Лабораторная работа № 4. Системы обеспечения информационной безопасности от НСД. Secret Net.

Управление доступом в системе Secret Net 5.1

Для организации эффективной совместной работы пользователей и обеспечения надежной защиты ресурсов компьютера от несанкционированного доступа в системе Secret Net 5.1 используются следующие механизмы управления доступом пользователей к ресурсам компьютера:

* механизм избирательного управления доступом;
* механизм полномочного управления доступом;
* механизм замкнутой программной среды (ЗПС).

Система защиты информации Secret Net 5.1 для избирательного (дискреционного) управления доступом использует стандартные механизмы ОС Windows, а также собственные средства для разграничения доступа к дискам, портам и другим устройствам

– механизм разграничения доступа к устройствам.

Механизм полномочного управления доступом предназначен для разграничения доступа пользователей к ресурсам компьютера на основании полномочного (мандатного) принципа разграничения доступа, а также для контроля потоков конфиденциальной информации в системе.

Механизм замкнутой программной среды позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска.

Избирательное разграничение доступа к устройствам

В системе Secret Net 5.1 все устройства, входящие в состав или подключаемые к компьютеру, разделены на группы. В каждой группе устройства разделены на классы. В классы входят собственно устройства.

Для объектов каждого уровня определен набор параметров, с помощью которых настраивается механизм разграничения доступа к устройствам.

Для настройки механизма разграничения доступа к устройствам

необходимо настроить права доступа пользователей к устройствам и включить нужный режим работы механизма.

Для настройки прав доступа пользователей к устройствам:

1. Вызовите оснастку для управления параметрами объектов групповой политики («Пуск | Все программы | Secret Net 5 | Локальная политика безопасности») и перейдите к разделу «Параметры безопасности | Параметры Secret Net».
2. Выберите папку «Устройства».

В правой части окна оснастки появится список устройств.

3) Выберите в списке объект (группу, класс или устройство), вызовите контекстное меню и активируйте команду «Свойства».

На экране появится диалоговое окно настройки свойств объекта.

4) Если требуется отключить наследование параметров, установите отметку в поле «Использовать заданные здесь настройки».

После этого станут доступны параметры подключения и отключения устройства.

5) Удалите или установите отметки в параметрах подключения и отключения и

перейдите к диалогу «Разрешения»ё

В верхней части диалога «Разрешения» расположен список учетных записей, для которых выполняется настройка прав доступа к данному объекту. В нижней части диалога приведены параметры доступа для выбранной учетной записи.

1. При необходимости отредактируйте список учетных записей:
   * чтобы добавить в список учетную запись, нажмите кнопку «Добавить» и выберите нужный объект в стандартном диалоге выбора объектов ОС Windows;
   * чтобы удалить учетную запись из списка, выберите ее в списке и нажмите кнопку «Удалить».
2. Для изменения параметров доступа выберите в списке нужную учетную запись и затем расставьте разрешения и запреты на выполнение операций. При этом учитывайте принцип наследования параметров от родительских объектов дочерними: явно заданные параметры перекрывают унаследованные от родительских объектов.

Для отключения или включения режима переноса наследуемых разрешений нажмите кнопку «Дополнительно» и в открывшемся диалоговом окне удалите или установите отметку в поле «Наследовать от родительского объекта…».

1. В диалоге настройки свойств объекта нажмите кнопку «OK».
2. Для сохранения изменений нажмите на панели инструментов кнопку «Сохранить настройки политики контроля устройств».

Механизм разграничения доступа к устройствам может работать в следующих режимах:

* отключено. Права доступа пользователей к устройствам не контролируются;
* «мягкий». Права доступа пользователей к устройствам контролируются, но не ограничиваются, попытки доступа регистрируются в журнале Secret Net 5.1;
* «жесткий». При превышении пользователями прав доступа к устройствам доступ

блокируется, попытки доступа регистрируются в журнале Secret Net 5.1.

Для изменения режима работы механизма разграничения доступа к устройствам:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net».
2. Выберите папку «Настройки подсистем».

В правой части окна оснастки появится список параметров.

3) Вызовите контекстное меню для параметра «Разграничение доступа к устройствам: Режим работы» и активируйте в нем команду «Свойства».

На экране появится диалог настройки параметра.

4) Настройте действие параметра и нажмите кнопку «OK».

Полномочное управление доступом

Механизм полномочного управления доступом может работать в нескольких режимах:

- контроль потоков. Режим контроля потоков обеспечивает предотвращение несанкционированного распространения конфиденциальной информации. Под распространением понимается вывод конфиденциальной информации на внешние носители, которые могут быть извлечены из системы или на которых конфиденциальные файлы теряют признак конфиденциальности. Кроме того, в режиме контроля потоков блокируется несанкционированное понижение категории конфиденциальности ресурса (файла или каталога). При включенном режиме контроля потоков возможность доступа пользователя к конфиденциальным файлам определяется уровнем конфиденциальности сессии. Уровень сессии не может быть выше уровня допуска, назначенного пользователю. В зависимости от типа входа в систему уровень конфиденциальности сессии выбирается самим пользователем или автоматически назначается системой. Уровень конфиденциальности сессии нельзя изменить на

протяжении всего сеанса работы пользователя. После открытия сессии при выполнении пользователем операций с конфиденциальными ресурсами категории конфиденциальности ресурсов сравниваются с уровнем сессии. Выполнение операции разрешено, если категория конфиденциальности ресурса ниже или совпадает с уровнем сессии. Если контроль потоков отключен, система не контролирует распространение конфиденциальной информации. При попытке доступа к конфиденциальному файлу проверяется уровень допуска пользователя

и категория конфиденциальности ресурса;

* контроль печати. Режим контроля печати обеспечивает предотвращение несанкционированного вывода на печать конфиденциальных документов. Если контроль печати отключен, любому пользователю, который имеет доступ к конфиденциальному файлу, разрешено распечатывать этот файл. При печати в документ не добавляется гриф конфиденциальности. При включенном режиме контроля печати распечатывать конфиденциальные документы разрешено только пользователям, которым предоставлена привилегия «Печать конфиденциальных документов». При печати конфиденциальных документов в обязательном порядке добавляется гриф конфиденциальности.

Факт печати конфиденциального документа регистрируется в журнале. Для включения или отключения режима контроля потоков:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net».
2. Выберите папку «Настройки подсистем».

В правой части окна оснастки появится список параметров.

3) Вызовите контекстное меню для параметра «Полномочное управление доступом: Режим работы» и активируйте в нем команду «Свойства».

На экране появится диалог настройки параметра.

1. Включите или отключите действие режима, установив отметки в соответствующих полях.
2. Для включения контроля потоков в расширенном режиме установите отметку в поле «Расширенный контроль вывода информации».
3. Нажмите кнопку «OK».

Для включения или отключения режима контроля печати:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net».
2. Выберите папку «Настройки подсистем».

В правой части окна оснастки появится список параметров.

3) Вызовите контекстное меню для параметра «Полномочное управление доступом: Режим контроля печати конфиденциальных документов» и активируйте в нем команду «Свойства».

На экране появится диалог настройки параметра.

4) Включите или отключите действие режима, установив отметки в соответствующих полях, и нажмите кнопку «OK».

Назначение уровней допуска и привилегий пользователям

Уровень допуска и привилегии назначаются администратором безопасности каждому пользователю индивидуально.

Для назначения уровня допуска и привилегий:

1) Активируйте команду «Пуск | Все программы | Secret Net 5 | Управление компьютером».

На экране появится окно консоли с загруженной оснасткой для управления параметрами компьютера.

2) Перейдите к разделу «Управление компьютером (локальным) | Служебные программы» и выберите папку «Локальные пользователи и группы | Пользователи».

В правой части окна консоли с загруженной оснасткой для управления параметрами компьютера появится список пользователей (рисунок 1).

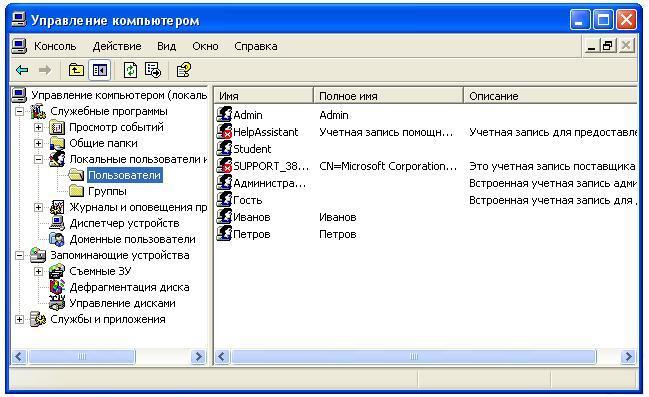


Рисунок 1 – Список зарегистрированных в системе пользователей

1. Вызовите окно настройки свойств пользователя и перейдите к диалогу «Secret Net 5».
2. В панели выбора режима выберите режим «Доступ» (рисунок 2).

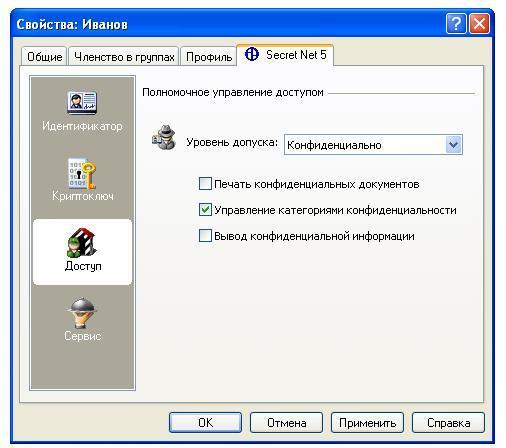


Рисунок 2 – Назначение пользователю уровня допуска и привилегий

5) Установите уровень допуска пользователя в одноименном поле.

Для уровней «конфиденциально» и «строго конфиденциально» становится доступным назначение привилегий.

1. Для предоставления или отмены привилегий пользователя установите или удалите отметки в соответствующих полях:
   * управление категориями конфиденциальности. Пользователь может изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска и управлять режимом наследования категорий конфиденциальности каталогов;
   * печать конфиденциальных документов. Используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном режиме контроля печати конфиденциальных документов;
   * вывод конфиденциальной информации. Пользователю разрешается выводить конфиденциальную информацию на внешние носители.
2. Нажмите кнопку «OK».

Параметры вступят в силу при следующем входе пользователя в систему.

Присвоение категорий конфиденциальности ресурсам

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию «Управление категориями конфиденциальности». Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS.

Для изменения категории конфиденциальности каталога:

1) В программе «Проводник» вызовите контекстное меню каталога и активируйте команду «Свойства». В появившемся на экране окне «Свойства» перейдите к диалогу «Secret Net» (рисунок 3).

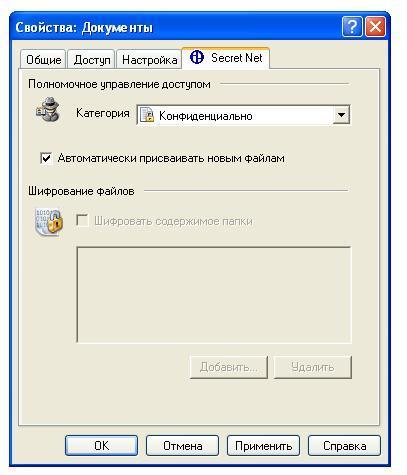


Рисунок 3 – Изменение категории конфиденциальности каталога

1. Укажите необходимые значения параметров:
   * выберите в раскрывающемся списке поля «Категория» нужную категорию конфиденциальности для каталога;
   * выберите режим автоматического присвоения категории конфиденциальности файлам каталога, установив параметр «Автоматически присваивать новым файлам» в положение «Включено» или «Выключено».
2. Нажмите кнопку «OK».

Если каталог содержит файлы и подкаталоги, на экране появится диалог, предлагающий изменить категории конфиденциальности файлам и подкаталогам (рисунок 4).

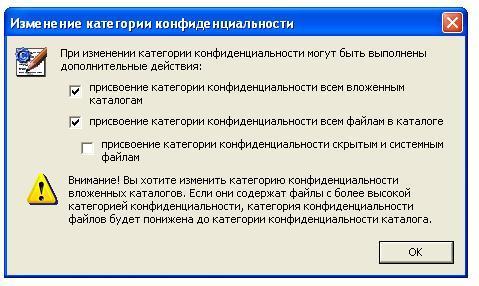


Рисунок 4 – Изменение категории конфиденциальности вложенных в каталог файлов и подкаталогов

Выполните следующие действия:

* если требуется присвоить подкаталогам выбранную для каталога категорию конфиденциальности, а также изменить для подкаталогов состояние параметра «Автоматически присваивать новым файлам», поставьте отметку в поле «присвоение категории конфиденциальности всем вложенным каталогам»;
* если требуется, чтобы всем файлам в каталоге, а также и в подкаталогах (только при условии, что первый выключатель содержит отметку), за исключением скрытых и системных файлов, была присвоена выбранная для каталога категория конфиденциальности, поставьте отметку в поле «присвоение категории конфиденциальности всем файлам в каталоге»;
* если требуется, чтобы категория конфиденциальности была также присвоена находящимся в каталоге и подкаталогах скрытым и системным файлам, поставьте отметку в поле «присвоение категории конфиденциальности скрытым и системным файлам». Внимание: во избежание нарушений в работе системы без особой необходимости не рекомендуется присваивать скрытым и системным файлам категории «конфиденциально» и «строго конфиденциально»;
* нажмите кнопку «OK».

Пояснение. Если в каталоге и подкаталогах имеются файлы, категории конфиденциальности которых выше назначаемой каталогу, то категории конфиденциальности таких файлов будут автоматически понижены до категории конфиденциальности, назначаемой каталогу.

Если для каталога, содержащего подкаталоги, изменено значение параметра «Автоматически присваивать новым файлам», а категория конфиденциальности каталога

осталась прежней, на экране появится диалог, предлагающий изменить признак наследования для вложенных каталогов (рисунок 5).

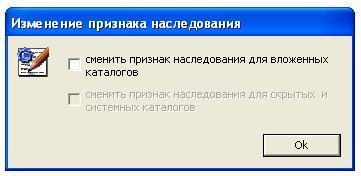


Рисунок 5 – Изменение признака наследования Выполните следующие действия:

* если требуется изменить для подкаталогов состояние параметра «Автоматически присваивать новым файлам», поставьте отметку в поле «сменить признак наследования для вложенных каталогов»;
* если требуется изменить состояние параметра «Автоматически присваивать новым файлам» также и для скрытых и системных каталогов, поставьте отметку в поле второго выключателя;
* нажмите кнопку «OK».

Для изменения категории конфиденциальности файла:

1. Вызовите программу «Проводник».
2. Вызовите контекстное меню файла и активируйте в нем команду «Свойства».
3. В появившемся на экране окне «Свойства» перейдите к диалогу «Secret Net» (рисунок 6).

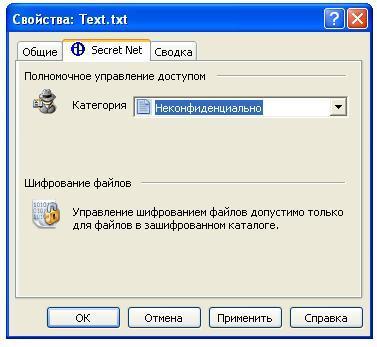


Рисунок 6 – Изменение категории конфиденциальности файла

1. Выберите в раскрывающемся списке поля «Категория» нужную категорию конфиденциальности файла.
2. Нажмите кнопку «OK».

Замкнутая программная среда

Механизм замкнутой программной среды предназначен для ограничения доступа к исполняемым файлам. Доступ ограничивается только теми программами, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят только разрешенные для запуска программы. Попытки запуска других программ блокируются, а в журнале безопасности регистрируются события несанкционированного доступа.

Настройка механизма замкнутой программной среды выполняется в программе «Контроль программ и данных» («Пуск | Все программы | Secret Net 5 | Контроль программ и данных».) Интерфейс программы «Контроль программ и данных» представлен на рисунке 7.

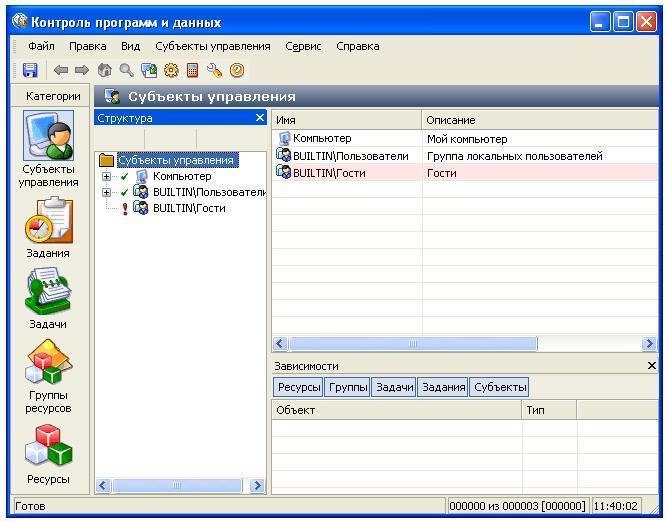


Рисунок 7 – Интерфейс программы «Контроль программ и данных»

Модель данных

В ходе настройки механизма замкнутой программной среды формируется модель данных, определяющая списки разрешенных программ и некоторые другие параметры.

Модель данных представляет собой иерархию объектов и описание связей между ними. В модели используются 5 категорий объектов:

* ресурс. Однозначно определяет местонахождение контролируемого ресурса и его тип. Ресурсом может быть файл, каталог, переменная реестра или ключ реестра

Windows;

* группа ресурсов. Объединяет множество ресурсов заданного типа, отобранных по какому-либо признаку. Группа ресурсов может объединять либо файлы и каталоги, либо объекты системного реестра Windows. Например, файлы одного и того же типа;

* задача. Объединяет множество групп ресурсов, отобранных по какому-либо признаку. Например, исполняемые файлы какой-либо прикладной программы, разрешенные для запуска пользователям определенной группы пользователей. Задача должна включать в себя как минимум одну группу ресурсов. Одна и та же группа ресурсов может входить в несколько разных задач;
* задание. Задание для механизма замкнутой программной среды объединяет задачи, на основании которых формируются списки исполняемых файлов, разрешенных для запуска пользователям;
* субъект управления. Субъектом управления может быть компьютер, группа пользователей и отдельные пользователи. Задания замкнутой программной среды применяются к пользователям и группам пользователей.

Объекты одной категории являются подчиненными или вышестоящими по отношению к объектам другой категории. Включение ресурсов в группы, групп в задачи, а задач – в задания называется установлением связей между объектами. В конечном итоге задания назначаются субъектам. Модель, включающая в себя объекты всех категорий, между которыми установлены все нужные связи, – это подробная инструкция системе Secret Net 5.1, определяющая, что и как должно контролироваться.

Пояснение. Модель также может содержать объекты, не связанные с другими, или неполные цепочки объектов, но работать будут только те фрагменты, которые объединяют все уровни модели.

Построение фрагмента модели данных по умолчанию

Выполнение этого этапа требуется только при формировании новой модели данных.

Для построения фрагмента модели данных по умолчанию: 1) Откройте программу «Контроль программ и данных».

Если программа управления запускается первый раз на данном компьютере, происходит автоматический запуск Мастера создания модели данных.

Если программа управления запускается не первый раз, на экране появится основное окно программы управления. Чтобы из основного окна перейти к работе с Мастером, активируйте команду «Файл | Новая модель данных».

На экране появится диалог «Настройка контроля по умолчанию» (рисунок 8).

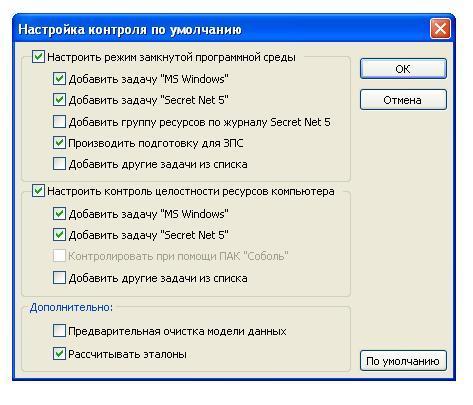


Рисунок 8 – Настройка контроля по умолчанию

Диалог предназначен для задания настроек, в соответствии с которыми автоматически будет создана модель данных. Отметки, установленные в диалоге по умолчанию, предлагают сформировать модель для ресурсов Windows и Secret Net.

* диалоге имеется возможность добавления в модель и других задач, относящихся к ресурсам других прикладных программ. Используйте для этого выключатели

«Добавить другие задачи из списка». 2) Нажмите кнопку «OK».

Начнется формирование модели данных, и после его успешного завершения в основном окне программы управления появится новая структура, включающая в себя субъекты «Компьютер» и «Пользователи» с назначенными для них заданиями.

3) Активируйте в меню команду «Файл | Сохранить».

6.1.2 Добавление заданий в модель данных

Для формирования задания:

1) Выберите категорию «Задания» и активируйте в меню «Задания | Создать задание».

На экране появится диалог выбора типа задания.

2) Выберите тип задания (ЗПС) и нажмите кнопку «OK».

На экране появится диалог «Создание нового задания на ЗПС» (рисунок 9).

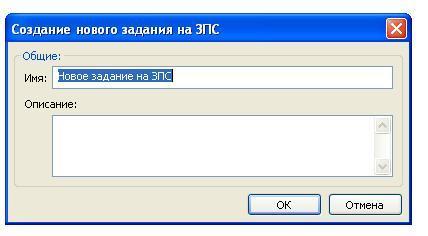


Рисунок 9 – Создание нового задания на ЗПС

3) Введите имя задания, его краткое описание и нажмите кнопку «OK».

Добавление задач в модель данных

Для добавления задач в модель данных могут быть использованы как ручные методы, так и специальное средство – механизм генерации задач. Во втором случае задачи создаются на основании сведений об установленных на компьютере программных продуктах. Для этого используются сведения MS Installer и ярлыки меню «Пуск» ОС Windows. При этом в задачи будут автоматически включены ресурсы, связанные с исполняемыми модулями выбранного программного обеспечения. Кроме того, можно задать дополнительные условия фильтрации отбираемых ресурсов.

Рекомендуется использовать механизм генерации при наполнении модели данных сложными задачами, включающими в себя большое количество ресурсов.

Для добавления в модель данных задач с помощью механизма генерации: 1) Выберите в меню «Сервис» команду «Генератор задач».

На экране появится диалог, предлагающий создать задачи по установленным программам (рисунок 10).

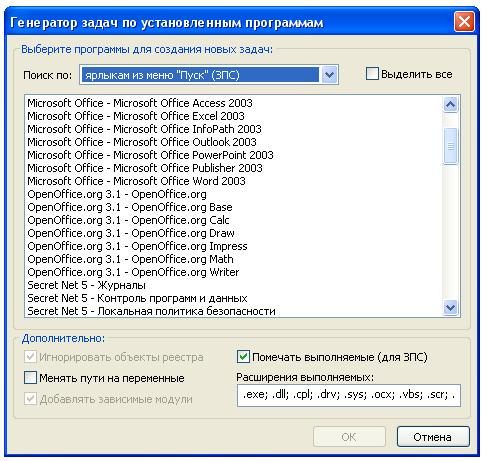


Рисунок 10 – Создание задач по установленным программам

Диалог предназначен для выбора программ, а также задания дополнительных условий отбора ресурсов.

1. Выберите в поле «Поиск по» – «ярлыкам из меню «Пуск» (ЗПС)».
2. Выберите в списке программы и укажите в нижней части диалога дополнительные условия отбора ресурсов.

Для выделения нескольких программ используйте клавишу <Ctrl>. Для выделения всего списка поставьте отметку в поле «Выделить все».

Для ЗПС доступны следующие условия отбора ресурсов:

* менять пути на переменные. При записи в модель данных абсолютные пути к файлам и каталогам меняются на имена системных переменных окружения ОС

Windows;

* помечать выполняемые. Выполняемые файлы при отображении в окне программы управления помечаются специальным значком. К выполняемым относятся файлы, имеющие расширения, указанные в строке «Расширения

выполняемых». Перечень расширений можно изменить, вручную добавив или удалив из строки элементы.

4) Нажмите кнопку «OK».

Начнется процесс генерации. Затем появится сообщение об успешном его завершении.

5) Нажмите кнопку «OK» в окне сообщения.

В модель добавятся новые задачи, включающие в себя группы ресурсов, но не связанные с вышестоящими объектами (заданиями), на что указывает значок .

6) Активируйте в меню команду «Файл | Сохранить». Для добавления в модель данных задачи вручную:

1) Выберите категорию «Задачи» и активируйте в меню команду «Задачи | Создать задачу | Вручную».

Появится диалог для настройки параметров задачи.

2) Введите имя задачи, ее краткое описание и нажмите кнопку «OK».

В модели данных появится новая задача, не связанная с другими объектами.

3) Активируйте в меню команду «Файл | Сохранить».

При добавлении в модель данных задачи вручную необходимо включить в эту задачу необходимые ресурсы.

Включение задач в задание

Для включения задач в задание:

1. Выберите категорию «Задания» на панели категорий.
2. В окне структуры вызовите контекстное меню для задания и активируйте команду «Добавить задачи/группы | Существующие».

Появится диалог со списком всех задач и групп ресурсов, еще не включенных в данное задание.

1. Выберите задачи, включаемые в задание.
2. Нажмите кнопку «OK».
3. Активируйте в меню команду «Файл | Сохранить».

Добавление группы ресурсов в задачу

Для добавления в задачу группы ресурсов вручную:

1) Выберите категорию «Задачи», найдите объект, для которого необходимо добавить группу ресурсов, вызовите для него контекстное меню, и активируйте команду «Добавить группы | Новую группу вручную…».

Появится диалог для настройки параметров группы ресурсов.

2) Заполните поля диалога и нажмите кнопку «OK».

Добавленная группа ресурсов будет связана с вышестоящим объектом.

3) Активируйте в меню команду «Файл | Сохранить».

Добавление ресурсов в группу ресурсов

Для добавления ресурсов в группу ресурсов:

1. Выберите категорию «Группы ресурсов».
2. Выберите в дополнительном окне структуры группу, в которую предполагается добавить новые ресурсы, вызовите контекстное меню и активируйте команду «Добавить ресурсы | Существующие».

На экране появится диалог со списком всех ресурсов, имеющихся в модели данных, но не входящих в данную группу. Выберите в списке те ресурсы, которые требуется включить в группу, и нажмите кнопку «OK». Выбранные ресурсы будут добавлены в группу.

3) Активируйте в меню команду «Файл | Сохранить».

Установка связей субъектов управления с заданиями

На данной стадии настройки необходимо назначить субъектам управления сформированные задания. Если в модели данных нет нужного субъекта управления, его нужно добавить.

Для добавления субъекта управления в модель данных:

1. Выберите категорию «Субъекты управления» на панели категорий.
2. В меню «Субъекты управления» выберите команду «Добавить в список». Появится стандартный диалог выбора пользователей и групп.
3. Выполните стандартные действия для поиска и выбора нужных объектов.
4. Нажмите кнопку «OK».

В окне программы управления появятся новые субъекты, не связанные с другими объектами и отмеченные знаком .

Для установления связи субъекта управления с заданием:

1) Выберите категорию «Субъекты управления» на панели категорий.

2) Найдите в дополнительном окне структуры или в области списка объектов нужного субъекта управления, с которым требуется связать задание, вызовите контекстное меню и активируйте команду «Добавить задания | Существующие».

На экране появится диалог, содержащий список имеющихся заданий. Для каждого задания в списке указано количество субъектов, с которыми оно связано.

1. Выберите задания ЗПС, которые требуется назначить субъекту.
2. Нажмите кнопку «OK».

Выбранные задания будут назначены субъекту.

5) Активируйте в меню команду «Файл | Сохранить».

Подготовка ресурсов для замкнутой программной среды

Для того чтобы ресурсы контролировались механизмом замкнутой программной среды, они должны иметь признак «выполняемый» и входить в задание ЗПС. Присвоение ресурсам признака «выполняемый» называется подготовкой ресурсов для ЗПС. Этот признак присваивается всем файлам, имеющим заданные расширения.

Таким образом, файлы, имеющие признак «выполняемый» и входящие в задание ЗПС, образуют список разрешенных для запуска программ. После связывания задания с пользователем и включения «мягкого» или «жесткого» режима система Secret Net 5.1 начнет контролировать запуск программ пользователем и регистрировать соответствующие события в журнале.

При построении модели данных с помощью автоматизированных средств подготовка ресурсов для ЗПС включена в соответствующие процедуры и выполняется по умолчанию. При построении модели вручную и ее модификации подготовка ресурсов для ЗПС выполняется как отдельная процедура.

Для подготовки ресурсов для ЗПС:

1) Выберите в меню «Сервис» команду «Ресурсы ЗПС».

На экране появится диалог для настройки параметров процедуры.

2) Если требуется, чтобы в ходе подготовки были проанализированы все имеющиеся в модели ресурсы (в том числе и те, у которых ранее был установлен признак «выполняемый»), оставьте отметку в поле «Предварительно сбросить флаг «выполняемый» у всех ресурсов». В этом случае список ресурсов, имеющих признак «выполняемый», будет построен заново. При этом время выполнения процедуры будет зависеть от общего числа ресурсов в модели данных.

Если требуется, чтобы были проанализированы только ресурсы, не имеющие признака «выполняемый», удалите отметку.

1. Удалите из списка или добавьте в него расширения файлов, для которых должен быть установлен признак «выполняемый».
2. Для добавления в модель данных зависимых модулей оставьте отметку в поле «Добавлять зависимые модули».

Если добавление зависимых модулей не требуется, удалите отметку. 5) Нажмите кнопку «OK».

Начнется процесс подготовки ресурсов к использованию в механизме замкнутой программной среды и появится информационное окно, отображающее ход выполнения процесса. После окончания появится сообщение об успешном завершении процесса.

6) Активируйте в меню команду «Файл | Сохранить».

Включение механизма замкнутой программной среды в «жестком» режиме

Механизм замкнутой программной среды может функционировать в «мягком» и «жестком» режимах работы. «Мягкий» режим нужен для настройки механизма, «жесткий» – основной штатный режим работы механизма. В «мягком» режиме пользователю разрешается запускать любые программы. Если при этом пользователь

запускает программы, не входящие в перечень разрешенных, в журнале Secret Net 5.1 регистрируются соответствующие события несанкционированного доступа. В «жестком» режиме разрешается запуск только тех программ, которые входят в список разрешенных. Запуск других программ блокируется, а в журнале Secret Net 5.1 регистрируются события несанкционированного доступа.

Для включения механизма ЗПС в «жестком» режиме:

1. Выберите категорию «Субъекты управления» на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер, вызовите контекстное меню и активируйте команду «Свойства».

В появившемся окне «Свойства субъекта управления» перейдите к диалогу «Режимы».

1. Установите отметку в поле «Режим ЗПС включен» и удалите отметку из поля «Мягкий» режим» (если она там установлена).
2. При необходимости установите дополнительные параметры контроля:
   * проверять целостность модулей перед запуском. При запуске программ,

входящих в список разрешенных, проверяется их целостность;

* + проверять заголовки модулей перед запуском. В процессе контроля включается дополнительный механизм, повышающий надежность разделения ресурсов на исполняемые и неисполняемые файлы, т.е. подлежащие и не подлежащие проверке.

1. Нажмите кнопку «OK».
2. Активируйте в меню команду «Файл | Сохранить».

На данном компьютере начнет действовать механизм ЗПС в «жестком» режиме.

Выполнение лабораторной работы

1 Вход в систему и изучение параметров системы.

1. Зайдите в систему под учетной записью Администратора: - имя пользователя – Администратор;

- пароль – (пароль необходимо спросить у преподавателя).

1. Вызовите оснастку для управления параметрами объектов групповой политики
   * оснастку для управления параметрами компьютера. Сделайте выводы о параметрах системы, установленной на рабочей станции.

2 Предварительная настройка параметров полномочного управления доступом. 2.1 На диске С:\ создайте иерархию каталогов:

* С:\Folder1\Folder2\
* С:\Folder3\Folder4\

Из каталога С:\Secret Net\ распределите следующим образом 4 файла:

* С:\Folder1\text1.txt
* С:\Folder1\Folder2\text2.txt
* С:\Folder3\text3.txt
* С:\Folder3\Folder4\text4.txt

2.2 В программе «Проводник» вызовите контекстное меню каталога Folder1, активируйте команду «Свойства» и перейдите к диалогу «Secret Net». Установите категорию конфиденциальности – «конфиденциально», выбрав значение из раскрывающегося списка поля «Категория». Установите отметку в поле «Автоматически присваивать новым файлам». Нажмите кнопку «ОК». На экране появится диалог, предлагающий изменить категории конфиденциальности вложенным файлам и подкаталогам. Установите отметку только в поле «Присвоение категории конфиденциальности всем файлам в каталоге» и нажмите кнопку «ОК».

1. В программе «Проводник» вызовите контекстное меню каталога Folder3, активируйте команду «Свойства» и перейдите к диалогу «Secret Net». Установите категорию конфиденциальности – «строго конфиденциально», выбрав значение из раскрывающегося списка поля «Категория». Установите отметку в поле «Автоматически присваивать новым файлам». Нажмите кнопку «ОК». На экране появится диалог, предлагающий изменить категории конфиденциальности вложенным файлам и подкаталогам. Установите отметки в поля «Присвоение категории конфиденциальности всем вложенным каталогам» и «Присвоение категории конфиденциальности всем файлам в каталоге» и нажмите кнопку

«ОК».

1. Убедитесь, что каталог:

* Folder1 и входящий в него файл имеют категорию конфиденциальности – «конфиденциально». Folder1 имеет отметку в поле «Автоматически присваивать новым файлам»;
* Folder2 и входящий в него файл имеют категорию конфиденциальности – «неконфиденциально»;
* Folder3, Folder4 и входящие в них файлы имеют категорию конфиденциальности – «строго конфиденциально». Folder3, Folder4 имеют отметки в поле «Автоматически присваивать новым файлам».

1. В программе «Проводник» вызовите контекстное меню каталога Folder3, активируйте команду «Свойства» и перейдите к диалогу «Secret Net». Установите категорию конфиденциальности – «конфиденциально», выбрав значение из раскрывающегося списка поля «Категория». Установите отметку в поле «Автоматически присваивать новым файлам». Нажмите кнопку «ОК». На экране появится диалог, предлагающий изменить категории конфиденциальности вложенным файлам и подкаталогам. Установите отметку только в поле «Присвоение категории конфиденциальности всем файлам в каталоге» и нажмите кнопку «ОК».
2. В программе «Проводник» вызовите контекстное меню каталога Folder1, активируйте команду «Свойства» и перейдите к диалогу «Secret Net». Установите категорию конфиденциальности – «строго конфиденциально», выбрав значение из раскрывающегося списка поля «Категория». Установите отметку в поле «Автоматически присваивать новым файлам». Нажмите кнопку «ОК». На экране появится диалог, предлагающий изменить категории конфиденциальности вложенным файлам и подкаталогам. Установите отметки в поля «Присвоение категории конфиденциальности всем вложенным каталогам» и «Присвоение категории конфиденциальности всем файлам в каталоге» и нажмите кнопку

«ОК».

1. Убедитесь, что каталог:

* Folder1, Folder2 и входящие в них файлы имеют категорию конфиденциальности – «строго конфиденциально». Folder1, Folder2 имеют отметки в поле «Автоматически присваивать новым файлам».
* Folder3 и входящий в него файл имеют категорию конфиденциальности – «конфиденциально». Folder3 имеет отметку в поле «Автоматически присваивать новым файлам»;
* Folder4 и входящий в него файл имеют категорию конфиденциальности –

«неконфиденциально».

2.8 Вызовите оснастку для управления параметрами компьютера («Пуск | Все программы | Secret Net 5 | Управление компьютером»). Перейдите к разделу «Управление компьютером (локальным) | Служебные программы» и выберите папку «Локальные пользователи и группы | Пользователи». В правой части окна

оснастки появится список пользователей. Вызовите окно настройки свойств пользователя user1 и перейдите к диалогу «Secret Net 5». В панели выбора режима выберите режим «Доступ». В поле «Уровень допуска» выберите уровень допуска к конфиденциальной информации – «конфиденциально». Нажмите кнопку «OK».

3 Предварительная настройка параметров избирательного разграничения доступа к устройствам.

1. Вызовите оснастку для управления параметрами объектов групповой политики. Перейдите к разделу «Параметры безопасности | Параметры Secret Net». Выберите папку «Устройства». В правой части окна оснастки появится список устройств. Выберите диск (D:). Вызовите на экран окно настройки свойств диска (D:), убедитесь, что поле «Использовать заданные здесь настройки» содержит отметку, и перейдите к вкладке «Разрешения». Для пользователя user1 сделайте доступным только «Чтение». Задавать особые разрешения или параметры (кнопка «Дополнительно») не нужно. Сохраните изменения в политике контроля устройств (см. п. 4).
2. Попробуйте поменять права доступа на системный диск (C:). Сделайте вывод. 4 Предварительная настройка механизма замкнутой программной среды.

4.1 Откройте программу «Контроль программ и данных». Для пользователя user1 запретите запуск программы «Калькулятор».

Для этого необходимо создать новое задание:

1. Выберите категорию «Задания» и активируйте в меню «Задания | Создать задание».
2. Выберите тип задания (ЗПС) и нажмите кнопку «OK».
3. Введите имя задания, его краткое описание и нажмите кнопку «OK».

Затем необходимо создать задачу и включить ее в задание. Для создания вручную новой задачи:

1. Выберите категорию «Задачи» и активируйте в меню команду «Задачи | Создать задачу | Вручную».
2. Введите имя задачи, ее краткое описание и нажмите кнопку «OK».
3. Активируйте в меню команду «Файл | Сохранить».

Для включения задачи в задание:

1. Выберите категорию «Задания» на панели категорий.
2. В окне структуры вызовите контекстное меню для задания и активируйте команду «Добавить задачи/группы | Существующие».
3. Выберите задачи, включаемые в задание.
4. Нажмите кнопку «OK».
5. Активируйте в меню команду «Файл | Сохранить».

Затем нужно добавить в задачу группу ресурсов:

1. Выберите категорию «Задачи», найдите объект, для которого необходимо добавить группу ресурсов, вызовите для него контекстное меню, и активируйте команду «Добавить группы | Новую группу вручную…».
2. Введите имя группы ресурсов, ее краткое описание, в поле «Тип» выберите «Файлы/Каталоги» и нажмите кнопку «OK».
3. Активируйте в меню команду «Файл | Сохранить».

Далее необходимо добавить в группу ресурсов ресурсы:

1. Выберите категорию «Группы ресурсов».
2. Выберите в дополнительном окне структуры группу, в которую предполагается добавить новые ресурсы, вызовите контекстное меню и активируйте команду «Добавить ресурсы | Существующие».

На экране появится диалог со списком всех ресурсов, имеющихся в модели данных, но не входящих в данную группу. Для того, чтобы запретить пользователю запускать программу «Калькулятор», не нужно добавлять в группу ресурсов файл С:\WINDOWS\system32\calc.exe. Выберите все файлы кроме С:\WINDOWS\system32\calc.exe и нажмите кнопку «OK». Для выбора нескольких ресурсов используйте клавишу <Ctrl> или поле «Выделить все». Выбранные ресурсы будут добавлены в группу.

3) Активируйте в меню команду «Файл | Сохранить».

Далее нужно добавить субъект управления в модель данных и установить связь субъекта с заданием.

Для добавления субъекта управления в модель данных:

1. Выберите категорию «Субъекты управления» на панели категорий.
2. В меню «Субъекты управления» выберите команду «Добавить в список».
3. Выполните стандартные действия для поиска и выбора нужных объектов.
4. Нажмите кнопку «OK».

Для установления связи субъекта управления с заданием:

1. Выберите категорию «Субъекты управления» на панели категорий.
2. Найдите в дополнительном окне структуры или в области списка объектов нужного субъекта управления, с которым требуется связать задание, вызовите контекстное меню и активируйте команду «Добавить задания | Существующие».
3. Выберите задания ЗПС, которые требуется назначить субъекту.
4. Нажмите кнопку «OK».

Выбранные задания будут назначены субъекту.

5) Активируйте в меню команду «Файл | Сохранить».

Затем выполните подготовку ресурсов для ЗПС и включите ЗПС в «жестком» режиме.

Контрольные вопросы

1. Какие механизмы управления доступом пользователей к ресурсам компьютера используются в системе Secret Net 5.1?
2. Каковы особенности функционирования механизма разграничения доступа к устройствам в «мягком» режиме?
3. Каковы особенности функционирования механизма разграничения доступа к устройствам в «жестком» режиме?
4. Можно ли поменять права доступа на системный диск (C:)?
5. Для чего предназначен механизм замкнутой программной среды?
6. Что представляет собой модель данных в системе Secret Net 5.1?
7. Какие категории объектов используются в модели данных?
8. Какие пользователи имеют право изменять категорию конфиденциальности ресурсов в системе Secret Net 5.1?
9. На дисках с какой файловой системой должны быть расположены ресурсы в системе Secret Net 5.1, чтобы им можно было присвоить категорию конфиденциальности?
10. Назовите привилегии, доступные для пользователей с уровнем допуска к конфиденциальной информации «конфиденциально» или «строго конфиденциально».
11. Назовите особенности работы механизма замкнутой программной среды в «мягком» режиме.
12. Назовите особенности работы механизма замкнутой программной среды в «жестком» режиме.