Методические рекомендации к практическому занятию №3

С.А. Краснов

УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД «SECRET NET+ ПАК "СОБОЛЬ"»

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ № 3

**УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД «SECRET NET+ ПАК "СОБОЛЬ"»**

**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:

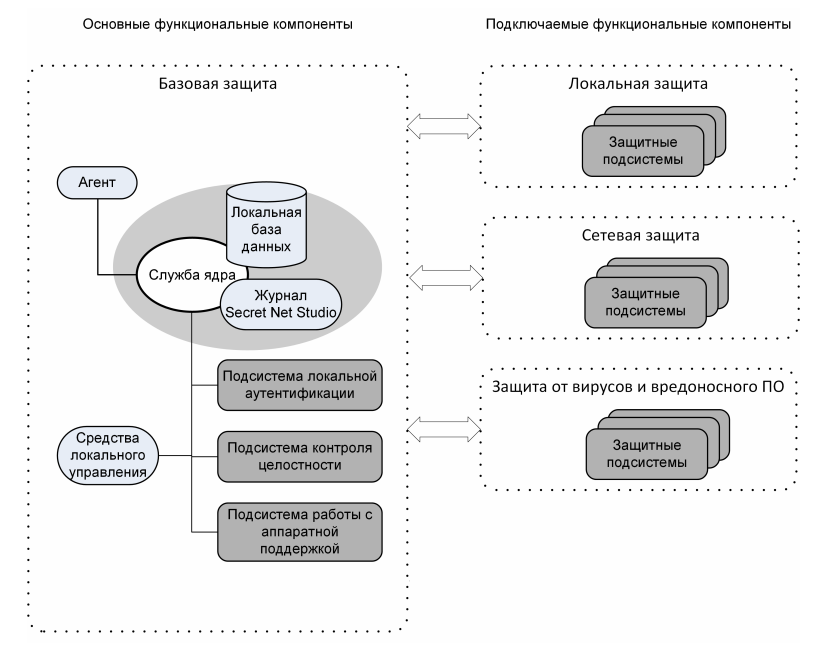
- основные программные службы, модули и защитные подсистемы (базовая защита);

- 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, 5].

**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).

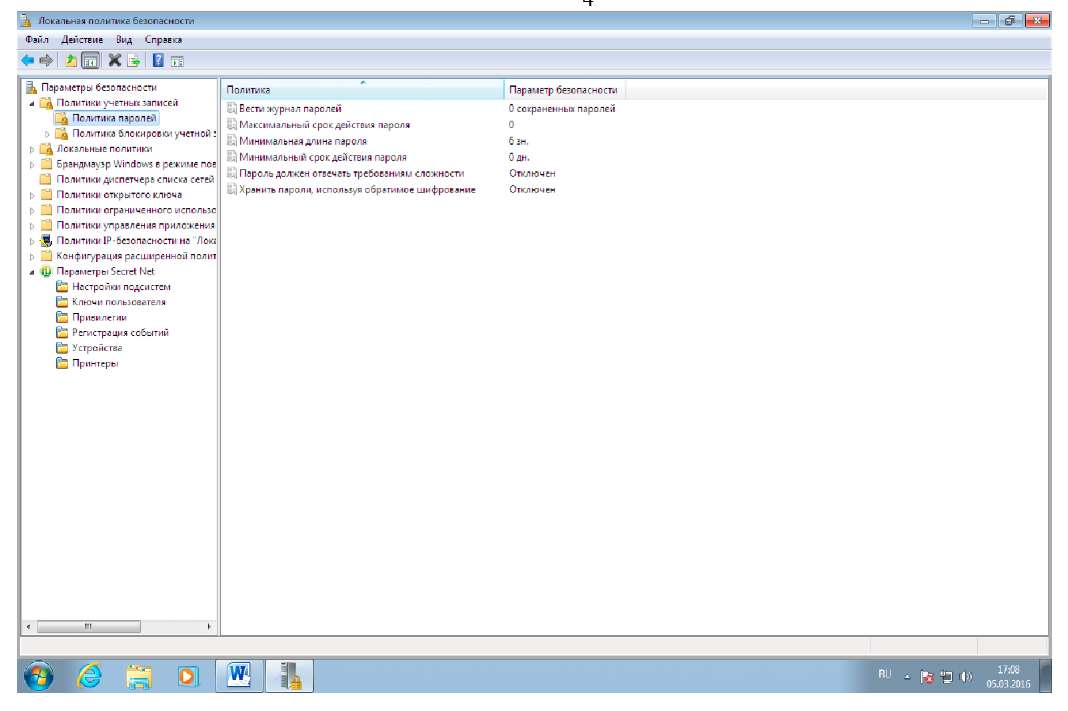


Рисунок 17. Окно настройки паролей

**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);

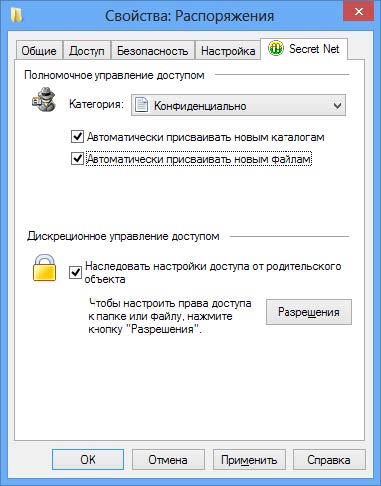


Рисунок 18. Окно «Свойства»

- 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);

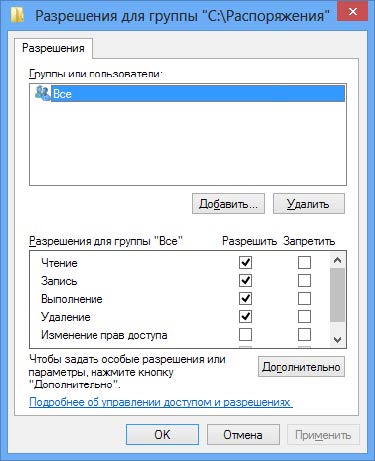


Рисунок 19. Окно «Разрешения»

- 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 "OK".

**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).

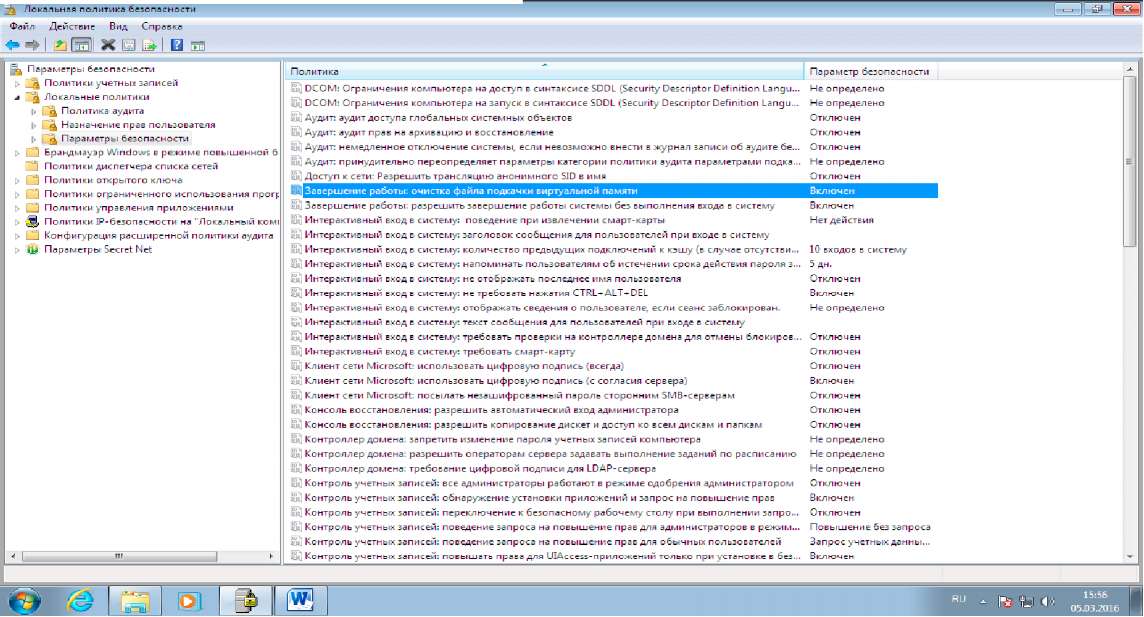


Рисунок 20. Окно локальной политики безопасности

**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);

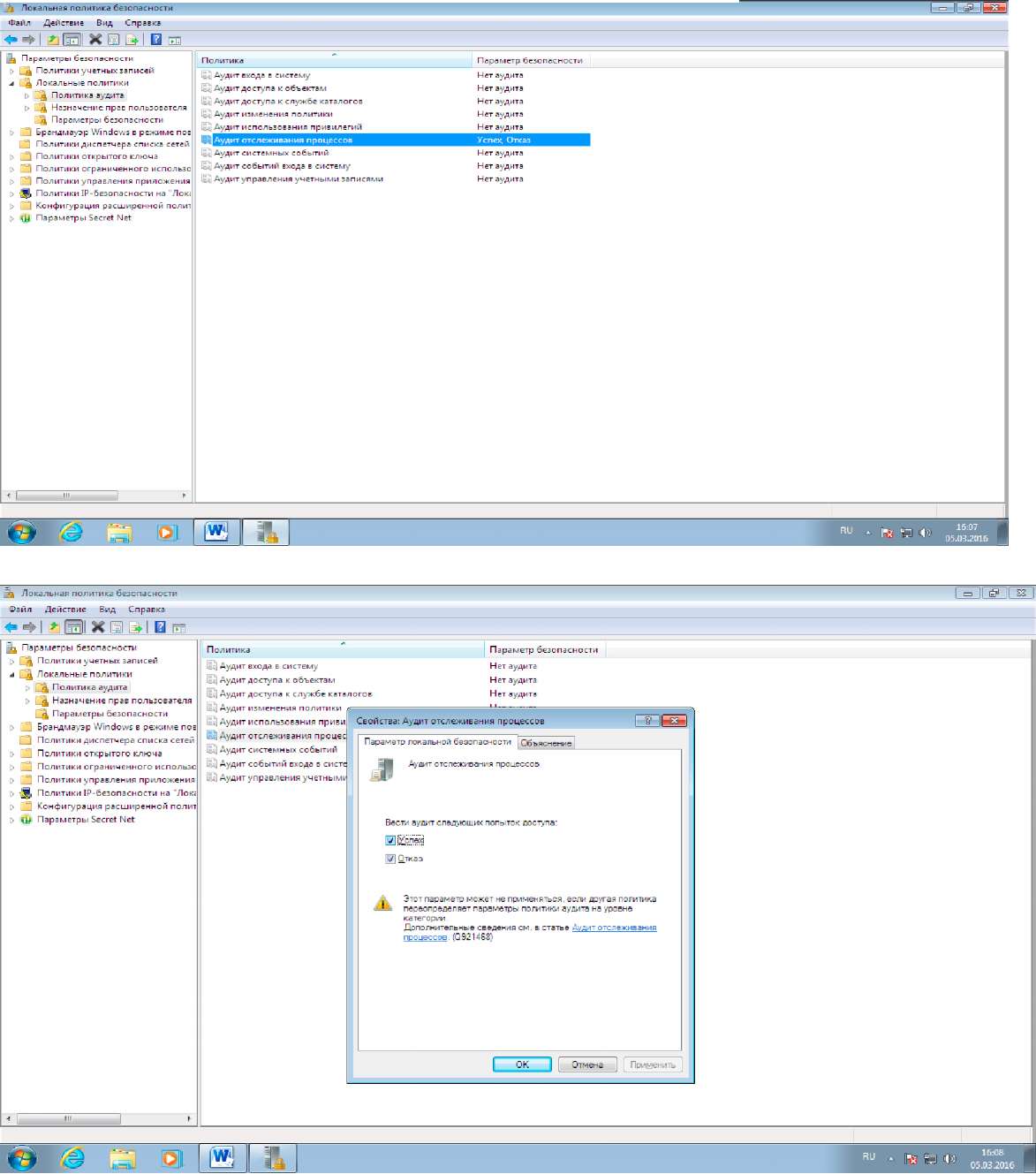


Рисунок 21. Окно настройки аудита процессов

**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 «OK». 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);

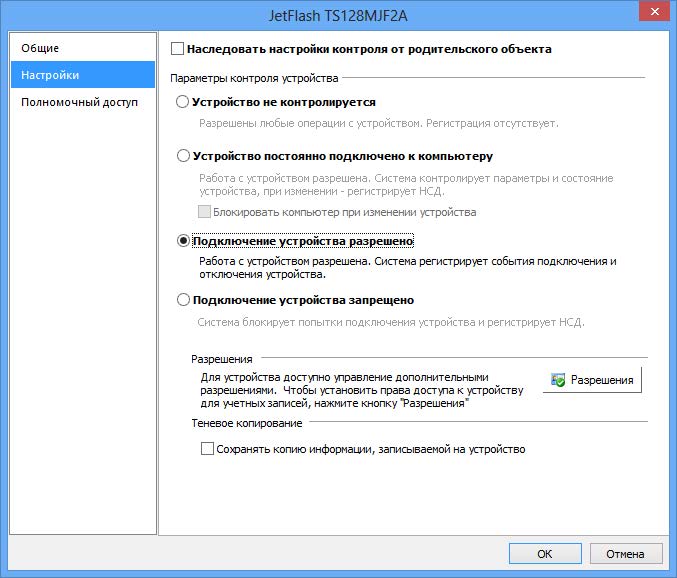


Рисунок 22. Окно настройки устройства

- 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);

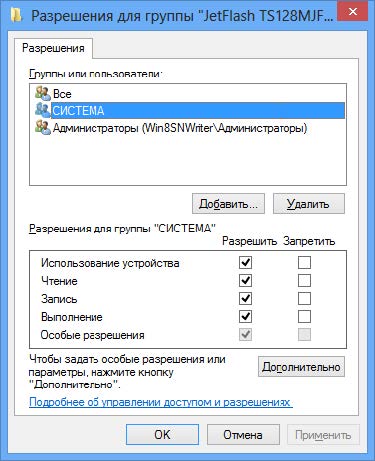


Рисунок 23. Окно «Разрешения»

- 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.

**Контрольные вопросы**

1. Какими важными достоинствами обладает Secret Net?
2. Что используется в качестве аппаратных средств Secret Net?
3. Какие механизмы защиты информации от несанкционированного доступа содержит Secret Net
4. Какие события позволяет отслеживать СЗИ от НСД Secret Net
5. Охарактеризуйте возможности Secret Net развернутого в сложной доменной сети с большим количеством сегментов
6. Из каких частей состоит СЗИ от НСД Secret Net
7. Перечислите журналы регистрации событий в Secret Net
8. Перечислите режимы работы с аппаратными средствами идентификации
9. Охарактеризуйте мягкий режим работы с аппаратными средствами идентификации в Secret Net
10. Охарактеризуйте обычный режим работы с аппаратными средствами идентификации в Secret Net
11. Охарактеризуйте усиленный режим работы с аппаратными средствами идентификации в Secret Net
12. Охарактеризуйте жесткий режим работы с аппаратными средствами идентификации в Secret Net
13. Перечислите перечень ресурсов компьютера, защищаемых средствами системы Secret Net
14. Перечислите состав средств разграничения доступа пользователей к ресурсам компьютера в системе Secret Net
15. Охарактеризуйте механизм избирательного управления доступом
16. Охарактеризуйте механизм полномочного управления доступом
17. Перечислите компоненты подсистемы контроля целостности Secret Net.
18. Охарактеризуйте модуль входа Secret Net

**Дополнительные материалы, информационные источники**

1. Код безопасности Средство защиты информации Secret Net 7. Руководство администратора. Настройка механизмов защиты // Securitycode [Электронный ресурс]. 19.12.2019. – URL: https://www.securitycode.ru/upload/documentation/secret\_net/Secret\_Net\_Admin\_Guide\_Construction\_Principles.pdf (дата обращения: 19.12.2019).

2. 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.

3. Краснов, Сергей Александрович. Настройка средств защиты компьютерной информации [Текст]: учеб.­метод. пособие / С. А. Краснов, А. К. Племянников, Д. А. Решетняк, 2020. ­71 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 № 3 состоит из:

1. Работа с лекционным материалом, с учебной литературой – 2,5 ак.ч;

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

3. Самостоятельное изучение разделов дисциплины - 2 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.