avast! Internet Security 6.0

Краткое руководство "Начало работы"

Вас приветствует avast! Internet Security 6.0

Антивирусная программа avast! 6.0 во многом повторяет нашу предыдущую, очень успешную версию 5.0 и при этом включает ряд новых функций и усовершенствований, таких как avast! Auto-Sandbox ("автоматическая песочница") и поддержка 32- и 64-разрядных операционных систем. avast! Internet Security предназначен для индивидуальных пользователей, малых/домашних офисов и малых предприятий. Корпоративным пользователям и более крупным организациям мы рекомендуем использовать наши продукты, предполагающие централизованное управление – как и рассматриваемая здесь версия, они продаются на веб-сайте avast!.

Программа avast! Internet Security, работа которой основывается на отмеченном рядом наград антивирусном ядре avast!, включает технологию для защиты от "шпионских программ", сертифицированную West Coast Labs Checkmark, модуль защиты от руткитов и надежный модуль самозащиты. А последняя версия обеспечивает еще более высокую скорость сканирования и усовершенствованную функцию обнаружения вредоносных программ. Кроме того, программа avast! Internet Security 6.0 включает следующие функции:

- **avast! SafeZone** – это чистый рабочий стол, с которого вы можете проводить свои конфиденциальные операции в безопасной, защищенной среде.
- **Сканер командной строки** – возможность запускать сканирование еще до запуска системы.
- **Брандмауэр** – дополнительная защита от "хакеров".
- **Антиспамовый фильтр** – более полный контроль над электронной почтой.

Как у и всех антивирусных продуктов avast! 6.0, работа avast! Internet Security 6.0 основана на нескольких экранах в реальном времени, которые непрерывно отслеживают вашу электронную почту и соединения с Интернетом, а также проверяют файлы в вашем компьютере при каждом их открытии или закрытии. После установки программа avast! незаметно работает в фоновом режиме, защищая ваш компьютер от всех известных форм вредоносного программного обеспечения. Если все идет хорошо, вы даже не заметите, что avast! работает в вашей системе – установив программу, вы просто забудете о ней!

Расширенная справка

Руководство "Начало работы" представляет собой лишь краткий обзор программы и ее основных функций. Это руководство пользователя нельзя назвать полным. Более подробные сведения о программе и расширенные настройки программы см. в Центре справки, открыть который можно из интерфейса программы – или же просто нажмите клавишу F1, чтобы просмотреть справку для открытого в данный момент окна.

Если при пользовании антивирусной программой avast! у вас возникли какие-либо сложности, которые вы не можете устранить с помощью этого руководства или системы справки в программе, нужные ответы в можете получить в Центре технической поддержки на нашем веб-сайте **http://support.avast.com**.

- В разделе **Knowledgebase** содержатся ответы на некоторые наиболее распространенные вопросы.

- Можно также воспользоваться форумом технической поддержки avast! (avast! Support Forum). Здесь вы можете пообщаться с другими пользователями avast!, которые, возможно, уже сталкивались с вашей проблемой и знают ее решение. Для пользования форумом необходима регистрация, выполнить которую быстро и просто. Чтобы зарегистрироваться на форуме, перейдите на страницу **http://forum.avast.com/**.

Если и это не помогло вам решить проблему, перейдите по ссылке "**Submit a ticket**" для обращения в нашу службу технической поддержки. В этом случае вам также необходимо будет зарегистрироваться. Описывая нам свою проблему, постарайтесь указать как можно более подробную информацию.

Установка avast! Internet Security 6.0

На последующих страницах описано, как загрузить и установить avast! Internet Security 6.0 на вашем компьютере, а также как начать пользоваться программой после завершения загрузки и установки. Программу можно загрузить для бесплатного пользования в течение 30-дневного пробного периода, однако после этого необходимо приобрести лицензионный код. На последующих страницах вы увидите, как выглядят различные окна программы в операционной системе Windows XP – в других версиях Windows программа может иметь несколько иной вид.

Ниже перечислены минимальные рекомендуемые системные требования для установки и запуска avast! Internet Security 6.0:

- операционная система Microsoft Windows XP SP2 или выше (любой выпуск, 32- или 64-разр.), Microsoft Windows Vista (любой выпуск, 32- или 64-разр.) или Microsoft Windows 7 (любой выпуск, 32- или 64-разр.);
- Windows-совместимый компьютер с процессором Intel Pentium III или выше (в зависимости от требований используемой версии операционной системы и установленного ПО сторонних производителей);
- не менее 256 Мбайт оперативной памяти (в зависимости от требований используемой версии операционной системы и установленного ПО сторонних производителей);
- 370 Мбайт свободного места на жестком диске (для загрузки и установки программы);
- подключение к Интернету (для загрузки и регистрации продукта, а также для автоматического обновления программы и антивирусной базы данных);
- оптимальное разрешение экрана – не менее 1024 x 768 пикселов.

Обратите внимание, что программа не предназначена для использования в серверной операционной системе (на серверах Windows NT/2000/2003).

Шаг 1. Загрузите avast! Internet Security 5.с веб-сайта www.avast.com

Настоятельно рекомендуется перед началом скачивания закрыть все прочие программы Windows.

Нажмите "Скачать", затем "Скачать программы" и выберите avast! Internet Security.

Если вы используете веб-браузер Internet Explorer, на экране отобразится следующее окно:

После того, как вы нажмете кнопку "Запустить" или "Сохранить", начнется загрузка установочного файла на ваш компьютер.

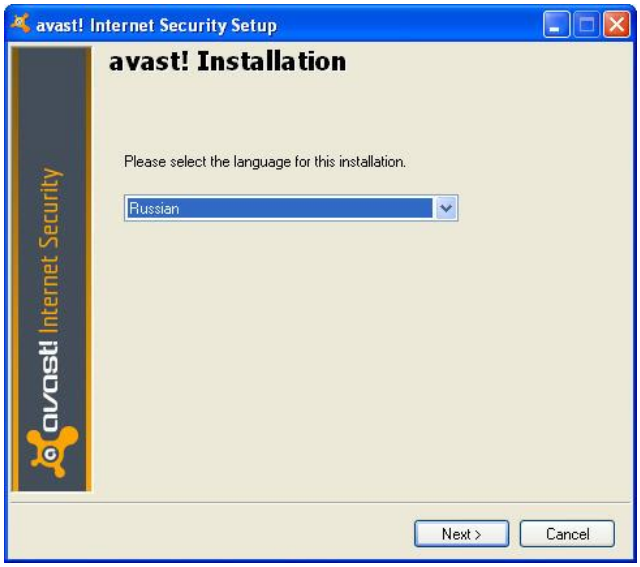
Если вы хотите установить avast! Internet Security 6.0 сразу после загрузки установочного файла, нажмите "Запустить".

Возможно, в других веб-браузерах вам будет предложен только один вариант – "Сохранить" файл. Если нажать кнопку "Сохранить", программа avast! будет загружена на ваш компьютер, однако ее установка не начнется автоматически. Чтобы завершить процесс установки, вам понадобится запустить установочный файл вручную, поэтому запомните, в какой папке вы его сохранили!

Шаг 2. Установите avast! Internet Security 6.0 на компьютере

Чтобы установить avast! Internet Security 6.0 на компьютере, необходимо запустить установочный файл. После запуска установочного файла (для этого нажмите кнопку "Запустить", как это указано выше, или дважды щелкните файл, сохраненный на вашем компьютере), отобразится следующее окно:

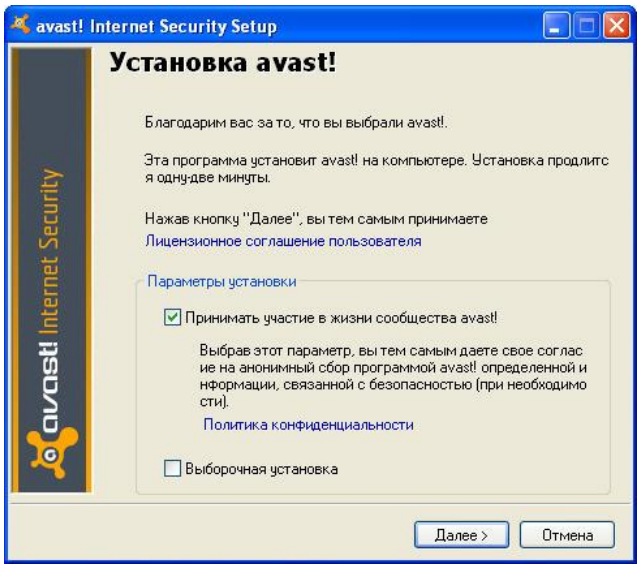
После того, как вы нажмете кнопку "Выполнить", откроется экран установки avast!:



В выпадающем меню выберите нужный язык установки (например, русский – "Russian") и нажмите кнопку "Next" (Далее).

На следующем экране вы можете указать, хотите ли вы принимать участие в деятельности сообщества avast!.

Сила программы avast! в том, что обеспечиваемая ею защита основана на общем опыте более 100 миллионов пользователей во всем мире. Участвуя в жизни сообщества avast!, вы тем самым помогаете нам и в будущем обеспечивать наилучшую возможную защиту для всех пользователей.



Если вы согласитесь принять участие в деятельности сообщества, avast! будет автоматически собирать информацию о новых угрозах сразу после их появления и с соблюдением анонимности передавать эту информацию в компанию Avast Software.

Программой собирается только информация о новых вирусах и файлах, поведение которых является подозрительным. Собранная информация анализируется и используется для совершенствования защиты, которую avast! предоставляет своим пользователям во всем мире.

Вся информация передается в Avast Software с соблюдением анонимности – никакие личные данные программой не собираются. Если вы не желаете участвовать в деятельности сообщества, просто снимите соответствующий флажок – в этом случае никакая информация передаваться не будет.

Дополнительные сведения см. в документе "Политика конфиденциальности avast!", ознакомиться с которым можно, перейдя по ссылке на экране.

На этом экране также можно настроить выборочную установку, однако мы рекомендуем использовать стандартную установку – для этого, не устанавливая флажок "Выборочная установка", нажмите кнопку "Далее".

На следующем шаге вы сможете выбрать один из двух вариантов – использовать программу в пробном режиме или указать действительную лицензию.

- Если вы хотите использовать программу в пробном режиме, вам необходимо будет подключение к Интернету, т.к. пробная лицензия будет автоматически загружена в ходе установки. Вы сможете ознакомиться с возможностями программы в течение пробного периода в 30 дней, однако если вы хотите пользоваться программой и далее, по истечении 30-дневного пробного периода вам необходимо будет указать полную действительную лицензию – см. следующую страницу.

- Если вы уже купили лицензию и сохранили ее на компьютере, с помощью кнопки "Обзор" перейдите в папку на компьютере, в которую вы сохранили файл лицензии. Щелкните по файлу, чтобы выбрать его, затем нажмите "Открыть", чтобы автоматически ввести файл лицензии в программу. После этого вы сможете без ограничений пользоваться программой до окончания срока действия лицензии.

- Если вы приобрели антивирусную программу avast! с кодом активации, вы можете ввести его здесь, чтобы активировать свою лицензию.

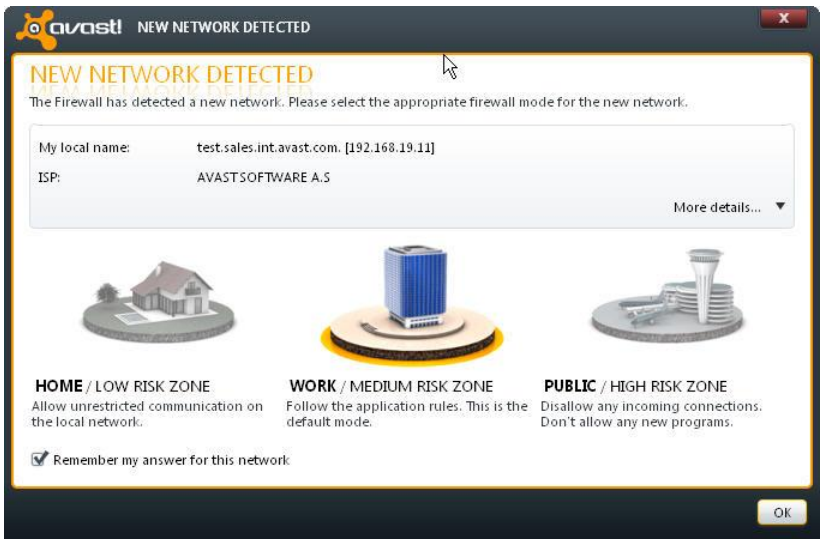
Для продолжения нажмите кнопку "Далее".

После завершения установки программа avast! выполнит быстрое сканирование вашего компьютера с целью проверки, все ли в порядке.

Когда вы увидите последний экран установки, это будет означать, что установка avast! успешно завершена. Нажмите "Готово".

После этого необходимо перезагрузить компьютер.

После перезагрузки вам будет предложено выбрать, какой режим брандмауэра следует использовать для вашей сети:



Выбрав один из трех доступных параметров, вы тем самым определите, какой режим обмена данными с другими внешними сетями разрешен для вашей сети.

Режим по умолчанию – "Работа / зона средней опасности". Это означает, что программа avast! сама будет определять, какие внешние подключения разрешены, а какие нет. Наиболее безопасный параметр – "Интернет", при котором блокируются все входящие данные. Можно также выбрать "Дом", при котором будет разрешен весь обмен данными. Поэтому данный режим рекомендуется использовать только в случае, когда вы используете компьютеры в локальной сети без внешних подключений (т.е. без подключения к Интернету). Перечисленные параметры подробно описываются далее в этом руководстве, в разделе "Брандмауэр".

На рабочем столе вы увидите оранжевый значок avast!, а в панели задач в правом нижнем углу экрана (рядом с часами) – оранжевый шарик avast!

Если вы используете ОС Windows Vista (или более позднюю версию) с боковой панелью, также отобразится значок боковой панели avast!. Этот значок отображает текущее состояние программы avast!. Если вам нужно быстро просканировать файлы, можно просто перетащить их на значок avast!.

Начало работы

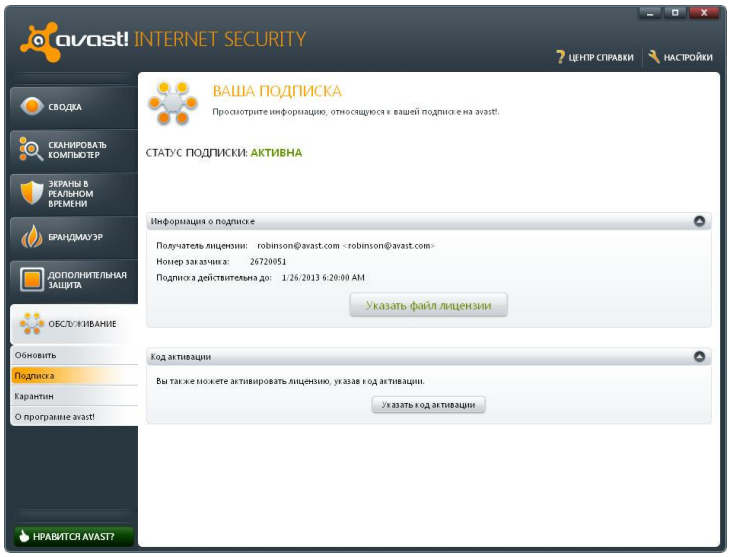
Программу можно использовать бесплатно в течение 30-дневного пробного периода. Однако если вы хотите пользоваться программой и по окончании пробного периода, необходимо приобрести лицензию и ввести ее в программе.

Лицензии на пакет avast! Internet Security для использования ПО дома или в небольшой домашней/учрежденческой сети можно приобрести на 1, 2 или 3 года и на 3, 5, или 10 компьютеров.

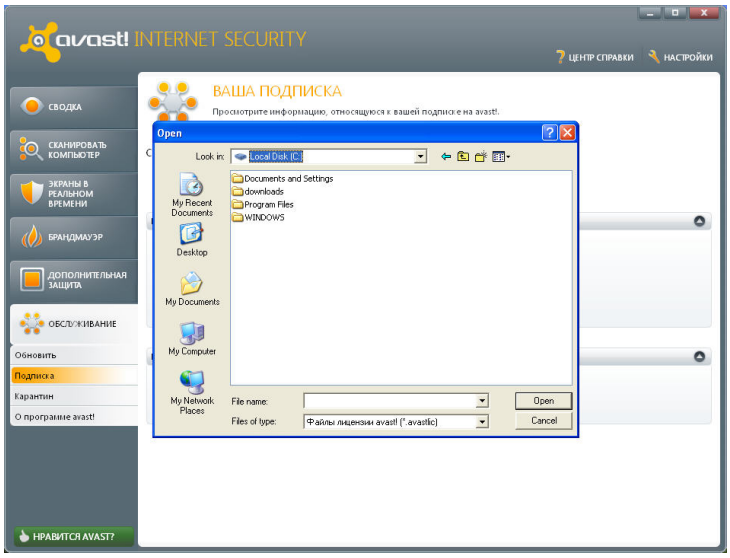
Корпоративным пользователям и более крупным организациям мы рекомендуем использовать наши продукты, которые предоставляют возможность централизованного управления всеми компьютерами в сети организации. Более подробные сведения о наших продуктах, предполагающих централизованное управление, см на веб-сайте www.avast.com.

Чтобы приобрести лицензию, перейдите на веб-сайт **www.avast.com** и щелкните вкладку "Купить" вверху экрана. Затем выберите "Решения для рабочих станций" и введите количество, тип и срок действия лицензий, которые вы хотите купить.

Получив файл лицензии, просто дважды щелкните его, и лицензия будет введена в программу автоматически. Можно также сохранить файл лицензии на компьютере, открыть интерфейс avast! и перейти на вкладку "Обслуживание". На этой вкладке выберите "Подписка" и нажмите "Указать файл лицензии".



Откроется новое окно, в котором вы сможете перейти к местоположению файла лицензии на компьютере.



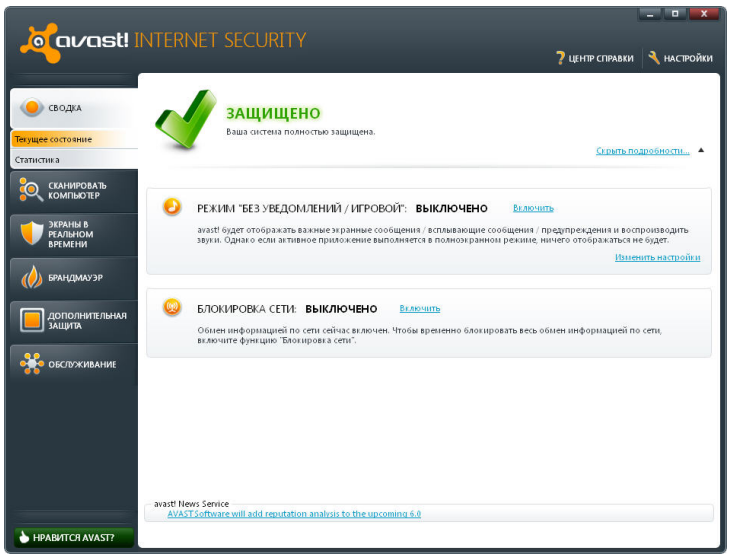
Перейдя в нужную папку, дважды щелкните файл лицензии, чтобы автоматически ввести его в программу.

Если вы приобрели множественную лицензию, позволяющую использовать программу на нескольких компьютерах, необходимо будет выполнить эту процедуру для каждого компьютера, на котором установлен avast! – скажем, вы можете переслать электронное письмо, в которое вложен лицензионный код, каждому пользователю, или же сохранить файл лицензии на общедоступном диске, USB-накопителе и т.п.

После ввода лицензии вы сможете регулярно получать автоматические обновления – а значит, ваш компьютер будет защищен от последних угроз.

Использование программы

Если открыть главное окно программы, вы увидите текущее состояние защиты вашего компьютера. Как правило, это окно будет иметь следующий вид:



Щелкнув "Подробности", вы выведете на экран подробные данные о текущем статусе программы и определениях вирусов.

Экраны в реальном времени

Как видно из названия, экраны в реальном времени защищают ваш компьютер от угроз в "режиме реального времени", т.е. в момент обнаружения этих угроз – поэтому состояние экранов в общем случае должно быть "Включено". Если какой-либо из экранов отключен, вы увидите состояние "Выключено". Чтобы вновь включить экраны, нажмите кнопку "Включить".

Брандмауэр

Брандмауэр отслеживает весь обмен информацией между вашим компьютером и внешним миром, предотвращая несанкционированный доступ. В общем случае вы увидите здесь состояние "Включено".

Версия определений вирусов

Здесь вы увидите текущую версию определений вирусов. По умолчанию эти определения обновляются автоматически. Если вы хотите выполнить обновление вручную, нажмите кнопку "Обновить". После этого вы сможете выбрать, хотите вы обновить только программу или программу и определения вирусов вместе.

Версия программы

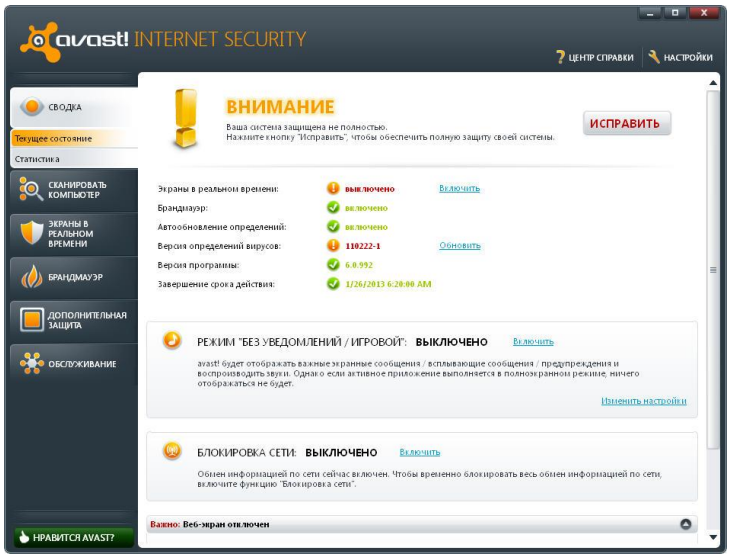
Здесь отображается текущая версия программы. Чтобы вручную выполнить обновление, нажмите "Обновить".

Автообновление определений

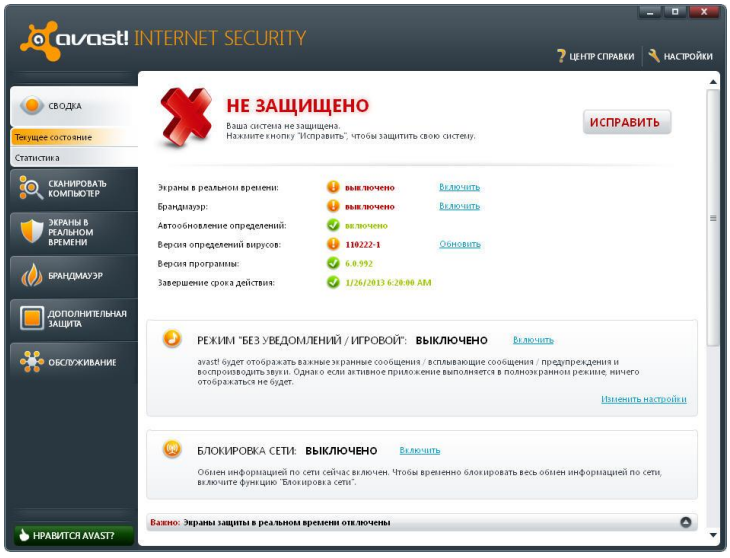
В общем случае вы увидите здесь состояние "Включено". В этом случае определения вирусов будут автоматически обновляться при каждом подключении

к Интернету. Чтобы включить или отключить эту функцию, нажмите "Изменить". Рекомендуется всегда использовать "Автоматическое обновление" модуля сканирования и определений вирусов.

Если главное окно выглядит, как на рисунке ниже, это обычно означает, что определения вирусов на вашем компьютере устарели, либо один или несколько экранов в реальном времени отключены. Чтобы исправить положение, нажмите кнопку "Исправить".



Состояние "Не защищено" означает, что все экраны в реальном времени отключены. Чтобы включить все экраны и полностью защитить компьютер, нажмите кнопку "Исправить". Можно также с помощью кнопок со стрелкой ВНИЗ в правой части экрана включить каждый экран отдельно.



Режим "Без уведомлений / Игровой"

Из основного окна программы также можно перейти к настройкам режима "Без уведомлений / Игровой". По умолчанию вы увидите здесь состояние "Выключено", при этом в полноэкранных приложениях не будут отображаться экранные сообщения. Нажав кнопку "Изменить настройки", вы можете указать, что экранные сообщения не следует отображать никогда (режим "Без уведомлений" включен), а можете полностью выключить режим "Без уведомлений / Игровой".

Блокировка сети

Блокировка сети позволяет временно отключить весь обмен данными через сеть. Эта функция полезна, когда вы работаете с секретными данными и хотите быть уверены, что к данным не может получить доступ никто другой, или когда вы по каким-либо причинам считаете, что ваш компьютер подвергается атакам извне. Включив блокировку сети, вы сделаете свой компьютер полностью недоступным из сети.

Подробнее об экранах в реальном времени

Экраны в реальном времени – это наиболее важные элементы программы, которые непрерывно защищают ваш компьютер от заражения вирусами. Они отслеживают все действия вашего компьютера, проверяя все программы и файлы в реальном времени – т.е. в момент запуска программы и открытия или закрытия файла.

Обычно экраны в реальном времени автоматически начинают работать при запуске компьютера. Присутствие оранжевого значка avast! в правом нижнем углу экрана вашего компьютера говорит о том, что экраны в реальном времени работают. Любой из экранов можно отключить, но делать это не рекомендуется, т.к. это может привести к снижению уровня защиты.

В состав антивируса avast! 6.0 входят следующие экраны в реальном времени:

Экран файловой системы – проверяет все программы в момент их запуска и все файлы в момент их открытия или закрытия. Если обнаружено что-то подозрительное, экран файловой системы не допустит запуска соответствующей программы или открытия файла, таким образом предотвратив потенциальный ущерб компьютеру и данным.

Экран почты – проверяет входящие и исходящие сообщения электронной почты, не позволяя получать и отправлять сообщения, которые, возможно, содержат вирусы.

Веб-экран – защищает ваш компьютер от вирусов при пользовании Интернетом (просмотре сайтов, загрузке файлов и т.п.), а также может блокировать доступ к зараженным веб-страницам. Если при загрузке файла из Интернета обнаружен вирус, загрузка будет остановлена. Таким образом, возможное заражение вашего компьютера будет предотвращено.

Экран P2P – проверяет файлы, загружаемые с помощью распространенных пиринговых программ (программ для обмена файлами).

Экран интернет-чатов – проверяет файлы, загружаемые программами для мгновенного обмена сообщениями через Интернет (ICQ и т.п.).

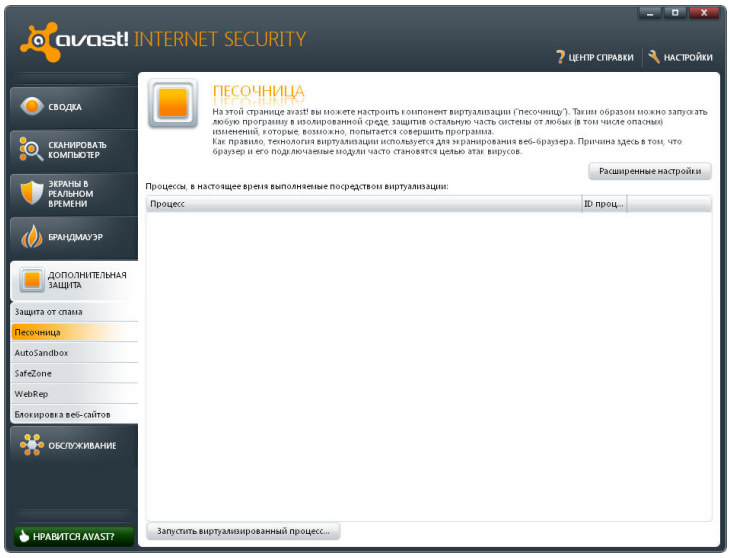
Сетевой экран – отслеживает всю сетевую активность и блокирует любые обнаруженные в сети угрозы. Этот экран также блокирует доступ к известным вредоносным веб-сайтам.

Экран поведения – отслеживает все действия в вашем компьютере, обнаруживая и блокируя любые нестандартные действия, которые могут указывать на присутствие вредоносного ПО. Этот экран непрерывно следит за входными каналами вашего компьютера, используя специальные датчики для выявления любых подозрительных действий.

Экран сценариев - отслеживает все сценарии, которые запускаются на компьютере – выполняемые как удаленно, например, при посещении интернет-сайтов, так и локально, при открытии файлов на компьютере.

Виртуализация процессов ("песочница")

Песочница avast! (Sandbox) позволяет заходить на веб-сайты или запускать другие приложения в полностью безопасной среде. Это особенно полезно при посещении (как случайном, так и намеренном) веб-сайтов, представляющих высокую опасность: браузер будет помещен в "песочницу", что позволит предотвратить любой ущерб вашему компьютеру.

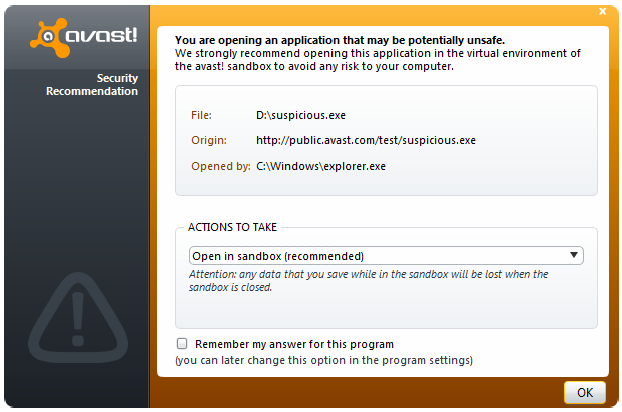


"Песочницу" также можно использовать для запуска любых других приложений, которые вы считаете подозрительными – вы можете запустить программу в песочнице, чтобы определить, представляет ли она опасность. При этом ваша система будет полностью защищена от любых вредоносных действий, которые, возможно, попытается выполнить эта программа.

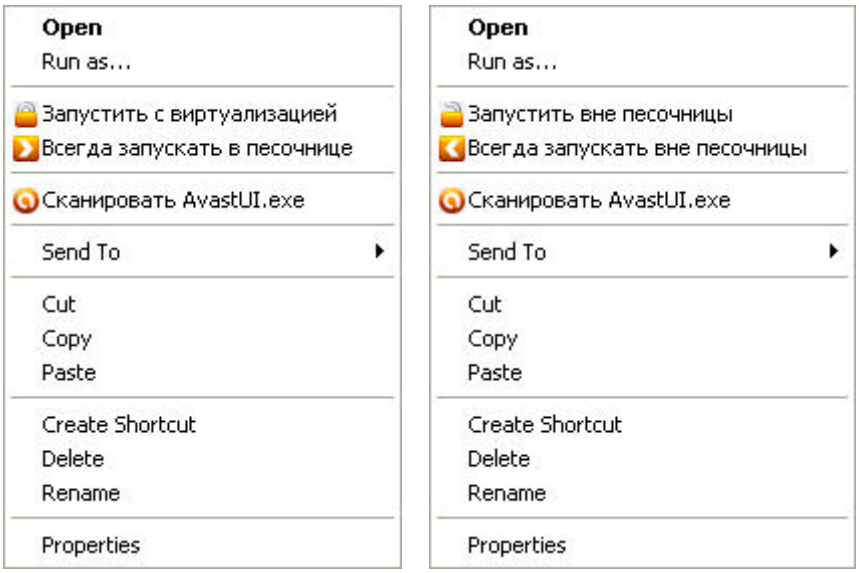
Чтобы запустить приложение или выйти в Интернет с использованием "песочницы", просто нажмите кнопку "Запустить виртуализированный процесс", затем перейдите к нужной программе на компьютере – например, к браузеру Internet Explorer. После этого браузер или другое приложение откроется в особом окне с красной каймой, которая указывает, что программа запущена в "песочнице".

В "Расширенных настройках" вы также можете задать приложения, которые всегда следует запускать в режиме виртуализации, и доверенные приложения, которые виртуализировать не надо.

Если при попытке запустить приложение avast! обнаруживает что-то подозрительное, вы увидите сообщение с вопросом, хотите ли вы запустить это приложение в песочнице.



Также можно запускать приложения в "песочнице", не открывая пользовательский интерфейс avast!. Для этого просто щелкните нужное приложение правой кнопкой мыши – откроется контекстное меню, изображенное внизу слева.



Чтобы запустить приложение в "песочнице", выберите пункт "Запустить с виртуализацией". Приложение откроется в окне с красной каймой. Чтобы приложение выполнялось в "песочнице" при каждом запуске, выберите пункт "Всегда запускать в песочнице".

Щелкнув правой кнопкой мыши приложение, уже помещенное в песочнице, вы откроете меню, изображенное сверху справа. В этом случае вы сможете однократно запустить приложение вне песочницы или полностью удалить его из песочницы, чтобы при каждом запуске оно выполнялось в обычной среде.

Виртуализация процессов (SafeZone)

avast! SafeZone – это дополнительная функция обеспечения безопасности, входящая в состав продуктов "Антивирус avast! Pro" и "avast! Internet Security". Эта функция позволяет просматривать веб-страницы из конфиденциального, надежно защищенного "кабинета", невидимого из остальной части системы. Например, если вы выполняете в Интернете банковские операции, покупки или другие операции, включающие передачу уязвимых данных, вы можете быть уверены, что ваши персональные данные не будут украдены шпионской программой или программой, считывающей вводимую с клавиатуры информацию.

В отличие от песочницы avast! (Sandbox), которая предназначена для безопасного хранения содержимого, способного нанести вред системе, avast! SafeZone нужна для того, чтобы не впускать ничего ненужного в ваш конфиденциальный "кабинет".

Чтобы открыть безопасный рабочий стол SafeZone, перейдите на вкладку "Дополнительная защита", затем откройте вкладку "SafeZone" и нажмите "Перейти в SafeZone".

При переходе в SafeZone автоматически запустится веб-браузер SafeZone. Браузер SafeZone – это специальный браузер, не содержащий дополнительных подключаемых модулей, которые нередко используются для распространения шпионских программ.

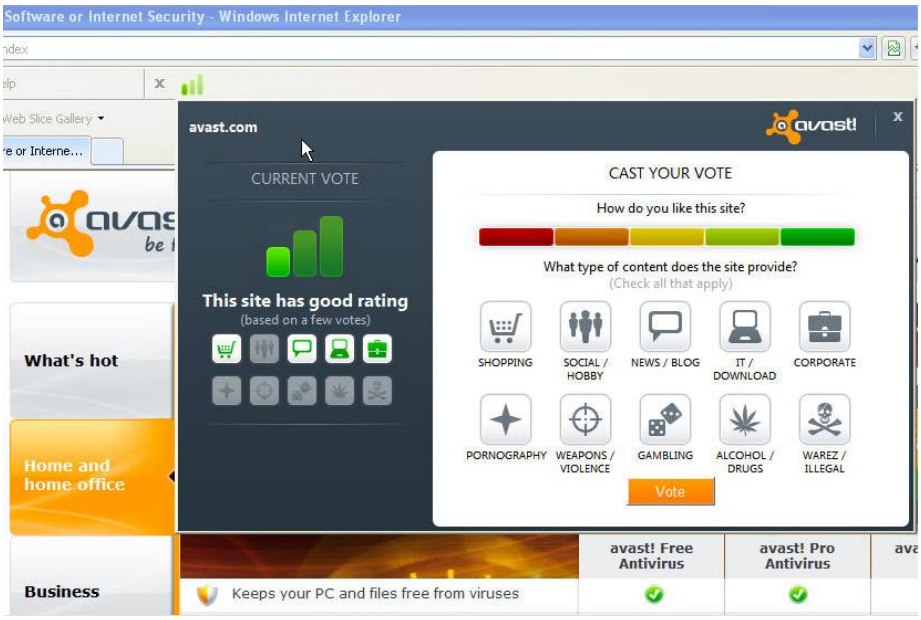
Закончив, войдите в меню "Пуск" и выберите "Отключить", чтобы закрыть браузер и вернуться к стандартному рабочему столу. Ваши настройки браузера и все файлы, которые вы загрузили, будут автоматически сохранены, и при следующем входе в SafeZone вы сможете открыть их. Если вы не хотите ничего сохранять, нажмите кнопку "Сбросить SafeZone", чтобы удалить все данные. Содержимое SafeZone, в том числе все настройки браузера, перейдет в первоначальное состояние.

avast! WebRep

avast! WebRep – это дополнительная функция, которая может быть установлена вместе с антивирусной программой avast!. Также можно установить эту функцию позже: для этого откройте интерфейс программы avast!, перейдите на вкладку "Дополнительная защита", выберите пункт "WebRep" и нажмите "Установить". В этом окне также можно перед установкой функции проверить, поддерживается ли ею ваш веб-браузер.

Функция WebRep использует полученную от всемирного сообщества пользователей avast! информацию, относящуюся к содержимому и степени безопасности посещаемых веб-сайтов, и снабжает пользователей полезными данными. Вы тоже можете внести свою лепту в работу этой функции, оценивая содержимое и степень безопасности веб-сайтов, которые вы посещаете – см. ниже.

При посещении того или иного веб-сайта вы увидите индикатор из трех полосок (красных, желтых или зеленых), показывающий, как другие пользователи оценивали этот веб-сайт. Такой же индикатор вы увидите напротив каждого из результатов поиска, полученных при использовании популярных поисковых систем.



Цвет индикатора сообщает вам, как другие пользователи оценили этот сайт – как "хороший" (зеленый), "средний" (желтый) или "плохой" (красный). Число подсвеченных полосок представляет надежность оценки. Одна, две или три подсвеченные полоски указывают соответственно на небольшое, среднее или большое число "голосов", поданных за этот сайт.

Если щелкнуть цветовой индикатор, откроется окно, в котором вы сможете просмотреть дополнительную информацию о системе оценки сайта, а также подать собственный голос.

Слева вы увидите общий рейтинг. Под рейтингом расположены значки меньшего размера, представляющие категории, к которым относится этот сайт.

Справа вы можете выставить сайту свою оценку. Здесь вы увидите разделенную на пять разноцветных сегментов полосу, с помощью которой можно дать домену более подробную оценку. Под полосой расположены все те же значки категорий. Щелкните один или несколько значков, чтобы отнести домен к категориям, которым он соответствует. Чтобы передать свою оценку в нашу базу данных, нажмите кнопку "Проголосовать".

Сканер командной строки

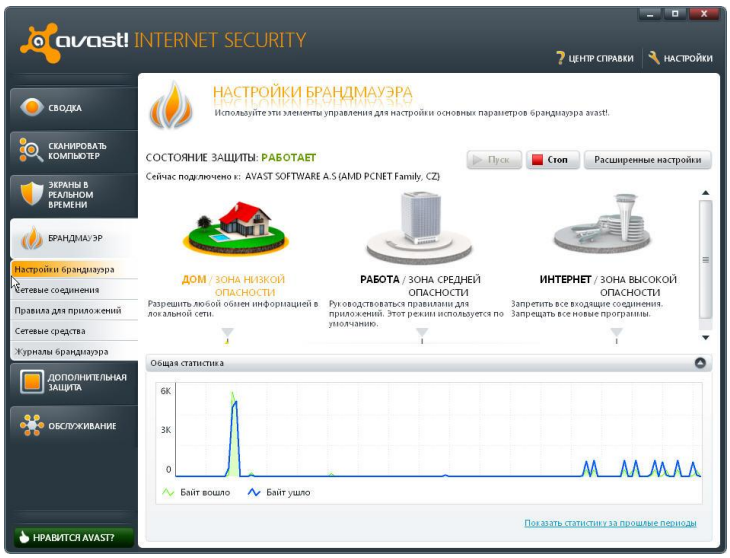
Сканер командной строки позволяет вручную запускать сканирование компьютера, не открывая интерфейс avast! – в том числе и до запуска операционной системы. Сканер командной строки использует для выявления потенциальных заражений вредоносным ПО те же модули сканирования avast!, что и стандартный интерфейс программы, так что результаты сканирования при ее использовании будут точно такими же. Сканер командной строки avast! – ashCmd.exe – обычно устанавливается в каталог C:\Program Files\AVAST Software\Avast.

Сканирование запускается из командной строки с применением различных ключей и параметров. Для просмотра описания этих параметров найдите файл ashCmd и дважды щелкните по нему. Откроется новое окно с описанием возможных параметров программы. Список параметров также можно найти в справке avast!.

Брандмауэр

Пакет avast! Internet Security включает полностью интегрированный брандмауэр, управлять которым можно прямо из пользовательского интерфейса avast!.

Брандмауэр отслеживает весь обмен информацией между вашим компьютером и внешним миром и блокирует неразрешенные действия, руководствуясь правилами "Разрешить" и "Запретить". Таким образом брандмауэр предотвращает утечку уязвимых данных с вашего компьютера, а также блокирует попытки взлома вашей системы со стороны интернет-хакеров.



В этом окне вы можете отрегулировать настройки защиты брандмауэром, задав ограничения для внешних подключений в соответствии с тем, в какой среде используется компьютер.

Существует три уровня защиты:

- **Дом / зона низкой опасности** – рекомендуется при использовании компьютера в домашней или частной сети. Если выбран этот уровень, брандмауэр допускает обмен любыми данными в сети.
- **Работа / зона средней опасности** – рекомендуется применять, когда компьютер подключен к более широкой общедоступной сети, а также может напрямую подключаться к Интернету. Этот уровень используется по умолчанию, на нем брандмауэр будет пропускать только те входящие и исходящие данные, которые разрешены "правилами для приложений". Если правила не были созданы, программа будет спрашивать у вас, следует ли разрешить обмен данными с теми или иными приложениями.
- **Интернет / зона высокой опасности** – рекомендуется применять, когда ваш компьютер подключен к общедоступной сети, и вы хотите обеспечить максимальный уровень безопасности. Это наиболее безопасный уровень, при его использовании входящие подключения будут блокироваться. Если выбрать эту настройку, ваш компьютер будет фактически невидим извне.

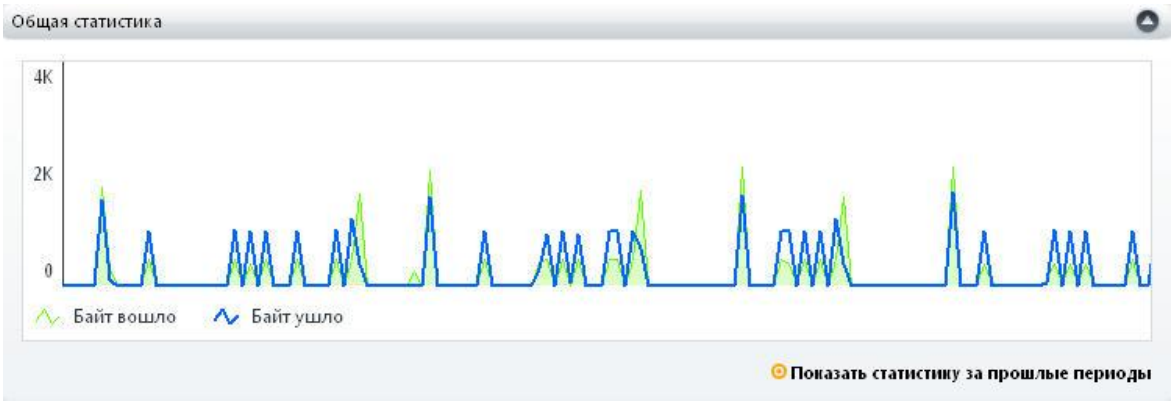
Настроить уровень защиты можно, либо щелкнув соответствующий значок, либо щелкнув по оранжевому ползунку и перемещая его влево или вправо с удерживаемой кнопкой мыши.

В этом окне вы также можете полностью отключить брандмауэр – либо навсегда, либо на заданное время. Чтобы сделать это, нажмите кнопку "Стоп" и выберите нужный вариант. Чтобы запустить брандмауэр вновь, нажмите кнопку "Пуск".

Экран, аналогичный изображенному, также будет появляться при каждом обнаружении новой сети. Вы сможете задать уровень безопасности для новой сети и указать, что эту настройку следует запомнить с тем, чтобы она автоматически применялась каждый раз при обнаружении этой же сети в будущем.

Статистика брандмауэра

На графике в нижней части окна в реальном времени отображается объем входящих и исходящих данных.

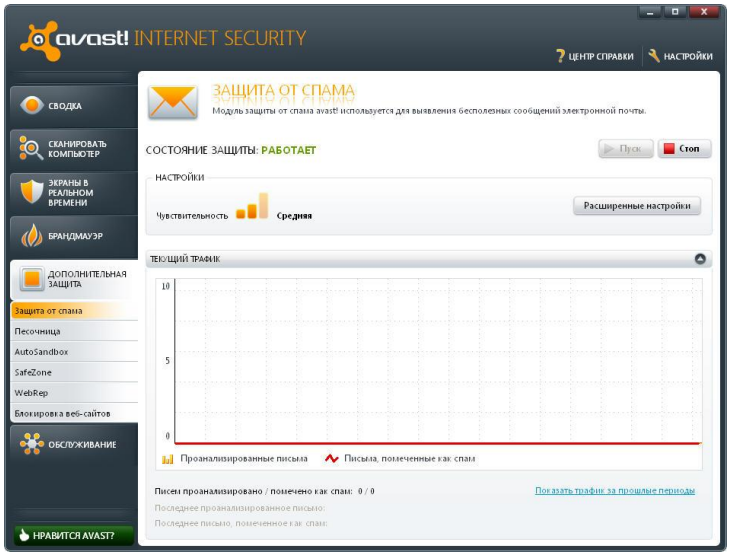


Чтобы перейти в более подробное представление данных, нажмите кнопку "Показать статистику за прошлые периоды". На экране "Статистика" вы можете просматривать объемы данных для брандмауэра, антиспамового фильтра или любых фильтров в реальном времени за выбранный период. Чтобы изменить масштаб любой части графика, щелкните по вертикальной полосе и перетащите ее вправо. Чтобы вернуться в начальное представление данных, просто нажмите "Показать".

В левой части экрана показаны другие параметры брандмауэра, описание которых есть в справке программы.

Антиспамовый фильтр

Антиспамовый фильтр avast! анализирует всю входящую электронную почту, чтобы определить, является она нужной или нет ("спамом"). Письма, квалифицированные как спам, перед доставкой в вашу папку "Входящие" будут соответствующим образом помечены. Если вы пользуетесь программой Microsoft Outlook, можно указать дополнительную папку, в которую будут перемещаться электронные письма, признанные спамом – см. следующий раздел.



По умолчанию avast! будет проверять все входящие сообщения электронной почты по глобальной базе данных в Интернете, содержащей информацию о спаме, и лишь после этого будет выполнен эвристический и другие виды анализа, позволяющего выявить потенциальный спам. В заголовок сообщений, квалифицированных как спам, перед их доставкой в папку "Входящие" буде вставлено особое сообщение.

Можно регулировать чувствительность эвристического анализа, щелкая по соответствующим оранжевым полоскам.

Повышение чувствительности увеличивает вероятность обнаружения спама, но также повышает вероятность "ложной тревоги" – если вы обнаружили, что часть "хороших" электронных писем помечаются как спам, попробуйте понизить чувствительность анализа.

Доверенные адреса электронной почты можно добавлять в "белый список" антиспамового экрана avast!. Письма от контактов в "белом списке" никогда не будут помечаться как спам – такие сообщения доставляются в папку "Входящие" напрямую. С другой стороны, если внести адрес электронной почты в "черный список", письма от этого отправителя всегда будут помечаться как спам. Чтобы внести адрес в "белый" или "черный" список, нажмите "Расширенные настройки", затем соответственно "Белый список" или "Черный список".

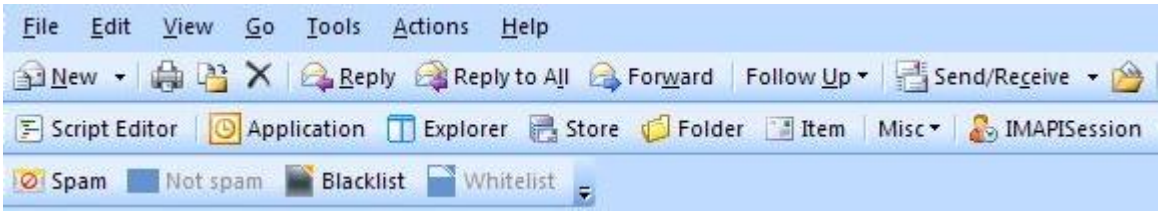
Наконец, в окне основных настроек можно указать, как будут помечаться сообщения электронной почты, которые программа считает спамом – скажем,

SPAM. Эти настройки можно использовать для создания новых правил в вашей программе для работы с электронной почтой – например, правила, согласно которому помеченные как спам письма автоматически перемещаются в другую папку.

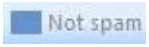
Microsoft Outlook

Антиспамовый фильтр avast! можно использовать как подключаемый модуль в Microsoft Outlook – т.е. некоторыми его функциями можно управлять прямо из Outlook.

Открыв Outlook после установки пакета avast! Internet Security, вы увидите в панели инструментов Outlook ряд дополнительных опций:



переносит сообщение в папку для нежелательной почты, заданную в настройках антиспамового фильтра avast!. По умолчанию используется папка "avast! Junk".



извлекает сообщение из папки "avast! Junk".

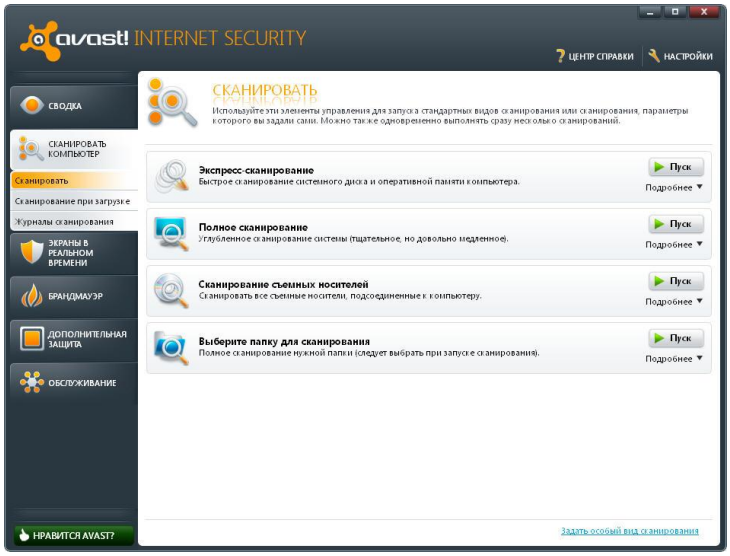
добавляет отправителя сообщения в "черный список".

добавляет отправителя сообщения в "белый список".

Чтобы перенести сообщение в папку для нежелательной почты, необходимо сначала выделить сообщение, затем нажать кнопку "Спам". При необходимости папка "avast! Junk" будет автоматически создана и добавлена в структуру папок Outlook.

Сканирование компьютера вручную

Чтобы выполнить сканирование компьютера вручную, перейдите на вкладку "Сканировать компьютер". Откроется изображенное ниже окно "Сканировать".



avast! Internet Security 6.0 включает ряд стандартных видов сканирования, которые устанавливаются по умолчанию.

Экспресс-сканирование – сканирование только системного раздела (как правило, это диск C:\ на компьютере). Обычно этого достаточно для выявления большей части вредоносных программ. По умолчанию сканируются только "опасные" расширения, т.е. файлы с такими расширениями, как "exe", "com", "bat" и т.п. При этом проверяются только части файла, расположенные в его начале и конце – то есть в местах, где обычно находятся вирусы.

Полное сканирование – более тщательное сканирование жестких дисков компьютера. По умолчанию все файлы сканируются по их содержимому – другими словами, avast! "заглядывает" в каждый файл, чтобы определить его тип и решить, следует ли его проверять. При этом выполняется проверка файла целиком, а не только частей файла, расположенных в его начале и конце – там, где обычно находятся вирусы. Этот вид сканирования полезен, если ваш компьютер заражен, однако источник заражения не удалось выявить при помощи экспресс-сканирования.

Сканирование съемных носителей – сканирование всех съемных носителей, подключенных к компьютеру. При сканировании носителей avast! будет искать программы, автоматически запускаемые при подключении устройства (auto-run).

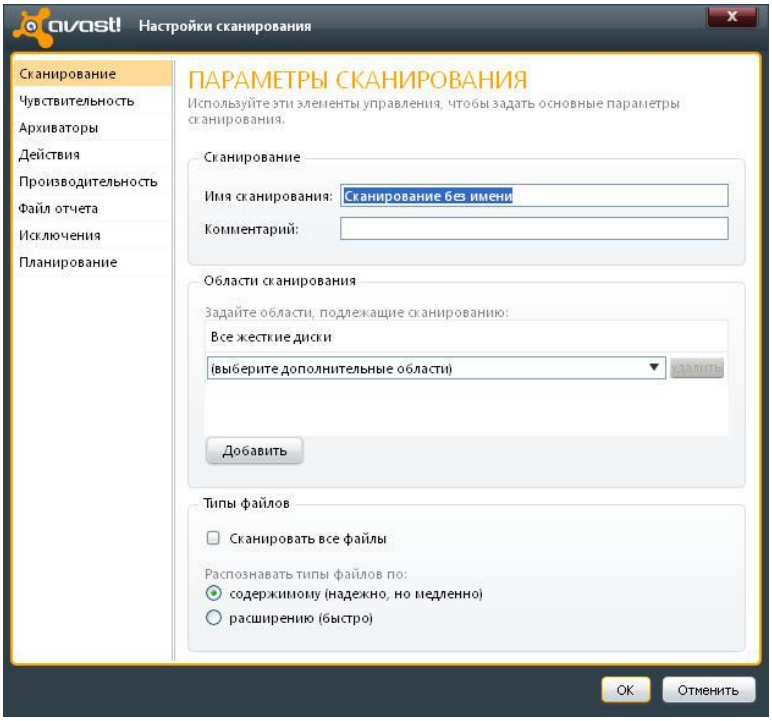
Выберите папку для сканирования – эта опция позволяет просканировать только определенную папку или несколько папок.

Чтобы запустить одно из стандартных сканирований, нажмите кнопку "**Пуск**". Кроме того, нажав кнопку "Настройки", вы можете запланировать регулярное сканирование нужного типа или однократное сканирование в нужный день и время. С помощью других параметров на экранах "Настройки" можно дополнительно настроить сканирования.

Можно также создать новое сканирование с нужными параметрами, нажав кнопку "Задать особый вид сканирования".

Создание особого вида сканирования

Нажав кнопку "Задать особый вид сканирования", вы можете создать совершенно новое сканирование с нужными вам параметрами. Откроется новое окно, где вы можете задать имя для нового вида сканирования, а также указать, какие части компьютера и какие типы файлов следует сканировать.



По умолчанию используется область сканирования "Все жесткие диски". Чтобы выбрать для сканирования новую область, откройте выпадающее меню и выберите дополнительную область сканирования. Чтобы удалить ненужную область, щелкните по ней и нажмите "Удалить". Также вы можете указать, как avast! должен распознавать потенциально подозрительные файлы, подлежащие сканированию – по расширению файла или по его содержимому.

Если выбрано "**по содержимому**", avast! будет проверять каждый файл, определяя его тип и на этом основании решая, следует ли сканировать файл.

Если же выбрано "**по расширению**", сканироваться будут только файлы с такими расширениями, как "exe", "com", "bat" и т.п.

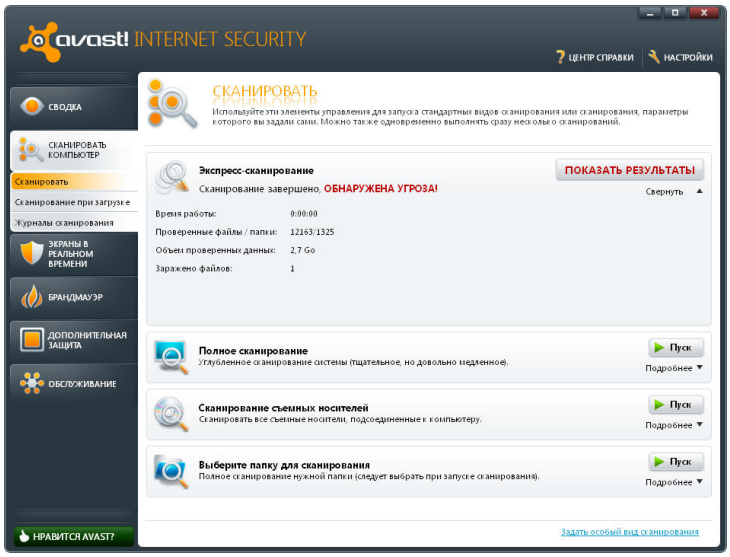
На этом экране также доступны другие настройки. Например, можно запланировать регулярное сканирование или сканирование, которое должно однократно выполниться в заданное время. Можно также исключить из области сканирования конкретные папки или файлы либо указать, какие действия должны

выполнять программа при обнаружении вируса – например, удалить файл или автоматически перенести его в карантин.

Программа позволяет создавать отчеты о просканированных файлах и ошибках, которые произошли во время сканирования. Кроме того, вы можете настраивать скорость и глубину сканирования.

Что делать при обнаружении вируса

В конце сканирования, если программа обнаружила подозрительный файл, отобразится сообщение "Обнаружена угроза" – см. ниже.



Подробную информацию о подозрительном файле и доступных вариантах действий можно просмотреть, нажав кнопку "Показать результаты".

Вы увидите список файлов, которые avast! считает подозрительными, и сможете указать, какое действие программа должна выполнить относительно каждого из файлов – т.е. "Удалить", "Переместить в карантин" и т.п. Выбрав нужное действие, нажмите "Применить".

РЕКОМЕНДУЕМОЕ ДЕЙСТВИЕ – переместить файл в **Virus Chest**. Карантин представляет собой особую область, используемую для безопасного хранения зараженных или подозрительных файлов до их удаления. Файлы, которые хранятся здесь, не могут нанести вред другим файлам в вашем компьютере. Кроме того, файлы можно попробовать вылечить и вернуть туда, где они находились до этого.

По умолчанию подозрительные файлы, выявленные экранами в реальном времени, автоматически перемещаются в карантин.

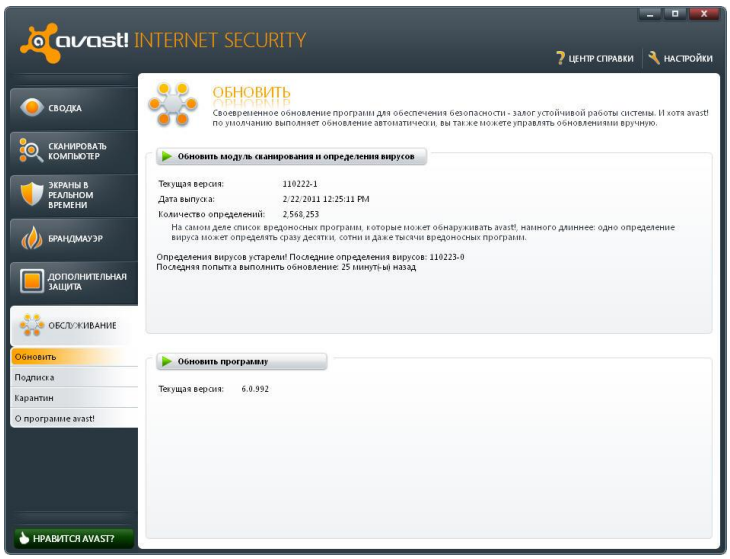
Вы можете в любое время просмотреть результаты сканирования повторно, войдя в раздел "Журналы сканирования" и выбрав сканирование, которое вы хотите просмотреть.

Обновление avast

Любая антивирусная программа – это прежде всего база данных с известными определениями вирусов. Такая база используется для обнаружения угроз для вашего компьютера, поэтому очень важно обеспечить регулярное обновление определений вирусов.

По умолчанию модуль сканирования avast! и определения вирусов обновляются автоматически при выходе каждой новой версии модуля или определений. Чтобы убедиться, что выбрано "Автоматическое обновление" модуля сканирования и определений вирусов, выберите "Настройки", затем "Обновления".

На вкладке "Обслуживание" нажмите "Обновить". В открывшемся окне вы сможете вручную обновить как модуль сканирования и определения вирусов, так и программу в целом.



"Модуль сканирования" – это часть программы, которая с помощью определений вирусов ищет потенциальные угрозы для вашего компьютера. "Программа" – это то, что вы видите на экране: пользовательский интерфейс, с помощью которого вы управляете действиями программы.

Чтобы обновить модуль сканирования и определения вирусов или саму программу, нажмите кнопку с зеленой стрелкой. Обратите внимание, что нажав "Обновить программу", вы автоматически обновите как программу, так и модуль сканирования с определениями вирусов.

Благодарим вас за то, что вы выбрали avast!