Методические рекомендации к практическому занятию №2

С.А. Краснов

УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД «DALLAS LOCK+ СМАРТ-КАРТЫ»

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ № 2

**УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД «DALLAS LOCK+ СМАРТ-КАРТЫ»**

***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, 5].

**ПРИЛОЖЕНИЕ А**

**Пример настройки СЗИ НСД «Dallas Lock»**

**Создание пользователя системы.** Необходимо выполнить следующие действия:

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

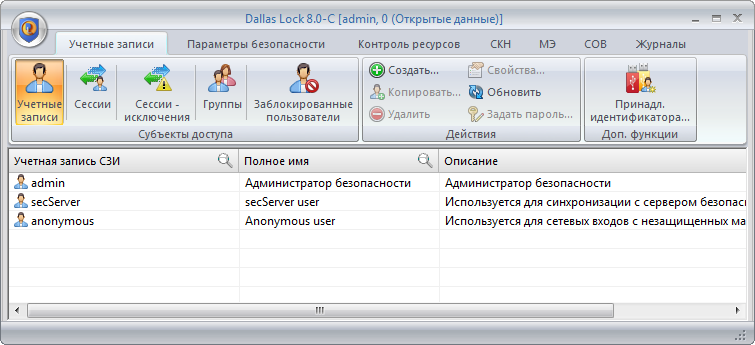


Рисунок 1. Окно оболочки администратора системы защиты

- 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).

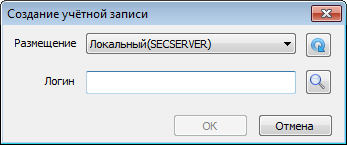


Рисунок 2. Окно создания учетной записи

- 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);

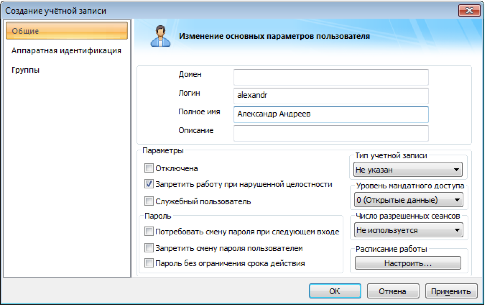


Рисунок 3. Окно редактирования параметров учетной записи

- 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;

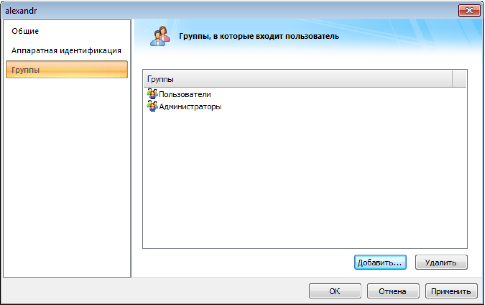


Рисунок 4. Окно редактирования списка групп пользователя

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

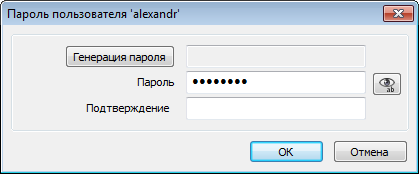


Рисунок 5. Окно формы ввода пароля

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);

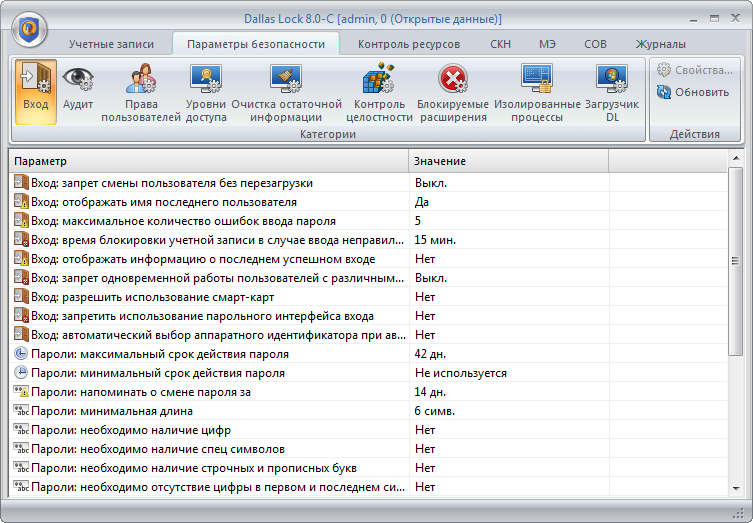


Рисунок 6. Список параметров входа

- 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);

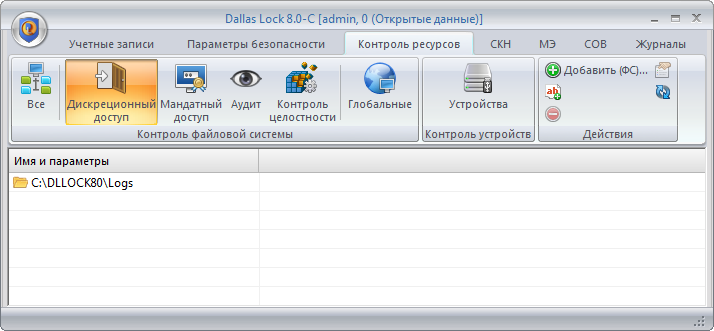


Рисунок 7. Окно дискреционного доступа

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

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

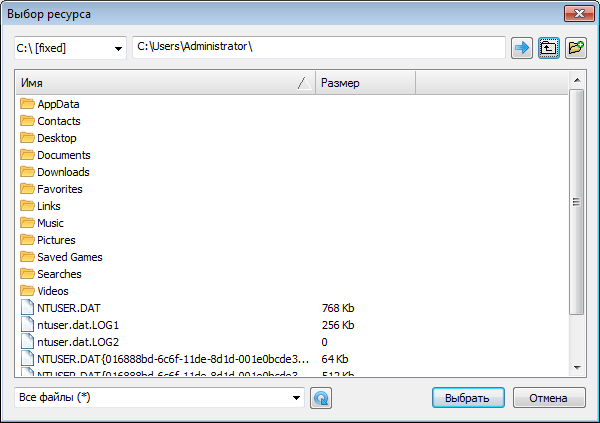


Рисунок 8. Окно выбора объекта ФС

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

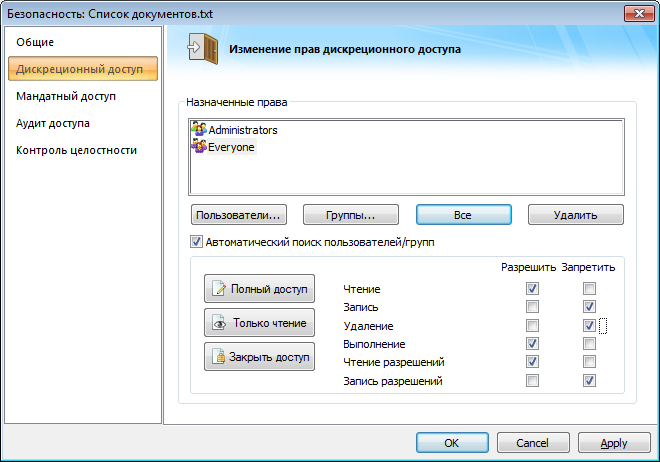


Рисунок 9. Окно назначения прав дискреционного доступа

- 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);

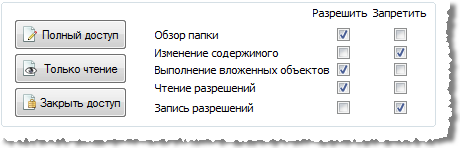


Рисунок 10. Список прав дискреционного пользования

- 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);

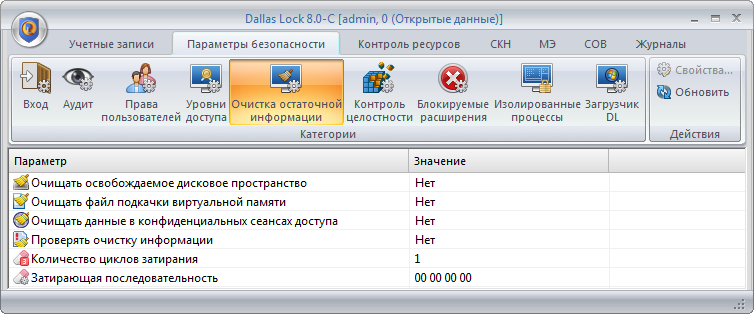


Рисунок 11. Параметры очистки остаточной информации

- 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);

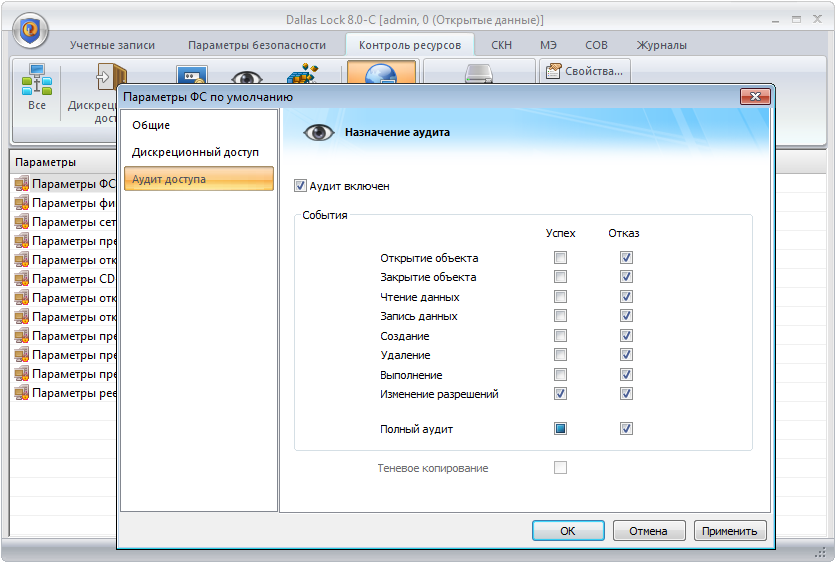


Рисунок 12. Окно назначения аудита на ресурс файловой системы

- 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);

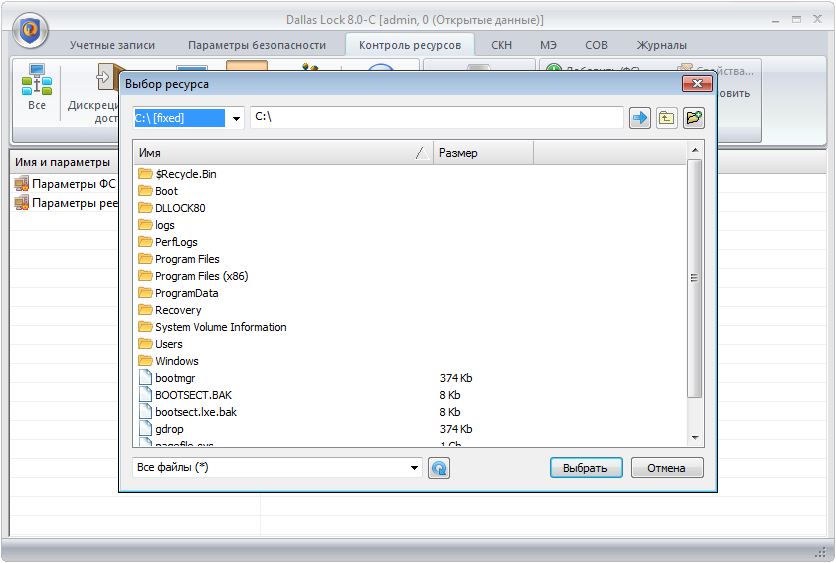


Рисунок 13. Выбор ресурса для назначения аудита

- 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);

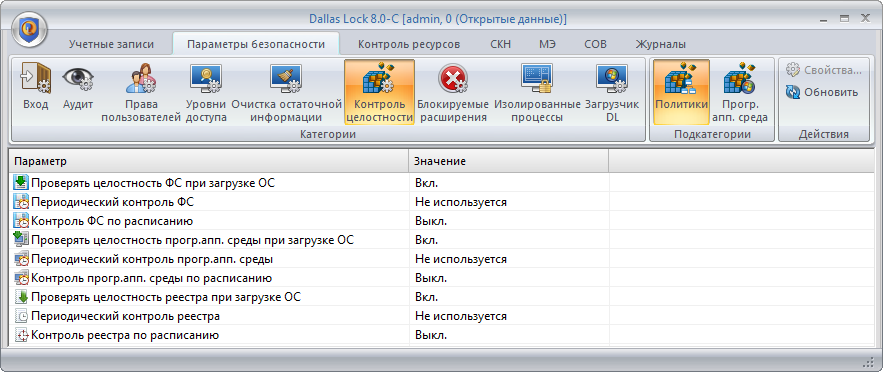


Рисунок 14. Вкладка контроль целостности в оболочке администратора

- 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);

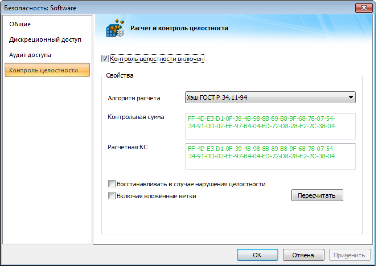


Рисунок 15. Контроль целостности ресурса файловой системы

- 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);

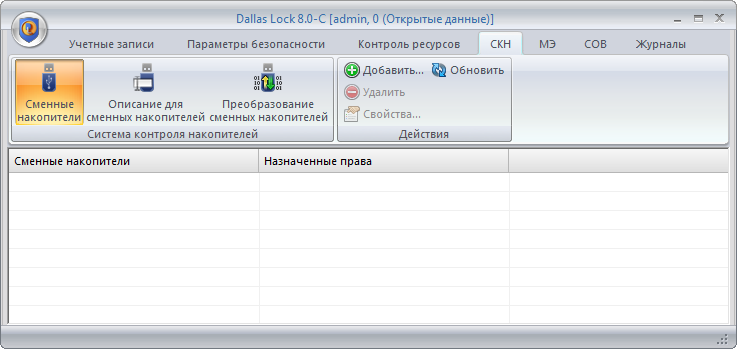


Рисунок 16. Окно настройки прав разграничения доступа для внешних носителей информации

- 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.

**Контрольные вопросы**

1. Перечислите основные руководящие документы ФСТЭК по классификации АС, средств вычислительной техники (СВТ), межсетевых экранов (МЭ) и программного обеспечения (ПО)?

2. Каким приказом определены требования Межсетевым экранам

3. Перечислите типы МЭ?

4. Охарактеризуйте МЭ типа «А»:

5. Охарактеризуйте МЭ типа «Г»:

6. Каким угрозам безопасности информации должен противодействовать МЭ типа «А» согласно «Профилям МЭ»?

7. Каким угрозам безопасности информации должен противодействовать МЭ типа «Б» согласно «Профилям МЭ»?

8. Что следует учитывать при написание правил МЭ

9. Опишите назначение и возможности механизма защиты МЭ Dallas Lock?

10. Что включает в себя подсистема регистрации и учета МЭ Dallas Lock?

**Дополнительные материалы, информационные источники**

1. Сайт компании ”Конфидент” https://dallaslock.ru/

2. Конфидент Система защиты информации от несанкционированного доступа Dallas Lock 8.0 Руководство по эксплуатации // Dallas Lock [Электронный ресурс]. 19.12.2019. – URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/%D0%A1%20%D0%98%D0%9A5%202017/RU.48957919.501410-02%2092%20%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%BF%D0%BE%20%D1%8D%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D0%B8.pdf (дата обращения: 19.12.2019).

3. Макаренко С.И., Ковальский А.А., Краснов С.А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учеб. пособие. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. - СПб.: Наукоемкие технологии, 2020. - 357 с.

**Методика текущего контроля**

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

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

**Текущая СРС по ПЗ № 2 состоит из:**

1. Работа с лекционным материалом, с учебной литературой – 2 ак.ч;

2. Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) 1,5 ак.ч.

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

4. Подготовка к лабораторным работам, к практическим и семинарским занятиям - 2 ак.ч

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

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

Доцент кафедры ИБ

Краснов С.А.