные требования .....	3
2.2. Рекомендуемые системные требования .....	3
2.3. Требования к программному обеспечению .....	4
3. Установка продукта Bitdefender .....	5
3.1. Установка из Bitdefender Central .....	5
3.2. Установка продукта с установочного диска .....	7
<b>Начало работы</b> .....	<b>13</b>
4. Основы .....	14
4.1. Откройте окно Bitdefender .....	15
4.2. Устранение неисправностей .....	16
4.2.1. Мастер проблем безопасности .....	17
4.2.2. Настройка оповещений о статусе .....	18
4.3. Уведомления .....	18
4.4. Автопилот .....	19
4.5. Профили .....	20
4.5.1. Настройка автоматической активации профилей .....	21
4.6. Защищенные паролем настройки Bitdefender .....	21
4.7. Анонимные отчеты об использовании .....	22
4.8. Уведомления о специальных предложениях .....	23
5. Bitdefender интерфейс .....	24
5.1. Значок системный трей .....	24
5.2. Главное окно .....	26
5.2.1. Область состояния .....	27
5.2.2. Левая боковая панель инструментов .....	28
5.2.3. Кнопки действий и доступ к области функций .....	29
5.2.4. Нижняя панель .....	29
5.3. Разделы Bitdefender .....	30
5.3.1. <b>Защита</b> .....	30
5.3.2. <b>Приватность</b> .....	32
5.4. Виджет Безопасности .....	33
5.4.1. Сканирование файлов и папок .....	34
5.4.2. Показать / скрыть Виджет безопасности .....	34
5.5. Действие .....	35
5.5.1. Проверка Отчета о безопасности .....	37
5.5.2. Включение/отключение уведомлений о состоянии системы безопасности .....	38
6. Bitdefender Central .....	39
6.1. Доступ к Bitdefender Central .....	39



6.2. Мои подписки .....	40
6.2.1. Проверка доступных подписок .....	40
6.2.2. Добавить новое устройство .....	40
6.2.3. Продлить подписку .....	41
6.2.4. Активировать подписку .....	41
6.3. Мои устройства .....	42
6.4. Моя учетная запись .....	44
6.5. Уведомления .....	44
<b>7. Поддержка Bitdefender в обновленном состоянии .....</b>	<b>45</b>
7.1. Проверка обновлений Bitdefender .....	46
7.2. Выполнение обновления .....	46
7.3. Включение и отключение автоматического обновления .....	47
7.4. Настройка параметров обновления .....	47
7.5. Непрерывные обновления .....	49

## **Советы .....** **50**

<b>8. Установка .....</b>	<b>51</b>
8.1. Как установить Bitdefender на второй компьютер? .....	51
8.2. Как переустановить Bitdefender? .....	51
8.3. На каком веб-сайте можно загрузить Bitdefender? .....	53
8.4. Как изменить язык продукта Bitdefender? .....	53
8.5. Как пользоваться лицензионным ключом Bitdefender после обновления Windows? .....	55
8.6. Как перейти к последней версии Bitdefender? .....	58
<b>9. Подписки .....</b>	<b>59</b>
9.1. Как активировать подписку на Bitdefender, используя лицензионный ключ? .....	59
<b>10. Bitdefender Central .....</b>	<b>61</b>
10.1. Как войти в Bitdefender Central используя другую учетную запись? .....	61
10.2. Как отключить справочные сообщения Bitdefender Central? .....	61
10.3. Я забыл пароль, установленный для учетной записи Bitdefender. Как сбросить его? .....	62
10.4. Как управлять сеансами входа в систему, связанными с моей учетной записью Bitdefender? .....	63
<b>11. Сканирование с Bitdefender .....</b>	<b>64</b>
11.1. Как выполнить сканирование файла или папки? .....	64
11.2. Как выполнить сканирование системы? .....	64
11.3. Как составить график сканирования? .....	65
11.4. Как создать пользовательское задание сканирования? .....	65
11.5. Как исключить папку из сканирования? .....	66
11.6. Что делать в случае обнаружения Bitdefender вируса в заведомо надежном файле? .....	67
11.7. Как проверить, какие вирусы обнаружил Bitdefender? .....	68
<b>12. Защита приватности .....</b>	<b>70</b>
12.1. Как убедиться, что моя транзакция в Интернете безопасна? .....	70



12.2. Как удалить файл навсегда с Bitdefender? .....	70
<b>13. Полезная информация .....</b>	<b>71</b>
13.1. Как протестировать антивирусное решение? .....	71
13.2. Как удалить Bitdefender? .....	71
13.3. Как удалить BitdefenderVPN? .....	72
13.4. Как автоматически выключить компьютер после завершения сканирования? .....	73
13.5. Как настроить Bitdefender для использования прокси-сервера при подключении к Интернету? .....	74
13.6. Определение используемой версии Windows (32- или 64-разрядная) .....	75
13.7. Как отобразить скрытые объекты в Windows? .....	76
13.8. Как удалить другие решения безопасности? .....	77
13.9. Как перезагрузить компьютер в безопасном режиме? .....	78

## **Управление безопасностью .....**

<b>14. Антивирусная защита .....</b>	<b>82</b>
14.1. Резидентное сканирование (защита в реальном времени) .....	83
14.1.1. Включение или отключение защиты в реальном времени .....	83
14.1.2. Настройка дополнительных параметров защиты в режиме реального времени .....	84
14.1.3. Восстановление настроек по умолчанию .....	88
14.2. Сканирование по запросу .....	89
14.2.1. Сканирование файла или папки на предмет наличия вредоносных программ .....	89
14.2.2. Запуск быстрого сканирования .....	90
14.2.3. Запуск проверки системы .....	90
14.2.4. Настройка пользовательского сканирования .....	91
14.2.5. Мастер антивирусного сканирования .....	94
14.2.6. Просмотр журналов сканирования .....	98
14.3. Автоматическое сканирование съемных носителей .....	99
14.3.1. Как это работает? .....	99
14.3.2. Управление сканированием съемных носителей .....	101
14.4. Сканирование хост-файлов .....	101
14.5. Настройка исключений сканирования .....	102
14.5.1. Исключение файлов или папок из сканирования .....	102
14.5.2. Исключение расширений файлов из сканирования .....	103
14.5.3. Управление исключениями сканирования .....	104
14.6. Управление файлами в карантине .....	105
<b>15. АКТИВНЫЙ КОНТРОЛЬ УГРОЗ .....</b>	<b>107</b>
15.1. Включение и выключение Активный Контроль Угроз: .....	107
15.2. Проверка обнаруженных вирусов-вымогателей .....	107
15.3. Проверка обнаруженных подозрительных приложений .....	108
15.4. Добавление процессов к исключениям .....	108
<b>16. Веб-защита .....</b>	<b>110</b>
16.1. Уведомления Bitdefender в браузере .....	111
<b>17. Уязвимости .....</b>	<b>113</b>



17.1. Сканирование системы на наличие уязвимостей .....	113
17.2. Использование автоматического мониторинга уязвимостей .....	115
17.3. Советник безопасности Wi-Fi .....	117
17.3.1. Включение/отключение уведомлений Wi-Fi Советника безопасности .....	118
17.3.2. Настройка домашней сети Wi-Fi .....	118
17.3.3. Публичные Wi-Fi .....	119
17.3.4. Проверка информации о сетях Wi-Fi .....	119
<b>18. Безопасные файлы .....</b>	<b>122</b>
18.1. Включение или выключение Безопасных Файлов .....	122
18.2. Защита личных файлов от атак вымогателей .....	123
18.3. Настройка доступа к приложениям .....	124
18.4. Защита при загрузке системы .....	124
<b>19. Защита ваших учетных данных при помощи Менеджер паролей .....</b>	<b>125</b>
19.1. Создание новой базы данных Кошелька .....	126
19.2. Импорт существующей базы данных .....	126
19.3. Экспорт базы данных Wallet .....	127
19.4. Синхронизация ваших Кошельков в облаке .....	127
19.5. Управление учетными данными Кошелька .....	128
19.6. Включение и отключение защиты Менеджера паролей .....	129
19.7. Управление настройками Менеджера паролей .....	129
<b>20. VPN .....</b>	<b>133</b>
20.1. Установка VPN .....	133
20.2. Открытие VPN .....	134
20.3. Интерфейс VPN .....	134
20.4. Подписки .....	135
<b>21. Безопасный платеж - безопасность для онлайн-транзакций .....</b>	<b>136</b>
21.1. Использование Bitdefender Safepay™ .....	137
21.2. Настройка параметров .....	138
21.3. Управление закладками .....	140
<b>22. Защита данных .....</b>	<b>141</b>
22.1. Окончательное удаление файлов .....	141
<b>23. USB иммунизация .....</b>	<b>143</b>
<b>Оптимизация системы .....</b>	<b>144</b>
<b>24. Профили .....</b>	<b>145</b>
24.1. Профиль Работа .....	146
24.2. Профиль Кино .....	147
24.3. Профиль Игры .....	148
24.4. Профиль публичный Wi-Fi .....	149
24.5. Профиль режима батареи .....	150
24.6. Оптимизация в реальном времени .....	151



<b>Неполадки .....</b>	<b>152</b>
<b>25. Решение распространенных проблем .....</b>	<b>153</b>
25.1. Система работает медленно .....	153
25.2. Сканирование не начинается .....	155
25.3. Не удается использовать приложение .....	157
25.4. Что делать, если Bitdefender блокирует безопасный веб-сайт или онлайн приложение .....	158
25.5. Что делать, если Bitdefender определяет безопасное приложение в качестве программы-вымогателя .....	159
25.6. Обновление Bitdefender при низкой скорости подключения к Интернету .....	160
25.7. Службы Bitdefender не отвечают .....	160
25.8. Функция "Автозаполнение" в Кошельке не работает .....	161
25.9. Сбой удаления Bitdefender .....	162
25.10. Моя система не загружается после установки Bitdefender .....	164
<b>26. Удаление вредоносного ПО из системы .....</b>	<b>168</b>
26.1. Bitdefender Режим Восстановления (Rescue Environment в Windows 10) .....	168
26.2. Действия в случае обнаружения Bitdefender вирусов на компьютере ...	173
26.3. Как удалить вирус из архива? .....	174
26.4. Как очистить от вирусов архив электронной почты? .....	175
26.5. Что делать, если имеются подозрения в том, что файл является опасным? .....	177
26.6. Что представляют собой защищенные паролями файлы в журнале сканирования? .....	177
26.7. Поиск пропущенных элементов в журнале сканирования .....	178
26.8. Поиск файлов с избыточным сжатием в журнале сканирования .....	178
26.9. Почему Bitdefender автоматически удалил зараженный файл? .....	178
<b>Свяжитесь с нами .....</b>	<b>179</b>
<b>27. Обращение за помощью .....</b>	<b>180</b>
<b>28. Онлайн-ресурсы .....</b>	<b>183</b>
28.1. Центр поддержки Bitdefender .....	183
28.2. Форум техподдержки Bitdefender .....	184
28.3. Портал HOTforSecurity .....	184
<b>29. Контактная информация .....</b>	<b>185</b>
29.1. Веб-адреса .....	185
29.2. Местные дистрибьюторы .....	185
29.3. Офисы Bitdefender .....	186
<b>Глоссарий .....</b>	<b>189</b>



## **УСТАНОВКА**





## 1. ПОДГОТОВКА К УСТАНОВКЕ

Перед установкой Bitdefender Antivirus Plus 2018 завершите эти приготовления для обеспечения беспрепятственной установки:

- Убедитесь, что компьютер, на котором вы собираетесь установить Bitdefender, соответствует минимальным системным требованиям. Если компьютер не соответствует минимальным системным требованиям, Bitdefender не будет установлен, либо не будет работать должным образом и это приведет к замедлению работы и нестабильности системы. С полным списком системных требований можно ознакомиться в разделе *«Системные требования»* (р. 3).
- Войдите в систему под учетной записью администратора.
- Удалите все другие программы безопасности с компьютера. 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. Защитник Windows будет отключен по умолчанию перед началом установки.
- Рекомендуется обеспечить подключение компьютера к Интернету во время установки, даже если установка выполняется с CD- или DVD-диска. Если доступны новые версии файлов приложения, включенные в пакет установки, Bitdefender можно загрузить и установить их.



## 2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Вы можете установить Bitdefender Antivirus Plus 2018 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 типе Вашей системы.

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

### 2.1. Минимальные системные требования

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

### 2.2. 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)

## 2.3. Требования к программному обеспечению

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

- Microsoft Edge 40 и более новые версии
- Internet Explorer 10 и более новые версии
- Mozilla Firefox 51 более новые версии
- Google Chrome 34 и более новые версии
- Skype 6.3 более новые версии



## 3. УСТАНОВКА ПРОДУКТА BITDEFENDER

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

Если Ваша покупка охватывает более чем один компьютер (например, Вы приобрели Bitdefender Antivirus Plus 2018 для 3 ПК), повторите процесс установки и зарегистрируйте продукт с помощью лицензионного ключа на каждом компьютере. Необходимо использовать аккаунт, который содержит активную подписку на Ваш Bitdefender.

### 3.1. Установка из Bitdefender Central

Из аккаунта Bitdefender Central можно скачать установочный комплект, соответствующий приобретенной подписке. Как только процесс установки завершен, Bitdefender Antivirus Plus 2018 будет активирован.

Для скачивания Bitdefender Antivirus Plus 2018 из Bitdefender Central необходимо:

1. Войдите в **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. Дождитесь окончания загрузки, затем запустите программу установки.



## Проверка установки

Сначала Bitdefender проверит Вашу систему для подтверждения установки.

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

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

В Bitdefender Antivirus Plus 2018 инсталляционный пакет постоянно обновляется.



### Замечание

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

Если установка прошла проверку, появится мастер установки. Выполните следующие шаги для установки Bitdefender Antivirus Plus 2018.

## 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 Antivirus Plus 2018

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 об использовании продукта



отправляются на серверы Bitdefender. Эта информация имеет важное значение для улучшения 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 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»* (р. 90)

## 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 Antivirus Plus 2018 интерфейс.

## 3.2. Установка продукта с установочного диска

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



В течение нескольких секунд должен появиться 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 установка продукта Bitdefender будет выполнена с диска и будет загружена более новая версия 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 при медленных интернет-соединениях.

Если установка прошла проверку, появится мастер установки. Выполните следующие шаги для установки Bitdefender Antivirus Plus 2018.

## 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 Antivirus Plus 2018

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 об использовании продукта отправляются на серверы Bitdefender. Эта информация имеет важное значение для улучшения 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 хотите использовать в продукте.

## Шаг 2 - Ход выполнения установки

Дождитесь завершения установки. Отображаются подробные сведения о ходе выполнения.

Идет проверка наиболее важных областей системы на наличие вирусов и запуск служб Bitdefender. Выполнение этого шага может занять несколько минут. Нажмите кнопку **ПРОПУСТИТЬ СКАНИРОВАНИЕ** если Вы хотите сканировать систему позже. Дополнительные сведения о проведении сканирования системы см. в *«Запуск проверки системы»* (р. 90)

## 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*» (р. 39).

Выполните действия, соответствующие текущей ситуации.

## Я хочу создать учетную запись Bitdefender

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

Предоставленные сведения останутся конфиденциальными.

Пароль должен содержать не менее 8 символов и цифру.

Прочитайте Условия предоставления услуг Bitdefender, прежде чем продолжить.



### Замечание

После создания учетной записи Вы можете использовать имеющийся адрес электронной почты и пароль для входа в учетную запись <https://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, можете использовать ее, чтобы войти в свою учетную запись Bitdefender. Если Вы забыли пароль, то сначала нужно перейти к <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

Для входа используйте Вашу учетную запись Microsoft, Facebook или Google:

1. Выберите службу, которую 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, например, 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 создание новой учетной записи Bitdefender на предыдущем шаге или если 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 Antivirus Plus 2018 интерфейс.



## **НАЧАЛО РАБОТЫ**



## 4. ОСНОВЫ

Установка Bitdefender Antivirus Plus 2018 обеспечивает защиту от всех типов вредоносных программ, таких как вирусы, шпионские программы и программы-вымогатели, эксплойты, бот-сети и трояны.

Приложение использует технологию Фотон для повышения скорости и производительности процесса антивирусного 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 Вашими действиями и найти подходящий момент для хищения личных данных, кроме того Ваш IP-адрес 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» (р. 133).

Можете отслеживать пароли и учетные данные, сохранив их в «*Защита ваших учетных данных при помощи Менеджер паролей*» (р. 125) Хранилище. Используя один мастер-пароль Вы можете защитить персональные данные от злоумышленников, которые могут попытаться вывести Ваши денежные средства.

Чтобы обеспечить защиту от потенциальных мошенников и нарушителей во время подключения устройства к незащищенной точке доступа, Bitdefender проводит анализ уровня безопасности и, если это необходимо, предлагает необходимые решения для повышения безопасности Ваших действий в сети. Для получения инструкций как сохранить в безопасности персональные данные см. «*Советник безопасности Wi-Fi*» (р. 117)

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 на сегодняшний день вредоносного ПО, а именно, вируса-вымогателя. Информацию о том, каким образом перенести личные файлы в хранилище, см. «*Безопасные файлы*» (р. 122)



Во время Вашей работы, игры или просмотра фильма, Bitdefender может предложить непрерывную работу путем отсрочки задач обслуживания, устраняя перебои и регулируя системные визуальные эффекты. Вы можете воспользоваться всеми этими преимуществами, активируя и настроив *«Профили»* (р. 145).

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»* (р. 18).

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

Чтобы использовать онлайн-возможности Bitdefender Antivirus Plus 2018 и управлять своими подписками и устройствами, войдите в Вашу учетную запись Bitdefender. Для получения дополнительной информации перейдите к *«Bitdefender Central»* (р. 39).

В разделе *«Советы»* (р. 50) Вы найдете пошаговые инструкции о том, как выполнять общие задачи. Если у вас возникли проблемы при использовании Bitdefender, проверьте раздел *«Решение распространенных проблем»* (р. 153) для возможных решений наиболее распространенных проблем.

## 4.1. Откройте окно Bitdefender.

Выполните следующую процедуру, чтобы войти в главный интерфейс Bitdefender Antivirus Plus 2018:

### ● В Windows 7:

1. Нажмите **Пуск** и перейдите в **Все программы**.
2. Нажмите **Bitdefender 2018**.
3. Нажмите **Bitdefender Antivirus Plus 2018** или дважды нажмите на Bitdefender **B** иконку в 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 **B** 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 **B** иконку в системном трее.

Дополнительную информацию об окне и значке Bitdefender в области уведомлений см. в *«Bitdefender интерфейс»* (п. 24).


## 4.2. 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(некритические) проблемы** - могут повлиять на защиту системы в ближайшем будущем.

Изменение цвета значка Bitdefender в **системном трее** 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.

## 4.2.1. Мастер проблем безопасности

Чтобы устранить обнаруженные проблемы, следуйте инструкциям мастера **Проблемы Безопасности**.

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 Интерфейс** 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 **ОК**. Чтобы остановить мониторинг проблем соответствующей категории, выберите **Постоянно**.

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

3. Для устранения выбранных проблем, нажмите **Устранить**. Некоторые проблемы моментально будут устранены. Мастер поможет устранить остальные.

Проблемы, которые помогает устранить мастер, можно сгруппировать в следующие основные категории:

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






## 4.2.2. Настройка оповещений о статусе

Bitdefender может сообщать Вам об обнаружении проблем при эксплуатации следующих программных компонентов:

- Антивирус
- 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 Интерфейс**.
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.

## 4.3. Уведомления

Bitdefender ведет подробный журнал событий, связанных с действиями, которые продукт выполняет на Вашем компьютере. Всякий раз, когда происходит что-то, имеющее отношение к безопасности системы и данных, в область уведомлений Bitdefender добавляется новое сообщение, аналогично новому сообщению, появляющегося в папке «Входящие».

Уведомления являются важным средством мониторинга и управления Вашей защиты Bitdefender. Например, Вы можете легко проверить, успешно ли было выполнено обновление, были ли обнаружены вредоносные программы или неисправности на 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 боковой панели инструментов **Bitdefender Интерфейс**. Каждый раз, когда происходит критическое событие, счетчик можно заметить на иконке .



В зависимости от типа и степени серьезности, уведомления группируются в:

- **Критические** события указывают на критические проблемы. Вы должны проверить их немедленно.
- **Предупреждающие** события указывают на некритичные проблемы. Их следует проверить и исправить в ближайшее время.
- **Информационные** события показывают успешно выполненные операции.

Нажмите каждую вкладку, чтобы найти дополнительные сведения о созданных событиях. Краткие сведения отображаются при нажатии одной кнопки на каждом названии события, а именно: краткое описание, действие, принятое Bitdefender по отношению к нему, когда это случилось, а также дата и время, когда это произошло. При необходимости могут быть предоставлены варианты выбора дальнейших действий.

Чтобы упростить управление регистрируемыми событиями, в окне уведомлений можно удалить или пометить как прочитанные все события в этом разделе.

## 4.4. АВТОПИЛОТ

Для пользователей, которым требуется, чтобы система безопасности обеспечивала защиту и не отвлекала, в Bitdefender Antivirus Plus 2018 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.
- Веб-защита.
- Автоматические обновления.



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

Пока режим "Автопилот" остается включенным, значок Bitdefender в системном трее будет иметь вид .



## Важно

При включении Автопилота изменение любого из параметров, которыми он управляет, приведет к его отключению.

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

## 4.5. Профили

Некоторые компьютерные мероприятия, такие как онлайн-игры или видеопрезентации, требуют повышенной отзывчивости системы, высокой производительности и отсутствия прерываний. Если Ваш ноутбук работает от батареи, лучше отложить операции, которые потребляют дополнительную мощность до подключения ноутбука к источнику бесперебойного питания.

Профили Bitdefender назначают больше системных ресурсов работающим приложениям путем временного изменения параметров защиты и настройки конфигурации системы. Следовательно, влияние системы на Ваши действия сведено к минимуму.

Для адаптации к различным видам деятельности, Bitdefender поставляется со следующими профилями:

### Профиль Работа

Оптимизирует эффективность работы, определяя и регулируя параметры продукта и системы.

### Профиль Кино

Усиливает визуальные эффекты и устраняет перебои при просмотре фильмов.

### Профиль Игры

Улучшает визуальные эффекты и устраняет прерывания во время игры.



## Профиль публичный Wi-Fi

Применяет параметры продукта, чтобы воспользоваться полной защитой при подключении к незащищенной беспроводной сети.


## Профиль режима батареи

Применяет параметры продукта и удерживает фоновую активность для экономии заряда аккумулятора.

## 4.5.1. Настройка автоматической активации профилей

Для простоты использования, можно настроить Bitdefender для управления рабочим профилем. В этом случае Bitdefender автоматически обнаруживает действие, которое Вы выполняете, и применяет настройки системы и оптимизации продукта.

Чтобы разрешить Bitdefender активировать профили необходимо:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Выберите вкладку **ПРОФИЛИ**.
3. Используйте соответствующий переключатель чтобы включить **Активировать профиль автоматически**

Если Вы не хотите, чтобы профили были автоматически активированы, выключите выключатель.


Чтобы вручную активировать профиль, нажмите соответствующую кнопку включения/выключения. Только один профиль может быть активирован вручную одновременно.

Для получения дополнительной информации о Профилях, пожалуйста, обратитесь к *«Профили»* (р. 145)

## 4.6. Защищенные паролем настройки Bitdefender

Если Вы являетесь не единственным пользователем с правами администратора для этого компьютера, рекомендуется защитить параметры Bitdefender паролем.

Чтобы настроить защиту паролем для параметров Bitdefender:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. В окне **Общие** включите **Защита паролем**, щелкнув соответствующий переключатель.



3. Введите пароль в два поля, затем нажмите **ОК**. Пароль должен содержать не менее 8 символов.


После установки пароля любой пользователь, пытающийся изменить настройки Bitdefender, сначала должен будет ввести 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.

Чтобы удалить защиту паролем:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. В окне **ОБЩИЕ** отключите защиту паролем, щелкнув соответствующий переключатель.
3. Введите пароль и затем нажмите **ОК**




## Замечание

Чтобы изменить пароль для Вашего продукта, нажмите на ссылку **Изменить пароль**. Введите текущий пароль и нажмите **ОК**. В появившемся новом окне введите новый пароль, который вы хотите использовать, чтобы ограничить доступ к параметрам Bitdefender.

## 4.7. Анонимные отчеты об использовании

По умолчанию Bitdefender отправляет отчеты, содержащие сведения о том, как вы используете его на серверах Bitdefender. Эта информация поможет нам усовершенствовать продукт и предложить в будущем более широкие возможности. Обратите внимание, что эти отчеты не будут содержать конфиденциальных данных, таких как Ваше имя или IP-адрес, и что они не будут использоваться в коммерческих целях.

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


1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Выберите вкладку **Расширенный**.
3. Нажмите соответствующую кнопку включения/выключения.



## 4.8. Уведомления о специальных предложениях

Когда доступны рекламные предложения, продукт Bitdefender настроен на уведомление через всплывающее окно. Это дает Вам возможность воспользоваться выгодными ценами и сохранить Ваши устройства защищенными в течение более длительного периода времени.

Включение и отключение уведомлений о специальных предложениях:

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

Опция специальные предложения и уведомления о продуктах включена по умолчанию.



## 5. BITDEFENDER ИНТЕРФЕЙС

Bitdefender Antivirus Plus 2018 удовлетворяет требованиям как технически подкованных пользователей, так и новичков. Его графический пользовательский интерфейс разработан в соответствии с каждой категорией 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 **системном трее** 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.

### 5.1. Значок системный трей


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



#### 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 Панели 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.

● **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.

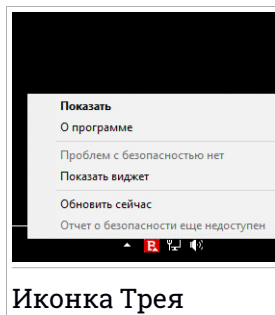
● **Просмотр проблем безопасности** -помогает удалить текущие уязвимости системы безопасности. Если параметр недоступен, значит проблем, требующих решения, нет.

Для получения дополнительной информации перейдите к *«Устранение неисправностей»* (р. 16).

● **Скрыть / Показать Виджет Безопасности** - включает / отключает **Виджет Безопасности**.

● **Обновить сейчас** - запускает немедленное обновление. Вы можете следить за состоянием обновления на панели обновления главного окна **Bitdefender**.

● **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.



Иконка Трех





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

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

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

**E** Задействована функция **Автопилот** в Bitdefender.

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

## 5.2. 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 защитить систему. 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.

## 5.2.1. 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»* (р. 16).








- **АВТОПИЛОТ** позволяет осуществлять оптимальную защиту и пользоваться полностью тихой безопасностью. Для получения дополнительной информации перейдите к *«Автопилот»* (р. 19).
- **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»* (р. 45).
- **Активный Профиль** отображает текущий профиль, включенный в продукте Bitdefender. Для получения дополнительной информации перейдите к *«Профили»* (р. 145).



## 5.2.2. Левая боковая панель инструментов

Наводящие значки доступны на левой боковой панели, предоставляя 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. Кроме того, становятся видны сведения о заблокированных приложениях, обнаруженных угрозах и атаках. Щелкните **ПРОСМОТР ФУНКЦИЙ** для доступа к области конфигурации.
-  **Приватность.** Кнопки действий **Безопасный платеж** и **VPN** становятся видимыми в левом нижнем углу интерфейса Bitdefender. Кроме того, отображается информация об обнаруженных кошельках и уничтоженных файлах. Щелкните **ПРОСМОТР ФУНКЦИЙ** для доступа к области конфигурации.
-  **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** Доступны сведения об учетной записи Bitdefender и использовании подписки. Доступ к учетной записи Bitdefender для проверки подписок и выполнения задач безопасности на управляемых устройствах.
-  **Параметры.** Отсюда Вы можете получить доступ к общим настройкам.
-  **Поддержка.** Отсюда, когда нужна помощь в решении проблем с Вашим Bitdefender Antivirus Plus 2018, Вы можете обратиться в отдел технической поддержки Bitdefender.



## 5.2.3. Кнопки действий и доступ к области функций

С помощью кнопки быстрого действия Вы можете быстро запускать важные задачи. Кнопки быстрых действий становятся видимыми в левом нижнем углу интерфейса Bitdefender при выборе одного из двух разделов: **Protection** и **Privacy** из 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

## 5.2.4. 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 требуемую операционную систему и нажмите кнопку **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 Antivirus Plus 2018 на 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.



## 5.3. Разделы Bitdefender

Продукт Bitdefender поставляется с тремя разделами, разделенными на полезные функции, которые помогут Вам оставаться защищенными во время работы, просмотра веб-страниц, во время игр или совершении онлайн-платежей.

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 интерфейса:

-  Защита
-  Приватность

### 5.3.1. Защита

В разделе Защита вы можете настроить дополнительные параметры безопасности, настроить безопасные файлы и функции веб-защиты, проверить и устранить потенциальные уязвимости системы и оценить безопасность беспроводных сетей, к которым вы подключаетесь.

Функции, которыми вы можете управлять в разделе Защита:

#### АНТИВИРУС

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

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

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

Дополнительную информацию о задачах сканирования и процедуре настройки защиты антивируса см. в «Антивирусная защита» (р. 82).



## ВЕБ-ЗАЩИТА

Web Protection 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»* (р. 110).

## 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»* (р. 107).

## 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 ищек .

Дополнительные сведения о настройке защиты уязвимостей можно найти в *«Уязвимости»* (р. 113).

## 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»* (р. 122).

## 5.3.2. Приватность

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

Функции, которыми вы можете управлять в разделе Конфиденциальность:

### VPN

VPN обеспечивает защиту Вашей онлайн-активности и скрывает Ваш IP-адрес каждый раз, когда вы подключаетесь к незащищенным публичным 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»* (р. 133).

### МЕНЕДЖЕР ПАРОЛЕЙ

Bitdefender Менеджер паролей помогает вам отслеживать ваши пароли, защищает вашу конфиденциальность и обеспечивает безопасный просмотр.

Дополнительные сведения о настройке Менеджер Паролей см. *«Защита ваших учетных данных при помощи Менеджер паролей»* (р. 125).

### 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»* (р. 136).



## ЗАЩИТА ДАННЫХ

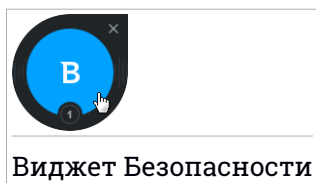
Функция защиты данных позволяет постоянно удалять файлы. Нажмите **Шредер файлов** на панели «Защита данных» для запуска мастера, который позволит полностью удалить файлы из Вашей системы.

Для получения более подробной информации о настройке Защита данных, пожалуйста, обратитесь *«Защита данных»* (р. 141).

## 5.4. Виджет Безопасности

**Виджет безопасности** является быстрым и простым способом для контроля и управления Bitdefender Antivirus Plus 2018. Добавление этого небольшого и ненавязчивого виджета на рабочий стол позволяет увидеть важную информацию и выполнить ключевые задачи в любое время:

- открыть главное окно Bitdefender.
- Мониторинг активности сканирования в режиме реального времени.
- Отслеживайте состояние безопасности системы и устраняйте существующие проблемы.
- Просмотр, когда выполняется обновление.
- 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.



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  для одного непрочитанного события, чтобы открыть окно Уведомления. Для получения дополнительной информации, пожалуйста, перейдите [«Уведомления»](#) (р. 18).

## 5.4.1. Сканирование файлов и папок

Вы можете использовать Виджет безопасности для быстрого сканирования файлов и папок. Перетащите файл или папку, которую Вы хотите просканировать, 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 попытается вылечить их (удалить вредоносный код). Если действие не будет успешно, то Мастер сканирования даст вам возможность определить дальнейшие действия по отношению к данным файлам.

## 5.4.2. Показать / скрыть Виджет безопасности

Если вы больше не хотите видеть виджет, нажмите .

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



- Из 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 Интерфейс**.
  2. Выберите вкладку **ОБЩИЕ**.
  3. Нажмите на соответствующий переключатель **Отобразить Виджет безопасности**, чтобы включить виджет.

Виджет безопасности Bitdefender по умолчанию отключен.

## 5.5. Действие

Окно Действия отображает информацию о действиях, предпринятых Bitdefender на устройстве в течение последних 30 дней. Здесь вы можете проверить, какие приложения, угрозы и атаки были заблокированы в течение этого периода, а также были ли какие-либо попытки атаки вымогателей.

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 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 в отчете безопасности делится на две 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»* (р. 82).

## ● Отсканированные веб-страницы

Позволяет проверить количество веб-страниц, сканированных и заблокированных 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»* (р. 110).

## ● 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»* (р. 113).

## ● 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»* (р. 18).

- Раздел **Оптимизация** - просматривает информацию, связанную с очищенным пространством, количеством оптимизированных приложений и ресурс батареи, сэкономленный с помощью профиля Режим батареи.

## ● 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 режима батареи»* (р. 150).



## ● Оптимизированные приложения

Позволяет увидеть количество приложений, используемых в Профилях.

Для получения более подробной информации о Профилях, пожалуйста, обратитесь к «Профили» (р. 145).

## 5.5.1. 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 Интерфейс**.

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 отобразится 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:


- **Зеленая зона**. - проблем нет. Ваш компьютер и данные защищены.



- **Желтая зона.** Некритические угрозы безопасности системы. Их следует проверить и исправить в ближайшее время.
- **Красная зона.** - критические угрозы безопасности системы. Эти проблемы следует разрешить незамедлительно.

## 5.5.2. Включение/отключение уведомлений о состоянии системы безопасности.

Включение/отключение уведомлений о состоянии системы безопасности:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. В окне **ОБЩИЕ**, выберите соответствующий переключатель вкл/выкл. Уведомление Отчета о состоянии системы безопасности всплывает по умолчанию.



## 6. 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 Antivirus Plus 2018
  - Антивирус Bitdefender для Mac
  - Bitdefender Мобильная безопасность & Антивирус для Android
  - Bitdefender Мобильная безопасность для iOS
- Управление и обновление своей Bitdefender подпиской.
- Добавлять новые устройства к сети и управлять ими, где бы вы не находились.

### 6.1. Доступ к Bitdefender Central

Есть несколько способов доступа к Bitdefender Central. 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 Интерфейс**.
  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.

## 6.2. Мои подписки

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

### 6.2.1. Проверка доступных подписок

Проверка доступных подписок:

1. Войдите в **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 подписке или продлить имеющуюся, выбрав карту подписки.



#### Замечание

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

### 6.2.2. Добавить новое устройство

Если ваша подписка охватывает более одного устройства, вы можете добавить новое устройство и установить на нем Bitdefender Antivirus Plus 2018 следующим образом:

1. Войдите в **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. Дождитесь окончания загрузки, затем запустите программу установки.

## 6.2.3. Продлить подписку

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

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

В веб-браузере откроется веб-страница, на которой можно продлить Bitdefender.

## 6.2.4. Активировать подписку

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

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

Активация подписки с помощью кода активации:

1. Войдите в **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.






## 6.3. Мои устройства

Область **Мои устройства** в вашем Bitdefender Central дает возможность установить, управлять и принимать удаленные действия в Bitdefender на любом устройстве, при условии, что оно включено и подключено к Интернету. Карты 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 идентифицировать устройства, можно настроить имя устройства:

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

Для удаленного обновления Bitdefender на устройстве:

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

Для других возможностей удаленного управления и информации о вашей 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 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. Отсюда вы можете вручную исправить проблемы, влияющие на безопасность ваших 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 процессах сканирования, пожалуйста, обратитесь *«Запуск проверки системы»* (р. 90) и *«Запуск быстрого сканирования»* (р. 90).
- **Уязвимость.** 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 **Подробная информация** чтобы получить доступ к подробному отчету о найденных проблемах. Для более подробной информации об этой функции, пожалуйста, обратитесь **«Уязвимости»** (р. 113).


## 6.4. Моя учетная запись

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

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

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

## 6.5. Уведомления

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



## 7. ПОДДЕРЖКА BITDEFENDER В ОБНОВЛЕННОМ СОСТОЯНИИ

Каждый день 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?»* (р. 74).
- 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»* (р. 160).
- Если вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять Bitdefender по запросу. Для получения дополнительной информации перейдите к *«Выполнение обновления»* (р. 46).



## 7.1. Проверка обновлений 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 Интерфейс**.
2. На вкладке **ВСЕ**, выберите уведомления относительно последнего обновления.

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

## 7.2. Выполнение обновления

Для выполнения обновления требуется подключение к Интернету.

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

Вам может потребоваться перезагрузка компьютера, для 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 **Bitdefender Central**.
2. Выберите **Мои устройства** на панели справа.
3. Нажмите  иконку желаемой карточки устройства, затем выберите **Обновить**.

## 7.3. Включение и отключение автоматического обновления

Чтобы включить или выключить автоматическое обновление:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Выберите вкладку **ОБНОВИТЬ**.
3. Нажмите соответствующую кнопку включения/выключения.
4. Появится окно предупреждения. Необходимо подтвердить выбор. Для этого в меню следует выбрать период, на который требуется отключить автообновление. 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.

## 7.4. Настройка параметров обновления

Обновление может быть выполнено через локальную сеть, через Интернет, напрямую или через прокси-сервер. По умолчанию Bitdefender ежедневно 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 Интерфейс**.



2. Выберите вкладку **ОБНОВИТЬ** и измените настройки в соответствии с вашими предпочтениями.

## Частота обновлений

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

## Место обновлений

В Bitdefender настроено получение обновлений с серверов обновлений Bitdefender в Интернете. Местом сервера обновлений является универсальный Интернет-адрес, который автоматически перенаправляет Вас на ближайший сервер обновления 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 перезагрузки, 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 **Отложить перезагрузку**, нажав на соответствующий переключатель.

## 7.5. Непрерывные 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.





## **СОВЕТЫ**



## 8. УСТАНОВКА

### 8.1. Как установить Bitdefender на второй компьютер?

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

Установить Bitdefender на второй компьютер:

1. Нажмите 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 требуемую операционную систему и нажмите кнопку **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.

### 8.2. Как переустановить Bitdefender?

Типичные ситуации, в которых может потребоваться переустановка Bitdefender:

- вы переустановили операционную систему.
- Вы хотите исправить проблемы, которые могут привести к замедлению и сбоям.
- ваш продукт Bitdefender не запускается или не работает должным образом.

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

- В **Windows 7**:



1. Нажмите **Пуск** и перейдите в **Все программы**.
2. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
3. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
4. Для завершения процесса необходимо будет перезагрузить компьютер.

● В **Windows 8 и Windows 8.1**:

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
5. Для завершения процесса необходимо будет перезагрузить компьютер.

● В **Windows 10**:

1. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.
2. Нажмите иконку **Система** в области **Настройки**, затем выберите **Программы & компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Щелкните **УДАЛИТЬ**.
6. Для завершения процесса необходимо будет перезагрузить компьютер.



## **Замечание**

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие параметры могут быть переключены обратно в конфигурацию по умолчанию.



## 8.3. На каком веб-сайте можно загрузить Bitdefender?

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



### 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 **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.

## 8.4. Как изменить язык продукта Bitdefender?


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

Чтобы пользоваться Bitdefender на другом языке:

1. Удалите Bitdefender, выполнив следующие действия:

- **В Windows 7:**



- a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
  - b. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
  - c. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
  - d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- В **Windows 8 и Windows 8.1**:
- a. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
  - b. Нажмите **Удалить программу** или **Программы и компоненты**.
  - c. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
  - d. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
  - e. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- В **Windows 10**:
- a. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.
  - b. Нажмите иконку **Система** в области **Настройки**, затем выберите **Установленные приложения**.
  - c. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
  - d. Нажмите **Удалить** снова, чтобы подтвердить выбор.
  - e. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
  - f. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
2. Изменение языка в Bitdefender Central:
- a. Войдите в **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 раскрывающегося 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.

## 8.5. Как пользоваться лицензионным ключом 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.



- Обновление от предыдущей версии Bitdefender Total Security до последней доступной Bitdefender Total Security.

## Существует 2 варианта развития событий:

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

В этом случае необходимо переустановить продукт, выполнив следующие действия:

- В **Windows 7**:

1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
2. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
3. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

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

- В **Windows 8 и Windows 8.1**:

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

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

- В **Windows 10**:

1. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.



2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

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



## Замечание

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие параметры могут быть переключены обратно в конфигурацию 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 **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*» (р. 5).

## 8.6. 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: **111 <https://www.bitdefender.com/Downloads/>**. Активация возможна только при наличии действительной подписки.



## 9. ПОДПИСКИ

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


Если у вас есть действующий лицензионный ключ и Вы хотите использовать его для активации подписки на Bitdefender Antivirus Plus 2018, есть два возможных варианта:

● Вы обновили предыдущую версию Bitdefender на новую:

1. После завершения обновления до Bitdefender Antivirus Plus 2018 вам будет предложено войти в свою учетную запись Bitdefender.
2. Нажмите **Войти**, затем введите адрес электронной почты и пароль для Вашей учетной записи Bitdefender.
3. Нажмите **Войти** чтобы продолжить.
4. На экране вашего аккаунта появится уведомление о том, что подписка была создана. Созданная подписка будет действительна в течение оставшихся дней на вашем лицензионном ключе и для того же количества пользователей.

На устройствах, использующих предыдущие версии Bitdefender и зарегистрированных с помощью лицензионного ключа, необходимо активировать продукт с той же учетной записью Bitdefender.

● Bitdefender ранее не устанавливался в системе:

1. Как только процесс установки будет завершен, вам будет предложено войти в свой аккаунт Bitdefender.
2. Нажмите **Войти**, затем введите адрес электронной почты и пароль для Вашей учетной записи Bitdefender.
3. Нажмите **ВОЙТИ** чтобы продолжить и затем нажмите кнопку **ЗАКОНЧИТЬ** чтобы перейти к интерфейсу Bitdefender Antivirus Plus 2018.
4. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 одинаковой доступностью и количеством пользователей вашего лицензионного ключа связана с вашей учетной записью.




## 10. BITDEFENDER CENTRAL

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

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

Для того, чтобы успешно использовать другую учетную запись:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Нажмите кнопку **ПОМЕНИТЬ 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»* (р. 180).

### 10.2. Как отключить справочные сообщения Bitdefender Central?

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

Если вы хотите прекратить просмотр такого рода сообщений:


1. Войдите в **Bitdefender Central**.
2. Нажмите  иконку в верхней правой части экрана.
3. Нажмите **Моя учетная запись** в слайд-меню.
4. Выберите вкладку **Параметры**.
5. Отключить опцию **Включение/выключение сообщений**.



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

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

● Из интерфейса Bitdefender:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.



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

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

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



## 11. СКАНИРОВАНИЕ С BITDEFENDER

### 11.1. Как выполнить сканирование файла или папки?

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

Для завершения сканирования следуйте инструкциям мастера антивирусного сканирования. Bitdefender будет автоматически предпринимать рекомендуемые действия для обнаруженных файлов.


Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

Типичные ситуации, в которых вы можете пользоваться этим методом сканирования:

- Вы подозреваете, что файл или папка заражены.
- Когда вы загружаете из Интернета файлы, которые, как вам кажется, могут быть опасны.
- Сканирование общей сетевой папки перед копированием файлов на компьютер.

### 11.2. Как выполнить сканирование системы?

Чтобы выполнить полную проверку системы:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Системное сканирование**.
4. Для завершения сканирования следуйте инструкциям мастера сканирования системы. Bitdefender будет автоматически предпринимать рекомендуемые действия для 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*» (р. 94).

## 11.3. Как составить график сканирования?

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

Чтобы запланировать сканирование:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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


## 11.4. Как создать пользовательское задание сканирования?

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

Для создания пользовательской задачи сканирования выполните следующие действия:





1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 дополнительные 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 поведение по умолчанию каждый раз при выполнении 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.

## 11.5. 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 Интерфейс**.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. Выберите  иконку в правом верхнем углу на панели **АНТИВИРУС**.
4. Перейдите на 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 он должен быть исключен.
7. Нажмите **Добавить** чтобы сохранить изменения и закрыть окно.

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



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

1. Отключите антивирусную защиту Bitdefender в режиме реального времени:
  - a. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
  - 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?»* (р. 76).
3. Восстановление файла из области карантина:
  - a. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
  - 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?»* (р. 66).
5. Включите 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»* (р. 180).

## 11.7. 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 Интерфейс**.



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**.





## 12. ЗАЩИТА ПРИВАТНОСТИ

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

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

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

Для обеспечения безопасности и приватности онлайн-действий:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Нажмите кнопку быстрого действия **Безопасный платеж**.
3. Нажмите кнопку  для доступа к **Виртуальной клавиатуре**.

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

### 12.2. Как удалить файл навсегда с Bitdefender?

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

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

1. Щелкните правой кнопкой мыши по файлу или папке, которые требуется удалить навсегда в Bitdefender, и выберите **Файловый шредер**.
2. 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



## 13. ПОЛЕЗНАЯ ИНФОРМАЦИЯ

### 13.1. Как протестировать антивирусное решение?

Чтобы убедиться в правильности работы продукта Bitdefender, рекомендуется использовать тест EICAR.

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

Чтобы проверить ваше антивирусное решение:

1. Загрузите тестовый файл с официального веб-сайта 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 **скачать области с помощью стандартного протокола http**.
5. Вы получите уведомление о том, что страница, к которой вы пытаетесь получить доступ, содержит EICAR-Test-файл (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»* (р. 180).

### 13.2. Как удалить Bitdefender?

Если вы хотите удалить Bitdefender Antivirus Plus 2018:

#### ● В Windows 7:

1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
2. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.



3. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

## ● В Windows 8 и Windows 8.1:

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

## ● В Windows 10:

1. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.
2. Нажмите иконку **Система** в области **Настройки**, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.



### **Замечание**

Эта процедура переустановки навсегда удалит настроенные параметры.

## 13.3. Как удалить BitdefenderVPN?

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

### ● В Windows 7:



1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.

2. Найдите **BitdefenderVPN** и выберите **Удалить**.

Дождитесь завершения процесса удаления.

● **В Windows 8 и Windows 8.1:**

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.

2. Нажмите **Удалить программу** или **Программы и компоненты**.

3. Найдите **BitdefenderVPN** и выберите **Удалить**.

Дождитесь завершения процесса удаления.

● **В Windows 10:**

1. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.

2. Нажмите иконку **Система** в области **Настройки**, затем выберите **Установленные приложения**.

3. Найдите **BitdefenderVPN** и выберите **Удалить**.

4. Нажмите **Удалить** снова, чтобы подтвердить выбор.

Дождитесь завершения процесса удаления.

## 13.4. Как автоматически выключить компьютер после завершения сканирования?

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 хотите, чтобы вся система проверялась на наличие вредоносного по Bitdefender.





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

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 дополнительные параметры сканирования, выберите вкладку **Расширенное**.
6. Выберите завершение работы компьютера после завершения 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» (р. 94)**.

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

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




### Важно

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



Чтобы настроить параметры прокси-сервера:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Выберите вкладку **Расширенный**.
3. Включите использование прокси с помощью соответствующего переключателя.
4. Нажмите ссылку **Управление прокси**.
5. Настройки прокси-сервера можно задать двумя способами:

- **Импортировать настройки прокси 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

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

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

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

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

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

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



- В **Windows 7**:
  1. Нажмите **Пуск**.
  2. Найдите элемент **Компьютер** в меню **Пуск**.
  3. Щелкните правой кнопкой мыши по **Компьютер** и выберите **Свойства**.
  4. Войдите в раздел **Система** для просмотра сведений о системе.
- В **Windows 8**:
  1. Введите **Компьютер** в Стартовом окне Windows, (например, можно вводить «Компьютер» непосредственно в Стартовом окне) и затем щелкните правой кнопкой мыши по его значку.  
В **Windows 8.1**, найдите **Этот компьютер**.
  2. Выберите **Свойства** в нижнем меню.
  3. Посмотрите в системной области, чтобы увидеть ваш тип системы.
- В **Windows 10**:
  1. Введите "Система" в поле поиска на панели задач и щелкните значок.
  2. Найдите в системной области сведения о типе системы.

## 13.7. Как отобразить скрытые объекты в Windows?

Эти 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**.

## 13.8. Как удалить другие решения безопасности?

Основной причиной использования решения безопасности является обеспечение защиты и безопасности данных. Что происходит, если на компьютере установлено несколько решений безопасности?

Одновременное использование нескольких решений безопасности на компьютере приводит к нестабильности системы. Установщик Bitdefender Antivirus Plus 2018 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**, а затем нажмите кнопку **Параметры**.
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 деинсталляции.

## 13.9. Как перезагрузить компьютер в безопасном режиме?

Безопасный режим представляет собой операционный диагностический режим, который используется в основном для поиска и устранения неисправностей, негативно влияющих на нормальную работу Windows. Проблема такого типа может быть вызвана любыми причинами — от конфликта драйверов до 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 **ОК** для подтверждения.
6. Для запуска Windows в обычном режиме просто перезагрузите систему.

## ● In Windows 8, Windows 8.1 и Windows 10:

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

Ваша система перезагрузится в безопасном режиме с доступом к сети.

Для перезагрузки в обычном режиме, переключите настройки, снова запустив **Работа системы** и снимите флажок с **Безопасная загрузка**.



Нажмите **ОК** и затем нажмите **ПЕРЕЗАПУСК**. Подождите, пока будут применены новые параметры.



## **УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ**





## 14. АНТИВИРУСНАЯ ЗАЩИТА

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

- **Проверка при доступе** – предотвращает попадание новых вредоносных угроз в вашу систему. К примеру, Bitdefender будет сканировать документ Word на наличие известных угроз при его открытии и сообщать об электронной почте 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»** (р. 99).

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»** (р. 102).

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»** (р. 105).





В случае заражения компьютера вирусом см. информацию в «*Удаление вредоносного ПО из системы*» (р. 168). 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)*» (р. 168). 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.

## 14.1. Резидентное сканирование (защита в реальном времени)

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

### 14.1.1. 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 Интерфейс**.
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.

## 14.1.2. Настройка дополнительных параметров защиты в режиме реального времени

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

Чтобы настроить дополнительные параметры защиты в режиме реального времени:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 **гlossарии**. 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, в то время



как сканирование только файлов 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. Хакер может узнать конфиденциальную информацию из украденных данных, таких как номера банковских счетов и пароли, и использовать его для получения личных преимуществ.
- **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 Интерфейс**.



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:

### Принять соответствующие меры

Bitdefender выполнит рекомендуемые действия в зависимости от типа обнаруженного файла:

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

Файлы, которые не удастся 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»* (р. 105).



### Важно

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

- **Подозрительные файлы.** Файлы помеченные эвристическим анализатором 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»* (р. 105).



## **Запретить доступ**

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

## **14.1.3. Восстановление настроек по умолчанию**

Настройки по умолчанию защиты в режиме реального времени позволяют обеспечить качественную защиту от 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 Интерфейс**.
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.

## 14.2. 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.

### 14.2.1. 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).

## 14.2.2. 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 Интерфейс**.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Быстрое сканирование**.
4. Следуйте инструкциям **Мастера антивирусного сканирования** для выполнения проверки. Bitdefender будет автоматически предпринимать рекомендуемые действия для 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**.

## 14.2.3. 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»* (р. 45).

- 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»* (р. 91).

Чтобы запустить Системное сканирование:

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

## 14.2.4. Настройка пользовательского сканирования

Чтобы подробно настроить пользовательское сканирование и затем запустить его:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 дополнительные 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** . Понижить 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** . Минимизирует окно сканирования в **в системном трее**. 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 [гlossарии](#). 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; абр; 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; пyc; 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; xlsn; 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. Commercial keyloggers — 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.

## 14.2.5. Мастер антивирусного сканирования

Всякий раз, когда вы инициируете сканирование по запросу (например, щелкните правой кнопкой мыши папку, наведите указатель на Bitdefender и выберите **Сканирование с Bitdefender**), появится Мастер



антивирусного сканирования Bitdefender. Следуйте инструкциям мастера для завершения процесса сканирования.



## Замечание

Если Мастер сканирования не отображается, сканирование может быть настроено на запуск в фоновом режиме. Найдите **В** 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 пароль неизвестен, выберите один из вариантов.
- **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 **ОК** 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:

### Принять соответствующие меры

Bitdefender выполнит рекомендуемые действия в зависимости от типа обнаруженного файла:

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

Файлы, которые не удастся 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»* (р. 105).



## Важно

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

- **Подозрительные файлы.** Файлы помеченные эвристическим анализатором 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 незараженными, 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 предпринимайте 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»* (р. 168).

## 14.2.6. Просмотр журналов сканирования

Каждый раз при выполнении сканирования создается журнал сканирования и Bitdefender записывает обнаруженные неполадки в окне Антивируса. Журнал сканирования содержит подробные сведения о регистрируемом процессе сканирования, такие как параметры сканирования, цель сканирования, найденные угрозы и действия, предпринятые в отношении этих угроз.

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

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

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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**.

## 14.3. Автоматическое сканирование съемных носителей

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

### 14.3.1. 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 **B** 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»** (р. 168)



## 14.3.2. Управление сканированием съемных носителей

Для управления автоматической проверкой съемных носителей:

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


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

Параметры 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.

## 14.4. Сканирование хост-файлов

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

Для настройки сканирования хост-файлов:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Выберите вкладку **Расширенный**.
3. Нажмите соответствующую кнопку включения/выключения.



## 14.5. 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 требованию, позволяет анализировать всю систему на наличие вредоносных угроз, которые могут угрожать безопасности Ваших данных. Контекстное сканирование — это тип сканирования по запросу: щелкните правой кнопкой мыши файл или папку, которую необходимо сканировать, и выберите **Сканировать с Bitdefender**.

### 14.5.1. Исключение файлов или папок из сканирования

Чтобы исключить файлы или папки из сканирования:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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:
  - а. 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**.

## 14.5.2. Исключение расширений файлов из сканирования



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



### Важно

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

Исключение расширений файлов из сканирования:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 необходимо исключить из сканирования, разделяя их точками 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**.

## 14.5.3. 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 Интерфейс**.
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**.





## 14.6. Управление файлами в карантине

Bitdefender изолирует зараженные вирусами файлы, которые невозможно вылечить, и подозрительные файлы в безопасной области, называемой карантин. 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. Очищенные файлы автоматически перемещаются обратно в исходное местоположение.

Чтобы проверить и управлять файлами на карантине:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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. Очищенные файлы автоматически перемещаются обратно в исходное местоположение.





## **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 старше 30 дней удаляются автоматически. Для того, чтобы изменить интервал, введите новое значение в соответствующем поле. Для того, 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**.



## 15. АКТИВНЫЙ КОНТРОЛЬ УГРОЗ


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

Активный Контроль Угроз непрерывно отслеживает приложения, работающих 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.

### 15.1. Включение и выключение Активный Контроль Угроз:

Чтобы включить или выключить Активный Контроль Угроз:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 короткий промежуток времени.

### 15.2. Проверка обнаруженных вирусов-вымогателей

Для проверки обнаруженных атак вирусов-вымогателей:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 нее.

## 15.3. Проверка обнаруженных подозрительных приложений

Для проверки обнаруженных атак вирусов-вымогателей:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.

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.

## 15.4. Добавление процессов к исключениям


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 Интерфейс**.

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.





## 16. ВЕБ-ЗАЩИТА

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

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 Интерфейс**.
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, размещенные 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 Интерфейс**.
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.

## 16.1. Уведомления Bitdefender в браузере

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

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

Вам необходимо принять решения для дальнейших действий. Доступны следующие опции:



- Перейдите на веб-страницу, нажав кнопку **Снова защищать**.
- Игнорируя предупреждение, перейдите на веб-страницу, нажав кнопку **Я осознаю риск. Перейти все равно**.



## 17. УЯЗВИМОСТИ

Важным шагом в защите компьютера от вредоносных действий и приложений является сохранение операционной системы и приложений, которые регулярно используются в актуальном состоянии. Кроме того, для предотвращения несанкционированного физического доступа к вашему компьютеру, надежные пароли (пароли, которые не могут быть легко угаданы) должны быть настроены для каждой учетной записи пользователя Windows и для сетей Wi-Fi, к которым вы подключаетесь.

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

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


Bitdefender предоставляет два простых способа устранения уязвимостей системы:

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

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

### 17.1. Сканирование системы на наличие уязвимостей

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

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 ссылке **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.

## 17.2. Использование автоматического мониторинга уязвимостей

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


Чтобы проверить и исправить обнаруженные проблемы:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 **ПОМЕНИТЬ 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 Интерфейс**.
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.

### **Ненадежные 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, DVD, 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 получить доступ к Вашим приватным действиям.



### Замечание

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

## 17.3. Советник безопасности Wi-Fi

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

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



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



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

Bitdefender Wi-Fi Советник безопасности предоставляет информацию о:

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


## 17.3.1. Включение/отключение уведомлений Wi-Fi Советника безопасности

Чтобы включить или выключить уведомления Wi-Fi Советника Безопасности:

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

## 17.3.2. Настройка домашней сети Wi-Fi

Для того, чтобы приступить к настройке домашней сети:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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**.


### 17.3.3. Публичные Wi-Fi

При подключении к незащищенной или небезопасной беспроводной сети будет активирован профиль Публичный Wi-Fi. Во время работы в этом профиле, Bitdefender Antivirus Plus 2018 автоматически применяет следующие настройки программы:

- Активный Контроль Угроз включен
- 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.

### 17.3.4. 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 Интерфейс**.
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: **Домашний Wi-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 при использовании этой сети, 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 ли 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 небезопасными. Поэтому мы настоятельно рекомендуем вам проверить информацию о типе шифрования, чтобы быть уверенным в защите во время серфинга в Интернете.
- **Канал/Частота** - здесь вы можете просмотреть частоту канала, используемого в выбранной сети.
- **Надежность пароля** - здесь вы можете посмотреть надежность пароля. Обратите внимание, что сети, в которых используются слабые пароли, представляют собой мишень для кибер-преступников.



- **Тип входа** - здесь вы можете посмотреть защищена ли выбранная сеть с помощью пароля или нет. Настоятельно рекомендуется подключаться только к сетям, которые используют надежные пароли.
- **Тип аутентификации** - здесь вы можете просмотреть тип аутентификации, используемый в выбранной сети.

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





## 18. 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 шифруется, только пользователь 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.

## 18.1. Включение или выключение Безопасных Файлов

Чтобы включить или отключить функцию **Безопасные Файлы**:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.

## 18.2. Защита личных файлов от атак вымогателей

Если вы хотите хранить личные файлы под защитой:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 ПАПЕК**.
5. Выберите папку, которую Вы хотите защитить и нажмите **ОК**.

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

Папки «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.



### 18.3. Настройка доступа к приложениям

Те приложения, которые попытаются изменить или удалить защищенные файлы могут быть помечены как потенциально опасные и будут добавлены в список Заблокированных приложений. Если такое приложение блокируется, но Вы уверены в безопасности его поведения, Вы можете исключить его, выполнив следующие действия:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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**.

### 18.4. Защита при загрузке системы

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

Чтобы отключить Защиту при загрузке:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.



## 19. 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 удастся 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
- Доступ к данным для учетных записей электронной почты



- Пароли к приложениям
- Пароли к сетям Wi-Fi


## 19.1. Создание новой базы данных Кошелька

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

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 выберете **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**.

## 19.2. Импорт существующей базы данных

Импорт базы данных бумажника, хранящейся локально:



1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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**.

## 19.3. Экспорт базы данных Wallet

Чтобы экспортировать базу данных Кошелька:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.

## 19.4. Синхронизация ваших Кошельков в облаке

Чтобы включить или выключить синхронизацию кошельков в облаке:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.



2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **КОШЕЛЕК** нажмите **Мои кошельки**.
4. Нажмите на 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.

## 19.5. Управление учетными данными Кошелька

Для управления вашими паролями:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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**.



## 19.6. Включение и отключение защиты Менеджера паролей

Чтобы включить или отключить защиту Менеджера Паролей:

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

## 19.7. Управление настройками Менеджера паролей

Чтобы детально настроить мастер-пароль:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 Интерфейс**.
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 Интерфейс**.
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.

● **Автозаполнение 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 Кошелек 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.



## 20. VPN

Приложение VPN может быть установлено из продукта Bitdefender и использоваться каждый раз, когда вы хотите добавить дополнительный уровень защиты для вашего соединения. 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.

## 20.1. Установка VPN

Приложение VPN можно установить из интерфейса Bitdefender следующим образом:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.


## 20.2. 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 Интерфейс**.
2. Нажмите кнопку действия **VPN**.

## 20.3. Интерфейс VPN

Интерфейс VPN отображает состояние приложения, подключенного или отключенного. Расположение сервера для пользователей с бесплатной версией автоматически устанавливается Bitdefender на более подходящий, 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»* (р. 135).

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

При подключении в нижней части интерфейса отображается затраченное время и IP-адрес, автоматически назначенный устройству.

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.

## 20.4. Подписки

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

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

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

Подписка Bitdefender Premium VPN не зависит от подписки Bitdefender Antivirus Plus 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 Antivirus Plus 2018, Вы вернетесь к бесплатной версии.



## 21. 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»* (р. 125).

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™.

## 21.1. Использование Bitdefender Safepay™

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

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

- Из **интерфейса Bitdefender**:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Нажмите кнопку быстрого действия **Безопасный платеж**.

- 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 окне Bitdefender 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 .
- нажмите  рядом с адресной строкой, чтобы управлять **Закладками**.
- нажмите , чтобы открыть виртуальную клавиатуру.
- 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**.

## 21.2. 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 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 хотите дать подтверждение перед началом процесса печати.

## 21.3. Управление закладками

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

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

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



### 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**.



## 22. ЗАЩИТА ДАННЫХ

### 22.1. Окончательное удаление файлов


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

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

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

1. Щелкните правой кнопкой мыши по файлу или папке, которую хотите удалить.
2. Выберите **Bitdefender** > **Файловый шредер** в появившемся контекстном меню.
3. 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.

Также файлы можно уничтожать через интерфейс Bitdefender следующим образом:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.

**с. Сводка результатов**

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



## 23. 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-накопители и карты памяти, подключенные через карт-ридер. 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 иммунизировано, 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 устройство и щелкните правой кнопкой мыши по его значку.
3. В контекстном меню выберите пункт **Bitdefender** и выберите **Имунизировать этот диск**.



### Замечание

Если накопитель уже был иммунизирован, то вместо опции Иммунизация появится сообщение **Устройство USB, защищено от вредоносного программного обеспечения на основе автозапуска**.

Чтобы предотвратить запуск вредоносных программ с неиммунизированным USB-устройством, отключите функцию автозапуска мультимедиа. Для получения дополнительной информации перейдите к **«Использование автоматического мониторинга уязвимостей»** (р. 115).



## **ОПТИМИЗАЦИЯ СИСТЕМЫ**



## 24. 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 режима батареи

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

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

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

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

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





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

Во время работы в профиле Публичный Wi-Fi, Bitdefender Antivirus Plus 2018 устанавливается для автоматического выполнения следующих настроек программы:


- Активный Контроль Угроз включен
- Включены следующие настройки Веб-защиты:
  - Сканировать SSL
  - Защита от мошенничества
  - Защита от фишинга

## 24.1. Профиль Работа

Выполнение нескольких задач на работе, таких как отправка электронной почты, наличие видеосвязи с удаленными коллегами или работа с приложениями-конструкторами, 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 Интерфейс**.
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




- Отложенные фоновые программы и задачи обслуживания
- 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 Интерфейс**.
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. Перейдите к исполняемому файлу приложения, выберите его и нажмите **ОК**, чтобы добавить его в список.

## 24.2. Профиль Кино

Отображение высококачественного видеоконтента, такого как фильмы 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 Интерфейс**.
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
  - Отложенные фоновые программы и задачи обслуживания
  - Отложить автоматические обновления Windows
  - Настройка параметров схемы питания для фильмов
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 плееров**.

Чтобы вручную добавить видео-плееры в список профиля Фильм:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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. Перейдите к исполняемому файлу приложения, выберите его и нажмите **ОК**, чтобы добавить его в список.


## 24.3. Профиль Игры

Наслаждайтесь бесперебойной игрой без снижения 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 непрерывно.



## Настройка профиля Игра


Настройка действий, выполняемых в профиле Игра:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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
  - Отложенные фоновые программы и задачи обслуживания
  - Отложить автоматические обновления Windows
  - Настройка параметров плана электропитания 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 Интерфейс**.
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. Перейдите к исполняемому файлу игры, выберите его и нажмите **ОК**, чтобы добавить его в список.

## 24.4. Профиль публичный Wi-Fi


Отправка электронных писем, ввод конфиденциальных учетных данных или совершение покупок в Интернете при подключении к небезопасным



беспроводным сетям может подвергнуть риску ваши персональные данные. Профиль Публичный Wi-Fi регулирует настройки продукта, чтобы у вас была возможность совершать платежи в Интернете и использовать конфиденциальную информацию в защищенной среде.

## Настройка профиля Публичный Wi-Fi

Чтобы настроить Bitdefender на применение параметров продукта при подключении к небезопасной беспроводной сети:


1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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**.

## 24.5. Профиль режима батареи

Профиль Режим батареи разработан специально для пользователей ноутбуков и планшетных ПК. Его цель — свести к минимуму влияние системы и Bitdefender на энергопотребление, если уровень заряда аккумулятора ниже, чем тот, который выбран по умолчанию.

## Настройка профиля Режим Батареи

Чтобы настроить профиль Режим батареи:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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 батареи.
  - Отложите фоновые программы и задачи обслуживания.
  - Отложить автоматические обновления Windows



- Настройте параметры схемы питания для Режима батареи.
- Отключить 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.

## 24.6. Оптимизация в реальном 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 загрузки процессора, плагин отслеживает все процессы, ориентируясь на те, которые занимают более высокую нагрузку, чтобы приспособить их к вашим потребностям.

Чтобы включить или выключить Оптимизацию в реальном времени:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.



## **НЕПОЛАДКИ**



## 25. РЕШЕНИЕ РАСПРОСТРАНЕННЫХ ПРОБЛЕМ

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» (р. 153)*
- *«Сканирование не начинается» (р. 155)*
- *«Не удается использовать приложение» (р. 157)*
- *«Что делать, если Bitdefender блокирует безопасный веб-сайт или онлайн приложение» (р. 158)*
- *«Что делать, если Bitdefender определяет безопасное приложение в качестве программы-вымогателя» (р. 159)*
- *«Обновление Bitdefender при низкой скорости подключения к Интернету» (р. 160)*
- *«Службы Bitdefender не отвечают» (р. 160)*
- *«Функция "Автозаполнение" в Кошельке не работает» (р. 161)*
- *«Сбой удаления Bitdefender» (р. 162)*
- *«Моя система не загружается после установки Bitdefender» (р. 164)*

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» (р. 180)*.

### 25.1. Система работает медленно

Как правило, после установки программного обеспечения безопасности допускается незначительное снижение быстродействия системы, которое в определенной степени является нормальным.

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?»](#) (р. 77).

- **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»](#) (р. 3).

- **Вы установили приложение, которое не используете.**

На любом компьютере имеются программы или приложения, которые не используются. И многие нежелательные программы запускаются в фоновом режиме, занимая место на диске и память. 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 Интерфейс**.



2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Системное сканирование**.
4. Следуйте инструкциям мастера.

## 25.2. Сканирование не начинается

Неисправности такого типа могут возникать вследствие двух основных причин:

- **Установленная ранее версия Bitdefender, которая не была удалена полностью, или некорректно установленная версия Bitdefender.**

В этом случае переустановите Bitdefender:

- **В Windows 7:**

1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
2. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
3. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- **В Windows 8 и Windows 8.1:**

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- **В Windows 10:**

1. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.



2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.



## Замечание

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие параметры могут быть переключены обратно в конфигурацию 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?»* (р. 77).
2. Переустановите Bitdefender:

### ● В Windows 7:

- a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
- b. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
- c. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
- d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

### ● В Windows 8 и Windows 8.1:

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



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

- b. Нажмите **Удалить программу** или **Программы и компоненты**.
  - c. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
  - d. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
  - e. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- В **Windows 10**:
- a. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.
  - b. Нажмите иконку **Система** в области **Настройки**, затем выберите **Установленные приложения**.
  - c. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
  - d. Нажмите **Удалить** снова, чтобы подтвердить выбор.
  - e. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
  - f. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.



## Замечание

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие параметры могут быть переключены обратно в конфигурацию по умолчанию.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе [«Обращение за помощью»](#) (р. 180).

## 25.3. 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 эта функция основана на эвристической системе, могут быть случаи, когда легальные приложения распознаются Активным контролем угроз как вирусы.

При возникновении такой ситуации можно исключить соответствующее приложение из мониторинга с помощью Активного контроля угроз.

Чтобы добавить программу в список исключений:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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»* (р. 180).


## 25.4. 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 Интерфейс**.
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»* (р. 180).


## 25.5. 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 защищаемых файлов, оно будет считаться небезопасным, 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 Интерфейс**.
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.

## 25.6. Обновление Bitdefender при низкой скорости подключения к Интернету

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

Чтобы поддерживать систему в актуальном состоянии с помощью новейших сигнатур вредоносных программ Bitdefender:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
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.

## 25.7. Службы Bitdefender не отвечают

Эта статья поможет устранить неполадки **Bitdefender Службы не отвечают**. Эта ошибка может возникнуть следующим образом:

- Значок Bitdefender в **области уведомления** отображается серым цветом, информируя о том, что службы Bitdefender не отвечают.

- Окно Bitdefender указывает, что службы Bitdefender не отвечают.

Ошибка может быть вызвана одним из следующих условий:

- 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?»* (р. 77).

Если ошибка продолжает возникать, свяжитесь с нашей службой поддержки, как описано в разделе *«Обращение за помощью»* (р. 180).

## 25.8. Функция "Автозаполнение" в Кошельке не работает

Вы сохранили свои учетные данные в вашем Менеджере Паролей Bitdefender и обратили внимание, что автозаполнение не работает. Обычно эта проблема возникает, когда расширение Bitdefender Кошелек в вашем браузере не установлено.

Для того, чтобы устранить эту проблему, выполните следующие действия:

- В **Internet Explorer**:
  1. Откройте Internet Explorer.
  2. Нажмите Инструменты
  3. Нажмите кнопку Управление надстройками.
  4. Щелкните Панели инструментов и Расширения.
  5. Наведите указатель мыши на **Bitdefender Кошелек** и нажмите **Включить**.





## ● В Mozilla Firefox:

1. Открыть Mozilla Firefox.
2. Нажмите Инструменты
3. Нажмите кнопку дополнения.
4. Нажмите кнопку расширения.
5. Наведите указатель мыши на **Bitdefender Кошелек** и нажмите **Включить**.

## ● В Google Chrome:

1. Открыть Google Chrome.
2. Перейдите к значку меню.
3. Нажмите кнопку Дополнительные инструменты.
4. Нажмите кнопку расширения.
5. Наведите указатель мыши на **Bitdefender Кошелек** и нажмите **Включить**.



### Замечание

Надстройка будет включена после перезагрузки веб-браузера.

Теперь проверьте, работает ли функция автозаполнения в Кошельке для вашей учетной записи в интернете.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (р. 180).

## 25.9. Сбой удаления Bitdefender

Если вы хотите удалить продукт Bitdefender и заметили, что процесс или система зависают, нажмите **Отмена**, чтобы прервать действие. Если это не помогло, перезапустите систему.

При сбое удаления некоторые ключи и файлы Bitdefender могут оставаться в системе. Такие остатки могут препятствовать новой установке Bitdefender. Также они могут повлиять на производительность и стабильность системы.

Для того, чтобы полностью удалить Bitdefender из вашей системы:



## ● В Windows 7:

1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
2. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
3. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

## ● В Windows 8 и Windows 8.1:

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

## ● В Windows 10:

1. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.
2. Нажмите иконку **Система** в области **Настройки**, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.



## 25.10. Моя система не загружается после установки Bitdefender

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

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

Любую ситуацию можно разрешить следующим образом:

### ● Вы использовали Bitdefender ранее и не удалили продукт корректно.

Чтобы решить эту проблему:

1. Перезагрузите систему и запустите Безопасный режим. Инструкции для этой процедуры см. в *«Как перезагрузить компьютер в безопасном режиме?»* (р. 78).
2. Удалите Bitdefender из системы:

#### ● В Windows 7:

- a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
- b. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
- c. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
- d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- e. Перезагрузите систему в обычном режиме.

#### ● В Windows 8 и Windows 8.1:

- a. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
- b. Нажмите **Удалить программу** или **Программы и компоненты**.
- c. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.



- d. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
- e. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- f. Перезагрузите систему в обычном режиме.

● В **Windows 10**:

- a. Нажмите **Пуск**, а затем нажмите кнопку **Параметры**.
- b. Нажмите иконку **Система** в области **Настройки**, затем выберите **Установленные приложения**.
- c. Найдите из списка **Bitdefender Antivirus Plus 2018** и выберите **Удалить**.
- d. Нажмите **Удалить** снова, чтобы подтвердить выбор.
- e. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
- f. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- g. Перезагрузите систему в обычном режиме.

3. Заново установите продукт Bitdefender.

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

Чтобы решить эту проблему:

1. Перезагрузите систему и запустите **Безопасный режим**. Инструкции для этой процедуры см. в *«Как перезагрузить компьютер в безопасном режиме?»* (р. 78).
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**, а затем нажмите кнопку **Параметры**.
- 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?»* (р. 78).
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»* (р. 180).



## 26. УДАЛЕНИЕ ВРЕДНОСНОГО 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)»* (р. 168)
- *«Действия в случае обнаружения Bitdefender вирусов на компьютере»* (р. 173)
- *«Как удалить вирус из архива?»* (р. 174)
- *«Как очистить от вирусов архив электронной почты?»* (р. 175)
- *«Что делать, если имеются подозрения в том, что файл является опасным?»* (р. 177)
- *«Что представляют собой защищенные паролями файлы в журнале сканирования?»* (р. 177)
- *«Поиск пропущенных элементов в журнале сканирования»* (р. 178)
- *«Поиск файлов с избыточным сжатием в журнале сканирования.»* (р. 178)
- *«Почему Bitdefender автоматически удалил зараженный файл?»* (р. 178)

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»* (р. 180).

### 26.1. Bitdefender Режим Восстановления (Rescue Environment в Windows 10)

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




После того, как Bitdefender Antivirus Plus 2018 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 Среда спасения интегрирована с Windows RE, то есть нет необходимости загружать любой Режим восстановления в этой операционной системе, и эта функция не может быть использована при возникновении проблем с запуском. Чтобы очистить систему перед загрузкой служб Windows, рекомендуется использовать загрузочный компакт-диск Bitdefender.

Bitdefender Rescue CD - это бесплатный инструмент, который сканирует и очищает ваш компьютер всякий раз, когда вы подозреваете, что угроза вредоносных программ влияет на его работу. Полезные статьи, содержащие сведения о создании и использовании, доступны на платформе центра поддержки Bitdefender в <http://www.bitdefender.com/support/consumer.html>.

## Загрузка изображения Bitdefender Режим 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 Интерфейс**.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Режим Восстановления**.
4. Нажмите **ДА** в окне подтверждения, которое появляется для перезагрузки компьютера.

Подождите, пока файл изображения Режим спасения Bitdefender не 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 Режим 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 Спасения 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 Интерфейс**.
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 ВосстановленияBitdefender будет запущен через несколько минут.

## ● В Windows 8 и Windows 8.1:

1. Нажимайте клавишу **F8** , пока не появится экран **Расширенные параметры запуска**.
2. Выберите опцию **Использовать другую операционную систему**, затем Bitdefender Режим Восстановления.

Режим ВосстановленияBitdefender будет запущен через несколько минут.




## Замечание

Можно загрузить Ваш компьютер в Режиме Восстановления только в том случае, если файл изображения Режима Восстановления был загружен ранее, как описано в «[Загрузка изображения Bitdefender Режима Восстановления](#)» (р. 169).

## Запуск системы в Среде восстановления в Windows 10

Вход в Среду восстановления возможен только с ВашегоBitdefender продукта, как показано ниже:

1. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
2. Нажмите ссылку **ПРОСМОТРЕТЬ ФУНКЦИИ**.
3. В области **АНТИВИРУС** нажмите **Среда восстановления**.
4. Нажмите кнопку **Перезагрузить** в появившемся окне.

Bitdefender Среда восстановления загрузится через несколько минут.

## Сканирование системы в Режиме восстановления (Среда восстановления в Windows 10)

Сканировать систему в Режиме Восстановления (Среда Восстановления):

- В Windows 7, Windows 8 и Windows 8.1:



1. Перейдите в Режим восстановления, как описано в разделе «**Запуск системы в Режиме Спасения в Windows 7, Windows 8 и Windows 8.1**» (р. 170).
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 Антивирусное сканирование по запросу".
6. Нажмите **Сканировать сейчас**, выберите цель сканирования в появившемся окне, а затем нажмите **Открыть**, чтобы начать сканирование.

Рекомендуется выполнить сканирование всего раздела Windows.



## Замечание

При работе в Режиме восстановления 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 Режиме восстановления щелкните правой кнопкой мыши в пустой области рабочего стола, выберите в появившемся меню **Выход**, затем выберите перезагрузку или выключение компьютера.

## ● В Windows 10:

1. Перейдите в Среду восстановления, как описано в «**Запуск системы в Среде восстановления в Windows 10**» (р. 171)
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.

## 26.2. Действия в случае обнаружения Bitdefender вирусов на компьютере

Обнаружить в компьютере вирус можно одним из следующих способов:

- Выполнено сканирование компьютера. Bitdefender обнаружил зараженные элементы.
- Оповещение о вирусе сообщает о блокировке Bitdefender одного или нескольких вирусов, проникших в компьютер.

В таких ситуациях обновите Bitdefender, чтобы убедиться, что у вас есть последние сигнатуры вредоносных программ, и запустите сканирование системы для анализа.



Как только сканирование системы будет закончено, выберите нужное действие для инфицированных элементов (лечить, удалить, переместить в карантин).

### **Внимание**

Если вы считаете, что этот файл является частью операционной системы Windows, или сомневаетесь в том, что файл заражен вирусом, выполните следующие действия и как можно скорее свяжитесь со службой поддержки клиентов Bitdefender.

Если выбранное действие не может быть выполнено и в журнале сканирования отображаются сведения об обнаруженном вирусе, который невозможно удалить, необходимо удалить файл(ы) вручную:

**Первый метод можно использовать в нормальном режиме:**

1. Отключите антивирусную защиту Bitdefender в режиме реального времени:
  - a. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
  - 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?»* (р. 76).
3. Перейдите в папку, где находится зараженный файл (проверьте журнал сканирования), и удалите этот файл.
4. Включите 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?»* (р. 78).
2. Отображать скрытые объекты в Windows. Инструкции для этой процедуры см. в *«Как отобразить скрытые объекты в Windows?»* (р. 76).
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»* (р. 180).

## **26.3. Как удалить вирус из архива?**

Архив представляет собой файл или набор файлов, сжатых в специальном формате в целях уменьшения пространства на диске, требуемого для хранения файлов.



Некоторые из этих форматов являются открытыми, что дает Bitdefender возможность просканировать их изнутри и выполнить после этого соответствующие действия для их удаления.

Другие форматы архивов являются частично или полностью закрытыми. Bitdefender может только обнаруживать присутствие в них вирусов, не выполняя каких-либо дополнительных действий.

В тех случаях, когда Bitdefender выводит уведомление об обнаружении вируса в архиве, не предлагая доступных действий, это означает, что удаление вируса невозможно из-за ограничений, установленных для параметров разрешений архива.

Удалить вирус из архива можно следующим образом:



1. Определите архив, который включает в себя вирус посредством проверки системы.
2. Отключите антивирусную защиту Bitdefender в режиме реального времени:
  - a. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
  - 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»* (р. 180).



## 26.4. Как очистить от вирусов архив электронной почты?

Bitdefender также может идентифицировать вирусы в базах данных электронной почты и архивах электронной почты, хранящихся 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. Отключите антивирусную защиту Bitdefender в режиме реального времени:
  - a. Нажмите на  иконку в нижнем левом углу **Bitdefender Интерфейс**.
  - 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 используйте идентификационную информацию (subject, from, to) зараженных сообщений, чтобы найти их в почтовом клиенте.
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. Включите 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»** (р. 180).



## 26.5. Что делать, если имеются подозрения в том, что файл является опасным?

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

Чтобы убедиться, что ваша система защищена:

1. Запустите **Сканирование системы** с помощью Bitdefender. Инструкции для этой процедуры см. в *«Как выполнить сканирование системы?»* (р. 64).
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»* (р. 180).

## 26.6. Что представляют собой защищенные паролем 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.





## 26.7. Поиск пропущенных элементов в журнале сканирования

Все файлы, отображаемые в отчете о сканировании с пометкой "Пропущено", не заражены.

В целях улучшения производительности Bitdefender не сканирует файлы, которые не были изменены с момента выполнения последнего сканирования.

## 26.8. Поиск файлов с избыточным сжатием в журнале сканирования.

Элементами с чрезмерным сжатием называются те элементы, которые сканер не может извлечь, либо элементы, дешифрование которых занимает слишком много времени, в результате чего система становится нестабильной.

"Чрезмерное сжатие" означает то, что Bitdefender пропустил этот архив при сканировании, поскольку для его распаковки потребовался бы слишком большой объем системных ресурсов. При необходимости содержимое будет сканироваться в режиме реального времени.

## 26.9. Почему Bitdefender автоматически удалил зараженный файл?

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

Для 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.



**СВЯЖИТЕСЬ С НАМИ**



## 27. ОБРАЩЕНИЕ ЗА ПОМОЩЬЮ

Bitdefender предоставляет своим клиентам беспрецедентный уровень быстрой и точной поддержки. Если вы испытываете какие-либо проблемы, или если у вас есть какие-либо вопросы о продукте Bitdefender, вы можете использовать несколько Интернет-ресурсов, чтобы найти решение или ответ. Также вы можете обратиться в службу поддержки Bitdefender. Наши представители службы поддержки своевременно ответят на ваши вопросы и окажут необходимую помощь.

В разделе *«Решение распространенных проблем»* (р. 153) предоставляет необходимую информацию о наиболее частых проблемах, с которыми вы можете столкнуться при использовании данного продукта.


Если вы не найдете ответ на свой вопрос в предоставленных ресурсах, то вы можете обратиться непосредственно к нам:

- *«Свяжитесь с нами через интерфейс Bitdefender»* (р. 180)
- *«Свяжитесь с нами через онлайн-центр поддержки»* (р. 181)

## 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 Интерфейс**.
2. Для выбора доступны следующие параметры:

- **РУКОВОДСТВО**

Доступ к нашей базе данных и поиск необходимой информации.

- **ЦЕНТР ПОДДЕРЖКИ**

Доступ к статьям и видео-урокам.

- **СВЯЗАТЬСЯ СО СЛУЖБОЙ ПОДДЕРЖКИ**

Нажмите кнопку **ОБРАТИТЬСЯ В СЛУЖБУ ПОДДЕРЖКИ**, для запуска средства поддержки Bitdefender и обратитесь в Отдел обслуживания клиентов.



- a. Заполните форму отправки, указав необходимые данные:
  - i. Выберите тип возникшей проблемы.
  - 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 **Закрыть**, чтобы выйти из мастера. С Вами свяжется в кратчайшие сроки 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 <http://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 **Поиск**.

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.html> и свяжитесь с нашими представителями поддержки.



## 28. ОНЛАЙН-РЕСУРСЫ

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

- Центр поддержки Bitdefender:  
<http://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.

### 28.1. 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

<http://www.bitdefender.com/support/consumer.html>.



## 28.2. 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 **Дом & Защита Дома Офиса**, раздел, посвященный потребительским товарам.

## 28.3. 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>.



## 29. КОНТАКТНАЯ ИНФОРМАЦИЯ

Эффективное взаимодействие с клиентами является ключом к успешному бизнесу. 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. Если у вас есть какие-либо вопросы, не стесняйтесь обращаться к нам.

### 29.1. Веб-адреса

Отдел продаж: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Центр поддержки: <http://www.bitdefender.com/support/consumer.html>

Документация: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)

Местные дистрибьюторы: <https://www.bitdefender.com/partners>

Партнерская программа: [partners@bitdefender.com](mailto:partners@bitdefender.com)

Отдел по связям со СМИ: [pr@bitdefender.com](mailto:pr@bitdefender.com)

Вакансии: [jobs@bitdefender.com](mailto:jobs@bitdefender.com)

Отправка вирусов: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)

Отправка спама: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)

Жалобы: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)

Сайт: <http://www.bitdefender.ru>

### 29.2. Местные дистрибьюторы

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

Поиск дистрибьютора 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 вы не нашли дистрибьютора Bitdefender в вашей стране, вы можете связаться с нами по электронной почте по адресу [sales@bitdefender.com](mailto:sales@bitdefender.com). Указывайте адрес электронной почты на английском языке, чтобы мы смогли своевременно обработать ваш вопрос.





## 29.3. 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](mailto: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](mailto:info@bitdefender.co.uk)

Телефон: (+44) 2036 080 456

Продажи: [sales@bitdefender.co.uk](mailto: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](mailto: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](mailto: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](mailto: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](mailto:mena-sales@bitdefender.com)

Техническая

поддержка:

<https://www.bitdefender.com/support/consumer.html>



Сайт: <https://www.bitdefender.com>



## Глоссарий

### ActiveX

ActiveX является моделью для написания программ, чтобы другие программы и операционная система могли вызывать их. Технология ActiveX используется вместе с программой Microsoft Internet Explorer для создания интерактивных страниц, которые выглядят и работают скорее как компьютерные программы, нежели как простые страницы. С помощью ActiveX пользователь может задавать и отвечать на вопросы, «нажимать» на кнопки и другим способом взаимодействовать с веб-страницей. Элементы ActiveX чаще всего пишутся на языке Visual Basic.

Главный недостаток технологии ActiveX – полное отсутствие какой-либо защиты. Поэтому эксперты по компьютерной безопасности не одобряют ее использование в сети Интернет.

### IP-адрес

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

### Java апплет

Java-программа, предназначенная для запуска только на веб-странице. 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, он не может считывать или записывать данные на этот компьютер. Кроме того, апплеты могут считывать и записывать данные только с того домена, которым они обслуживаются.

### Архив

Диск, лента или каталог, содержащие резервные копии файлов.



Файл, содержащий один или несколько файлов в сжатом формате.

## **Ботнет**

Термин «ботнет» состоит из слов «робот» и «сеть». Ботнеты - это устройства, подключенные к Интернету и зараженные вредоносными программами, они используются для отправки спам-писем, кражи данных, удаленного управления уязвимыми устройствами или для распространения программ-шпионов, вымогателей и других видов вредоносного ПО. Их цель - заразить как можно больше подключенных устройств, таких как ПК, серверы, мобильные или IoT-устройства, принадлежащие крупным компаниям или отраслям.

## **Браузер**

Веб-браузер – программное приложение, используемое для поиска и отображения веб-страниц. Популярными браузерами являются Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. Это графические браузеры, что означает, что они могут отображать графику, а также текст. Кроме того, большинство современных браузеров могут отображать мультимедийную информацию, включая звук и видео-изображения, хотя некоторые из них требуют установки дополнительных расширений.

## **Виртуальная частная сеть (VPN)**

Это технология, которая позволяет временное и зашифрованное прямое подключение к определенной сети через менее безопасную сеть. Таким образом, отправка и получение данных являются безопасными и зашифрованными действиями, которые не поддаются перехвату. 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 работает с гибкими дисками.

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

## **Загрузка**

Копирование данных (обычно целых файлов) из основного местоположения на внешнее устройство. Этот термин часто используется для описания процесса копирования файла из Интернет-службы на свой компьютер. Загрузка также может означать 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.) Для загрузочных дисков загрузочный сектор также содержит программу, которая загружает 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**

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**

Это уникальный ключ, который можно купить в розницу и использовать для активации определенного продукта или услуги. Код активации включает активацию действительной подписки на определенный период времени и число устройств, а также может использоваться для продления подписки с условием, которое будет сгенерировано для того же продукта или услуги.



## **Командная строка**

В интерфейсе командной строки пользователь вводит команды в пространстве, предоставляемом непосредственно на экране с помощью языка команд.

## **Лазейки в системе**

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**

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 (системный трей)**

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 для замены устаревшей версии этого продукта. Кроме того, многие обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет – обновление невозможно.

У Bitdefender есть свой собственный модуль обновления, который позволяет вручную проверять наличие или автоматически обновлять программный продукт.

## **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.

## **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.

## **Почтовый клиент**

Клиент электронной почты - это приложение, которое позволяет отправлять и получать электронную почту.

## **Программа-шпион**

Любого рода программа-шпион, которая тайно и без ведома пользователя - чаще всего в рекламных целях - собирает информацию о пользователе во время его соединения с сетью Интернет. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать из сети Интернет, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в сети Интернет, к которым обращается пользователь, и тайно пересылает эту информацию третьим лицам. Программы-шпионы могут собирать информацию об адресах электронной почты, паролях и номерах кредитных карт.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионов обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионов являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти и ресурсов канала соединения с сетью Интернет, за счет передачи информации программой-шпионом своему источнику при подключении пользователя к сети Интернет. За счет потребления



памяти и системных ресурсов программами-шпионами, работа последних в фоновом режиме может приводить к неустойчивой работе системы и ее сбоям.

## **Протокол TCP/IP**

Протокол управления передачей/интернет-протокол (Transmission Control Protocol/Internet Protocol) – набор сетевых протоколов, широко используемых в сети Интернет. Они объединяют в одну большую сеть множество взаимосвязанных сетей, состоящих из компьютеров с различной архитектурой и с различными операционными системами. Протокол TCP/IP включает в себя стандарты связи между компьютерами, общепринятые правила объединения сетей и маршрутизации трафика.

## **Путь**

Точное расположение файла на компьютере. Это местоположение обычно описывается средствами иерархической файловой системы сверху вниз.

Маршрут между двумя объектами, например, канал связи между двумя компьютерами.

## **Развитая устойчивая угроза**

Развитая устойчивая угроза (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 развитой устойчивой угрозы - оставаться незамеченными в течение длительного времени с возможностью мониторинга и собора важной информации, не повреждая целевые машины. Метод, используемый для введения вируса в сеть - запуск через PDF файл или документ Office, которые выглядят безвредными настолько, что любой пользователь может запустить данные файлы.

## **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 программу, содержащую рекламное ПО. 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, собранная 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 периферийных устройств, если их встроить в соответствующее программное обеспечение.

По своей природе руткиты не являются вредоносным ПО. 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**

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопкой мыши, или нажатие клавиши, или системные события, например, переполнение памяти.

## **Спам**

"Мусорная" электронная почта или "мусорная" новостная рассылка. Более известна как нежелательная электронная почта.

## **Сценарий**

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

## **Троян**

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от 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 ворота, 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 Интернет-индустрии cookies описаны как небольшие файлы, содержащие информацию об отдельных компьютерах, которые могут быть проанализированы и использованы рекламодателями для отслеживания ваших приоритетов и вкусов. 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», аналогично тому, как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

## **Фишинг**

Это действие, заключающееся в отправке пользователю электронного письма, якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации, которая будет использоваться для кражи личных данных. В получаемом сообщении электронной почты пользователя, с помощью вложенной ссылки, приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные (например, пароли и номера банковских счетов, кредитной карточки, карточки социального обеспечения). На самом деле такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

## **Фотон**

Фотон является инновационной ненавязчивой технологией Bitdefender, предназначенной для минимизации влияния антивирусной защиты на производительность. Контролируя деятельность вашего компьютера в фоновом режиме, он создает



модели использования, которые помогают оптимизировать загрузку и сканирование процессов.

## **Червь**

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

## **Эвристический анализ**

Метод определения новых вирусов на основе правил. 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».

## **Эл. почта**

Электронная почта. Сервис, отправляющий сообщения на другие компьютеры через локальную или глобальную сеть.

## **Элементы запуска**

Все файлы, помещенные в эту папку будут открываться при запуске компьютера. 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.