МИНОБРАНАУКИ РОССИИ

Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

НАСТРОЙКА СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Методические указания к практическим работам

Санкт-Петербург
СПбГЭТУ «ЛЭТИ»

2019

Авторы: **Краснов С.А, Племянников А.К., Решетняк Д. А.**
Настройка средств защиты компьютерной информации СПбГЭТУ «ЛЭТИ», 2019. 77 с.

Содержит методические указания по выполнению практических работ под руководством преподавателя и самостоятельно. Приводятся краткие теоретические сведения о правилах и вариантах настройки технических средств, входящих в состав информационных систем в защищенном исполнении.

Предназначены для студентов специальности 10.05.01, также могут быть полезны преподавателям и специалистам в области защиты информации.

Одобрено
Методической комиссией факультета
компьютерных технологий и информатики
в качестве методических указаний

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ

АС – автоматизированные системы;
БВС – базы вирусных сигнатур;
БД – база данных;
ЗПС – замкнутая программная среда;
ЛВС – локальная вычислительная сеть;
НСД – несанкционированный доступ;
ОС – операционные системы;
ПО – программное обеспечение;
ПРД – правла разграничения доступа;
РФ – Российская Федерация;
САВЗ – средства антивирусной защиты;
СЗИ – Средства защиты информации;
СН – специальное назначение;
СПО – специальное программное обеспечение;
ФС – файловая система;
ЭВМ – электронно-вычислительная машина;
ЭЦП – электронно-цифровая подпись.

ВВЕДЕНИЕ

Темы практических работ, представленные в данном сборнике, направлены на закрепление материала по настройке технических средств информационных систем в защищенном исполнении.

Предполагается, что обучающиеся к моменту начала выполнения практических заданий прошли дисциплины «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Криптографические методы защиты информации», «Модели нарушения безопасности и вирусология», «Защита операционных систем и систем управления базами данных», «Защита компьютерных сетей и телекоммуникаций» и знают основные угрозы безопасности информации в АС СН и способах их реализации, проблемы обеспечения безопасности информации в специальных автоматизированных системах, принципы работы СЗИ от НСД и САВЗ, инструментарием по администрированию специальных ОС, а так же владеют способами защиты специальных автоматизированных систем, навыками разработки моделей угроз и информационной безопасности специальных автоматизированных систем, способами защиты специальных автоматизированных систем, способами выявления вредоносных программ в вычислительных системах.

В ходе практических работ предполагается выполнение студентами двух видов настройки системы защиты информации автоматизированного рабочего места (персонального компьютера): настройку системы защиты информации от несанкционированного доступа и настройку средства антивирусной защиты.

В настройку системы защиты информации от несанкционированного доступа входят:

- настройка идентификации и аутентификации;
- настройка разграничения прав доступа субъектов доступа к объектам доступа;
- настройка очистки освобождаемых областей оперативной памяти;
- настройка регистрации событий;
- настройка контроля целостности;
- настройка учета внешних носителей информации.

В настройку средства антивирусной защиты входят:

- настройка файлового антивируса;

- настройка почтового антивируса;
- настройка веб-антивируса;
- настройка IM-антивируса;
- настройка сетевого экрана;
- настройка защиты от сетевых атак;
- настройка мониторинга системы;
- настройка обновления вирусных баз.

Настройку следует выполнять по определенным правилам, установленным нормативными или нормативно-методическими документами. Все необходимые примеры настройки находятся в приложениях сборника и могут быть использованы студентами в качестве образцов при выполнении практических работ.

Все практические работы имеют однотипное описание, включающее: название, цель, теоретические сведения, постановку задачи и последовательность действий исполнителя.

Требования к отчетам по практическим работам также типизированы:

1. Наличие титульного листа с названием работы и подписью исполнителя.
2. Описание цели работы.
3. Протокол действий по выполнению настройки средств защиты информации с комментариями исполнителя.
4. Выводы по выполненной работе.
5. Список использованной литературы.

1. НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «DALLAS LOCK»

Цель работы. Получить практические навыки настройки СЗИ НСД «Dallas Lock».

Теоретические сведения. СЗИ НСД «Dallas Lock» предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил, обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему и выходящими за её пределы. А также для обеспечения защиты информации в АС посредством её фильтрации.

Система защиты Dallas Lock представляет собой программный комплекс средств защиты информации в ОС семейства «Windows» с возможностью подключения аппаратных идентификаторов.

Использование системы защиты Dallas Lock в проектах по защите информации позволяет привести АС в соответствие требованиям законодательства РФ.

Система защиты предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (файловых, контроллерах домена и терминального доступа).

Система защиты Dallas Lock состоит из следующих основных компонентов:

Программное ядро (Драйвер защиты). Является ядром системы защиты и выполняет основные функции СЗИ НСД:

- обеспечивает мандатный (для редакции «С») и дискреционный режимы контроля доступа к объектам файловой системы и устройствам;
- обеспечивает доступ к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;
- обеспечивает работу механизма делегирования полномочий;
- обеспечивает проверку целостности СЗИ НСД, объектов ФС, программно-аппаратной среды и реестра;
- драйвер защиты осуществляет полную проверку правомочности и корректности администрирования СЗИ НСД.

Драйвер защиты автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы. Драйвер осуществляет управление подсистемами и модулями системы защиты и обеспечивает их взаимодействие. С драйвером защиты взаимодействуют защитные подсистемы, перечисленные ниже.

Подсистема администрирования. Включает в себя:

- подсистему локального администрирования. Обеспечивает возможности по управлению СЗИ НСД, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Включает в себя подсистему внедрения в интерфейс «Windows» Explorer («проводник»). Обеспечивает отображение пунктов в контекстном меню объектов, необходимых для назначения прав доступа к объектам ФС, вызова функции принудительной зачистки объектов ФС, преобразования.
- подсистему удаленного администрирования. Позволяет выполнять настройку системы защиты с удалённого компьютера.
- подсистему централизованного управления. Позволяет объединять защищенные компьютеры в Домен безопасности для централизованного и оперативного управления клиентами.

Подсистема управления доступом. Включает в себя:

- подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов;
- подсистему доступа к файловой системе, реестру и устройствам, в составе которой:
    - подсистема дискреционного доступа;
    - подсистема мандатного доступа (для редакции «С»);

Подсистема регистрации и учета. Включает в себя:

- подсистему аудита. Обеспечивает ведение аудита и хранение информации 8-ми категорий событий в журналах;
- подсистему печати. Обеспечивает разграничение доступа к печати, добавление штампа на документы, сохранение их теневых копий, регистрацию событий печати.

Подсистема идентификации и аутентификации. Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему.

Подсистема гарантированной зачистки информации. Обеспечивает зачистку остаточной информации.

Подсистема преобразования информации. Обеспечивает:

- преобразование информации в файлах-контейнерах;
- преобразование сменных накопителей для защиты от доступа в обход СЗИ НСД;
- работу с данными при одновременном их преобразовании в файл-дисках;
- прозрачное преобразование жестких дисков (для редакции «С») для предотвращения доступа к данным, расположенным на жестких дисках, в обход СЗИ НСД.

Подсистема контроля устройств. Обеспечивает возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

Подсистема межсетевого экранирования. Обеспечивает контроль, а также фильтрацию потоков информации, поступающих в автоматизированную систему и выходящих за её пределы.

Подсистема обнаружения вторжений. Обеспечивает обнаружение и блокирование основных угроз безопасности, выполняет одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализирует некоторые отдельные сетевые протоколы.

Подсистема контроля целостности. Обеспечивает контроль целостности файловой системы, программно-аппаратной среды и реестра, периодическое тестирование СЗИ НСД, наличие средств восстановления СЗИ НСД, восстановление файлов и веток реестра в случае нарушения их целостности.

Подсистема восстановления после сбоев. Предусматривает процедуры восстановления после сбоев и отказов оборудования, которые должны обеспечивать полное и оперативное восстановление свойств СЗИ НСД. Реализована возможность возвращения всех настроек СЗИ НСД к исходным (установка параметров по умолчанию), что равносильно переустановке СЗИ НСД.

Подсистема развертывания (установочные модули). Выполняет все необходимые функции по установке СЗИ НСД на рабочую станцию и удалению с нее. В процессе развертывания реализована возможность установки конфигурации по умолчанию и другой рабочей конфигурации СЗИ НСД. В процессе развертывания реализована возможность автоматического ввода рабочей станции под управление сервера безопасности.

В ходе данной практической работы выполняется настройка системы защиты. Выполнение работ при установке и настройке системы защиты информации для действующей информационной системы в общем случае разделяется на следующие этапы:

1) Подготовка средств вычислительной технике к настройке;
2) Установка и настройка общесистемного программного обеспечения;
3) Установка и настройка прикладного программного обеспечения;
4) Установка и настройка сетевого оборудования;
5) Установка и настройка периферийного оборудования;
6) Установка и настройка средств антивирусной защиты;
7) Установка и настройка системы защиты информации от несанкционированного доступа.

В этой работе подробно рассмотрен последний 7-ой этап работ. В этом случае этап подготовки к установке и настройке СЗИ НСД включает в себя:

1) Проверку наличия дистрибутива СЗИ НСД последней версии.
2) Проверку наличия лицензионного ключа и формуляра.
3) Проверку наличия матрицы доступа.

Постановка задачи. Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать защищаемые каталоги (объект доступа).

Шаг 4. Установить объектам доступа права разграничения доступа по отношению к субъектам доступа.

Шаг 5. Выполнить настройку очистки остаточной информации.

Шаг 6. Выполнить настройку регистрации событий для объектов доступа.

Шаг 7. Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды.

Шаг 8. Выполнить настройку внешних носителей информации.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение А представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [1].

2. НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «SECRET NET»

Цель работы. Получить практические навыки настройки СЗИ НСД «Secret Net».

Теоретические сведения. Система «Secret Net» предназначена для обеспечения безопасности информационных систем на компьютерах, функционирующих под управлением ОС семейства «Windows».

При использовании соответствующих подсистем изделие обеспечивает:

- защиту от несанкционированного доступа к информационным ресурсам компьютеров;
- контроль устройств, подключаемых к компьютерам;
- обнаружение вторжений в информационную систему;
- антивирусную защиту;
- межсетевое экранирование сетевого трафика;
- авторизацию сетевых соединений.

Управление функционированием системы «Secret Net» может осуществляться централизованно или локально.

Система «Secret Net» реализует следующие основные функции:

- Контроль входа пользователей в систему (идентификация и аутентификация пользователей).
- Дискреционное разграничение доступа к файловым ресурсам, устройствам, принтерам.
- Мандатное (полномочное) разграничение доступа к файловым ресурсам, устройствам, принтерам, сетевым интерфейсам, включая:
- контроль потоков конфиденциальной информации в системе;
- контроль вывода информации на съемные носители.
- контроль состояния устройств компьютера с возможностями:
- блокирования компьютера при изменении состояния заданных устройств;
- блокирования подключения запрещенного устройства (устройства из запрещенной группы).
- Теневое копирование информации, выводимой на внешние носители и на печать.
- Автоматическая маркировка документов, выводимых на печать.
- Контроль целостности файловых объектов и реестра.

- Создание замкнутой программной среды для пользователей (контроль запуска исполняемых модулей, загрузки динамических библиотек).

- Очистка оперативной и внешней памяти при ее перераспределении.

- Изоляция процессов (выполняемых программ) в оперативной памяти.

- Защита содержимого локальных жестких дисков при несанкционированной загрузке операционной системы.

- Антивирусная защита компьютеров.

- Обнаружение вторжений.

- Межсетевое экранирование сетевого трафика.

- Авторизация сетевых соединений.

- Функциональный контроль ключевых защитных подсистем.

- Регистрация событий безопасности.

- Централизованное и локальное управление параметрами работы механизмов защиты.

Система «Secret Net» состоит из следующих программных пакетов, устанавливаемых на компьютерах:

Клиент. Клиент системы «Secret Net» предназначен для реализации защиты компьютера, на котором установлен данный компонент. Защита реализуется путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС «Windows». Защитные механизмы – это совокупность настраиваемых программных средств, входящих в состав клиента и обеспечивающих безопасное использование ресурсов. Клиент может функционировать в следующих режимах:

- автономный режим – предусматривает только локальное управление защитными механизмами;

- сетевой режим – предусматривает локальное и централизованное управление защитными механизмами, а также централизованное получение информации и изменение состояния защищаемых компьютеров.

Сервер безопасности. Сервер безопасности реализует возможности централизованного управления клиентами в сетевом режиме функционирования. Данный компонент обеспечивает:

- хранение данных централизованного управления;

- координацию работы других компонентов в процессе централизованного управления системой;

- получение от клиентов и обработку информации о состоянии защищаемых компьютеров;

- управление пользователями и авторизацией сетевых соединений;

- централизованный сбор, хранение и архивирование журналов.

Программа управления. Программа управления используется для централизованного управления серверами безопасности и клиентами в сетевом режиме функционирования. Данный компонент обеспечивает:

- управление параметрами объектов;

- отображение информации о состоянии защищаемых компьютеров и произошедших событиях тревоги;

- загрузку журналов событий;

- оперативное управление компьютерами.

В состав клиента системы «Secret Net» входят следующие функциональные компоненты:

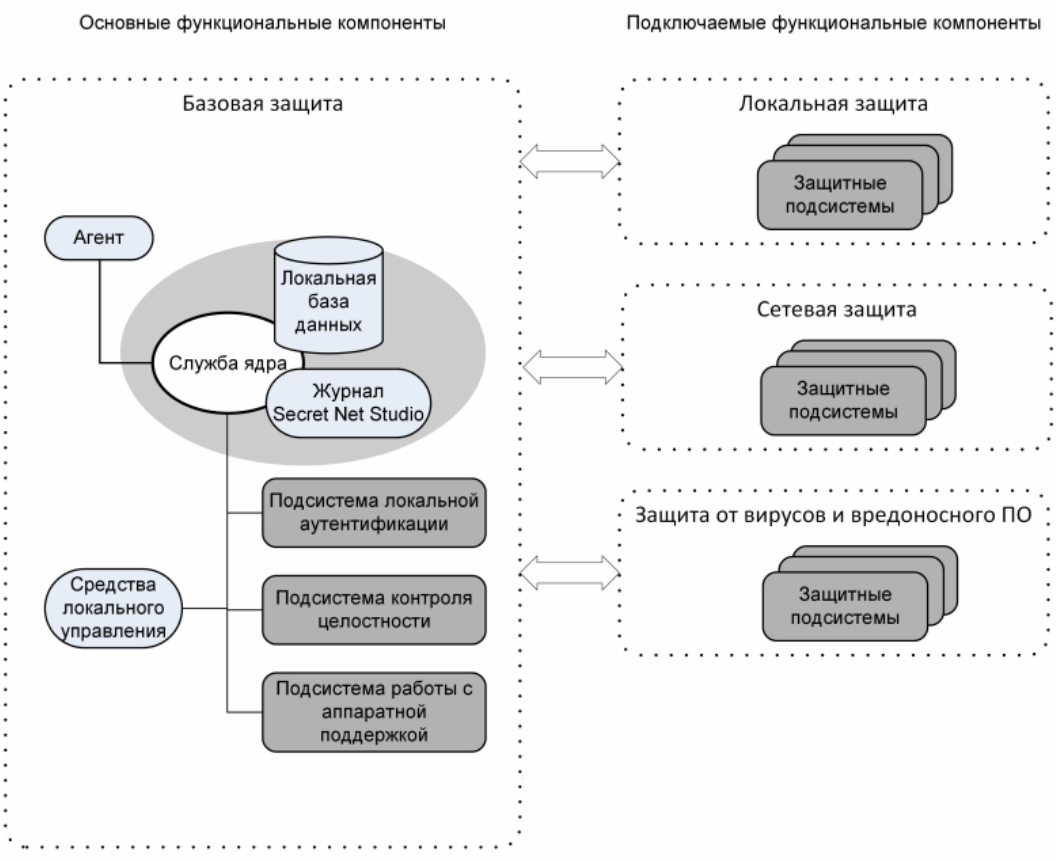
- основные программные службы, модули и защитные подсистемы (базовая защита);

- дополнительно подключаемые функциональные компоненты, условно разделенные на следующие группы:

- локальная защита;

- защита от вирусов и вредоносного ПО;

- сетевая защита.



Базовая защита. В базовую защиту входят следующие программные службы, модули и защитные подсистемы:

Ядро. Служба ядра автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Она осуществляет управление подсистемами и обеспечивает их взаимодействие. Ядро выполняет следующие функции:

- обеспечивает обмен данными между подсистемами клиента и обработку поступающих команд;

- обеспечивает доступ других компонентов к информации, хранящейся в локальной базе данных «Secret Net;

- обрабатывает поступающую информацию о событиях, связанных с безопасностью системы, и регистрирует их в журнале «Secret Net».

Подсистема регистрации является одним из элементов ядра клиента. Она предназначена для управления регистрацией событий, связанных с работой системы защиты. Такие события регистрируются в журнале «Secret Net». Эта информация поступает от подсистем «Secret Net», которые следят за происходящими событиями. Перечень событий «Secret Net», подлежащих регистрации, устанавливается администратором безопасности. В локальной

БД «Secret Net» хранится информация о настройках системы защиты, необходимых для работы защищаемого компьютера. Локальная БД размещается в реестре ОС «Windows» и специальных файлах.

Агент. Агентом является программный модуль в составе клиента, обеспечивающий взаимодействие с сервером безопасности. Агент принимает команды от сервера безопасности и отправляет ему данные о состоянии компьютера. Агент используется только в сетевом режиме функционирования клиента.

Средства локального управления. Средства локального управления обеспечивают:

- управление объектами защиты (устройствами, файлами, каталогами);
- управление параметрами пользователей и защитных механизмов;
- формирование заданий на контроль целостности;
- просмотр локальных журналов.

Подсистема локальной аутентификации. Подсистема используется в механизме защиты входа в систему. Совместно с ОС «Windows» подсистема обеспечивает:

- проверку возможности входа пользователя в систему;
- оповещение остальных модулей о начале или завершении работы пользователя;
- блокировку работы пользователя;
- загрузку данных с персональных идентификаторов пользователя;
- усиленную аутентификацию пользователя при входе в систему.

При обработке входа пользователя в систему осуществляется формирование контекста пользователя: определение его привилегий, уровня допуска и др. Дополнительно выполняется функциональный контроль работоспособности системы «Secret Net».

Подсистема контроля целостности. Подсистема контроля целостности обеспечивает проверку неизменности ресурсов компьютера: каталогов, файлов, ключей и значений реестра. В составе механизма контроля целостности подсистема реализует защиту от подмены ресурсов, сравнивая их с определенными эталонными значениями. Данная подсистема выполняет контролирующие функции не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе (загрузка, вход пользователя, контроль по расписанию).

Подсистема работы с аппаратной поддержкой. Подсистема используется в механизме защиты входа в систему для работы с устройствами аппаратной поддержки. Она обеспечивает взаимодействие системы «Secret Net» с определенным набором устройств и состоит из следующих модулей:

- модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам аппаратной поддержки;
- модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
- драйверы устройств аппаратной поддержки (если они необходимы).

Подключаемые функциональные компоненты клиента. В подключаемые функциональные компоненты клиента входят следующие защитные подсистемы:

Локальная защита. К группе локальной защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- контроль устройств;
- контроль печати;
- замкнутая программная среда;
- полномочное управление доступом;
- дискреционное управление доступом к ресурсам файловой системы;
- затирание данных;
- защита информации на локальных дисках;
- шифрование данных в криптоконтейнерах;
- паспорт ПО.

Сетевая защита. К группе сетевой защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- межсетевой экран;
- авторизация сетевых соединений.

Защита от вирусов и вредоносного ПО. К группе защиты от вирусов и вредоносного ПО относятся подсистемы, реализующие применение следующих механизмов защиты:

- обнаружение и предотвращение вторжений;
- антивирус.

Постановка задачи. Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать защищаемые каталоги (объект доступа).

Шаг 4. Установить объектам доступа права разграничения доступа по отношению к субъектам доступа.

Шаг 5. Выполнить настройку очистки остаточной информации.

Шаг 6. Выполнить настройку регистрации событий для объектов доступа.

Шаг 7. Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды.

Шаг 8. Выполнить настройку внешних носителей информации.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение Б представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [2].

3. НАСТРОЙКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОС СН «ASTRA LINUX»

Цель работы. Получить практические навыки настройки СЗИ НСД в ОС СН «Astra Linux».

Теоретические сведения. ОС СН предназначена для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Основная задача, решаемая ОС в процессе своего функционирования – обеспечение интерфейса для доступа ПО к устройствам вычислительной системы посредством управления устройствами, вычислительными процессами, а также эффективное распределение вычислительных ресурсов между вычислительными процессами в соответствии с требованиями руководящих документов по обеспечению защиты информации, содержащей сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Для решения основной задачи функционирования ОС она декомпозируется на следующие основные классы задач:

Идентификация и аутентификация пользователей. Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании механизма PAM, который представляет собой набор разделяемых библиотек (модулей), с помощью которых администратор может организовывать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации. Подобный подход позволяет изменять процедуру аутентификации без изменения исходного кода и повторного компилирования PAM. Сценарии описываются в конфигурационных файлах.

В ОС реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хэш-функции по ГОСТ Р 34.11-94 и по ГОСТ Р 34.11-2012.

Дискреционное разграничение доступа. В ОС механизм дискреционного разграничения доступа обеспечивает проверку дискреционных ПРД, формируемых в виде базовых ПРД ОС семейства

Linux, формируемых в виде идентификаторов субъектов (идентификатор пользователя (UID) и идентификатор группы (GID), имеющих доступ к объекту (чтение, запись, исполнение). Кроме того, для формирования дискреционных ПРД в ОС используются списки контроля доступа (ACL) и механизм системных привилегий ОС семейства Linux.

Мандатное разграничение доступа. Решение задачи мандатного разграничения доступа процессов к ресурсам основан на реализации соответствующего механизма в ядре ОС. При этом, принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом.

Правила приятия решения могут быть записаны следующим образом. Пусть контекст безопасности субъекта содержит уровень L0 и категории C0, а мандатная метка объекта содержит уровень L1 и категории C1. В ОС определены следующие операции сравнения уровней и категорий:

- уровень L0 меньше уровня L1 (L0<L1), если численное значение L0 меньше численного значения L1;

- уровень L0 равен уровню L1 (L0=L1), если численные значения L0 и L1 совпадают;

- категории C0 меньше категорий C1 (C0<C1), если все биты набора C0 являются подмножеством набора бит C1;

- категории C0 равны категориям C1 (C0=C1), если значения C0 и C1 совпадают;

Таким образом, в механизме мандатного разграничения доступа действуют следующие правила:

- операция записи разрешена, если L0=L1 и C0=C1;

- операция чтения разрешена, если L0>=L1 и C0>=C1;

- операция исполнения разрешена, если L0>=L1 и C0>=C1.

В остальных случаях анализируются полномочия и тип мандатной метки. Тип метки может использоваться для того, чтобы изменять ее эффектные действия. Ненулевой тип метки может быть установлен только привилегированным процессом.

Изоляция адресных пространств процессов. Решение задачи изоляции адресных пространств процессов основано на архитектуре ядра ОС, которое

обеспечивает для каждого процесса в системе собственное изолированное адресное пространство. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми и работает процессор) преобразуются в разные физические для разных адресных пространств. Процесс не может несанкционированным образом получить доступ к пространству другого процесса, так как непривилегированный пользовательский процесс лишен возможности работать с физической памятью на прямую.

Механизм разделяемой памяти является санкционированным способом получить нескольким процессам доступ к одному и тому же участку памяти и находится под контролем дискреционных и мандатных ПРД.

Адресное пространство ядра защищено от прямого воздействия пользовательских процессов с использованием механизма страничной защиты. Страницы пространства ядра являются привилегированными и доступ к ним из непривилегированного кода вызывает исключение процессора, которое обрабатывается корректным образом ядром ОС. Единственным санкционированным способом доступа к ядру ОС из пользовательской программы является механизм системных вызовов, который гарантирует возможность выполнения пользователем только санкционированных действий.

Регистрация событий. В ОС реализована расширенная подсистема протоколирования, осуществляющая регистрацию событий в двоичные файлы с использованием сервиса parlogd.

В библиотеках подсистемы безопасности PARSEC реализован программный интерфейс для протоколирования событий с использованием расширенной подсистемы протоколирования.

Очистка оперативной и внешней памяти. Решение задачи очистки ОП основано на архитектуре ядра ОС, которое гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено ПРД. Это означает, что средства взаимодействия между процессами контролируются с помощью ПРД, и процесс не может получить неочищенную память (как оперативную, так и дисковую).

Решение задачи очистки памяти на внешних носителях основано на реализации механизма, который очищает неиспользуемые блоки ФС непосредственно при их освобождении. Работа названного механизма снижает скорость выполнения операция удаления и усечения размера файла. Механизм является настраиваемым и позволяет обеспечить работу ФС ОС в одном из следующих режимов:

- данные любых удаляемых/урезаемых файлов пределах ФС предварительно очищаются маскирующей последовательностью;
- данные ФС освобождаются обычным образом (без предварительного маскирования).

Режим работы ФС может быть выбран администратором ОС и задан в виде параметра монтирования ФС.

Контроль целостности. Решение задач контроля целостности основано на использовании библиотеки libgost, в которой реализованы функции хэширования в соответствии с ГОСТ Р 34.11- 94, ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит. Данная библиотека используется в средствах контроля целостности дистрибутива и средствах контроля целостности ФС.

Контроль целостности дистрибутива обеспечивается методом расчета его контрольной суммы и сравнения полученного значения с эталонным значением контрольной суммы.

Контроль целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств, который предоставляет возможность периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки libgost и контроль целостности связанных с файлами атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования).

Создание замкнутой программной среды. Средства создания замкнутой программной среды предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав устанавливаемого СПО и в расширенные атрибуты файловой системы.

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС digsig_verif, который является не выгружаемым модулем ядра Linux, и может функционировать в одном из следующих режимов:

1) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение запрещается (штатный режим функционирования);

2) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в СПО);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный режим для тестирования СПО).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы также реализован в модуле ядра ОС digsig_verif и может функционировать в одном из следующих режимов:

1) запрещается открытие файлов, поставленных на контроль файлов, с неверной ЭЦП или без ЭЦП;

2) открытие файлов, поставленных на контроль файлов, с неверной ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в расширенных атрибутах файловой системы);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется.

Постановка задачи. Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать защищаемые каталоги (объект доступа).

Шаг 4. Установить объектам доступа права разграничения доступа по отношению к субъектам доступа.

Шаг 5. Выполнить настройку очистки остаточной информации.

Шаг 6. Выполнить настройку регистрации событий для объектов доступа.

Шаг 7. Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды.

Шаг 8. Выполнить настройку внешних носителей информации.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение В представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [3].

4. 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].

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Конфидент Система защиты информации от несанкционированного доступа Dallas Lock 8.0 Руководство по эксплуатации RU.48957919.501410-02 92, 2017

2. Код безопасности Средство защиты информации Secret Net 7 Руководство администратора Настройка механизмов защиты RU.88338853.501410.015 91 3, 2016

3. Справочный центр Astra Linux https://wiki.astralinux.ru

4. Kaspersky Endpoint Security 10 для «Windows», 2017

ПРИЛОЖЕНИЕ А

Пример настройки СЗИ НСД «Dallas Lock»

Создание пользователя системы. Необходимо выполнить следующие действия:

- открыть оболочку администратора системы защиты (рис. 1);

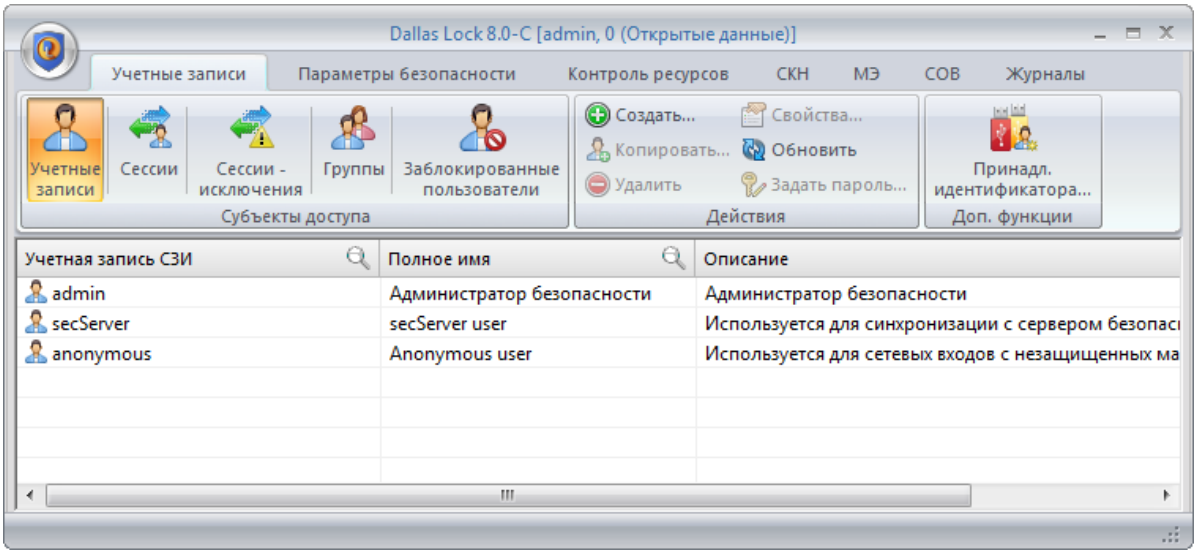


Рисунок 1. Окно оболочки администратора системы защиты

- выбрать категорию «Учетные записи»;

- нажать кнопку «Создать» в категории «Действия» или выбрать соответствующую кнопку из контекстного меню, нажав правую кнопку мыши.

- на экране появится окно создания новой учетной записи (рис. 2).

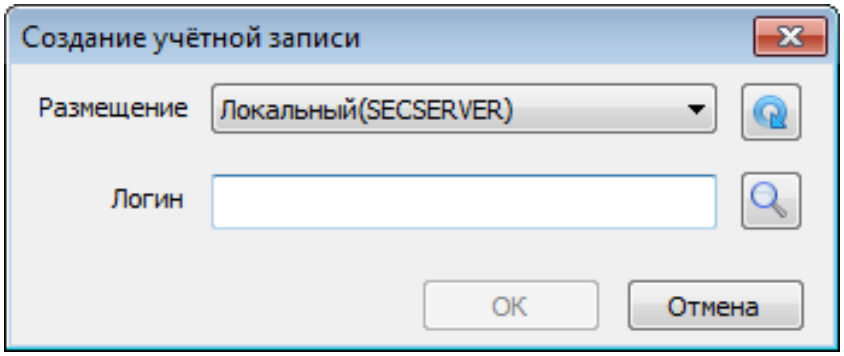


Рисунок 2. Окно создания учетной записи

- в поле «Размещение» необходимо выбрать значение «Локальный»;

- в поле «Логин» необходимо ввести логин (имя) регистрируемого пользователя;

При вводе имени в системе существуют следующие правила:

максимальная длина имени - 20 символов;

имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ [ ] : | < > + = ; , ? @ *); разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

- нажать кнопку «ОК» для открытия окна редактирования параметров учетной записи (рис. 3);

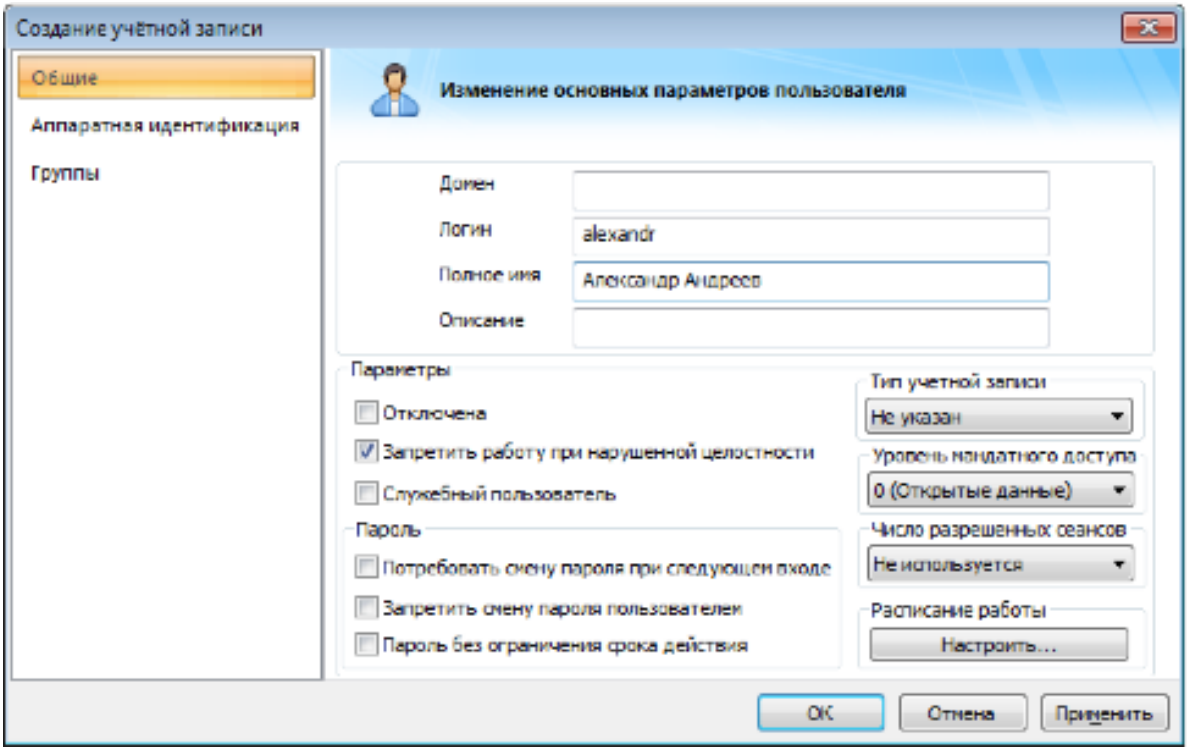


Рисунок 3. Окно редактирования параметров учетной записи

- заполнить поля «Полное имя», «Описание»;

- установить включенными следующие параметры: «Запретить работу при нарушенной целостности», «Запретить смену пароля пользователем».

- во вкладке «Группы» (рис. 4) добавить необходимые группы в соответствии с ролью пользователя;

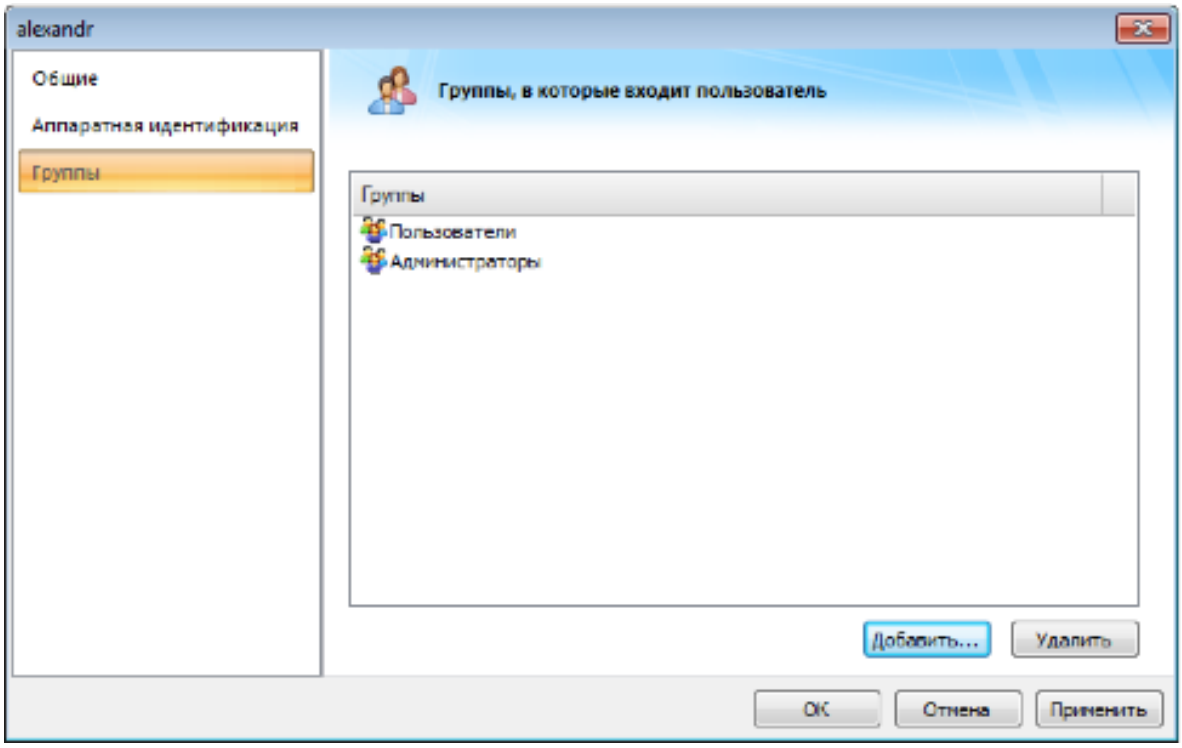


Рисунок 4. Окно редактирования списка групп пользователя

- после заполнения всех необходимых параметров в окне создания учетной записи нажать кнопку «ОК» для открытия формы ввода пароля (рис.5);

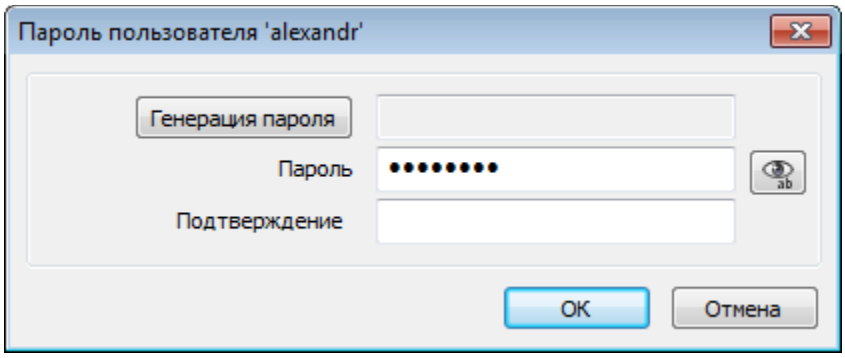


Рисунок 5. Окно формы ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля 32 символа;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором.

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку с надписью «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

- для завершения создания пользователя нажать кнопку «ОК».

Настройка идентификации и аутентификации. Необходимо выполнить следующие действия:

- открыть оболочку администратора системы защиты;

- перейти во вкладку «Параметры безопасности», «Вход» (рис. 6);

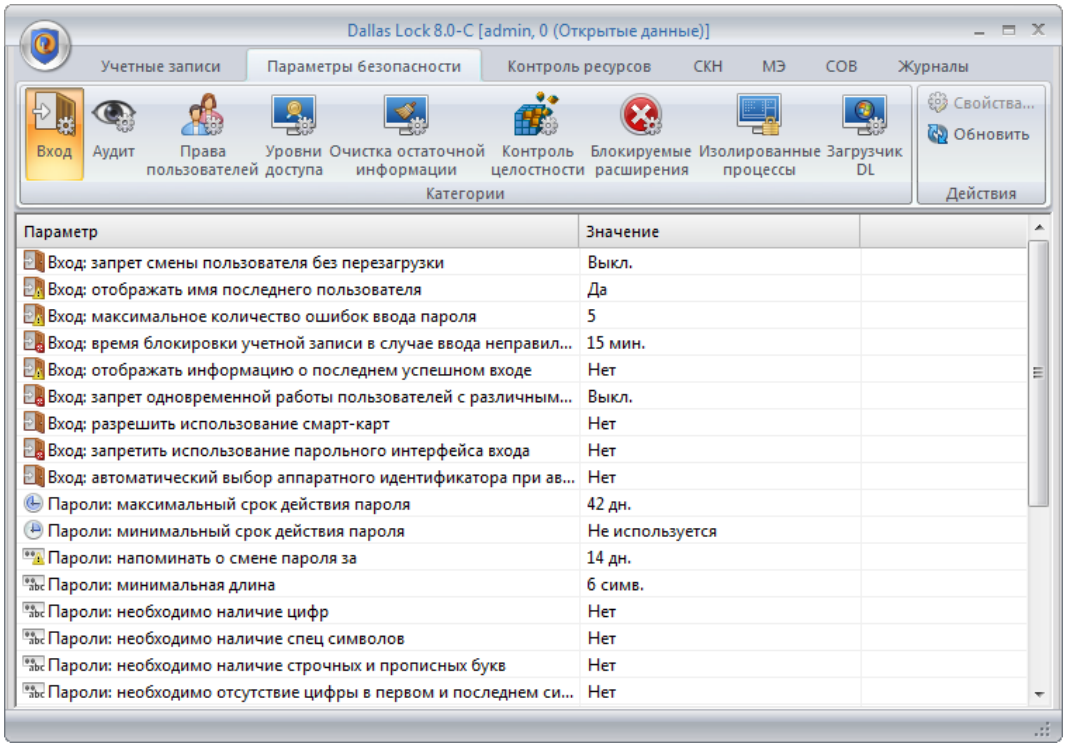


Рисунок 6. Список параметров входа

- в соответствии с требованиями политики безопасности настроить все параметры, расположенные в списке параметров «Вход», «Пароли».

Установка прав разграничения доступа. Необходимо выполнить следующие действия:

- открыть оболочку администратора системы защиты;

- перейти в категорию «Дискреционный доступ» на вкладке «Контроль ресурсов» (рис. 7);

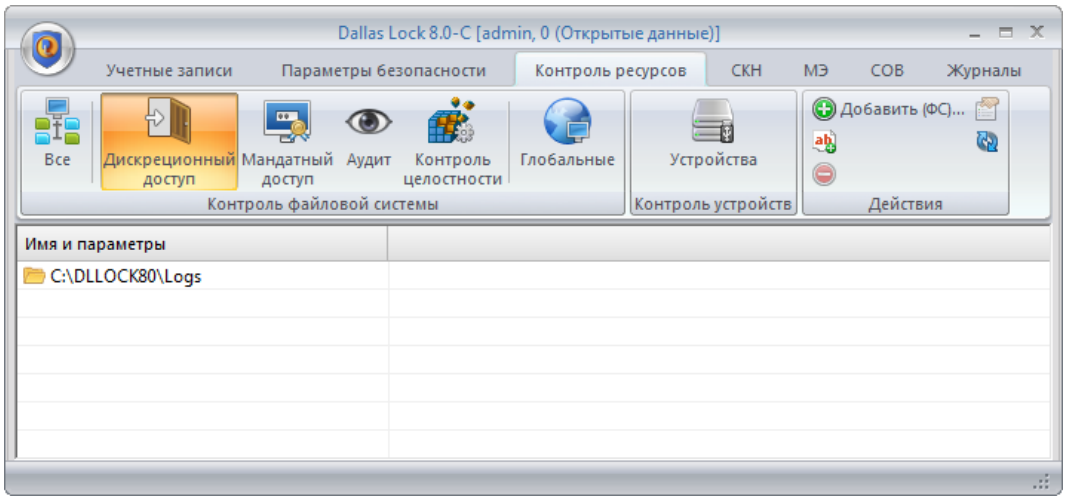


Рисунок 7. Окно дискреционного доступа

- в меню выбрать действие «Добавить (ФС)»;

- в появившемся окне проводника (рис. 8) необходимо найти нужный объект ФС и нажать кнопку «Выбрать»;

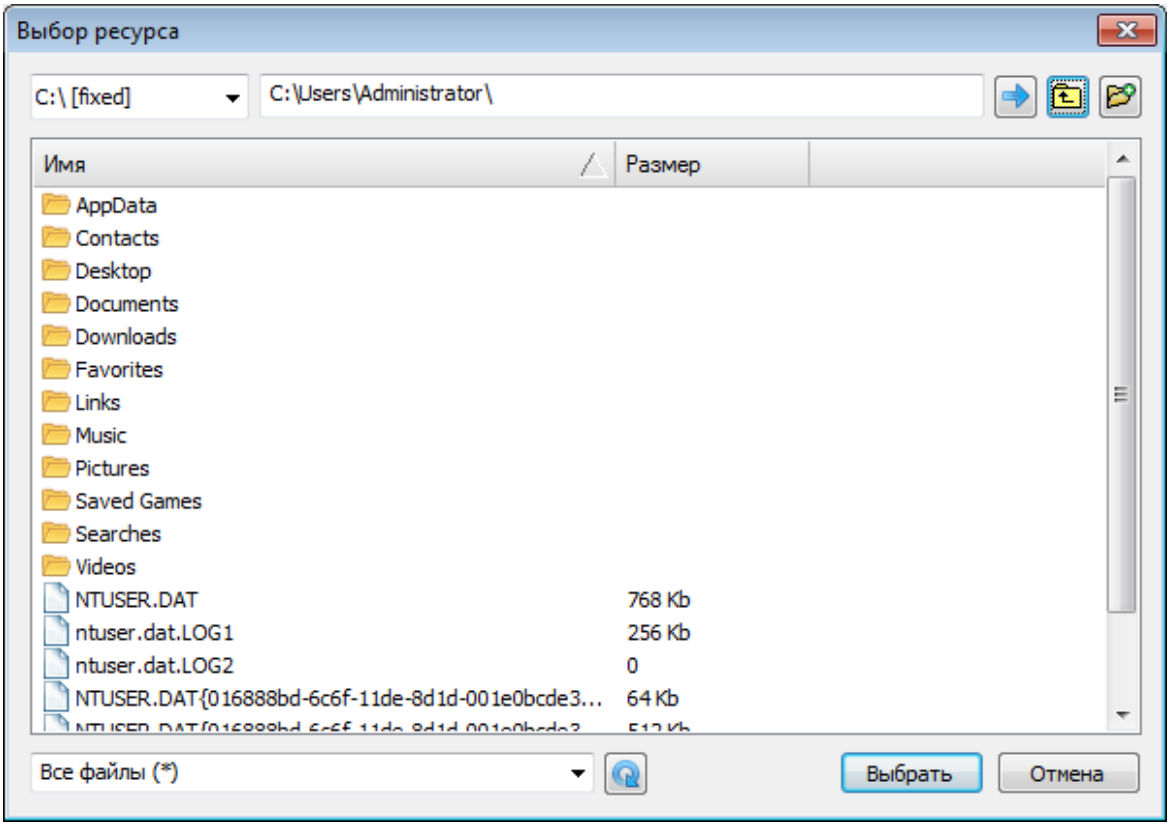


Рисунок 8. Окно выбора объекта ФС

- в окне настроек безопасности необходимо выбрать вкладку «Дискреционный доступ» (рис.9);

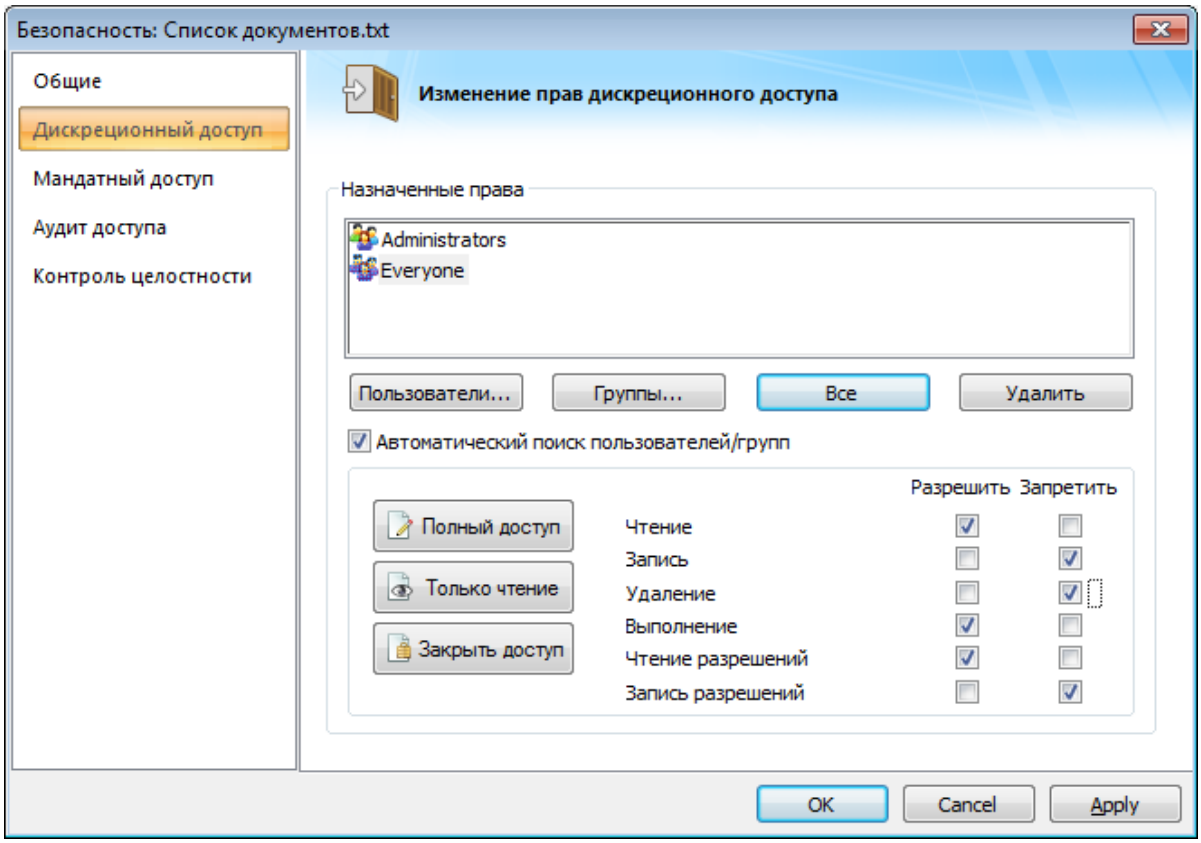


Рисунок 9. Окно назначения прав дискреционного доступа

- чтобы назначить определенные дискреционные права для определенных пользователей необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп;

- для выбранных пользователей/групп необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту (рис. 10);

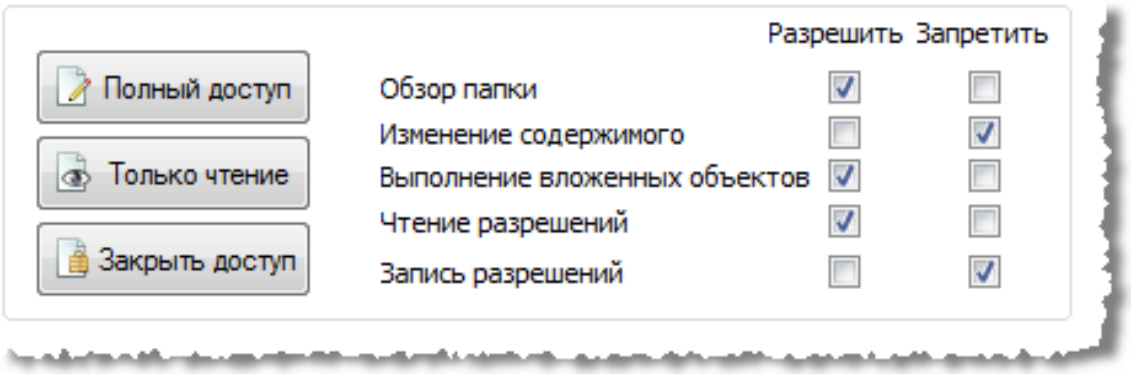


Рисунок 10. Список прав дискреционного пользования

- для завершения настройки разграничения доступа к выбранному объекту нажать кнопку «ОК».

Объекты, на которые назначен дискреционный доступ, автоматически появятся в списке объектов в окне категории «Дискреционный доступ» на вкладке «Контроль ресурсов».

Настройка очистки остаточной информации. Необходимо выполнить следующие действия:

- открыть оболочку администратора системы защиты;

- перейти в категорию «Очистка остаточной информации» на вкладке «Параметры безопасности» (рис. 11);

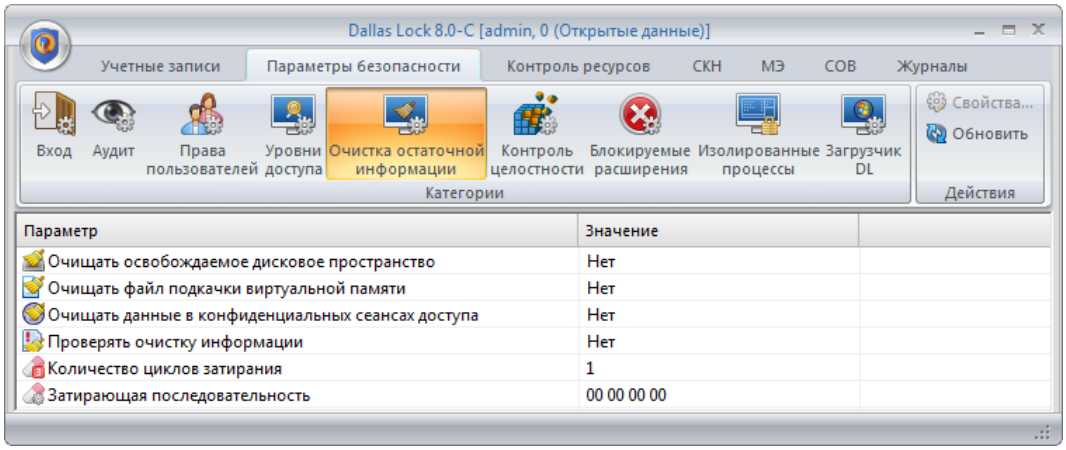


Рисунок 11. Параметры очистки остаточной информации

- установить значение «Да» для следующих параметров: «Очищать освобождаемое дисковое пространство», «Очищать файл подкачки виртуальной памяти», «Проверять очистку информации»;

- установить «Количество циклов затирания» в соответствии с требованиями политики безопасности.

Настройка регистрации событий. Необходимо выполнить следующие действия:

- открыть оболочку администратора системы защиты;

- перейти в категорию «Аудит» на вкладке «Параметры безопасности»;

- для настройки аудита доступа к ресурсам необходимо установить для определенного параметра значение «Включен» в окне редактирования параметров безопасности;

- для настройки аудита глобальных параметров перейти в категорию «Глобальные» на вкладке «Контроль ресурсов»;

- выбрать глобальный параметр и нажать «Свойства»;

- открыть вкладку «Аудит доступа» (рис. 12);

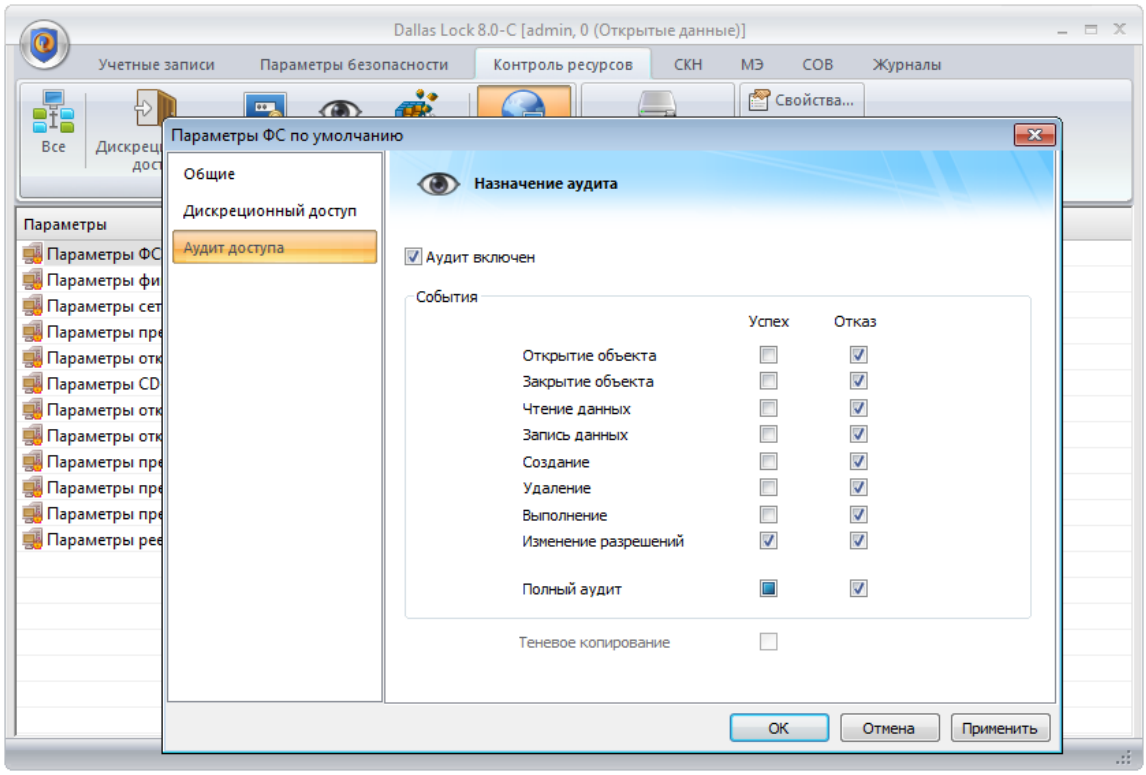


Рисунок 12. Окно назначения аудита на ресурс файловой системы

- перед выбором событий включить аудит, отметив флажком поле «Аудит включен»;

- отметить необходимые события;

- нажать «ОК»;

- для настройки аудита локальных объектов ФС необходимо перейти в категорию «Аудит» на вкладке «Контроль ресурсов»;

- нажать «Добавить (ФС)» и выбрать ресурс для назначения аудита (рис. 13);

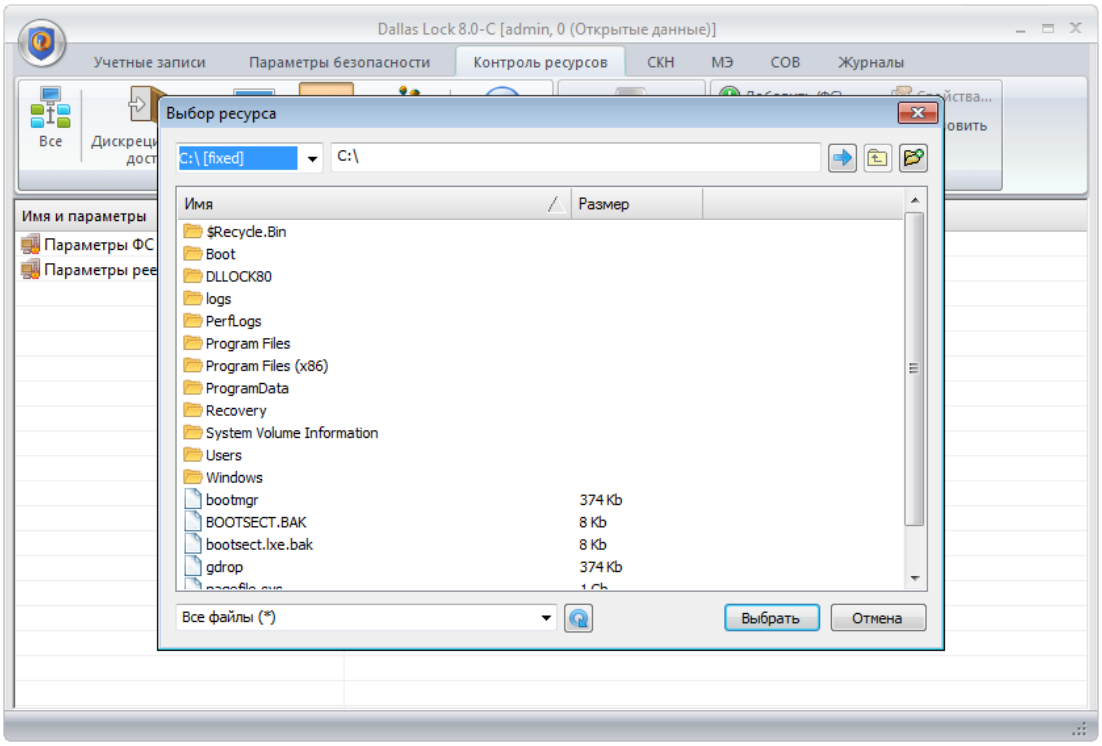


Рисунок 13. Выбор ресурса для назначения аудита

- открыть вкладку «Аудит доступа»;

- перед выбором событий включить аудит, отметив флажком поле «Аудит включен»;

- отметить необходимые события;

- нажать «ОК».

Настройка контроля целостности файловой системы и программно-аппаратной среды. Необходимо выполнить следующие действия:

- открыть оболочку администратора системы защиты;

- для настройки общих параметров необходимо перейти в категорию «Контроль целостности» на вкладке «Параметры безопасности» (рис. 14);

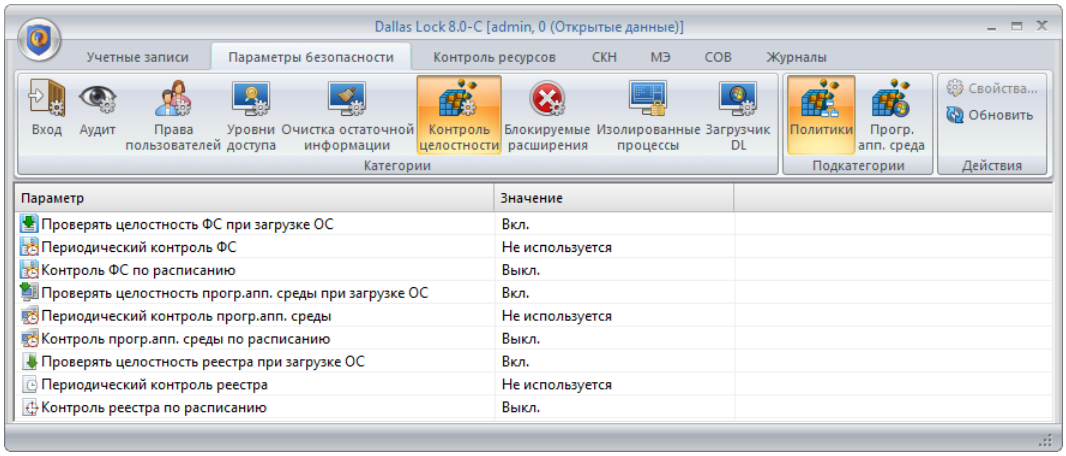


Рисунок 14. Вкладка контроль целостности в оболочке администратора

- выполнить необходимые настройки по периодичности проверки целостности отдельно для объектов ФС, отдельно для объектов программно-аппаратной среды и отдельно для реестра

- для настройки контроля целостности объектов ФС необходимо нажать «Добавить (ФС) в категории «Контроль целостности» на вкладке «Параметры безопасности»;

- выбрать объект и в появившемся окне открыть вкладку «Контроль целостности» (рис. 15);

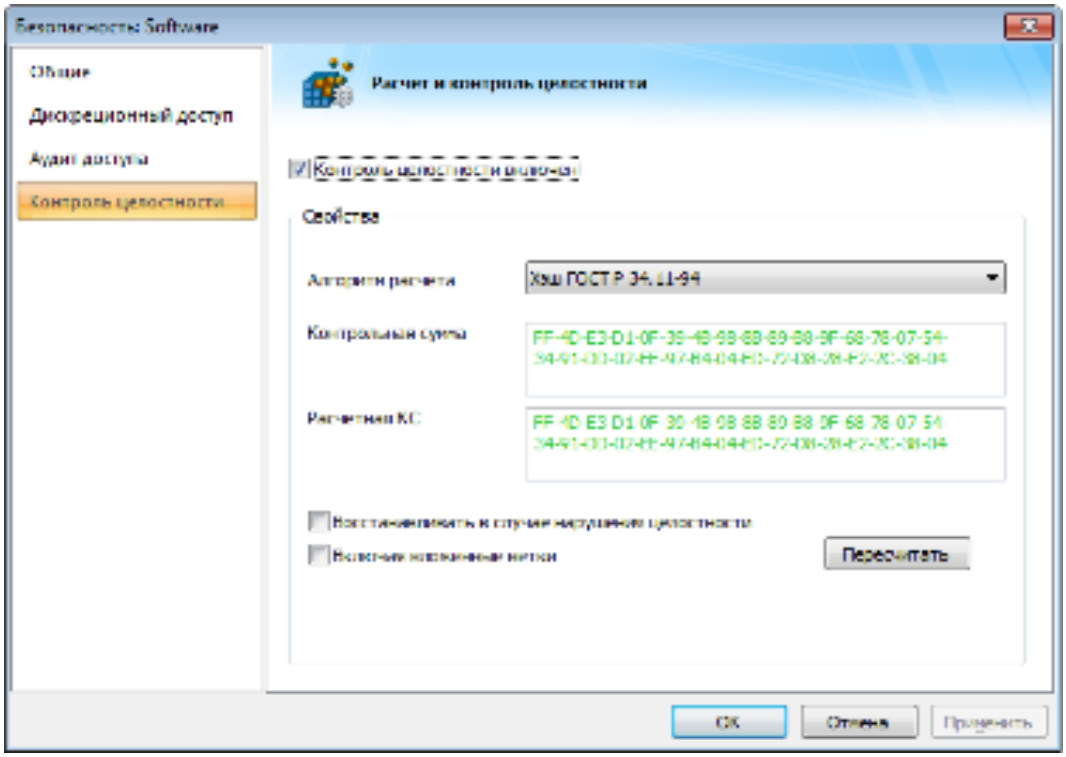


Рисунок 15. Контроль целостности ресурса файловой системы

- отметить флажком поле «Контроль целостности включен»;

- выбрать алгоритм расчета контрольной суммы (CRC32, ГОСТ Р 34.11-94, MD5) и нажать кнопку «Пересчитать»;

- нажать кнопки «Применить» и «ОК».

Настройка прав разграничения доступа для внешних носителей информации. Необходимо выполнить следующие действия:

- подключить внешний носитель;

- открыть оболочку администратора системы защиты;

- перейти в категорию «Сменные накопители» на вкладке «СКН» (рис. 16);

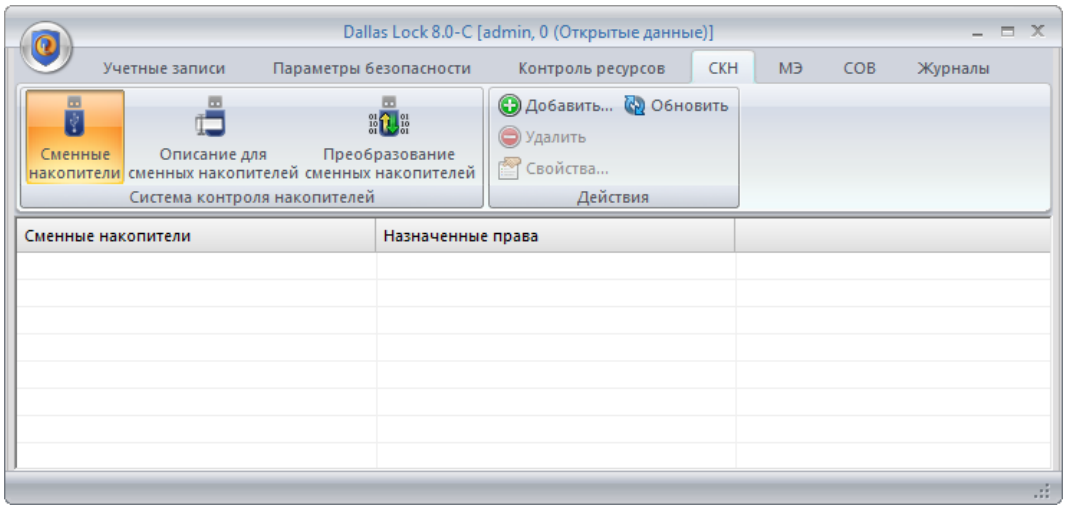


Рисунок 16. Окно настройки прав разграничения доступа для внешних носителей информации

- нажать кнопку «Добавить…» и выбрать необходимый носитель информации;

- дальнейшая настройка прав разграничения доступа для внешних носителей информации соответствует настройке прав разграничения доступа для объектов ФС.

ПРИЛОЖЕНИЕ Б

Пример настройки СЗИ НСД «Secret Net»

Создание пользователя системы. Создание пользователя может выполняться как функциями ОС, так и с помощью СЗИ НСД.

Настройка идентификации и аутентификации. Необходимо выполнить следующие действия:

Назначить минимальную длину пароля:

- зайти в меню «Пуск», «Все программы», «Код безопасности», «Secret Net», «Локальная политика безопасности»;

- в открывшемся окне перейти в «Локальные политики», «Политика учетных записей», «Политика паролей»;

- выбрать политику «Минимальная длина пароля» и установить необходимый параметр безопасности (рис. 17).

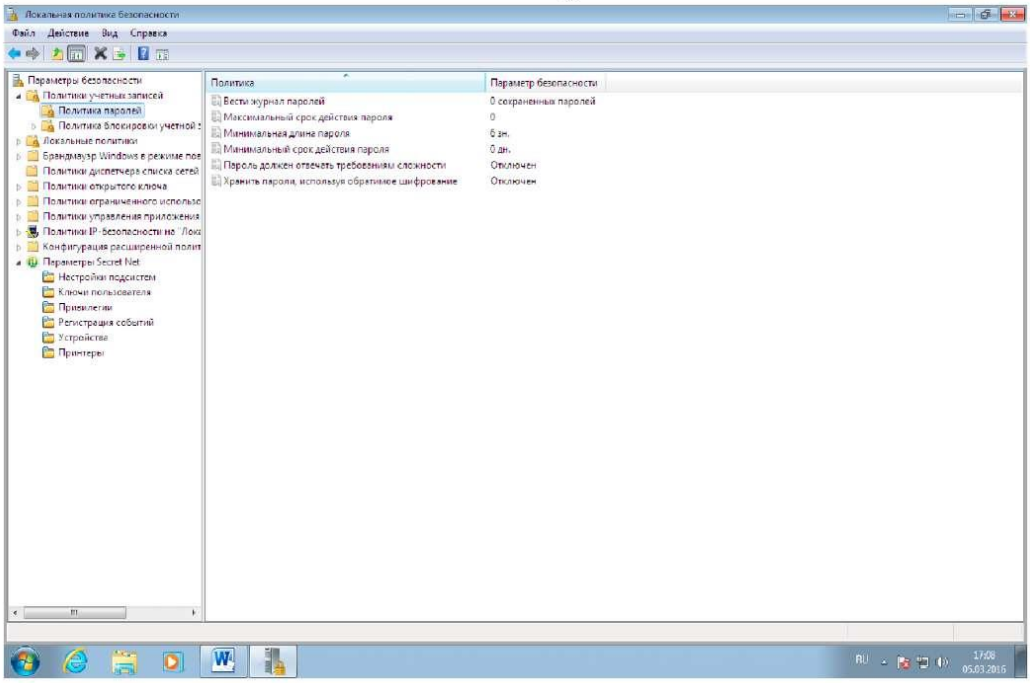


Рисунок 17. Окно настройки паролей

Установка прав разграничения доступа. Необходимо выполнить следующие действия:

- открыть оснастку СЗИ НСД;

- зайти в «Параметры безопасности», «Параметры Secret Net»;

- зайти в папку «Привилегии». В правой части появится список привилегий;

- выбрать элемент «Дискреционное управление доступом: Управление правами доступа» и вызвать диалог настройки параметра;

- в диалоге отредактировать список пользователей и групп пользователей, которым предоставлена привилегия, и нажмите кнопку "ОК";

- в программе «Проводник» вызвать контекстное меню ресурса (каталога или файла) и выбрать команду «Свойства». В появившемся на экране окне «Свойства» перейти к диалогу «Secret Net» (рис. 18);

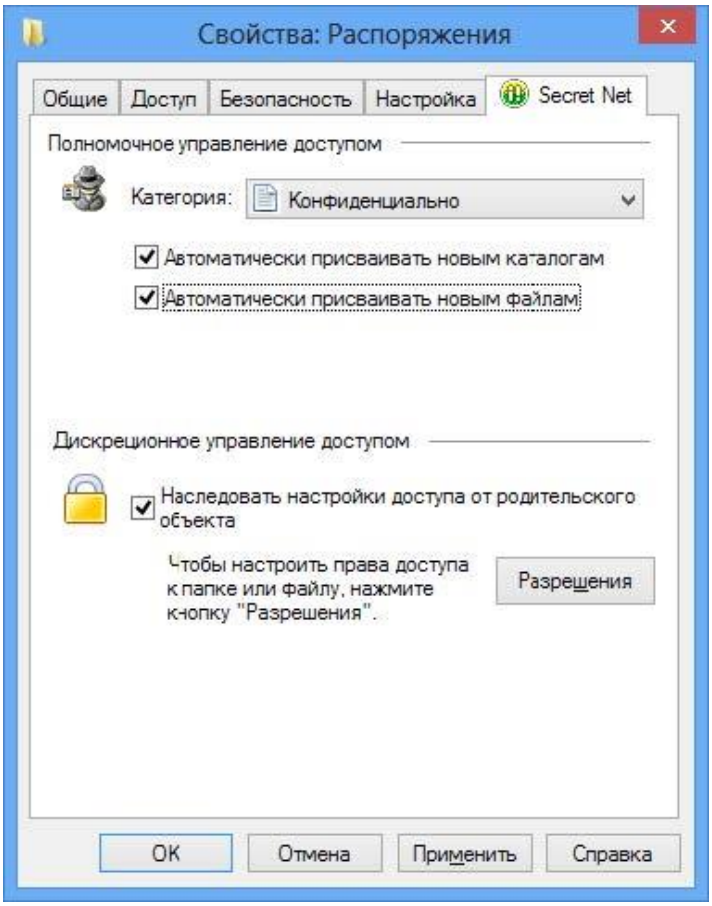


Рисунок 18. Окно «Свойства»

- если установлена отметка в поле «Наследовать настройки доступа от родительского объекта» (то есть для ресурса включен режим наследования прав), то необходимо удалить отметку из поля, чтобы явно указать права доступа. Если отметка отсутствует или необходимо ознакомиться с наследуемыми правами доступа — то необходимо нажать кнопку «Разрешения». На экране появится диалог ОС Windows "Разрешения...". В диалоге используются те же методы работы, как в аналогичных стандартных средствах ОС Windows (рис. 19);

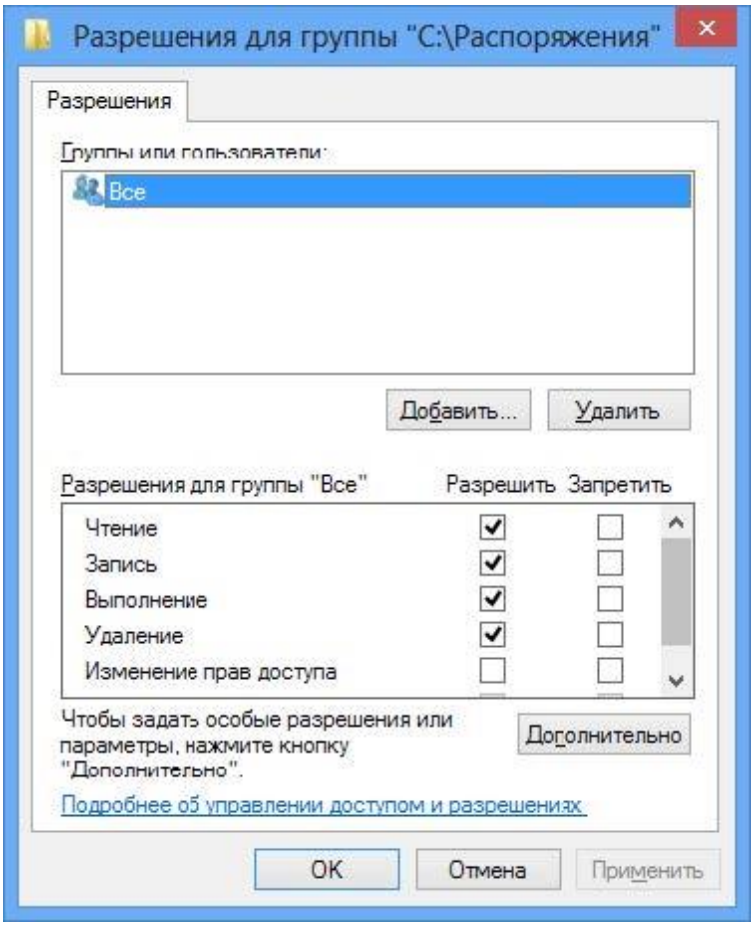


Рисунок 19. Окно «Разрешения»

- при необходимости можно отредактировать список учетных записей в верхней части диалога с помощью кнопок "Добавить" и "Удалить";

- для изменения параметров доступа нужно выбрать в списке нужную учетную запись и затем расставить разрешения и запреты на выполнение операций. Если требуется получить дополнительные сведения (например, об источнике наследуемых параметров) или настроить особые параметры (включая параметры аудита операций с ресурсом) — нужно нажать кнопку "Дополнительно" и выполнить нужные действия в появившемся окне дополнительных параметров безопасности ОС Windows;

- по окончании настройки закрыть ранее открытые диалоги с помощью кнопки "ОК".

Настройка очистки остаточной информации. Необходимо выполнить следующие действия:

- зайти в меню «Пуск», «Все программы», «Код безопасности», «Secret Net», «Локальная политика безопасности»;

- в открывшемся окне перейти в «Локальные политики», «Параметры безопасности»;

- включить параметр «Завершение работы: очистка файла подкачки виртуальной памяти», установив параметр безопасности в значение «Включить» (рис. 20).

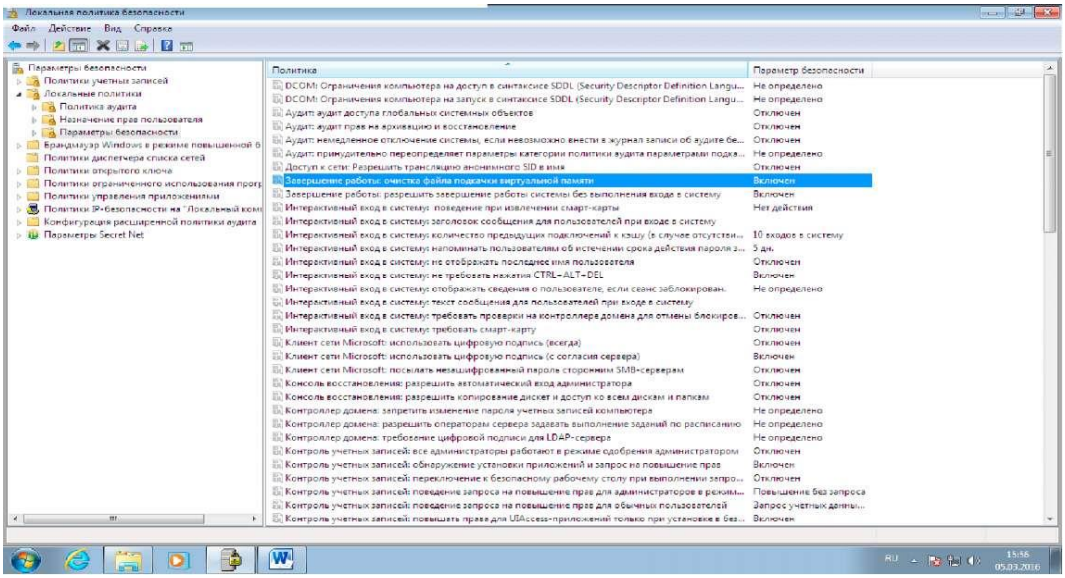


Рисунок 20. Окно локальной политики безопасности

Настройка регистрации событий. Необходимо выполнить следующие действия:

- зайти в меню «Пуск», «Все программы», «Код безопасности», «Secret Net», «Локальная политика безопасности»;

- в открывшемся окне перейти в «Локальные политики», «Политика аудита»;

- зайти в свойства и поставить галочку напротив значений «Успех» и/или «Отказ» (рис. 21);

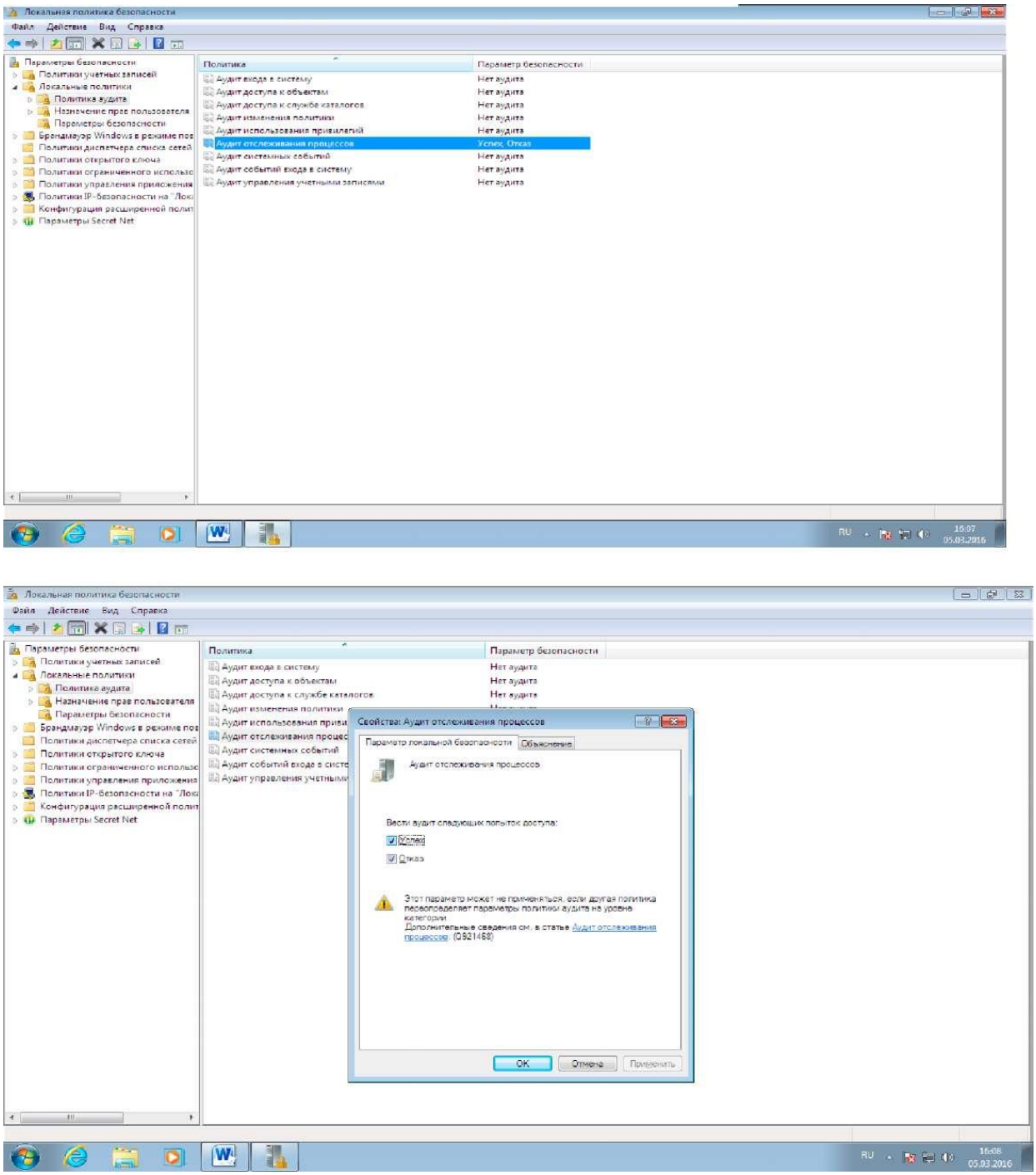


Рисунок 21. Окно настройки аудита процессов

Настройка контроля целостности файловой системы и программно-аппаратной среды. Необходимо выполнить следующие действия:

- запустить программу «Контроль программ и данных» в локальном режиме;

- сформировать новую модель данных (фрагмент модели) с настройкой контроля по умолчанию. Для этого выбрать команду «Файл», «Новая модель

данных». В появившемся диалоге настроить параметры для режима замкнутой программной среды:

- отметить представленные стандартные задачи для ОС и СЗИ;

- оставить отмеченным поле «Производить подготовку для ЗПС»;

- установить отметку в поле «Добавить другие задачи из списка» и нажать кнопку для выбора задач. В появившемся диалоге выбрать в списке элементы, необходимые для работы любого пользователя компьютера. Список содержит установленные на компьютере программы, представленные в меню «Пуск»;

- оставить отмеченным поле «Рассчитывать эталоны».

- нажать кнопку «ОК». При появлении диалога запроса на продолжение операции нажать кнопку «Да». По окончании процесса формирования модели данных в списке заданий появится задание ЗПС, которое будет применяться для всех пользователей группы Users и блокировать запуск программ, не включенных в список ресурсов задания.

Настройка прав разграничения доступа для внешних носителей информации. Необходимо выполнить следующие действия:

- вызвать оснастку для управления параметрами объектов групповой политики и перейти к разделу «Параметры безопасности», «Параметры Secret Net»;

- выбрать папку «Устройства». В правой части окна оснастки появится список устройств;

- выбрать в списке объект (класс или устройство), вызвать контекстное меню и выбрать команду «Свойства». На экране появится диалог для настройки параметров объекта;

- перейти к группе параметров «Настройки» (рис. 22);

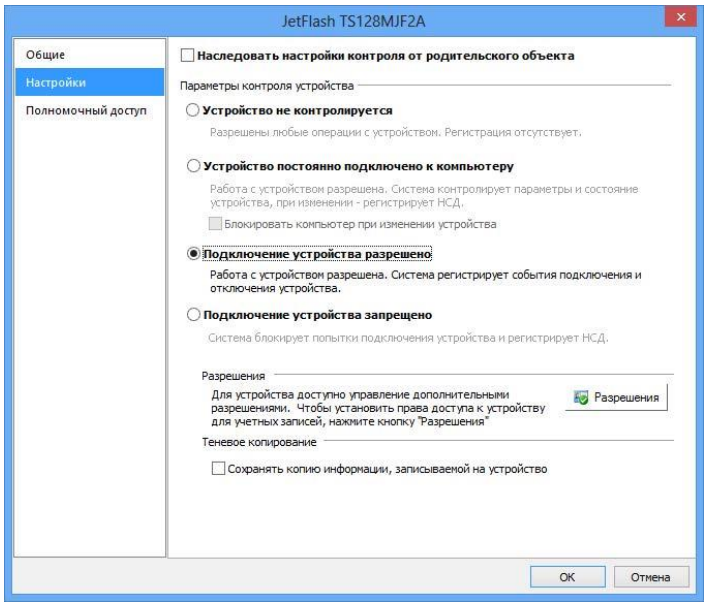


Рисунок 22. Окно настройки устройства

- удалить отметку из поля «Наследовать настройки контроля от родительского объекта»; После этого станут доступны параметры контроля устройства;

- отметить режим контроля «Устройство постоянно подключено к компьютеру» или «Подключение устройства разрешено» и нажать кнопку «Разрешения». На экране появится диалог ОС Windows "Разрешения..." (рис. 23);

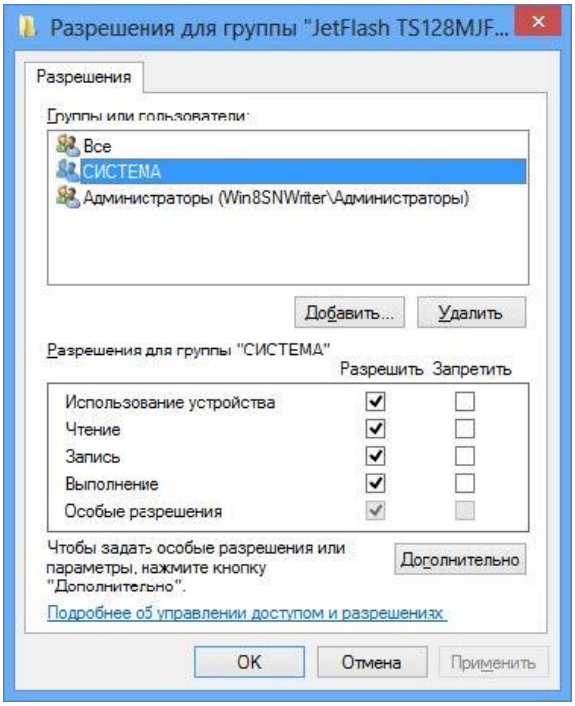


Рисунок 23. Окно «Разрешения»

- при необходимости отредактировать список учетных записей в верхней части диалога;

- Для изменения параметров доступа выбрать в списке нужную учетную запись и затем расставить разрешения и запреты на выполнение операций. При этом учитывать принцип наследования параметров от родительских объектов дочерними: явно заданные параметры перекрывают унаследованные от родительских объектов. Для настройки особых разрешений нажмите кнопку "Дополнительно" и настройте параметры в открывшемся диалоговом окне.

ПРИЛОЖЕНИЕ В

Пример настройки ОС СН «Astra Linux»

Создание пользователя системы. Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;
- перейти по вкладке «Пользователи» (рис. 24);

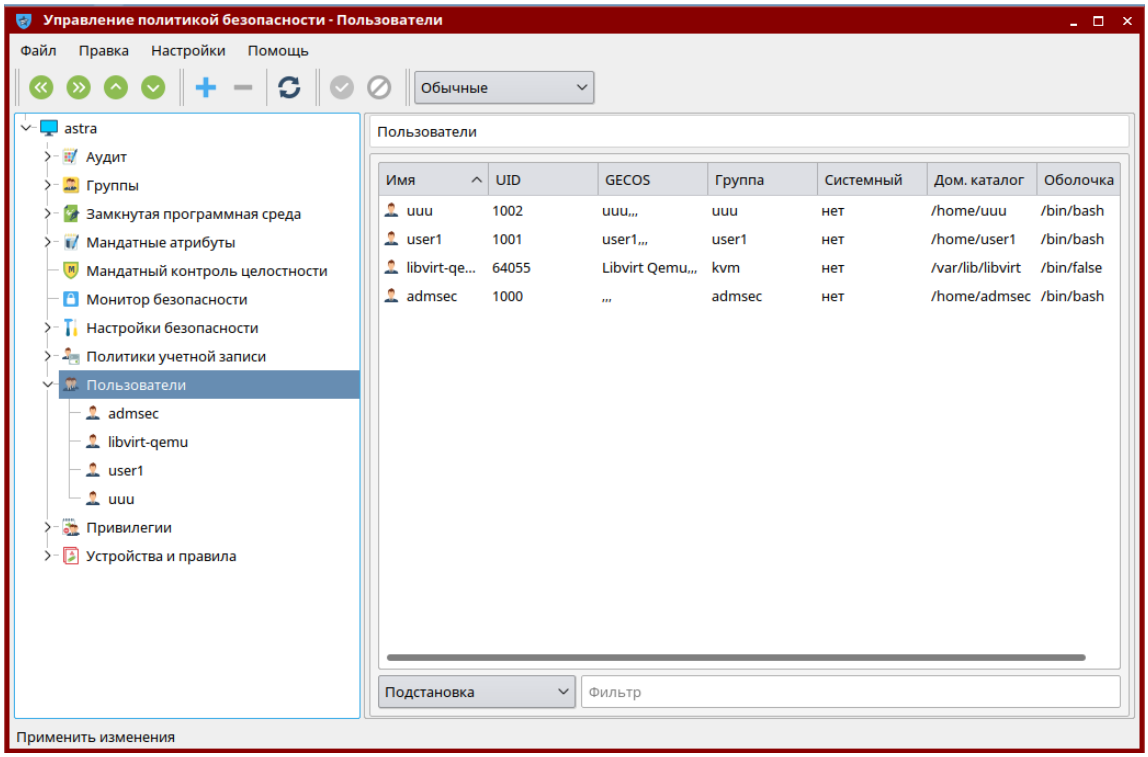


Рисунок 24. Окно учетных записей

- нажать кнопку «Создать новый элемент»;
- ввести имя пользователя;
- выбрать необходимые группы для пользователя (рис. 25);

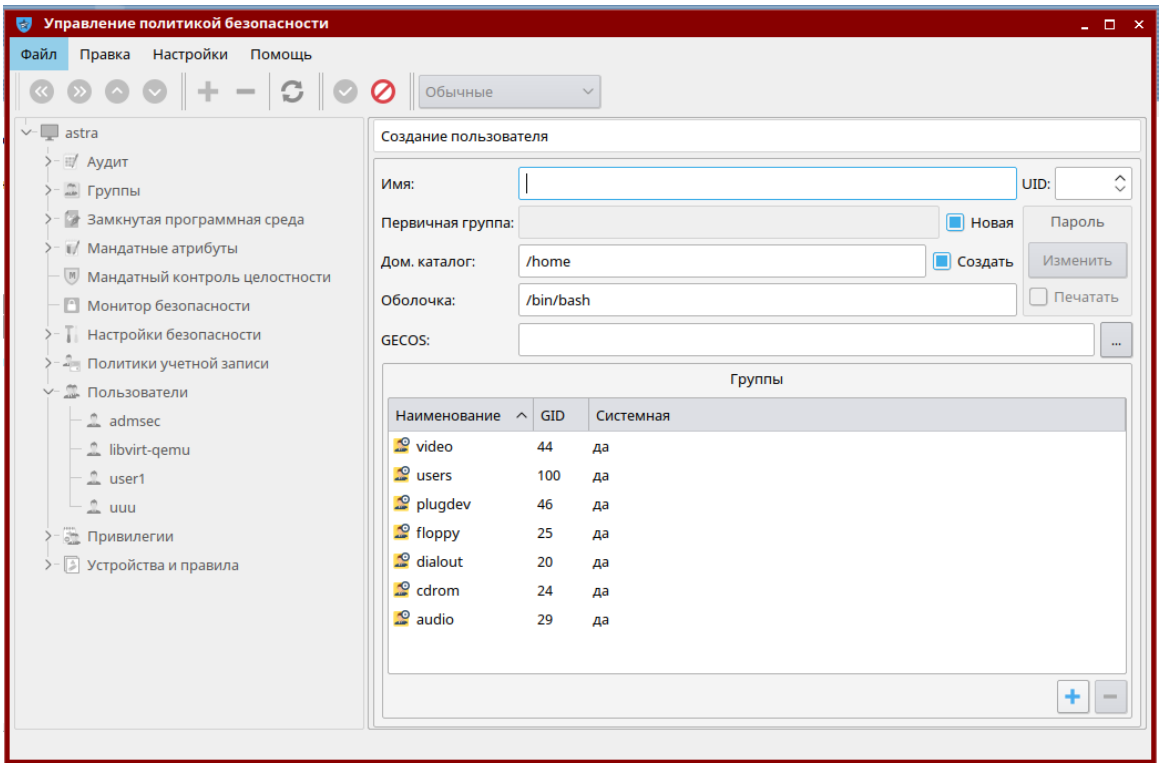


Рисунок 25. Окно создания учетной записи

- нажать кнопку «Применить изменения»;

- в форме «Пароль» нажать кнопку «Изменить» и добавить новый пароль для пользователя;

- выполнить необходимые настройки во вкладках «Блокировка», «Аудит», «МРД», «Срок действия» (рис. 26).

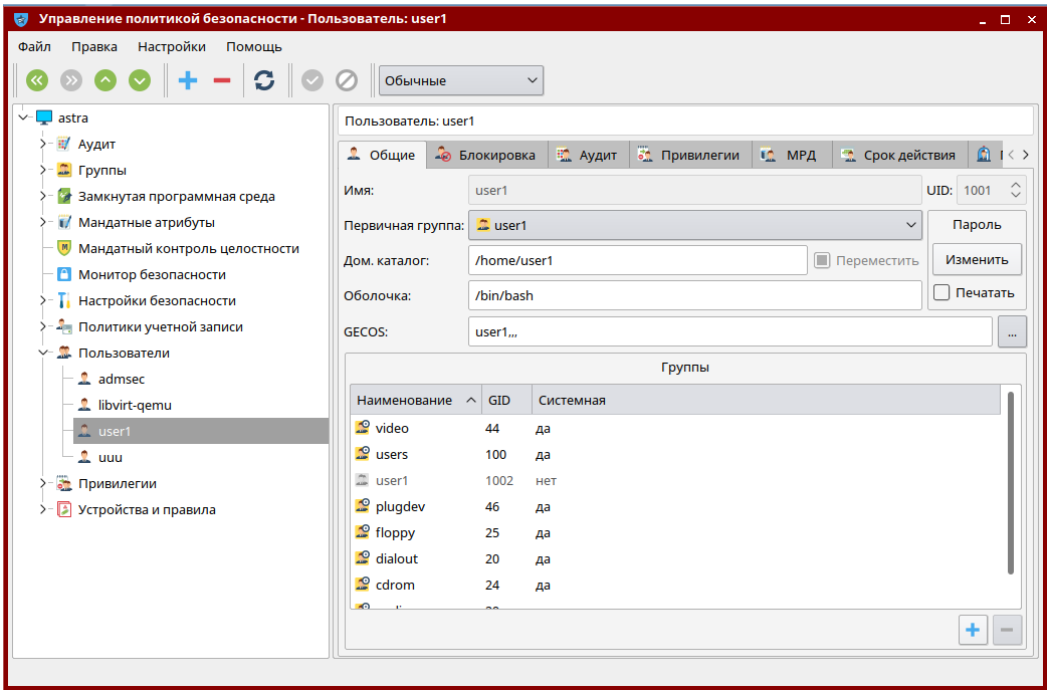


Рисунок 26. Окно настройки учетной записи

Настройка идентификации и аутентификации. Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;
- перейти по вкладке «Политики учетной записи» (рис. 27);

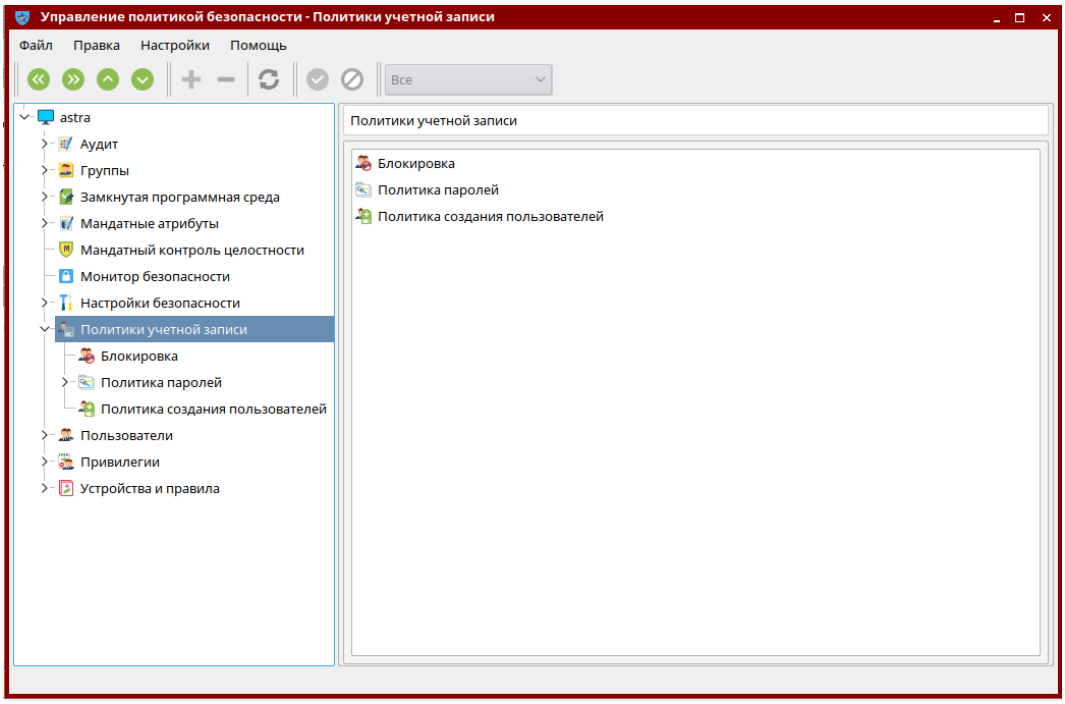
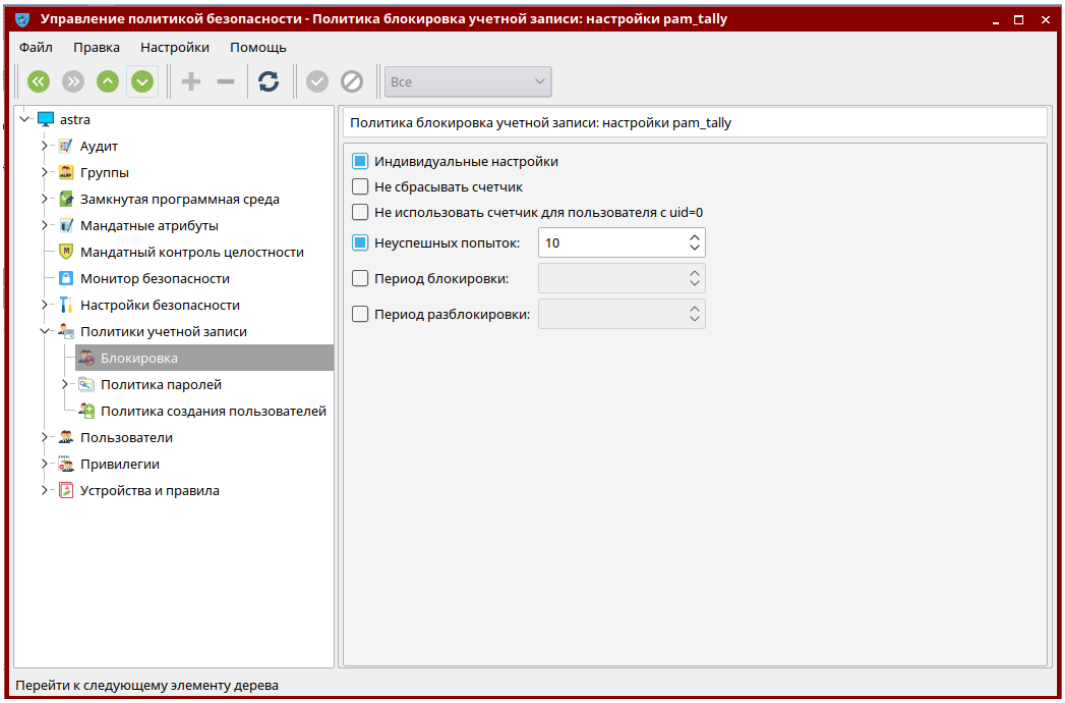


Рисунок 27. Окно настройки политик учетной записи

- выполнить необходимые настройки во вкладках «Блокировка», «Политика паролей» (рис. 28).



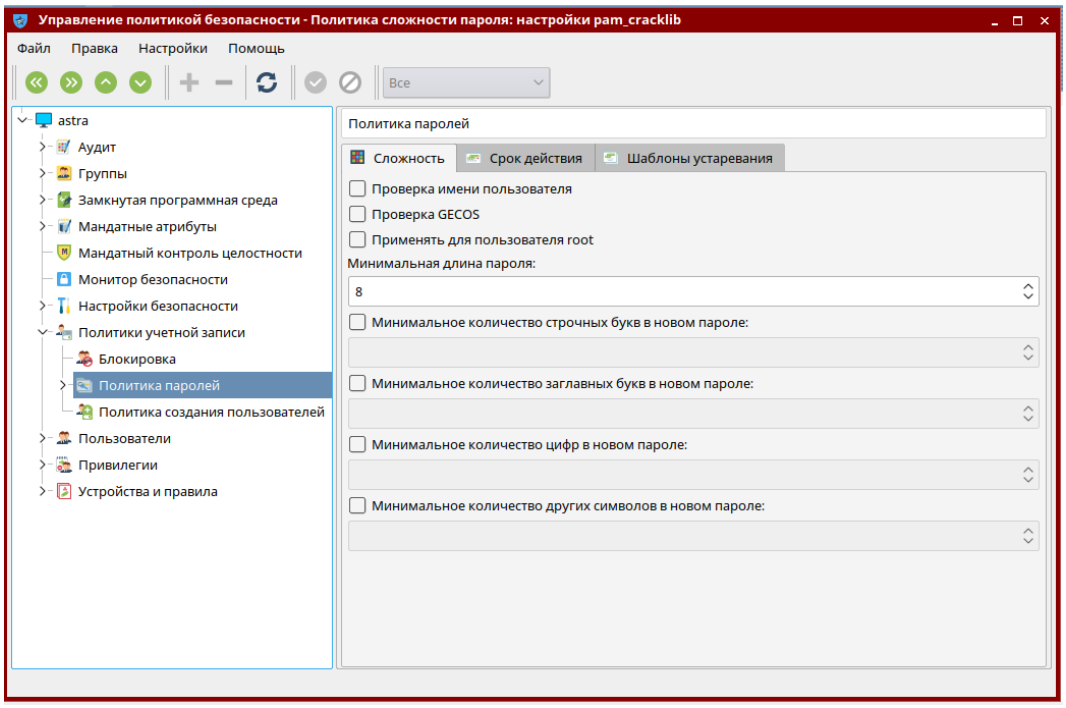


Рисунок 28. Окна настройки блокировки и политики паролей учетных записей

Установка прав разграничения доступа. Необходимо выполнить следующие действия:

- нажать сочетание клавиш «Win+R» и в появившемся окне ввести команду «sudo fly-fm» (рис. 29);

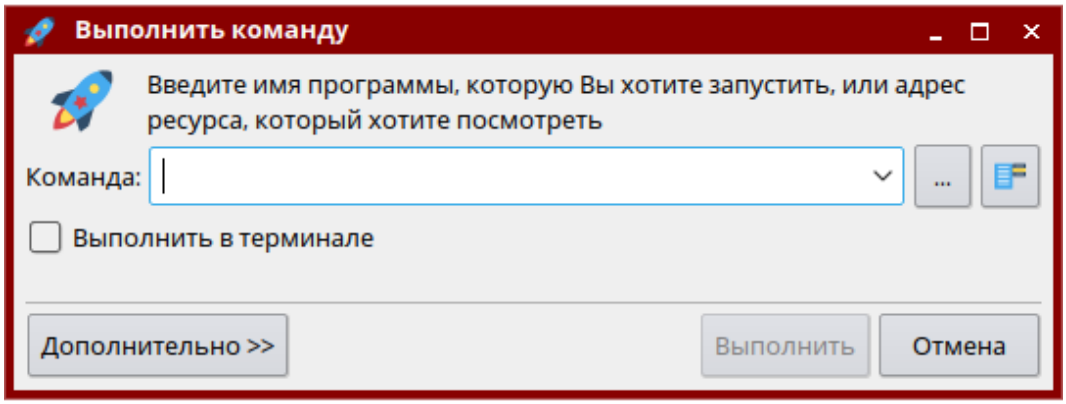


Рисунок 29. Окно выполнения команд

- откроется «Менеджер файлов» (рис. 30);

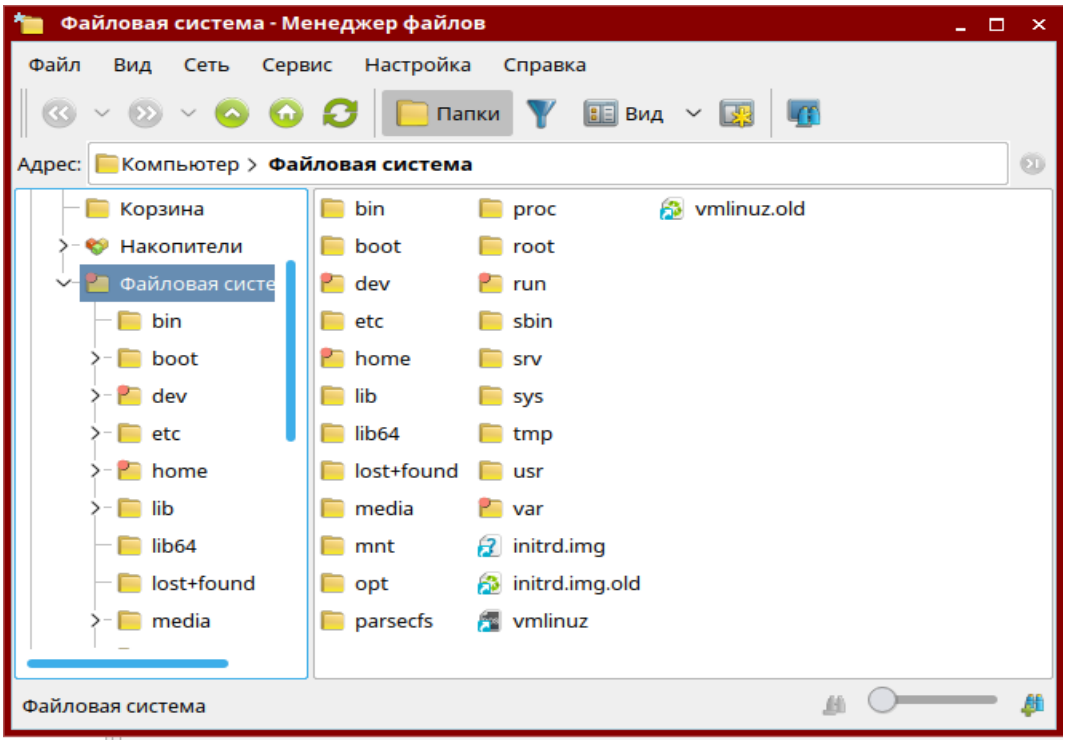


Рисунок 30. Окно менеджера файлов

- на выбранном объекте вызвать контекстное меню и нажать кнопку «Свойства»;

- открыть вкладку «Дискреционные атрибуты» (рис. 31);

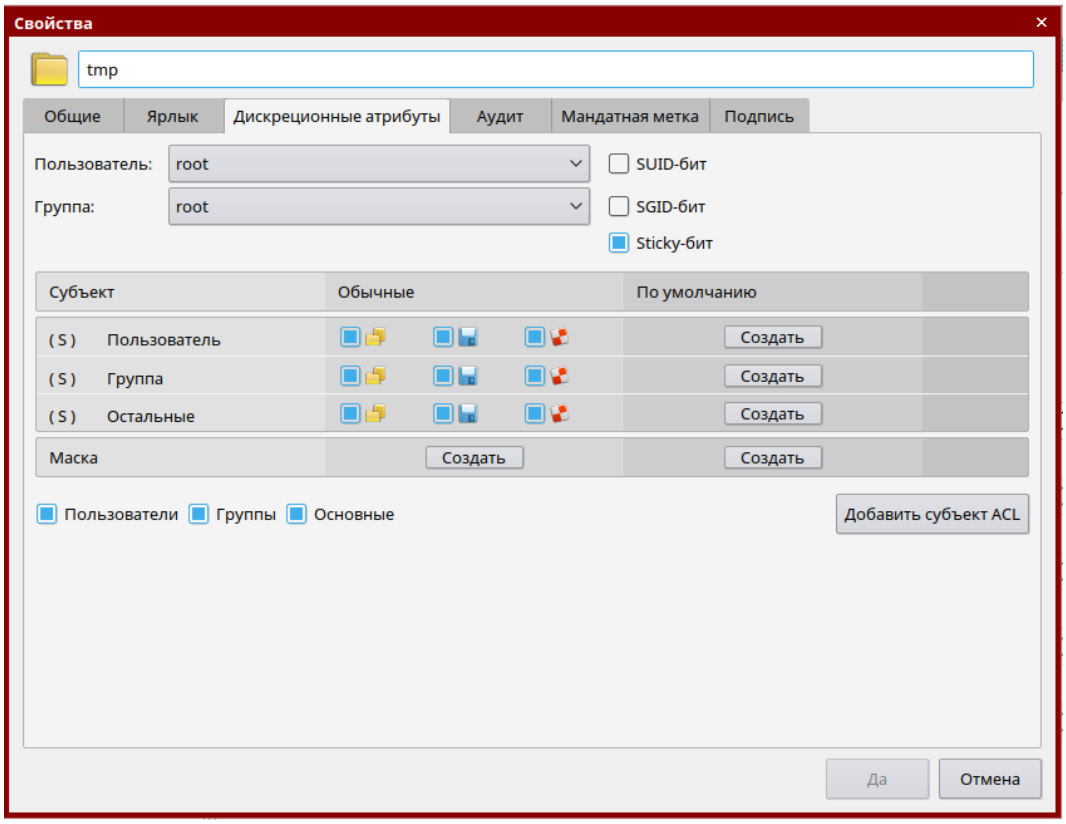


Рисунок 31. Окно настройки дискреционных прав разграничения доступа

- выполнить необходимые настройки разграничения доступа и нажать кнопку «Да».

Настройка очистки остаточной информации. Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;

- перейти по вкладке «Настройки безопасности», «Параметры очистки памяти» (рис. 32);

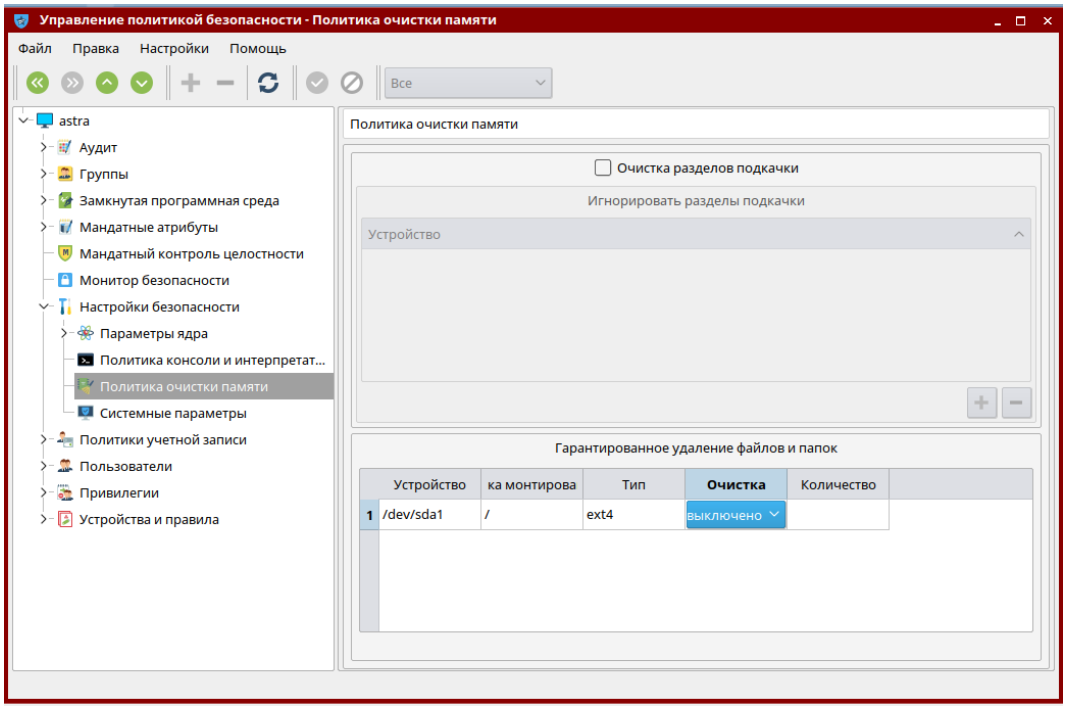


Рисунок 32. Окно настройки политики очистки памяти

- включить «Очистка разделов подкачки»;

- в форме «Гарантированное удаление файлов и папок» для нужного устройства выбрать необходимый тип очистки и количество затираний;

- нажать «Применить изменения».

Настройка регистрации событий. Необходимо выполнить следующие действия:

- настройка регистрации событий пользователя выполнялась при создании пользователей;

- для настройки регистрации событий по отношению к объектам доступа нажать сочетание клавиш «Win+R» и в появившемся окне ввести команду «sudo fly-fm» (рис. 33);

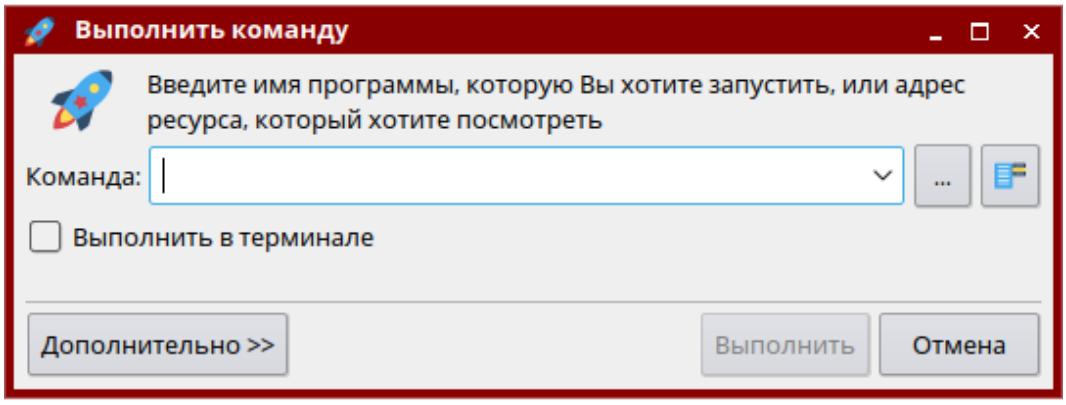


Рисунок 33. Окно выполнения команд

- откроется «Менеджер файлов» (рис. 34);

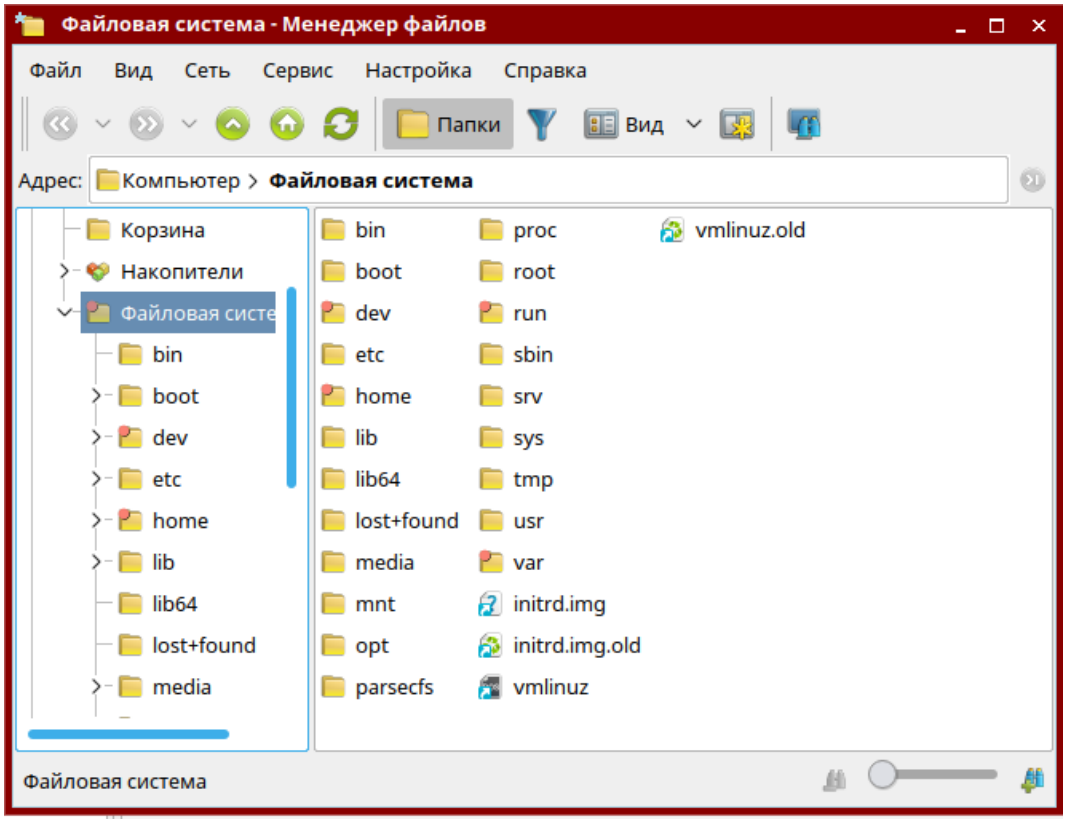


Рисунок 34. Окно менеджера файлов

- на выбранном объекте вызвать контекстное меню и нажать кнопку «Свойства»;

- открыть вкладку «Аудит» и нажать кнопку «Добавить элемент аудита» (рис. 35);

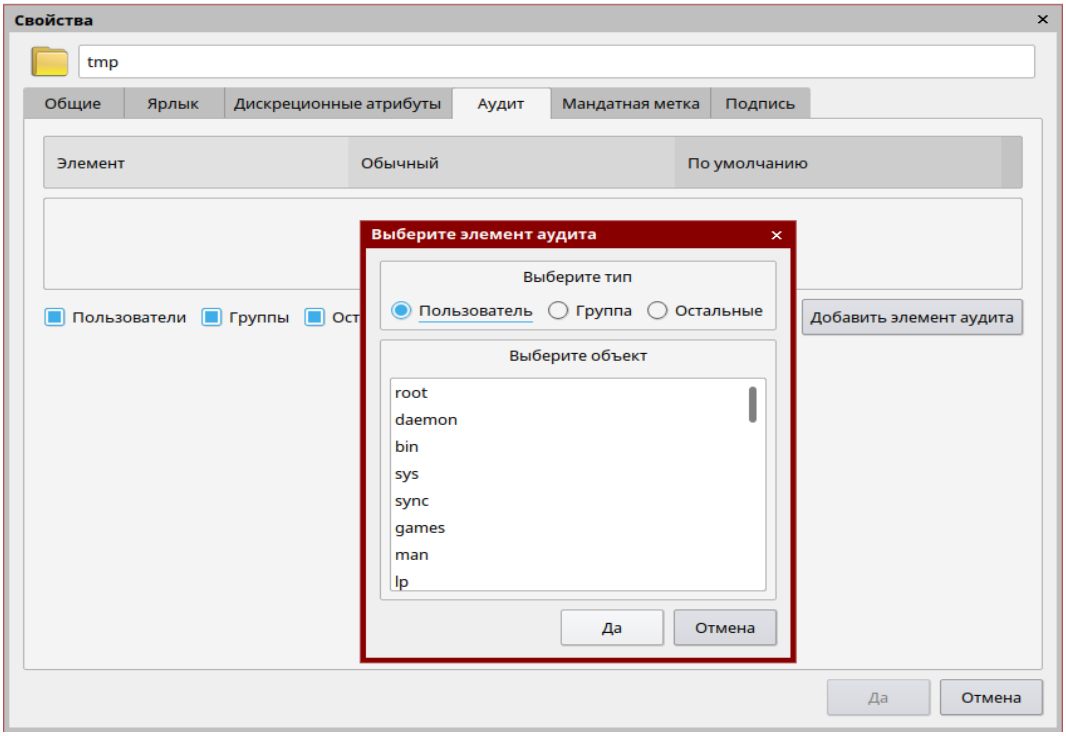


Рисунок 35. Окно выбора элемента аудита

- выбрать необходимых субъектов доступа, по отношению к которым настраивается аудит;

- добавить необходимые события аудита для выбранных субъектов доступа и нажать кнопку «Да» (рис. 36).

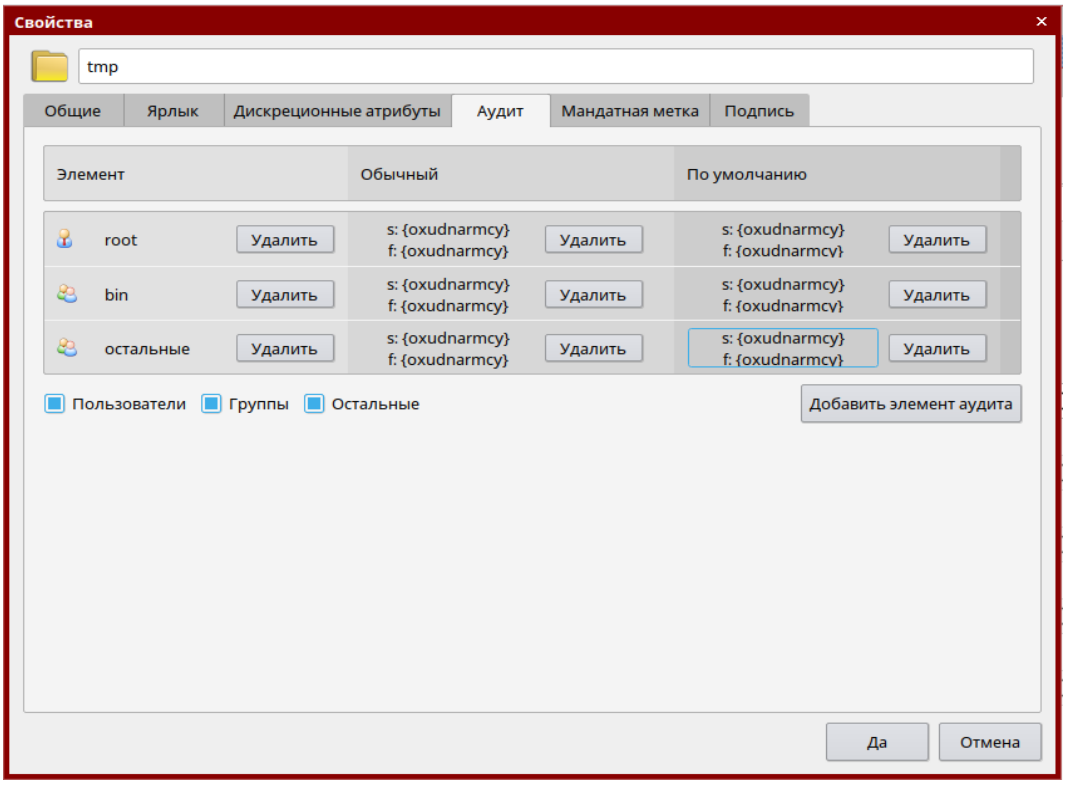


Рисунок 36. Окно настройки аудита

Настройка контроля целостности файловой системы и программно-аппаратной среды. Необходимо выполнить следующие действия:

- Изменить в файле «/etc/cron.daily/afick_cron» параметры:

```
LOGFILE="/dev/null"
ERRORLOG="/dev/null"
nice -n $NICE $AFICK -c $CONFFILE -k > $LOGFILE 2>$ERRORLOG
```

- Изменить в файле «/etc/afick.conf» параметры:

```
history := /var/log/afick/afick.log
#archive := /var/lib/afick/archive
/boot md5
/lib/modules md5
/etc/security md5
/etc/pam.d md5
/lib/x86_64-linux-gnu/security md5
/lib/security md5
/sbin md5
/etc/fstab md5
/usr/sbin md5
```

- в «Терминал Fly» выполнить следующие команды:

```
sudo touch /etc/init.d/afick.sh
sudo chmod 755 /etc/init.d/afick.sh
```

- в файл «/etc/init.d/afick.sh» необходимо вписать:

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          afick
# Required-Start:    $local_fs
# Required-Stop:     $local_fs
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Контроль целостности при старте системы
# Description:       Контроль целостности при старте системы
### END INIT INFO

PATH=/sbin:/bin:/usr/sbin:/usr/bin
. /lib/lsb/init-functions

case $1 in
   start)
   log_daemon_msg "Starting integrity check" "afick"
   log_end_msg 0
   /usr/bin/afick -c /etc/afick.conf -k 2>&1 > /dev/null
   status=$?
   log_daemon_msg "Integrity check results" "afick"
   log_end_msg $status
   if [ $status -ne "0" ];
   then
```

```
    sleep 2
    fi
    ;;

    *)
    echo "Для использования данного скрипта необходимо запустить его с параметром start. Например: afick.sh start"
    ;;
esac
```

- в «Терминал Fly» выполнить следующие команды:

```
sudo afick -i
sudo update-rc.d afick.sh defaults
```

Настройка прав разграничения доступа для внешних носителей информации. Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;
- перейти по вкладке «Устройства и правила», «Устройства» (рис. 37);

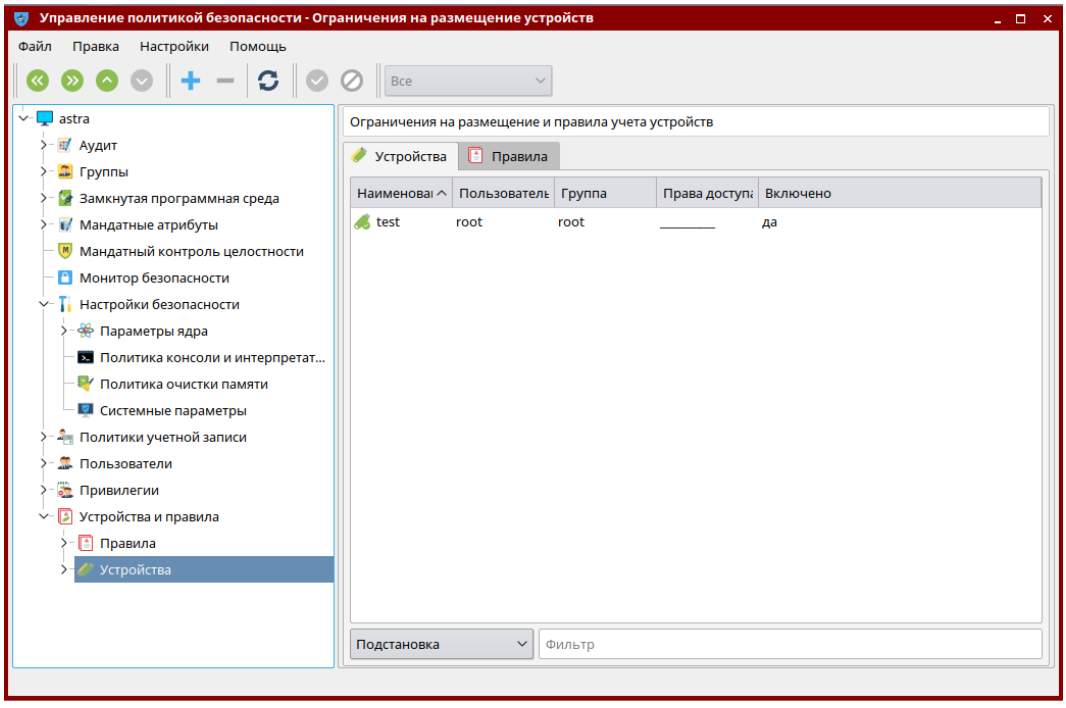


Рисунок 37. Окно зарегистрированных устройств

- вставить носитель информации;
- нажать «Создать новый элемент»;
- выбрать необходимый носитель;
- выполнить все необходимые настройки разграничения доступа к устройству и включить разграничение (рис. 38);

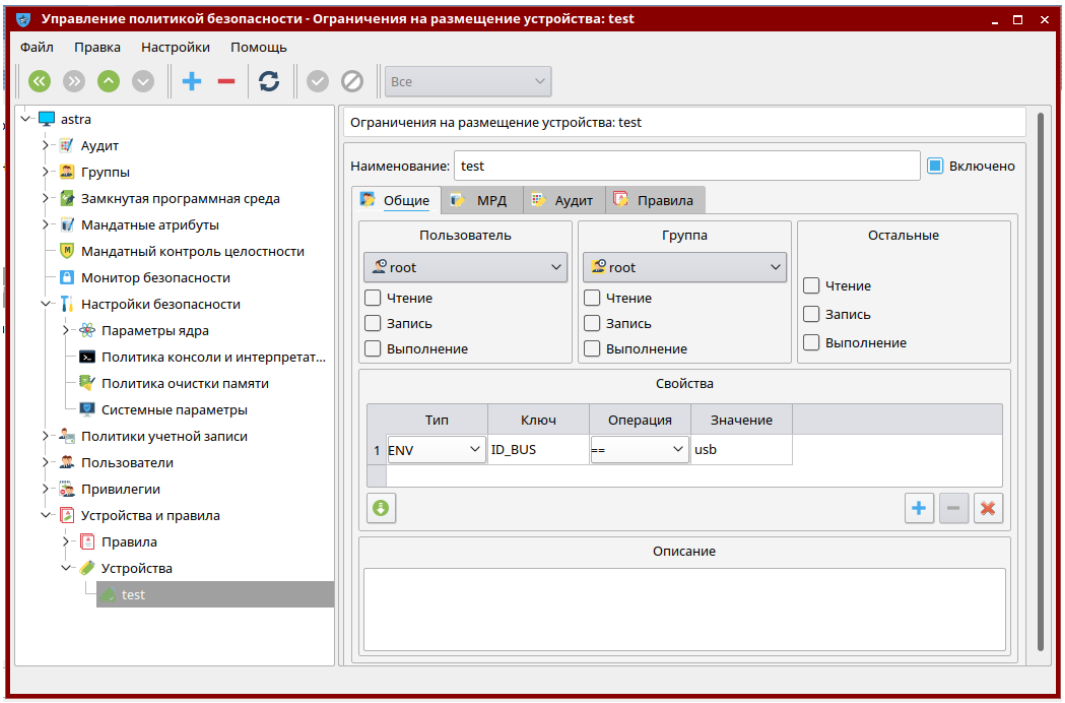


Рисунок 38. Окно настройки разграничения прав доступа к устройству

- нажать «Применить изменения».

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).

1. 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 «ОК» (рис. 39);

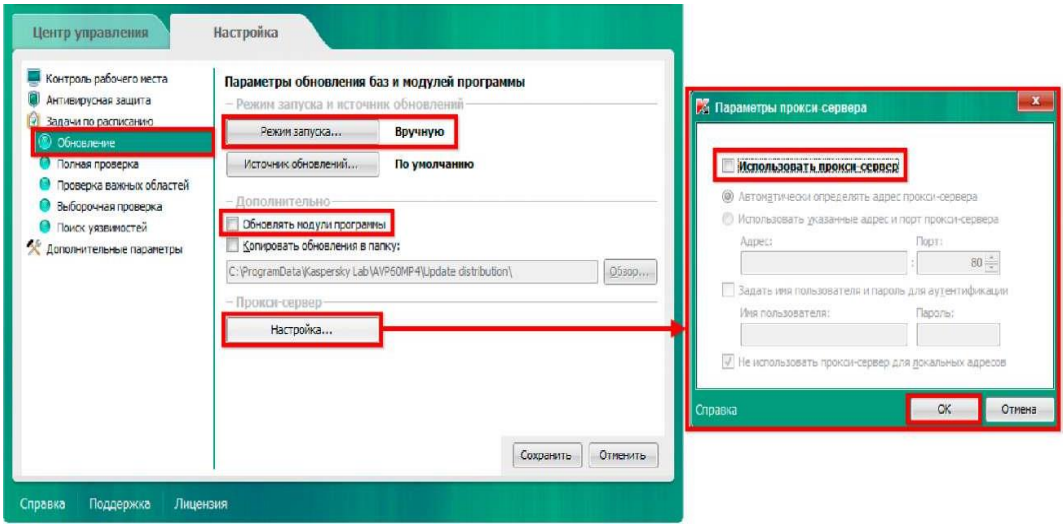


Рисунок 39. Настройка параметров обновления БВС для автономного рабочего мест АИС, не имеющего подключения к Интернет

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

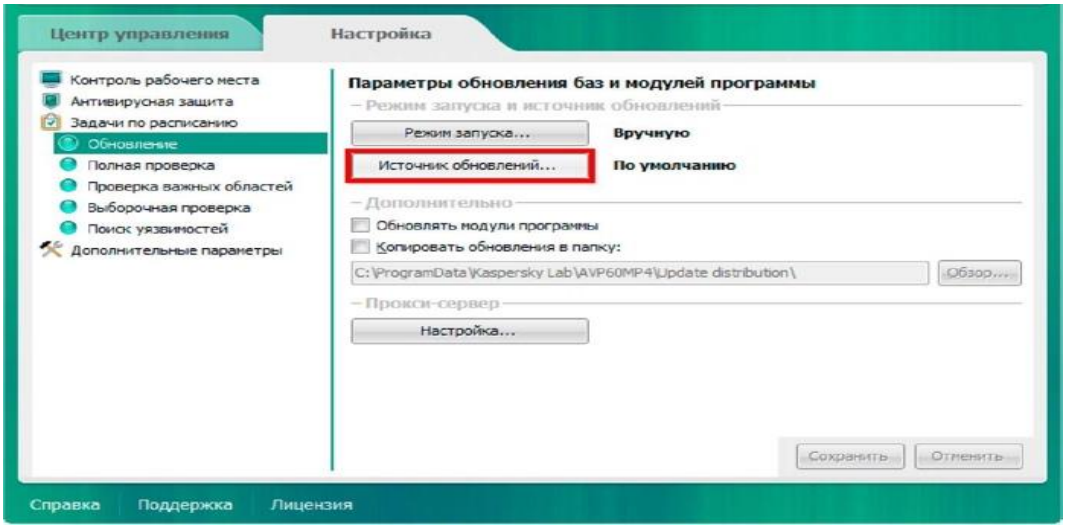


Рисунок 40. Настройка источника обновлений

- 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 «ОК». Далее в окне «Обновление» нажать кнопку «ОК» (рис. 41);

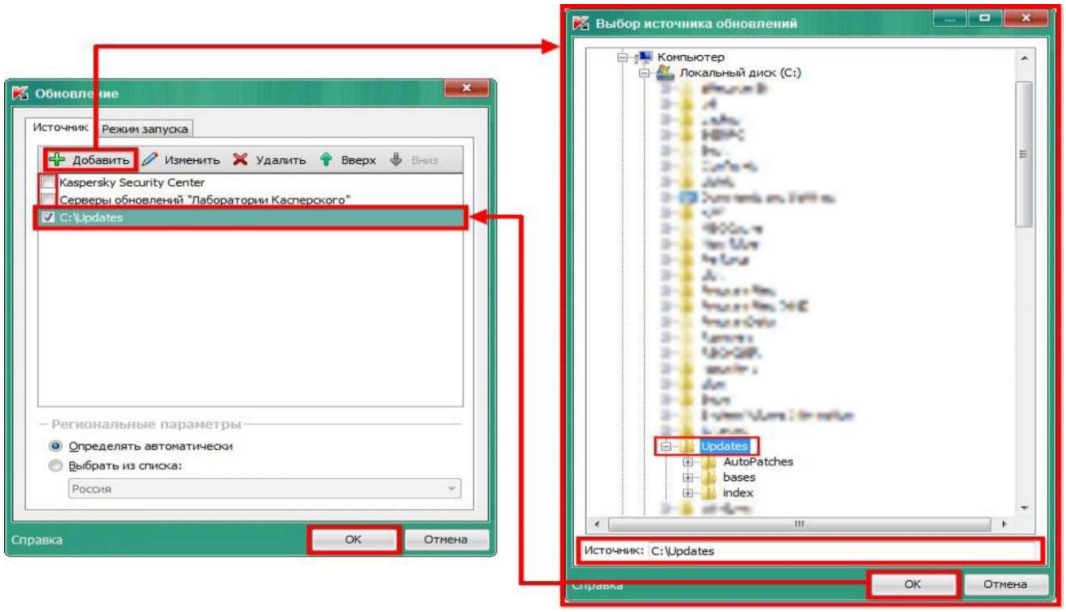


Рисунок 41. Указание источника обновлений

- 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).

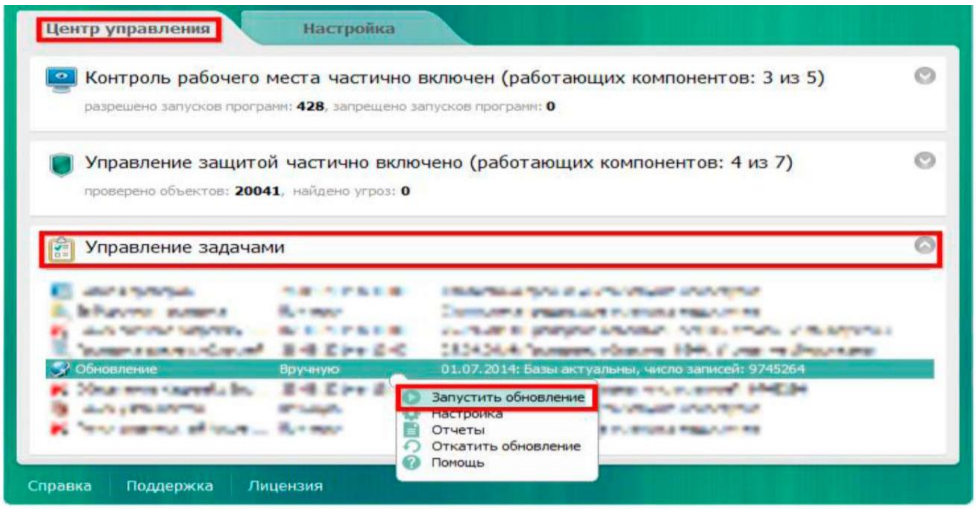


Рис. 42 Запуск обновлений

2. 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 «ОК» (рис. 43).

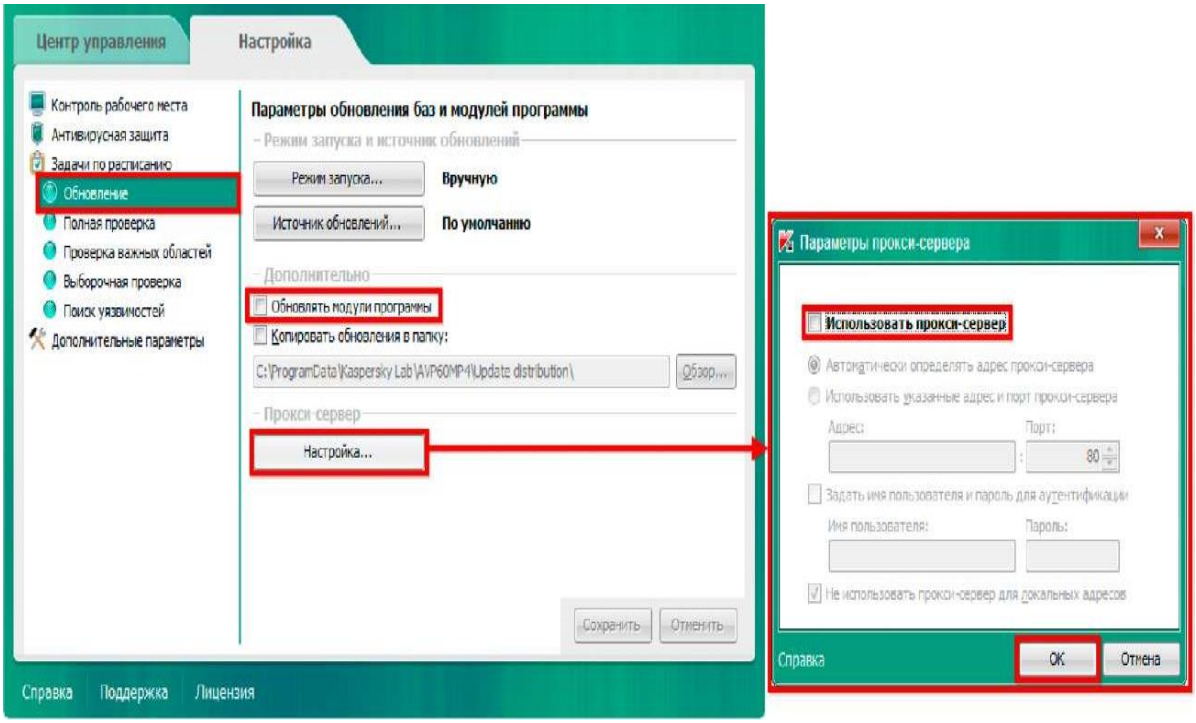


Рисунок 43. Настройка параметров обновления БВС для АИС, имеющего подключение к Интернет

- 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 «ОК» (рис. 44).

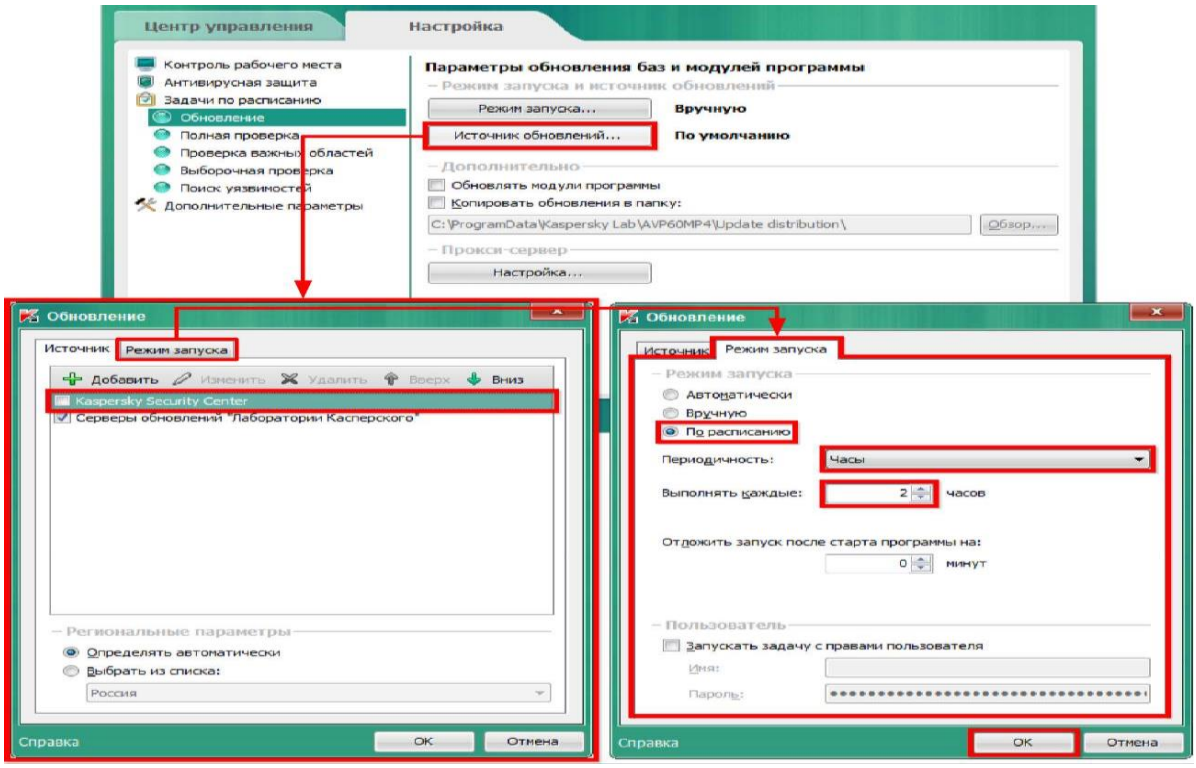


Рисунок 44. Настройка источника и режима запуска задачи обновления БВС

Настройка файлового антивируса. Необходимо выполнить следующие действия:

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

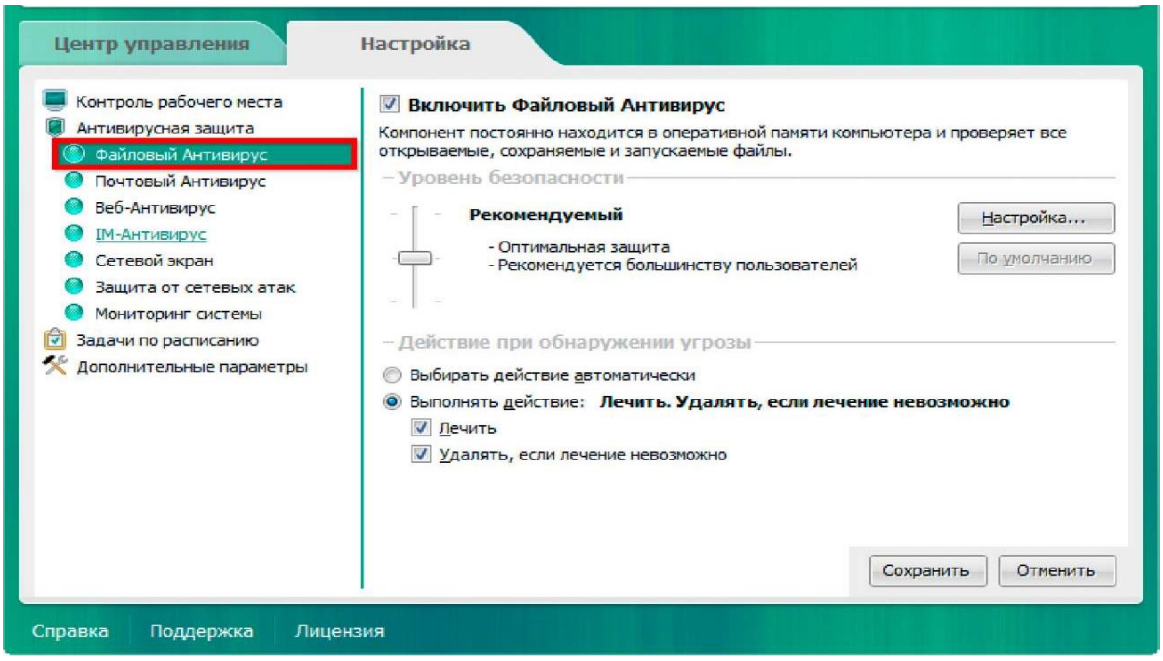


Рисунок 45. Окно настроек файлового антивируса

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

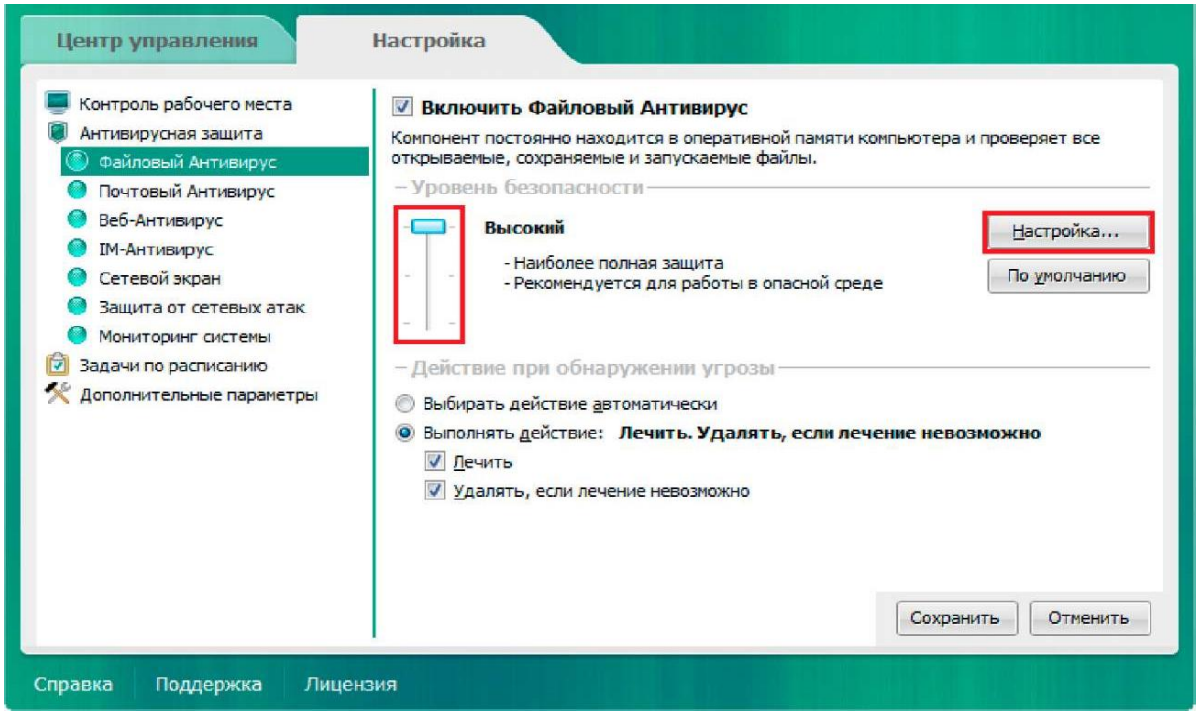


Рисунок 46. Общие параметры файлового антивируса

- 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 «ОК» (рис. 47).

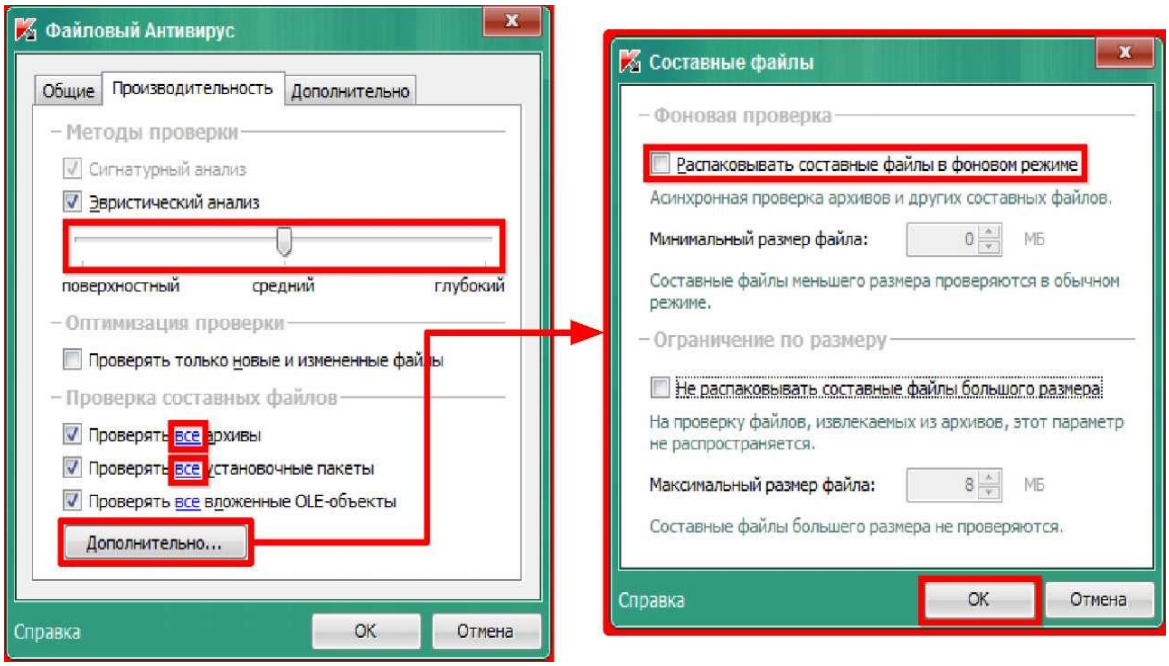


Рисунок 47. Изменение производительности файлового антивируса и настройка проверки составных файлов

- в окне «Файловый Антивирус» нажать кнопку «ОК», 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);

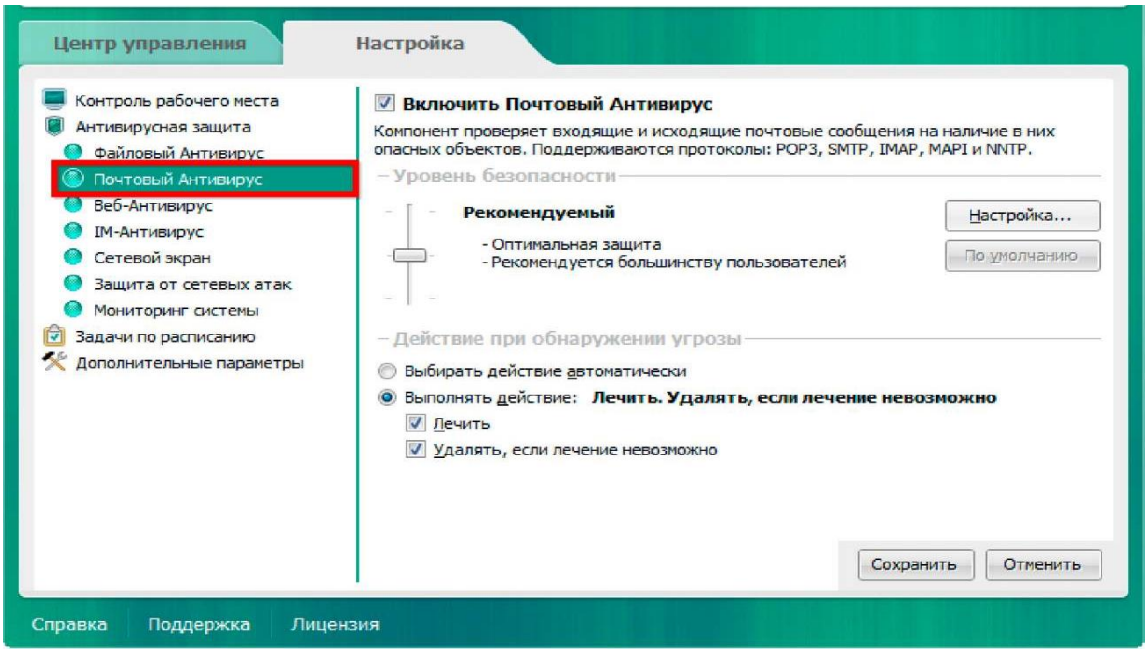


Рисунок 48. Окно настроек почтового антивируса

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

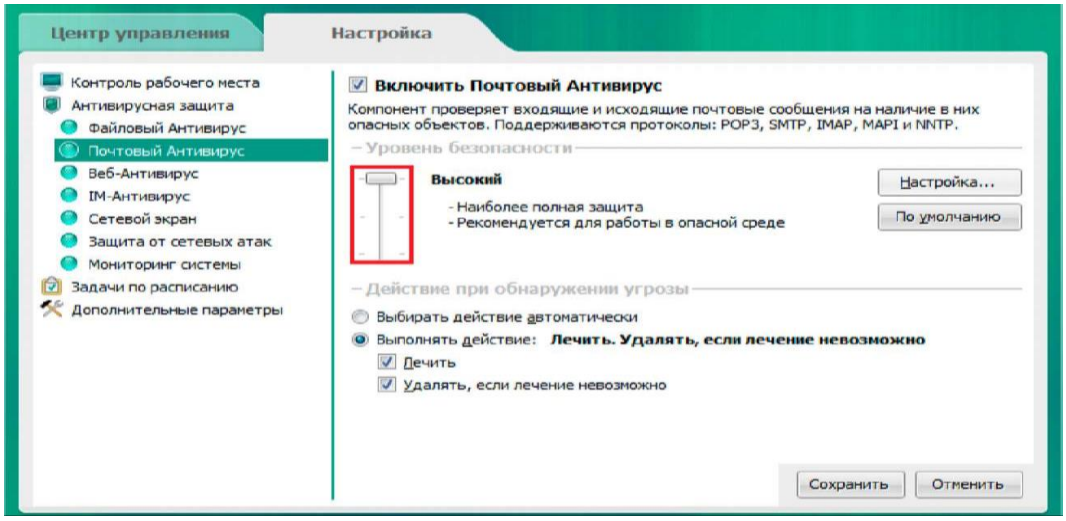


Рисунок 49. Изменение параметров уровня безопасности почтового антивируса

- 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;

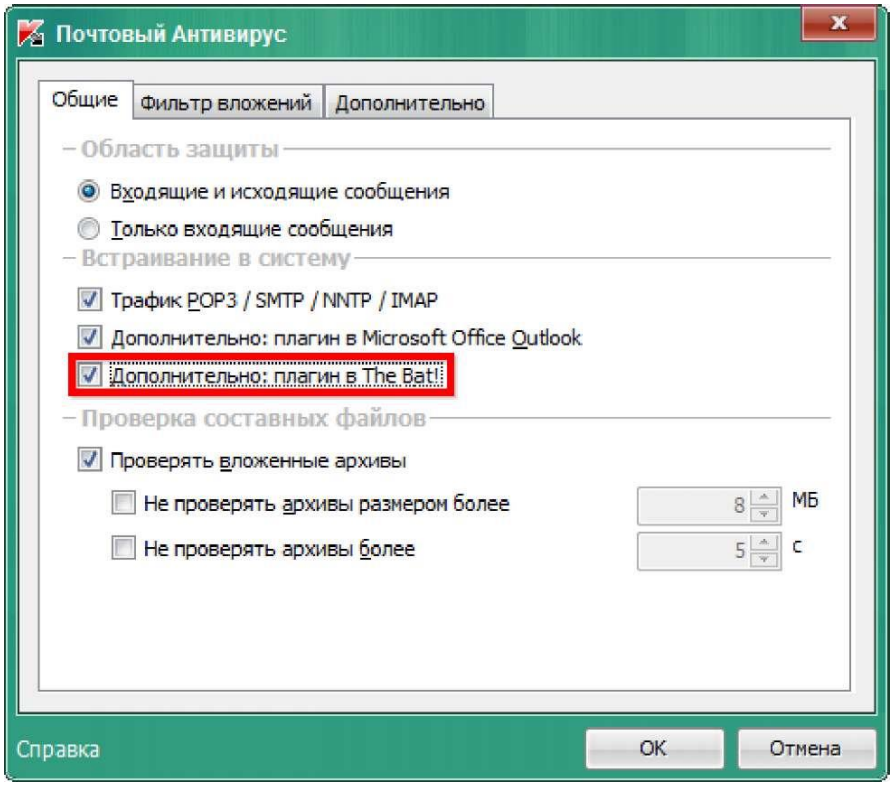


Рисунок 50. Общие настройки почтового антивируса

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

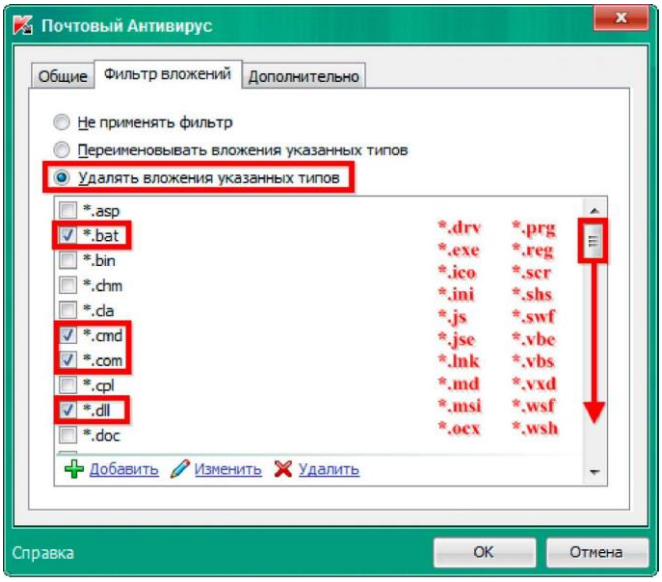


Рисунок 51. Изменение параметров фильтра вложений

- 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.

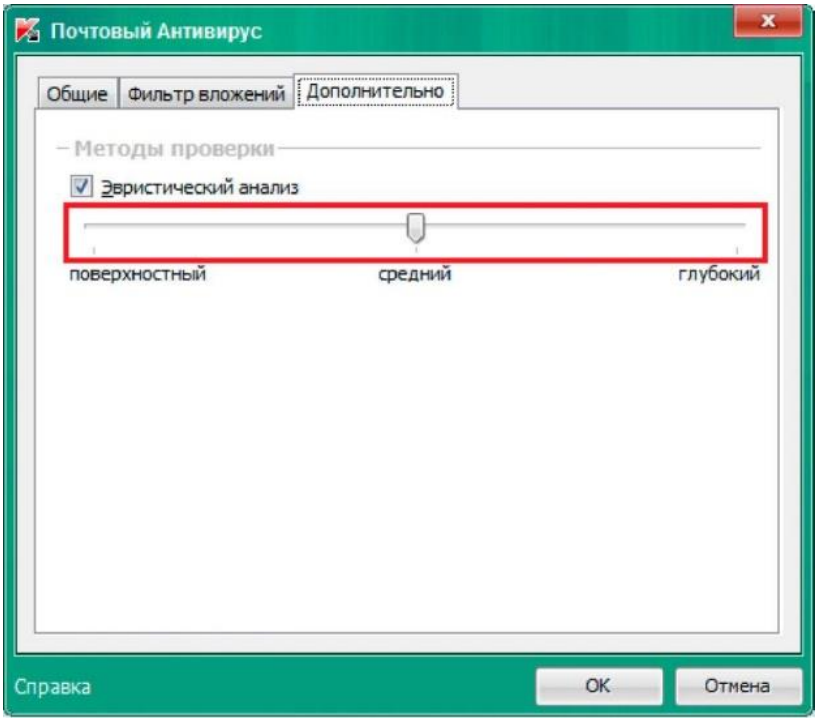


Рисунок 52. Изменение параметров методов проверки

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);

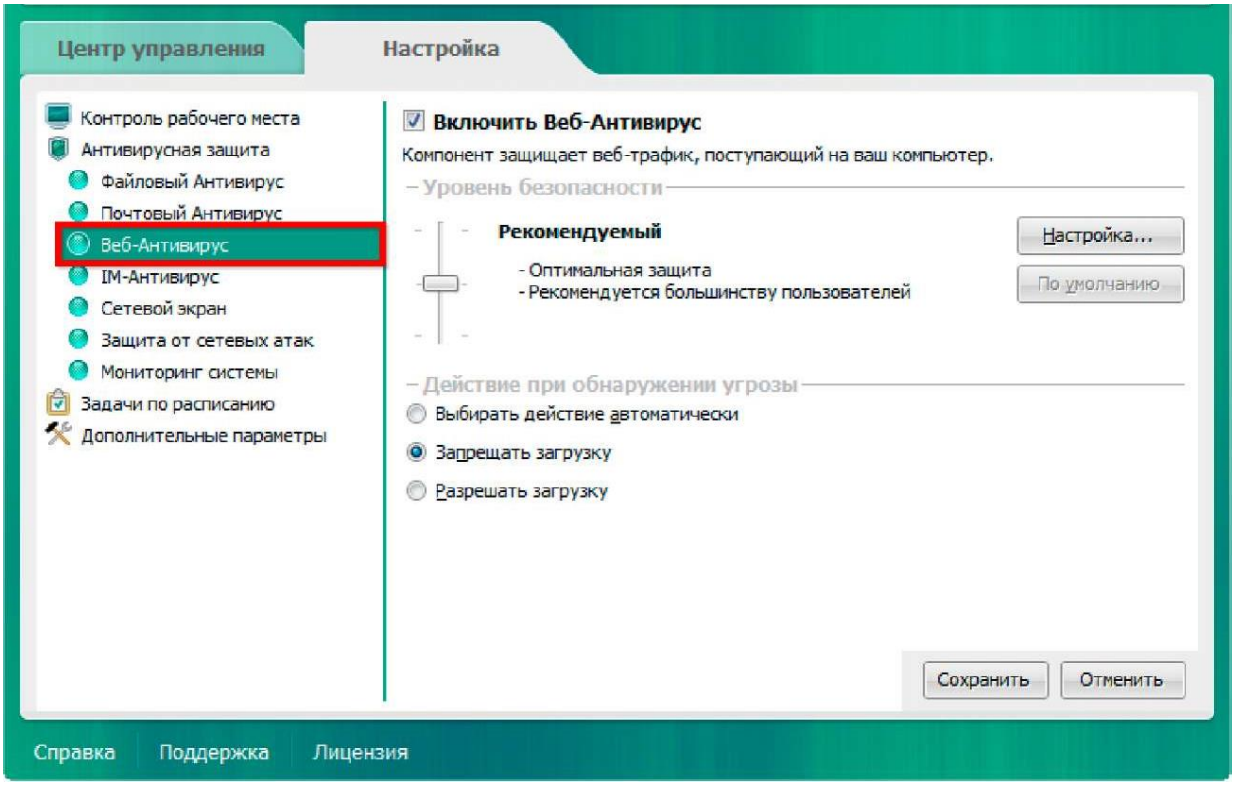


Рисунок 53. Окно настроек веб-антивируса

- 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).

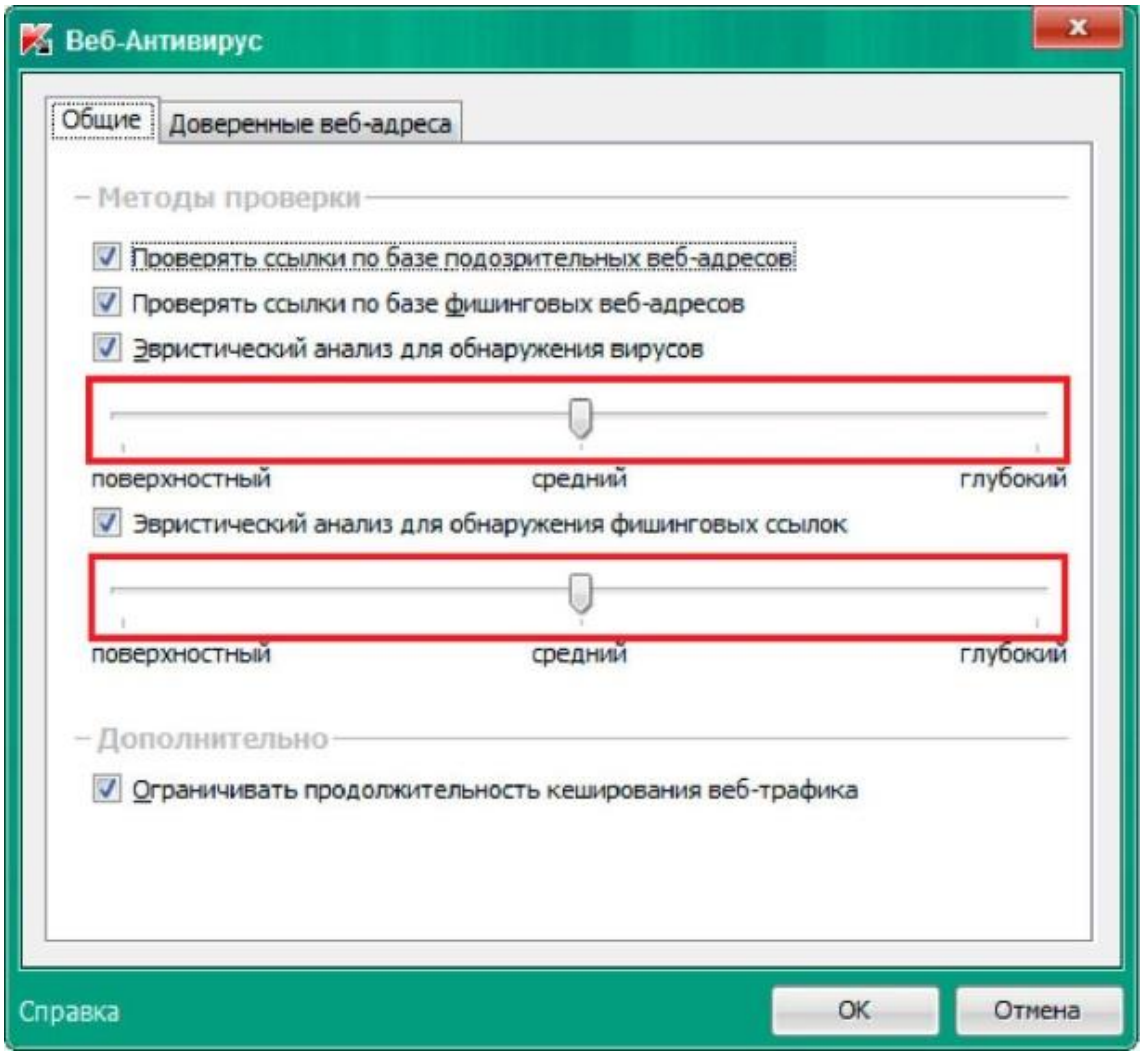


Рисунок 54. Изменение параметров настройки Веб-Антивируса.

- 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);

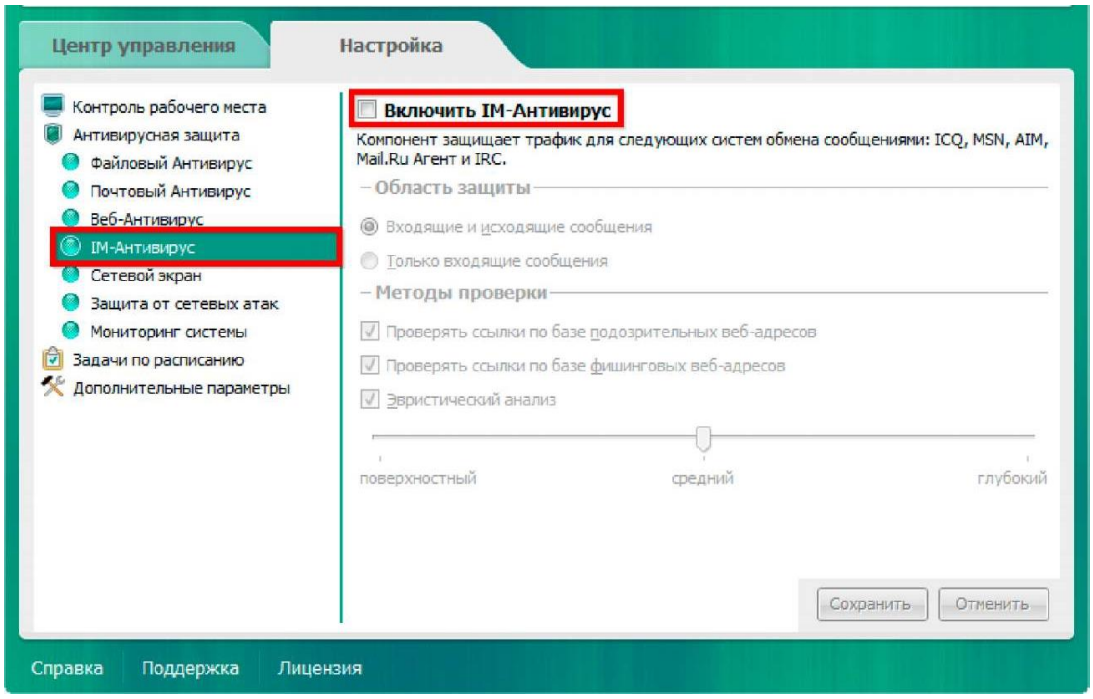


Рисунок 55. Окно настроек IM-антивируса

- 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);

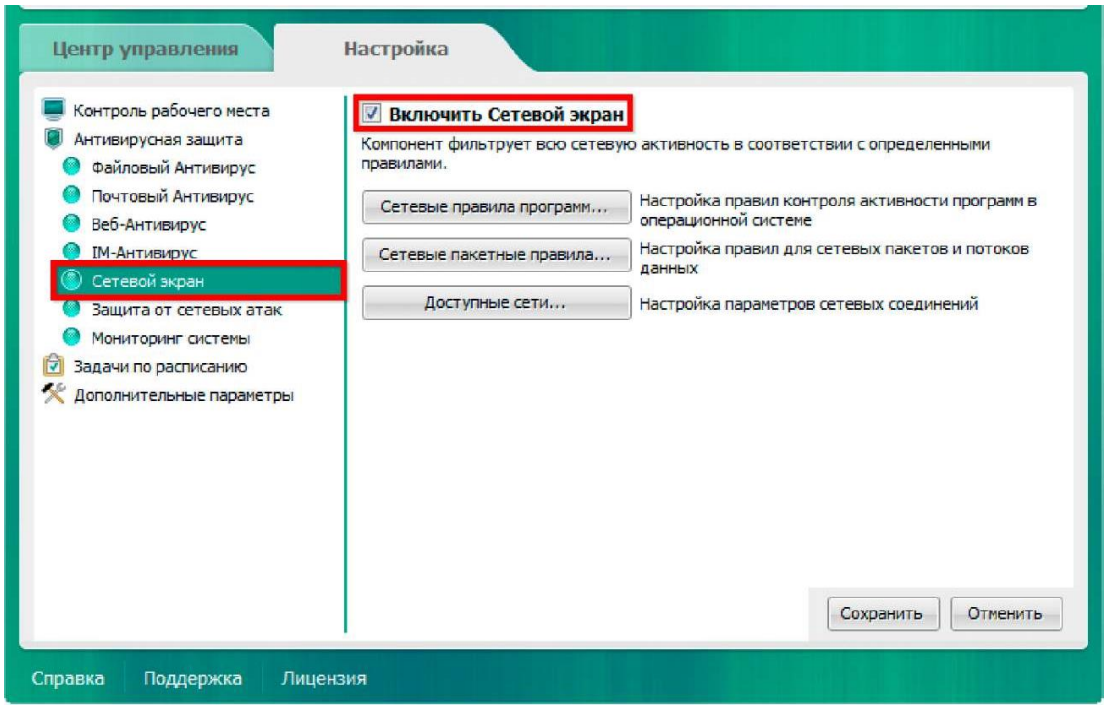


Рисунок 56. Окно настроек сетевого экрана

- 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.

1. 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);

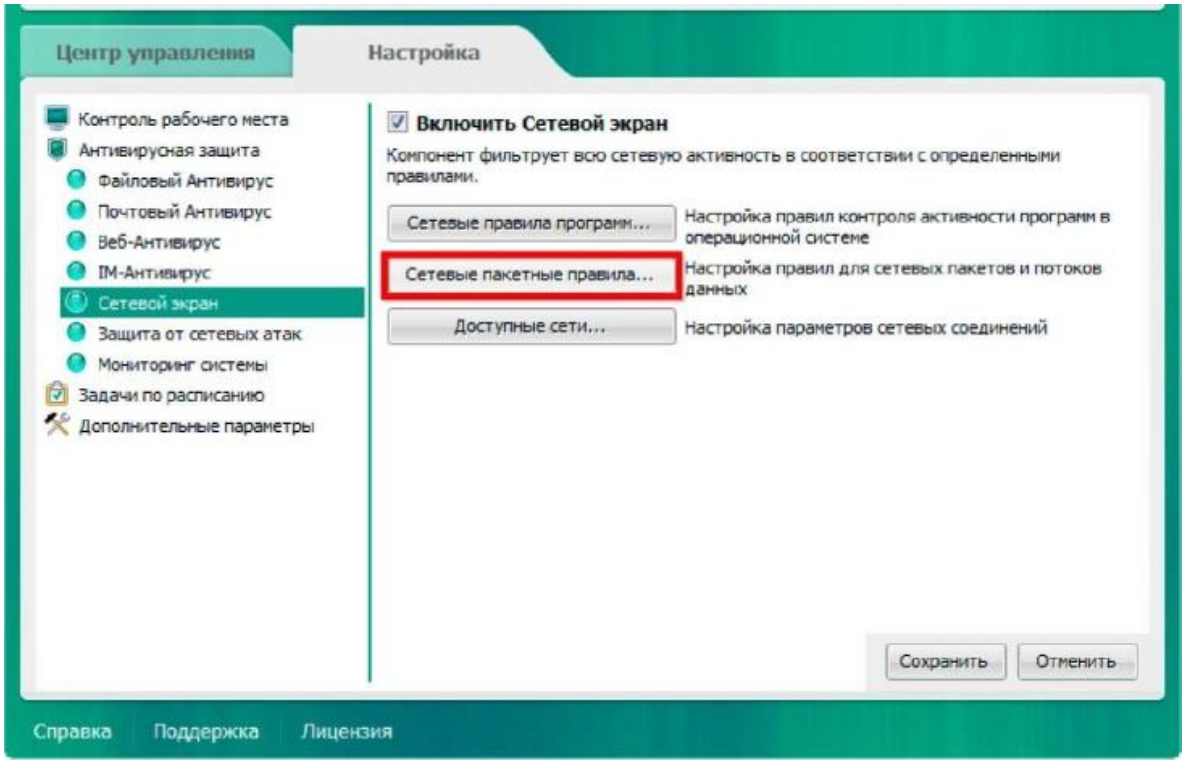


Рисунок 57. Выбор сетевых пакетных правил

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

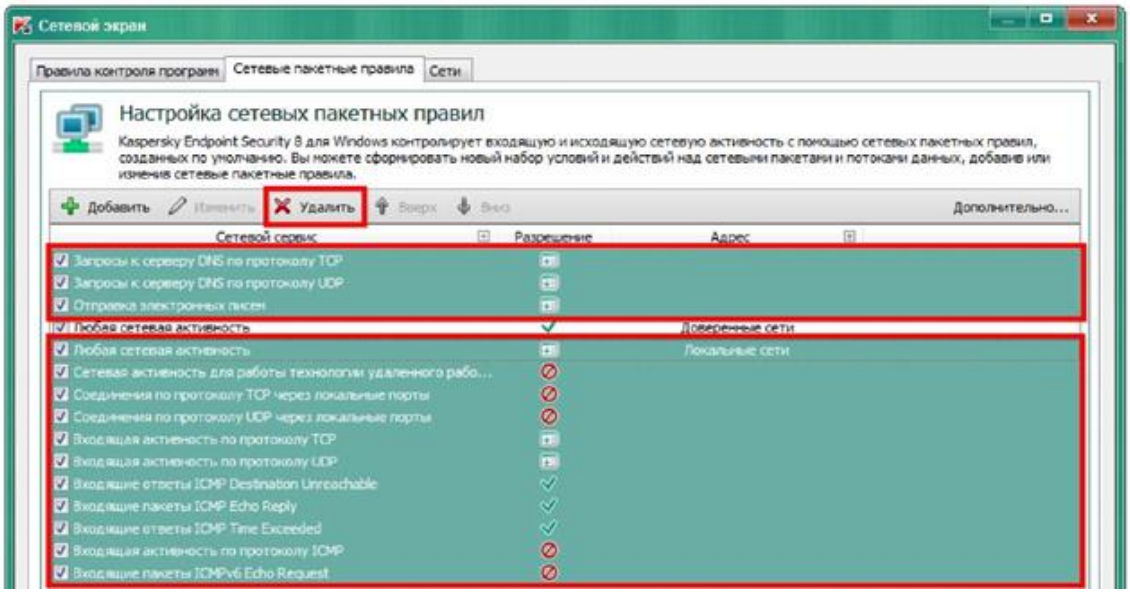


Рисунок 58. Пакетные правила

- 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);

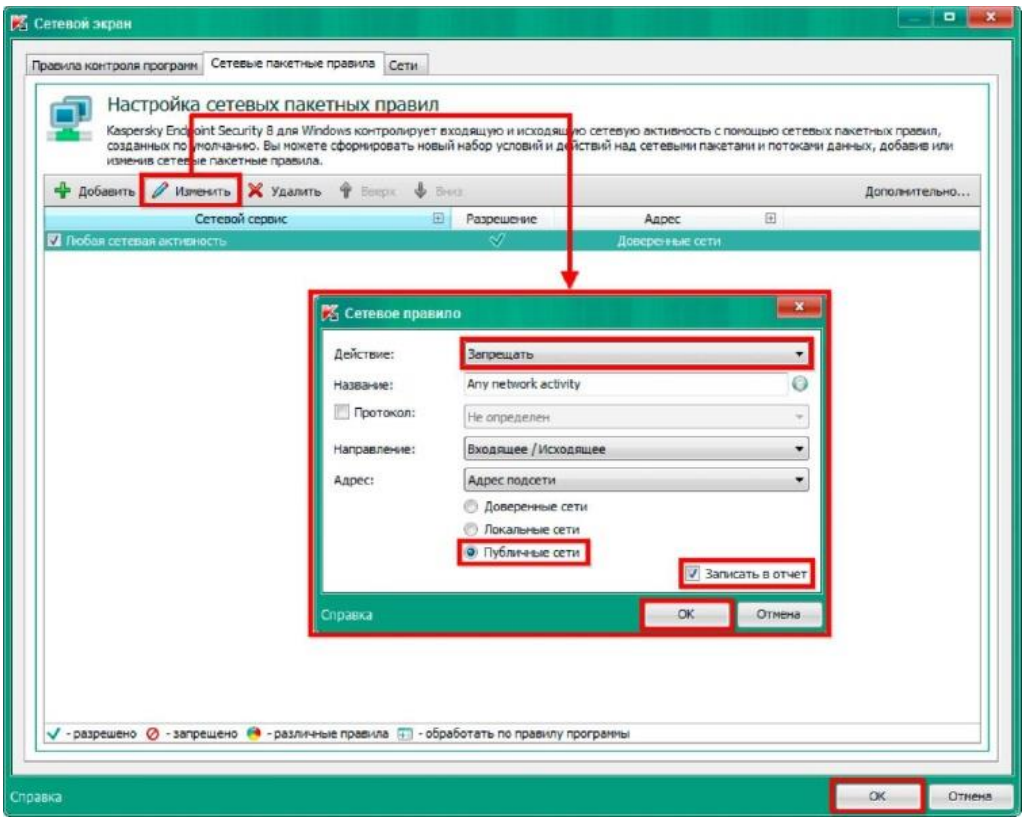


Рисунок 59. Настройки сетевого экрана для автономной ЭВМ

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

2. 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).

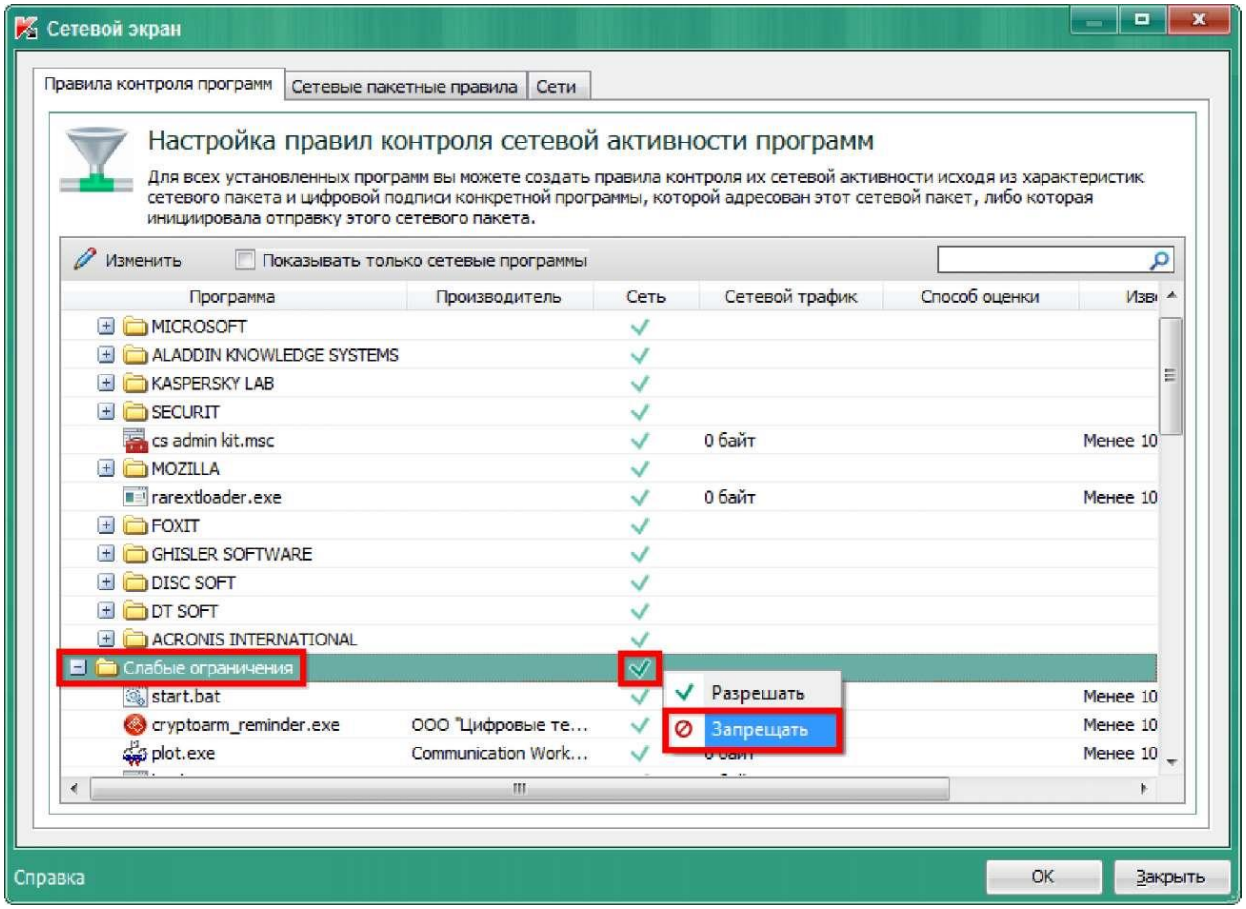


Рисунок 60. Настройка прав доступа к сети группы «Слабые ограничения»

- 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).

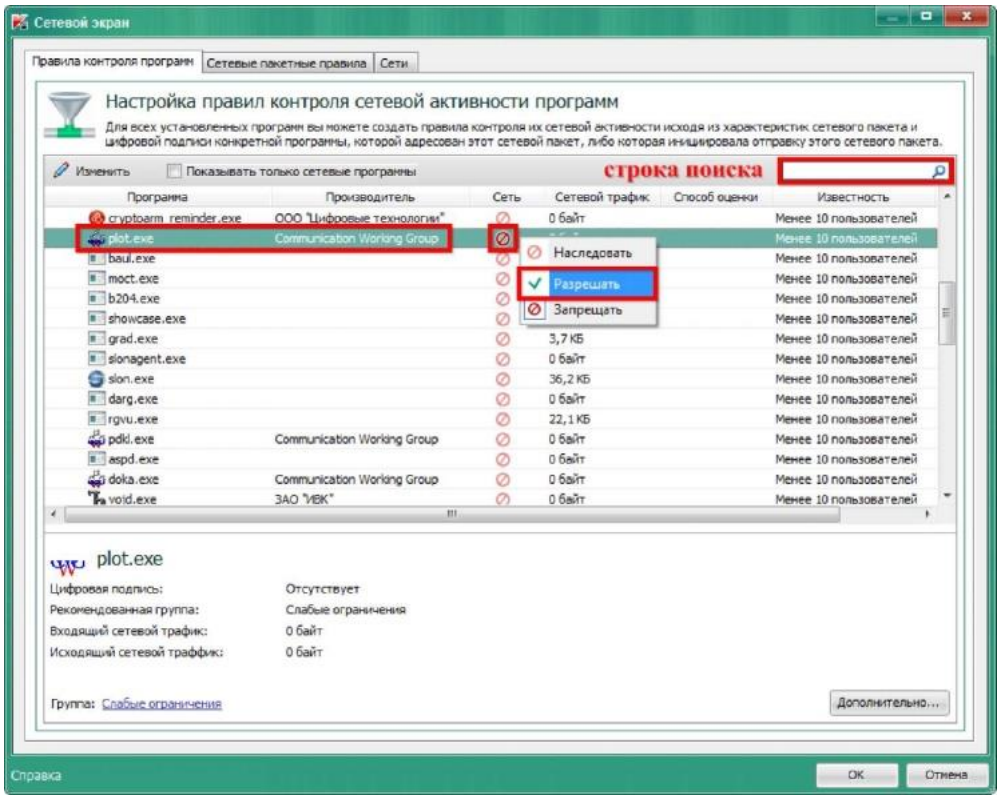


Рисунок 61. Предоставление программе доступ к сети

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

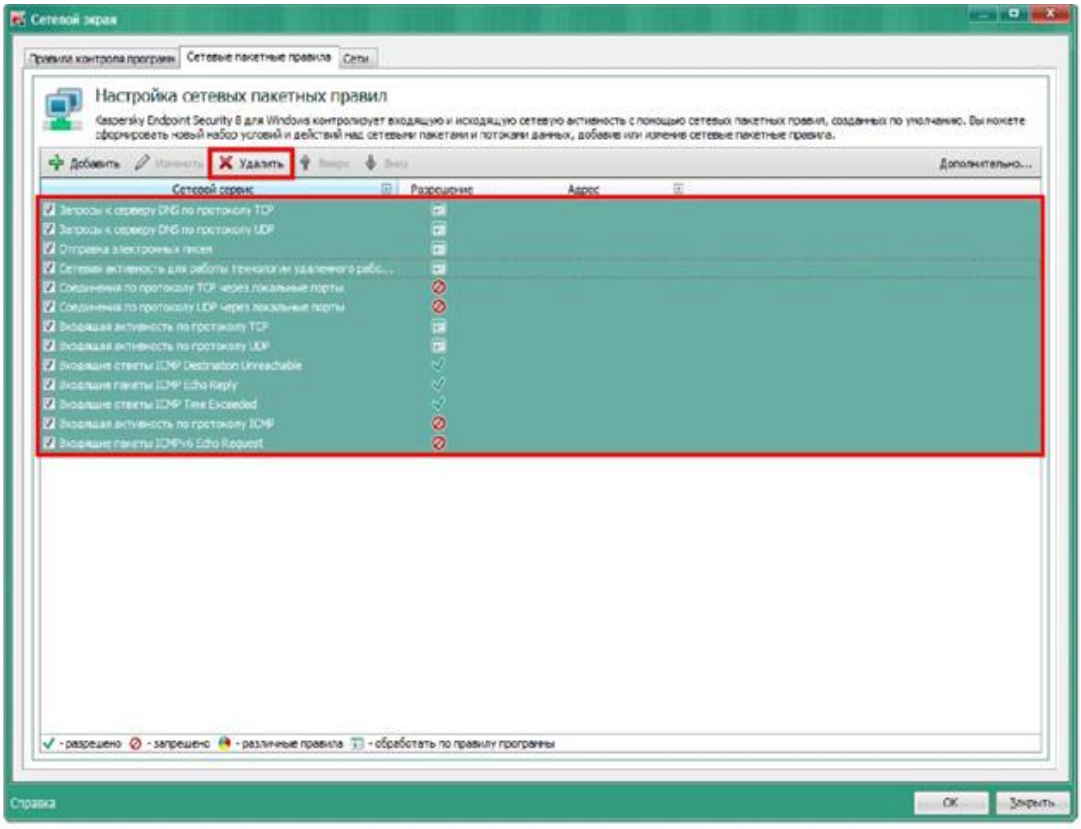


Рисунок 62. Удаление всех сетевых пакетных правил

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);

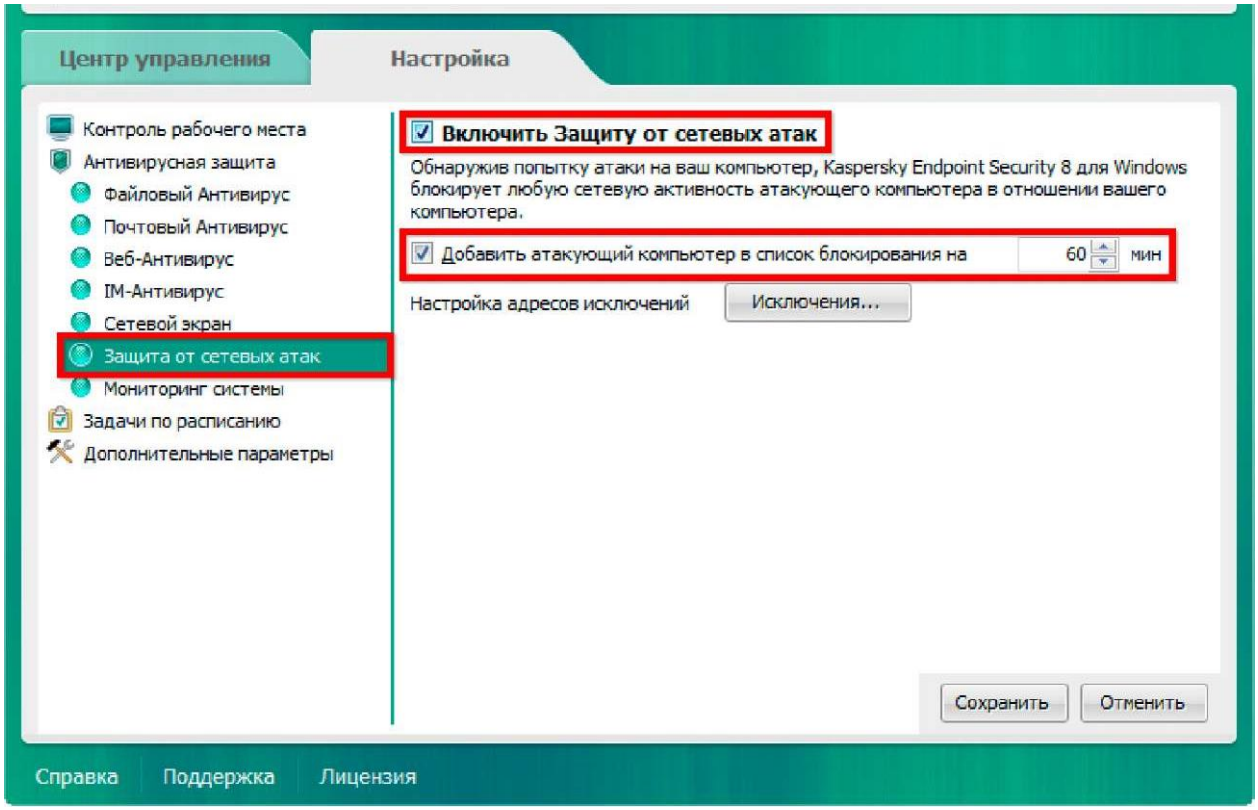


Рисунок 63. Окно настроек компонента защиты от сетевых атак

- 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);

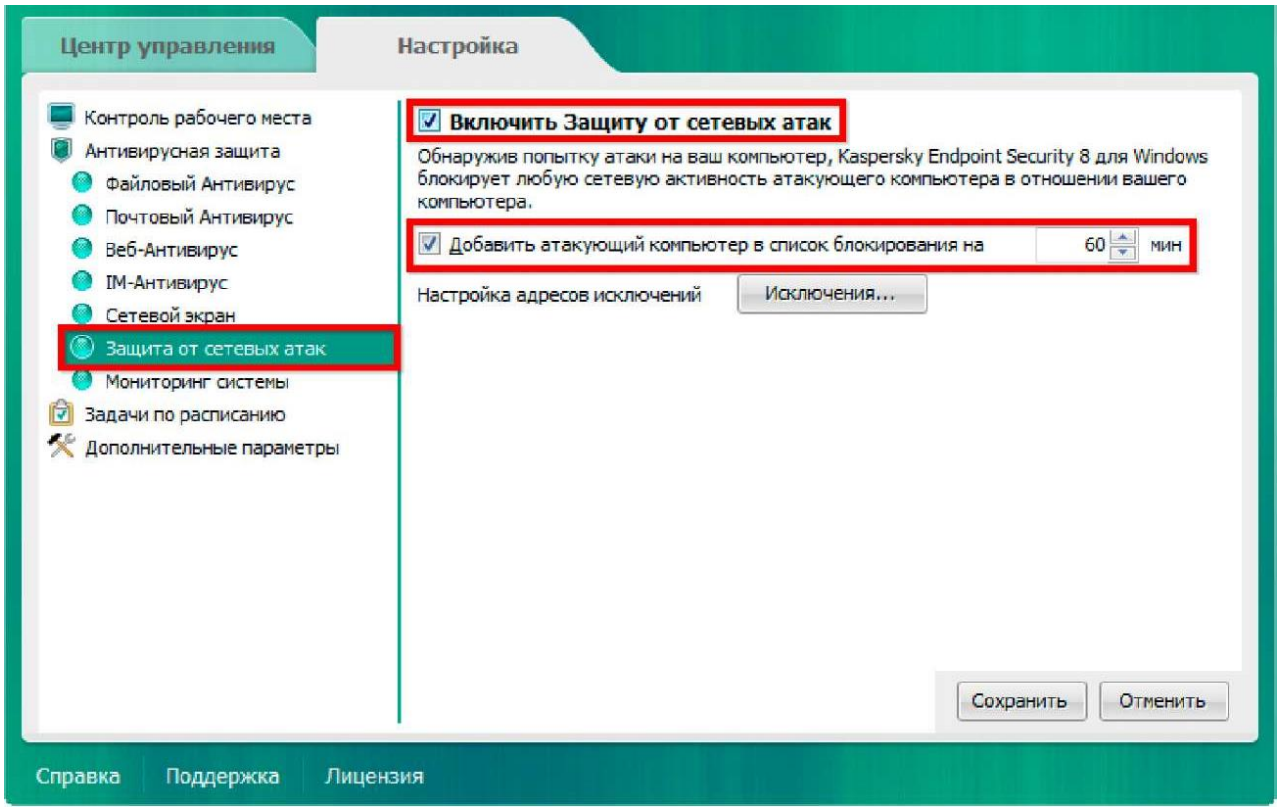


Рисунок 64. Окно настроек мониторинга системы

- нажать кнопку «Сохранить» в правом нижнем углу.

Методические указания к практическим работам

Краснов Сергей Александрович
Племянников Александр Кимович
Решетняк Данил Александрович

Настройка средств защиты компьютерной информации

Издание публикуется в авторской редакции

СПбГЭТУ «ЛЭТИ»
197376, Санкт-Петербург, ул. Проф. Попова, 5