ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Кафедра информационной безопасности

В.В. Пугин, С.А. Лабада

Криптографические протоколы

Методические указания к выполнению лабораторных работ

Самара
2018

УДК
ББК

П
Рекомендовано к изданию методическим советом ПГУТИ, протокол №1, от 27.09.18 г.

Рецензент:

начальник управления организации учебного процесса ФГБОУ ВО ПГУТИ,
к.т.н., доц. Кустова М.Н.

Пугин, В.В., Лабада С.А.
П Криптографические протоколы: методические указания к выполнению лабораторных работ / В.В. Пугин, С.А. Лабада. – Самара: ПГУТИ, 2018. – 51 с.

В методических указаниях рассматриваются актуальные вопросы обеспечения информационной безопасности в информационных системах и компьютерных сетях с помощью программного комплекса средств защиты информации Secret Net версии 5.1. Методические указания разработаны в соответствии с ФГОС ВО по направлениям подготовки студентов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» и направлению 10.03.01 «Информационная безопасность» и предназначено для проведения самостоятельной подготовки, практических и лабораторных занятий по дисциплине «Защита информации в компьютерных сетях».

ISBN

©, Пугин В.В., Лабада С.А., 2018

Содержание

Лабораторная работа №1.

«Защита от несанкционированного входа в систему Secret Net 5.1»

Содержание

Лабораторная работа №1

«Защита от несанкционированного входа в систему Secret Net 5.1»

1 Цель работы

Целью работы является ознакомление с системой защиты информации Secret Net 5.1, получение практических навыков работы с системой, а именно вход в систему, настройку ограничений и выполнение действий пользователя.

2 Вход в систему

На компьютере, защищенном Secret Net 5.1, существует несколько способов входа пользователя в систему. Какой из них используется в данный момент, зависит от того, оснащена ли система защиты дополнительными средствами аппаратной поддержки и введены ли они в эксплуатацию. В таблице 2.1 показаны способы входа в систему.

Таблица 2.1 – Способы входа в систему при различных режимах

Режим	**Способ входа в систему**	**Условия применения**
Стандартный	С помощью комбинации клавиш <Ctrl>+ <Alt>+<Del>	В системах, не оснащенных аппаратными средствами контроля входа
Только по идентификатору	Только при предъявлении персонального идентификатора	В системах, оснащенных аппаратными средствами, когда у всех пользователей есть персональные идентификаторы
Смешанный	С помощью комбинации клавиш <Ctrl>+ <Alt>+<Del> или персонального идентификатора	В системах, оснащенных аппаратными средствами, когда еще не всем пользователям выданы персональные идентификаторы

В данной лабораторной работе будет использоваться стандартный режим входа в систему.

При стандартном режиме приглашение на вход в систему имеет следующий вид (рисунок 2.1).

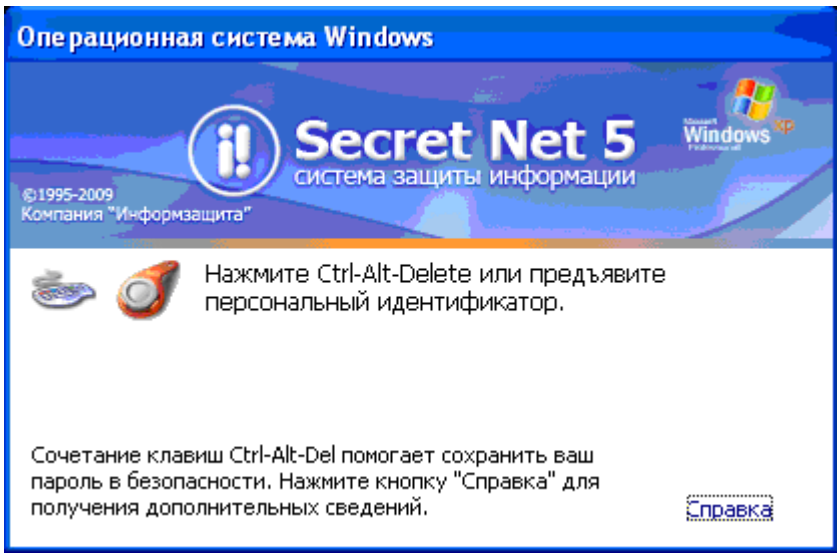

Рисунок 2.1 – Вход в систему

1) Выполните требуемые действия: нажмите одновременно комбинацию клавиш <Ctrl>+ <Alt>+<Del>.

На экране появится запрос на ввод имени и пароля (рисунок 2.2).

2) Укажите в полях диалога необходимые значения, учитывая следующие особенности заполнения полей:

- введите свое имя в поле "Пользователь".
- в поле "Пароль" введите свой пароль. В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

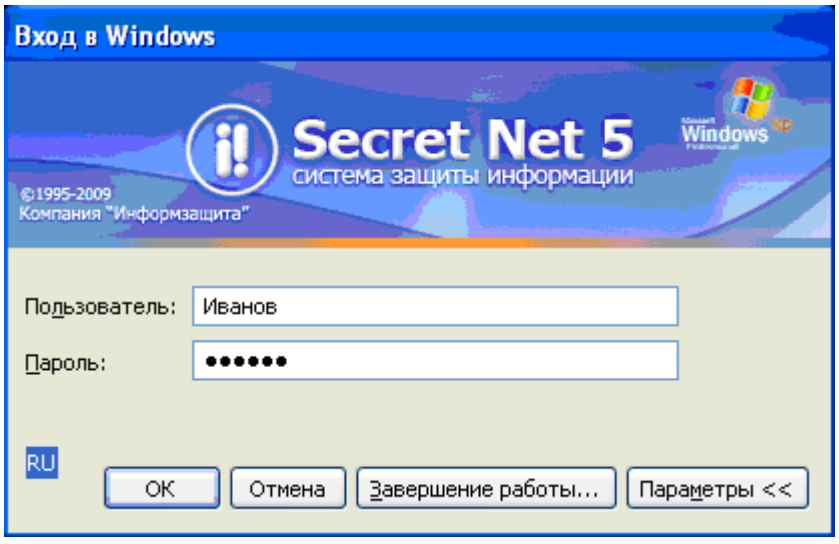

Рисунок 2.2 – Ввод пароля пользователя для входа в систему

Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <Backspace> или <Delete> и заново повторите ввод символов.

3) Нажмите кнопку "OK" для продолжения работы.

Если учетные данные введены правильно, выполняется вход в систему. В процессе загрузки на экран будут вводиться сообщения о выполняемых действиях.

2.1 Получение информации о пользователях компьютера

В консоли "Управление компьютером" можно посмотреть состав пользователей компьютера и получить сведения о группах, в которые входит каждый из них.

Для просмотра состава пользователей компьютера:

1) В левой части окна программы выберите папку "Локальные пользователи" | "Пользователи" и вызовите ее контекстное меню. В правой части окна отобразится список пользователей (рисунок 2.3).

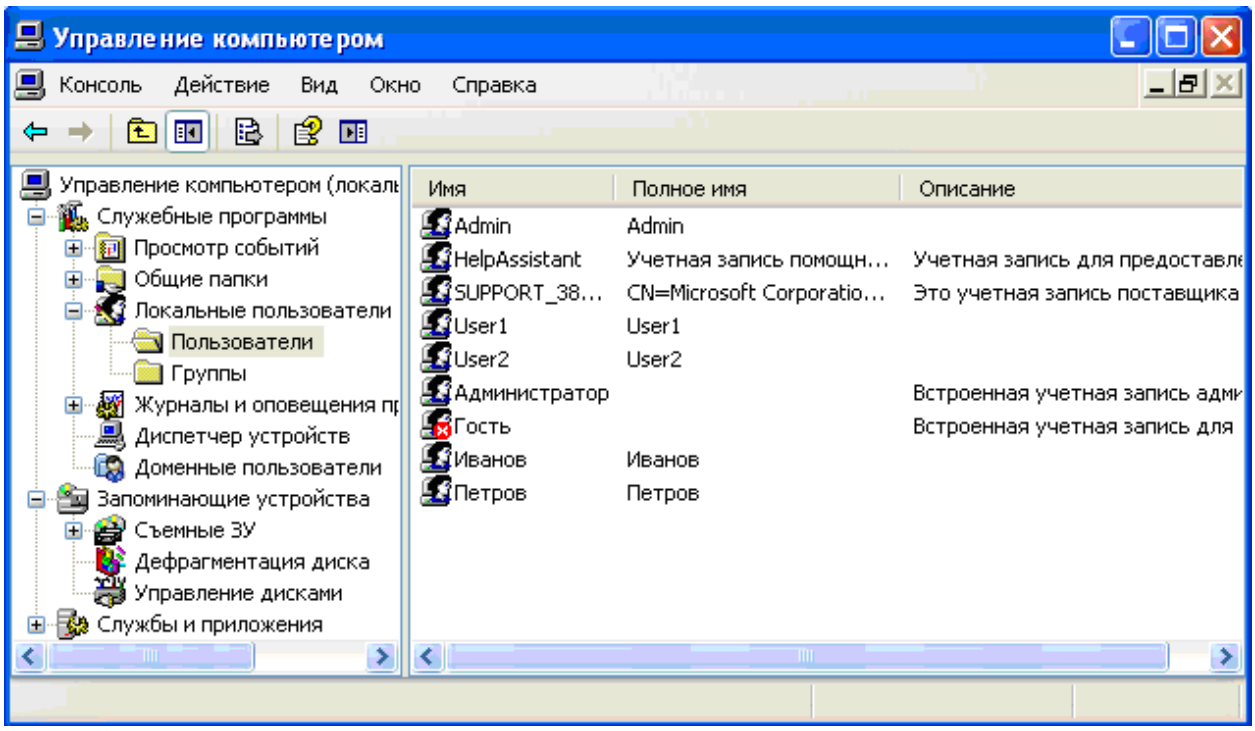

Рисунок 2.3 – Просмотр зарегистрированных пользователей (автономный вариант программы Secret Net 5.1)

Для просмотра перечня групп, в которые входит пользователь, выберите интересующего вас пользователя в папке "Пользователи", активируйте команду "Действие" | "Свойства" | "Членство в группах" (рисунок 2.4).

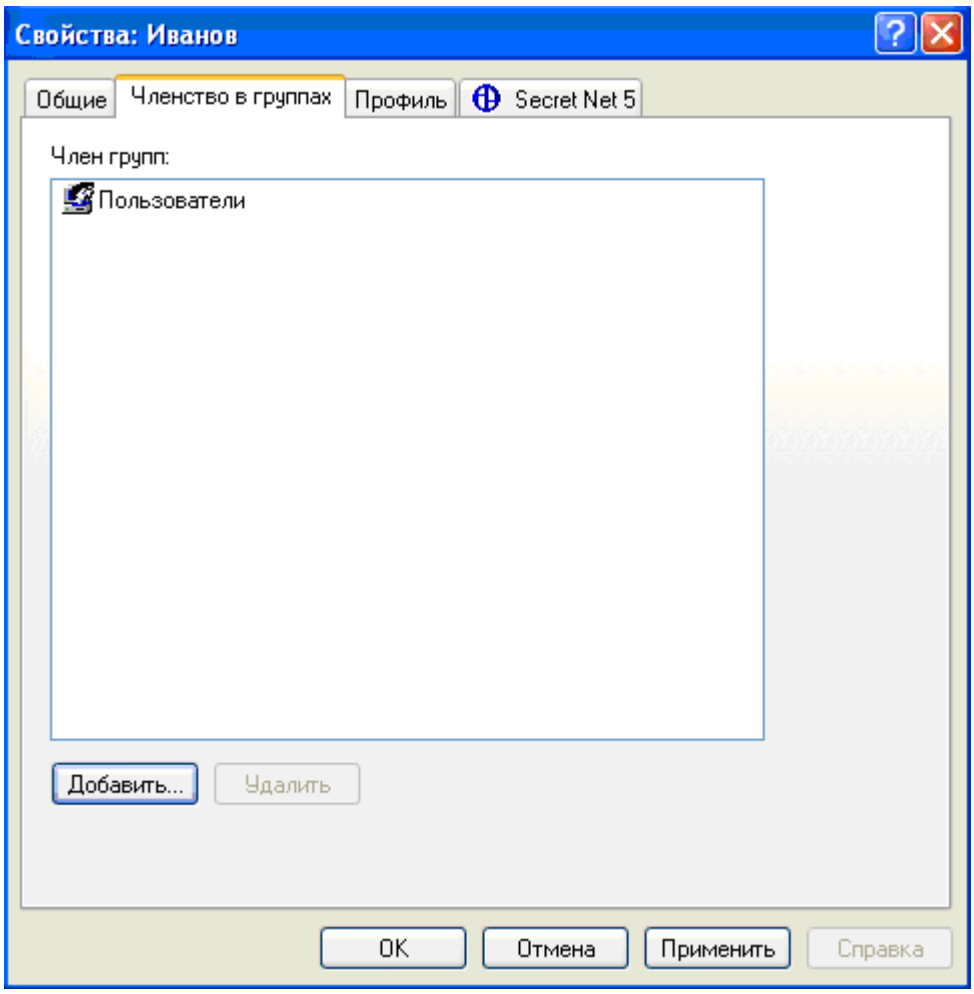

Рисунок 2.4 - Членство пользователя в группах

2.2 Создание пользователя

Чтобы включить нового локального пользователя в состав пользователей компьютера необходимо создать соответствующий ему объект" Пользователь".

Для создания локального пользователя:

1) Откройте оснастку "Управление компьютером".
2) В дереве консоли выберите папку "Пользователи".

В правой части окна отобразится список всех пользователей, зарегистрированных на компьютере.

3) В меню" Действие" выберите "Новый пользователь".
4) Введите соответствующие сведения в диалоговое окно.

Необходимо указать имя и пароль на вход в систему, после чего в списке пользователей появится новый объект.

5) Установите или снимите перечисленные ниже флажки:

- потребовать смену пароля при следующем входе в систему;
- запретить смену пароля пользователем;
- срок действия пароля не ограничен;
- отключить учетную запись.

6) Нажмите кнопку "Создать", а затем кнопку "Закрыть".

3 Настройка ограничений

3.1 Общие ограничения на пароль

К общим для всех локальных пользователей ограничениям на использование пароля относятся срок действия пароля, длина пароля, и контроль его уникальности.

Для настройки общих ограничений на использование пароля необходимо:

1) Открыть оснастку "Локальная политика безопасности".
2) Выбрать в дереве консоли папку "Политики учетных записей"│ "Политика паролей".

В правой части окна отображаются предъявляемые к паролям требования, которые действуют по отношению ко всем локальным пользователям компьютера. Для доменных пользователей действует доменная политика учетных записей, изменить которую можно только средствами централизованного управления доменом.

3) Установите необходимые значения параметров безопасности.

В меню "Действие" выберите "Свойства" или щелкните правой кнопкой мыши и выберите "Свойства" (рисунок 3.1).

4) Нажмите кнопку "ОК".

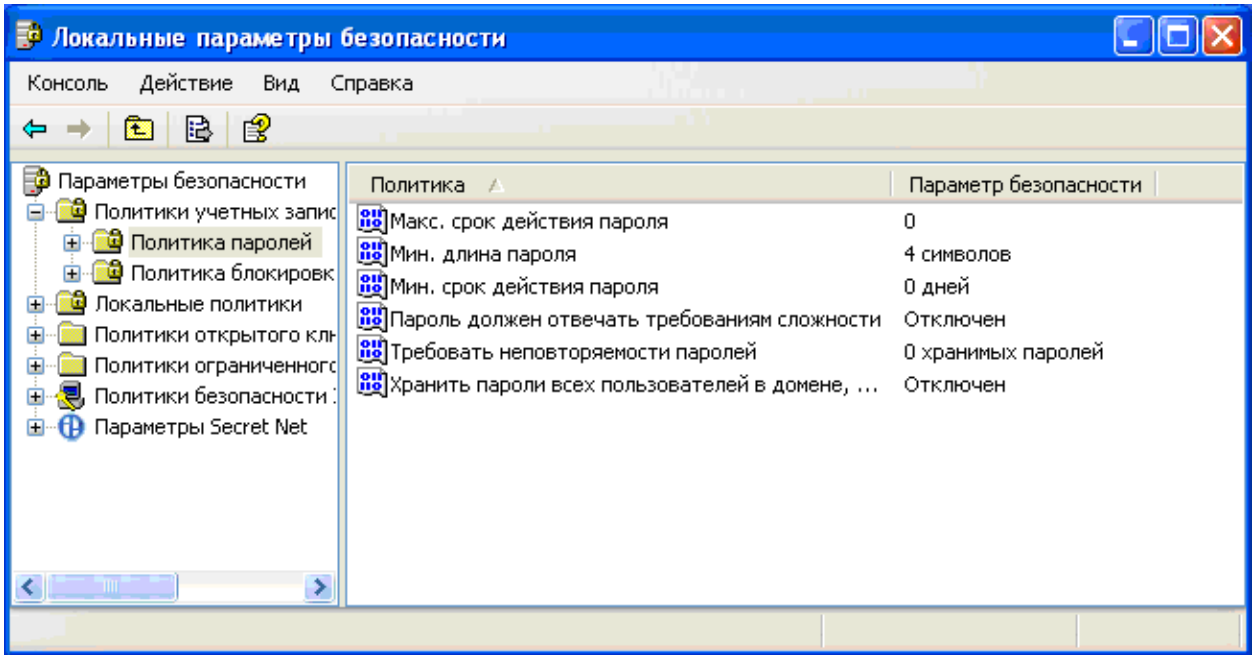

Рисунок 3.1 - Локальные параметры безопасности

3.2 Персональные ограничения на пароль

К персональным ограничениям на пароль относятся: запрет его смены, разрешение на использование постоянного пароля или его смена при следующем входе в систему. Настройку этих параметров можно выполнить только для локальных пользователей, для доменных пользователей применяют средства централизованного управления доменом.

Для настройки персональных ограничений на пароль:

1) Открыть оснастку "Управление компьютером "│" Пользователи".
2) Выберите пользователя и активируйте команду "Действие" │ "Свойства" │ "Общие".
3) Укажите необходимые значения параметров, а именно "Срок действия пароля неограничен" (рисунок 3.2).
4) Нажмите кнопку "ОК" или "Применить" в окне настройки свойств пользователя.

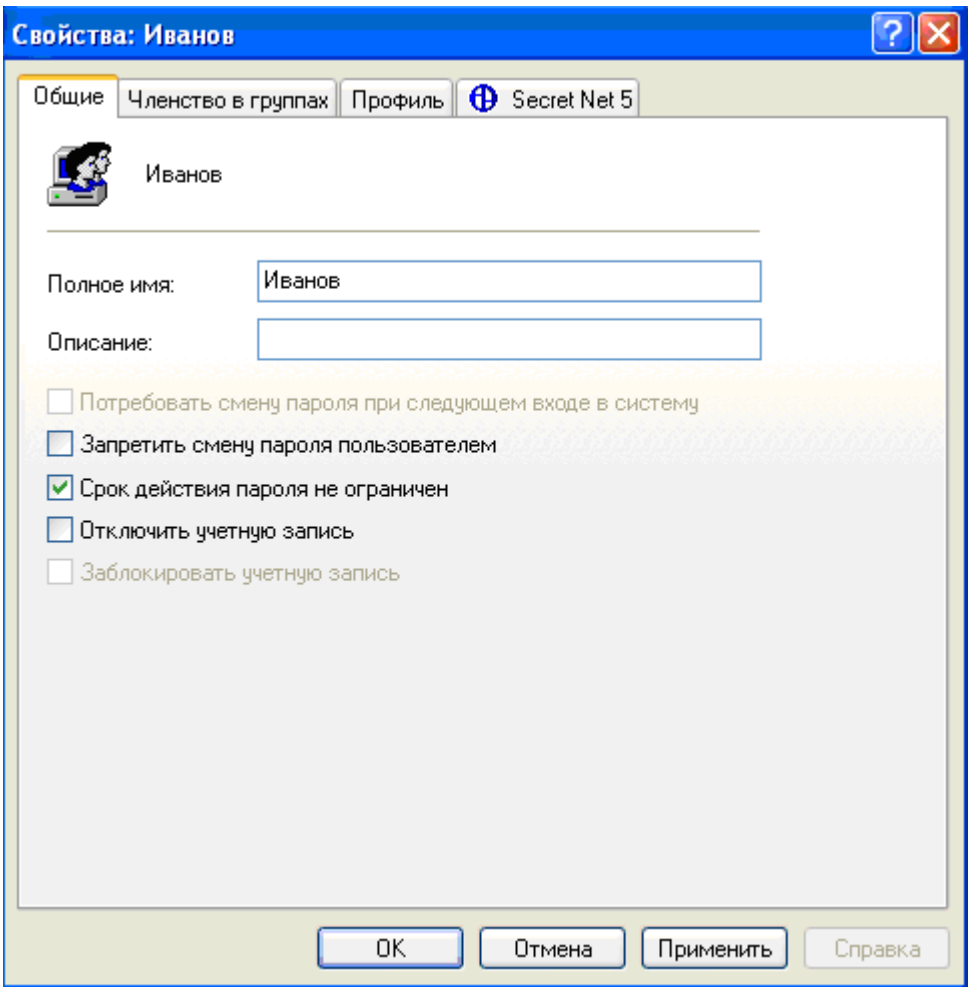

Рисунок 3.2 - Персональные ограничения на пароль

4 Действия пользователя

4.1 Вызов консоли для выполнения типовых операций

Средства управления, необходимые для работы пользователя, сосредоточены в диалоге "Безопасность Windows".

Для вызова консоли нажмите комбинацию клавиш <Ctrl>+ <Alt>+<Del>(рисунок 4.1).

На экране появится диалог" Безопасность Windows".

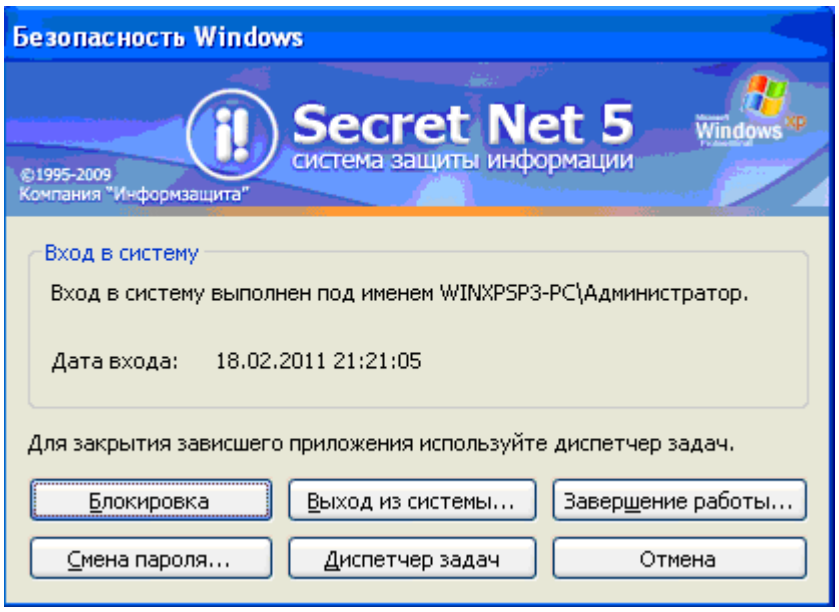

Рисунок 4.1 - Безопасность Windows

Типовые операции выполняются с помощью кнопок, расположенных в нижней части диалога (таблица 4.1).

Таблица 4.1 – Типовые операции, выполняемые с помощью консоли

Кнопка	**Выполняемая операция**
Блокировка	Временная блокировка работы компьютера (клавиатуры и монитора) для предотвращения использования его посторонним лицом.
Выход из системы	Вызов диалога завершения сеанса работы с Windows XP без выключения компьютера.
Завершение работы	Вызов диалога выключения или перезагрузки компьютера
Смена пароля	Вызов диалога замены текущего пароля на новый, если эта операция пользователю разрешена.
Диспетчер задач	Вызов диспетчера задач Windows XP.
Отмена	Отмена операции и закрытие диалогового окна.

Для закрытия диалогового окна "Безопасность Windows" нажмите кнопку "Отмена" или клавишу "Esc".

4.2 Смена пароля

Для смены пароля:

1) Вызовите диалог Безопасность Windows , нажав комбинацию клавиш <Ctrl>+ <Alt>+<Del>.
2) Нажмите кнопку "Смена пароля".

Если установленная политика паролей запрещает вам менять пароль, на экране появится сообщение об ошибке и процедура смены пароля будет прервана. В этом случае

для смены пароля обратитесь за помощью к администратору. Если же вам разрешено менять пароль, то на экране появится диалог (рисунок 4.2).

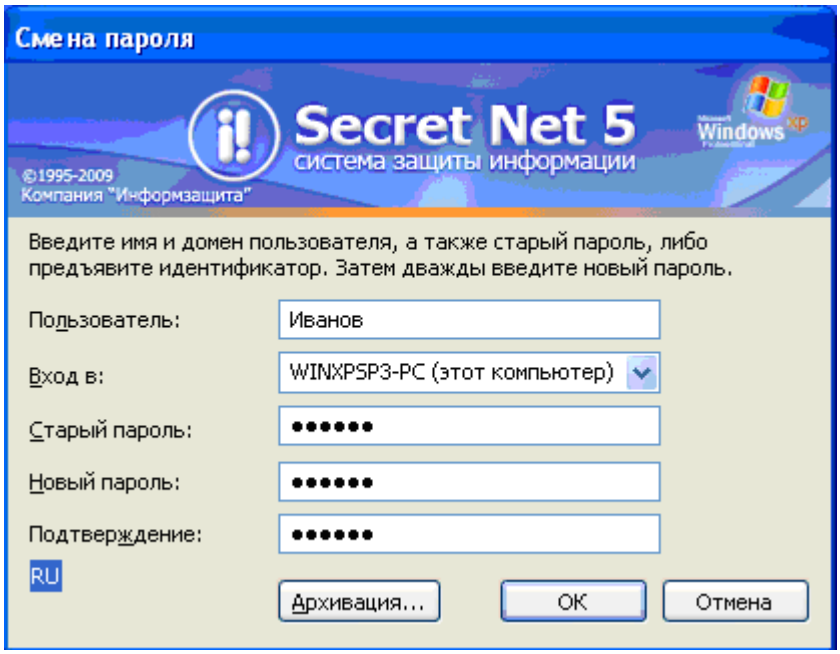

Рисунок 4.2 - Смена пароля

3) Заполните поля диалога:
- в поле "Старый пароль" введите ваш текущий пароль в системе;
- в поле "Новый пароль" введите новый пароль;
- повторите ввод нового пароля в поле "Подтверждение".

В целях безопасности символы пароля не отображаются в явном виде в строке ввода.

Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница. Если требования, предъявляемые в системе к паролям, нарушены или старый пароль указан не правильно, на экране появится сообщение об ошибке. Нажмите кнопку "ОК" в окне сообщения и повторите ввод паролей, указав их правильно. Если поля диалога смены пароля были заполнены правильно, на экране появится сообщение об успешном изменении пароля (рисунок 4.3).

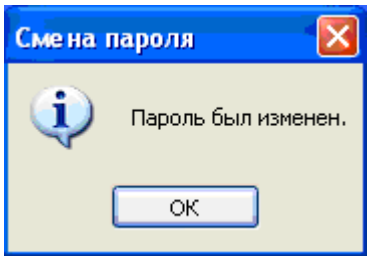

Рисунок 4.3 – Подтверждение изменения пароля

4) Нажмите кнопку "ОК".

4.3 Временная блокировка компьютера

Если вам необходимо временно прервать работу на компьютере, то для защиты от несанкционированного использования совсем не обязательно его выключать. Можно

воспользоваться функцией временной блокировки компьютера, при которой блокируется клавиатура и экран монитора.

Разблокировать компьютер может только работающий на нем пользователь или администратор. Разблокирование компьютера администратором сопровождается завершением текущего сеанса работы пользователя и потерей всех несохраненных данных.

Временную блокировку можно выполнить нажатием кнопки "Блокировка" на консоли "Безопасность Windows".

Этот способ не связан с настройками и применяется независимо от предоставленных пользователю прав. В системе предусмотрена автоматическая блокировка компьютера. Она включается, если в течение определенного времени не использовалась клавиатура и мышь. Такое время называется интервалом неактивности. Для включения автоматической блокировки необходимо, чтобы предварительно пользователем была выполнена настройка: выбрана и установлен интервал неактивности, отличный от 0.

Для настройки механизма блокировки компьютера:

1) На рабочем столе щелкнуть правой кнопкой мыши, откройте окно настройки свойств экрана и перейдите на вкладку "Заставка" (рисунок 4.4).
2) В списке доступных заставок выберите любое название, отличное от "Нет".
3) Установите значение параметра "Интервал" (3мин).
4) Нажмите кнопку "Применить" или "ОК".

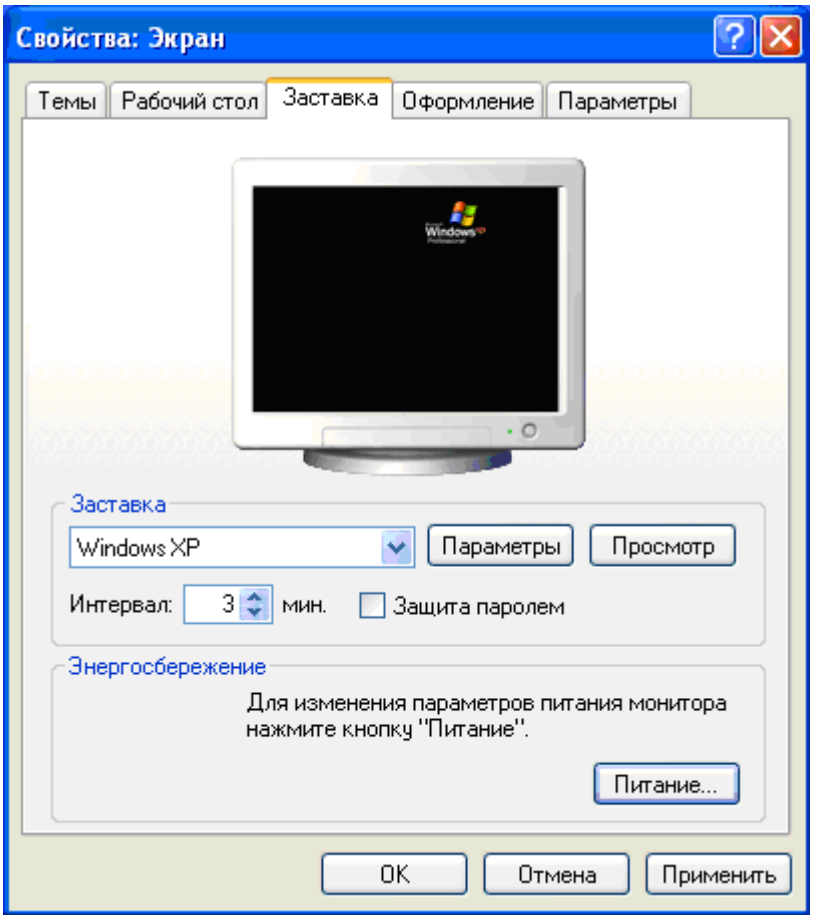

Рисунок 4.4 – Настройка параметров блокировки

4.3.1 Блокировка с помощью консоли

Для включения блокировки с консоли "Безопасность Windows":

1) Вызовите диалог "Безопасность Windows", нажав комбинацию клавиш <Ctrl>+ <Alt>+<Del>.
2) Нажмите кнопку "Блокировка". Клавиатура и экран будут заблокированы, а на экране появится сообщение (рисунок 4.5).

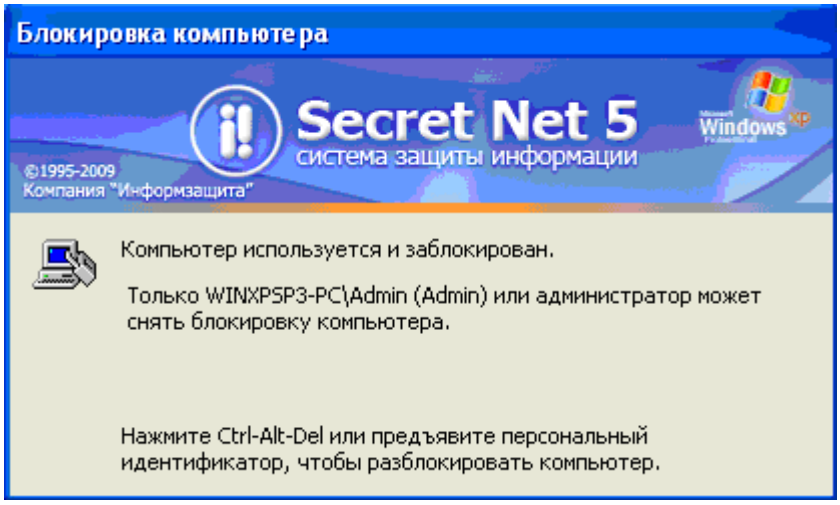

Рисунок 4.5 – Блокировка компьютера

Если предварительно вами была выбрана заставка, по истечении определенного времени, соответствующего интервалу неактивности, на экране заблокированного компьютера появится заставка, выбранная при настройке механизмов блокировки.

4.3.2 Как снять временную блокировку компьютера

Для разблокировки компьютера:

1) Нажмите комбинацию клавиш <Ctrl>+ <Alt>+<Del>.

На экране появится диалог для ввода учетных данных пользователя, где будет отображаться имя текущего пользователя. Если на компьютере используется устройство аппаратной идентификации, предъявите персональный идентификатор.

Если в идентификаторе отсутствует пароль или используется стандартный режим входа, система защиты предложит вам ввести пароль с клавиатуры.

2) Введите свой пароль.
3) Нажмите кнопку "ОК".

4.4 Завершение сеанса работы в Windows XP

Если вам необходимо закончить свою работу на компьютере и, не выключая его, предоставить возможность работать другому пользователю, вы должны завершить сеанс работы в Windows XP.

Для завершения сеанса работы:

1) Нажмите комбинацию клавиш <Ctrl>+ <Alt>+<Del>.
2) В диалоге "Безопасность Windows" нажмите кнопку "Выход из системы".
3) Нажмите кнопку" ОК".

После завершения сеанса на экране появится стандартное приглашение на вход в систему. Следующий пользователь должен будет выполнить вход в систему.

4.5 Перезагрузка и выключение компьютера

Для перезагрузки или выключения компьютера:

1) Нажмите комбинацию клавиш <Ctrl>+ <Alt>+<Del>.
2) В диалоге "Безопасность Windows" нажмите кнопку "Завершение работы".

На экране появится запрос для выбора режима завершения работы (рисунок 4.6).

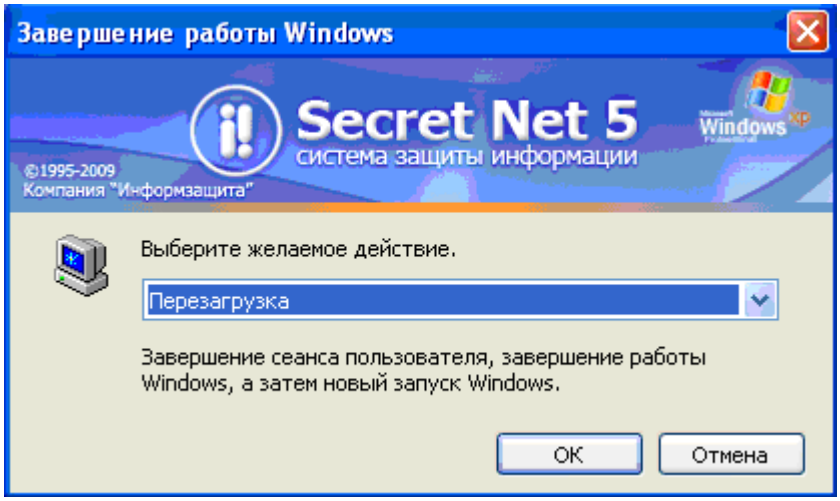

Рисунок 4.6 - Перезагрузка компьютера

3)Откройте список возможных значений и выберите режим завершения работы:

- завершение сеанса <имя пользователя>;
- завершение работы;
- перезагрузка;
- переход в ждущий режим.

4) Нажмите кнопку "ОК" для выполнения выбранного действия.
5) Для отказа от завершения работы нажмите кнопка "Отмена".

Для завершения сеанса работы можно использовать и стандартные средства Windows XP. Нажмите кнопка "Пуск", выберите в меню команду "Завершение работы" (рисунок 4.7) .

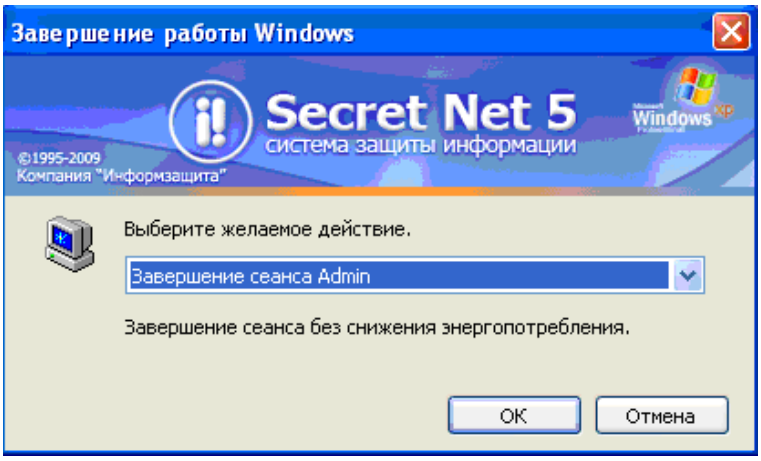

Рисунок 4.7 – Завершение работы Windows

Далее в появившемся диалоге выберите значение " Завершение сеанса <имя пользователя>" и нажмите кнопку "ОК".

Внимание!

В данной лабораторной работе используется только автономная версия программы Secret Net 5.1, т.е. рассматриваются только локальные пользователи.

5 Задание

При выполнении лабораторной работы необходимо выполнить следующие действия:

1. Войти в систему под именем "Администратор" с соответствующим паролем (пароль спросить у преподавателя);
2. Посмотреть состав пользователей компьютера;
3. Настроить общие ограничения на пароль;
4. Создать нового пользователя с именем User1 и любым паролем. Затем пользователя с именем User2 соответственно. Настроить персональные ограничения на пароль. (Имя и пароль пользователя запомнить для дальнейшего использования).

4.1 Для М- четных (М- последняя цифра студенческого билета) выполнить типовые действия пользователя:

- смена пароля;
- временная блокировка компьютера с помощью консоли "Безопасность Windows" и настроить механизмы блокировки компьютера;
- завершение сеанса работы в Windows XP средствами системы Secret Net с помощью консоли и с помощью кнопки "Пуск".

4.2 Для М- нечетных выполнить типовые действия пользователя:

- смена пароля;
- временная блокировка компьютера с помощью консоли "Безопасность Windows" и настроить механизмы блокировки компьютера;
- перезагрузка компьютера средствами системы Secret Net с помощью консоли и с помощью кнопки "Пуск".

6 Содержание отчета

Отчет должен содержать:

- формулировку цели;
- описание сценария лабораторной работы;
- выводы о проделанной работе.

7 Контрольные вопросы

1) Каково назначение системы Secret Net 5.1?
2) Какие режимы и соответствующие способы входа в систему существуют?
3) Сколько пользователей входит в состав компьютера?
4) Как создать нового пользователя?
5) Какие существуют ограничения на пароль?
6) Как устанавливаются персональные ограничения на пароль?
7) Как можно осуществить смену пароля?
8) Какие типовые операции выполняются с помощью диалогового окна Безопасность Windows?
9) Как настроить механизм блокировки компьютера?
10) Каким образом можно временно заблокировать компьютер?
11) Как разблокировать компьютер?
12) Как осуществляется завершение сеанса работы в Windows XP?
13) Как осуществить перезагрузку и выключение компьютера?

Лабораторная работа №2.

«Управление доступом и защита ресурсов в системе Secret Net 5.1»

Содержание

Лабораторная работа №2

«Управление доступом и защита ресурсов в системе Secret Net 5.1»

1 Подготовка рабочего места

На рабочем месте установлена автоматизированная система Secret Net 5.1. В системе существует учетная запись Администратора: уровень допуска – строго конфиденциально, привилегия – управление категориями конфиденциальности, полный доступ к дискам и портам. На системе включены механизмы разграничения доступа: избирательное разграничение доступа к устройствам, полномочное управление доступом и замкнутая программная среда. Режим контроля печати конфиденциальных документов отключен, контроль потоков отключен, механизм разграничения доступа к устройствам функционирует в «жестком» режиме.

2 Цель работы

Целью лабораторной работы является изучение принципов защиты ресурсов с помощью управления доступом и приобретение навыков администрирования системы защиты информации Secret Net 5.1.

3 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.

4 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 (рисунок 4.1).

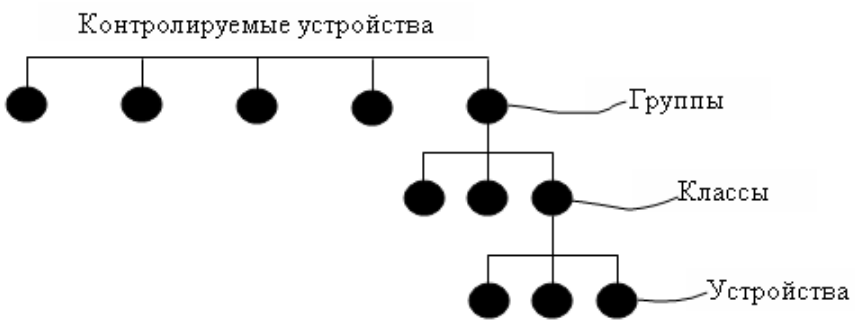

Рисунок 4.1 – Иерархия устройств в Secret Net 5.1

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» (рисунок 4.2).

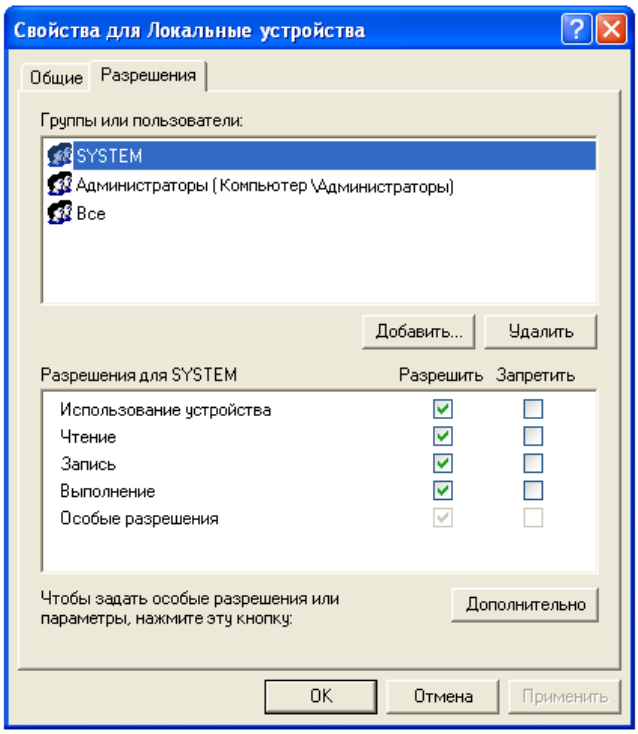

Рисунок 4.2 – Диалог «Разрешения»

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.

6) 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».

7) 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…».

8) В диалоге настройки свойств объекта нажмите кнопку «ОК».

9) 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 «ОК».

5 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.

4) Включите или отключите действие режима, установив отметки в соответствующих полях.
5) Для включения контроля потоков в расширенном режиме установите отметку в поле «Расширенный контроль вывода информации».
6) 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».

5.1 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 5.1).

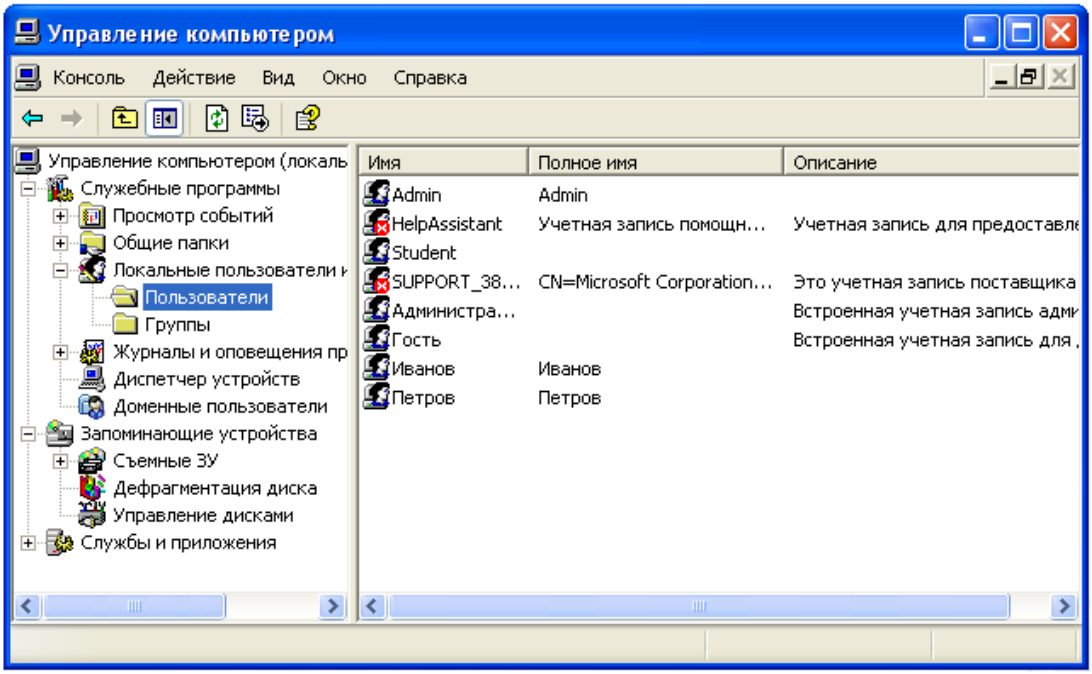

Рисунок 5.1 – Список зарегистрированных в системе пользователей

3) Вызовите окно настройки свойств пользователя и перейдите к диалогу «Secret Net 5».

4) В панели выбора режима выберите режим «Доступ» (рисунок 5.2).

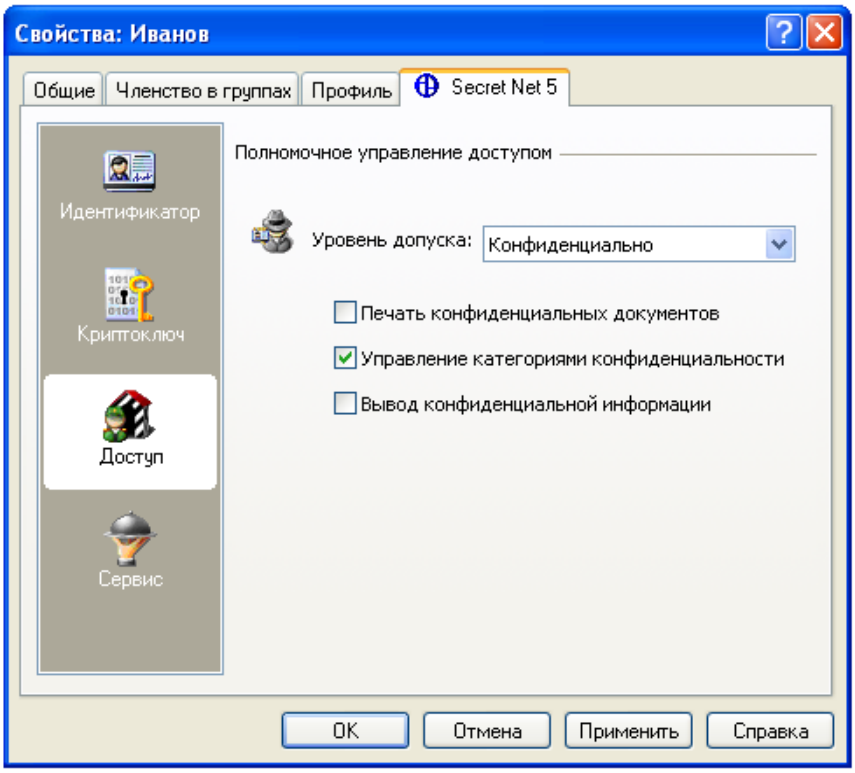

Рисунок 5.2 – Назначение пользователю уровня допуска и привилегий

5) Установите уровень допуска пользователя в одноименном поле.

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

6) 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.

7) Нажмите кнопку «OK».

Параметры вступят в силу при следующем входе пользователя в систему.

5.2 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 5.3).

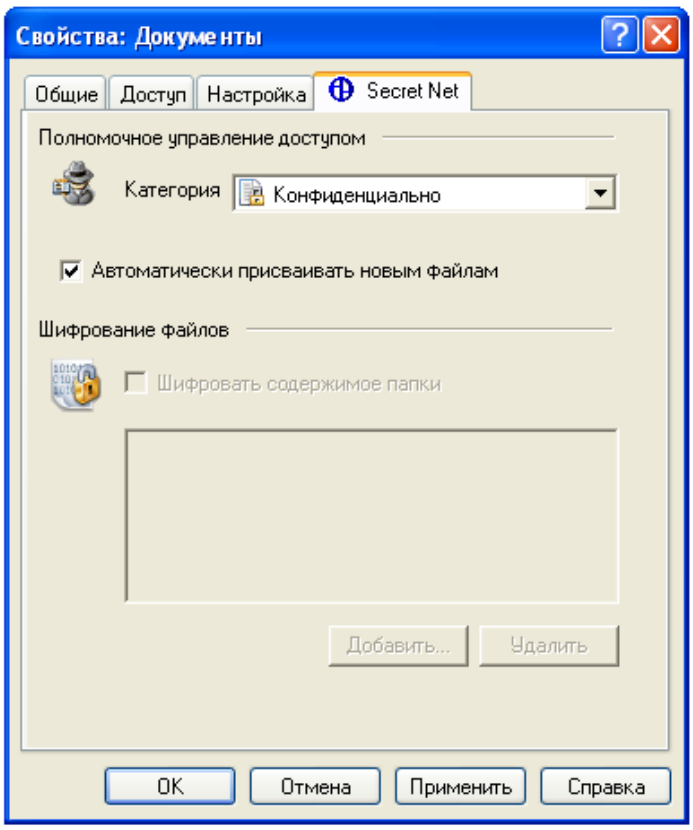

Рисунок 5.3 – Изменение категории конфиденциальности каталога

2) 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».

3) Нажмите кнопку «OK».

Если каталог содержит файлы и подкаталоги, на экране появится диалог, предлагающий изменить категории конфиденциальности файлам и подкаталогам (рисунок 5.4).

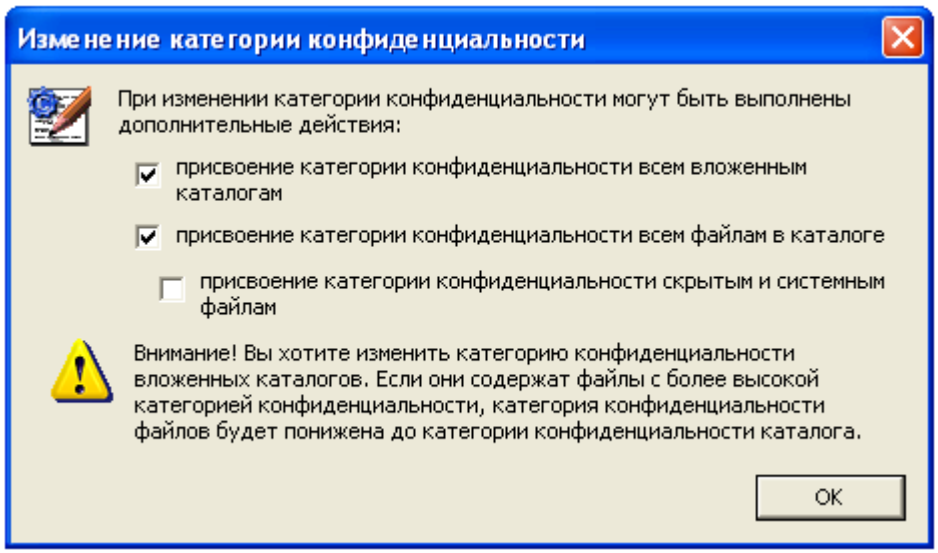

Рисунок 5.4 – Изменение категории конфиденциальности вложенных в каталог файлов и подкаталогов

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 5.5).

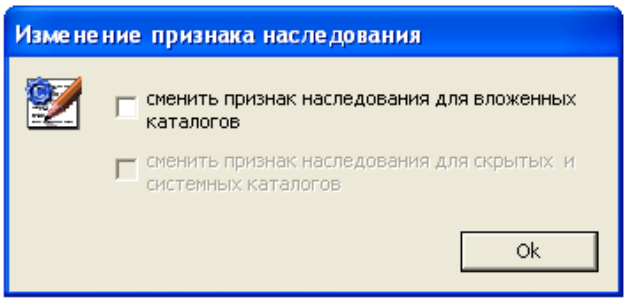

Рисунок 5.5 – Изменение признака наследования

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 «ОК».

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 5.6).

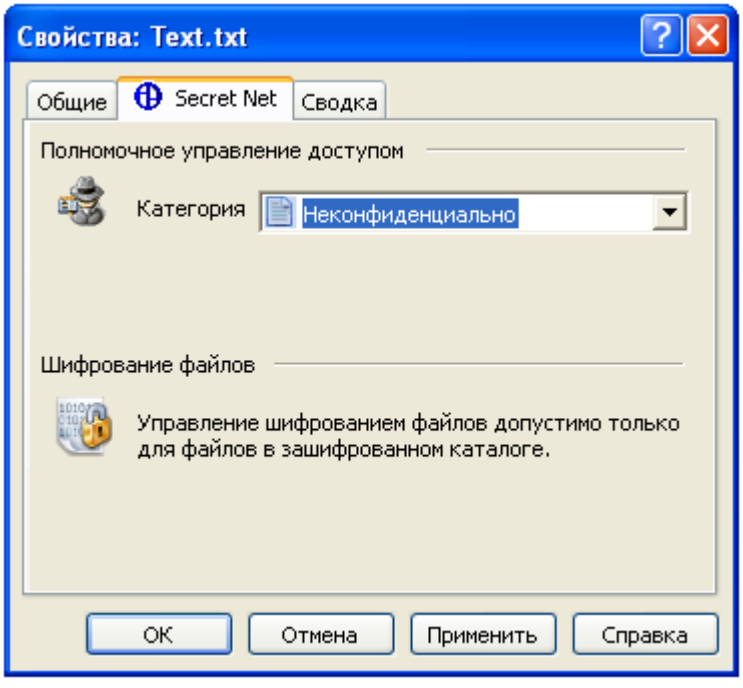

Рисунок 5.6 – Изменение категории конфиденциальности файла

4) Выберите в раскрывающемся списке поля «Категория» нужную категорию конфиденциальности файла.
5) Нажмите кнопку «ОК».

6 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 6.1.

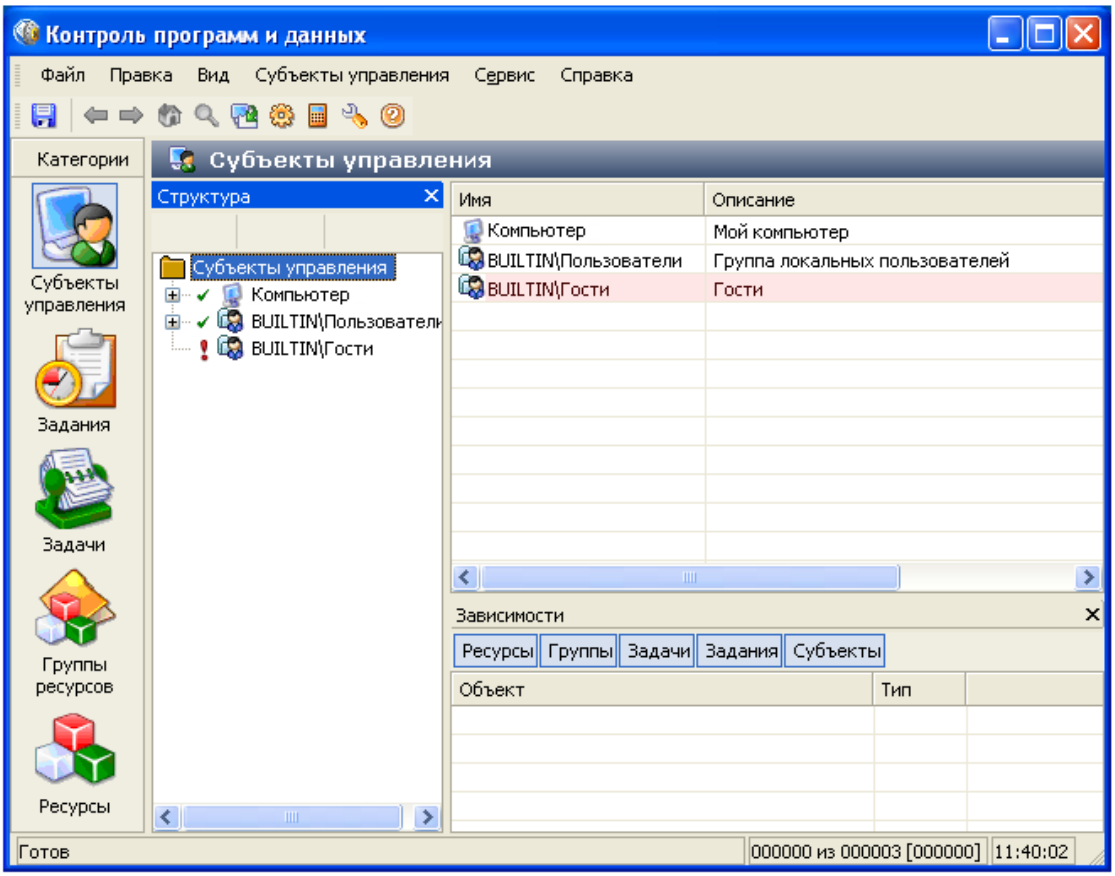

Рисунок 6.1 – Интерфейс программы «Контроль программ и данных»

6.1 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.

6.1.1 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 6.2).

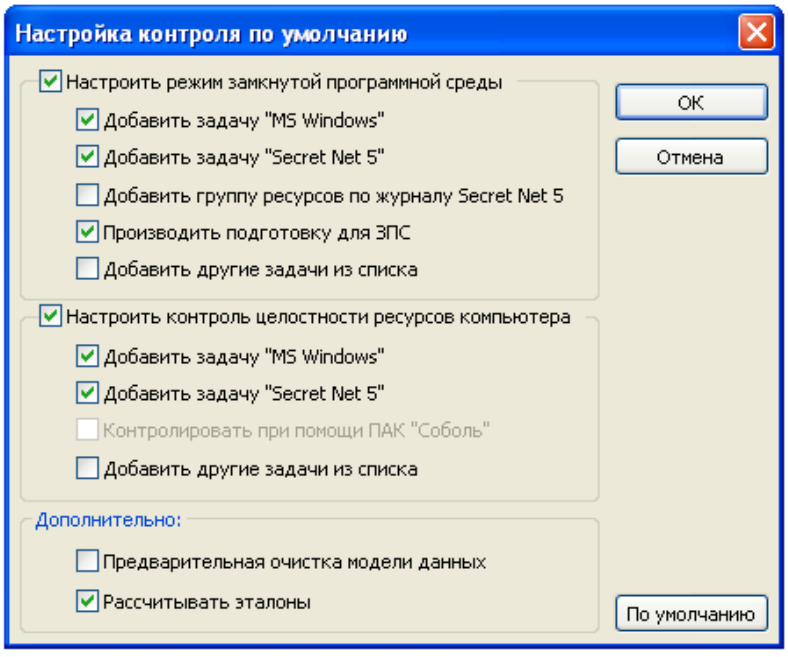

Рисунок 6.2 – Настройка контроля по умолчанию

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.

В 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 6.3).

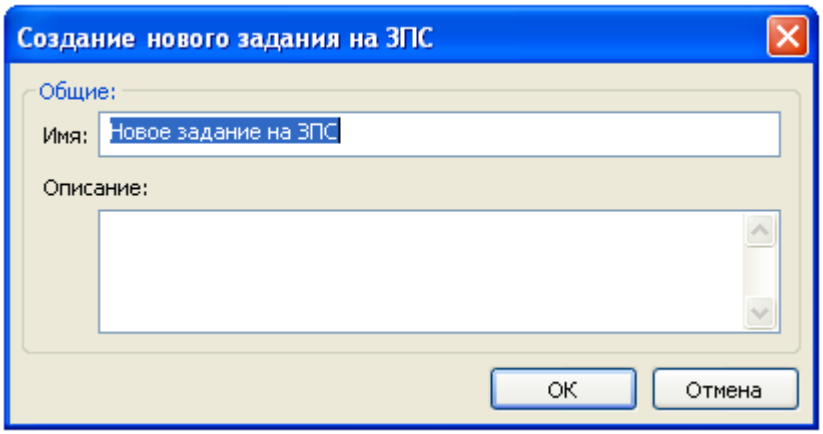

Рисунок 6.3 – Создание нового задания на ЗПС

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

6.1.3 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 6.4).

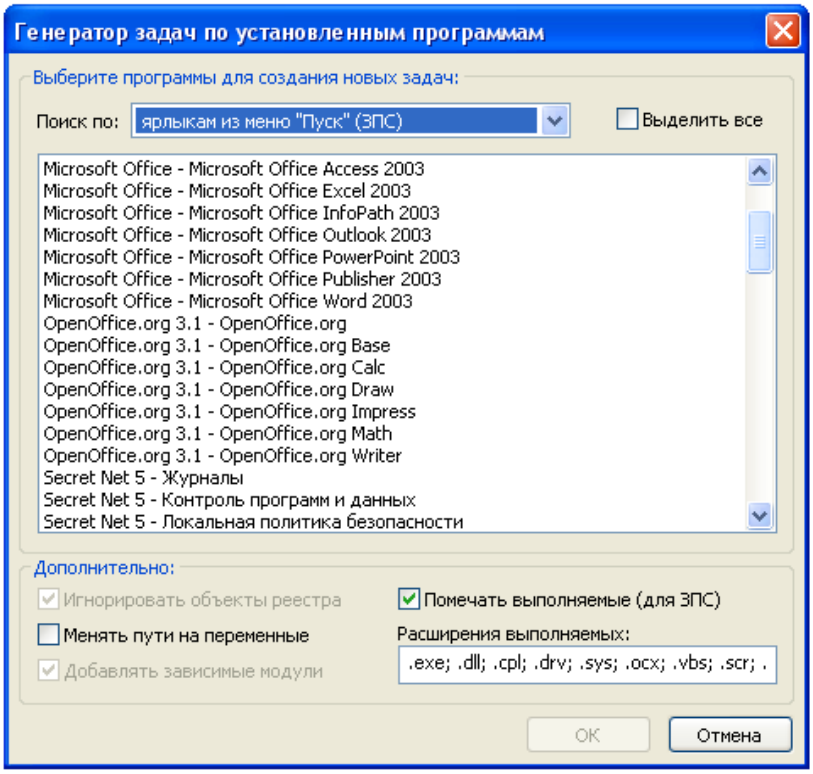

Рисунок 6.4 – Создание задач по установленным программам

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

2) Выберите в поле «Поиск по» – «ярлыкам из меню «Пуск» (ЗПС)».

3) 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.

6.1.4 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.

3) Выберите задачи, включаемые в задание.

4) Нажмите кнопку «OK».

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

6.1.5 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».

6.1.6 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».

6.1.7 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.

3) Выберите задания ЗПС, которые требуется назначить субъекту.

4) Нажмите кнопку «OK».

Выбранные задания будут назначены субъекту.

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

6.2 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.

3) Удалите из списка или добавьте в него расширения файлов, для которых должен быть установлен признак «выполняемый».

4) 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».

6.3 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».

3) Установите отметку в поле «Режим ЗПС включен» и удалите отметку из поля «Мягкий» режим» (если она там установлена).

4) 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.

5) Нажмите кнопку «ОК».

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

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

7 Выполнение лабораторной работы

1 Вход в систему и изучение параметров системы.

1.1 Зайдите в систему под учетной записью Администратора:

- имя пользователя – Администратор;
- пароль – _____ (пароль необходимо спросить у преподавателя).

1.2 Вызовите оснастку для управления параметрами объектов групповой политики и 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 C:\ создайте иерархию каталогов:

- C:\Folder1\Folder2\
- C:\Folder3\Folder4\

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

- C:\Folder1\text1.txt
- C:\Folder1\Folder2\text2.txt
- C:\Folder3\text3.txt
- C:\Folder3\Folder4\text4.txt

Для М-четных (М – последняя цифра номера студенческого билета):

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».

2.3 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».

2.4 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».

Для М - нечетных (М – последняя цифра номера студенческого билета):

2.5 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».

2.6 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».

2.7 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.

3.1 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).

3.2 Попробуйте поменять права доступа на системный диск (C:). Сделайте вывод.

4 Предварительная настройка механизма замкнутой программной среды.

Для М-четных:

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 C:\WINDOWS\system32\calc.exe. Выберите все файлы кроме C:\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 (см. пп. 6.2-6.3).

Для М-нечетных:

4.2 Откройте программу «Контроль программ и данных». Для пользователя user1 запретите запуск программы «Блокнот».

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 «Блокнот», не нужно добавлять в группу ресурсов файл C:\WINDOWS\system32\notepad.exe. Выберите все файлы кроме C:\WINDOWS\system32\notepad.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 (см. пп. 6.2-6.3).

4.3 Перезагрузите компьютер.

5 Проверка требований по разграничению доступа.

5.1 Войдите в систему под учетной записью user1.

5.2 Проверка выполнения полномочного управления доступом. Сделайте попытку запустить следующие файлы:

- C:\Folder1\text1.txt;
- C:\Folder1\Folder2\text2.txt;
- C:\Folder3\text3.txt;
- C:\Folder3\Folder4\text4.txt.

Фиксируются факты доступа и отказа в доступе (результаты фиксируются в отчете). Сделайте выводы по результатам проделанной проверки.

5.3 Проверка выполнения разграничения доступа к устройствам. Сделайте попытку:

- открыть файл D:\Secret Net\text5.txt;
- удалить файл D:\Secret Net\text5.txt;
- создать файл D:\Secret Net\text7.txt;
- скопировать файл D:\Secret Net\text5.txt в C:\Folder1\Folder2\;
- скопировать в каталог D:\Secret Net\ любой файл из каталога C:\Secret Net\.

Сделайте выводы по результатам проделанной проверки.

5.4 Проверка выполнения настроек замкнутой программной среды.

Запустите программы «Калькулятор» и «Блокнот». Сделайте вывод о полученном результате.

8 Содержание отчета

Отчет должен содержать:

- формулировку цели работы;
- описание сценария лабораторной работы;
- выводы.

9 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.

Лабораторная работа №3.

«Контроль целостности в системе Secret Net 5.1»

Содержание

Лабораторная работа №3

«Контроль целостности в системе Secret Net 5.1»

1 Цель работы

Изучить принцип работы и получить практические навыки по работе с системой контроля целостности.

2 Основные понятия

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютеров. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

3 Модель данных

Параметры, определяющие работу механизмов контроля целостности и замкнутой программной среды, объединены в рамках единой модели данных. Модель данных (МД**)** 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.

3.1 Структура

Объекты одной категории являются подчиненными или вышестоящими по отношению к объектам другой категории. Так ресурсы являются подчиненными по отношению к группам ресурсов, а группы — задачам. 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.

Модель данных состоит из двух частей. Одна часть относится к замкнутой программной среде, другая — к контролю целостности. Набор заданий для каждой из этих частей модели свой. Задачи, группы ресурсов и ресурсы могут входить как в одну, так и в другую часть модели.

3.2 Построение фрагмента модели данных по умолчанию

Выполнение этого этапа требуется только при формировании новой модели данных.

1) Нажмите кнопку «Пуск» и выберите в главном меню Windows команду «Программы | Secret Net 5 | 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:

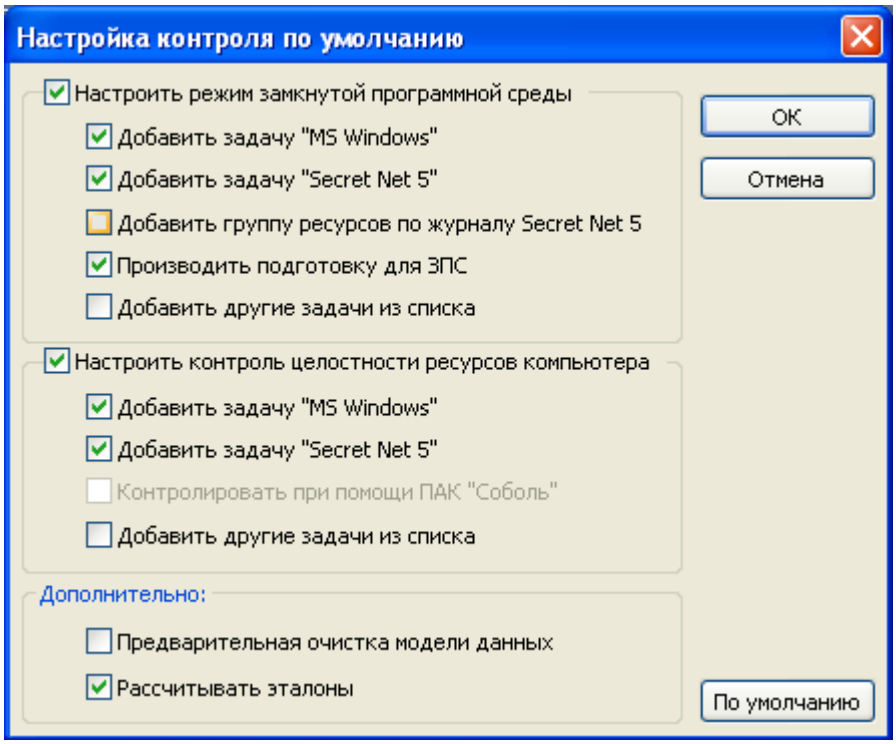

Рисунок 3.1 – Создание новой модели данных

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.

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».

3.3 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 ПО. Кроме того, можно задать дополнительное условие фильтрации отбираемых ресурсов.

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

3.3.1 Добавление в модель данных задач с помощью механизма генерации

1) Выберите в меню «Сервис» команду «Генератор задач». На экране появится диалог:

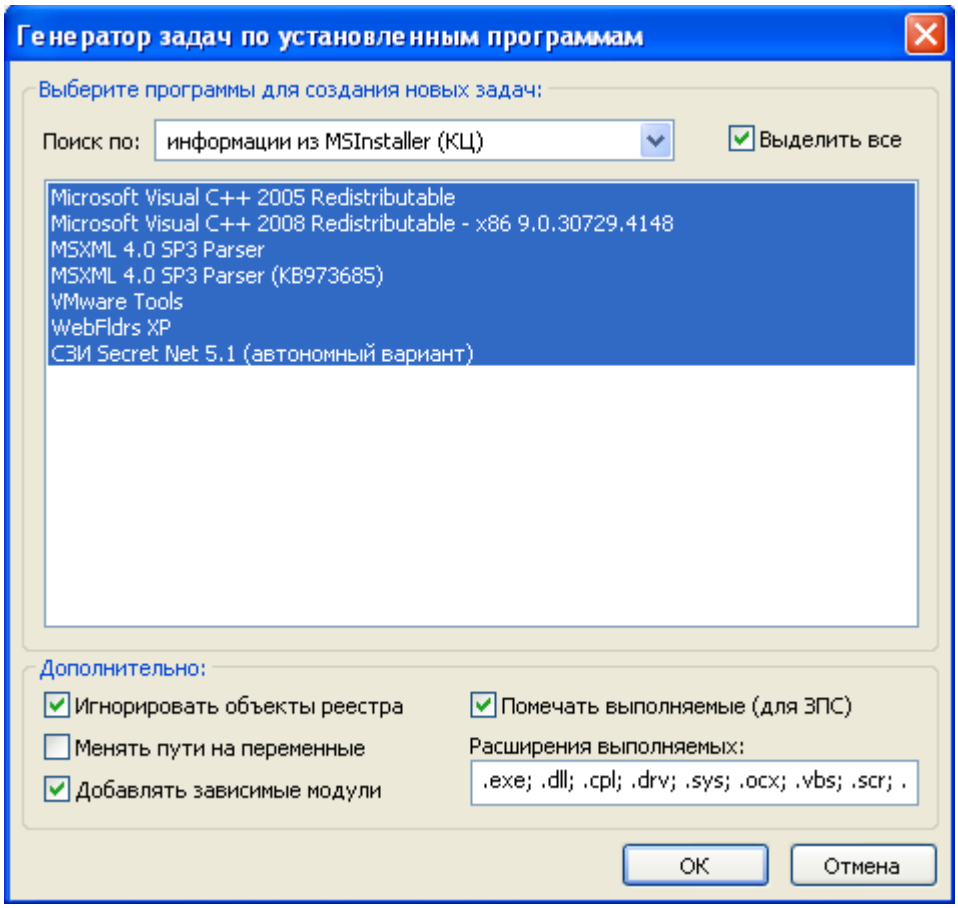

Рисунок 3.2 – Добавление задач с помощью механизма генерации

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

2) Укажите в поле «Поиск по» — из какого списка должны выбираться программы.
3) 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».

Условия отбора ресурсов:

- **игнорировать объекты реестра.** Ресурсы, являющиеся объектами реестра, в задачи не включаются;

- **менять пути на переменные.** При записи в модель данных абсолютные пути к файлам и каталогам меняются на имена системных переменных окружения ОС Windows;
- **добавлять зависимые модули.** К списку ресурсов задачи добавляются программные модули, связанные динамическими зависимостями с исполняемыми файлами выбранного ПО;
- **помечать выполняемые.** Выполняемые файлы при отображении в окне программы управления помечаются специальным значком. 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 (верхняя половина кружка окрашена красным цветом).
6) Активируйте в меню команду «Файл | Сохранить».

3.3.2 Добавление 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. При добавлении в модель данных задачи вручную необходимо включить в эту задачу необходимые ресурсы.
3) Активируйте в меню команду «Файл | Сохранить».

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».

3.4 Добавление 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». Для выбора нескольких ресурсов используйте клавишу <Ctrl>. Для выделения всего списка поставьте отметку в поле «Выделить все». Выбранные ресурсы будут добавлены в группу.
3) Активируйте в меню команду «Файл | Сохранить».

3.5 Добавление заданий и включение в них задач

Цель данного этапа — сформировать задания на основе задач, созданных на предыдущем этапе.

1) Выберите категорию «Задания» и активируйте в меню «Задания | Создать задание». На экране появится диалог выбора типа задания
2) Выберите тип задания (КЦ) и нажмите кнопку «ОК». На экране появится диалог:

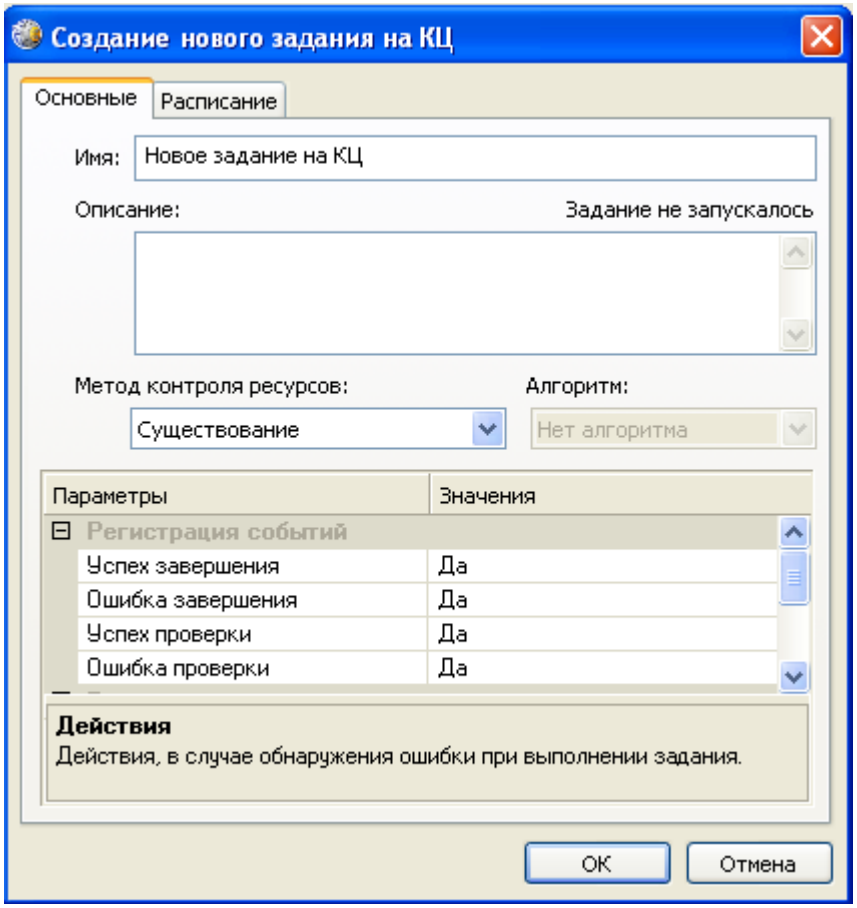

Рисунок 3.3 – Создание нового задания на КЦ (Основные)

3) Введите имя задания и краткое описание задания КЦ
4) Укажите метод контроля ресурсов, выбрав его из списка. Предусмотрено 4 метода:
   - **содержимое.** Целостность содержимого ресурсов;
   - **атрибуты.** Стандартные атрибуты, установленные для ресурсов;
   - **права доступа.** Категории конфиденциальности и атрибуты доступа Windows (дескриптор безопасности), установленные для ресурсов;
   - **существование.** Наличие ресурсов по заданному пути.

   При выборе типа контролируемых данных необходимо иметь в виду, что проверка будет выполняться только для определенных типов ресурсов. Сведения о применимости методов контроля для каждого из типов ресурсов в зависимости от выбранного типа контролируемых данных приведены ниже. При выборе метода контроля может оказаться, что с заданием связаны ресурсы, несовместимые с используемым в задании алгоритмом. Это довольно типичная ситуация, когда на контроль ставится комплексная задача, состоящая из большого количества разнородных ресурсов. Такой ситуации не следует опасаться — несовместимые ресурсы подсистемой контроля игнорируются. При расчете эталонов желательно на несовместимые ресурсы использовать реакции: "игнорировать" или "выводить запрос". Таким образом, можно связывать с задачей сразу несколько разных заданий на контроль, не беспокоясь, что наличие несовместимых с заданиями ресурсов вызовет сбои или НСД.

Таблица 3.1 - Соответствие типов ресурсов и методов контроля

	Содержимое объекта	**Атрибуты объекта**	**Права доступа**	**Существование объекта**
Файл	да	да	Да	да
Каталог	нет	да	Да	да
Ключ реестра	да	нет	Да	да
Значение реестра	да	нет	Нет	да

5) Настройте регистрацию событий. Для этого в столбце "Параметры" выберите нужное событие. В соответствующей строке столбца "Значения" появится значок раскрывающегося списка. Выберите в списке значение "Да", чтобы данное событие регистрировалось, или "Нет", чтобы оно не регистрировалось. Предусмотрена регистрация 4-х событий:
   - **успех завершения.** Обработка задания контроля завершена успешно;
   - **ошибка завершения.** Обнаружено нарушение целостности;
   - **успех проверки.** Проверка целостности ресурса завершена успешно;
   - **ошибка проверки.** Нарушение целостности ресурса.
6) Настройте реакцию системы. Для этого выделите в столбце "Параметры" строку "Действие", а в столбце "Значения" выберите нужный вариант. Предусмотрены следующие варианты:
   - **игнорировать.** Реакция системы отсутствует;
   - **заблокировать компьютер.** Компьютер блокируется. Снять блокировку может только администратор безопасности;
   - **восстановить из эталона.** Текущее значение контролируемого параметра ресурса восстанавливается из эталона;
   - **восстановить с блокировкой.** Текущее значение контролируемого параметра ресурса восстанавливается из эталона. Компьютер блокируется. Снять блокировку может только администратор безопасности;
   - **принять как эталон.** Текущее значение контролируемого параметра ресурса принимается за эталон.
7) Перейдите к диалогу "Расписание" и составьте расписание контроля в соответствии с требованиями к заданию.

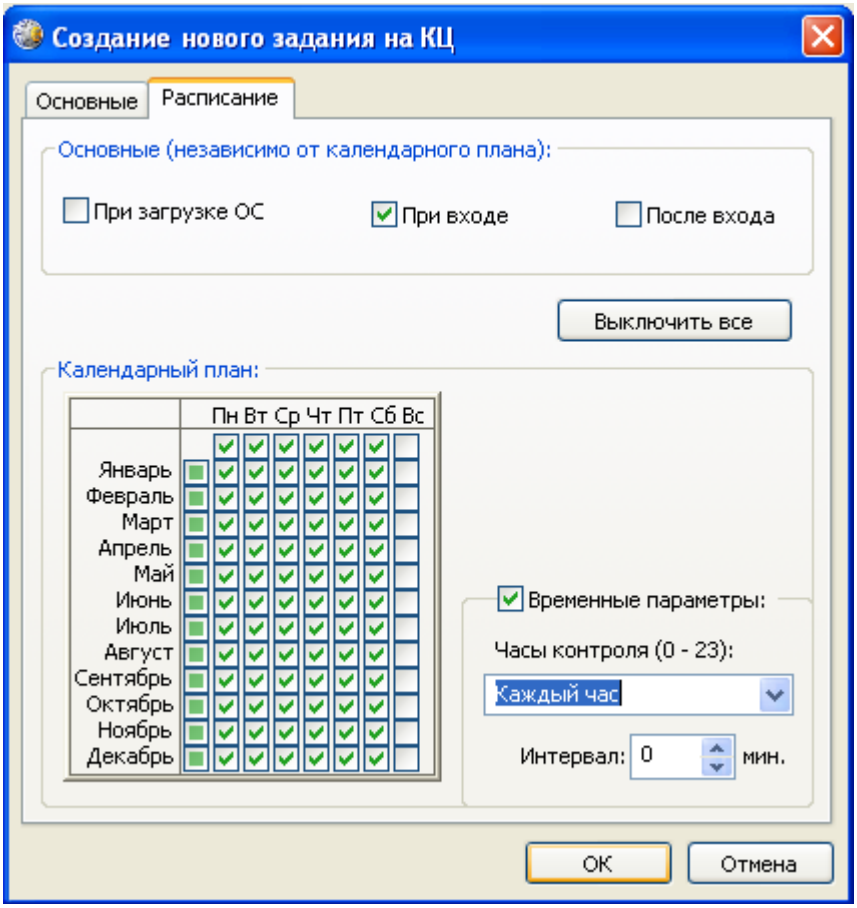

Рисунок 3.4 - Создание нового задания на КЦ (Расписание)

Диалог разделен на две части. В верхней части настраивается время проведения проверки независимо от календаря (при загрузке операционной системы, при входе пользователя в систему и после входа в систему). В нижней части расположен календарь и средства настройки расписания в течение суток:

- **календарный план.** Группа полей для включения контроля по месяцам, дням недели, часам и минутам;
- **календарь.** С помощью календаря можно указать расписание контроля по месяцам и дням недели;
- **временные параметры.** С помощью полей этой группы можно указать периодичность контроля в течение суток;
- **часы контроля.** Введите или выберите из раскрывающегося списка значение периодичности контроля в течение суток. Можно выбрать период, а можно и непосредственно ввести конкретные значения. Следует иметь ввиду, что отсчет начинается с нулевого часа;
- **интервал.** Укажите периодичность контроля в течение часа контроля. Если значение не указано, контроль выполняется в начале часа один раз. Так, например, если контроль должен производиться в 7 часов, а в поле «Интервал» указано значение 10, то процесс контроля первый раз начнется в 7 часов 00 минут, а затем будет повторяться каждые 10 минут в течение этого часа;
- **основное (расписание).** С помощью полей этой группы можно указать, на каком этапе своей работы система защиты должна контролировать целостность ресурсов. Проверка может проводиться при загрузке операционной системы, при входе пользователя в систему и после входа в систему. В режиме "При входе" проверка начинается после ввода пользователем идентификационных признаков, и до завершения проверки процесс входа в систему приостанавливается. Если установлен режим "После

входа" — проверка начнется после входа пользователя в систему и продолжается в фоновом режиме.

8) Нажмите кнопку "OK". В дополнительном окне структуры появится новое задание контроля целостности, не связанное с субъектами.

Включение задач в задание:

1) Выберите категорию «Задание» 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.
3) Выберите задачи, включаемые в задание. Для выбора нескольких задач используйте клавишу <Ctrl> или поле «Выделить все».
4) Нажмите кнопку «OK».
5) Активируйте в меню команду «Файл | Сохранить».

3.6 Расчет эталонов

Расчет может быть выполнен сразу для всех или для отдельных имеющихся в модели заданий КЦ. Перед проведением расчета эталонов необходимо настроить реакцию системы на возможные ошибки, которые могут возникнуть в процессе расчета. При перерасчете эталонов может возникнуть необходимость сохранения прежних ("старых") значений. Это связано с ситуацией, которая может возникнуть при автоматическом обновлении программного обеспечения на компьютере. Рассмотрим подробно, как могут развиваться события во времени:

1) До появления в сети нового ПО текущий эталон соответствуют прежнему ПО.
2) На сервере обновлений появляется новое ПО, выполняется расчет новых эталонов. Новое ПО готово к установке, но пользователь откладывает установку на более поздний срок.
3) Проверка эталонных значений может быть намечена на любой момент. И если проверка будет выполнена до установки нового ПО, обнаружится несоответствие прежнего ПО новым эталонным значениям. Для этого случая и сохраняются старые эталоны.
4) После обновления ПО на компьютере начинают использоваться новые эталоны.

Для расчета эталонов:

1) Активируйте в меню «Сервис» команду «Расчет эталонов». На экране появится одноименный диалог.
2) Если требуется сохранить старые значения эталонов, установите отметку в поле «Режим».
3) Настройте реакцию системы защиты на возможные ошибки при расчете эталонов. Для этого в левой части таблицы выберите вид ошибки, а в правой для него выберите одно из 4-х значений реакции системы. Ошибки могут быть трех видов:
   - метод / алгоритм расчета для данного ресурса не поддерживается;
   - к ресурсу нет доступа на чтение или он заблокирован;
   - ресурс по указанному пути не найден.

Для каждого вида ошибки можно задать одну из 4-х реакций:

- **игнорировать.** Реакция системы на ошибку отсутствует;
- **выводить запрос.** При возникновении ошибки система выводит соответствующее сообщение и запрос на выполнение последующих действий;
- **удалять ресурс.** При возникновении ошибки ресурс удаляется из модели данных;
- **снимать ресурс с контроля.** Ресурс снимается с контроля, но остается в модели данных. При этом нужно учитывать, что ресурс будет снят с контроля не только в том задании, где выявлена ошибка, но и во всех остальных заданиях, с которыми ресурс связан.

4) Нажмите кнопку «OK». Начнется расчет эталонов. Ход выполнения расчета отображается в специальном окне полосой прогресса. Если в процессе расчета обнаруживается ошибка, и в качестве реакции на нее установлено значение «Выводить запрос», процедура будет приостановлена и на экране появится запрос на продолжение процедуры. Предусмотрено 4 варианта продолжения процедуры:

- **игнорировать.** Процедура расчета будет продолжена. Реакция системы на ошибку отсутствует. Ресурс, вызвавший ошибку, остается в составе задачи (или задач). Проверка целостности этого ресурса вызовет событие НСД с соответствующей реакцией;
- **снять с контроля.** Процедура расчета будет продолжена. Ресурс, вызвавший ошибку, остается в составе задачи (или задач), снимается с контроля и не проверяется во всех заданиях, в которые входит;
- **удалить.** Процедура расчета будет продолжена. Ресурс, вызвавший ошибку, автоматически удаляется из модели данных;
- **прервать.** Процедура расчета будет прервана. Для расчета эталонов следует устранить причину, вызвавшую ошибку.

5) Для выбора варианта продолжения процедуры нажмите соответствующую кнопку в окне сообщения. В зависимости от выбранного варианта процедура будет продолжена или прервана, в каждом из этих случаев на экране появится сообщение.
6) Примите к сведению содержание сообщения и нажмите кнопку «OK».
7) Активируйте в меню команду «Файл | Сохранить».

3.7 Включение механизма КЦ

Механизм контроля целостности будет включен, как только компьютеру будет назначено задание на контроль целостности с заданным расписанием. Для включения механизма контроля целостности:

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 в нем команду "Добавить задание | Существующие".

Появится диалог, содержащий список заданий контроля целостности.

3) Выберите нужные задания и нажмите кнопку "OK".

Для данного компьютера начнет действовать механизм КЦ.

3.8 Проверка заданий

Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности параметров заданий. Проверка заключается в немедленном выполнении задания независимо от расписания. Такая проверка позволяет предотвратить нарушения в работе пользователей, связанные с некорректной настройкой заданий, и своевременно исправить ошибки, допущенные в настройках. По завершении проверки выдается список обнаруженных ошибок. В режиме полной имитации события регистрируются, и система отрабатывает реакцию на ошибки.

Для запуска проверки:

1) Выберите в меню "Сервис | Запуск задания". Появится диалог со списком всех заданий контроля целостности.
2) Выберите в списке задание, при необходимости укажите режим полной имитации и нажмите кнопку "OK". Начнется выполнение задания и по окончании будет выведено сообщение об успешном завершении или обнаруженных ошибках.

4 Выполнение лабораторной работы

1. Первый этап. Установка первичных параметров контроля целостности

1.1 Войдите в систему под учетной записью «Администратор». Нажмите кнопку «Пуск» и выберите в главном меню Windows команду «Программы | Secret Net | Контроль программ и данных». Нажмите кнопку «ОК».

Внимание!

При запуске программы "Контроль программ и данных" в момент выполнения задания на контроль целостности или в момент выполнения синхронизации система выдает сообщение: "В результате загрузки модели данных произошла ошибка. Идет обработка базы данных контроля целостности". В этом случае дождитесь завершения выполнения процесса, после чего повторите попытку запуска программы или нажмите клавишу <F5>.

1.2 Добавление нового ресурса в модель данных:

Для М-четных :

1) Выберите категорию «Ресурсы» и активируйте в меню команду «Ресурсы | Создать ресурс | Одиночный». Тип ресурса: Каталог. Имя ресурса можно ввести вручную: C\Folder3. Либо выполнить поиск ресурса в диалоговом режиме, используя для вызова диалога кнопку «Обзор».
2) Нажмите кнопку «ОК».
3) Активируйте в меню команду «Файл | Сохранить».

Для М-нечетных:

1) Выберите категорию «Ресурсы» и активируйте в меню команду «Ресурсы | Создать ресурс | Одиночный». Тип ресурса: Каталог. Имя ресурса можно ввести вручную: C\Folder1. Либо выполнить поиск ресурса в диалоговом режиме, используя для вызова диалога кнопку «Обзор».
2) Нажмите кнопку «ОК».
3) Активируйте в меню команду «Файл | Сохранить».

Внимание!

Уровни конфиденциальности используемых ресурсов должны остаться неизменными после л/р №2.

1.3 Добавление новой группы ресурсов:

1) Выберите категорию «Группы ресурсов» и активируйте команду «Группы ресурсов | Создать группу | Вручную…».
2) Введите имя группы ресурсов, ее краткое описание, в поле «Тип» выберите «Файлы/Каталоги» и нажмите кнопку «ОК».
3) Активируйте в меню команду «Файл | Сохранить».

1.3.1 Включение ресурса в группу ресурсов:

1) Выберите категорию «Группы ресурсов» на панели категорий.
2) В окне структуры вызовите контекстное меню для группы ресурсов и активируйте команду «Добавить ресурсы | Существующие».
3) Выберите ресурсы, включаемые в задание.
4) Нажмите кнопку «ОК».
5) Активируйте в меню команду «Файл | Сохранить».

1.4 Добавление новой задачи

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

1.4.1 Включение группы ресурсов в задачи

1) Выберите категорию «Задачи» на панели категорий.

2) В окне структуры вызовите контекстное меню для задачи и активируйте команду «Добавить группы | Существующие».
3) Выберите группы, включаемые в задание.
4) Нажмите кнопку «OK».
5) Активируйте в меню команду «Файл | Сохранить». Затем необходимо создать задание и включить в него задачу.

1.5 Формирование задания

1) Выберите категорию «Задания» и активируйте в меню «Задания | Создать задание».
2) Выберите тип задания (КЦ) и нажмите кнопку «OK».
3) Введите имя и краткое описание задания.
4) Укажите метод контроля ресурсов «Существование».
5) Настройте регистрацию событий. Выберите «Да», чтобы данное событие регистрировалось.
6) Настройте реакцию системы. Для этого выделите в столбце «Параметры» строку «Действие», а в столбце «Значения» выберите «Восстановить из эталона».
7) Перейдите к диалогу «Расписание». В верхней части диалога настройте время проведения проверки: при входе. Сформируйте календарный план проведения контроля – все дни, кроме воскресенья, периодичность контроля в течение суток – каждый час с нулевым интервалом.
8) Нажмите кнопку «OK».

1.6 Включение задач в задание

1) Выберите категорию «Задание» 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».

1.7 Расчет эталонов

1) Активируйте в меню «Сервис» команду «Расчет эталонов». Если требуется сохранить старые значения эталонов, установите отметку в поле «Режим».
2) Настройте реакцию системы защиты на ошибки при расчете эталонов. Для этого для каждого вида ошибки выберите значение «Выводить запрос».
3) Нажмите кнопку «OK».

1.8 Включение механизма контроля целостности

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 в нем команду "Добавить задание | Существующие".

Появится диалог, содержащий список заданий контроля целостности.

3) Выберите нужные задания и нажмите кнопку "OK".

Для данного компьютера начнет действовать механизм КЦ.

2 Проверка выполнения заданий контроля целостности, установленных в п.1

Для М-четных:

2.1 Удалите каталог C\Folder3.

Внимание!

Удаление должно производиться используя клавиатуру – del+shift либо необходимо задать параметры для корзины: удалять не помещая в корзину.

1) Откройте программу «Контроль программ и данных».
2) Выберите в меню «Сервис | Запуск задания». Появится диалог со списком всех заданий контроля целостности. Выберите в списке задание.

3) Нажмите кнопку «ОК». Убедитесь в наличии ошибки контроля целостности при выполнении этого задания.

4) Перезагрузите систему. Убедитесь, что каталог C\Folder3 восстановлен.

Для М-нечетных:

2.1 Удалите каталог C\Folder3.

Внимание!

Удаление должно производиться используя клавиатуру – del+shift либо необходимо задать параметры для корзины: удалять не помещая в корзину.

1) Откройте программу «Контроль программ и данных».

2) Выберите в меню «Сервис | Запуск задания». Появится диалог со списком всех заданий контроля целостности. Выберите в списке задание.

3) Нажмите кнопку «ОК». Убедитесь в наличии ошибки контроля целостности при выполнении этого задания.

4) Перезагрузите систему. Убедитесь, что каталог C:\Folder3 восстановлен.

3 Второй этап. Установка первичных параметров контроля целостности

3.1 С помощью аналогичных операций, описанных на первом этапе, создайте новую модель данных со следующими параметрами:

Для М-четных:

- имя ресурса: C:\Folder1; тип ресурса: «Каталог»
- Задание: «Существование», параметры задания идентичны первому этапу, кроме настройки реакции системы. Настройка реакции системы: Выделите в столбце «Параметры» строку «Действие», а в столбце «Значения» выберите «Восстановить с блокировкой».

Для М-нечетных:

- имя ресурса: C:\Folder3; тип ресурса: «Каталог»
- Задание: «Существование», параметры задания идентичны первому этапу, кроме настройки реакции системы. Настройка реакции системы: Выделите в столбце «Параметры» строку «Действие», а в столбце «Значения» выберите «Восстановить с блокировкой».

4 Проверка выполнения заданий контроля целостности, установленных в пункте 3

4.1 Убедитесь, что user2 имеет уровень доступа: «Строго конфиденциально». Если он не имеет этих прав, назначьте ему их. (Смотреть л/р №2)

Для М-четных:

4.2 Завершите сеанс «Администратор». Зайдите в систему под учетной записью user1.

4.3 Удалите ресурс C:\Folder1. Заметьте, что при категории конфиденциальности «Строго конфиденциально» данная операция была бы невозможна. Подумайте почему.

Внимание!

Помимо установления прав доступа пользователю в программе Secret Net 5.1, также необходимо предоставить права на удаление, используя возможности Windows (в свойствах папки).

4.4 Завершите сеанс user1. Зайдите в систему под учетной записью user2. Почему пользователь не смог зайти в систему?

4.5 Завершите сеанс user2. Зайдите в систему под учетной записью «Администратор». Проверьте наличие ресурса C:\Folder1.

Для М-нечетных:

4.2 Завершите сеанс «Администратор». Зайдите в систему под учетной записью user1.

4.3 Удалите ресурс C:\Folder3. Заметьте, что при категории конфиденциальности «Строго конфиденциально» данная операция была бы невозможна. Подумайте почему.

Внимание!

Помимо установления прав доступа пользователю в программе Secret Net 5.1,также необходимо предоставить права на удаление, используя возможности Windows (в свойствах папки).

4.4 Завершите сеанс user1. Зайдите в систему под учетной записью user2. Почему пользователь не смог зайти в систему?

4.5 Завершите сеанс user2. Зайдите в систему под учетной записью «Администратор». Проверьте наличие ресурса C:\Folder3.

Внимание!

После выполнения данной лабораторной работы уровни конфиденциальности используемых ресурсов должны остаться такими же, как и после л/р №2. Восстановите их, войдя через «Администратора».

5 Содержание отчета

Отчет должен содержать:

- формулировка цели работы;
- описание сценария лабораторной работы;
- выводы.

6 Контрольные вопросы

1) Дайте определение целостности информации
2) На чем основано действие механизма целостности?
3) Какие типы ресурсов существуют?
4) Что собой представляет модель данных?
5) Почему нельзя удалить ресурс с помещением в корзину?
6) Что собой представляет задание на контроль целостности?
7) Каким образом связаны между собой все 5 категорий объектов в модели?
8) Что значит поле «Восстановить из эталона» в диалоге настроек задания реакции системы?
9) Что значит поле «Восстановить с блокировкой» в диалоге настроек задания реакции системы?
10) Как добавить новый ресурс в модель данных?
11) Что собой представляет механизм генерации задач?
12) Для чего при перерасчете эталонов сохраняют старые значения?
13) Как устанавливаются связи между объектами в модели данных?
14) Что собой представляет проверка корректности запуска заданий?