Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Практическое занятие №5**

**Тема «Настройка антивирусов»**

Студент: Городилов М. П.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**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**(рис.5.1) выбрать нужный режим фильтрации и нажать кнопку **OK**.

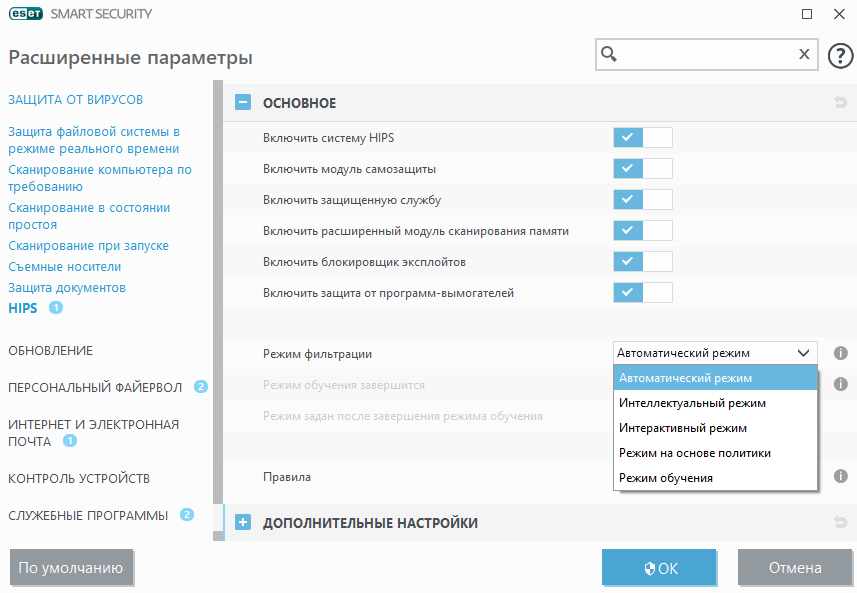


Рисунок 5.1 – Режим фильтрации

Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

**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.

**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.

**Задание к выполнению**

**1. Настройка режима фильтрации файервола антивируса.**

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.

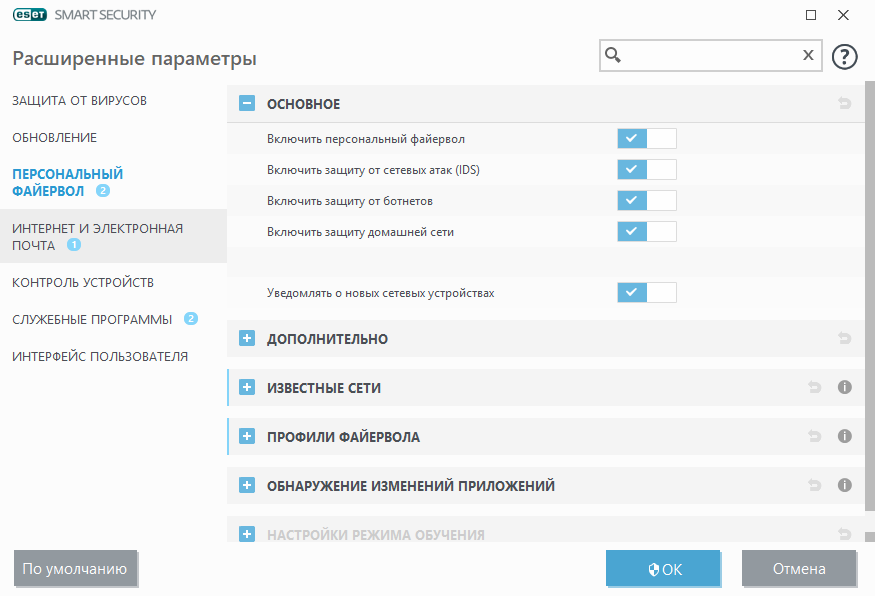


Рисунок 5.2 – Настройка файервола Eset Smart Security.

C помощью клавиши F5 заходим в расширенные параметры антивируса и выбираем пункт меню «Персональный файервол» (рис. 5.1). Затем в разделе режим фильтрации выбираем нужный режим. (рис. 5.2).

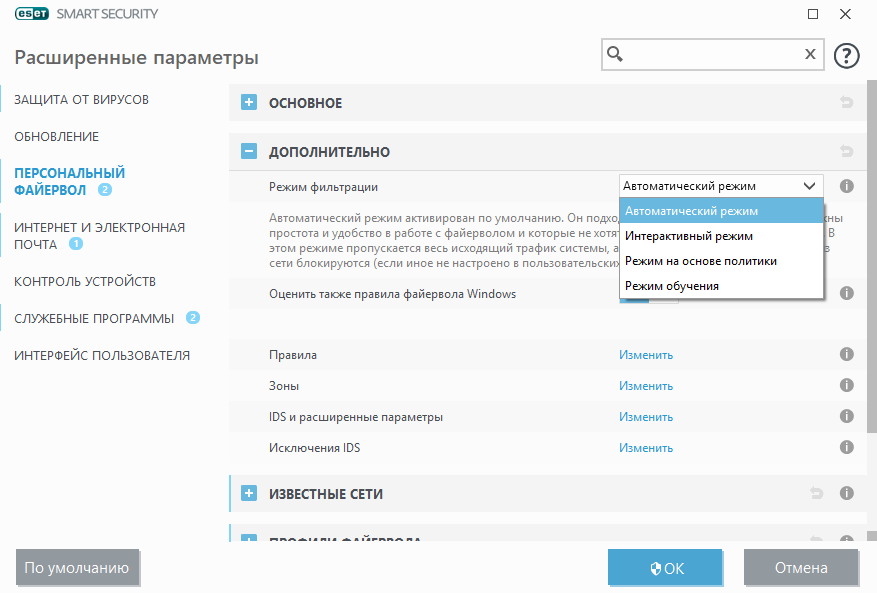


Рисунок 5.3 – Выбор режима фильтрации.

Существуют следующие режимы фильтрации файервола антивируса:

* автоматический режим;
* интерактивный режим;
* режим на основе политики;
* режим обучения.

**2. Настройка Оффлайн обновления сигнатур угроз из локальной папки.**

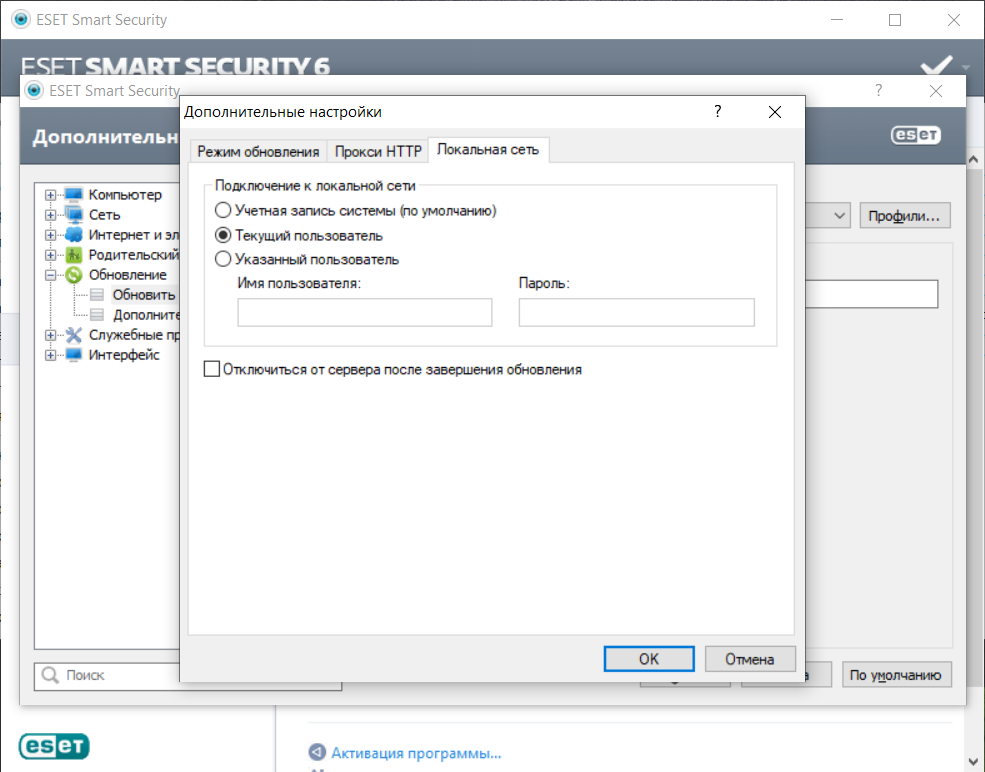


Рисунок 5.4 – Оффлайн обновление.

Для [обновления](https://support.kaspersky.ru/6582) компьютеров по локальной сети или отдельно стоящих компьютеров был реализован процесс ретрансляции антивирусных баз и программных модулей в локальный источник (папку на диске, сетевой ресурс). Для организации обновления антивирусных баз из локальной папки необходим как минимум один компьютер, имеющий доступ к сети Интернет.

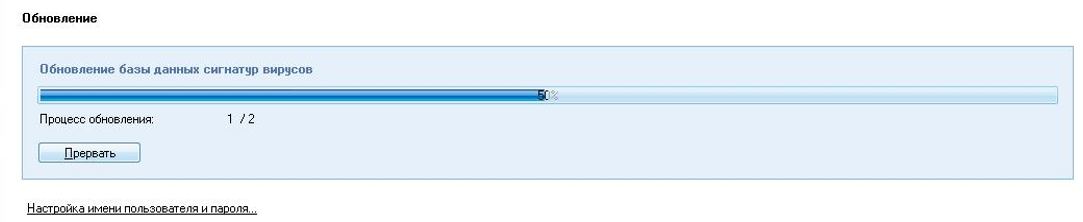


Рисунок 5.5 – Обновление баз данных.

Если у вас в локальной сети установлено несколько копий антивируса, то обновление для каждой копии можно настроить из локальной папки с помощью ретрансляции (приема и передачи) баз в эту папку.

**3. Настройка Оффлайн обновления сигнатур угроз с локального сервера по HTTP**

Вы можете настроить ваши клиенты  для загрузки обновления сигнатур вирусов напрямую с серверов компании ESET через интернет. Вы можете выбрать этот метод, если ваш локальный сервер является ненадежным или работает не постоянно. Таким образом, ваши клиенты будут иметь возможность производить обновления, если ваш сервер не работоспособен. Кроме того, ваши клиенты получат обновления моментально после их выхода на серверах ESET, а не будут дожидаться планового обновления на вашем сервере.

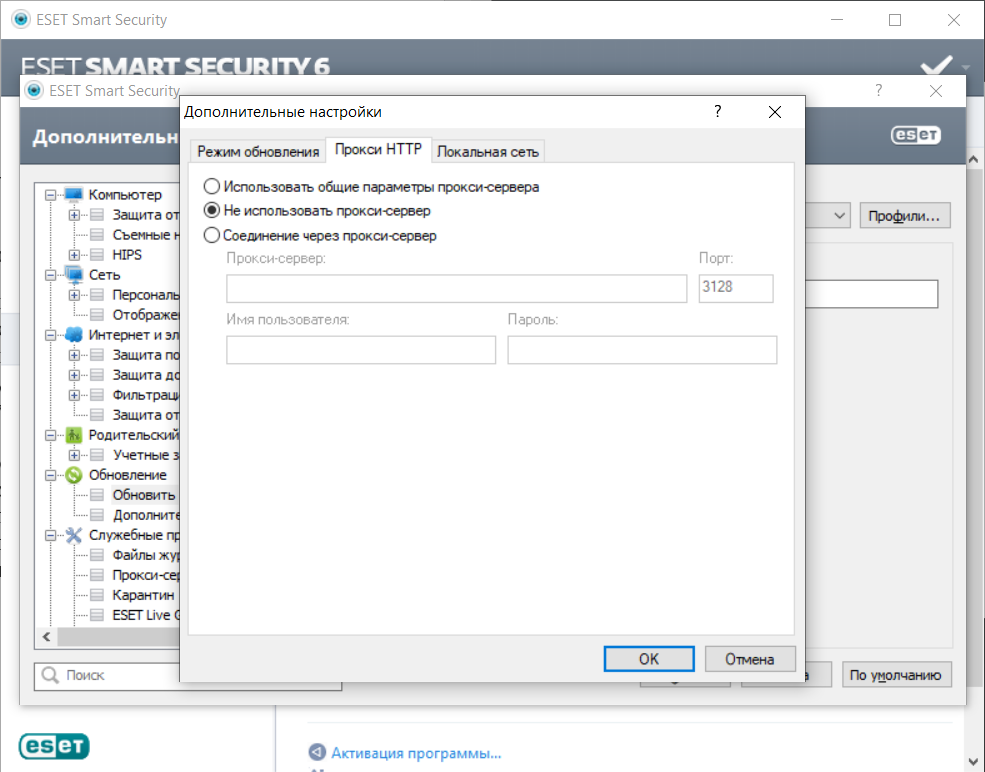


Рисунок 5.6 – Обновление по HTTP

**Вывод**

Антивирус – программа, специально разработанная для обнаружения и удаления компьютерных вирусов и вредоносных программ других типов.

Современные антивирусные программы способны эффективно обнаруживать вредоносные объекты внутри файлов программ и документов. В некоторых случаях антивирус может удалить тело вредоносного объекта из зараженного файла, восстановив файл.

Антивирус способен в большинстве случаев удалить вредоносный программный объект не только из программного файла, но и из файла офисного документа, не нарушив его целостность.

Использование антивирусных программ не требует высокой квалификации и доступно практически любому пользователю компьютера.