**Практическое занятие №5**

**Тема «**Настройка антивирусов**»**

Цель: Овладение навыками настройки и использования различных антивирусов.

**Теоретическое введение**

**Признаки заражения компьютера вредоносными программами.**

При заражении компьютера вредоносными программами важно их обнаружить. Для этого следует знать об основных признаках проявления вредоносных программ. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ:
* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение даты и времени модификации файлов;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* существенное уменьшение размера свободной оперативной памяти;
* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

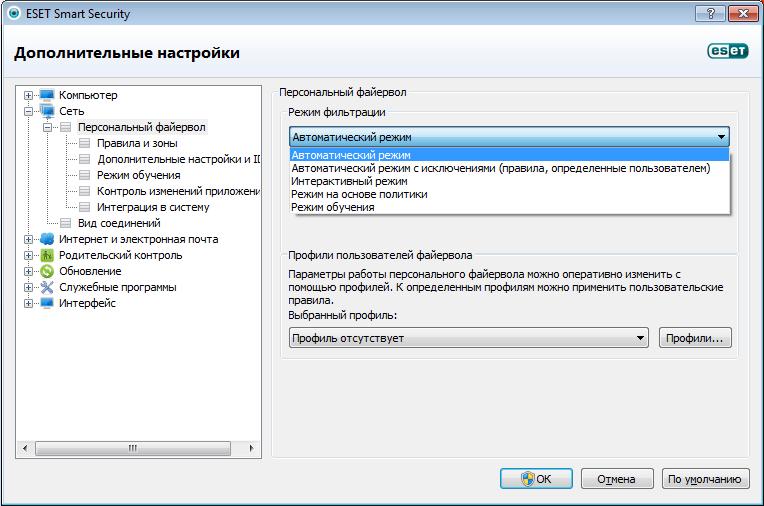
**Режимы работы файервола ESET NOD32 Smart Security и взаимодействие с пользователем**

Персональный файервол – это устройство, выполняющее функции драйвера сетевого трафика и управляющее взаимодействием в рамках локальной сети или Интернета. При помощи заранее определенных правил файервол анализирует это взаимодействие и принимает решение о его разрешении или запрете. Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

Доступны 5 отдельных режимов работы файервола, выбор которых зависит от требуемого уровня ограничений. Чтобы изменить поведение файервола, необходимо выбрать нужный режим фильтрации. Для изменения режима фильтрации нужно выполнить следующие действия:

1. Открыть программу ESET NOD32 Smart Security, щелкнув по значку программы в области уведомлений Windows или выбрав команды Пуск - Все программы - ESET- ESET NOD32 Smart Security.

2. Открыть дополнительные настройки, нажав клавишу F5 на клавиатуре – Персональный файервол. Откроется окно расширенной настройки. В расположенном справа раскрывающемся меню **Режим фильтрации** выбрать нужный режим фильтрации и нажать кнопку **OK**.



Вид меню **Режим фильтрации**

**Автоматический режим**

В автоматическом режиме сетевое взаимодействие автоматически контролируется параметрами, определенными пользователем. После подключения к сети пользователь решает, следует ли считать ее доверенной зоной. Взаимодействие в доверенной зоне не ограничивается в обоих направлениях. Взаимодействие в зоне ограничений: взаимодействие с Интернетом – разрешается только приложениям, устанавливающим исходящие подключения. Такие приложения считаются доверенными и для входящих подключений. Данный режим не требует участия пользователя (за исключением момента подключения к новой сети).

В общем, автоматический режим не использует заранее определенные правила, но при этом автоматически анализирует взаимодействие. Приложениям разрешается устанавливать исходящие подключения. Приложения, уже установившие исходящие подключения, считаются доверенными и для установки входящих подключений.

**Интерактивный режим**

В интерактивном режиме сетевое взаимодействие анализируется в соответствии с заранее определенными правилами. Если для подключения нет доступных правил, пользователю при помощи диалогового окна предлагается разрешить или запретить подключение. Через некоторое время пользователем будет создана группа правил, соответствующая его потребностям. Будьте осторожны, устанавливая этот режим в корпоративной среде, поскольку со временем некоторые пользователи могут начать игнорировать регулярно появляющиеся диалоговые окна и просто разрешать все, что предлагает им программа.

**Режим на основе политик**

В режиме на основе политик сетевое взаимодействие анализируется в соответствии с правилами, определенными администратором. Если доступных правил нет, подключение автоматически блокируется без уведомления пользователя. Данный режим рекомендуется выбирать только администраторам, желающим контролировать сетевое взаимодействие и знающим, каким приложениям следует его разрешить или запретить.

**Автоматический режим с исключениями**

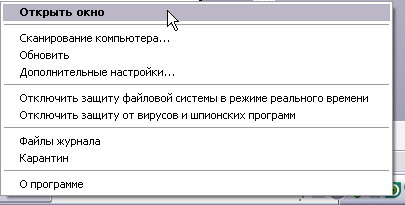
Данный режим позволяет настроить вручную правила. В этом случае, если будет запрос на соединение извне, файервол сначала проверит правила, которые прописал пользователь, и если найдет соответствующее, то оно будет задействовано. Если правила не будет, тогда соединение будет разорвано. Во всех остальных случаях этот режим полностью соответствует автоматическому режиму.

**Режим обучения**

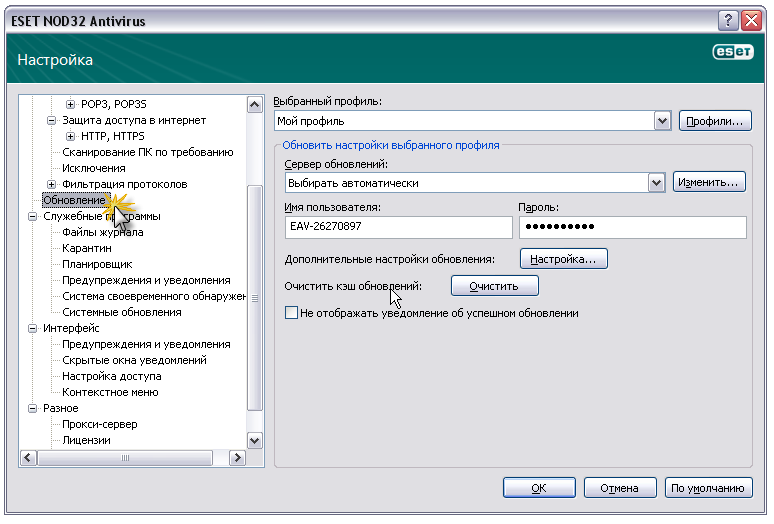
Автоматическое создание и сохранение правил, предназначен для первоначальной настройки персонального брандмауэра. Участие пользователя не требуется, потому что **ESET Smart Security** сохраняет правила согласно предварительно настроенным параметрам. Режим обучения является небезопасным, поэтому рекомендуется использовать его только до момента создания правил для всех необходимых соединений.

**Оффлайн обновление NOD32 – обновление сигнатур угроз из локальной папки**

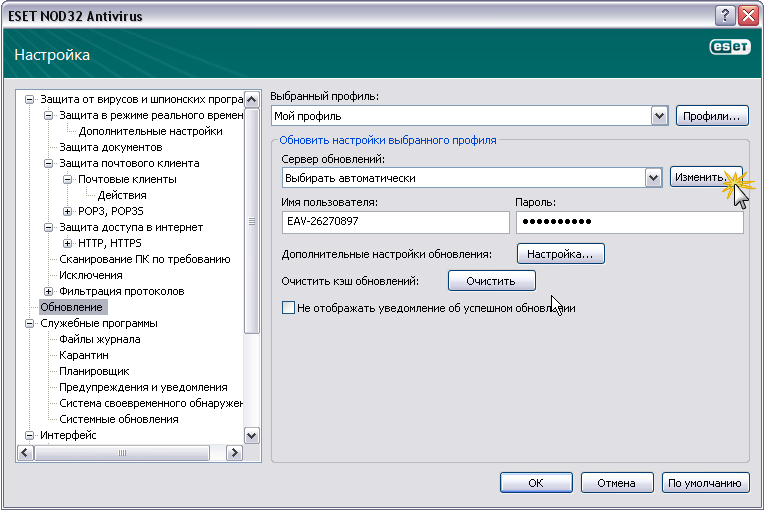
1. Открыть главное окно NOD32(в правом нижнем углу экрана щелкнуть правой кнопкой по значку).



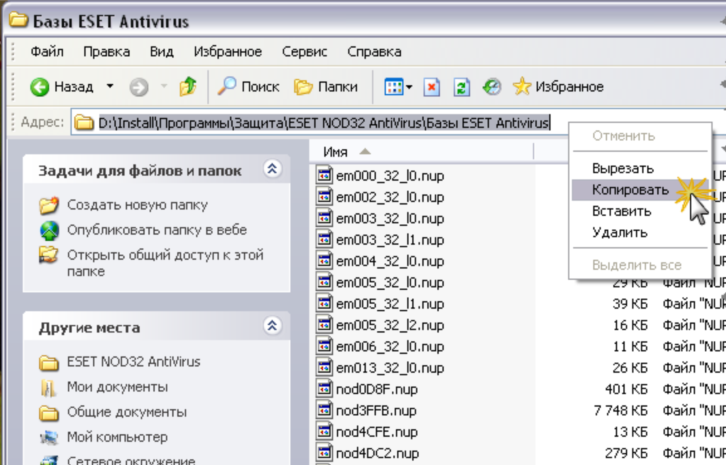
1. Нажать F5 для управления настройками NOD32 и выбрать пункт Обновление.



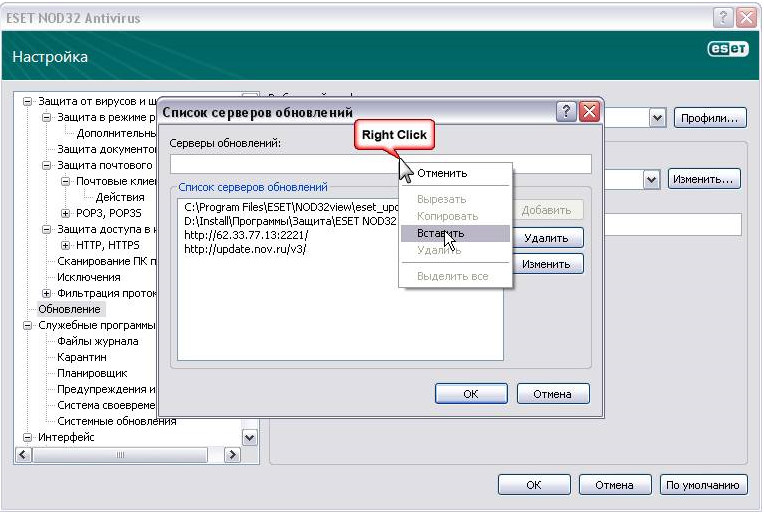
1. В NOD-e (в настройках обновления) нажать Изменить



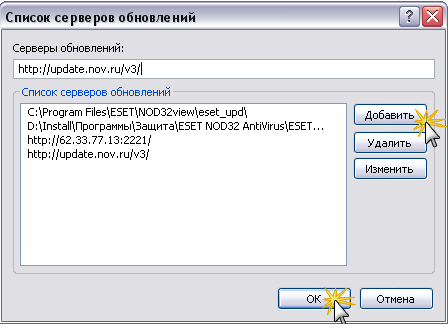
1. Скопировать путь к папке с сигнатурами угроз



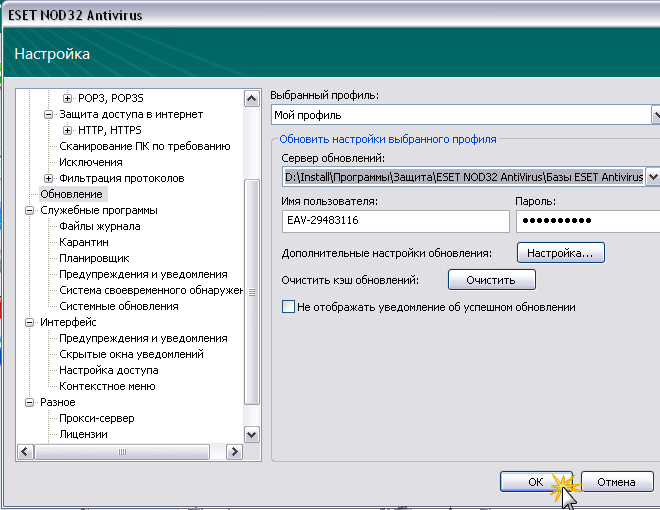
1. После, как показано ниже, вставить путь к папке с сигнатурами угроз (который был скопирован ранее).



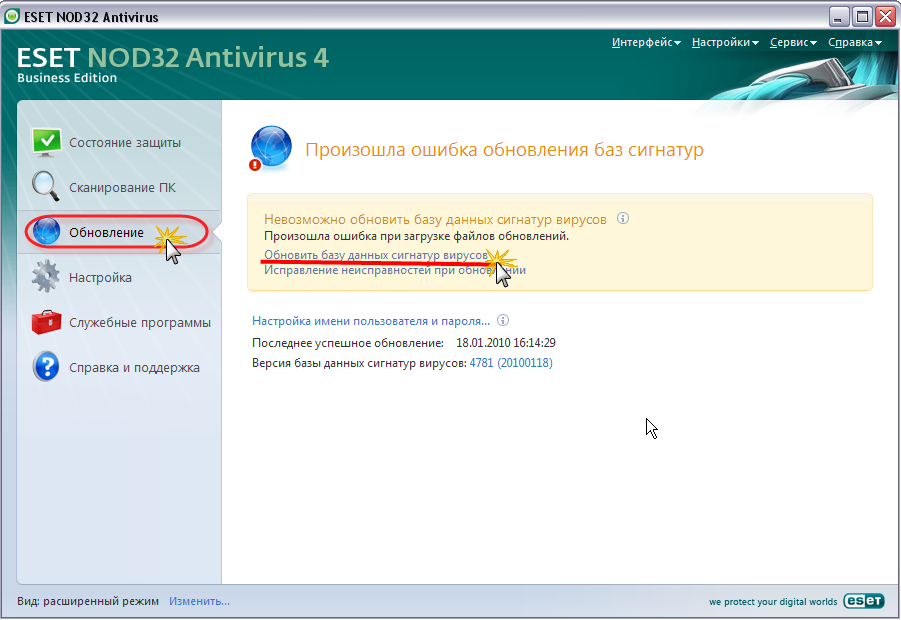
1. Затем нажать: 1. Добавить и 2. ОК



1. Нажать ОК для применения настроек.

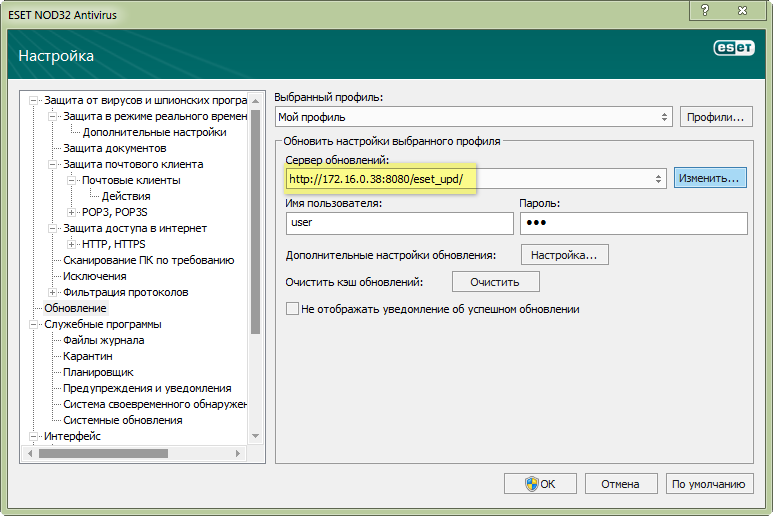


1. Далее перейдите на вкладку Обновление и нажмите Обновить базу данных сигнатур вирусов.

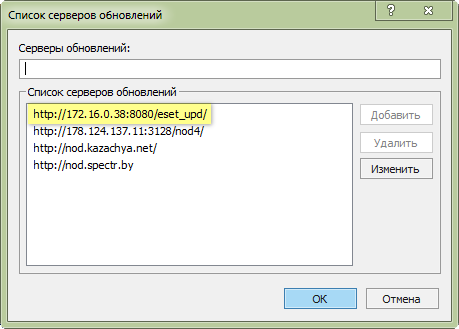


Для обновления вирусных баз с локального сервера по HTTP настройки производятся следующим образом:

1)необходимо нажать изменить

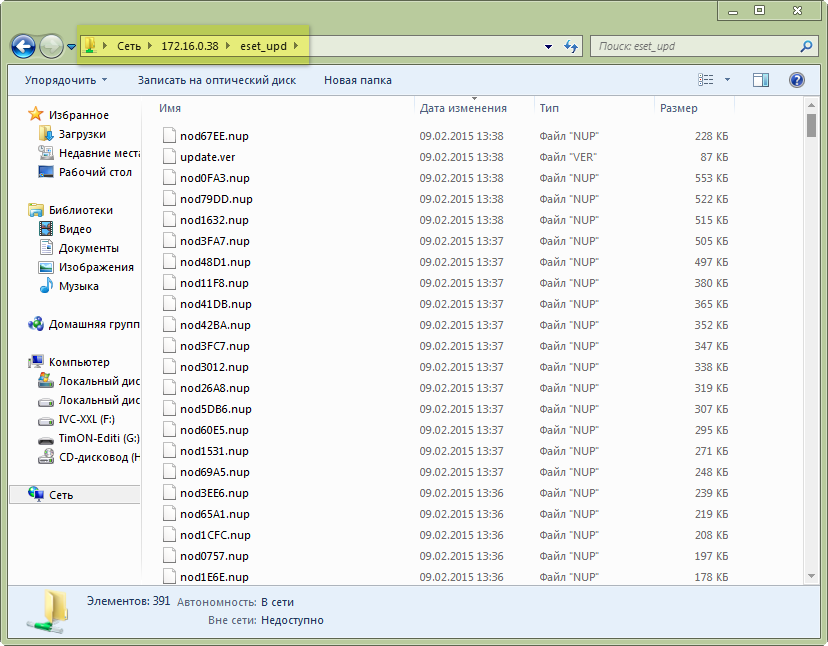


2) в открывшемся меню вводим необходимый адрес и нажимаем добавить.



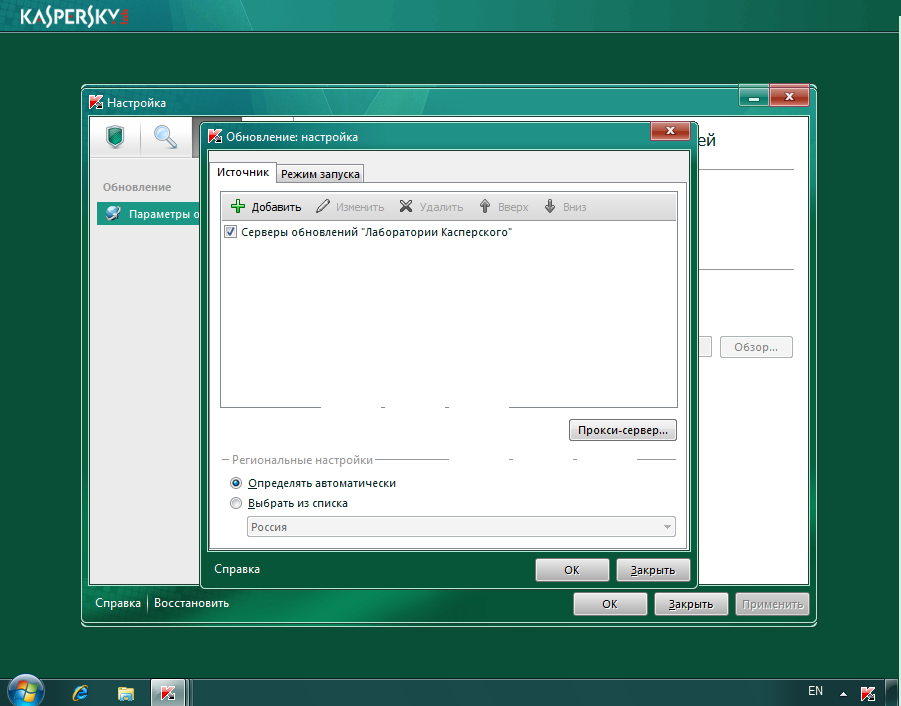
3) вернувшись в предыдущее окно вводим имя пользователя и пароль

Файлы обновлений можно увидеть по введенному адресу и данным пользователя через проводник



**Настройка сервера обновлений в антивирусе KASPERSKY**

Настройка сервера обновлений в антивирусе KASPERSKY производится в данном окне:

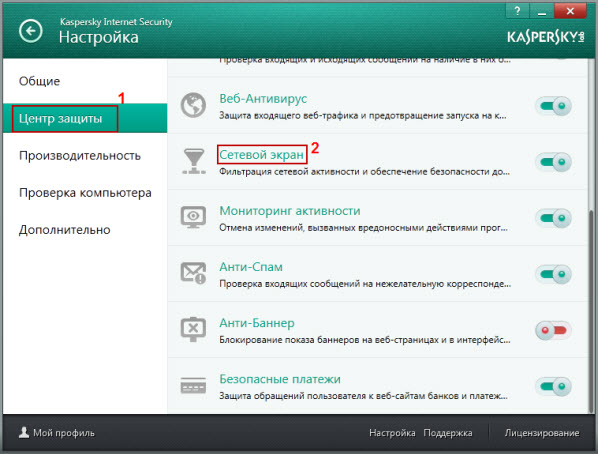


Чтобы заблокировать выход конкретной программы в интернет, вы можете создать правило для программы в Сетевом экране. Для этого выполните следующие действия:

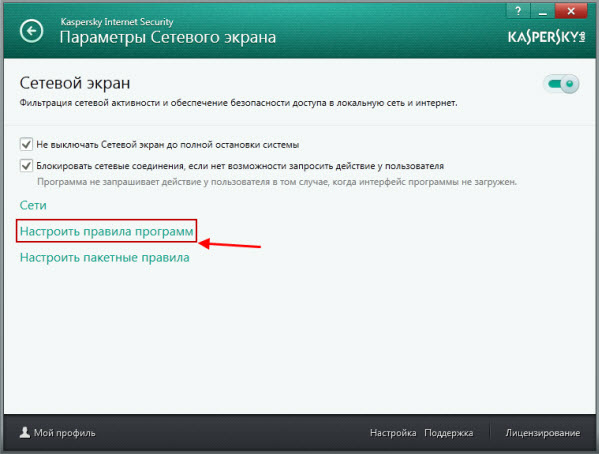
1. [Откройте Kaspersky Internet Security 2014](http://support.kaspersky.ru/10075).
2. В правом нижнем углу нажмите на ссылку Настройка.



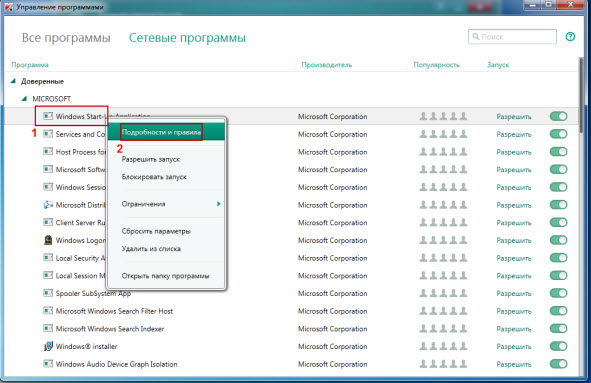
1. В окне **Настройка** перейдите в раздел **Центр защиты** и выберите пункт **Сетевой экран**.



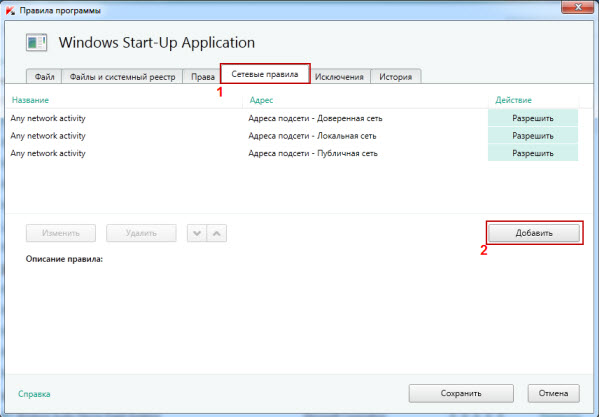
1. В окне **Параметры Сетевого экрана** нажмите на ссылку **Настроить правила программ**.



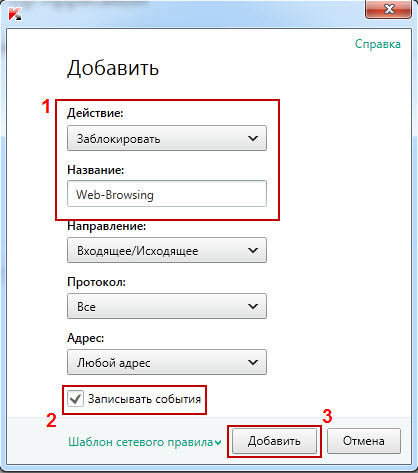
1. В окне **Управление программами** нажмите правой кнопкой мыши на необходимую вам программу и в контекстном меню выберите пункт **Подробности и правила**.



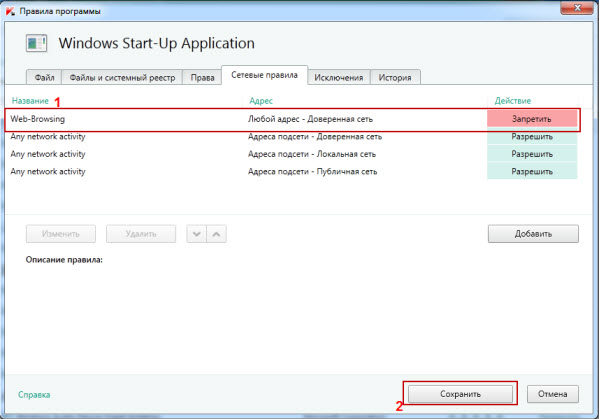
1. В окне **Правила программы** перейдите на закладку **Сетевые правила** и нажмите на кнопку **Добавить**.



1. В окне **Добавить** в разделе **Действие** выберите **Заблокировать**.
2. В разделе **Название** введите **Web-Browsing**.
3. Если вы хотите, чтобы результат данного сетевого правила фиксировался в отчете, то установите флажок **Записывать события**.
4. Нажмите на кнопку **Добавить**.



1. На закладке **Сетевые правила** появится правило со значком **Запретить**.
2. В окне **Правила программы** нажмите на кнопку **Сохранить**.



1. Закройте окно **Управление программами**.

**Задание к выполнению**

1. Настроить режим фильтрации файервола антивируса (один из описанных в теоретическом введении).
2. Настроить **Оффлайн обновление сигнатур угроз из локальной папки**
3. Настроить **Оффлайн обновление сигнатур угроз из локального сервера**

В электронный конспект поместить копии экрана с пояснениями проведенных действий).