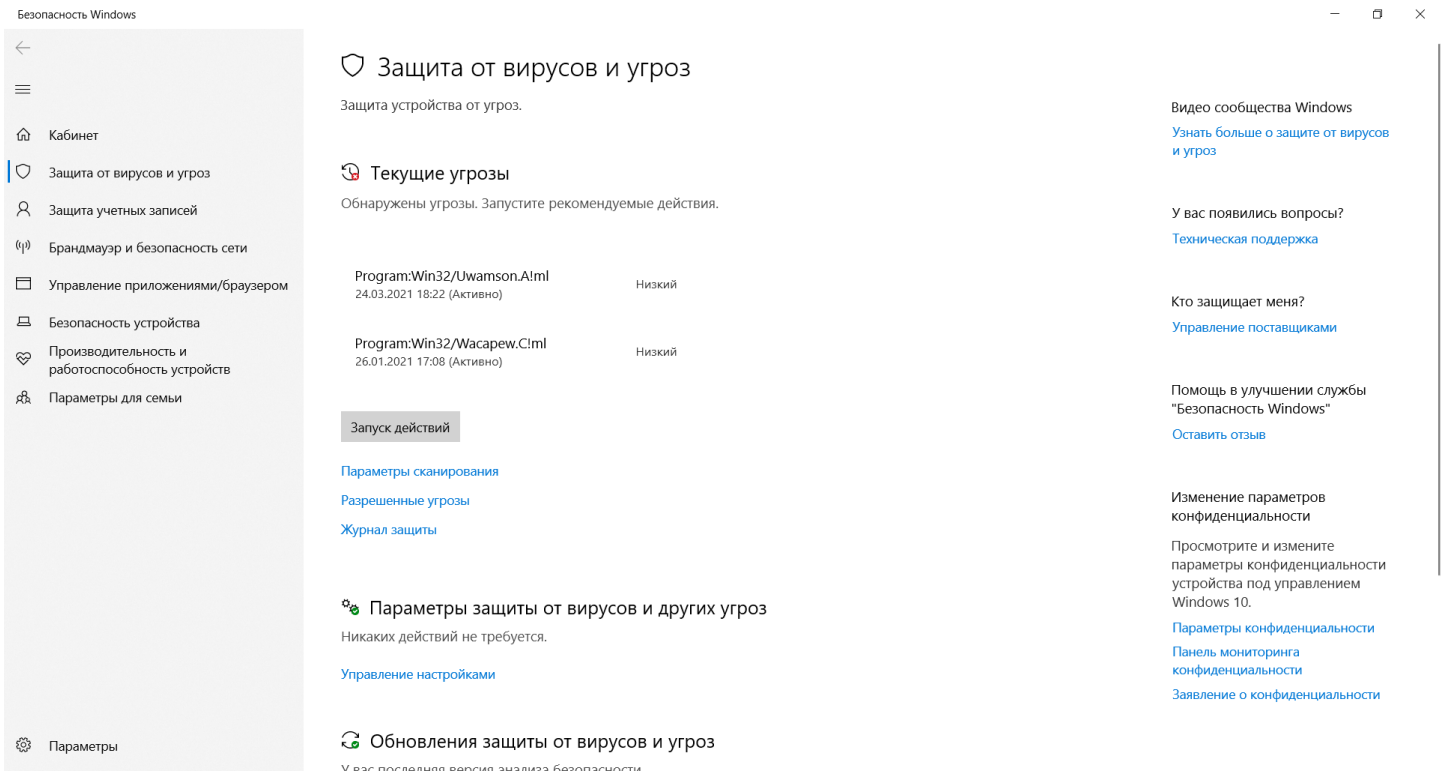
Как правильно настроить Защитник Windows

Операционные системы Windows поставляются со встроенным ПО для защиты от вирусов, шифровальщиков и эксплойтов. Также оно выполняет функции брандмауэра и родительского контроля. Технически все выполнено в виде всего одной утилиты под названием «Центр безопасности Защитника Windows».

Назначение Защитника Windows

Приложение обновляется по схеме, схожей с антивирусными программами, и не требует установки в систему, как это часто бывает с продуктами сторонних разработчиков. Большую часть времени его интерфейс скрыт от пользователя – нет всем надоевших значков в трее, защита работает прозрачно и автоматически блокирует потенциальные угрозы.



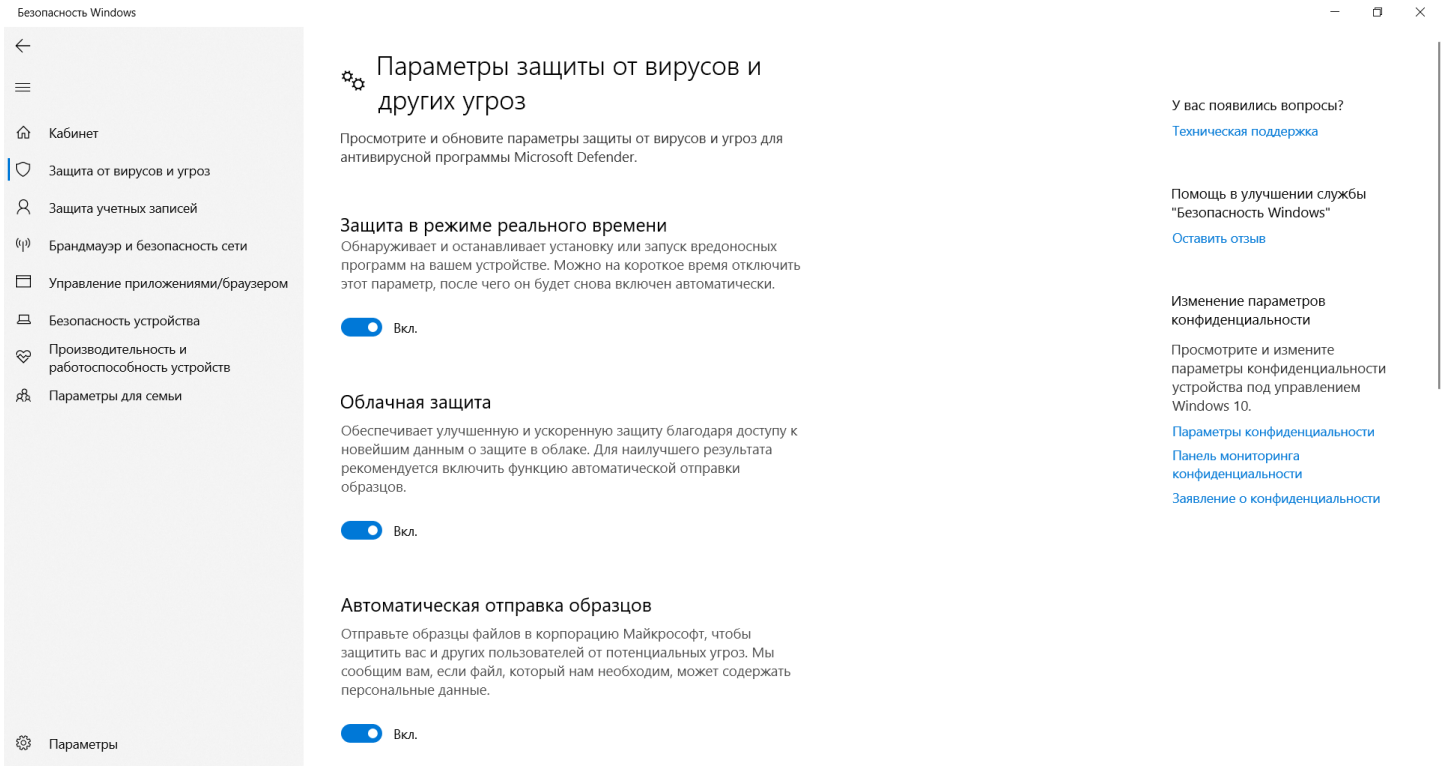
Особенности Защитника:

1. Обновление программы происходит через «Центр обновления Windows».
2. Эвристический анализ осуществляется с подключением к облачному серверу Microsoft.
3. Возможен ручной запуск проверки накопителей или отдельных файлов.

Чтобы открыть программу, достаточно в поиске Windows (комбинация клавиш <Win+S>) ввести фразу «защитник». И уже в процессе ввода система покажет ярлык нужного приложения, которое запускается для ручного управления настройками. Брандмауэр и антивирус «по умолчанию» имеют отдельные интерфейсы, хотя возможен быстрый переход между ними через левое меню.

Настройка компонента «Защита от вирусов и угроз»

При инсталляции операционной системы Windows все типы защиты подключаются автоматически, и в большинстве случаев настройки остаются в значении «по умолчанию» на весь период службы ПК. При необходимости есть возможность временно отключить антивирусный модуль или изменить параметры проверки файлов, а также подключить контролируемый доступ к папкам.



Последовательность действий:

1. Открыть окно «Защита от вирусов и угроз» через поиск Windows.
2. Выбрать пункт «Управление настройками» в разделе «Параметры защиты от вирусов и других угроз».
3. Отключить нужные функции или перейти в окно для настройки соответствующих функций вроде параметров уведомлений или добавления исключений.

Изменения принимаются автоматически и не требуют перезагрузки компьютера. Важно понимать, что при заражении компьютерным вирусом в период, когда антивирус неактивен, он останется на компьютере до тех пор, пока повторно включенный модуль не «наткнется» на него, например, при запуске инфицированной программы.

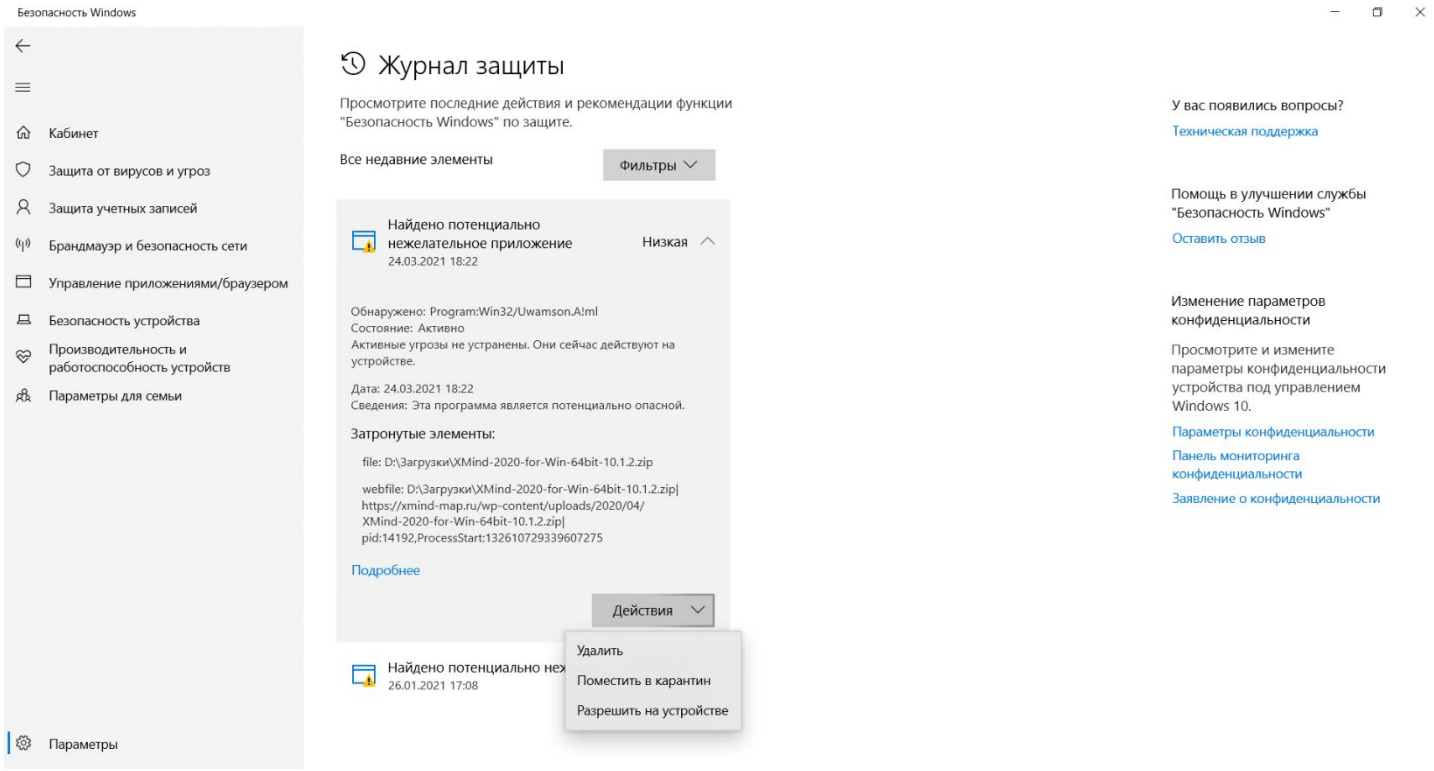
Небольшие пояснения по основным настройкам:

1. **Защита в режиме реального времени.** Сканирование всех типов файлов, открываемых при использовании компьютера.
2. **Облачная защита.** Система подключается к удаленному серверу для снижения нагрузки на локальное «железо».
3. **Автоматическая отправка образцов.** Передает подозрительные файлы службе поддержки Microsoft для изучения и выработки наилучшей защиты от новых угроз.

Встроенный антивирус неплохо «соседствует» с продуктами сторонних разработчиков. Иногда стороннее ПО при инсталляции автоматически отключает интегрированные функции, если их параллельная работа будет нестабильной. В большинстве случаев от пользователя не требуется ничего изменять вручную, инсталляторы сторонних антивирусов все выполняют самостоятельно.

История сканирования и угрозы, перенесенные в карантин

При обнаружении (хотя бы потенциально) опасного файла операционная система перемещает его в отдельный каталог (карантин). Там он огражден от случайного запуска, поэтому компьютер не заразится, даже если в код действительно проник вирус. Хранится такой архив в течение трех месяцев, после чего удаляется, минуя корзину.



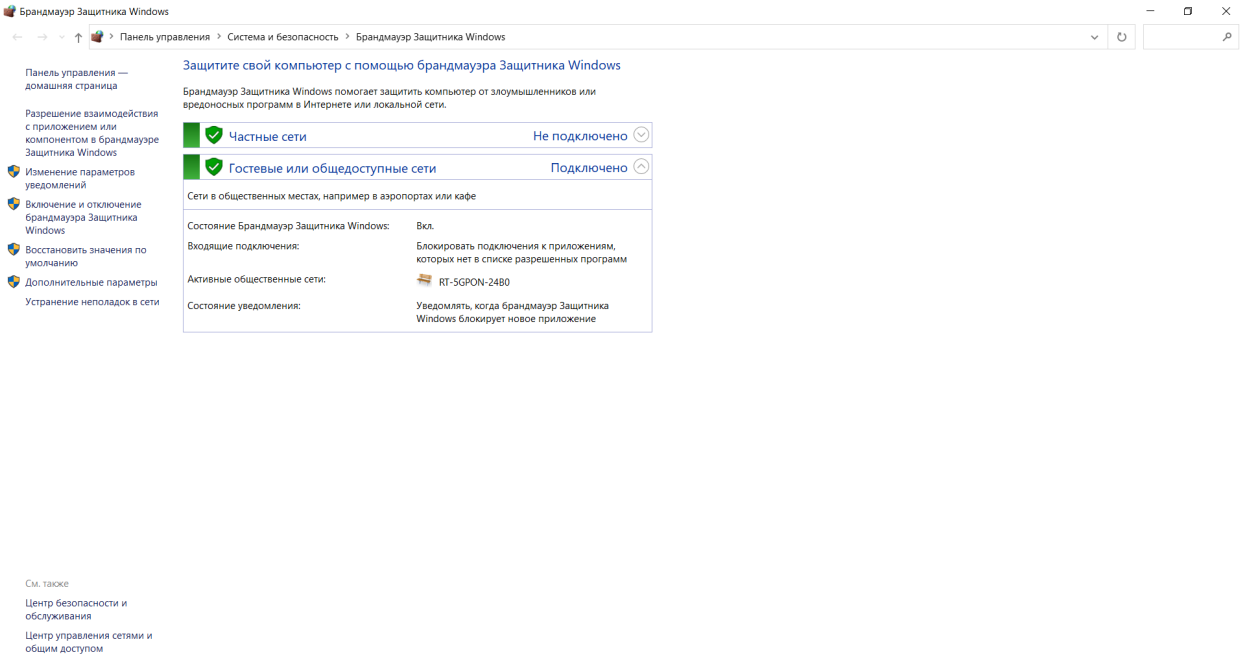
Последовательность действий при открытии журнала:

1. Запустить модуль «Защита от вирусов и угроз».
2. Выбрать пункт «Журнал защиты» и кликнуть по нему.
3. Просмотреть список угроз и указать действие для каждой.

Возможно ручное удаление, перенос в «карантин», если этого еще не было сделано, и отключение контроля конкретного файла. Последнее часто необходимо, если запускается программа, взятая из сети, например, игра с торрента. Предлагаемые действия обычно выбираются сразу, при обнаружении угрозы.

Брандмауэр и безопасности сети

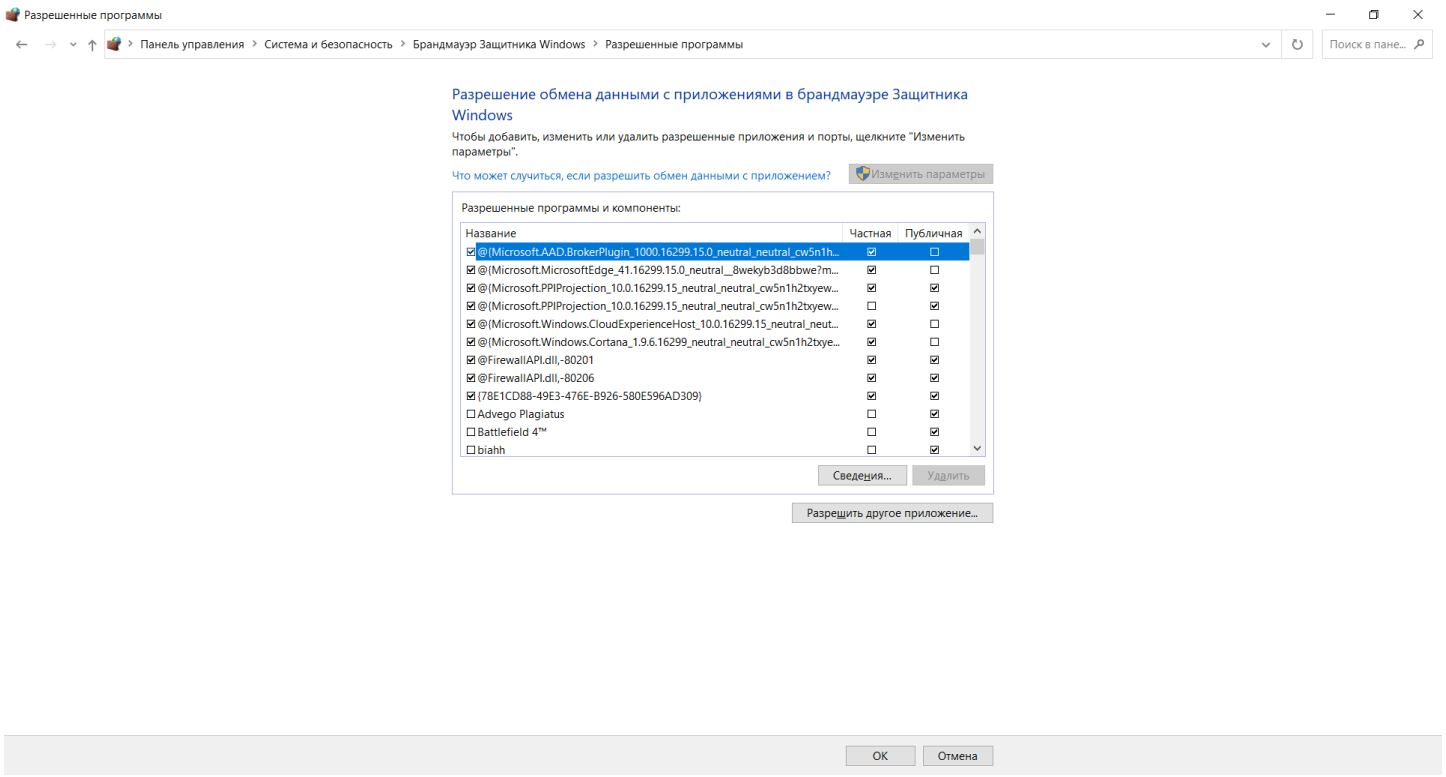
Брандмауэр представляет собой отдельный модуль, предназначенный для защиты от хакерских атак вроде несанкционированного удаленного подключения к компьютеру. Модуль раздельно работает по каждому соединению – проводному и Wi-Fi. В интерфейсе так же, как и в антивирусном блоке, есть возможность временного отключения функций.



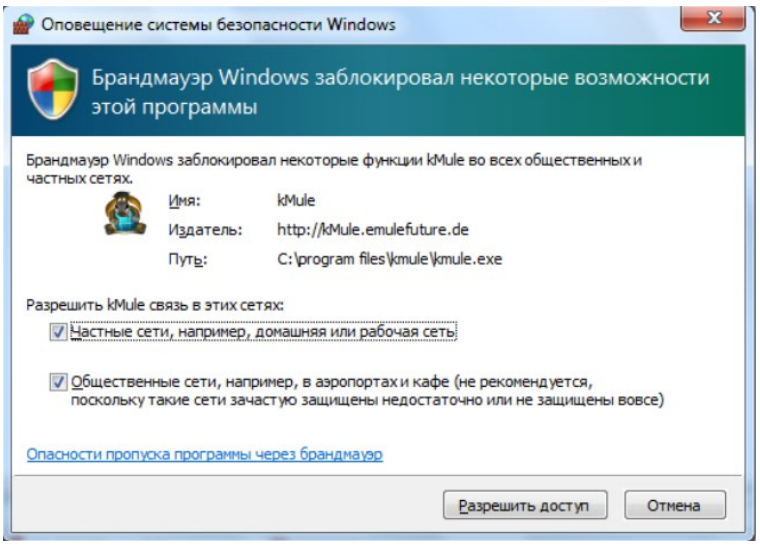
Последовательность управления:

1. Открыть окно «Брандмауэр Защитника Windows» через поиск.
2. Перейти в раздел «Включение и отключение брандмауэра Защитника Windows».
3. Выбрать желаемый режим работы защитного приложения по каждой сети отдельно.

Именно в этом окне настраивается перечень программ, которым разрешено выходить в интернет. Выполняется изменение параметров в пункте меню «Разрешение взаимодействия с приложением или компонентом в брандмауэре Защитника Windows». Владельцу компьютера рекомендуется периодически просматривать список и удалять незнакомые пункты.

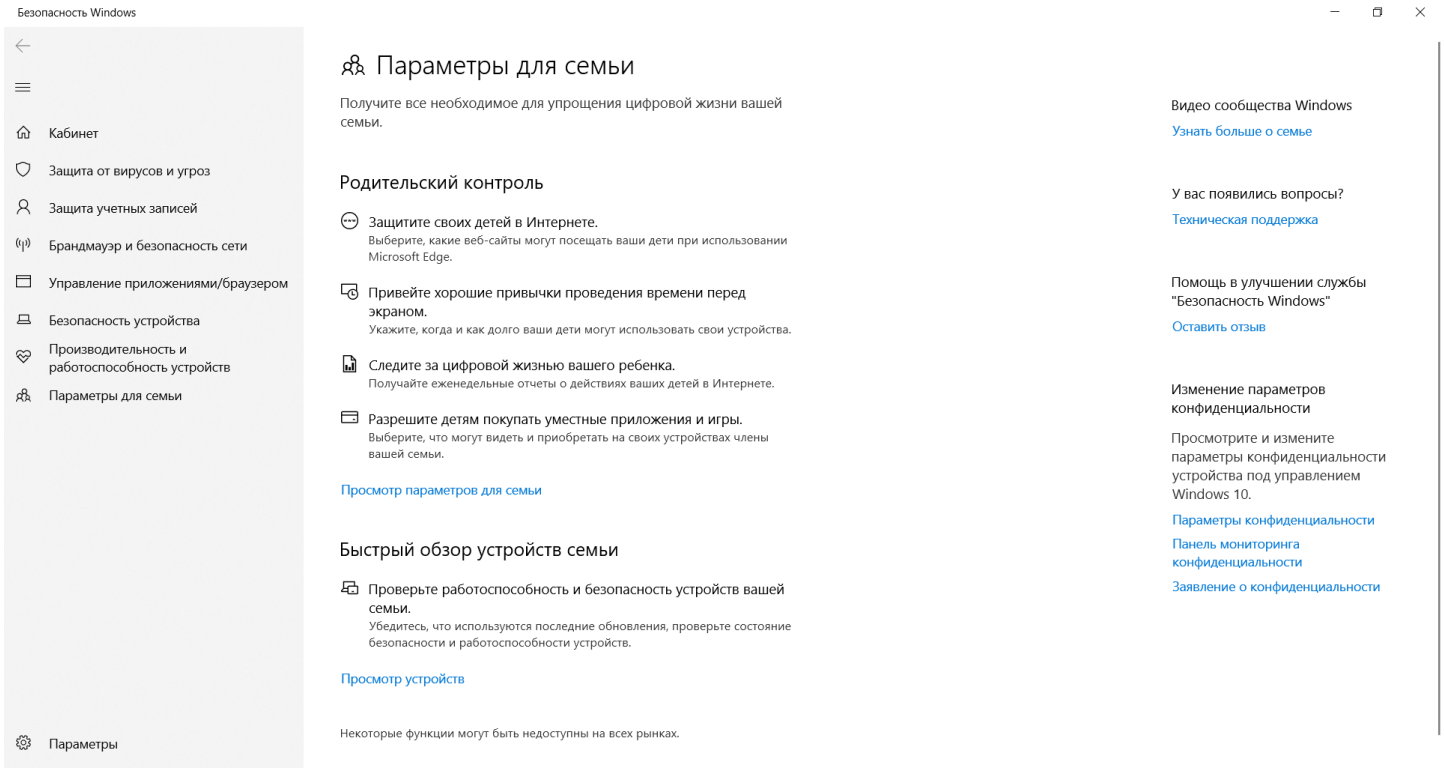


По умолчанию в сеть выпускаются все службы Windows и модули устанавливаемых программ, если в них при установке не был обнаружен вредоносный код. Игры обычно при первом запуске выдают запрос на разрешение доступа. Предоставлять его или нет, зависит от пользователя. Если никаких действий он не осуществляет, считается, что выходить в сеть разрешено.



Параметры для семьи

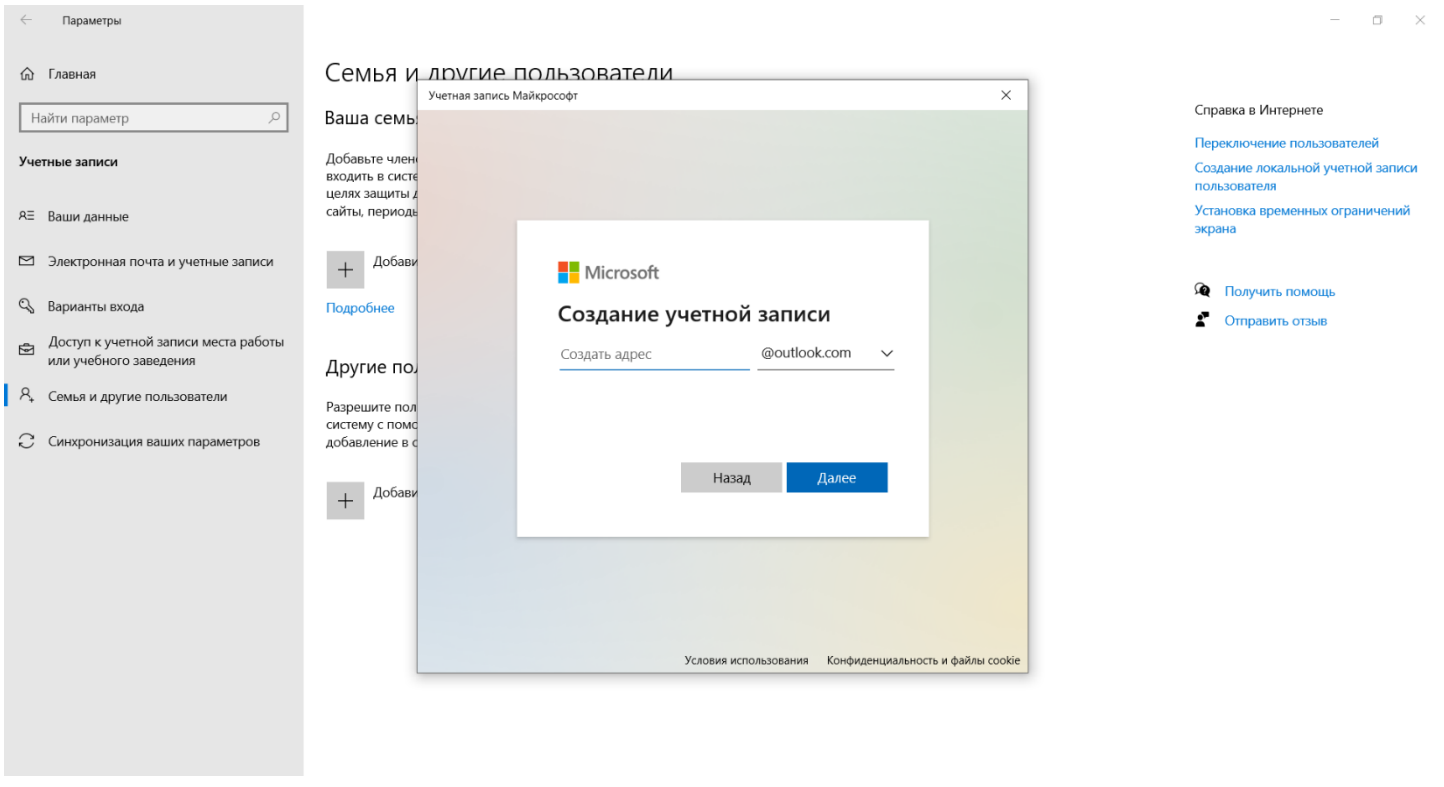
Модуль «Параметры для семьи» доступен, как и предыдущие, через поиск Windows. Это наиболее простой запуск настройки ограничений доступа в сеть для детей. Здесь же имеется доступ к истории посещений, счетчик времени, проведенного в интернете, перечень скачанных приложений, видео и другого мультимедийного контента.



Чтобы защита начала работать, нужно создать отдельный аккаунт для ребенка:

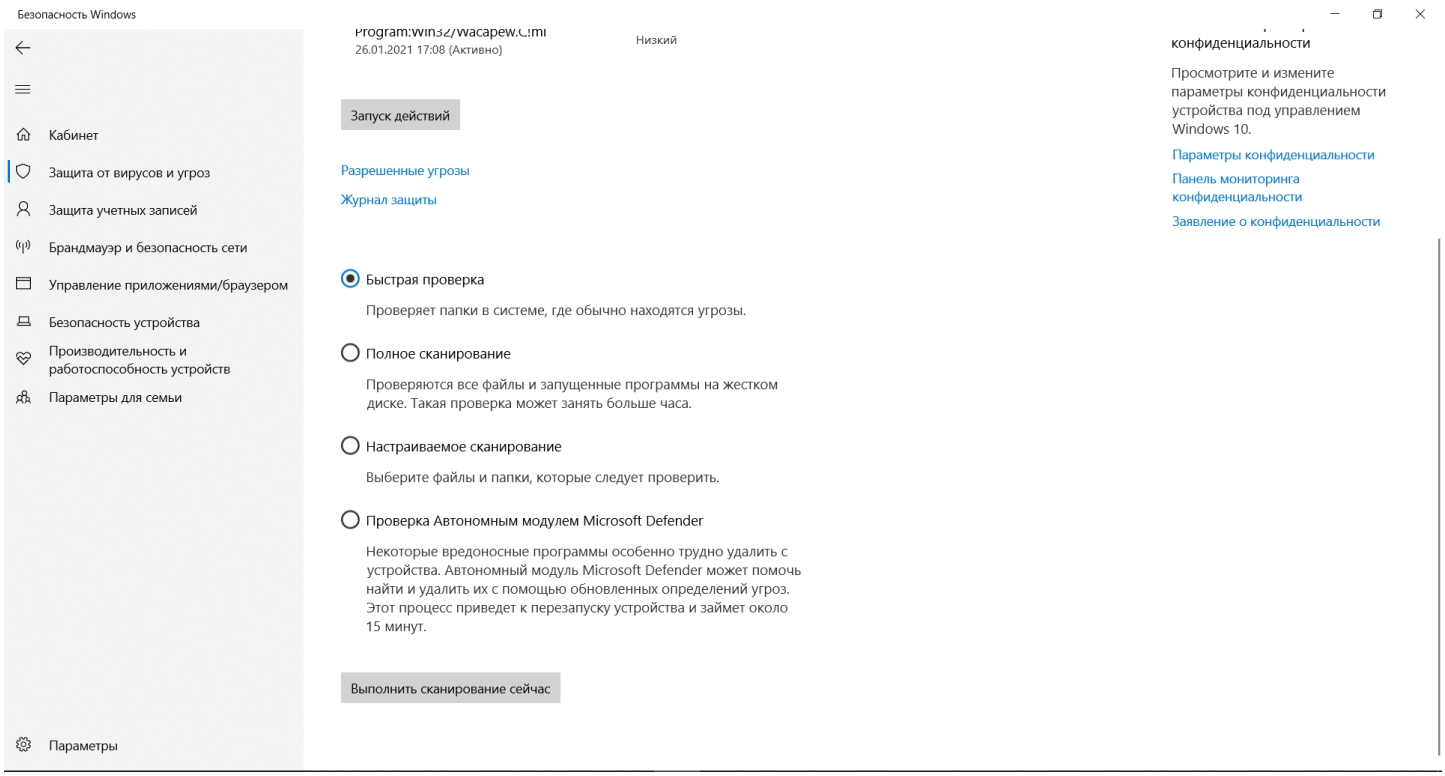
1. Открыть приложение «Параметры» через поиск Windows (комбинацией клавиш <Win+S>).
2. Выбрать пункт «Учетные записи», в котором нужно перейти в раздел «Семья и другие пользователи».
3. Нажать «Добавить члена семьи» и при запросе указать пункт «Создать для ребенка».

В идеале необходимо добавить аккаунт каждого, кто будет работать на компьютере. И в дальнейшем следить, чтобы все заходили в операционную систему под своей учетной записью. Система отчасти сложная, поэтому ее применяют редко – очень уж она похожа на систему безопасности в офисах. Домашние же ПК в основном приобретают для развлечений, а кому хочется что-то усложнять?



Принудительное сканирование

Если компьютер некоторое время работал с отключенной защитой, и у него появились симптомы заражения компьютерным вирусом, рекомендуется провести «ручную» проверку ПК. Процесс запускается в окне «Защита от вирусов и угроз». Для этого в главном окне выбирается пункт «Параметры сканирования».



Затем нужно выбрать режим (быструю или полную проверку) и нажать на кнопку «Выполнить сканирование сейчас». В отдельных случаях рекомендуется использовать автономный модуль Microsoft Defender или ручной выбор папок для антивирусной проверки. Последнее востребовано для только что скачанных файлов и при подключении внешних носителей.

Полное сканирование обычно продолжается несколько часов – все зависит от количества файлов на компьютере. Поэтому большинство пользователей ограничиваются защитой в режиме реального времени, ведь она выявляет те же угрозы, что и принудительная проверка. К тому же многие привыкли ко встроенному Защитнику и всегда оставляют его включенным.

Полностью отключать Защитник, не имея платного антивируса на руках, ни в коем случае не рекомендуется.