Факультет компьютерных наук
Кафедра информационной безопасности

КОНТРОЛЬНЫЕ ЗАДАНИЯ ПО МЕТОДАМ И СРЕДСТВАМ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Задание 1.

1. Загрузите оснастку "Управление компьютером", выберите пользователя и вызовите диалоговое окно "Свойства".
2. Перейдите к диалогу "Secret Net 5". В режиме "Идентификатор" в диалоге "Secret Net 5" отображаются сведения о персональных идентификаторах, присвоенных пользователю
Сведения представлены в виде списка идентификаторов. Для каждого идентификатора приводится следующая информация:
-тип и серийный номер;
-признак хранения в идентификаторе закрытых ключей — текущего и предыдущего;
-признак хранения пароля;
-разрешение на использование идентификатора в ПАК "Соболь" (признак интеграции).

Задание 2.

1. Выберите пользователя, вызовите диалоговое окно "Свойства" и перейдите к диалогу "Secret Net 5". В диалоге "Secret Net 5" отображаются сведения о персональных идентификаторах, присвоенных пользователю.
2. Запустите программу "Мастер присвоения персональных идентификаторов", для этого в диалоге "Secret Net 5" нажмите кнопку "Присвоить".
3. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".
Если выбрана операция "Записать пароль в идентификатор", "Разрешить вход в ПАК "Соболь" или "Записать в идентификатор закрытый ключ пользователя", на экране появится диалог мастера, отображающий ход выполнения операций ввода данных и диалоги для ввода данных.
4. Введите пароль пользователя и нажмите кнопку"OK".

Задание 3.

1. В оснастке "Управление компьютером" откройте папку "Служебные программы | Локальные пользователи и группы | Пользователи".
2. В правой части окна программы вызовите контекстное меню для ярлыка с именем нужного пользователя и активируйте в нем команду "Задать пароль". Появится стандартный диалог для ввода пароля
3. Дважды введите новый пароль пользователя и нажмите кнопку "OK".

Задание 4.

В Secret Net 5.0 предусмотрено 3 режима входа пользователей в систему:
Стандартный. Имя и пароль пользователя вводятся с клавиатуры.
Смешанный. Для входа в систему пользователь должен предъявить идентификатор или ввести имя и пароль с клавиатуры. Такой режим используется на этапе ввода системы защиты в эксплуатацию, когда еще не все пользователи получили персональные идентификаторы.
Только по идентификатору. Для входа в систему пользователь должен предъявить идентификатор. Данный режим обеспечивает максимальную защищенность и используется при наличии идентификатора у каждого пользователя. Режим входа в систему устанавливается администратором безопасности средствами редактирования локальной политики безопасности и распространяется на всех пользователей компьютера.
Изменение режима входа в систему
1. Вызовите оснастку "Локальная политика безопасности", раскройте узел "Параметры безопасности" и перейдите к папке "Настройки подсистем". В правой части появится список политик. Настройка режима входа осуществляется в политике "Вход в систему: режим входа пользователя". (По умолчанию действует смешанный режим).
2. Вызовите контекстное меню для политики "Вход в систему: режим входа пользователя" и активируйте в нем команду "Свойства". Появится диалог выбора режима
3. Для задания нужного режима поставьте отметку в соответствующем поле переключателя и нажмите кнопку "OK".

Задание 5.

Автоматическая блокировка компьютера, включаемая в том случае, если в течение определенного

времени не использовались клавиатура и мышь, настраивается каждым пользователем индивидуально. Администратор безопасности имеет возможность установить максимальное значе
ние интервала неактивности, распространяющееся на всех пользователей защищаемого компьютера. В этом случае пользователь не сможет установить интервал неактивности, превышающий значение, заданное администратором безопасности.

Задание максимального значения интервала неактивности:

1. Вызовите оснастку "Локальная политика безопасности", раскройте узел "Параметры безопасности" и перейдите в папку "Параметры Secret Net".

2. Раскройте папку "Настройки подсистем". В правой части появится список политик.

3. Вызовите контекстное меню для политики "Вход в систему: максимальный период неактивности до блокировки экрана" и активируйте в нем команду "Свойства". Появится диалог выбора режима.

4. Для задания максимального периода неактивности установите нужное значение и нажмите кнопку "OK".

Задание 6.

1. Вызовите оснастку "Локальная политика безопасности".

2. Откройте узел "Параметры Secret Net" и выберите папку "Устройства". В правой части появится список устройств. Параметр контроля объектов может быть унаследован от вышестоящих объектов или задан явно. В списке объекты, для которых параметр контроля задан
явно, помечаются отметкой зеленого цвета. По умолчанию для групп и устройств параметр контроля задан явно, а для классов — наследуется от групп.

3. Выберите в списке устройство (объект), для которого необходимо изменить параметр контроля, и вызовите окно настройки его свойств. Появится окно свойств устройства. Для объектов с явно заданными параметрами контроля поле "Использовать заданные здесь настройки" содержит отметку. Если отметка отсутствует, это означает, что параметр контроля для данного объекта наследуется от вышестоящего объекта (для устройства вышестоящим является класс, а для класса — группа).

4. Если данное устройство должно наследовать политику от вышестоящего элемента иерархии (группы или класса), установите отметку в поле "Наследовать настройки контроля от родительского объекта". Если для данного устройства требуется задать явно политику контроля, установите отметку в поле "Использовать заданные здесь настройки" и измените нужным образом состояние выключателя "Не контролировать параметры устройства":

-удалите отметку — чтобы включить контроль устройства;

-установите отметку — если нужно снять устройство с контроля;

5. Нажмите кнопку "OK".

Задание 7.

1. Вызовите оснастку "Локальная политика безопасности".

2. В узле "Параметры Secret Net" выберите папку "Настройки подсистем". В правой части окна появится список параметров (политик).

3. Выберите в списке параметр "Контроль устройств: режим работы" и вызовите окно настройки его свойств.

4. Выберите требуемый режим работы и нажмите кнопку "OK".

Задание 8.

В "мягком" и "жестком" режимах работы механизма при обнаружении системой изменений в аппаратной конфигурации на экран выводится соответствующее сообщение, а пиктограмма Secret Net на панели задач меняет свой цвет на красный. В "жестком" режиме работы механизма также выполняется блокировка компьютера. Снять блокировку компьютера и утвердить изменения в аппаратной конфигурации может только администратор безопасности — пользователь, входящий в локальную группу администраторов

Для утверждения конфигурации:

1. Вызовите контекстное меню к пиктограмме Secret Net на панели задач и выберите команду "Утвердить изменения в конфигурации". На экране появится диалог.

2. Нажмите кнопку "Утвердить" для утверждения изменений. В результате подключенное или отключенное устройство (или устройства) будет учтено в составе эталонной аппаратной конфигурации. При этом пиктограмма Secret Net на панели задач примет обычный цвет — синий.

Избирательное разграничение доступа к устройствам

Для настройки этого механизма необходимо:

1. Назначить права доступа пользователей к устройствам.

2. Настроить регистрацию событий и аудита.

3. Включить нужный режим работы механизма.

После настройки функции администратора безопасности сводятся к поддержке работы механизма:

- корректировке прав доступа в соответствии с изменениями в политике безопасности и с добавлением в систему новых устройств и новых пользователей;
- настройке регистрации событий и анализу нарушений;
- управлению режимом работы механизма.

Задание 9.

Для настройки прав доступа используется список устройств. Для того чтобы установить права доступа к отдельному устройству, устройство должно быть включено в список. Для просмотра списка устройств:

1. Вызовите оснастку "Локальная политика безопасности".

2. Раскройте узел "Параметры Secret Net" и выберите папку "Устройства".

3. В правой части оснастки появится список устройств

Как упоминалось ранее, при формировании списка автоматически устанавливаются права доступа 3-х групп пользователей к группам устройств. По умолчанию для всех групп устройств устанавливаются разрешения на все операции (полный доступ), запреты — не определены. Права доступа для групп устройств заданы явно. В списке это отображается отметкой **красного цвета**, стоящей перед наименованием группы (отметки **зеленого цвета** используются в механизме
контроля аппаратной конфигурации).

В системе поддерживается механизм наследования разрешений. Для всех классов устройств по умолчанию включен признак наследования разрешений. Поэтому пользователям, входящим в 3 указанные группы, по умолчанию разрешен полный доступ ко всем классам устройств. Если изменить права доступа для класса, перед его наименованием в списке появится отметка красного цвета.

Задание 10.

1. Выберите в списке объект (группу, класс или устройство), вызовите контекстное меню и активируйте команду "Свойства". Или наведите курсор на название устройства и дважды нажмите левую кнопку мыши. Появится диалоговое окно для настройки свойств устройства. По умолчанию режим наследования параметров от родительского объекта отключен и действуют параметры, заданные явно.

2. Если требуется включить наследование параметров, установите отметку в поле "Наследовать настройки контроля от родительского объекта". После этого будут доступны параметры подключения и отключения устройства.

3. Удалите или установите отметки в параметрах подключения и отключения и перейдите к диалогу "Разрешения". Можно изменить права доступа для родительского объекта (для группы) и затем, используя принцип наследования, применить их к классу.

4. Для изменения параметров доступа выберите в списке группу пользователей или пользователя и затем расставьте разрешения для каждой операции.

5. Нажмите кнопку "Применить".

Если требуется назначить права доступа к данному устройству другим пользователям или группам, отсутствующим в списке верхней части диалога, их следует добавить в список .

6. В диалоге настройки свойств объекта нажмите кнопку "OK". Диалог закроется.

7. Если требуется изменить параметры доступа и контроля для другого устройства, найдите его в списке и повторите шаги **1 — 6**.

8. Для сохранения изменений нажмите на панели инструментов кнопку "Сохранить настройки политики контроля устройств".

Задание 11.

1. Выберите в списке устройство (группу, класс), вызовите диалоговое окно настройки его свойств и перейдите к диалогу "Разрешения".

2. Нажмите кнопку "Добавить", расположенную под списком групп пользователей. Появится стандартный диалог выбора пользователя или группы.

3. Выберите пользователя или группу, которым необходимо установить права доступа к данному объекту и нажмите кнопку "OK". Диалог закроется, а выбранные пользователи или группы появятся в списке диалога "Разрешения":

4. Выберите в списке вновь добавленного пользователя (группу) и расставьте для него разрешения и запреты на доступ к данному объекту, учитывая принцип наследования параметров от родительских объектов дочерними.

5. Нажмите кнопку "Применить".

6. Если требуется предоставить права доступа к данному устройству другому пользователю или группе, отсутствующим в списке, повторите шаги **2 — 5**.

7. Для завершения работы с диалогом нажмите кнопку "OK".

8. По окончании процесса настройки закройте оснастку.

При появлении предупреждения об изменениях в политике контроля устройств нажмите кнопку "Да".

Задание 12.

1. Выберите в списке устройство или группу (класс), вызовите диалоговое окно настройки его свойств и перейдите к диалогу "Разрешения".

2. Выберите пользователя или группу и расставьте запреты на операции доступа.

3. Нажмите кнопку "Применить".

4. Нажмите кнопку "OK" в диалоговом окне настройки свойств устройства. Диалоговое окно закроется.

5. Закройте оснастку.

При появлении предупреждения об изменениях в политике контроля устройств нажмите кнопку "Да".

Задание 13.

Настройка выполняется отдельно по каждому устройству, зарегистрированному в списке устройств компьютера.

1. Вызовите оснастку "Локальная политика безопасности", раскройте узел "Параметры Secret Net" и раскройте папку "Устройства".

2. Выберите в списке устройство, вызовите контекстное меню и активируйте команду "Свойства". Или наведите курсор на название устройства и дважды нажмите левую кнопку мыши. Появится окно настройки свойств устройства.

3. Перейдите к диалогу "Разрешения" и нажмите кнопку "Дополнительно". Появится диалоговое окно "Параметры управления доступом".

4. Перейдите к диалогу "Аудит".

В диалоге представлен список установленных для данного устройства элементов аудита (элементами аудита являются "отказ", "успех", "все").

Для каждого элемента приводятся следующие параметры:

- имя — группа или пользователь, для которых назначен аудит;
- доступ — вид доступа (чтение, запись, особый и т.д.);
- применять — признак наследования, применяемый к данной группе или классу устройств.

5. Для просмотра или изменения настройки аудита выделенного в списке элемента нажмите кнопку "Показать / Изменить". Появится диалог с описанием элемента аудита, детализированным по операциям (вид доступа). Расставьте отметки в соответствии с требованиями аудита для данного устройства и данной группы пользователей и нажмите кнопку "OK". Диалог с описанием элемента закроется. Для настройки необходимо, чтобы в списке были представлены все пользователи (группы пользователей), доступ которых к данному устройству будет отслеживаться в рамках аудита.

6. В диалоге "Аудит" нажмите кнопку "Добавить". Появится стандартный диалог выбора пользователя (группы).

7. Выберите пользователя (группу), для которого необходимо настроить аудит, и нажмите кнопку "OK". Появится окно настройки аудита для выбранного пользователя (группы).

8. Расставьте отметки в соответствии с политикой аудита в отношении данного пользователя (группы). Нажмите кнопку "OK". Окно настройки аудита закроется и в списке появится новый элемент аудита.

Задание 14.

1. Вызовите оснастку "Локальная политика безопасности" и раскройте папку "Настройки подсистем". В правой части появится список политик. Настройка режима осуществляется в политике "Разграничение доступа к устройствам: режим работы".

2. Вызовите контекстное меню для политики "Разграничение доступа к устройствам: режим работы" и активируйте в нем команду "Свойства". Появится диалог выбора режима

3. Выберите нужный режим (мягкий) и нажмите кнопку "OK".

Задание 15.

Для назначения уровня допуска и привилегий:

Назначение уровня допуска и привилегий осуществляется в оснастке "Управление компьютером".

1. Выберите пользователя, откройте окно настройки его свойств и перейдите к диалогу "Secret Net 5".

2. Перейдите в режим "Доступ". Появится диалог включения / отключения режима контроля печати.

3. Установите переключатель в нужное положение и нажмите кнопку "OK".

4. Откройте оснастку "Управление компьютером" и у каждого пользователя компьютера проверьте, а при необходимости, установите или удалите привилегию "Печать конфиденциальных документов".

Присвоение категории конфиденциальности ресурсу

Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS или NTFS5. Категория конфиденциальности присваивается ресурсу пользователем, обладающим необходимыми правами или привилегией "Управление категориями конфиденциальности".

Задание 16.

Выбор (изменение) режима работы механизма полномочного разграничения доступа осуществляется администратором безопасности в узле "Параметры Secret Net" оснастки "Локальная политика безопасности".

1. В узле "Параметры Secret Net" выберите папку "Настройки подсистем". В правой части появится список политик.

2. Вызовите контекстное меню для политики "Полномочное управление доступом: режим работы" и активируйте в нем команду "Свойства". Появится диалог выбора режима работы.

3. Включите или отключите контроль потоков и если необходимо установить расширенный режим, поставьте отметку в соответствующем поле.

4. Нажмите кнопку "OK".

Задание 17.

При необходимости можно изменить используемые по умолчанию названия категорий конфиденциальности. Изменение осуществляется в узле "Параметры Secret Net" оснастки "Локальная

политика безопасности".

1. В узле "Параметры Secret Net" выберите папку "Настройки подсистем". В правой части появится список политик.

2. Вызовите контекстное меню для политики "Полномочное разграничение доступа: Названия уровней конфиденциальности" и активируйте в нем команду "Свойства". Появится диалог редактирования названий

3. Введите вручную названия для каждой категории и нажмите кнопку "OK".

Задание 18.

1. Нажмите кнопку "Пуск" ("Start") и выберите в главном меню Windows команду "Все 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 в первый раз, на экране проявится основное окно программы. Чтобы из основного окна перейти к работе с Мастером, выберите в меню "Файл" команду "Новая модель данных". На экране появится стартовый диалог Мастера.

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.

Для настройки механизма ЗПС обязательно нужно выполнить операцию подготовки, при которой для исполняемых файлов осуществляется поиск других, связанных с ними модулей. Это основное назначение этой операции, без нее настройка ЗПС будет неполноценной.

2. Оставьте в диалоге настройки по умолчанию (если настройки были изменены, вернитесь в исходное состояние, нажав кнопку "По умолчанию") и 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. Сохраните модель в базе данных, выполнив одно из следующих действий:

- нажмите кнопку "Сохранить модель";
- нажмите комбинацию клавиш <Ctrl>+<S>;
- в меню "Файл" активизируйте команду "Сохранить".

После сохранения модели данных можно приступать к следующему этапу настройки защитных механизмов — составлению списка задач.

Задание 19.

1. Выберите в меню "Сервис" команду "Генератор задач". Появится диалог. Диалог предназначен для выбора программ, а также задания дополнительных условий отбора ресурсов.

2. Укажите в поле "Поиск по" — из какого списка должны выбираться программы.(Предусмотрено два варианта выбора программ: по ярлыкам из меню "Пуск" или по списку MS Installer.)

3. Выберите в списке программы и укажите в нижней части диалога дополнительные условия отбора ресурсов.

4. Нажмите кнопку "OK". Начнется процесс генерации и появится сообщение об успешном его завершении.

5. Нажмите кнопку "OK" в окне сообщения. В модель данных будут добавлены новые задачи.

Задание 20.

1. Выберите категорию "Задания" одним из следующих способов:

- активируйте ярлык категории на панели категорий;
- нажмите комбинацию клавиш <Ctrl>+<2>;
- в меню "Вид" активизируйте команду "Задания".

2. Выберите в меню команду "Задания | Создать задание". Появится диалог выбора типа задания (КЦ или ЗПС)

3. Выберите тип задания и нажмите кнопку "OK". Выберите.

4. Если выбрана замкнутая программная среда (ЗПС). Введите имя задания, его краткое описание и нажмите кнопку "OK". В дополнительном окне структуры появится новое задание, помеченное знаком «!» (что указывает на отсутствие связи задания с другими объектами). Далее перейдите к формированию следующего задания.

5. Если был выбран контроль целостности. Введите имя и краткое описание задания.

6. Укажите метод контроля ресурсов, выбрав его из списка.

7. Если указан метод контроля "Содержимое", укажите алгоритм, выбрав его из списка. Предусмотрено 5 алгоритмов: CRC7, ЭЦП, ХЭШ, имитовставка, полное совпадение.

8. 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", что бы оно не регистрировалось.

9. Настройте реакцию системы на отказ. Для этого выделите в столбце "Параметры" строку "Действие", а

в столбце "Значения" выберите нужный вариант.

10. Перейдите к диалогу "Расписание" и составьте расписание контроля в соответствии с требованиями к заданию.

Задание 21.

1. Выберите категорию "Задание" одним из следующих способов:

- активизируйте ярлык категории на панели категорий;
- нажмите комбинацию клавиш <Ctrl>+<2>;
- в меню "Вид" активизируйте команду "Задание".

2. Выберите в дополнительном окне структуры или в области списка объектов задание, в которое необходимо включить задачу (или задачи), вызовите контекстное меню и выберите команду "Добавить задачи/группы | Существующие". Появится диалог для выбора объектов. В диалоге представлен список всех задач и групп ресурсов, еще не включенных в данное задание.

3. Выберите задачи, которые следует включить в задание.

4. Нажмите кнопку "OK". Выбранные задачи будут включены в задание.

Установление связей субъектов с заданиями ЗПС

На данном этапе необходимо назначить субъектам сформированные задания замкнутой программной среды. Задания назначаются субъектам "пользователь" и "группа пользователей". Первоначально при формировании новой модели данных с помощью Мастера в ней создаются два субъекта: данный компьютер и стандартная группа "Пользователи", зарегистрированная в операционной системе. Для того чтобы назначить задания другим группам или отдельным пользователям, их необходимо добавить в модель данных. Добавить в модель можно как локальных пользователей компьютера, так и доменных.

Задание 22.

1. Выберите категорию "Субъекты управления" одним из следующих способов:

- активизируйте ярлык категории на панели категорий;
- нажмите комбинацию клавиш <Ctrl>+<1>;
- в меню "Вид" активизируйте команду "Субъекты управления".

2. В меню "Субъекты управления" выберите команду "Добавить в список". Появится стандартный диалог выбора пользователей и групп.

3. Выберите пользователя (или пользователей). В нижней части диалога появится список выбранных пользователей.

4. Нажмите кнопку "OK". В окне программы управления появятся новые субъекты, отмеченные знаком «!» (т.е. не связанные с другими объектами).

Задание 23.

1. Выберите категорию "Субъекты управления" одним из следующих способов:

- активизируйте ярлык категории на панели категорий;
- нажмите комбинацию клавиш <Ctrl>+<1>;
- в меню "Вид" активизируйте команду "Субъекты управления".

2. Выберите в дополнительном окне структуры или в области списка объектов пользователя или группу пользователей, с которыми требуется связать задание, вызовите контекстное меню и выберите команду "Добавить задания | Существующие". Появится диалог, содержащий список заданий замкнутой программной среды. (Для каждого задания в списке указано количество субъектов, с которыми оно связано) .

3. Выберите задания, которые требуется назначить субъекту.

Задание 24.

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 и заключается в следующем: администратор безопасности задает перечень расширений файлов, разрешенных для запуска, после чего программа КПД начинает последовательно анализировать имеющиеся в модели данных ресурсы на соответствие заданному перечню расширений. Ресурсу, имеющему расширение, указанное в перечне, устанавливается признак "Выполняемый".

1. Выберите в меню "Сервис" команду "Ресурсы ЗПС". Появится диалог

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 количества ресурсов в модели данных. Если требуется, чтобы были проанализированы только ресурсы, не имеющие признака "выполняемый", удалите отметку.

3. Удалите из списка или введите в него вручную 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. Нажмите кнопку "OK" в окне сообщения.

Задание 25.

Расчет выполняется сразу для всех имеющихся в модели данных заданий на контроль целостности и заданий замкнутой программной среды. Эталоны ресурсов замкнутой программной среды используются при проверке целостности этих ресурсов, выполняемой при запуске пользователем разрешенных программ. 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.

1. Активируйте в меню "Сервис" команду "Расчет эталонов". Появится 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 выделите 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.

4. Нажмите кнопку "OK". Начнется расчет эталонов. Ход выполнения расчета отображается в специальном окне полосой прогресса.

Задание 26.

1. Вызовите оснастку "Локальная политика безопасности".

2. Откройте узел "Параметры Secret Net" и выберите папку "Привилегии". В правой части окна появится список политик.

3. Вызовите контекстное меню для строки "Замкнутая программная среда: мягкий режим" и активируйте в нем команду "Свойства". Появится диалог со списком пользователей, которым предоставлена данная привилегия.

4. Удалите из списка пользователей и группы пользователей, которым требуется включить "жесткий" режим, и нажмите кнопку "OK". Для всех пользователей компьютера, кроме привилегированных пользователей, начнет действовать механизм замкнутой программной среды в "жестком" режиме.

Задание 27.

Механизма контроля целостности будет включен, как только компьютеру будет назначено задание на контроль целостности.

1. Выберите категорию "Субъекты управления" одним из следующих способов:

- активируйте ярлык категории на панели категорий;
- нажмите комбинацию клавиш <Ctrl>+<1>;
- в меню "Вид" активизируйте команду "Субъекты управления".

2. Вызовите контекстное меню для субъекта управления. Для каждого задания в списке указано количество субъектов управления, с которыми оно связано.

3. Выберите задания, которые требуется назначить субъекту.

4. Нажмите кнопку "OK". Теперь механизм контроля целостности включен и может функционировать в штатном режиме.

Вопросы к экзамену по методам и средствам защиты компьютерной информации

1. Современная ситуация в области информационной безопасности.
2. Категории информационной безопасности.
3. Методы «взлома».
4. Криптография. Классификация криптоалгоритмов.
5. Симметричные криптоалгоритмы. Скремблеры.
6. Блочные шифры. Сеть Фейштеля.
7. AES — стандарт блочных шифров США. Общие сведения о конкурсе AES.
8. Финалист AES — шифр MARS.
9. Финалист AES — шифр RC6.
10. Финалист AES — шифр Serpent.
11. Финалист AES — шифр TwoFish. Псевдопреобразование Адамара.
12. Победитель AES — шифр Rijndael.
13. Симметричные криптосистемы. Функции криптосистемы. Алгоритмы создания цепочек.
14. Методы рандомизации сообщений. Генераторы случайных и псевдослучайных последовательностей.
15. Архивация. Общие принципы архивации. Алгоритм Хаффмана.
16. Архивация. Общие принципы архивации. Алгоритм Лемпеля-Зива.
17. Хэширование паролей.
18. Транспортное кодирование.

19. Ассиметричные криптоалгоритмы. Общие сведения.
20. Алгоритм RSA.
21. Технологии цифровых подписей.
22. Механизм распространения открытых ключей.
23. Обмен ключами по алгоритму Диффи-Хеллмана.
24. Протокол Wide-Mouth Frog (Лягушка с широким ртом).
25. Протокол Yahalom.
26. Протокол Needham-Schroeder (Неедхэма-Шредера).
27. Протокол Kerberos.
28. Протокол Otway-Rees (Отвея-Рииса)

СПИСОК ЛИТЕРАТУРЫ

А.П. Алферов и др. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. -М.: Гелиос АРВ, 2002.
Б. Шнайер. Прикладная криптография.- М.: Триумф, 2002.
А. Саломаа. Криптография с открытым ключом. – М.: Мир, 1995.