Методические рекомендации к практическому занятию №6

С.А. Краснов

УСТАНОВКА И НАСТРОЙКА СР-ВА АНТИВИРУСНОЙ ЗАЩИТЫ «KASPERSKY ENDPOINT SECURITY ДЛЯ «WINDOWS»

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ № 6

**УСТАНОВКА И НАСТРОЙКА СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ «KASPERSKY ENDPOINT SECURITY ДЛЯ «WINDOWS»**

***Цель работы.*** Получить практические навыки настройки САВЗ «***Kaspersky Endpoint Security***».

***Теоретические сведения.*** «Kaspersky Endpoint Security» обеспечивает комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак.

Каждый тип угроз обрабатывается отдельным компонентом. Компоненты можно включать и выключать независимо друг от друга, а также настраивать параметры их работы.

К компонентам контроля относятся следующие компоненты программы:

Контроль запуска программ. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

Контроль активности программ. Компонент регистрирует действия, совершаемые программами в операционной системе, и регулирует деятельность программ исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к персональным данным пользователя и ресурсам операционной системы. К таким данным относятся файлы пользователя (папка «Мои документы», файлы cookie, данные об активности пользователя), а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.

Мониторинг уязвимостей. Мониторинг уязвимостей в режиме реального времени проверяет программы, запущенные на компьютере пользователя, а также проверяет программы в момент их запуска.

Контроль устройств. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски, съемные носители информации, ленточные накопители, CD/DVD-диски), инструментами передачи информации (например, модемы), инструментами превращения информации в твердую копию (например, принтеры) или интерфейсами, с помощью которых устройства подключаются к компьютеру (например, USB, Bluetooth, Infrared).

Веб-Контроль. Компонент позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

К компонентам защиты относятся следующие компоненты программы:

Файловый Антивирус. Компонент позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте САВЗ, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных дисках. Файловый Антивирус перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.

Мониторинг системы. Компонент собирает данные о действиях программ на компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты компьютера.

Почтовый Антивирус. Компонент проверяет входящие и исходящие почтовые сообщения на наличие в них вирусов и других программ, представляющих угрозу.

Веб-Антивирус. Компонент проверяет трафик, поступающий на компьютер пользователя по протоколам HTTP и FTP, а также устанавливает принадлежность ссылок к вредоносным или фишинговым веб-адресам.

IM-Антивирус. Компонент проверяет трафик, поступающий на компьютер по протоколам программ для быстрого обмена сообщениями. Компонент обеспечивает безопасную работу со многими программами, предназначенными для быстрого обмена сообщениями.

Сетевой экран. Компонент обеспечивает защиту личных данных, хранящихся на компьютере пользователя, блокируя все возможные для операционной системы угрозы в то время, когда компьютер подключен к интернету или к локальной сети.

Мониторинг сети. Компонент предназначен для просмотра в режиме реального времени информации о сетевой активности компьютера.

Защита от сетевых атак. Компонент отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, САВЗ блокирует сетевую активность атакующего компьютера.

В программе «Kaspersky Endpoint Security» предусмотрены следующие задачи:

Полная проверка. САВЗ выполняет тщательную проверку операционной системы, включая системную память, загружаемые при старте объекты, резервное хранилище операционной системы, а также все жесткие и съемные диски.

Выборочная проверка. САВЗ проверяет объекты, выбранные пользователем.

Проверка важных областей. «Kaspersky Endpoint Security» проверяет объекты, загрузка которых осуществляется при старте операционной системы, системную память и объекты заражения руткитами.

Обновление. «Kaspersky Endpoint Security» загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты компьютера от новых вирусов и других программ, представляющих угрозу.

Поиск уязвимостей. САВЗ проверяет операционную систему и установленное программное обеспечение на наличие уязвимостей. Это позволяет диагностировать и своевременно решать возможные проблемы, которые могут быть использованы злоумышленниками.

***Постановка задачи.*** Выполнить все шаги работы, необходимые для осуществления настройки средства антивирусной защиты. Результаты зафиксировать в отчете.

***Последовательность действий.***

Шаг 1. Выполнить настройку обновления вирусных баз.

Шаг 2. Выполнить настройку файлового антивируса.

Шаг 3. Выполнить настройку почтового антивируса.

Шаг 4. Выполнить настройку веб-антивируса.

Шаг 5. Выполнить настройку IM-антивируса.

Шаг 6. Выполнить настройку сетевого экрана.

Шаг 7. Выполнить настройку защиты от сетевых атак.

Шаг 8. Выполнить настройку мониторинга системы.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке средства антивирусной защиты.

Для решения задачи в приложение Г представлен пример настройки средства антивирусной защиты. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [4, 5].

**ПРИЛОЖЕНИЕ Г**

**Пример настройки САВЗ «Kaspersky Endpoint Security»**

**Настройка обновления вирусных баз.** Необходимо выполнить следующие действия:

- необходимо определить к какой группе относится АРМ:

1. автономное рабочее место, не имеющее подключения к Интернет;

2. рабочее место, имеющее подключение к Интернет;

3. рабочее место, управляемое Kaspersky Security Center (далее - KSC).

## АРМ, не имеющий подключения к сети Интернет

- создать в корневом каталоге системного диска директорию для обновлений баз вирусных сигнатур (далее – БВС) с названием Updates (например: D:\Updates\).

- произвести настройку прав доступа к данной директории, для этого:

- отключить общий доступ к файлам (Панель управления; в правом верхнем углу в пункте «Просмотр:» выбрать пункт «Крупные значки» или «Мелкие значки»; «Параметры папок»; вкладка «Вид»; убрать флажок «Использовать мастер общего доступа (рекомендуется)»);

- нажать правой кнопкой «мыши» по директории «D:\Updates\»; «Свойства»; вкладка «Безопасность». В поле «Группы или пользователи» выбрать необходимого пользователя или группу, при необходимости добавить отсутствующих в списке пользователей или групп, нажав «Добавить» и введя имя пользователя или название группы. В поле «Разрешения для ...» выбрать разрешить «Полный доступ». Для этого в свойствах данной директории необходимо выбрать вкладку «Безопасность» и установить пользователям или группе пользователей полный доступ.

- разархивировать архив с актуальным полным комплектом БВС, загруженный ранее;

- скопировать каталоги AutoPatches, bases, index из директории с полным комплектом БВС в директорию D:\Updates\.

Для настройки задачи обновления необходимо:

- в окне программы на вкладке «Настройка» в разделе «Задачи по расписанию» выбрать пункт «Обновление»;

- в окне настроек обновления в поле «Режим запуска и источник обновлений» в пункте «Режим запуска» указать «Вручную»;

- в поле «Дополнительно» убрать галочку напротив пункта «Обновлять модули программы»;

- в поле «Прокси-сервер» нажать кнопку «Настройка...». В открывшемся окне «Параметры прокси-сервера» убрать галочку напротив пункта «Использовать прокси-сервер». Нажать кнопку «OK» (рис. 39);

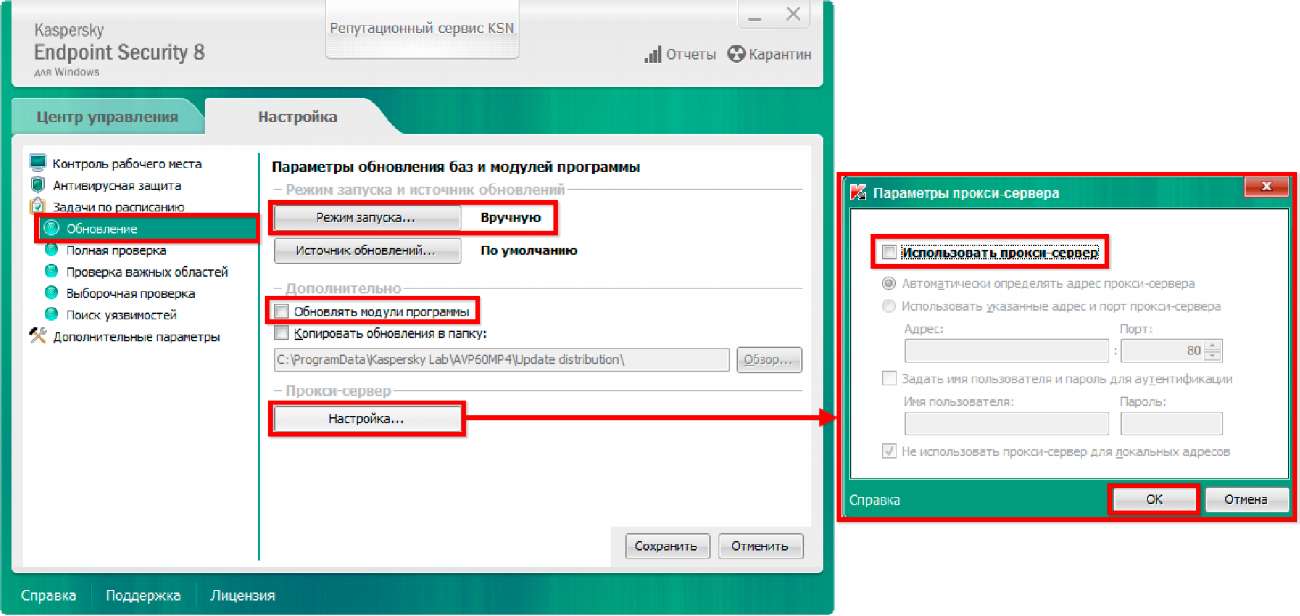


Рисунок 39. Настройка параметров обновления БВС для автономного рабочего мест АИС, не имеющего подключения к Интернет

- в окне настроек обновления в поле «Режим запуска и источник обновлений» нажать на кнопку «Источник обновлений.» (рис. 40);

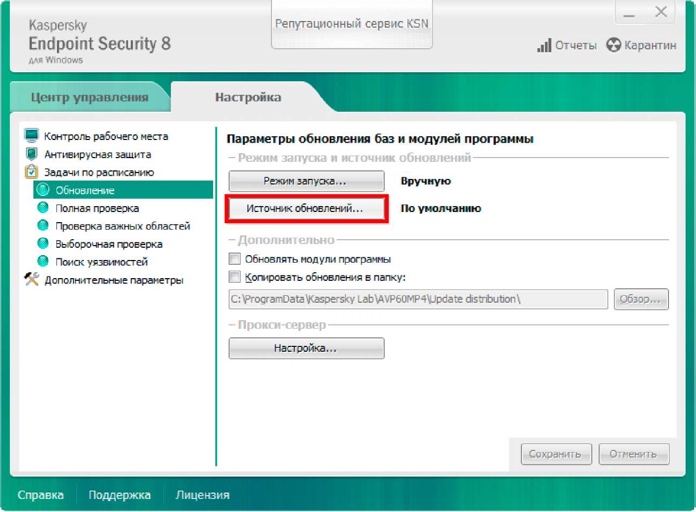


Рисунок 40. Настройка источника обновлений

- в открывшемся окне «Обновление» в разделе «Источник» снять галочки напротив пунктов «Kaspersky Security Center» и «Серверы обновлений "Лаборатории Касперского"». Нажать кнопку «Добавить» и указать путь к папке Updates, содержащую актуальные обновления и нажать кнопку «OK». Далее в окне «Обновление» нажать кнопку «OK» (рис. 41);

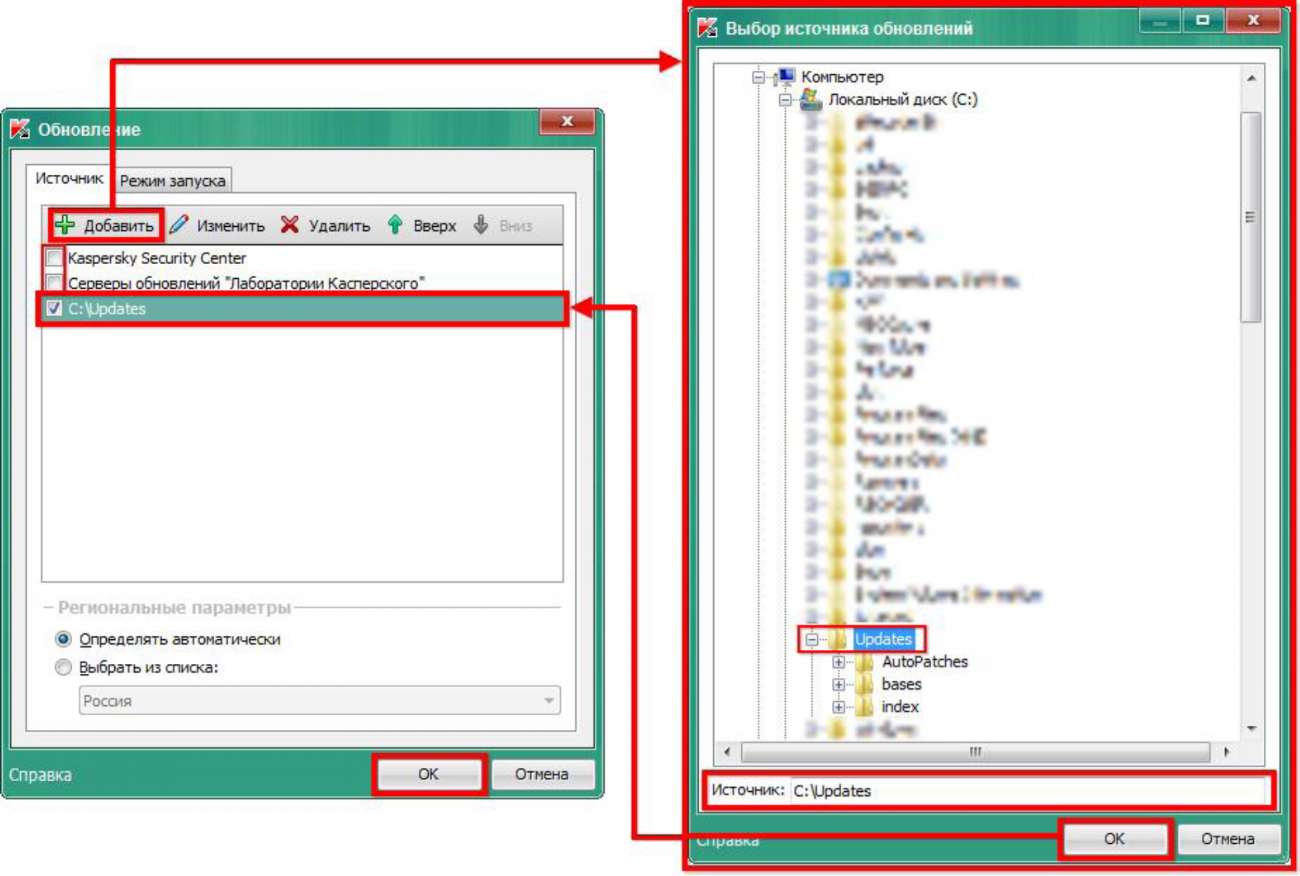


Рисунок 41. Указание источника обновлений

- для запуска обновления необходимо в окне программы на вкладке «Центр Управления» открыть раздел «Управление задачами»;

- в появившемся списке щелкнуть левой кнопкой мыши на задачу «Обновление» и в выпадающем меню выбрать пункт «Запустить обновление» (рис. 42).

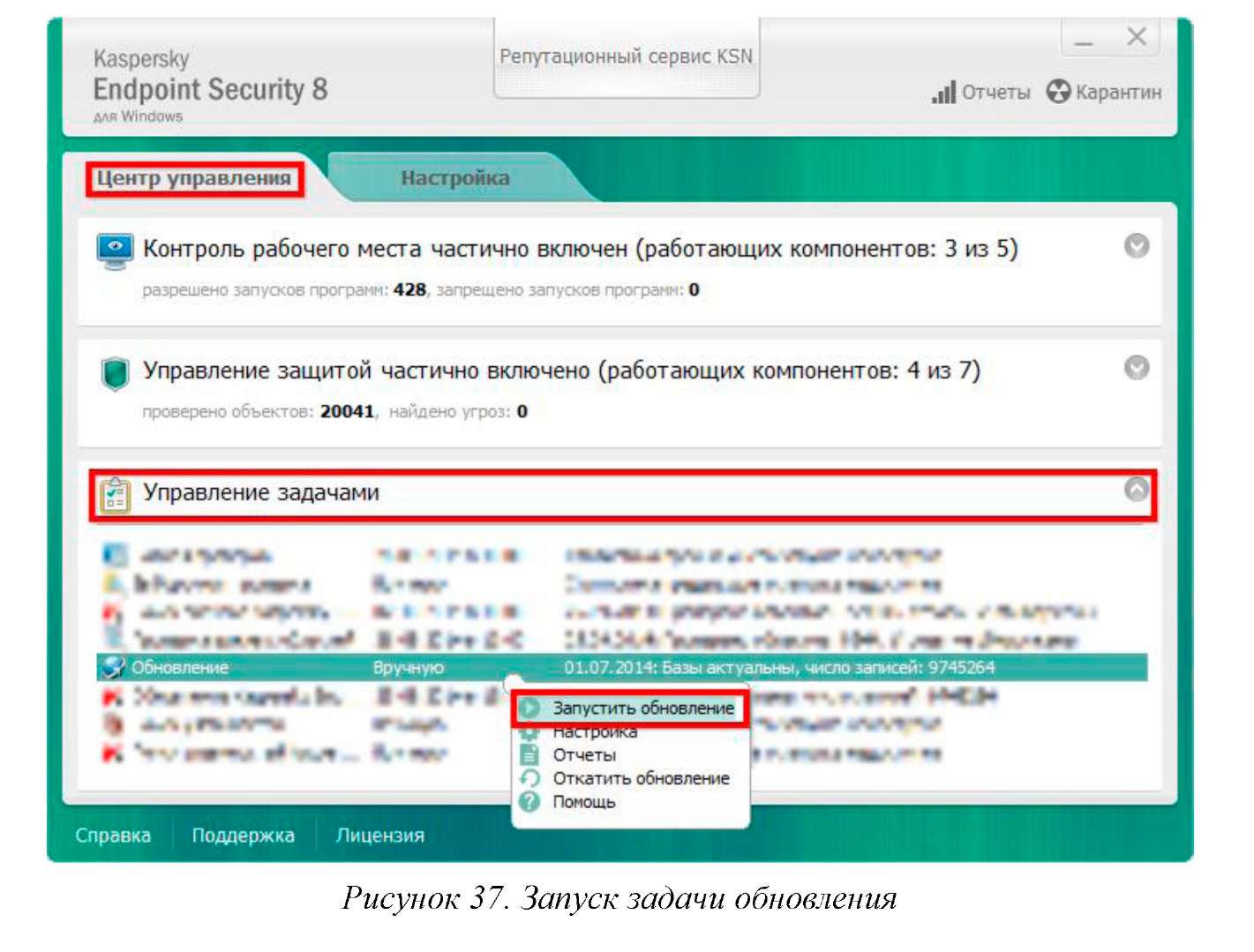


Рис. 42 Запуск обновлений

## АРМ, имеющий подключения к сети Интернет

- в окне программы на вкладке «Настройка» в разделе «Задачи по расписанию» выбрать пункт «Обновление»;

- в поле «Дополнительно» убрать галочку напротив пункта «Обновлять модули программы»;

- в поле «Прокси-сервер» нажать кнопку «Настройка...»;

- в открывшемся окне «Параметры прокси-сервера» убрать галочку напротив пункта «Использовать прокси-сервер». Нажать кнопку «OK» (рис. 43).

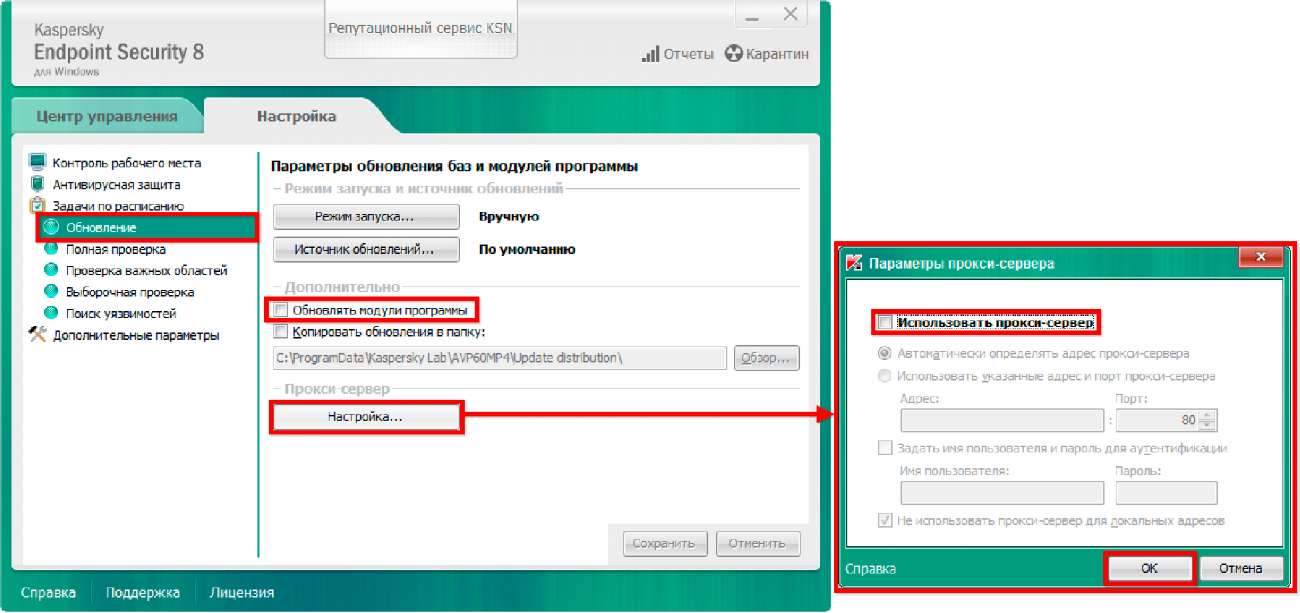


Рисунок 43. Настройка параметров обновления БВС для АИС, имеющего подключение к Интернет

- в поле «Режим запуска и источник обновлений» нажать на кнопку «Источник обновлений»;

- в открывшемся окне «Обновление» на вкладке «Источник» снять галочку напротив пункта «Kaspersky Security Center»;

- перейти на вкладку «Режим запуска»;

- выбрать пункт «По расписанию»;

- в пункте «Периодичность:» выбрать «Часы»;

- в пункте «Выполнять каждые:» ввести необходимое значение. Нажать кнопку «OK» (рис. 44).

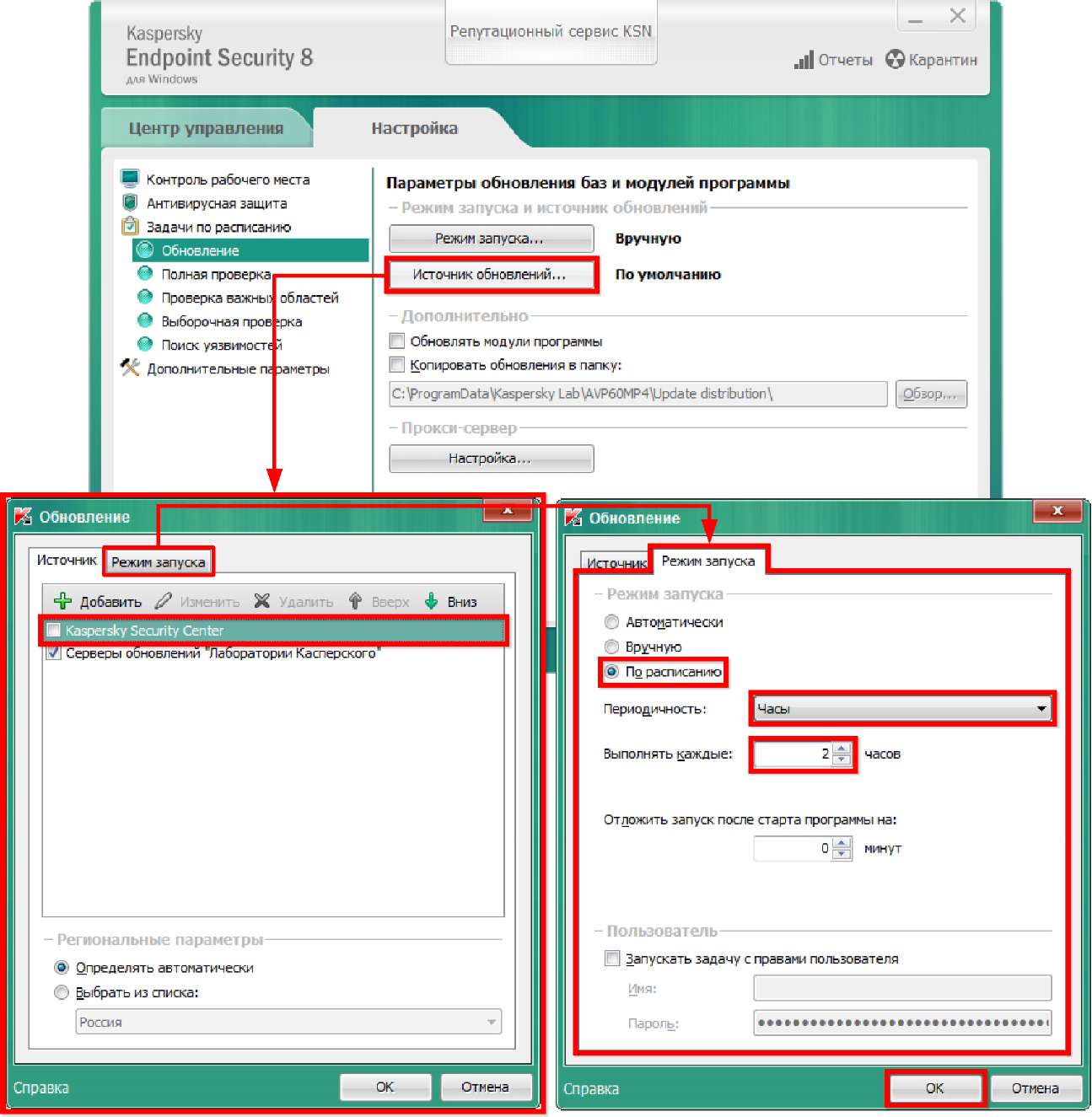


Рисунок 44. Настройка источника и режима запуска задачи обновления БВС

**Настройка файлового антивируса.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку Файловый Антивирус (рис. 45);

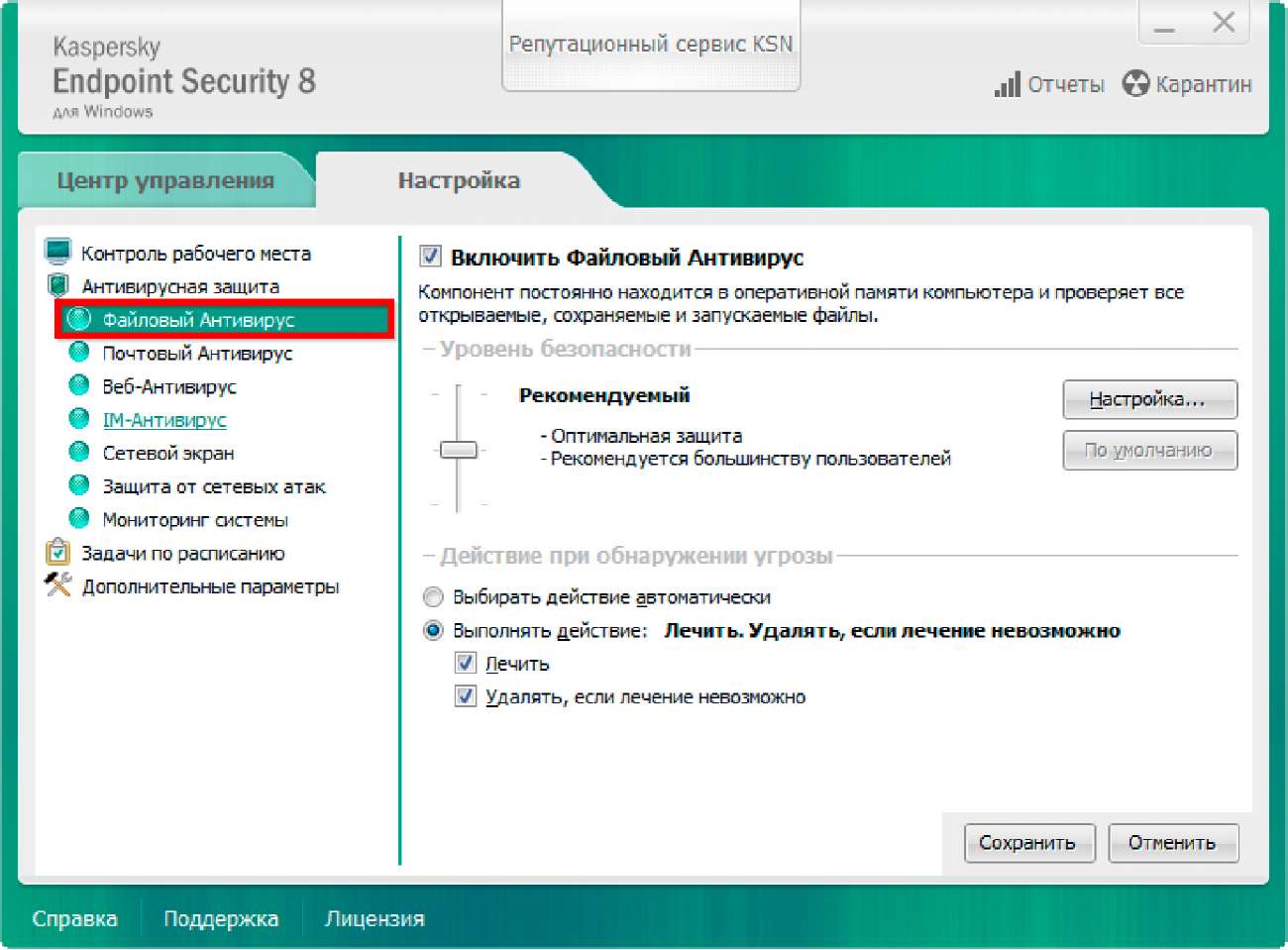


Рисунок 45. Окно настроек файлового антивируса

- в поле «Уровень безопасности» установить необходимый уровень безопасности (рис. 46);

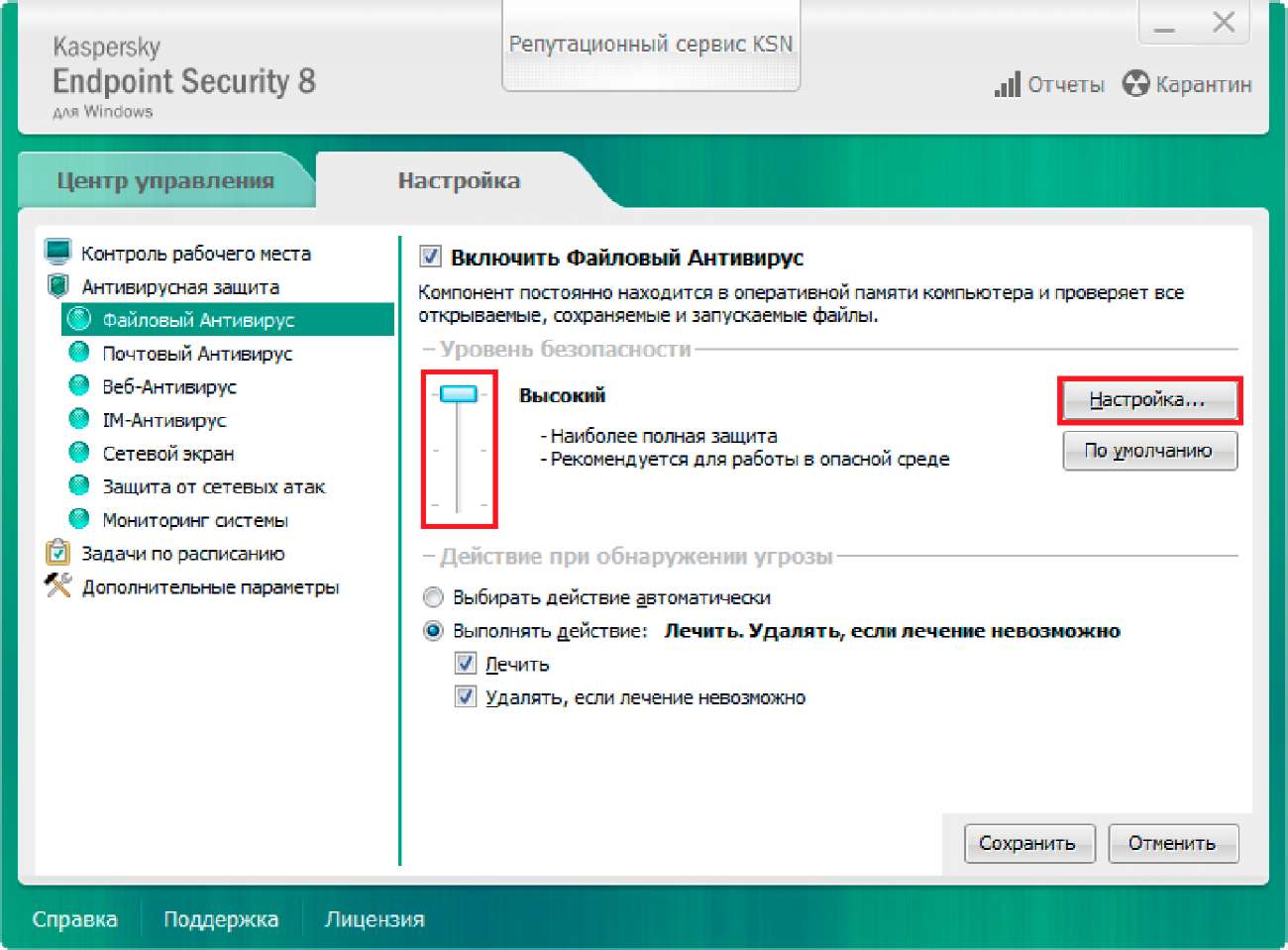


Рисунок 46. Общие параметры файлового антивируса

- далее нажать на кнопку «Настройка». Настройки во вкладке «Общие» оставить без изменений («Типы файлов» - «все файлы», «Область защиты» - «Все съемные диски», «Все жесткие диски», «Все сетевые диски»). Во вкладке «Производительность» выбрать уровень проверки. Настройки в поле «Оптимизация проверки» оставить без изменений. В поле «Проверка составных файлов» в строках «Проверять новые архивы» и «Проверять новые установочные пакеты» слово «новые» заменить на «все» путем нажатия на него, остальные параметры оставить без изменений («Проверять все вложенные OLE-объекты»). В этом же окне нажать на кнопку «Дополнительно». В появившемся окне снять галочку в строке «Не распаковывать составные файлы большого размера», а также удостовериться в отсутствии галочки напротив пункта «Не распаковывать составные файлы большого размера». Далее нажать кнопку «OK» (рис. 47).

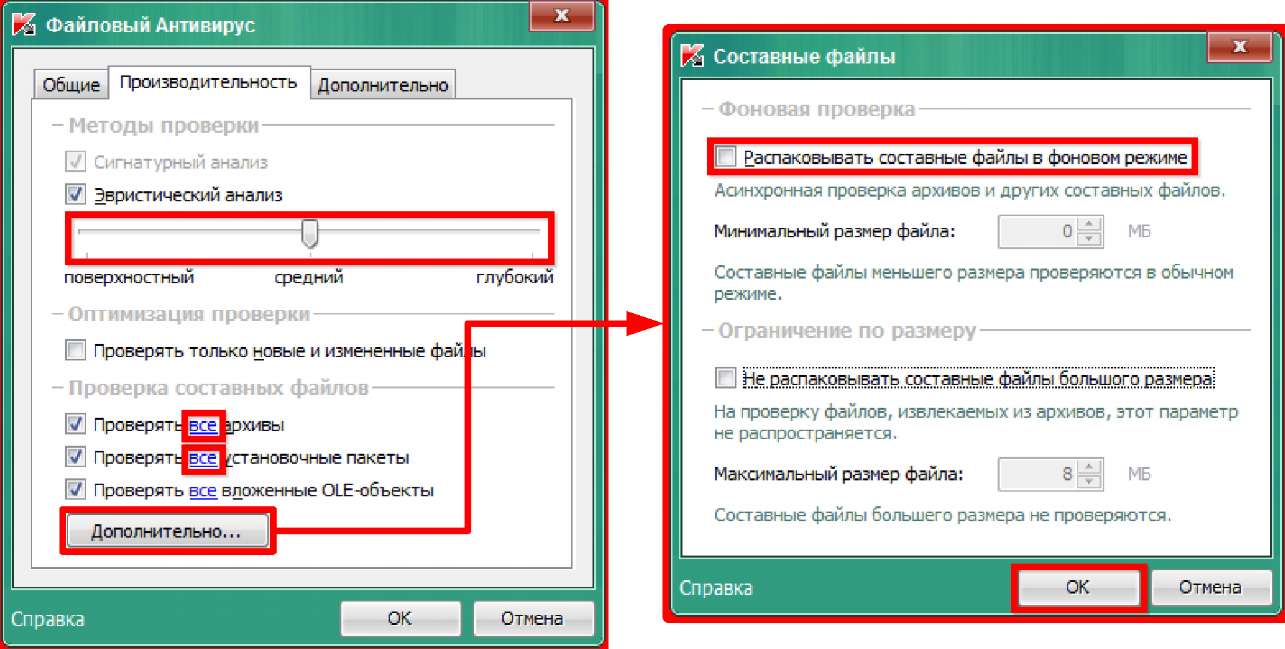


Рисунок 47. Изменение производительности файлового антивируса и настройка проверки составных файлов

- в окне «Файловый Антивирус» нажать кнопку «OK», далее нажать кнопку «Сохранить» в правом нижнем углу.

**Настройка почтового антивируса.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку Почтовый Антивирус (рис. 48);

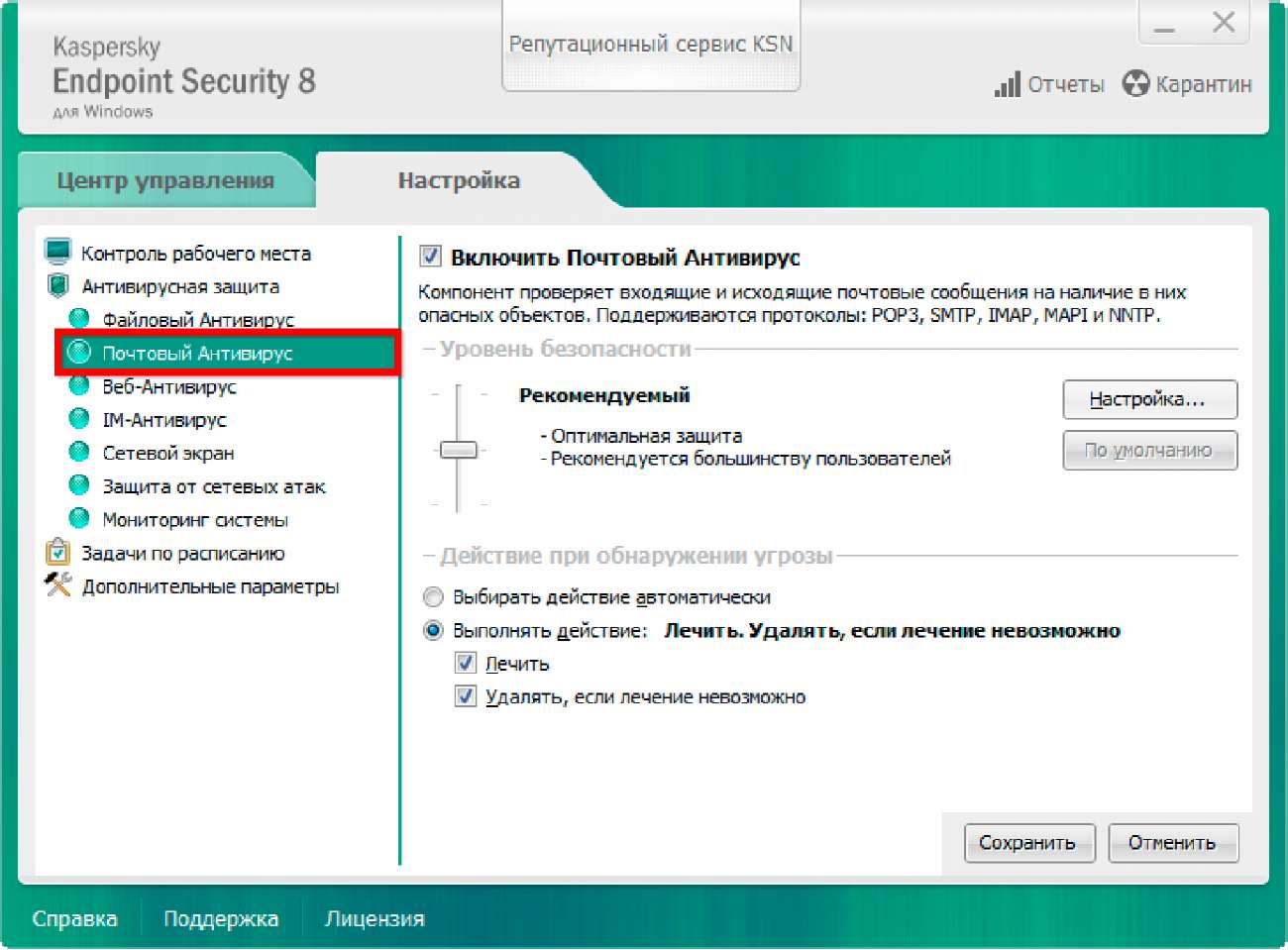


Рисунок 48. Окно настроек почтового антивируса

- в поле «Уровень безопасности» установить необходимый уровень безопасности (рис. 49);

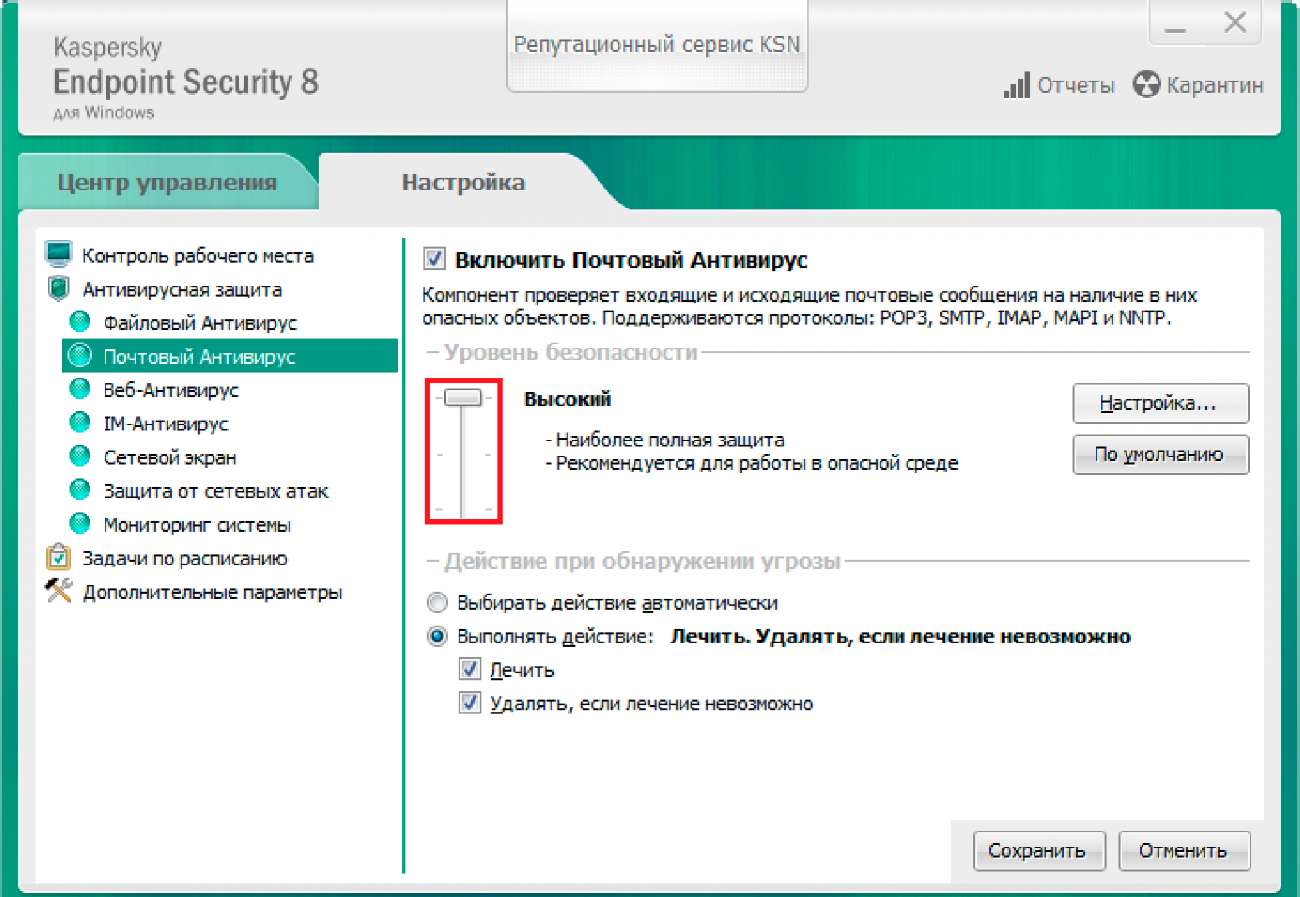


Рисунок 49. Изменение параметров уровня безопасности почтового

антивируса

- нажать на кнопку «Настройка». Перейти во вкладку «Общие». В поле «Встраивание в систему» поставить галочку напротив пункта «Дополнительно: плагин в «Название почтового клиента»» (рис. 50). Остальные настройки оставить без изменений;

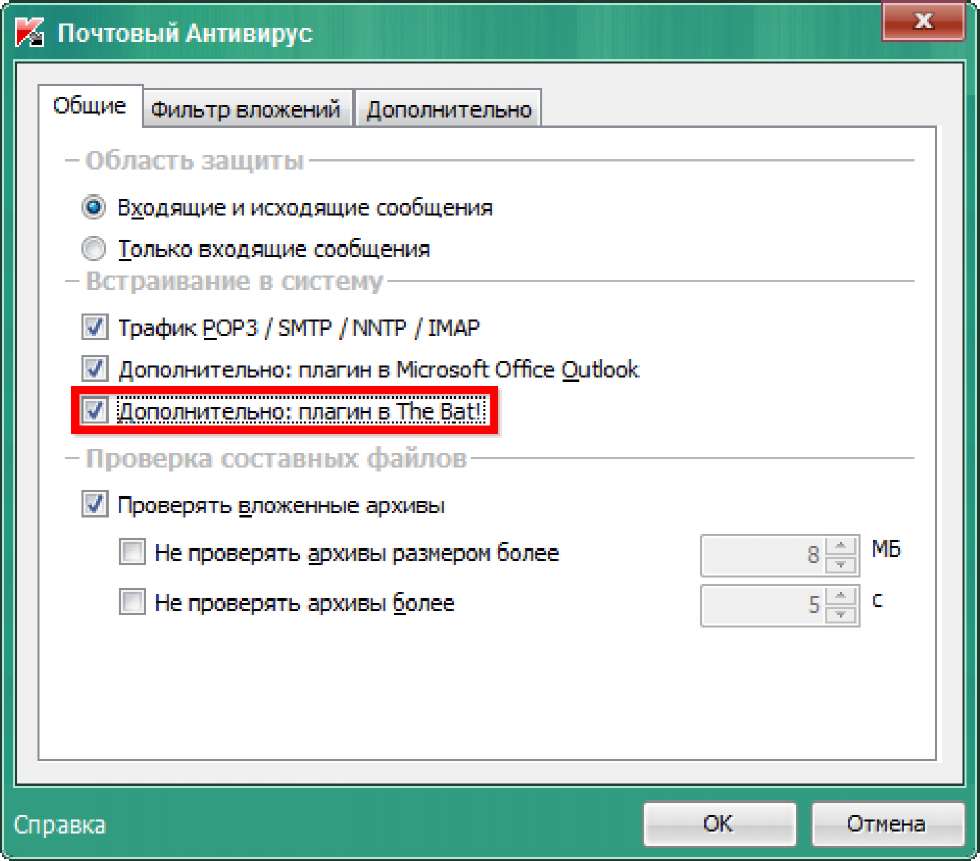


Рисунок 50. Общие настройки почтового антивируса

- Во вкладке «Фильтр вложений» выбрать пункт «Удалять вложения указанных типов». Далее поставить галочки напротив необходимых форматов (рис. 51);

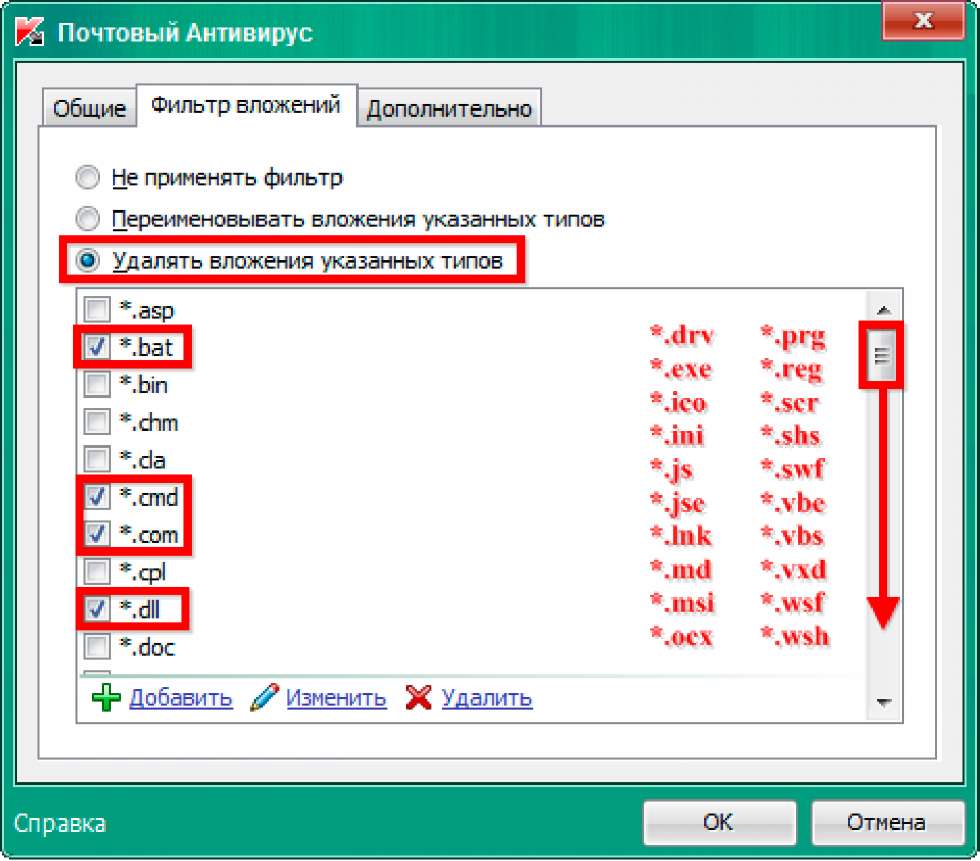


Рисунок 51. Изменение параметров фильтра вложений

- во вкладке «Дополнительно» выбрать уровень проверки эвристическим методом в зависимости от производительности АРМ, но не ниже значения «Средний» (рис. 52);

- нажать кнопку «ОК». Далее нажать кнопку «Сохранить» в правом нижнем углу.

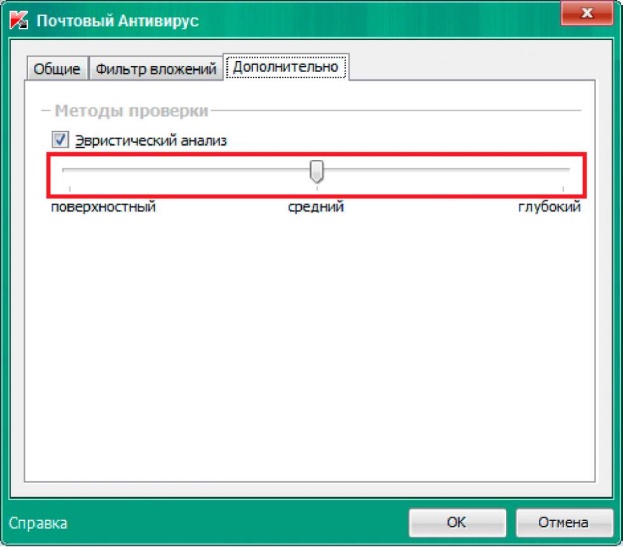


Рисунок 52. Изменение параметров методов проверки

**Настройка веб-антивируса.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку Веб-Антивирус и выполнить необходимые настройки (рис. 53);

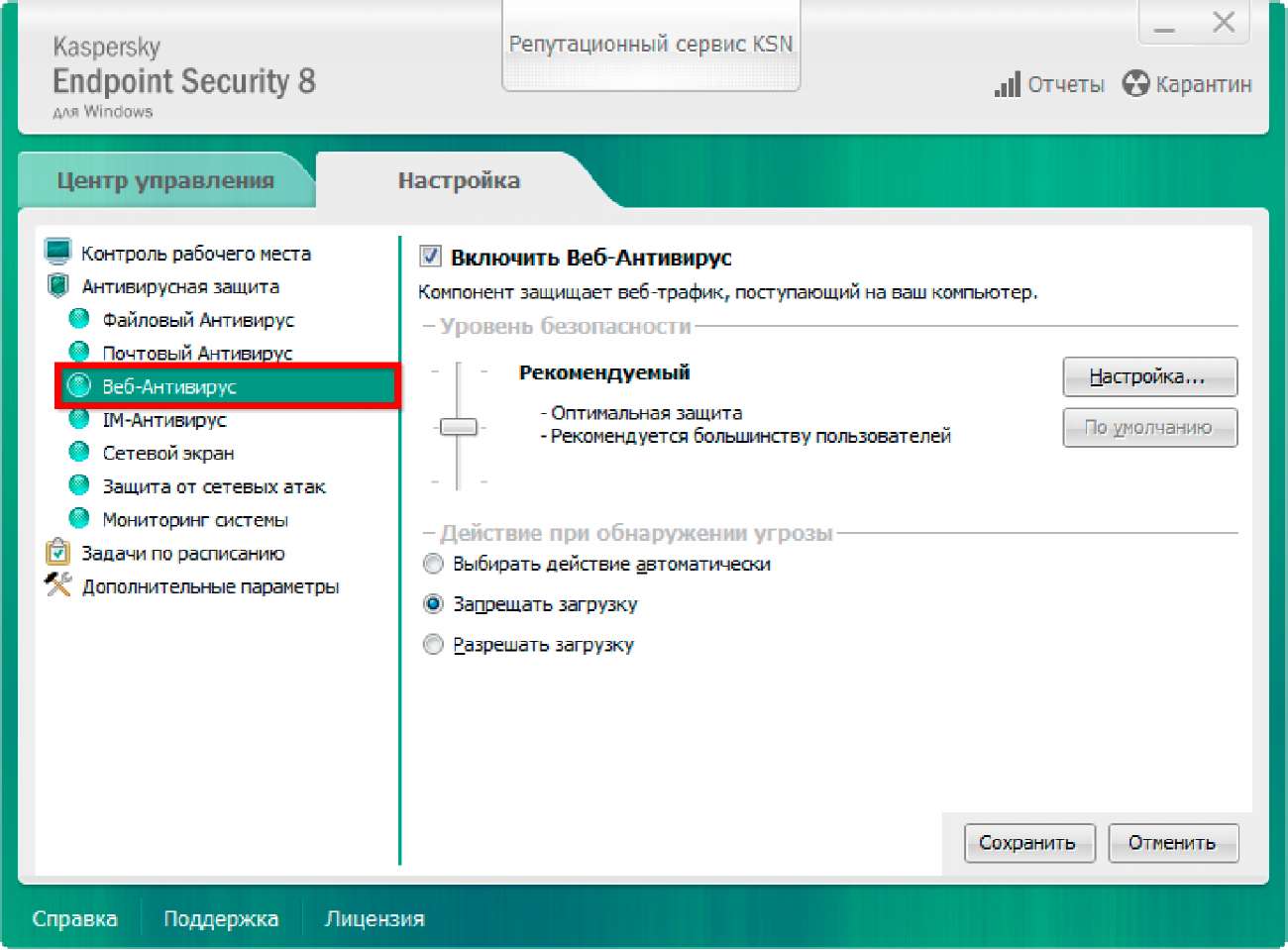


Рисунок 53. Окно настроек веб-антивируса

- Нажать на кнопку «Настройка»;

- в появившемся окне «Веб-Антивирус» настройки во вкладке «Доверенные веб-адреса» выполнить необходимые настройки;

- во вкладке «Общие» для пунктов «Эвристический анализ для обнаружения вирусов» и «Эвристический анализ для обнаружения фишинговых атак» выбрать уровень проверки эвристическим методом в зависимости от производительности АРМ. Установить необходимые параметры в поле «Методы проверки» (рис. 54).

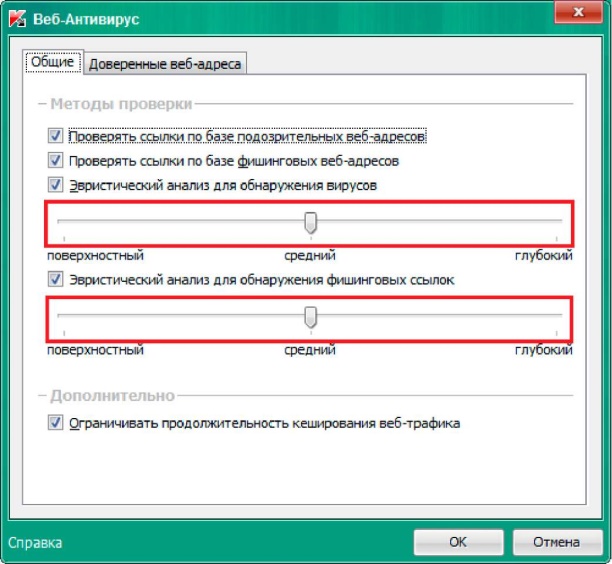


Рисунок 54. Изменение параметров настройки Веб-Антивируса.

- нажать кнопку «ОК». Далее нажать кнопку «Сохранить» в правом нижнем углу.

**Настройка IM-антивируса.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку IM-Антивирус и выполнить необходимые настройки (рис. 55);

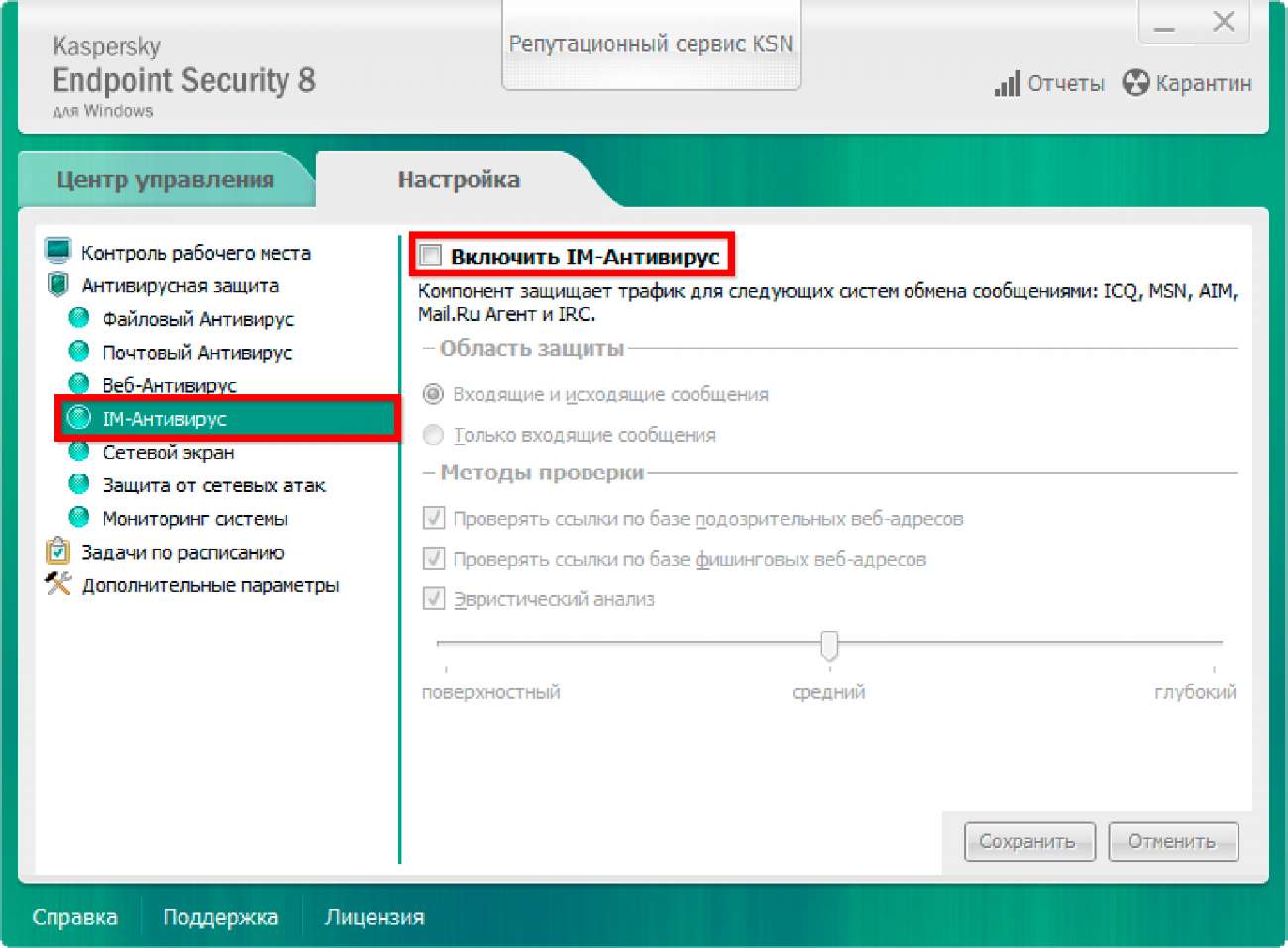


Рисунок 55. Окно настроек IM-антивируса

- нажать кнопку «Сохранить» в правом нижнем углу.

**Настройка сетевого экрана.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку «Сетевой экран» (рис. 56);

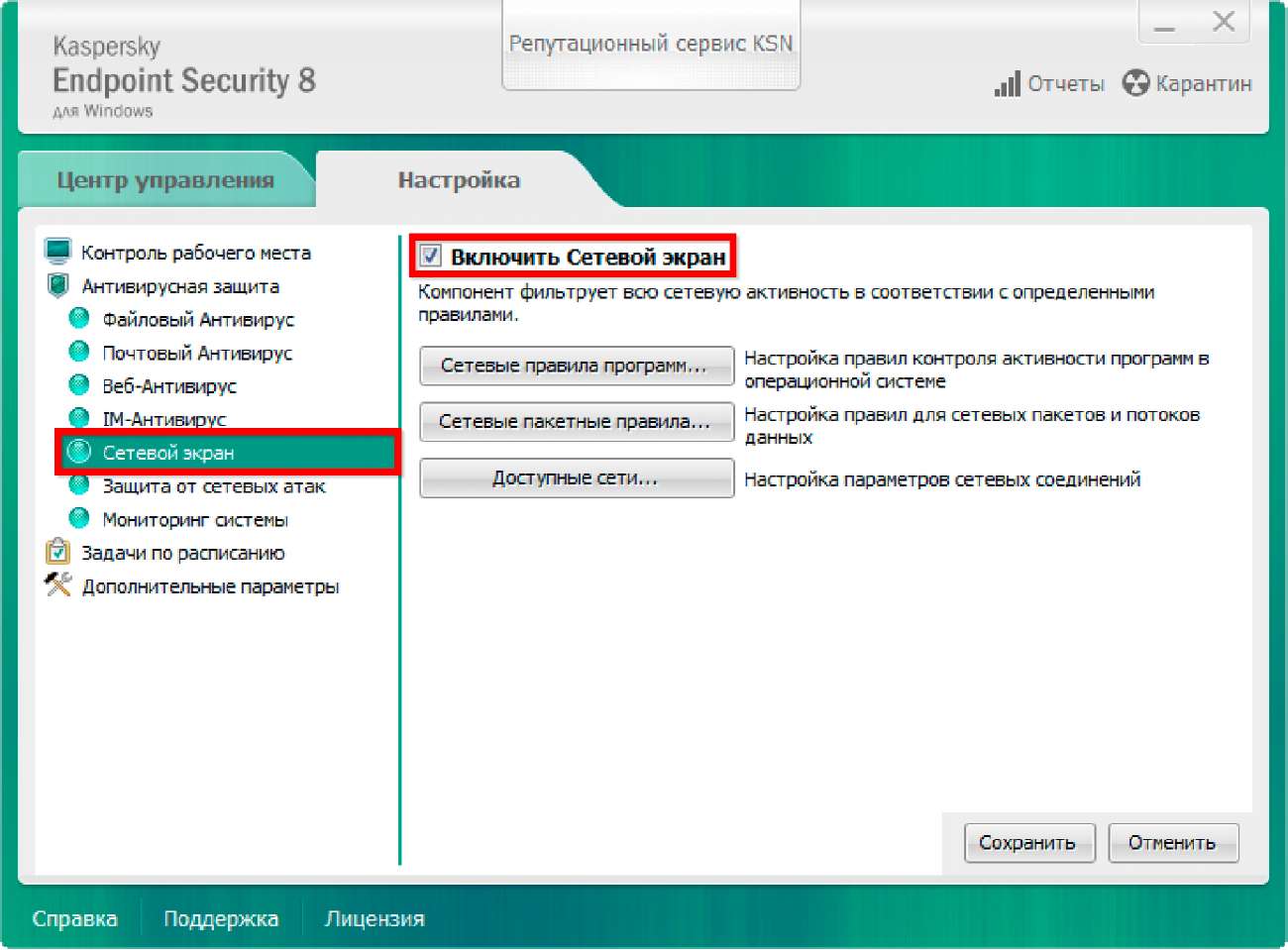


Рисунок 56. Окно настроек сетевого экрана

- далее необходимо определить к какой группе относится настраиваема ЭВМ:

1. ЭВМ, не входящая в состав ЛВС и не имеющая подключения к сети общего пользования Интернет;

2. рабочее место, входящее в состав локально-вычислительной сети и (или) имеющее подключение к сети общего пользования Интернет.

## ЭВМ, не входящая в состав ЛВС и не имеющая подключения к сети общего пользования Интернет

- в окне настроек сетевого экрана выбрать пункт «Сетевые пакетные правила...» (рис. 57);

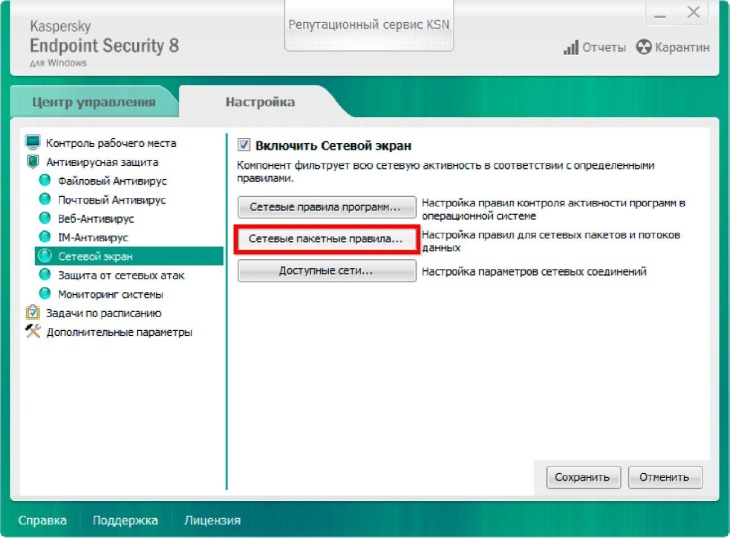


Рисунок 57. Выбор сетевых пакетных правил

- в появившемся окне «Сетевой экран» удалить все пакетные правила (рис. 58);

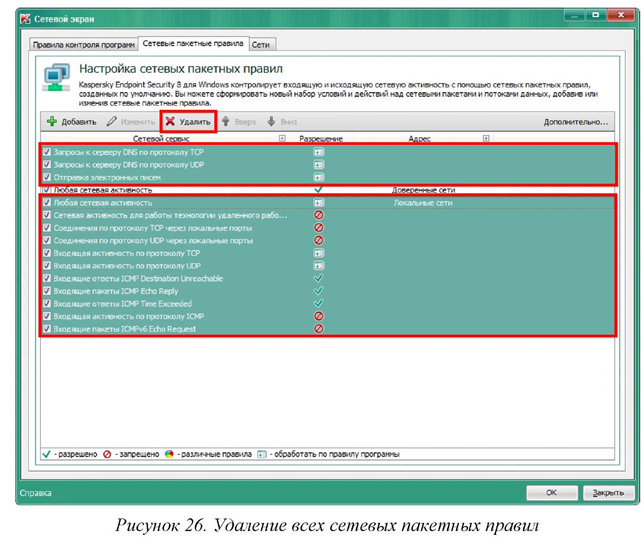


Рисунок 58. Пакетные правила

- в верхней панели действий (над сетевыми пакетными правилами) нажать на кнопку «Изменить» для настройки правила;

- в открывшемся окне «Настройка» в поле «Действие» выбрать «Запрещать». В поле «Адрес» выбрать пункт «Публичные сети». Поставить галочку в пункте «Записать в отчет». Нажать кнопку «ОК». В окне «Сетевой экран» нажать кнопку «ОК» (см. рис. 59);

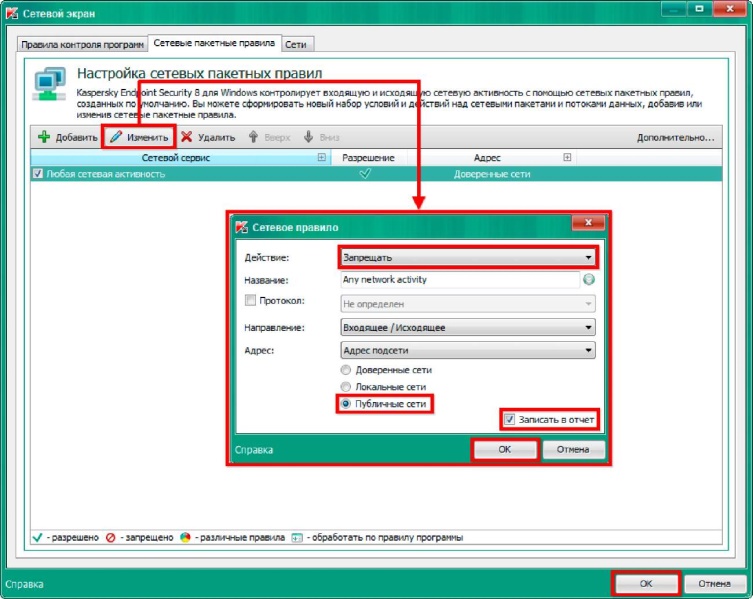


Рисунок 59. Настройки сетевого экрана для автономной ЭВМ

- в окне настроек сетевого экрана в правом нижнем углу нажать кнопку «Сохранить».

## ЭВМ, входящий в состав ЛВС и (или) имеющий подключение к сети общего пользования Интернет

- в окне настроек сетевого экрана выбрать пункт «Сетевые правила программ...».

- в появившемся окне «Сетевой экран» нажать левой кнопкой мыши на зеленую галочку в столбце «Сеть» для строки «Слабые ограничения». В открывшемся меню выбрать пункт «Запрещать» (рис. 60).

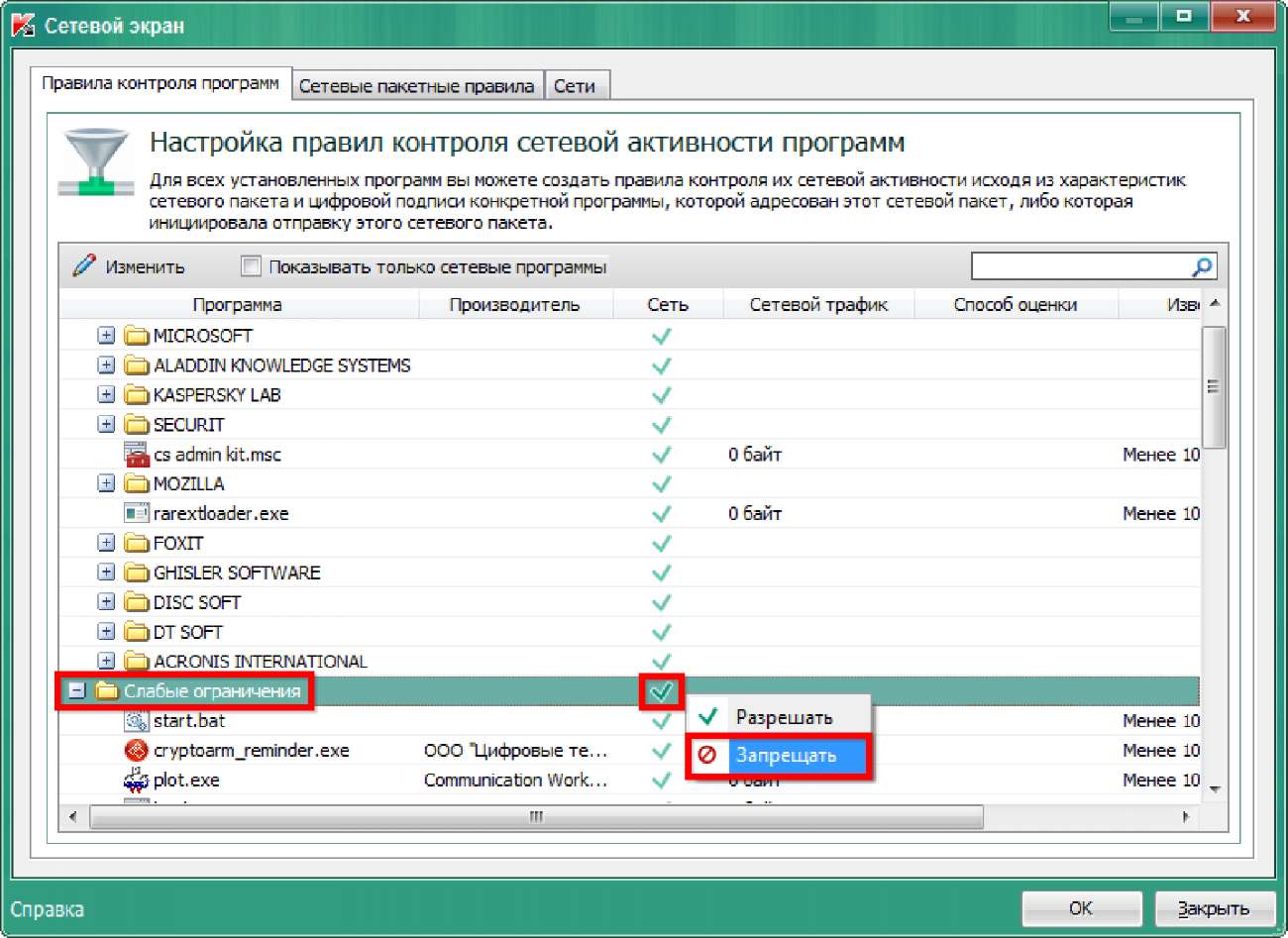


Рисунок 60. Настройка прав доступа к сети группы «Слабые ограничения»

- для того чтобы предоставить какой-либо программе из группы «Слабые ограничения» доступ к сети, необходимо либо вручную найти ее в списке программ группы «Слабые ограничения», либо использовать строку поиска. Далее в столбце «Сеть» для соответствующей программы нажать левой кнопкой мыши и в открывшемся меню выбрать пункт «Разрешать» (рис. 61).

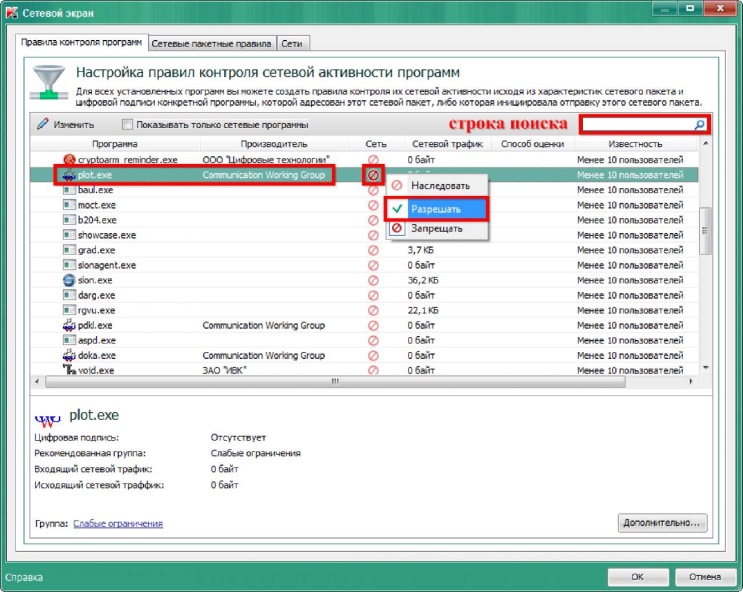


Рисунок 61. Предоставление программе доступ к сети

- Перейти на вкладку «Сетевые пакетные правила» и удалить все пакетные правила (рис. 62).

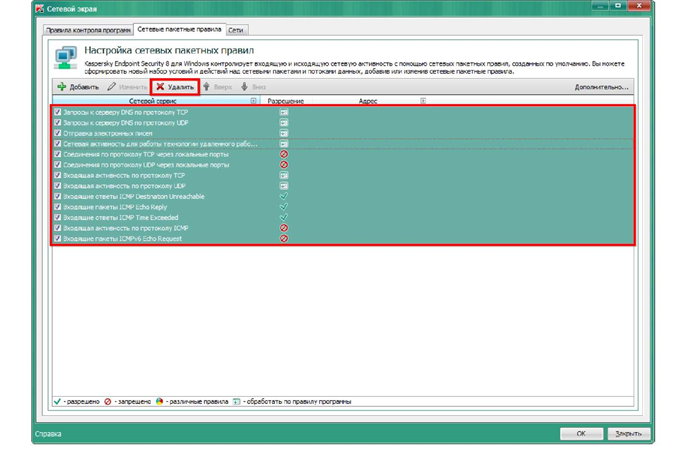


Рисунок 62. Удаление всех сетевых пакетных правил

**Настройка защиты от сетевых атак.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку «Защита от сетевых атак» и выполнить необходимые настройки (рис. 63);

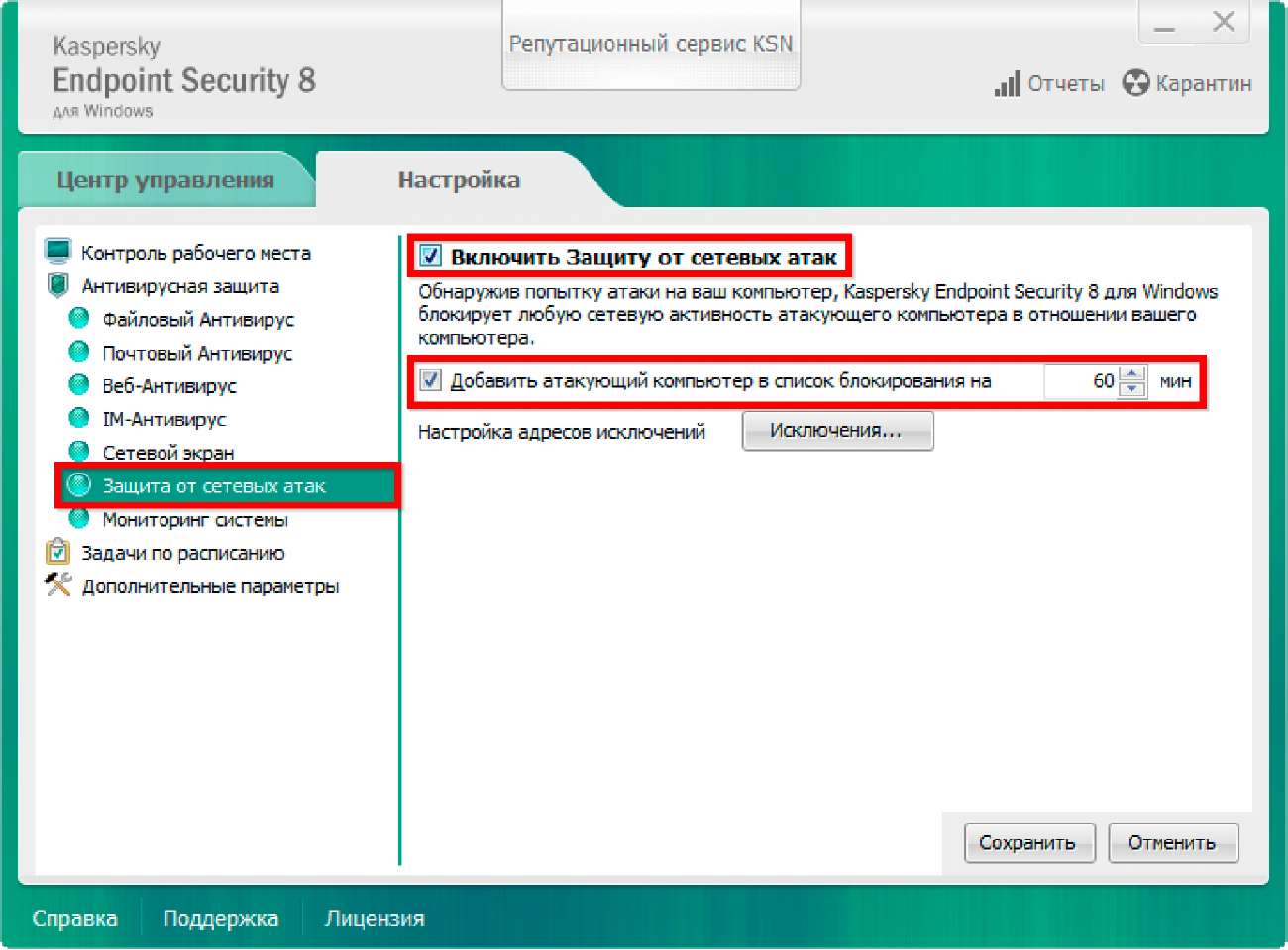


Рисунок 63. Окно настроек компонента защиты от сетевых атак

- нажать кнопку «Сохранить» в правом нижнем углу.

**Настройка мониторинга системы.** Необходимо выполнить следующие действия:

- в окне программы на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку «Мониторинг системы» и выполнить необходимые настройки (рис. 64);

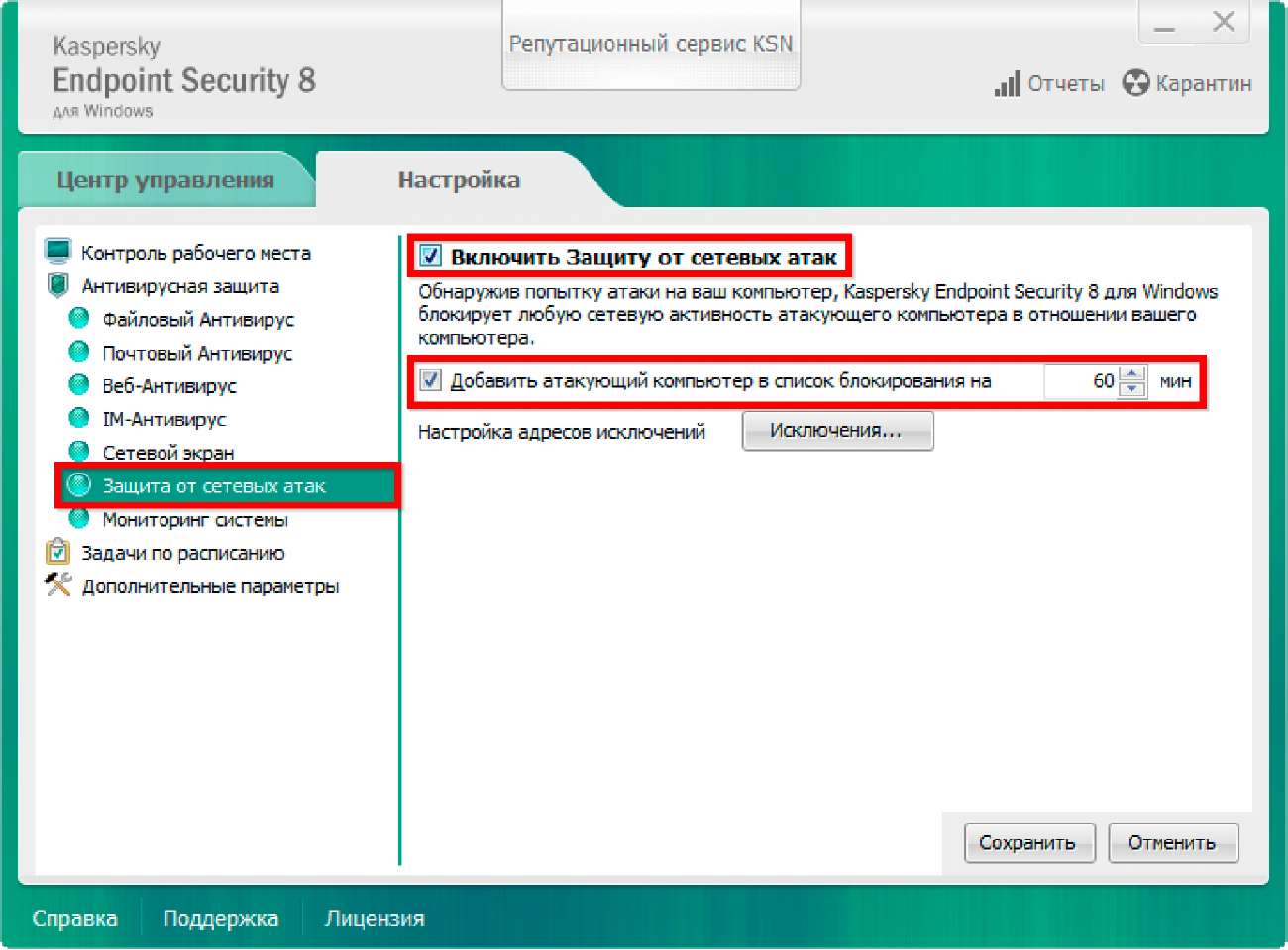


Рисунок 64. Окно настроек мониторинга системы

- нажать кнопку «Сохранить» в правом нижнем углу.

**Контрольные вопросы**

1. Вирус – это?
2. Перечислите и охарактеризуйте особенности вирусного ПО?
3. Перечислите признаки вирусной активности.
4. Перечислите признаки поражения сетевым вирусом через электронную почту:
5. Классификация ВПО (классическая): Люк, или лазейка - что это
6. Опишите жизненный цикл вирусного ПО
7. Перечислите уровни защиты от компьютерных вирусов
8. Опишите принципы защиты от вредоносного ПО
9. Технологии, применяемые в антивирусах, для борьбы с вредоносным ПО
10. Сигнатурный анализ – это
11. Эвристический анализ – это
12. Поведенческий анализ – это
13. Анализ контрольных сумм – это
14. Антивирусный мониторинг – это
15. Перечислите критерии качества антивирусных программ:
16. Перечислите типы антивирусных комплексов
17. Перечислите типы средств антивирусной защиты
18. В чем разница между закрытым и открытым исходным кодом? Что лучше?

**Методика текущего контроля**

Текущий контроль включает в себя контроль посещаемости (не менее 80 % занятий), сдача 4 коллоквиумов по тематике дисциплины (проверка знаний и умений по каждой теме) по результатам которого студент получает допуск на экзамен. На коллоквиумах проводится защиты работ, которые проводились на практических занятиях. В ходе проведения практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях. самостоятельной работы студентов

Изучение дисциплины сопровождается самостоятельной работой студентов (СРС) с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет. Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины. Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

**Текущая СРС по ПЗ № 5 состоит из:**

1. Работа с лекционным материалом, с учебной литературой – 1 ак.ч;

2. Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) 0,5 ак.ч.

3. Самостоятельное изучение разделов дисциплины - 1 ак.ч.

4. Подготовка к лабораторным работам, к практическим и семинарским занятиям – 1,5 ак.ч

5. Подготовка к контрольным работам, коллоквиумам – 1,5 ак.ч.

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методике, описанной выше.

Доцент кафедры ИБ

Краснов С.А.