

Лабораторная работа №8. Типовые средства обеспечения информационной безопасности. Антивирусы. Брандмауэры. Ограничение доступа к файлам с помощью архиваторов.

Целью лабораторной работы является овладение навыками работы с типовыми средствами обеспечения информационной безопасности, такими как брандмауэры и антивирусы, а также получение навыков ограничения доступа к файлам с помощью архиваторов.

Ход работы:

1 Брандмауэр Windows

Брандмауэр Windows представляет собой программный комплекс, который проверяет данные, входящие через интернет или локальную сеть, и в зависимости от параметров брандмауэра блокирует или разрешает их передачу на компьютер.

Брандмауэр (межсетевой экран, firewall) помогает предотвратить проникновение вредоносного программного обеспечения в ваш компьютер через локальную сеть или интернет. Брандмауэр также помогает предотвратить отправку вредоносных программ на другие компьютеры [1].

Для работы с брандмауэром перейдите в Панель управления (Пуск, Панель управления), выберите Брандмауэр Windows.

1.1 Включение/отключение брандмауэра, изменение параметров уведомлений

Для включения (отключения) брандмауэра и настройки параметров уведомлений нажмите кнопку Изменение параметров уведомлений (рисунок 1).

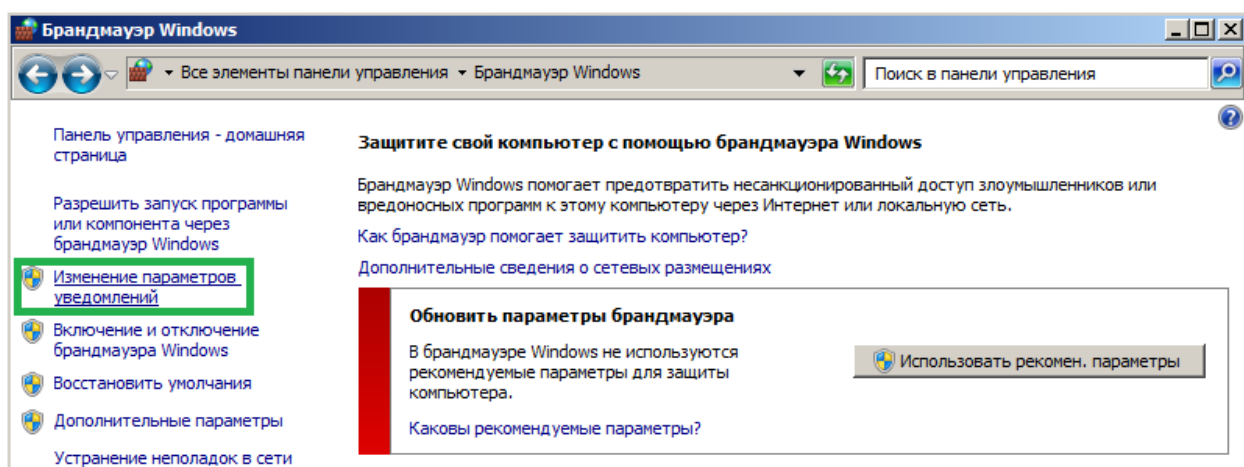


Рисунок 1 – Изменение параметров брандмауэра

В параметрах размещения в домашней или рабочей сети выберите пункт Включение брандмауэра Windows, и поставьте флаг напротив параметра Уведомлять, когда брандмауэр блокирует новую программу.

В параметрах размещения в общественной сети также включите брандмауэр и укажите параметр об уведомлении блокирования программ, нажмите кнопку ОК.

1.2 Добавление программы в список исключений

Чтобы добавить программу в список исключений брандмауэра (брандмауэр не будет блокировать программу) нажмите кнопку Разрешить запуск программы или компонента через брандмауэр Windows. В появившемся окне нажмите кнопку Разрешить другую программу, выберите из списка программу Mozilla Firefox и нажмите кнопку Добавить (рисунок 2).

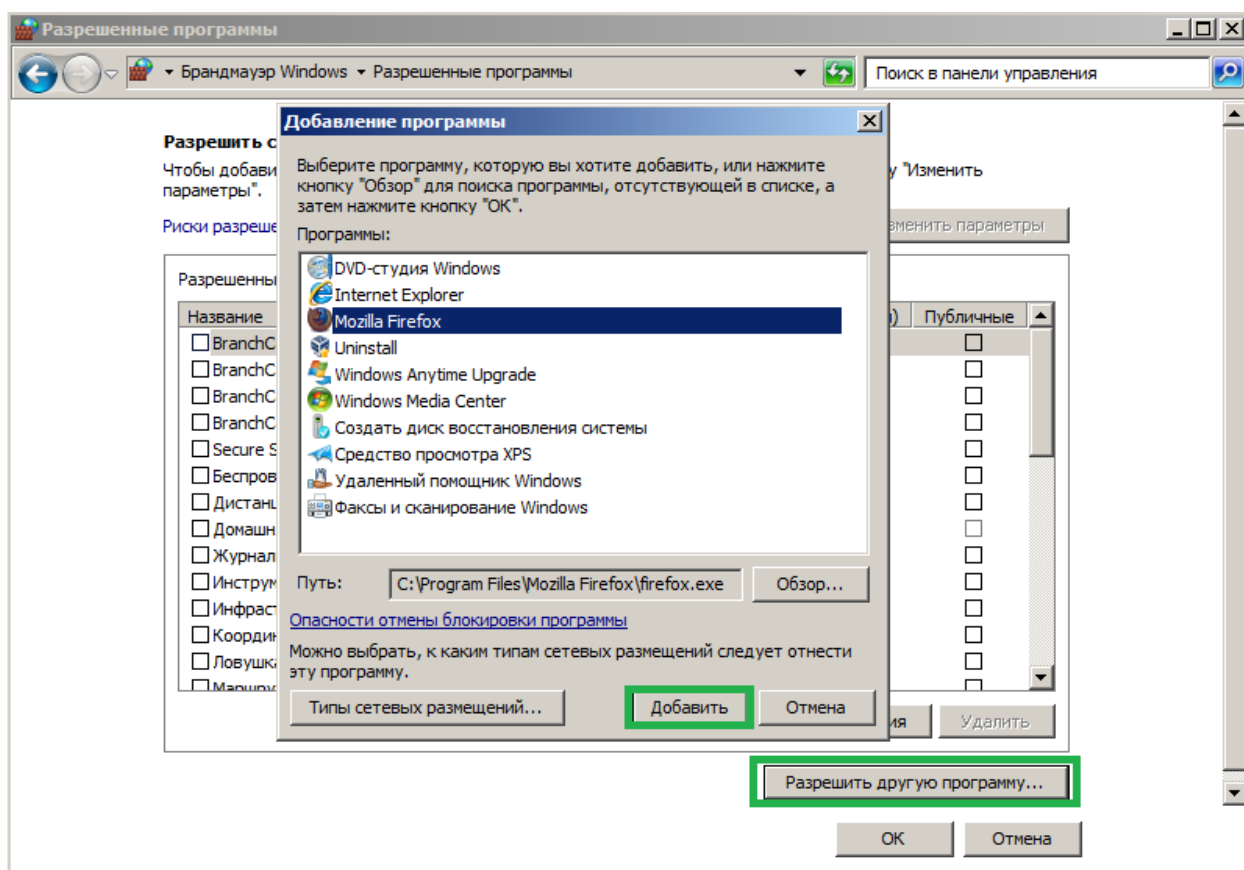


Рисунок 2 – Добавление программы в список исключений брандмауэра

1.2 Правила для входящих/исходящих подключений

У брандмауэра Windows есть расширенный режим, который позволяет более детально настраивать параметры подключений создавать правила подключений и т.д. В окне брандмауэра Windows нажмите кнопку

Дополнительные параметры и брандмауэр запустится в режиме повышенной безопасности. В режиме повышенной безопасности брандмауэр позволяет конфигурировать не только локальный компьютер, но и удаленные компьютеры, и объекты групповой политики.

Для всех профилей уже существуют предустановленные наборы правил. Можно изменить их или добавить собственные правила для входящих и исходящих подключений. Создание правил реализовано с помощью мастера.

Создайте правило блокирующее приложению доступ в Интернет, для этого:

- выберите в левой панели Правила для исходящего подключения;
- вызовите контекстное меню и выберите команду Создать правило (рисунок 3);
- в окне мастера создания правил выберите тип правила – для программы, нажмите Далее;
- в следующем окне укажите путь к программе C:\Program Files\Internet Explorer\iexplore.exe, и нажмите Далее;
- в настройках указания действия выберите параметр Блокировать подключение и нажмите Далее;
- в появившемся окне выберите все профили (Доменный, Частичный, Публичный);
- укажите имя создаваемого правила, добавьте описание и нажмите кнопку Готово.

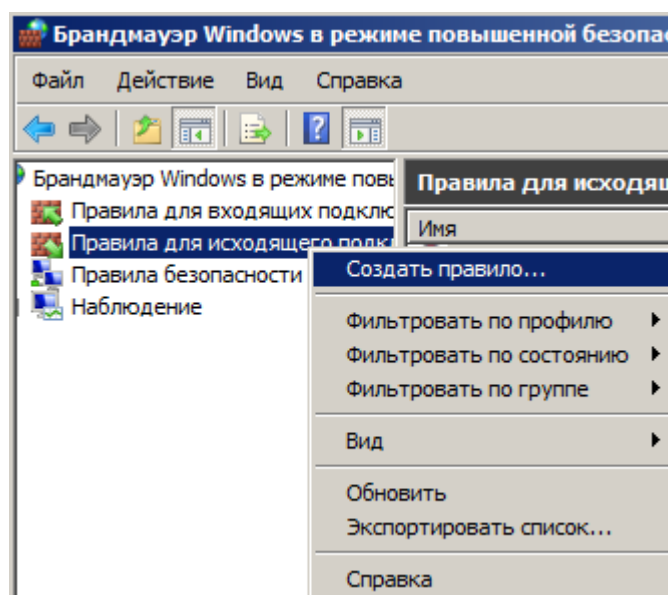


Рисунок 3 – Создание правила для исходящего подключения

Проверьте работоспособность правила – попробуйте перейти на какой-нибудь сайт через браузер Internet Explorer.

Созданное правило отображается в списке правил исходящего подключения, и если необходимо приостановить на некоторое время действие правила, либо выключить его – выберите его из списка, вызовите контекстное меню и выберите команду Отключить правило.

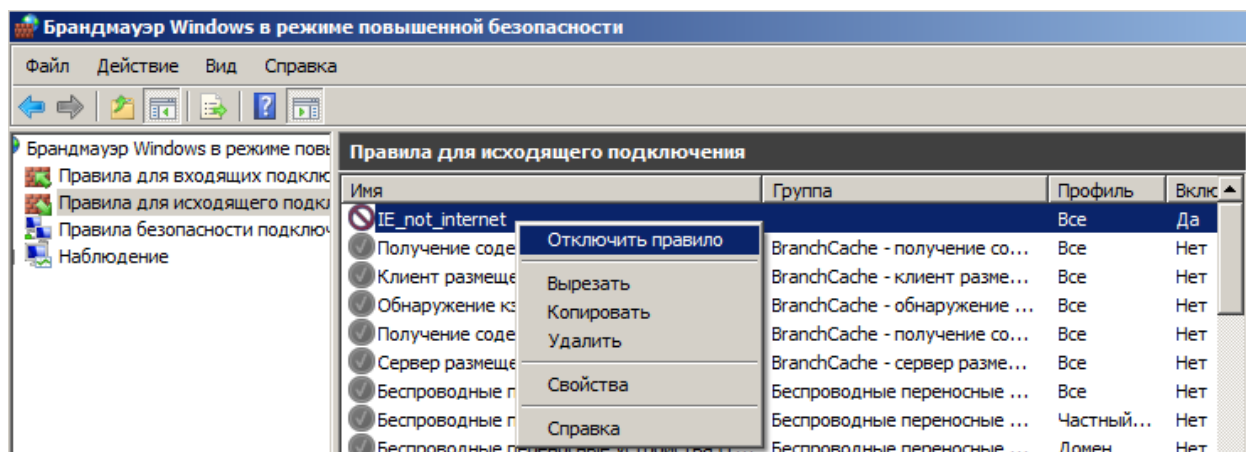


Рисунок 4 – Отключение правила

Отключите правило и снова попробуйте перейти на какой-нибудь сайт через браузер Internet Explorer.

С помощью брандмауэра также можно блокировать конкретные IP-адреса (либо диапазон адресов). Для начала выберите IP-адрес, доступ к которому будет блокироваться. Для определения IP-адреса какого-либо веб-узла можно воспользоваться командой nslookup (определение IP-адреса по доменному имени сайта). К примеру, можно узнать один из IP-адресов серверов google. Для этого:

- запустите командную строку – меню Пуск, Все программы, Стандартные, Командная строка (либо Win+R, cmd, OK);
- выполните команду nslookup google.ru (рисунок 5).

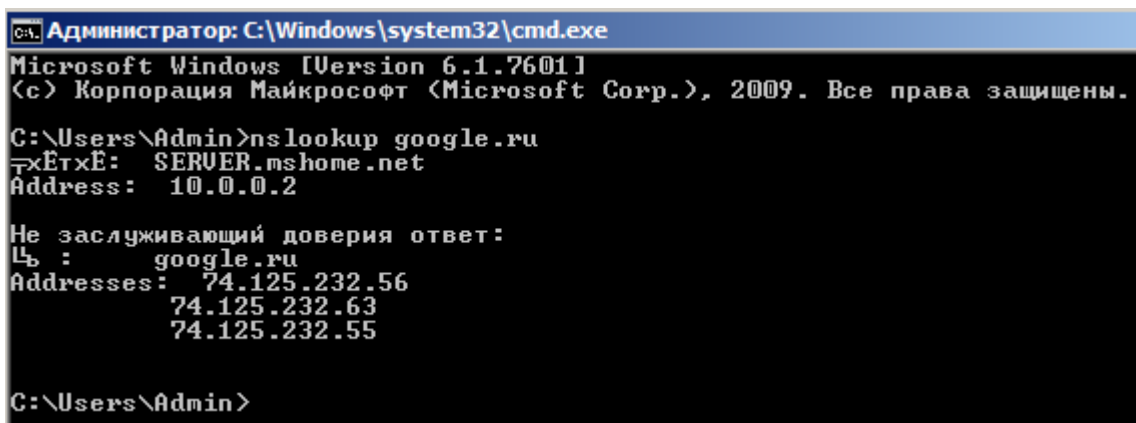


Рисунок 5 – Определение IP-адреса по доменному имени сайта

После того как адреса известны настройте блокировку данных адресов:

- откройте брандмауэр Windows в режиме повышенной безопасности;
- выберите правила для входящих подключений, вызовите контекстное меню и выберите команду создать правило;
- в появившемся окне выберите тип правила – Настраиваемые;
- в окне выбора программ выберите параметр – применять это правило ко всем программам;
- порты и протоколы указывать не нужно, нажмите Далее;
- в окне Область добавьте IP-адреса, которые появились у Вас, в поле Удаленные IP-адреса (рисунок 6);
- далее укажите действие, которое должно выполняться – Блокировать подключение;
- укажите все профили, для которых применяется правило (доменный, частный, публичный);
- укажите имя правило и его описание и нажмите кнопку Готово.

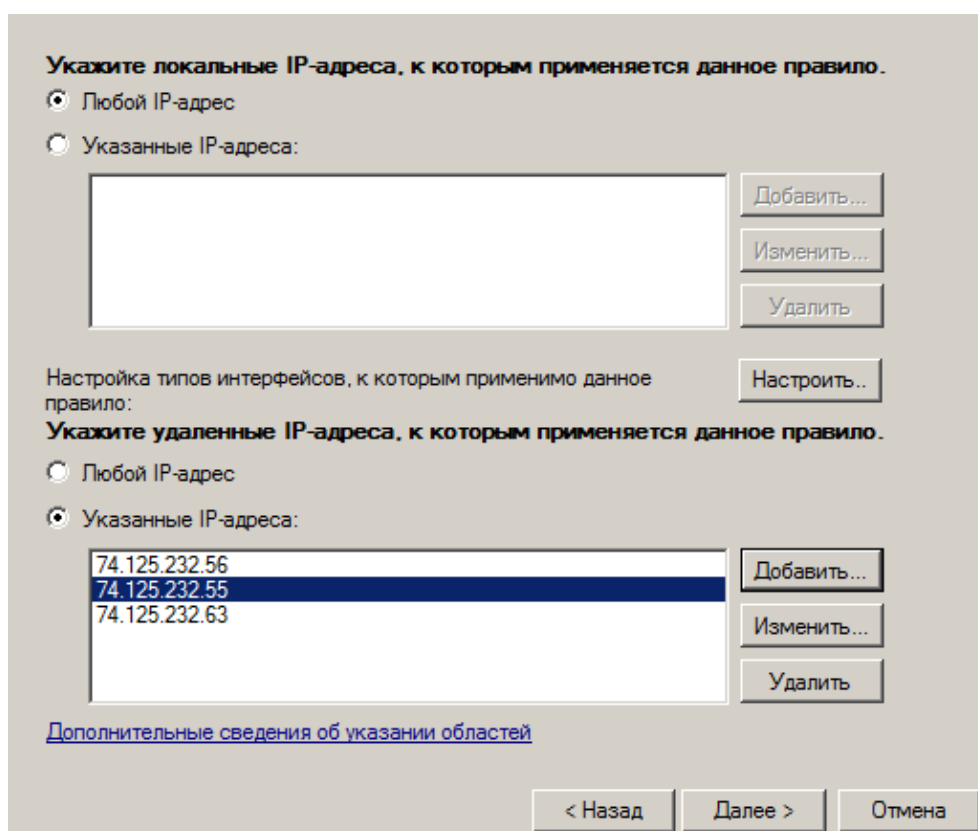


Рисунок 6 – Указание удаленных IP-адресов

Создайте аналогичное правило для исходящих подключений. После этого проверьте работоспособность созданных правил – попробуйте перейти по адресу <http://google.ru>. Отключите правила и снова попробуйте перейти по адресу.

2 Антивирусы

Антивирус – это программа, которая осуществляет защиту компьютера от различных вредоносных программ. Целями антивирусных программных продуктов является не только защита компьютера, но и обнаружение уже зараженных программ на нем и способность осуществить лечение этих программ. [1]

В данной лабораторной работе используется бесплатная версия антивируса Avira 12.0.0.144.

2.1 Установка

Для установки антивируса Avira запустите на рабочем столе файл Avira.exe. Выберите тип установки – Выборочная, нажмите Далее. Путь установки оставьте по умолчанию. В параметрах выбора компонентов поставьте флажки напротив всех компонентов из списка: Realtime Protection – контроль доступа к файлам в режиме реального времени, Rootkits Protection – распознавание вирусов и вредоносного ПО находящихся в системе, Shell Extension – проверка файлов на вирусы и наличие вредоносного ПО вручную. Нажмите Далее и дождитесь установки программы.

После установки появится окно основных настроек антивируса, нажмите кнопку Далее. В параметрах настройки эвристики «АНЕAD» включите эвристику и выберите высокий уровень обнаружения вирусов и вредоносного ПО. Далее выберите расширенные категории опасностей – выберите все из списка (рисунок 7).

В следующем окне выберите режим запуска Realtime Protection – Нормальный старт. Далее предлагается провести проверку системы на предмет обнаружения вирусов и другого вредоносного ПО – откажитесь от проверки системы, т.к. вероятность обнаружить все вирусы или другое вредоносное ПО без обновленных антивирусных практически нулевая. Завершите настройку антивируса – нажмите кнопку Готово.

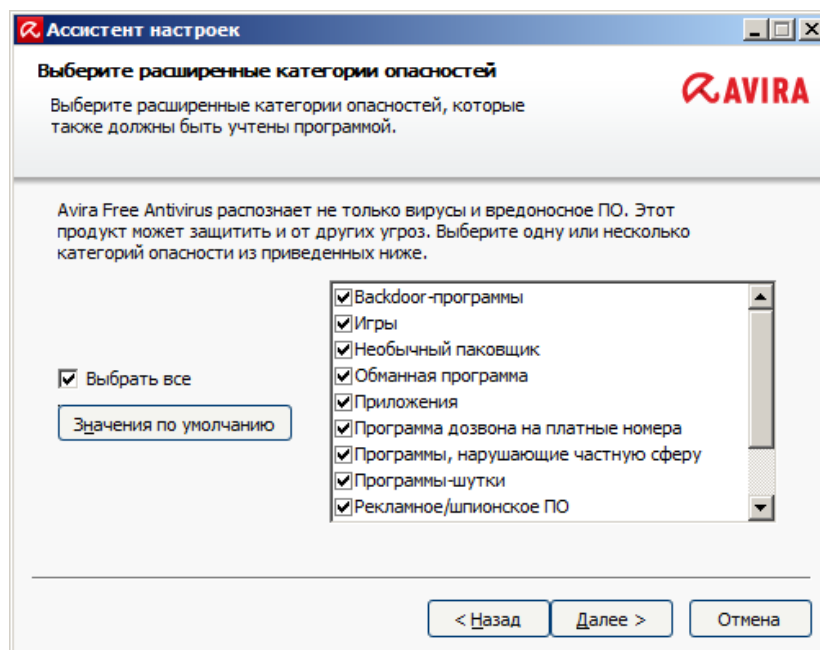


Рисунок 7 – Расширенные категории опасностей

2.2 Настройка антивируса

Для настройки дополнительных параметров антивируса запустите его, выбрав значок в трее, либо с помощью меню Пуск, Все программы, Avira. На рисунке 8 отображено главное окно программы в котором выделены 4 основных пункта управления антивирусом:

- 1 – включение или отключение антивируса;
- 2 – настройка дополнительных параметров антивируса;
- 3 – полное сканирование компьютера;
- 4 – принудительное обновление антивируса.

Откройте окно настроек антивируса, нажав соответствующую кнопку, либо через меню Сервис, Конфигурация. Выберите экспертный режим настройки программы (рисунок 9).

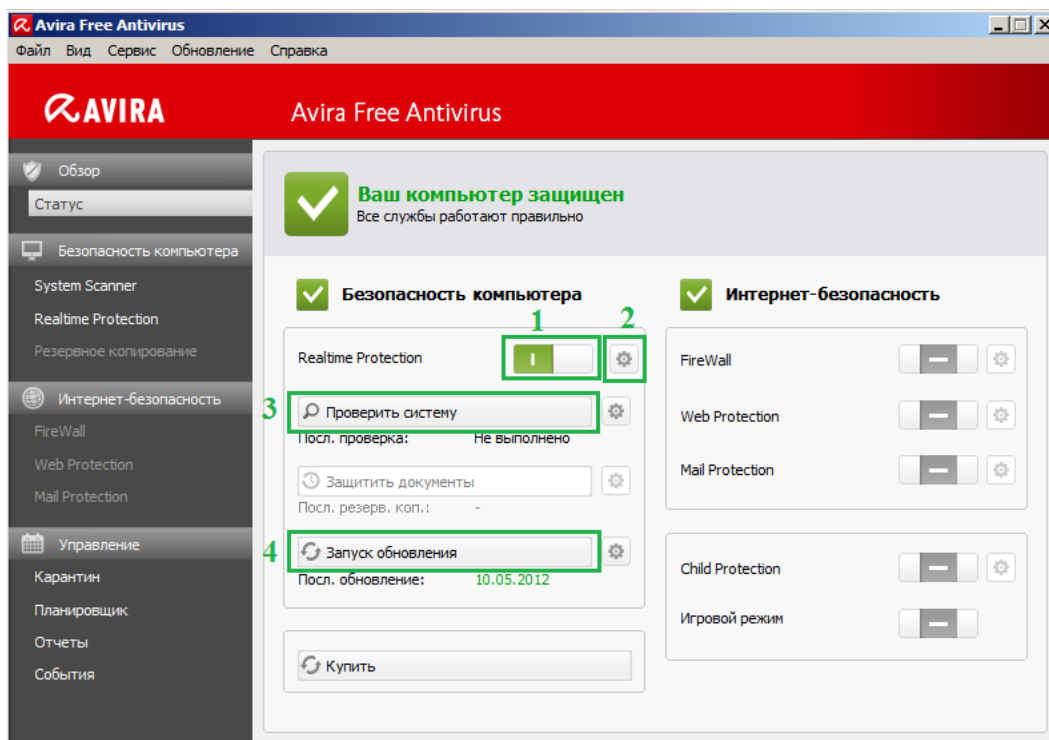


Рисунок 8 – Главное окно антивируса Avira

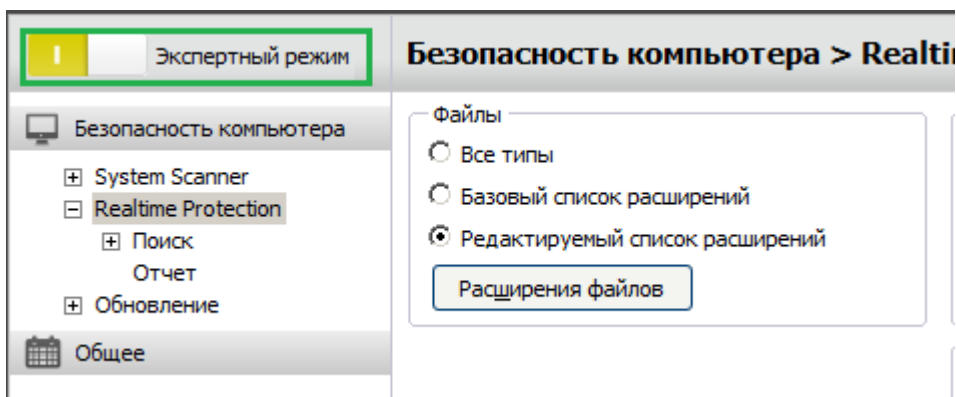


Рисунок 9 – Экспертный режим настройки антивируса

В окне настроек антивируса слева отображены два основных раздела: безопасность компьютера и общее. Перейдите в раздел Безопасность компьютера и раскройте структуру System Scanner. Перейдите на ветку Проверка и в группе Файлы выберите пункт Все файлы – для проверки всех файлов независимо от их содержания и расширения. В группе дополнительные настройки отметьте все пункты кроме пункта Следовать по ссылкам. В группе процесс сканирования поставьте флаг напроив параметра Разрешать остановку проверки и выберите средний приоритет сканирования.

Далее перейдите на вкладку Действие при обнаружении и установите параметр Интерактивно – об обнаружении вирусов будет сообщаться в диалоговом окне, где можно выбрать действие.

На вкладке Архивы установите проверку всех типов архивов и базовый список расширений.

Вкладка Исключения позволяет добавить файлы для того чтобы исключить их из проверки антивирусом.

Перейдите на вкладку Эвристика. В группе Макровирусы установите параметр Эвристическое обнаружение макровирусов, и выберите высокий уровень обнаружения вирусов и вредоносного ПО.

На вкладке Отчеты выберите тип отчета По умолчанию – протоколируются имена файлов с указанием пути.

Далее раскройте структуру Realtime Protection и перейдите на вкладку Поиск (сканирование). В группе Файлы выберите пункт Все файлы, режим сканирования – Во время чтения и записи.

На вкладке Действия при обнаружении установите параметр Журнал регистрации событий для добавления в журнал событий Windows соответствующей записи.

Вкладка Исключения также как и при настройке сканера позволяет добавлять файлы, исключаящиеся из проверки, только помимо объектов в исключения можно добавлять и процессы.

На вкладке Эвристика в группе Макровирусы установите параметр Эвристическое обнаружение макровирусов, и выберите высокий уровень обнаружения вирусов и вредоносного ПО.

Раскройте структуру Обновление, установите параметры Автоматического обновления – каждый день, и установите параметр Повторно запустить задание по истечении времени.

На вкладке Обновление продукта выберите параметр Уведомить о выходе следующего обновления продукта, повторное уведомление через 1 день.

На вкладке Настройки перезагрузки установите параметр Запрос, требуется ли перезагрузка компьютера, чтобы компьютер не перезагружался автоматически после обновления.

На вкладке Веб-сервер установите параметр Использовать существующее соединение с сетью. На вкладке прокси-сервер включите настройки Windows.

Перейдите в раздел Общее на вкладку Критерии угроз. Данные параметры настраивались при установке антивируса, проверьте чтобы в группе Выбор дополнительных категорий угроз было выбрано значений Выбрать все – для активации всех категорий угроз.

На вкладке Безопасность в группе автозапуск включите параметр Блокировать функцию автозапуска, исключать CD/DVD диски не нужно. В группе защита системы включите параметр Защитить хост-файл Windows от изменений (в хост-файлах вирусы или вредоносное ПО указывают перенаправление запросов на нежелательные страницы). В группе Защита продукта включите параметр Защитить процессы от нежелательного завершения и Защитить от манипуляций файлы и введенную информацию о регистрации (защита файлов конфигурации и записей в реестре от обработки). Отключите параметр Расширенная защита процессов – для этой функции требуется значительно большее количество ресурсов, чем на виртуальной машине.

На вкладке WMI (Windows Management Instrumentation) активируйте поддержку WMI – чтобы можно было вызвать оперативные данные программы через WMI.

Вкладка события позволяет настроить параметры сохранения событий в базе данных. Установите параметр Удалять все строки старше 30 дней. На вкладке Отчеты также настройте удаление отчетов старше 30 дней.

На вкладке Папки установите настройки по умолчанию – для работы с временными файлами используются настройки системы.

Перейдите на вкладку Уведомления и в группе Обновление установите сообщение уведомлений, если последнее обновление позднее 2 дней, включите параметр Уведомлять об устаревшем VDF-файле – вы получите сообщение если файл определений вирусов устареет. В группе Предупреждения/Указания в следующих ситуациях выберите все параметры, чтобы отображались все уведомления по антивирусной защите.

После изменения настроек антивируса для внесения изменений нажмите кнопку Принять.

Обновите антивирус. Для этого в главном окне программы нажмите кнопку Запуск обновления (рисунок 10).

После обновления баз антивируса запустите проверку системы. Для выполнения проверки системы в главном окне программы перейдите на вкладку Безопасность компьютера, выберите с списке профиль проверки – Быстрая проверка системы и нажмите кнопку Запуск администратором проверки с выбранным профилем (рисунок 11).

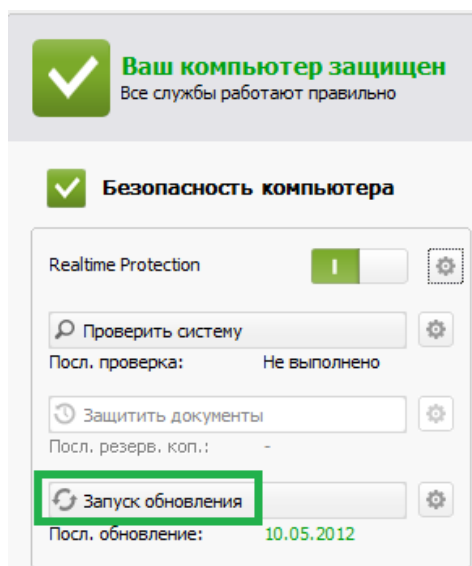


Рисунок 10 – Запуск обновления

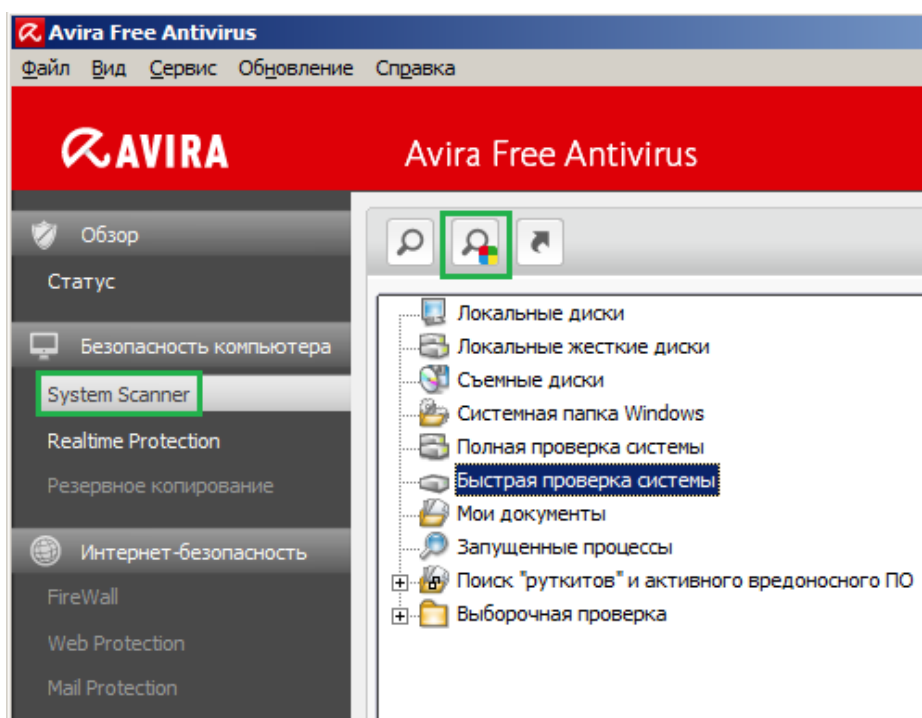


Рисунок 11 – Быстрая проверка компьютера

Перейдите в раздел Управление. На вкладке карантин отображаются обнаруженные вирусы угрозы и вирусы. На вкладке Отчеты отображаются результаты действий антивируса (обновления, поиск).

Перейдите на вкладку Планировщик. На данной вкладке можно задавать расписание автоматических проверок. По умолчанию присутствует Полная проверка системы, выберите ее и нажмите кнопку Редактировать выбранную задачу (рисунок 12).

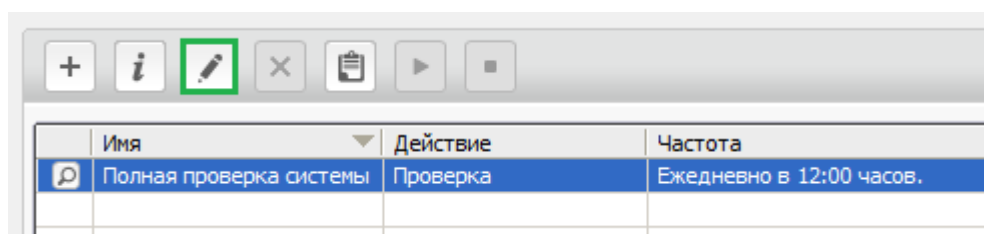


Рисунок 12 – Кнопка редактирования выбранной задачи

Профиль для проверки оставьте Полная проверка, график запуска задач – Ежедневно, Воскресенье, 10:00 час, Визуальный режим – Максимальный, и нажмите кнопку Готово.

3 Фаервол (межсетевой экран) Comodo

Для установки межсетевого экрана запустите файл cfw.exe. В появившемся окне выберите русский язык, далее снимите флажки с предложенных параметров (вводить адрес электронной почты не нужно) и нажмите кнопку Согласен, установить.

После установки автоматически будет обнаружена новая сеть, укажите местоположение – Я нахожусь в зоне общего доступа (рисунок 13).

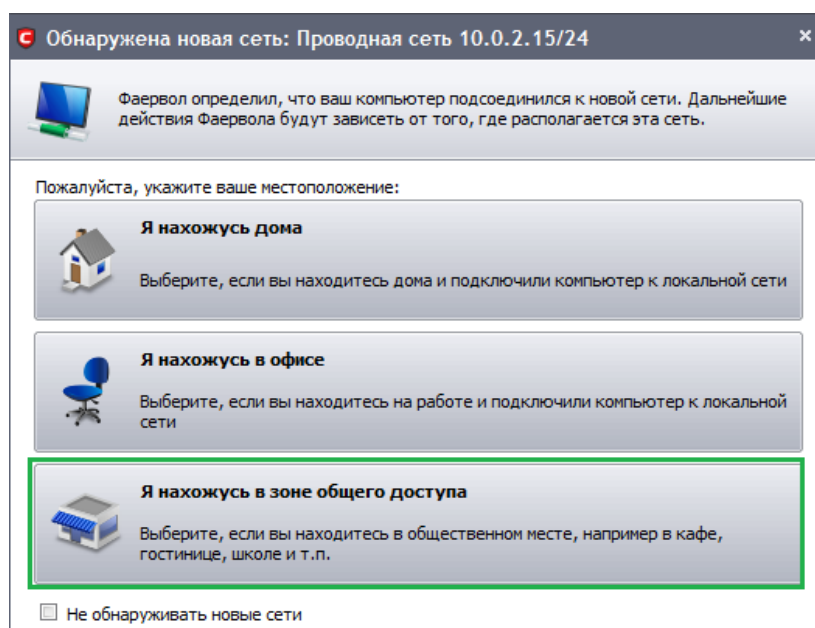


Рисунок 14 – Выбор местоположения

Далее будет предложено использовать TrustConnect для безопасного обмена данными. Для использования этого режима необходима регистрация, нажмите кнопку Продолжить в незащищенном режиме. Перезагрузите гостевую ОС.

3.1 Настройка фаервола

Comodo Firewall состоит из двух основных модулей: самого фаервола (вкладка Фаервол) и модуля проактивной защиты (вкладка «Защита+»). Основную информацию по работе этих модулей можно просмотреть на вкладке Сводка. С помощью вкладки Сводка Вы можете получить быстрый доступ к некоторым основным настройкам и статистике: посмотреть, сколько входящих и исходящих соединений и статистику вторжений; оценить, какие приложения проявляют наибольшую сетевую активность; сменить режимы работы фаервола и модуля «Защита+» или остановить все соединения.

Нажмите кнопку Остановить все соединения (рисунок 15) и попробуйте перейти по какому-нибудь веб-адресу. Затем восстановите все соединения.

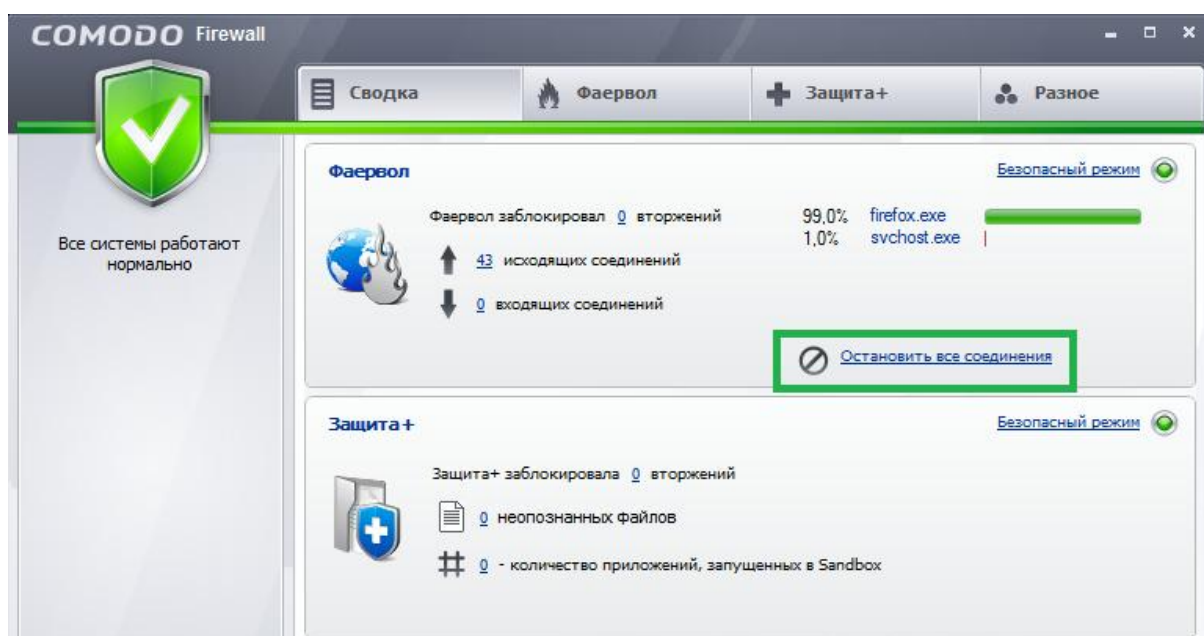


Рисунок 15 – Кнопка «Остановить все соединения»

Перейдите на вкладку Фаервол. Для того чтобы обезопасить компьютер от вторжений извне необходимо заблокировать все входящие соединения и скрыть порты. Нажмите кнопку Мастер скрытых портов и выберите параметр Блокировать все входящие соединения и скрыть мои порты для всех входящих соединений (рисунок 16).

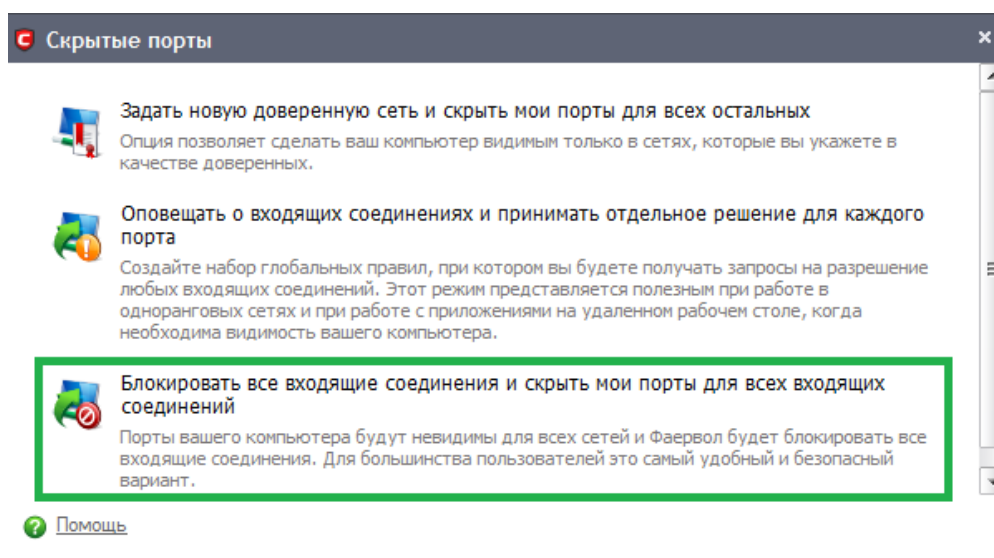


Рисунок 16 – Блокирование всех входящих соединений и скрытие портов

Для изменения параметров работы фаервола нажмите кнопку Настройки фаервола. На вкладке Общие настройки выберите Безопасный режим фаервола, поставьте флаг напротив параметра Создавать правила для безопасных приложений – для всех приложений, которые будут в списке безопасных у фаервола, автоматически будут создаваться разрешающие правила. Также поставьте флаг напротив параметра Автоматически обнаруживать новые частные сети.

На вкладке Настройки оповещений установите средний уровень частоты оповещений, и включите все параметры оповещений о запросах.

Перейдите на вкладку Расширенные и включите параметр Защищать ARP кэш. Закройте окно настроек фаервола нажатием кнопки ОК.

3.2 Настройка сетевой активности отдельных приложений и процессов

Firewall Comodo позволяет разрешить/запретить сетевую активность отдельных приложений (групп приложений). Для этого на вкладке Фаервол присутствуют пункты Добавить доверенное приложение и Добавить заблокированное приложение. Добавьте браузер Internet Explorer в список заблокированных приложений, для этого:

- на вкладке Фаервол нажмите кнопку Добавить заблокированное приложение;
- в появившемся окне нажмите кнопку выбрать и появившемся списке выберите Обзор;
- укажите путь к приложению (C:\Program Files\Internet Explorer\iexplorer.exe);
- нажмите кнопку Применить.

Запустите Internet Explorer и попробуйте перейти по какому-нибудь веб-адресу. Доступ в сеть заблокирован. Для удаления приложения из списка заблокированных на вкладке Фаервол нажмите кнопку Политики сетевой безопасности. В появившемся окне на вкладке Правила для приложений выберите из списка Internet Explorer (рисунок 17) и нажмите кнопку Удалить.

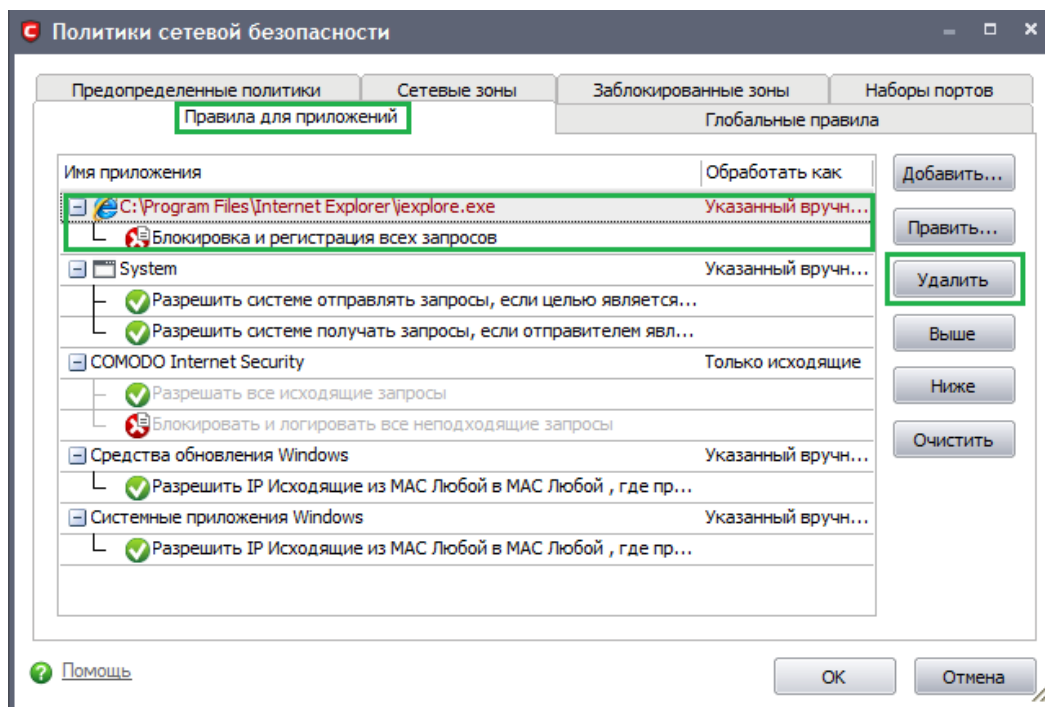


Рисунок 17 – Удаление приложения из списка заблокированных

Проверьте внесенные изменения – запустите браузер Internet Explorer и попробуйте перейти по какому-нибудь веб-адресу.

Также в список заблокированных приложений можно добавить запущенные процессы. Для этого на вкладке Фаервол нажмите кнопку Добавить заблокированное приложение и в появившемся окне нажмите кнопку Выбрать и выберите Запущенные процессы. В появившемся окне выберите процесс VBoxService.exe (рисунок 18) и нажмите кнопку Выбрать. Далее нажмите кнопку применить. Исключить процесс из списка можно также с помощью Политики сетевой безопасности.

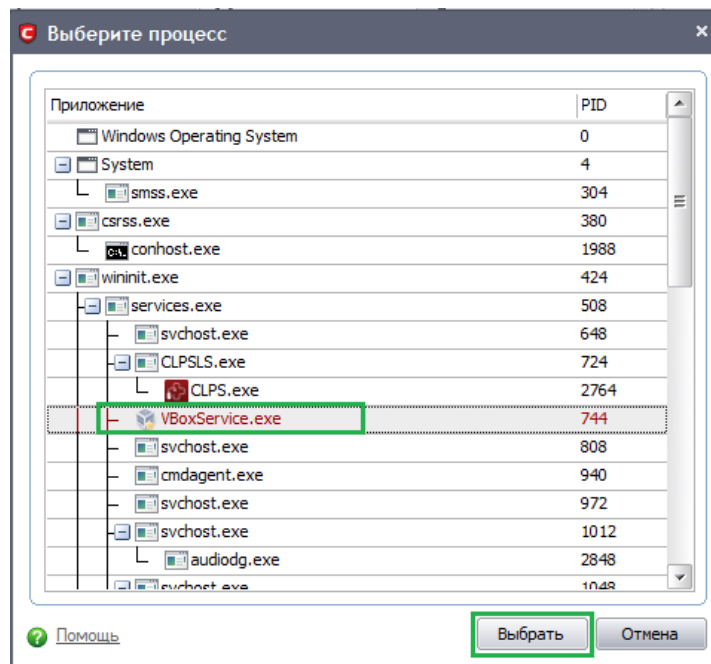


Рисунок 18 – Добавление процесса в список заблокированных

3.3 Настройка проактивной защиты

Модуль проактивной защиты занимается контролем всех файлов, которые запускаются на Вашем компьютере. Перейдите на вкладку Защита+.

В пункте Доверенные файлы Вы можете получить доступ к управлению локальной базой данных файлов исполняемых на вашем компьютере. По умолчанию внесен ряд системных файлов, а также добавляются те файлы, которые Вы объявите безопасными.

Все файлы, которые будут обнаружены, но при этом программа не сможет определить, безопасны ли они, добавляются в список неопознанных файлов. Доступ к этому списку можно получить в пункте Неопознанные файлы.

Все файлы попавшие в неопознанные будут запускаться в программе Sandbox. Это механизм безопасности, который создает виртуальную файловую систему и реестр, для запуска подозрительных файлов и приложений. Таким образом, любое приложение, запущенное через Sandbox, будет оказывать влияние только на её виртуальную среду, и не будет затрагивать операционную систему.

Нажмите кнопку Настройки проактивной защиты. В появившемся окне на вкладке Общие настройки установите Безопасный режим – применяется политика безопасности компьютера, любая активность безопасных файлов запоминается, неизвестных исполняемых файлов вызовет оповещение. Поставьте флажки напротив параметров (рисунок 19):

- блокировать все неизвестные запросы, если приложение закрыто;

- адаптировать режим работы при низких ресурсах системы;
- создавать правила для безопасных приложений.

На вкладке настройки контроля исполнения приложений включите контроль исполнения приложений для перехвата исполняемых файлов перед их загрузкой в память.

Остальные параметры оставьте по умолчанию и для завершения настроек проактивной защиты нажмите кнопку ОК.

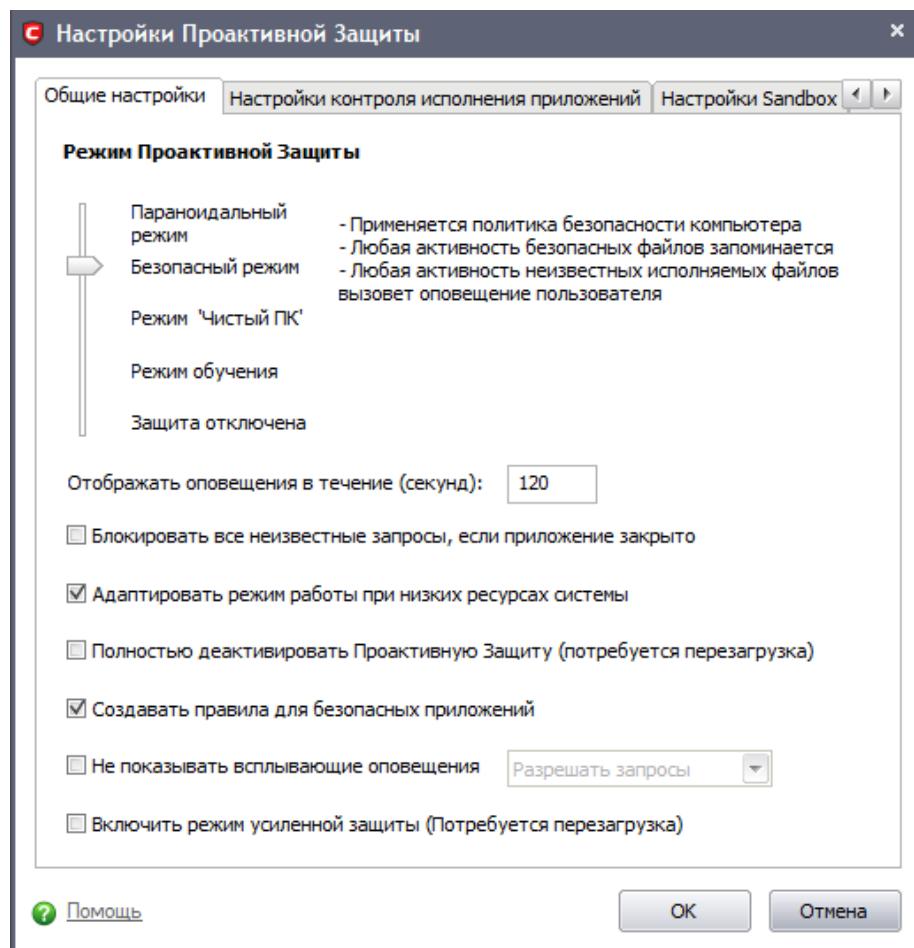


Рисунок 19 – Настройка режима проактивной защиты

4 Архиваторы

Архиватор — программа, предназначены для упаковки файлов в архив путем сжатия хранимой в них информации (либо без сжатия).

4.1 Параметры архивации

Для добавления файлов в архив необходимо их выделить, вызвать контекстное меню выбрать 7zip, и выбрать команду Add to archive. Выделите папку на рабочем столе и добавьте ее в архив (рисунок 12). Папка содержит текстовые файлы.

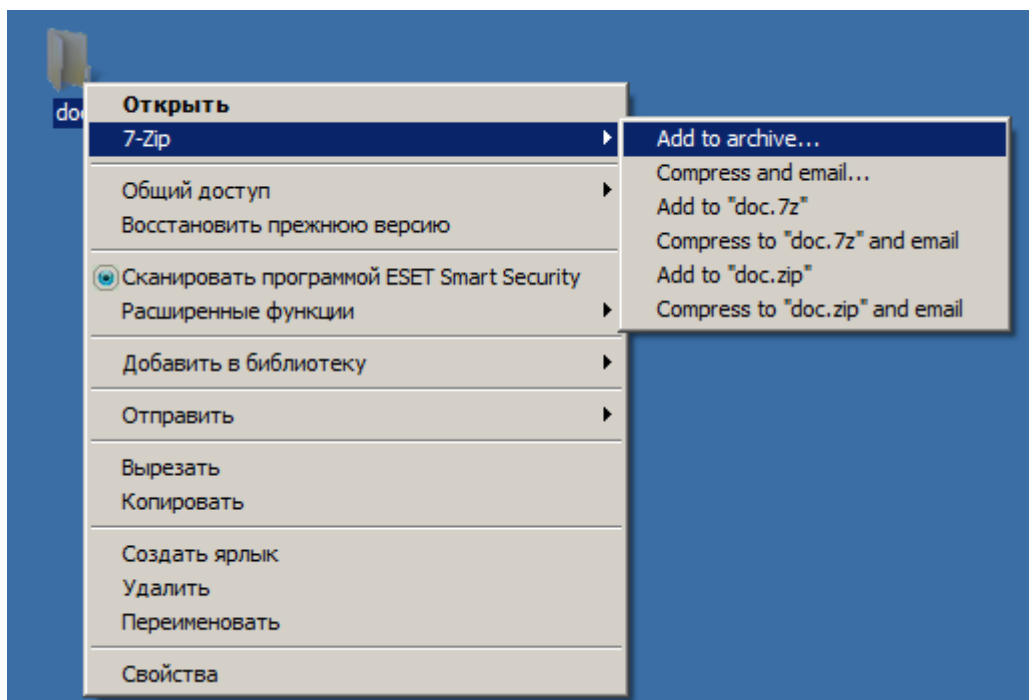


Рисунок 12 – Добавление файла в архив

В окне параметров архивирования:

- введите имя архива, выберите формат 7zip;
- выберите максимальный уровень сжатия – Ultra;
- метод сжатия LZMA ;
- размер словаря, размер слова, размер блока по умолчанию;
- в режиме обновления – добавлять и заменять файлы (add and replace files);
- нажмите ОК.

Сравните размер папки и размер архива. Разархивируйте папку: вызовите на ней контекстное меню, выберите программу 7zip, и выберите команду Extract files. Укажите путь для сохранения файлов и нажмите ОК.

Заархивируйте папку, используя несколько других методов и уровней сжатия, и сравните результаты.

4.2 Ограничение доступа к файлам архива

Для ограничения доступа к файлам с помощью архива при архивировании файлов устанавливается пароль для доступа к файлам архива.

Выберите папку, добавьте ее в архив и в параметрах архива установите пароль и поставьте флаг напротив параметра Шифровать имена файлов (рисунок 13), чтобы при попытке открытия архива не отображались имена файлов содержащиеся в нем. Для создания архива нажмите ОК.

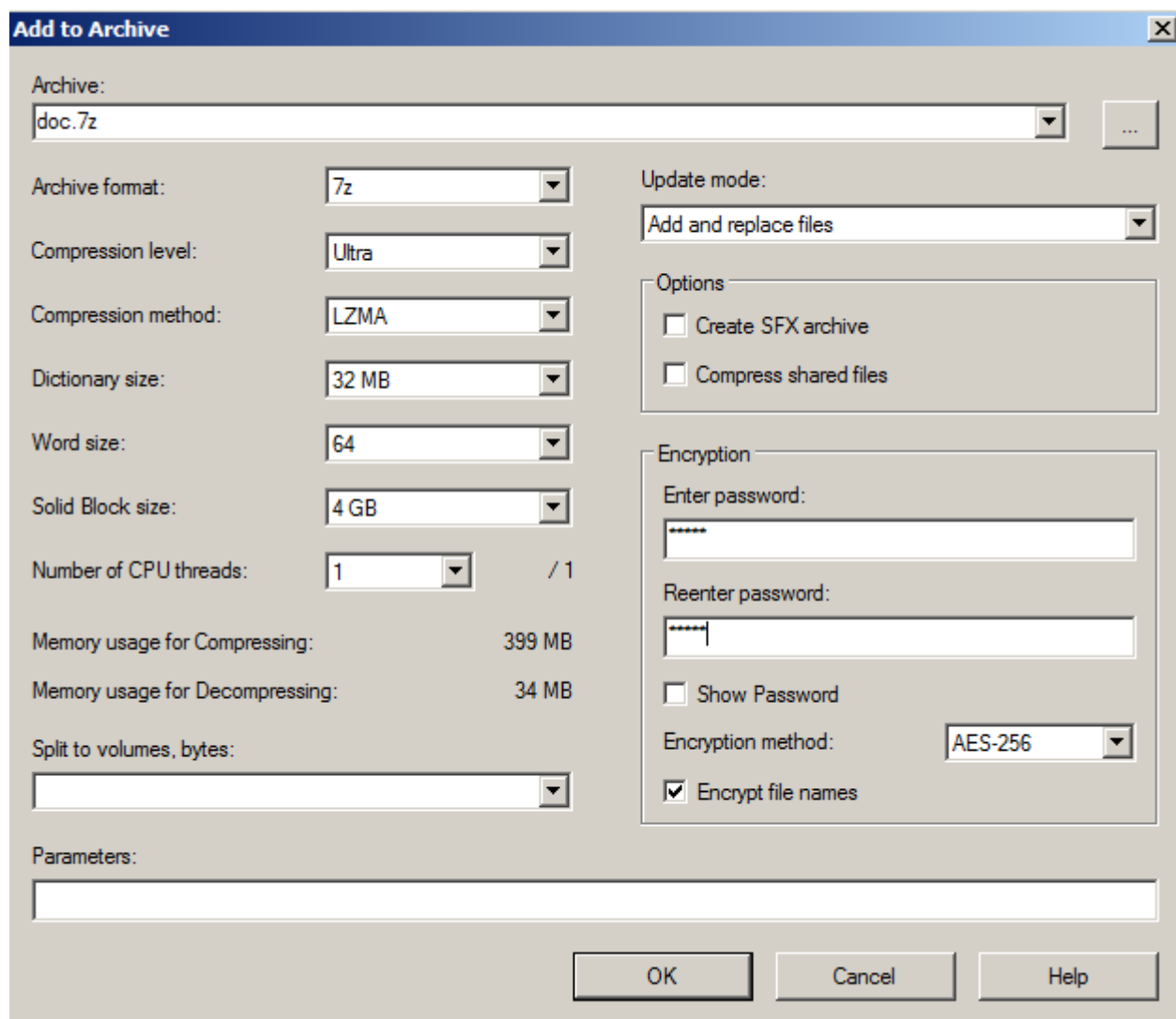


Рисунок 13 – Архивирование файлов с использованием пароля

Теперь для открытия архива или извлечения из него файлов необходимо ввести пароль. Разархивируйте файлы, содержащиеся в архиве.