ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 2022 г.

Практическое занятие № 8
по учебной дисциплине
«Защита информации»
на тему:

«Работа с антивирусом Касперского для Windows»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » _____ 202_ г. протокол № ___

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Тема практического занятия: «Работа с антивирусом Касперского для Windows».

Учебная цель:

1. Научиться установке АЗИ «Kaspersky End-point Security 8 для Windows» на ПЭВМ.

2. Научиться обновлять антивирусные базы ПЭВМ с магнитных носителей. Время - 180 мин.

Место – аудитория (класс) по расписанию занятий.

Учебно-материальное и методическое обеспечение

1. Лабораторные установки – персональные ЭВМ с установленным на них программным обеспечением.
2. Электронный практикум по ЗИ.
3. Учебно-методические материалы.

II. УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п\п	Учебные вопросы	Время, мин.
1.	***Вступительная часть. Контрольный опрос.***	10
2.	***Учебные вопросы.*** ОСНОВНАЯ ЧАСТЬ: 1. Обнаружение и удаление компьютерных вирусов (тестовых) с ПЭВМ. 2. Обновление вирусных баз ПЭВМ с магнитных носителей.	 85 80
3.	Заключительная часть. Задание и методические указания курсантам на самостоятельную подготовку	5

III. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПРЕПОДАВАТЕЛЮ ПРИ ПРОВЕДЕНИИ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Во вступительной части преподавателю объявить тему занятия, его цели, учебные вопросы, порядок его проведения, отметить практическую значимость для пользователя ПК знание антивирусной защиты, используемую литературу.

Проверку готовности слушателей к занятию осуществить проверкой наличия у них рабочих тетрадей, а также постановкой контрольных вопросов по знанию материала предыдущего группового занятия.

Отработку учебных вопросов осуществлять путем выполнения заданий, выдаваемых всей группе.

При отработке первого вопроса основное внимание обратить на приобретение курсантами первоначальных практических навыков в работе

с АЗИ «Kaspersky Endpoint Security 8 для Windows», знание обучающимися основных команд для запуска антивирусной проверки. Показать на конкретных примерах.

При отработке второго вопроса прививать практические навыки в самостоятельной работе по обновлению антивирусных баз ПЭВМ с магнитных носителей. Обратить внимание на то, что именно знание основ антивирусной защиты позволит грамотно выполнять свои обязанности в части работы с ПЭВМ.

В заключительной части занятия оценить работу учебной группы в целом, подвести итоги занятия, выставить оценки слушателям, ответить на возникшие вопросы. Сформулировать задание на самоподготовку и объявить тему следующего занятия.

IV. УЧЕБНЫЕ МАТЕРИАЛЫ

Вступительная часть

Товарищи курсанты, целью сегодняшнего занятия является - приобретение первоначальных практических первоначальных практических навыков в установке АЗИ «Kaspersky Endpoint Security 8 для Windows» на ПЭВМ, научиться обновлять антивирусные базы ПЭВМ.

Итак, тема сегодняшнего практического занятия - "Работа с антивирусом Касперского для Windows".

Для достижения поставленных учебных целей вам требуется отработать два учебных вопроса занятия:

1. Научиться осуществлять обнаружение и удаление компьютерных вирусов (тестовых) с ПЭВМ.
2. Научиться осуществлять обновление вирусных баз ПЭВМ.

Порядок проведения занятия будет следующий - сначала вы ответите на ряд контрольных вопросов, что позволит оценить вашу теоретическую готовность к занятию, а затем в рамках рассматриваемых вопросов занятия вы будете исполнять задания с использованием ПЭВМ. Ваша работа будет оцениваться на местах.

Контрольные вопросы до начала занятия.

Вопрос № 1: Для каких целей нужны СЗИ?

Вопрос № 2: Перечислите основные механизмы защиты АЗИ «Kaspersky End-point Security 8»?

Вопрос № 3: Что такое превентивная защита?

1. Задание на практическое занятие

1. Изучить документ «Типовая инструкция по настройке средства АЗИ «Kaspersky End-point Security 8 для Windows» и учебные материалы настоящей методической разработки.

2. Установить комплекс АЗИ «Kaspersky End-point Security 8 для Windows» на ПЭВМ.

3. Обнаружить и удалить компьютерные вирусы (тестовые) с ПЭВМ.

4. Обновить антивирусные базы ПЭВМ.

2. Подготовка к работе

Подготовка к работе проводится в часы самоподготовки. В ходе её каждый курсант обязан:

2.1. Изучить полученное задание.

2.2. Изучить документ «Типовая инструкция по настройке средства АЗИ «Kaspersky End-point Security 8 для Windows».

2.3. Изучить материалы лекции.

3. Выполнение работы

3.1. В классе ПЭВМ курсанты самостоятельно под руководством преподавателя выполняют задания, изучив п.4 данного руководства.

3.2. При выполнении задания работу следует спланировать таким образом, чтобы в первую очередь изучить документ «Типовая инструкция по настройке средства АЗИ «Kaspersky End-point Security 8 для Windows», а затем приступить к использованию «АЗИ Kaspersky End-point Security 8 для Windows».

3.3. В ходе практической работы запрещается вносить изменения, удалять или добавлять какие-либо компоненты, настройки и параметры операционной системы.

4.Теоретические сведения

Общие сведения

1. **Средство антивирусной защиты информации (далее - САВЗ)** «Kaspersky Endpoint Security 8 для Windows» обеспечивает комплексную защиту компьютера от вредоносного программного обеспечения, сетевых атак и спама.

2. **«Kaspersky Endpoint Security 8 для Windows»** имеет модульную структуру. Для корректной настройки «Kaspersky Endpoint Security 8 для Windows» необходимо последовательно настроить каждый модуль. Ниже приводится описание структуры «Kaspersky Endpoint Security 8 для Windows».

3. **I. Контроль рабочего места.**

4. Контроль запуска программ. Контроль активности программ. Мониторинг уязвимости программ. Контроль устройств. Веб-Контроль.

5. **II. Антивирусная защита.**

6. Файловый антивирус. Почтовый антивирус. Веб-антивирус. IM-антивирус. Сетевой экран. Защита от сетевых атак. Мониторинг системы.

7. **III. Задачи по расписанию.**

8. Обновление. Полная проверка. Проверка важных областей. Выборочная проверка. Поиск уязвимостей.

9. **IV. Дополнительные параметры.**

10. Отчеты и хранилища. Параметры KSN. Интерфейс. Импорт и экспорт настроек

IV.ЗАДАНИЯ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИХ ВЫПОЛНЕНИЮ

1. Обнаружение и удаление компьютерных вирусов (тестовых) с ПЭВМ.

1.1 Файловый антивирус

Файловый антивирус предназначен для защиты от заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

Для настройки файлового антивируса необходимо:

1. В окне программы «Kaspersky Endpoint Security 8 для Windows» на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку Файловый Антивирус (см. рис. 13).

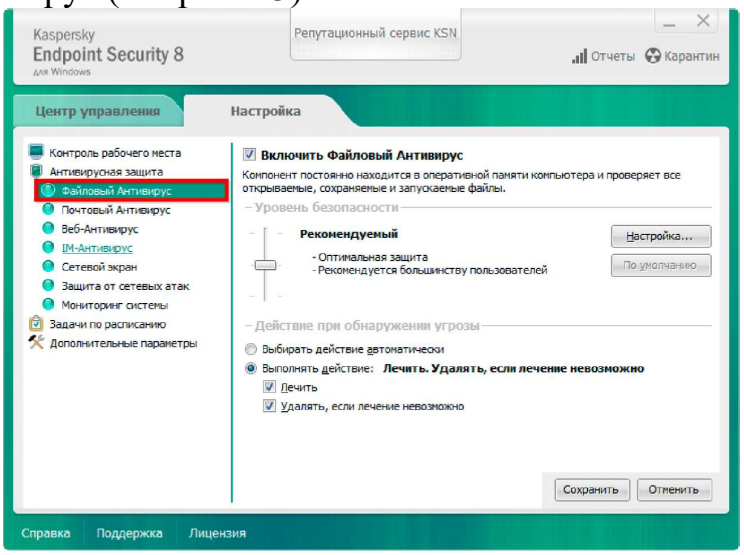

Рисунок 13. Окно настроек файлового антивируса

2. В поле «Уровень безопасности» переместить ползунок вверх и установить уровень безопасности «Высокий» (см. рис. 14).

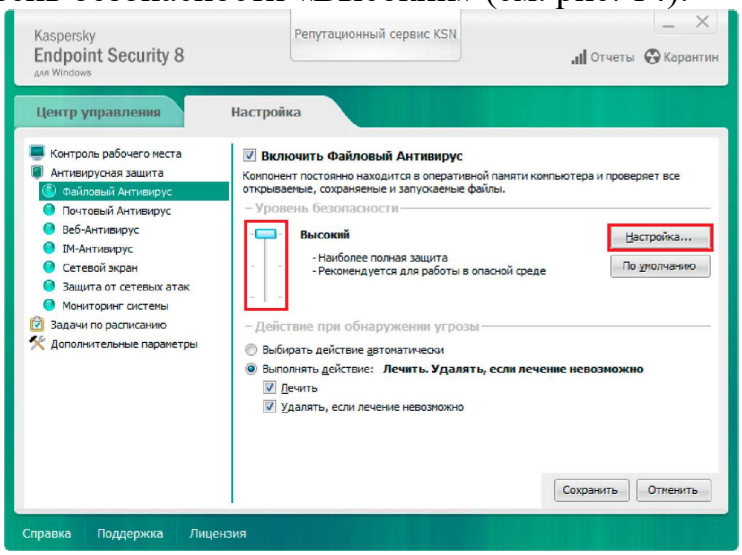

Рисунок 14. Общие параметры файлового антивируса

3. 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 эвристическим методом в зависимости от производительности автоматизированного рабочего места (далее - АРМ), но не ниже значения «Средний». Настройки в поле «Оптимизация проверки» оставить без изменений (отсутствие выбора в поле «Проверять только новые и измененные файлы»). 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 «ОК» (см. рис. 15).

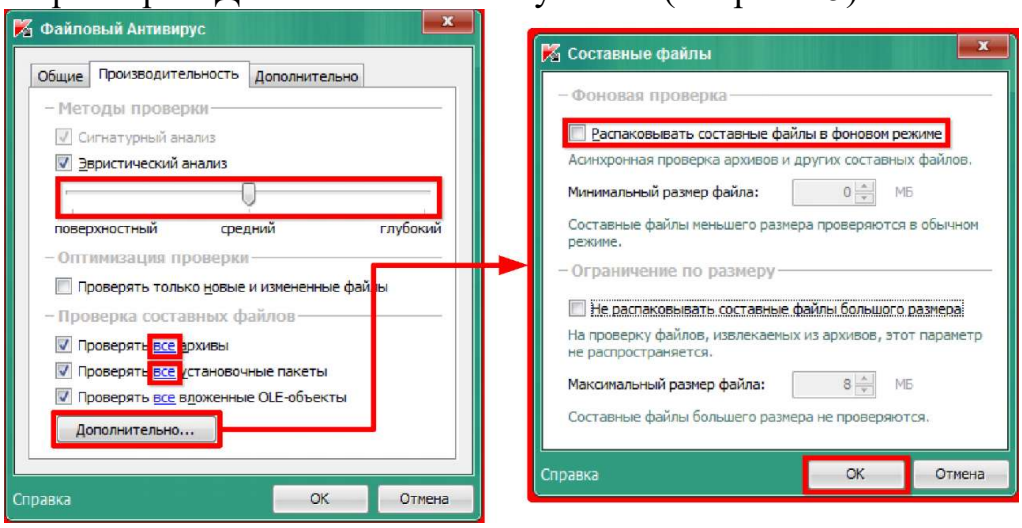

Рисунок 15. Изменение производительности файлового антивируса и настройка проверки составных файлов

4. В окне «Файловый Антивирус» нажать кнопку «ОК», далее нажать кнопку «Сохранить» в правом нижнем углу.

1.2 Почтовый антивирус

Почтовый Антивирус предназначен для проверки входящих и исходящих сообщений на наличие в них опасных объектов. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения по протоколам POP3, SMTP, IMAP и NNTP.

Для настройки почтового антивируса необходимо:

1. В окне программы «Kaspersky Endpoint Security 8 для Windows» на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку Почтовый Антивирус (см. рис. 16).

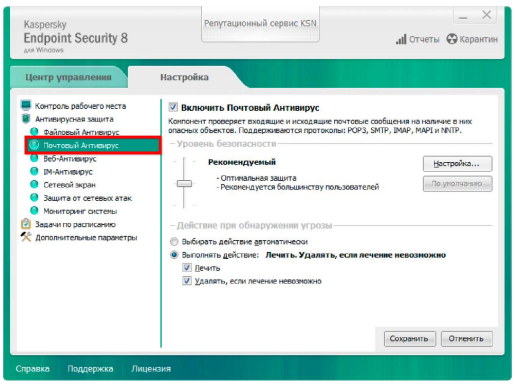

Рисунок 16. Окно настроек почтового антивируса

2. В поле «Уровень безопасности» перетащить ползунок вверх и установить уровень безопасности «Высокий» (см. рис. 17).

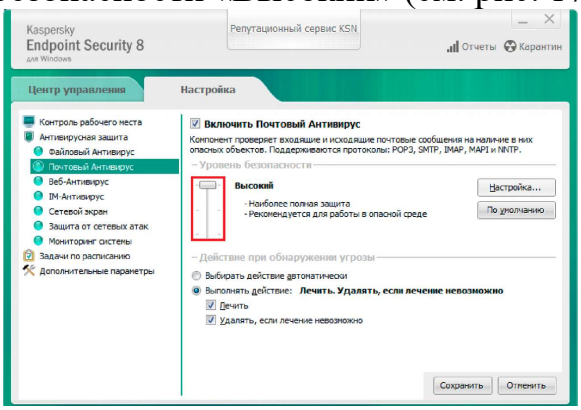

Рисунок 17. Изменение параметров уровня безопасности почтового антивируса

3. Нажать на кнопку «Настройка». Перейти во вкладку «Общие». В поле «Встраивание в систему» поставить галочку напротив пункта «Дополнительно: плагин в The Bat!» (см. рис. 18). Остальные настройки оставить без изменений («Область защиты» - «Входящие и исходящие сообщения», «Встраивание в систему» - «Трафик POP3/SMTP/NNTP/IMAP», «Дополнительно: плагин в Microsoft Office Outlook», Проверка составных файлов - «Проверять вложенные архивы»).

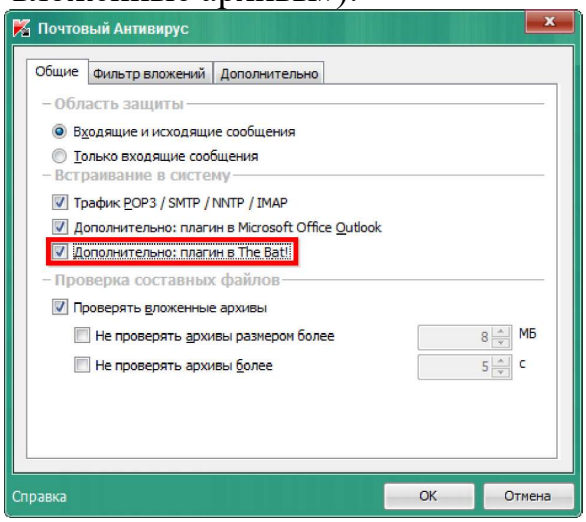

Рисунок 18. Общие настройки почтового антивируса

4. Во вкладке «Фильтр вложений» выбрать пункт «Удалять вложения указанных типов». Далее поставить галочки напротив следующих форматов: *.bat, *.cmd, *.com, *.dll, *.drv, *.exe, *.ico, *.ini, *.js, *.jse, *.lnk,*.md, *.ocx,

*.prg, *.reg, *.scr, *.shs, *.swf, *.vbe, *.vbs, *.vxd, *.wsf, *.msi *.wsh (см рис. 19)

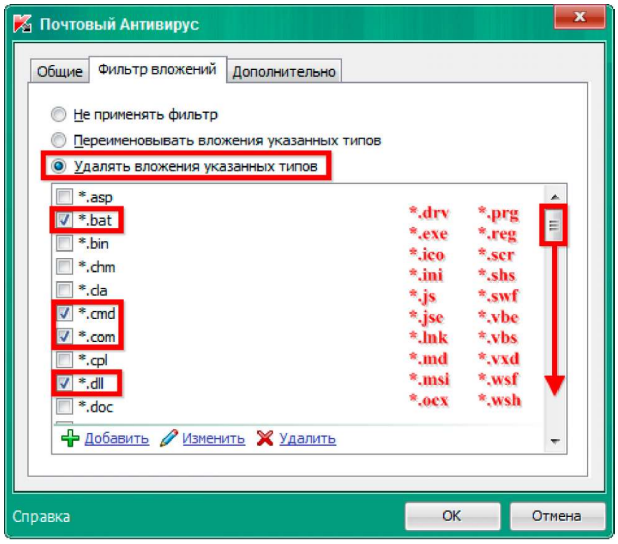

Рисунок 19. Изменение параметров фильтра вложений

5. Во вкладке «Дополнительно» выбрать уровень проверки эвристическим методом в зависимости от производительности АРМ, но не ниже значения «Средний» (см. рис. 20). Нажать кнопку «ОК». Далее нажать кнопку «Сохранить» в правом нижнем углу.

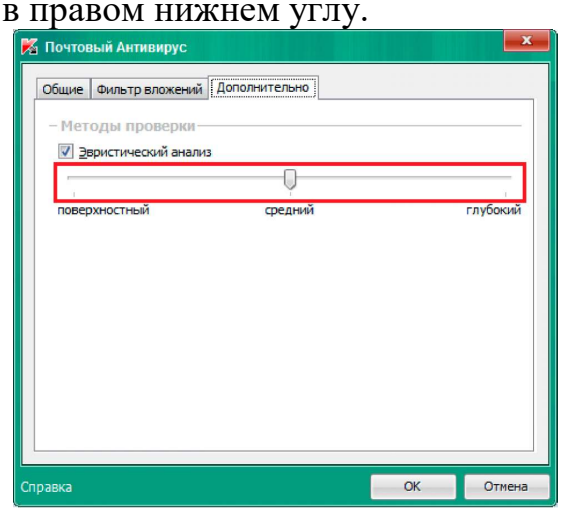

Рисунок 20. Изменение параметров методов проверки

1.3 Веб-антивирус

Веб-Антивирус предназначен для защиты информации, поступающей на компьютер по HTTP-протоколу, а также предотвращения запуска на компьютере опасных скриптов. Веб-защита предусматривает контроль HTTP- трафика, проходящего только через порты, указанные в списке контролируемых портов.

Для настройки веб-антивируса необходимо:

1. В окне «Kaspersky Endpoint Security 8 для Windows» на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку Веб-Антивирус (см. рис. 21).

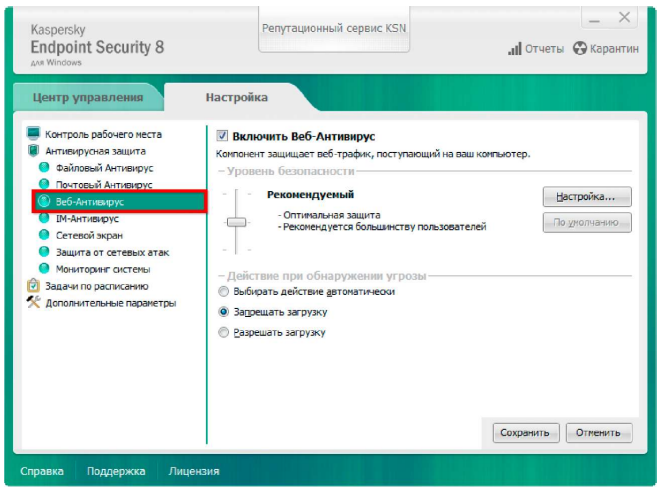

Рисунок 21. Окно настроек веб-антивируса

2. Нажать на кнопку «Настройка». Остальные настройки в этом окне оставить без изменений («Уровень безопасности» - «Рекомендуемый», «Действие» - «Запрещать загрузку»). В появившемся окне «Веб-Антивирус» настройки во вкладке «Доверенные веб-адреса» оставить без изменений (стоит галочка в пункте «Не проверять веб-трафик с доверенных веб-адресов:»). 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, но не ниже значения «Средний». Параметры в поле «Методы проверки» оставить без изменений (установлены галочки в следующих пунктах: «Проверять ссылки по базе подозрительных веб- адресов», «Проверять ссылки по базе фишинговых веб-адресов», «Эвристический анализ для обнаружения вирусов», «Эвристический анализ для обнаружения фишинговых атак») (см. рис. 22).

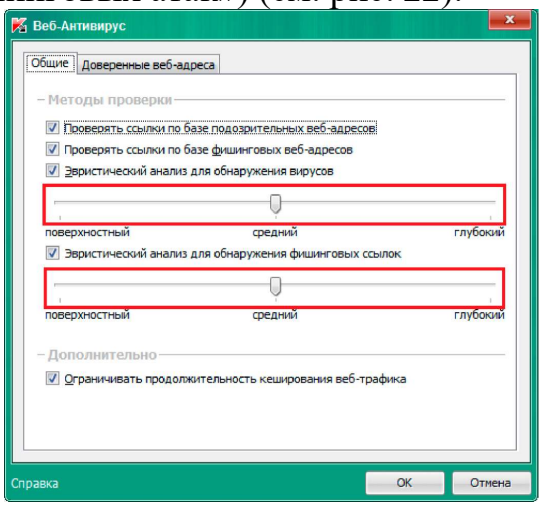

Рисунок 22. Изменение параметров настройки Веб-Антивируса.

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

1.4 IM-антивирус

IM-Антивирус предназначен для проверки трафика, передаваемого программами для быстрого обмена. Он перехватывает каждое сообщение, которое пользователь принимает или отправляет с помощью интернет -

пейджера, и проверяет сообщение на наличие в нем объектов, представляющих угрозу безопасности компьютера.

В Вооруженных Силах Российской Федерации подобные программы не используются, поэтому IM-антивирус можно отключить, убрав галочку напротив пункта «Включить IM-антивирус» (см. рис. 23).

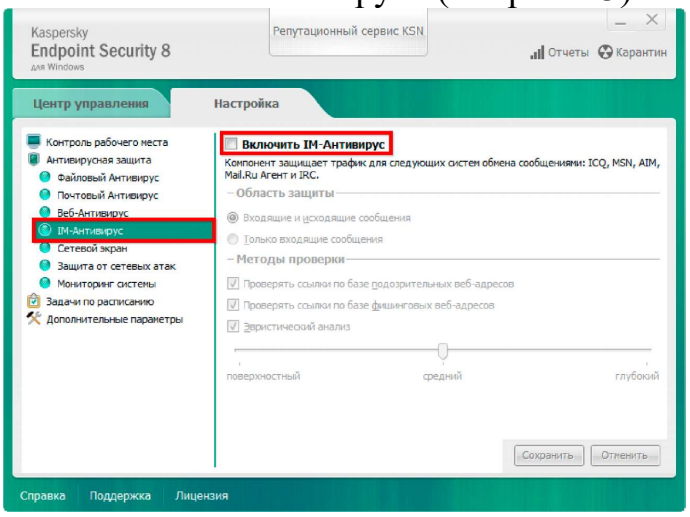

Рисунок 23. Выключение IM-антивируса

1.5 Сетевой экран

Сетевой экран обеспечивает защиту личных данных, хранящихся на компьютере пользователя, блокируя все возможные для операционной системы угрозы в то время, когда компьютер подсоединен к сети Интернет или к локальной сети. Сетевой экран позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Чтобы включить сетевой экран необходимо в окне программы «Kaspersky Endpoint Security 8 для Windows» на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку «Сетевой экран». Далее поставить галочку напротив пункта «Включить Сетевой экран» (см. рис. 24).

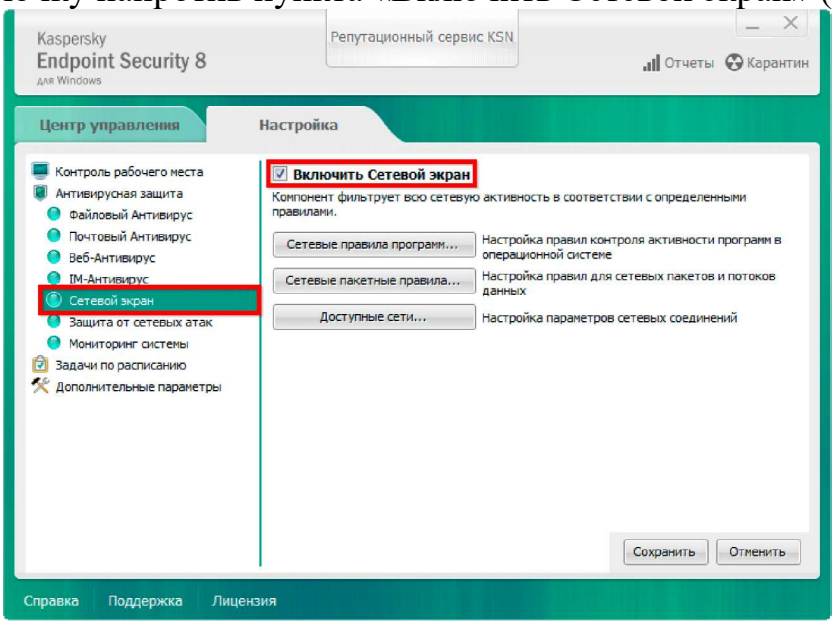

Рисунок 24. Окно настроек сетевого экрана

Для настройки сетевого экрана необходимо определить к какой группе относится автоматизированное рабочее место:

1. автономное рабочее место (далее - АРМ), не входящее в состав локально-вычислительной сети (далее - ЛВС) и не имеющее подключения к ИТКС ОП Интернет;
2. рабочее место, входящее в состав локально-вычислительной сети и (или) имеющее подключение к ИТКС ОП Интернет (самостоятельный абонентский пункт сети Интернет).

1.5.1 АРМ, не входящий в состав ЛВС и не имеющий подключения к ИТКС ОП Интернет

1. В окне настроек сетевого экрана выбрать пункт «Сетевые пакетные правила...» (см. рис. 25).

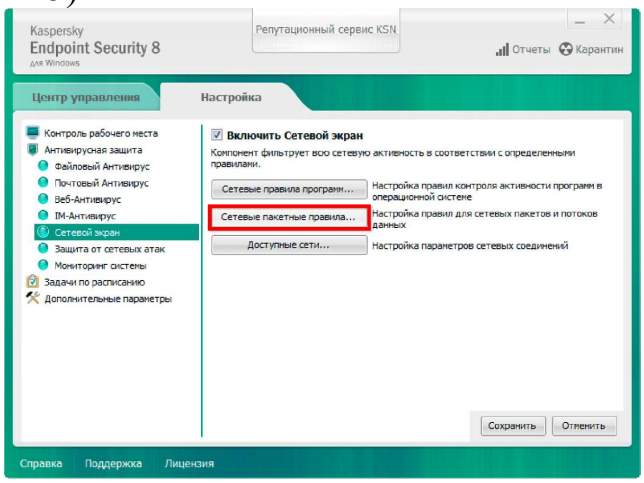

Рисунок 25. Выбор сетевых пакетных правил

1. В появившемся окне «Сетевой экран» выделить любое пакетное правило (нажать левой кнопкой мыши на него). Выделить все пакетные правила, нажав комбинацию клавиш Ctrl+A. Далее, удерживая клавишу Ctrl, нажать на одно из правил «Любая сетевая активность», чтобы снять с него выделение. В верхней панели действия (над сетевыми пакетными правилами) нажать на кнопку «Удалить» для удаления всех выделенных пакетных правил (см. рис. 26).

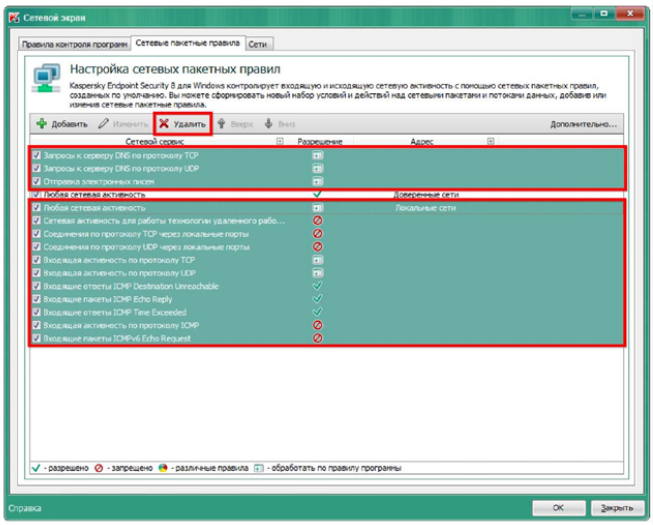

Рисунок 26. Удаление всех сетевых пакетных правил

3. В верхней панели действия (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 «О К» (см. рис. 27). Далее в окне настроек сетевого экрана в правом нижнем углу нажать кнопку «Сохранить».

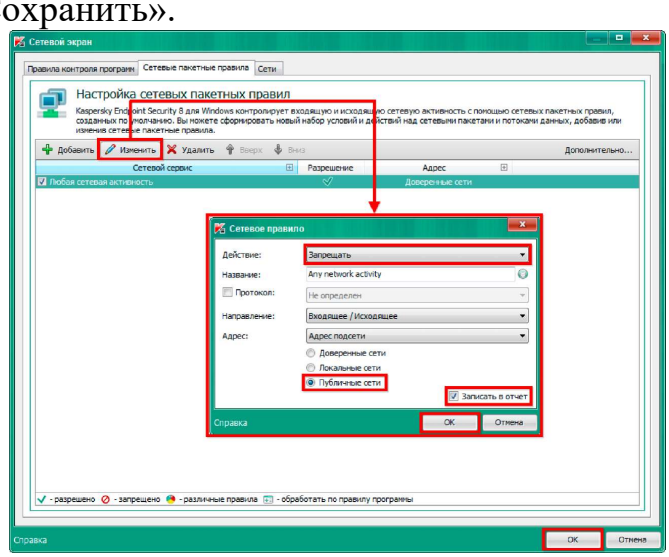

Рисунок 27. Настройки сетевого экрана для автономного АРМ

1.5.2 АРМ, входящий в состав ЛВС и (или) имеющий подключение к ИТКС ОП Интернет

1. В окне настроек сетевого экрана выбрать пункт «Сетевые правила программ...».

2. 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» (см. рис. 28).

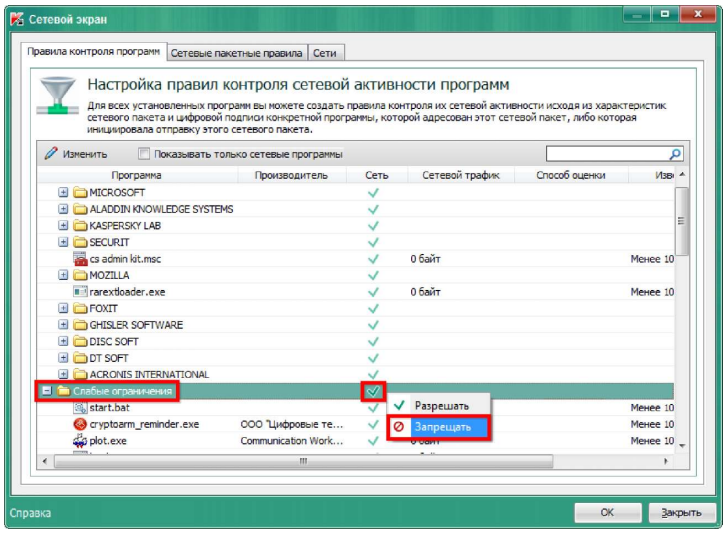

Рисунок 28. Настройка прав доступа к сети группы «Слабые ограничения»

3. 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» (см. рис. 29).

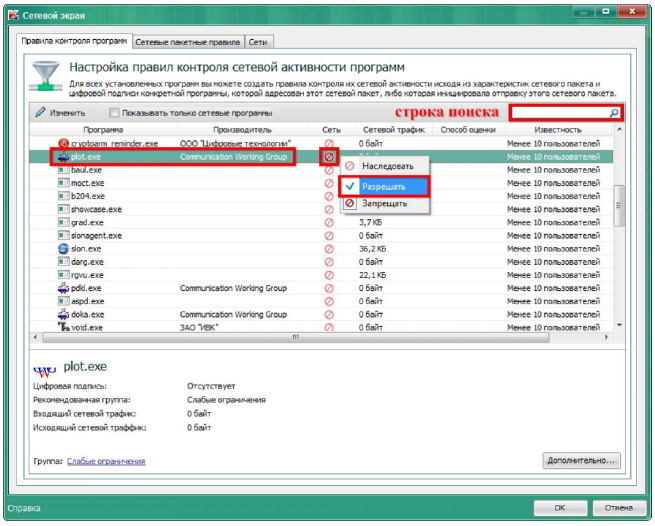

Рисунок 29. Предоставление программе plot.exe доступа к сети

4. Перейти на вкладку «Сетевые пакетные правила». Выделить все правила, нажав комбинацию клавиш Ctrl + A, затем удалить их, нажав на кнопку «Удалить» в верхней панели действий (см. рис. 30).

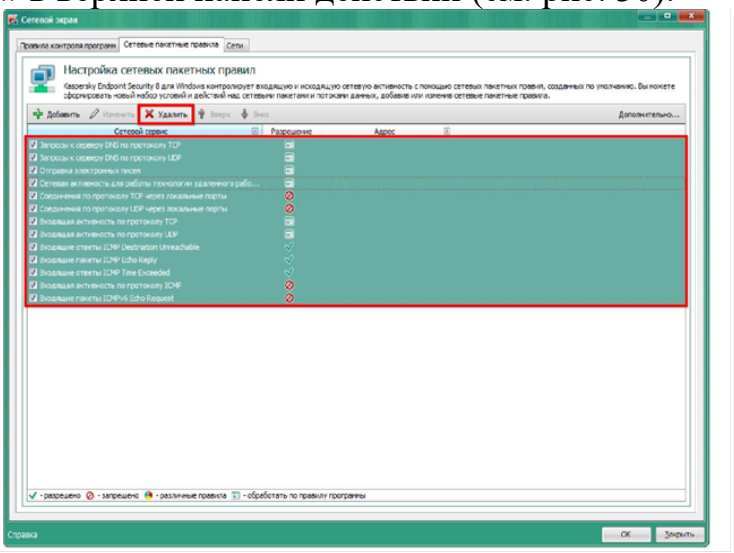

Рисунок 30. Удаление всех сетевых пакетных правил

1.6 Защита от сетевых атак

Защита от сетевых атак отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, «Kaspersky Endpoint Security 8 для Windows» блокирует сетевую активность атакующего компьютера. После этого на экран выводится уведомление о том, что была попытка сетевой атаки с указанием информации об атакующем компьютере.

Для настройки защиты от сетевых атак необходимо: В окне программы «Kaspersky Endpoint Security 8 для Windows» на вкладке «Настройка» в разделе «Антивирусная защита» нажать на ссылку «Защита от сетевых атак». Поставить галочки, если они отсутствуют, напротив следующих пунктов: «Включить Защиту от сетевых атак» и «Добавить атакующий компьютер в

список блокирования на» (см. рис. 31). В пункте «Добавить атакующий компьютер в список блокирования на» оставить значение по умолчанию (60 мин).

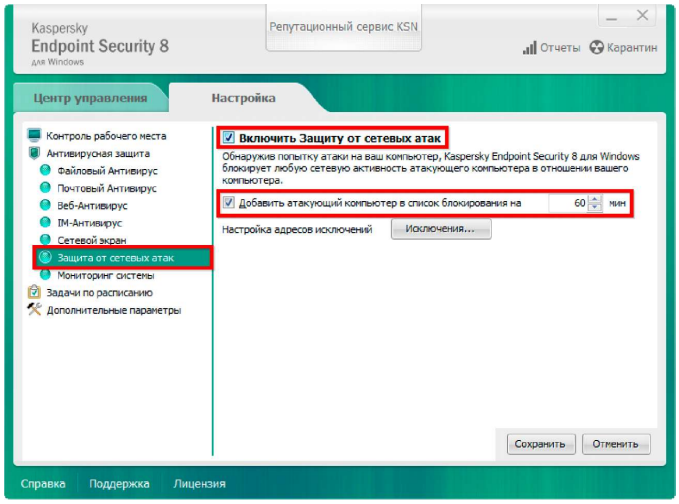

Рисунок 31. Окно настроек компонента защиты от сетевых атак

1.7 Мониторинг системы

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

Для настройки защиты от сетевых атак необходимо:

В окне программы «Kaspersky Endpoint Security 8 для Windows» на вкладке «Настройка» нажать на ссылку «Мониторинг системы». Поставить галочку напротив пункта «Включить Мониторинг системы». Убрать галочку напротив пункта ««Не контролировать активность программ, имеющих цифровую подпись». Остальные параметры оставить без изменений (стоит галочка напротив следующих пунктов: «Хранить историю активности программ для базы BSS», «Выполнять откат действий вредоносных программ при лечении», «Использовать обновляемые шаблоны опасного поведения (BSS)», при обнаружении вредоносной активности программы выбрано действие «Помещать файл на карантин» (см. рис. 32).

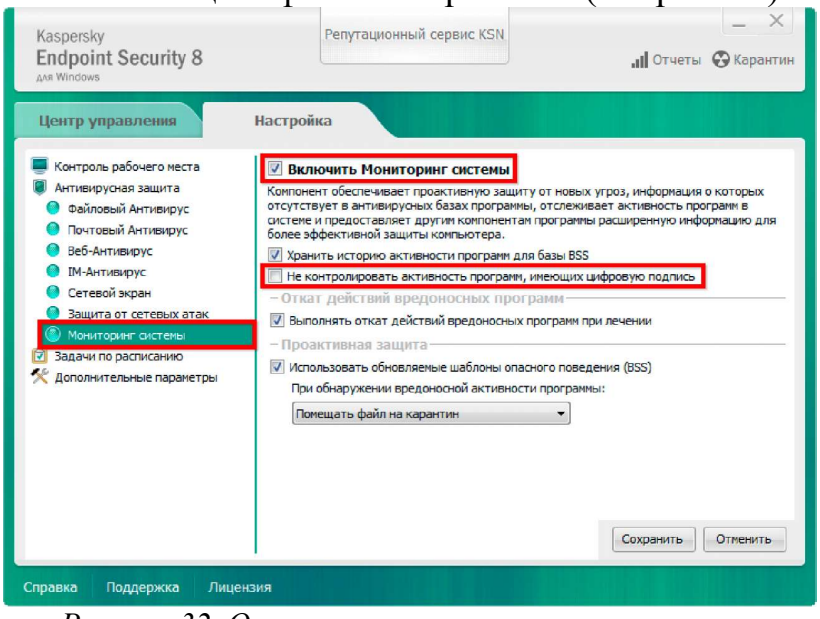

Рисунок 32. Окно настроек мониторинга системы

2. Обновление вирусных баз ПЭВМ

2.1 Обновление

Обновление баз вирусных сигнатур (далее - БВС) «Kaspersky Endpoint Security 8 для Windows» обеспечивает актуальность защиты компьютера.

Для настройки параметров установки обновлений БВС необходимо определить к какой группе относится автоматизированное рабочее место:

автономное рабочее место, не имеющее подключения к ИТКС ОП Интернет;

рабочее место, имеющее подключение к ИТКС ОП Интернет (абонентский пункт сети Интернет (далее - АП сети Интернет));

рабочее место, управляемое Kaspersky Security Center 9 (далее - KSC9).

2.1.1 АРМ, не имеющий подключения к ИТКС ОП Интернет

Перед непосредственной настройкой задачи обновления БВС необходимо выполнить следующие предварительные действия:

1. Создать в корневом каталоге системного диска директорию для обновлений БВС с названием Updates (полный путь: C:\Updates\).
2. 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 «C:\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.

3. Разархивировать архив с актуальным полным комплектом БВС, загруженный ранее.
4. Скопировать каталоги AutoPatches, bases, index из директории с полным комплектом БВС в директорию C:\Updates\.

Для настройки задачи обновления необходимо:

1. В окне программы «Kaspersky Endpoint Security 8 для Windows» 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 «ОК» (см. рис. 34).

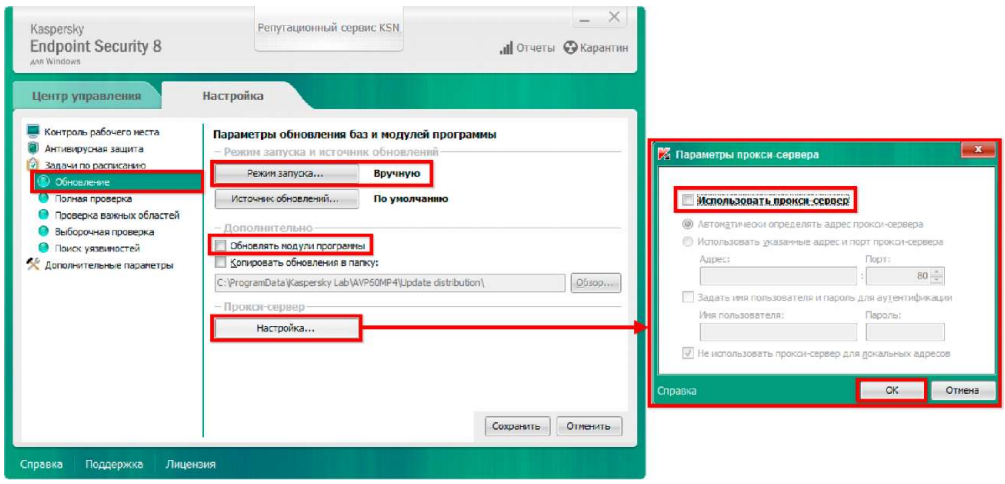

Рисунок 34. Настройка параметров обновления БВС для автономного рабочего места, не имеющего подключения к ИТКС ОП Интернет

2. В окне настроек обновления в поле «Режим запуска и источник обновлений» нажать на кнопку «Источник обновлений.» (см. рис. 35).

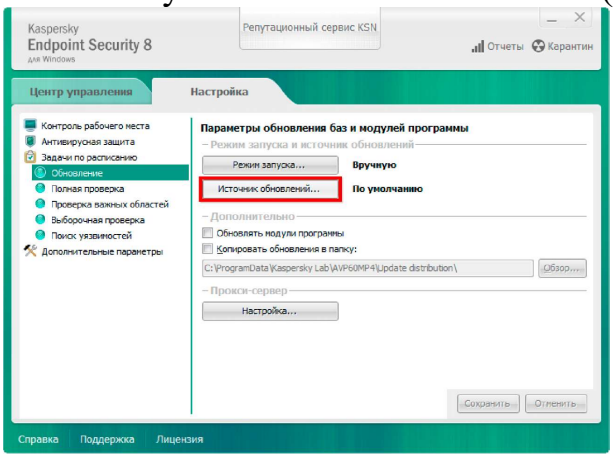

Рисунок 35. Настройка источника обновлений

3. 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 «ОК». Далее в окне «Обновление» нажать кнопку «ОК» (см. рис. 36).

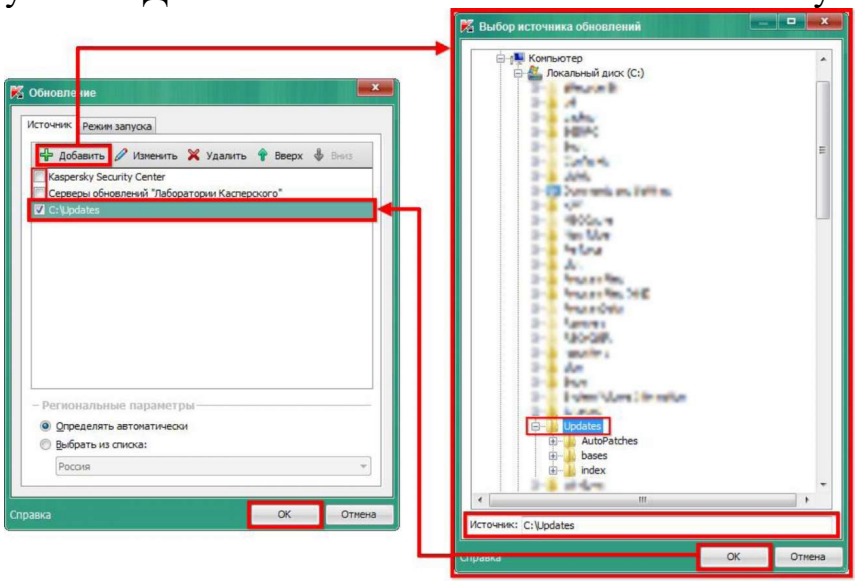

Рисунок 36. Указание источника обновлений

4. Для запуска обновления необходимо в окне программы «Kaspersky Endpoint Security 8 для Windows» 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» (см. рис. 37).

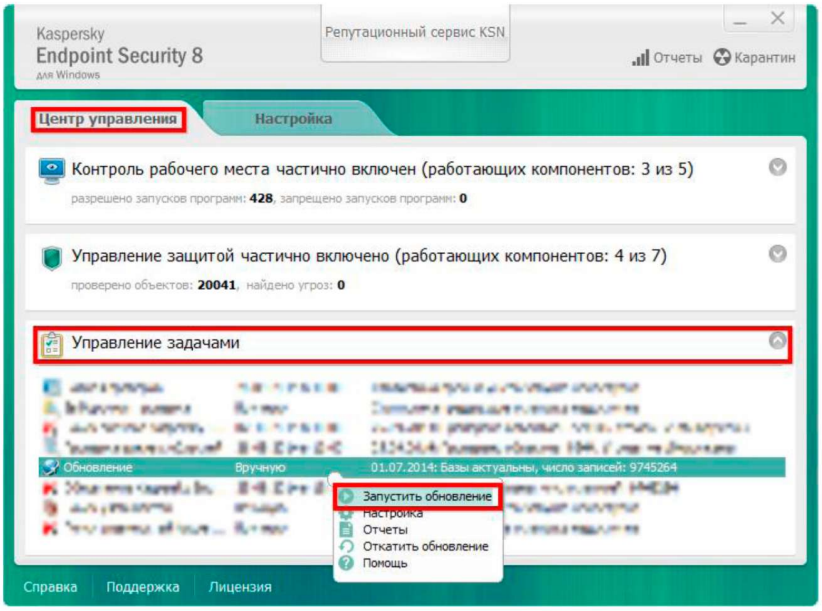

Рисунок 37. Запуск задачи обновления

2.1.2 АП сети Интернет

Для настройки задачи обновления необходимо:

1. В окне программы «Kaspersky Endpoint Security 8 для Windows» 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 «ОК» (см. рис. 38).

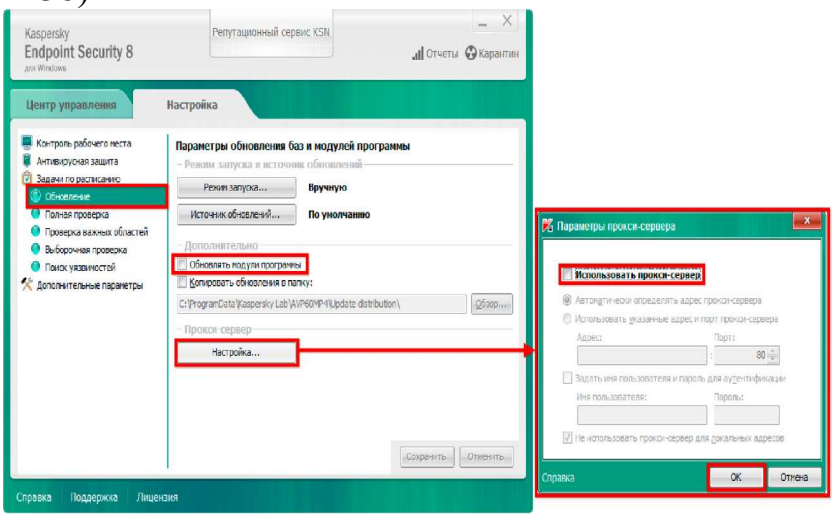

Рисунок 38. Настройка параметров обновления БВС для автоматизированного рабочего места, имеющего подключение к ИТКС ОП Интернет

2. 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 2. Нажать кнопку «ОК» (см. рис. 39).

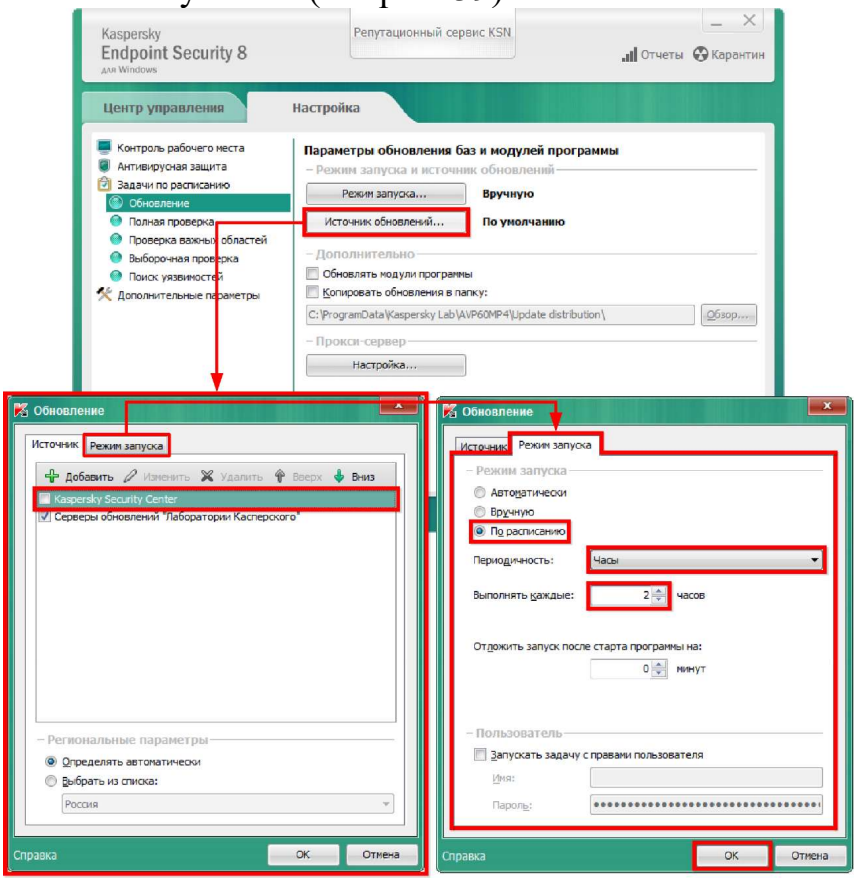

Рисунок 39. Настройка источника и режима запуска задачи обновления БВС

5. Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

– название практического занятия;

– текст индивидуального задания;

– цель работы;

– результаты проделанной работы;

– Выводы.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

6. Заключительная часть

В заключительной части подводятся итоги проделанной работы, дается краткая оценка действиям участников, прослеживается связь с теоретическими положениями и перспективой на будущую деятельность.

7.Задание и методические указания курсантам на самостоятельную подготовку:

1. Повторить по конспекту лекций и рекомендованной литературе основные возможности САВЗ.
2. Быть готовыми к самостоятельной настройке САВЗ.

V. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Эксплуатационный документ «Типовая инструкция по настройке средства АЗИ «Kaspersky End-point Security для Windows».

2. Информационная безопасность: – учебное пособие / В.М.Зима, СПб.: ВКА имени А.Ф.Можайского, 2017 с.

3. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Ч.2. Сетевые ОС и принципы обеспечения информационной безопасности в сетях / С.И. Макаренко, А.А. Ковальский, С.А. Краснов СПб.: Наукоемкие технологии 2020.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.