МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Программно–аппаратный комплекс защиты информации «SECRET NET 5.0», автономный вариант

Методические указания по выполнению лабораторной работы по дисциплине «Безопасность операционных систем и баз данных» для студентов укрупненной группы специальностей 10.00.00

Курск 2017

УДК 621.(076.1)
Составители: М.О. Таныгин.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *И.В. Калуцкий*

Программно–аппаратный комплекс защиты информации «SECRET NET 5.0» , автономный вариант: методические указания по выполнению лабораторной работы по дисциплине «Программно-аппапаратные средства обеспечения информационной безопасности» / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. Курск, 2017. 50 с.: ил., ,Библиогр.: с. 50.

Излагаются методические указания по выполнению лабораторной работы на персональной ЭВМ с программно–аппаратным комплексом защиты информации. Изучается основные возможности системы защиты информации Secret Net 5.0.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность автоматизированных систем», «Информационная безопасность».

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

ОГЛАВЛЕНИЕ

1. ЦЕЛЬ РАБОТЫ

Познакомиться с программно–аппаратной системой разграничения доступа Secret Net 5.0. Овладеть основными приёмами администрирования и управления политикой безопасности средствами Secret Net 5.0

2. НАЗНАЧЕНИЕ И ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ SECRET NET 5.0

Система Secret Net 5.0 предназначена для защиты от несанкционированного доступа к информационным ресурсам компьютеров, функционирующих на платформах операционных систем (ОС) MS Windows 2000 / XP / 2003. Компьютер с установленной системой может работать автономно, без подключения к сети, или в одноранговой сети, или в сети с доменной организацией.

Система Secret Net 5.0 не подменяет стандартные защитные механизмы, предоставляемые ОС Windows, и не ограничивает возможность их использования, а расширяет их за счет дополнительных программных и аппаратных средств.

2.1. Средства безопасности ОС Windows

Secret Net 5.0 использует следующие стандартные компоненты ОС Windows:

- Средства идентификации и аутентификации.
- Средства избирательного управления доступом.
- Механизм временной блокировки компьютера.
- Журнал безопасности Windows.
- Локальная база данных ОС Windows (SAM).

2.2. Механизмы Secret Net 5.0

С помощью программных и аппаратных средств Secret Net 5.0 реализуются следующие защитные механизмы:

1. Механизм контроля входа в систему с использованием аппаратных средств.

2. Механизмы разграничения доступа и защиты ресурсов:

- механизм полномочного разграничения доступа к объектам файловой системы;
- механизм замкнутой программной среды;
- механизм шифрования файлов;
- механизм разграничения доступа к устройствам компьютера;
- механизм затирания информации, удаляемой с дисков компьютера.

3. Механизмы контроля и регистрации:

- механизм функционального контроля;
- механизм регистрации событий безопасности;
- механизм контроля целостности;
- механизм контроля аппаратной конфигурации компьютера.

2.3. Аппаратные средства Secret Net 5.0

В системе Secret Net 5.0 поддерживается работа следующих аппаратных средств, которые можно объединить в три группы (табл. 1).

Таблица 1. - Функции аппаратных средств

Аппаратные средства	Основные функции
УВИП на базе идентификатора eTokenR2 и eToken Pro	1. Хранение данных для идентификации и аутентификации. 2. Хранение персональной криптографической информации.
Secret Net Touch Memory Card	1. Чтение данных для идентификации и аутентификации. 2. Чтение персональной криптографической информации. 3. Блокировка несанкционированной загрузки ОС со съемных носителей.

Аппаратные средства	Основные функции
ПАК "Соболь" / "Соболь-PCI"	1. Регистрация пользователей и назначение им персональных идентификаторов и паролей для входа в систему. 2. Идентификация и аутентификация пользователей при их входе в систему. 3. Чтение персональной криптографической информации. 4. Управление параметрами процедуры идентификации и аутентификации пользователя (защита от подбора пароля). 5. Контроль целостности файлов на жестком диске и секторов жесткого диска до загрузки ОС. 6. Блокировка несанкционированной загрузки ОС со съемных носителей. 7. Регистрация событий безопасности. 8. Возможность совместной работы (интеграции) с системой Secret Net 5.0.

2.4. Управление в Secret Net 5.0.

Система Secret Net 5.0 устанавливается на отдельный компьютер (рабочую станцию, сервер), работающий:

- автономно, без подключения к сети;
- в одноранговой сети;
- в сети с доменной организацией.

Администратор безопасности управляет средствами защиты непосредственно на защищаемом компьютере. В автономном варианте системы Secret Net 5.0 отсутствует возможность централизованного управления параметрами системы через механизм групповых политик, разрешено редактировать только параметры локальной политики.

Если требуется одинаковым образом настроить несколько компьютеров, необходимо использовать механизмы экспорта/импорта

параметров для тиражирования на другие компьютеры параметров системы.

В сети с доменной организацией при регистрации пользователей на компьютере целесообразно использовать уже имеющуюся в сети (домене) информацию о пользователях (доменных). Сформировать на компьютере список доменных пользователей можно двумя способами:

При установке системы начальный список доменных пользователей формируется по наличию на данном компьютере профилей доменных пользователей. После установки добавление доменных пользователей в список пользователей компьютера выполняет администратор. Сформированный список сохраняется в локальной базе данных (БД) Secret Net 5.0. В системе предусмотрена возможность управления параметрами Secret Net 5.0 для доменных пользователей.

Ядро системы обеспечивает хранение параметров доменных пользователей в локальной БД Secret Net 5.0. Здесь хранятся все параметры доменных пользователей (параметры полномочного управления, ключи, идентификаторы), а также идентификационная информация пользователей, получаемая с контроллера домена (SID, имя учетной записи, имя домена).

При входе на компьютер доменного пользователя, информация о котором отсутствует в локальной БД, ядро автоматически сохраняет информацию о нем в БД, присваивая параметрам Secret Net 5.0 значения по умолчанию.

2.5. Общие сведения о персональных идентификаторах

Персональный идентификатор — отдельное устройство, входящее в комплект аппаратного средства и предназначенное для хранения информации, необходимой для идентификации и аутентификации пользователя. Кроме того, в идентификаторе хранятся криптографические ключи пользователя. Для хранения криптографических ключей также может использоваться дискета.

В Secret Net 5.0 используются персональные идентификаторы iButton и eToken. Персональный идентификатор выдается пользователю компьютера администратором безопасности.

Один и тот же персональный идентификатор не может быть выдан нескольким пользователям. В то же время администратор может выдать пользователю несколько персональных идентификаторов для работы на одном или нескольких компьютерах с установленной системой Secret Net 5.0.

В процессе своей работы пользователь предъявляет персональный идентификатор по требованию системы. В процедурах, описанных в данном документе, часто используется операция предъявления идентификатора. Предъявить идентификатор означает сделать его доступным системе для выполнения операций чтения или записи данных.

В зависимости от типа устройства процедура предъявления персонального идентификатора выполняется по-разному. Идентификатор iButton необходимо приложить к считывателю так, чтобы между ними был надежный контакт, а идентификатор eToken следует вставить непосредственно или через удлинитель в разъем USB-порта компьютера. При выполнении этой процедуры могут возникать ошибки, связанные, например, с нарушением контакта со считывателем или неверным форматом данных идентификатора. В каждом таком случае система выведет на экран соответствующее сообщение с рекомендациями по продолжению работы.

Работа с персональными идентификаторами предполагает выполнение следующих операций.

- Просмотр сведений об идентификаторах. В окне настройки свойств пользователя на вкладке "Secret Net 5.0" в режиме "Идентификатор" приводится список всех присвоенных данному пользователю персональных идентификаторов с их кратким описанием (тип и номер, признак хранения пароля и ключей шифрования).
- Инициализация идентификатора. Форматирование, обеспечивающее возможность применения идентификатора с конкретным аппаратным устройством в системе Secret Net 5.0. Необходимость в инициализации возникает в тех случаях, когда в персональном идентификаторе по каким-либо причинам была

нарушена структура данных или до этого он использовался с другим устройством идентификации.

- Присвоение идентификатора. Добавление в базу данных Secret Net 5.0 сведений о том, что пользователю присвоен персональный идентификатор, включая информацию о самом идентификаторе (тип, уникальный серийный номер).
- Отмена присвоения идентификатора. Операция, противоположная предыдущей.
- Удаление из базы данных Secret Net 5.0 информации о принадлежности данного персонального идентификатора данному пользователю. Далее для простоты эту операцию будем называть удалением идентификатора.
- Включение режима хранения пароля в идентификаторе. Добавление в базу данных Secret Net 5.0 сведений о том, что для пользователя включен режим хранения пароля в его идентификаторе. Как правило, одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пользователю предоставляется возможность вводить свой пароль не с клавиатуры, а из своего идентификатора при его предъявлении.
- Отключение режима хранения пароля в идентификаторе. Операция, противоположная предыдущей. Как правило, одновременно с выключением режима хранения, выполняется удаление пароля из памяти персонального идентификатора. После выключения режима в тех случаях, когда система будет запрашивать пароль, пользователь должен будет вводить его с клавиатуры. Идентификатор остается закрепленным за пользователем и может использоваться для других целей, например, для хранения криптографических ключей.
- Включение (отключение) режима интеграции с ПАК "Соболь". Включение (отключение) режима означает, что пользователю разрешено (запрещено) использовать для входа в ПАК "Соболь" идентификатор, присвоенный в системе Secret Net 5.0.
- Запись (удаление) закрытых ключей. Используется для хранения в идентификаторе криптографических ключей пользователя.

- Проверка принадлежности. С помощью этой операции администратор безопасности может проверить — кому из пользователей компьютера присвоен данный персональный идентификатор.

Все основные операции с персональными идентификаторами, за исключением инициализации и проверки принадлежности, выполняются применительно к конкретному пользователю. Для их выполнения используются Мастер присвоения персональных идентификаторов и Мастер настройки режимов идентификаторов.

2.6. Средства управления

Средства управления — это инструменты, с помощью которых администратор безопасности управляет работой защитных механизмов и контролирует действия пользователей компьютера. Такими инструментами в Secret Net 5.0 являются:

- Узел "Параметры Secret Net" оснастки "Локальная политика безопасности" — предназначен для настройки группы параметров безопасности Secret Net 5.0, относящихся к конфигурации компьютера.
- Оснастка "Управление компьютером" — предназначена для настройки параметров работы локальных и доменных пользователей.
- Программа "Проводник" — используется для настройки параметров ресурсов файловой системы.
- Программа "Контроль программ и данных" — предназначена для управления механизмами контроля целостности и замкнутой программной среды.
- Программа "Журналы" — предназначена для управления журналом Secret Net 5.0.
- Контекстное меню пиктограммы Secret Net 5.0, находящейся в системной области панели задач Windows — содержит команды для выполнения операций с криптографическими ключами и некоторых других операций.
- Средства экспорта и импорта параметров — используются для тиражирования параметров системы Secret Net 5.0.

- Элемент панели управления Windows "Управление СЗИ Secret Net 5.0" —используется для управления режимом интеграции Secret Net 5.0 и ПАК "Соболь", а также для временного отключения защитных механизмов.

2.6.1. Узел "Параметры Secret Net"

Стандартная оснастка "Локальная политика безопасности" дополняется узлом "Параметры Secret Net".

Для настройки параметров:

1. Откройте панель управления Windows и активируйте элемент "Администрирование".

2. В появившемся списке активируйте элемент "Локальная политика безопасности". На экране появится окно консоли управления Microsoft (MMC).

3. Выберите узел "Параметры Secret Net".

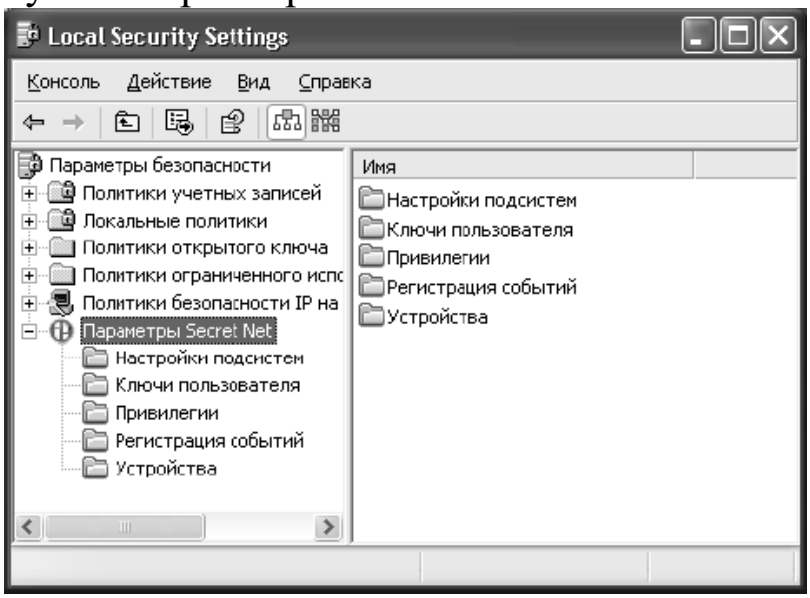

Рис. 1 - Узел «Параметры Secret Net»

Узел "Параметры Secret Net" содержит 5 групп параметров показанных в таблице 2.

Таблица 2. - Назначение параметров Secret Net

Группа	Назначение
Настройки подсистем	• Управление режимами работы механизма входа в систему • Управление режимом работы механизма контроля печати • Управление режимом работы механизма замкнутой программной среды. • Управление механизмом затирания удаляемой информации • Настройка параметров журнала • Управление режимом работы механизмов контроля устройств и разграничения доступа к устройствам.
Ключи пользователя	Настройка параметров ключей пользователей
Привилегии	Назначение пользователям привилегий, связанных с работой следующих механизмов: - шифрование файлов; - работа с журналом Secret Net 5.0; - работа в условиях замкнутой программной среды.
Регистрация событий	Настройка перечня событий, регистрируемых системой Secret Net 5.0: - разграничение доступа к устройствам; - разграничение полномочного доступа; - шифрование файлов; - контроль аппаратной конфигурации.
Устройства	Управление параметрами контроля устройств и правами доступа к устройствам.

2.6.2. Оснастка "Управление компьютером"

В стандартную оснастку "Управление компьютером" встроены средства управления параметрами системы Secret Net 5.0 для локальных и доменных пользователей.

С помощью этих средств можно управлять:

- персональными идентификаторами пользователей;
- криптографическими ключами пользователей;
- уровнем допуска пользователей к конфиденциальной информации.

Для настройки параметров необходимо открыть окно оснастки любым из следующих стандартных способов:

1. В панели управления Windows откройте элемент "Администрирование" и в появившемся списке элементов активируйте элемент "Управление компьютером".

2. Нажмите кнопку "Пуск" и активируйте в главном меню Windows команду "Все программы | Secret Net 5 | Управление компьютером".

3. Вызовите контекстное меню к ярлыку "Мой компьютер" и выберите в нем команду «Свойства».

Средства управления параметрами Secret Net 5.0 содержатся в папках "Служебные программы | Локальные пользователи и группы | Пользователи" и "Служебные программы | Доменные пользователи".

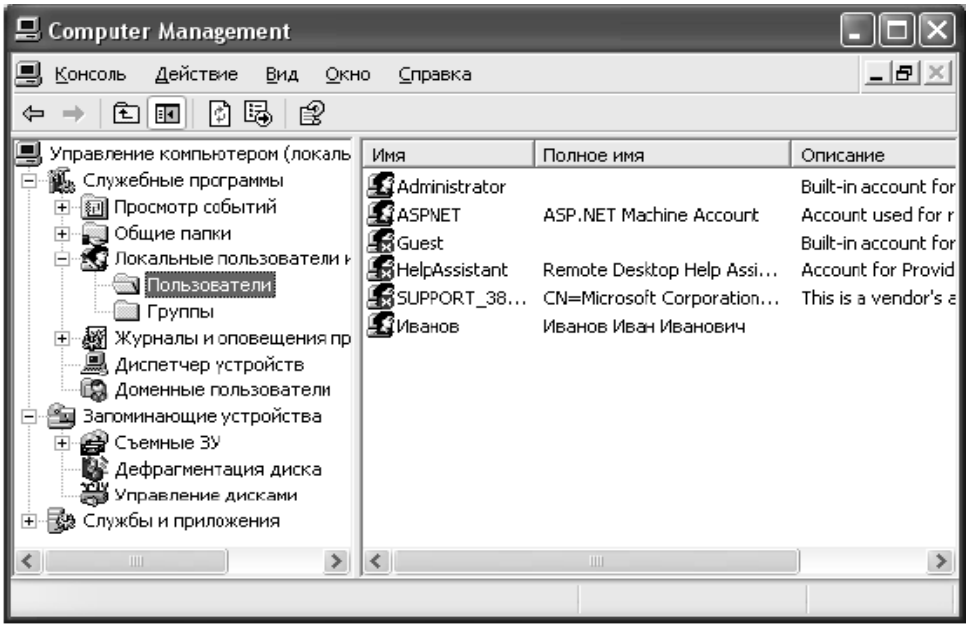

Рис. 2 - Оснастка «Управление компьютером»

Для настройки параметров пользователя:

1. Выберите папку "Пользователи" или "Доменные пользователи".

2. В правой части она программы в списке пользователей вызовите контекстное меню для ярлыка с именем нужного пользователя и активируйте в меню команду "Свойства".

На экране появится диалоговое окно настройки свойств пользователя.

3. Перейдите к диалогу "Secret Net 5".

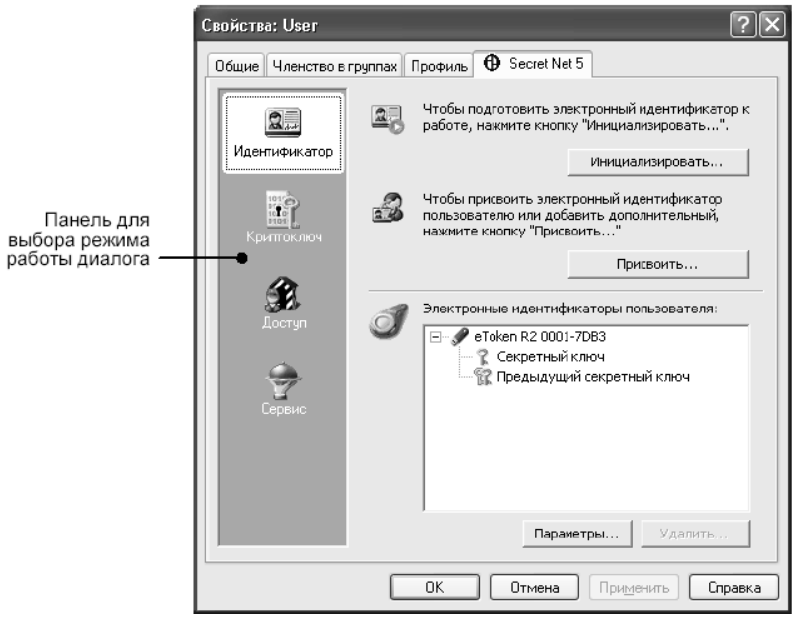

Рис. 3 - Свойства пользователей

2.6.3.Программа "Проводник"

Стандартная программа ОС Windows "Проводник" дополнена средствами управления Secret Net 5.0, позволяющими присваивать категории конфиденциальности файлам и каталогам и управлять шифрованием файлов и каталогов.

Для настройки параметров ресурсов:

1. В программе "Проводник" найдите нужный каталог или файл.

2. Вызовите контекстное меню для ярлыка каталога или файла и активируйте в меню команду "Свойства". На экране появится диалоговое окно настройки свойств каталога или файла.

3. Перейдите к диалогу "Secret Net".

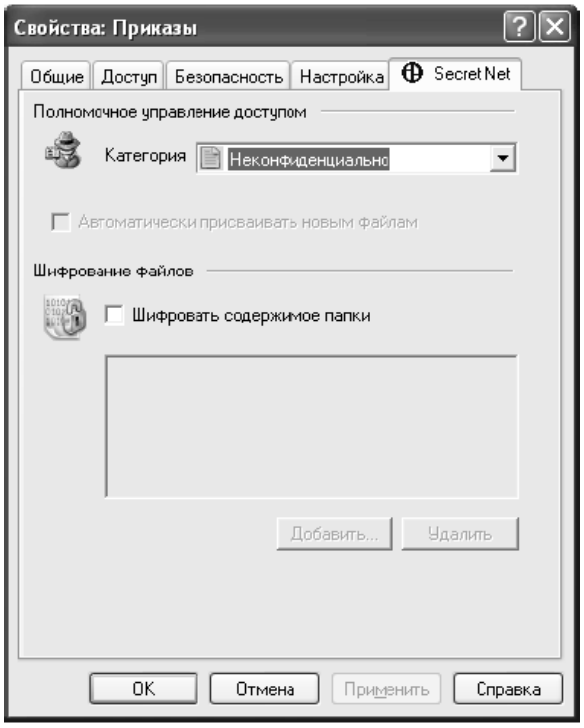

Рис. 4 - Работа с файлами через «Secret Net»

Группа полей "Полномочное управление доступом" используется для управления категориями конфиденциальности ресурса. Эти поля доступны для управления только тем пользователям, которые обладают необходимыми правами и привилегиями, и только в том случае, когда ресурс размещается на диске с файловой системой NTFS или NTFS5.

Группа полей "Шифрование файлов" используется для управления шифрованием каталогов и файлов. Эти поля доступны для управления только тем пользователям, которые обладают привилегией "Создание шифрованного ресурса", и только в том случае, когда пользователь является владельцем ресурса или владелец ресурса предоставил ему права на управление ресурсом.

2.6.4.Программа "Контроль программ и данных"

Программа "Контроль программ и данных" используется для настройки и управления работой механизмов контроля целостности и замкнутой программной среды.

Для вызова этой программы нажмите кнопку "Пуск" и активируйте в главном меню Windows команду "Все программы | Secret Net 5 | Контроль программ и данных".

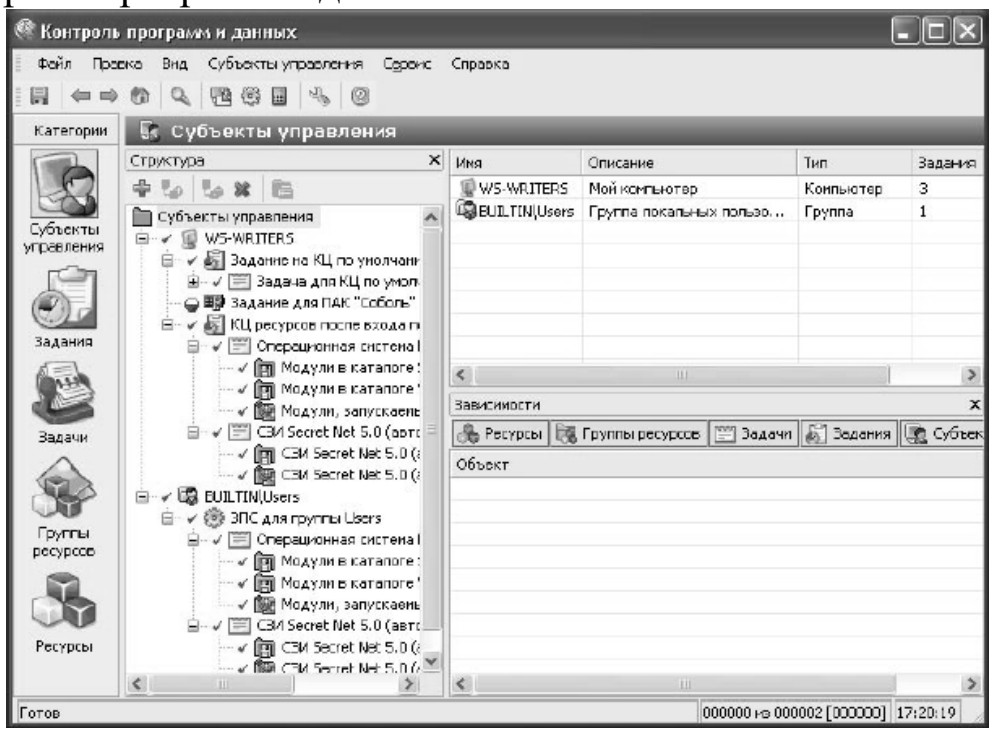

Рис. 5 - Программа «Контроль программ и данных»

2.6.5.Программа "Журналы"

Программа "Журналы" используется для просмотра и управления журналом Secret Net 5.0.

Для вызова этой программы нажмите кнопку "Пуск" и активируйте в главном меню

Windows команду "Все программы | Secret Net 5 | Журналы".

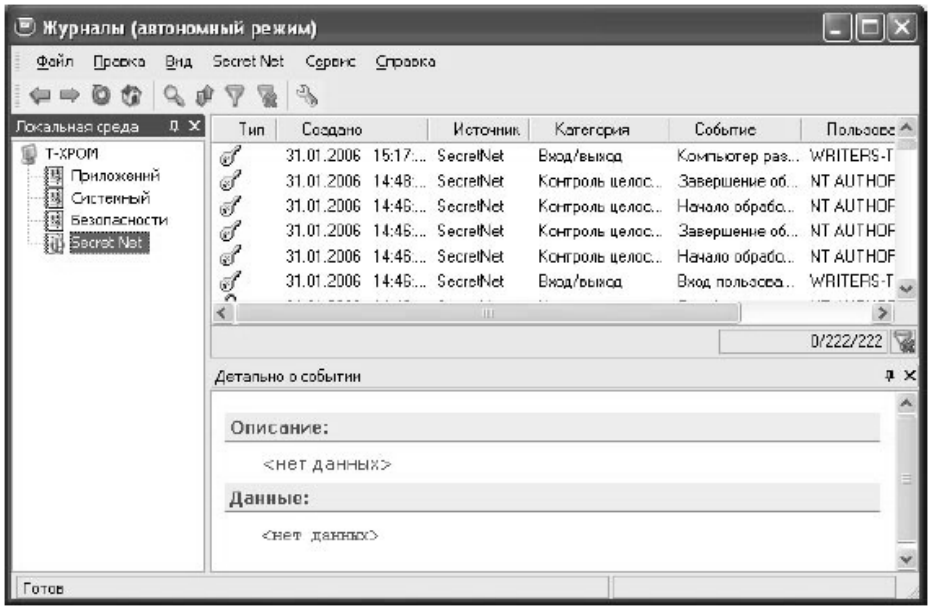

Рис. 6 - Программа «Журналы»

2.6.6.Средства экспорта и импорта параметров.

Для того чтобы настроить систему защиты одинаковым образом на нескольких компьютерах, в Secret Net 5.0 реализована возможность экспорта и импорта различных параметров системы. Предварительно система защиты настраивается на одном из компьютеров, принимаемом за эталонный. После проверки корректности работы защитных механизмов на эталонном компьютере выполняется экспорт значений параметров в файл. Далее на тех компьютерах, на которых параметры системы SecretNet 5.0 должны соответствовать эталонным значениям, выполняется операция импорта значений параметров из этого файла.

Экспорт и импорт осуществляется для параметров локальной политики безопасности (параметров системы Secret Net 5.0) и параметров пользователей. Кроме экспорта и импорта указанных параметров в Secret Net 5.0 можно экспортировать и импортировать параметры, используемые в механизмах контроля целостности и замкнутой программной среды.

Экспорт параметров системы Secret Net 5.0 осуществляется в файлы, содержимое которых в дальнейшем можно импортировать на любом компьютере с установленной системой Secret Net 5.0. Экспорт

выполняется в файлы, формат которых соответствует формату файлов сведений ОС Windows (*.inf).

2.7. Настройка механизма шифрования

Для того чтобы пользователи компьютера могли защищать свои файлы, используя механизм шифрования, и имели возможность работать с зашифрованными файлами других пользователей, администратор безопасности должен выполнить следующее:

- Предоставить пользователям привилегию на создание шифрованных ресурсов.
- Присвоить пользователям персональные идентификаторы.
- Выдать пользователям криптографические ключи.
- Настроить параметры смены криптографических ключей.
- Настроить регистрацию событий, связанных с работой механизма шифрования.
- Довести до сведения пользователей порядок работы с зашифрованными ресурсами.

Присваивание персональных идентификаторов.

Для хранения ключей шифрования могут использоваться идентификаторы iButton, eToken или дискета. Идентификаторы должны быть присвоены и выданы каждому пользователю, работающему с шифрованными ресурсами.

Настройка регистрации событий.

Для проведения аудита, связанного с работой механизма шифрования, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категории "Шифрование файлов" должны регистрироваться в журнале безопасности Secret Net 5.0.

В соответствии с требованиями политики безопасности администратор должен задать значения следующих параметров смены криптографических ключей:

- максимальный срок действия;
- минимальный срок действия;
- время предупреждения об истечении срока действия ключа.

Действие параметров распространяется на всех пользователей компьютера. По истечении максимального срока действия криптографические ключи пользователя не могут быть загружены в систему и, соответственно, пользователю будет отказано в работе с шифрованными ресурсами. В этом случае пользователь должен сменить криптографические ключи. Смена криптографических ключей самим пользователем возможна только по истечении минимального срока действия.

Работа с криптографическими ключами.

Для работы с шифрованными ресурсами пользователю необходимо иметь криптографический ключ.

Первоначально ключ выдается пользователю администратором безопасности. Для этого администратор безопасности должен инициировать в Secret Net 5.0 генерацию ключа для конкретного пользователя и записать этот ключ в присвоенный пользователю идентификатор. В дальнейшем пользователь может самостоятельно сменить свой ключ. После смены в идентификаторе всегда хранятся два ключа: предыдущий и текущий. При каждой смене предыдущий ключ удаляется, текущий становится предыдущим, а новый ключ — текущим.

В функции администратора безопасности помимо выдачи ключей входят следующие операции:

- копирование ключей из одного идентификатора в другой;
- смена ключей пользователя;
- удаление ключей.

Для того чтобы пользователь обладал возможностью создавать шифрованные ресурсы, ему необходимо предоставить привилегию “Шифрование файлов: Создание шифрованного ресурса”. Пользователь, создавший шифрованный ресурс, является его владельцем и может предоставлять доступ к ресурсу другим пользователям, а также делегировать им полномочия на управление шифрованным ресурсом. Пользователь ресурса может создавать новые зашифрованные файлы, удалять их, выполнять с ними любые операции чтения и записи.

Для генерации ключей пользователей применяется алгоритм, соответствующий требованиям ГОСТ Р34.10-2001. В результате создаются закрытый ключ и открытый ключ пользователя. Открытые ключи пользователей хранятся в локальной базе данных Secret Net 5.0, закрытые ключи — в персональном идентификаторе пользователя.

Для каждой ключевой пары в системе хранится время ее генерации, при необходимости можно установить для нее минимальное и максимальное время жизни. Если пользователь выполнит операцию смены ключей, то в системе будут храниться две ключевые пары (текущая и предыдущая). При первом же обращении к шифрованному ресурсу управляющая информация расшифровывается на старом ключе и зашифровывается на новом, при этом сами данные повторно не перешифровываются.

Ключи, используемые подсистемой шифрования показаны в таблице 3.

Таблица 3. - Ключи используемые при шифровании

Ключи	Наименование	Алгоритмы генерации
SKr	Закрытый ключ ресурса	Генерируется в соответствии с требованиями к ключам ГОСТ Р34.10-2001
PKr	Открытый ключ ресурса	- " -
SKu	Закрытый ключ пользователя	- " -
PKu	Открытый ключ пользователя	- " -
Kr	Ключ шифрования ресурса	Генерируется с помощью датчика случайных чисел (ДСЧ)
Kf	Ключ шифрования файла	- " -
SKur	Сессионный ключ	Генерируется в соответствии с алгоритмом Diffie-Hellman

Включение режима шифрования каталога.

При включении режима шифрования каталога:

1. В каталоге создается файл !Res.key.

2. Генерируются закрытый и открытый ключи ресурса (SKr, PKr) и ключ шифрования ресурса (Kr).

3. На основании закрытого ключа пользователя (SKu) и открытого ключа ресурса (PKr) вычисляется сессионный ключ (SKur).

4. Ключи Kr и SKr зашифровываются на ключе SKur и получаются соответственно значения Kr(SKur) и SKr(SKur), которые вместе с открытым ключом пользователя PKr сохраняются в файле !Res.key.

Включение режима шифрования для файла.

При зашифровании файла:

1. Из файла !Res.key считывается открытый ключ ресурса (PKr).

2. На основании открытого ключа ресурса (PKr) и закрытого ключа пользователя (SKu) вычисляется сессионный ключ (SKur).

3. С помощью сессионного ключа (SKur) из Kr(SKur) вычисляется ключ шифрования ресурса (Kr).

4. Генерируется ключ шифрования файла (Kf).

5. Содержимое файла шифруется на ключе шифрования файла (Kf).

6. С помощью ключа шифрования ресурса (Kr) зашифровывается ключ шифрования файла Kf(Kr) и помещается в отдельный служебный файл.

Доступ пользователя к зашифрованному файлу.

При расшифровании файла:

1. Из файла !Res.key считывается открытый ключ ресурса (PKr).

2. На основании открытого ключа ресурса (PKr) и закрытого ключа пользователя (SKu) вычисляется сессионный ключ (SKur).

3. С помощью сессионного ключа (SKur) из Kr(SKur) вычисляется ключ шифрования ресурса (Kr).

4. Из служебного файла считывается Kf(Kr) и расшифровывается.

5. Зашифрованное содержимое файла расшифровывается на ключе шифрования файла (Kf).

6. При последующем сохранении файла происходит его зашифрование на ключе шифрования файла (Kf).

Предоставление другому пользователю доступа к ресурсу.

Для предоставления другому пользователю доступа к шифрованному каталогу:

1. Владелец ресурса в свойствах каталога выбирает в списке имя пользователя, которому будет разрешен доступ к ресурсу. В список попадают только те пользователи, открытые ключи которых имеются в базе данных Secret Net 5.0.

2. На основании закрытого ключа владельца (SKu) и открытого ключа ресурса (PKr) из файла !Res.key вычисляется сессионный ключ (SKur). С использованием сессионного ключа расшифровываются другие ключи SKr и Kr.

3. Вычисляется значение сессионного ключа для нового пользователя ресурса SKu2r на основании закрытого ключа ресурса (SKr) и открытого ключа нового пользователя (PKu2).

4. Ключи SKr и Kr зашифровываются на сессионном ключе нового пользователя и сохраняются в файле !Res.key в виде дополнительного управляющего блока.

3. ОСНОВНЫЕ ОПЕРАЦИИ, ВЫПОЛНЯЕМЫЕ С ПОМОЩЬЮ СЗИ SECRET NET 5.0.

3.1. Определение права доступа работы на устройстве.

Назначение прав доступа выполняется отдельно для устройств, зафиксированных в базе данных при установке Secret Net 5.0 (т.е. тех устройств, которые фактически установлены на компьютере), и для устройств, которые могут подключаться в процессе работы.

Для просмотра списка устройств:

- Нажмите *Пуск», → Панель управления*.
- Вызовите оснастку "Локальная политика безопасности". Откройте узел "Параметры Secret Net" и выберите папку "Устройства" (рис. 7). В правой части окна появится иерархический список всех контролируемых средствами Secret Net 5.0 устройств компьютера:

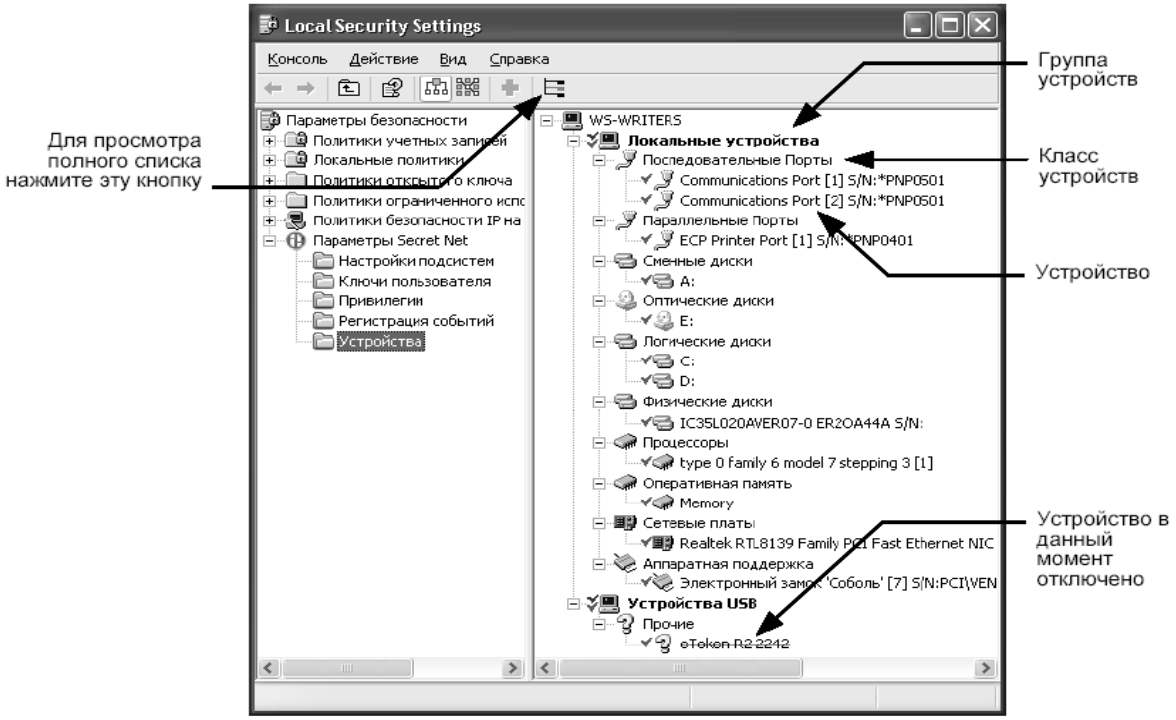

Рис. 7 - Раздел «Устройства»

В системе поддерживается механизм наследования разрешений. Для всех классов и всех устройств по умолчанию включен признак наследования разрешений.

Если изменить права доступа к классу или устройству, перед его наименованием в списке появится отметка красного цвета.

Изменить права доступа к классу или устройству можно с помощью запретов (при этом нужно учитывать или использовать принцип наследования) или изменив настройки доступа к группе, установленные по умолчанию.

Для просмотра или изменения параметров доступа к устройствам:

1. Выберите в списке объект (группу, класс или устройство), вызовите контекстное меню и выберите команду "Свойства". Или наведите курсор на название устройства и дважды нажмите левую кнопку мыши. Появится диалоговое окно настройки свойств устройства.

2. Перейдите к диалогу "Разрешения" (рис. 8).

На рисунке представлен диалог "Разрешения" для группы:

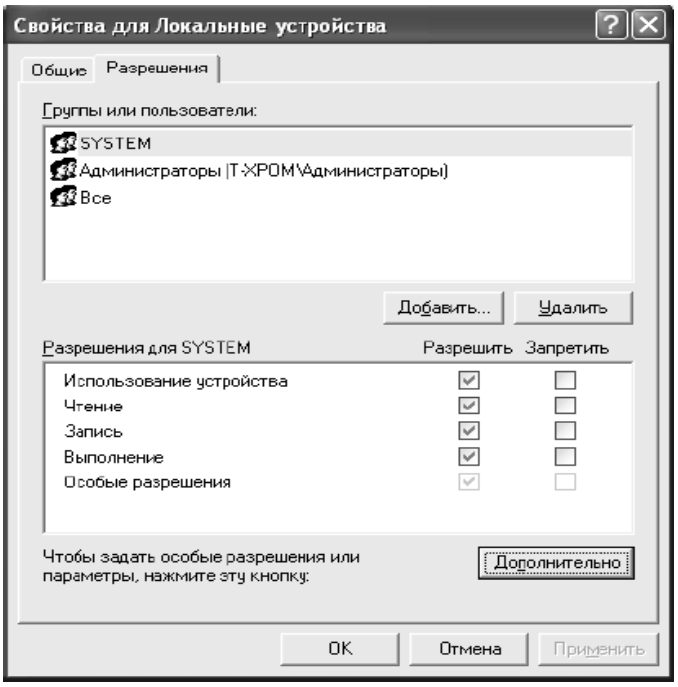

Рис. 8 - Свойства допуска к устройствам.

В верхней части диалога расположен список пользователей, для которых выполняется настройка прав доступа к данной группе (на рисунке проиллюстрирован случай, когда права доступа к устройствам не назначались и поэтому в списке присутствуют только 3 стандартные группы пользователей). В нижней части приведены параметры доступа групп пользователей, установленные системой Secret Net 5.0 по умолчанию.

3. Для изменения параметров доступа выберите в списке группу пользователей и затем расставьте разрешения для каждой операции, чтобы установить требуемый уровень доступа к данному устройству.

4. 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.

5. В диалоге настройки свойств объекта (группы, класса, устройства) нажмите кнопку "OK".

6. Если требуется изменить параметры доступа и контроля для другого устройства, найдите его в списке и повторите шаги 1 — 5.

7. По окончании процесса настройки закройте оснастку.

8. Появится предупреждение об изменениях в политике контроля устройств. Для сохранения изменений нажмите кнопку "Да", для отмены – "Нет".

3.2. Редактирование параметров аудита и периодов затирания файлов.

Под аудитом понимается регистрация событий, происходивших на компьютере в течение определенного времени. Общими задачами аудита являются следующие:

- контролирование состояния защищенности системы;
- выявление причин произошедших изменений;
- определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;
- установление времени изменений.

Для составления перечня регистрируемых событий:

1. Нажмите *Пуск →Панель управления*.

2. Вызовите оснастку "Локальная политика безопасности", откройте узел "Параметры Secret Net" и выберите папку "Регистрация событий".

В правой части появится список событий, регистрируемых Secret Net 5.0 (рис. 9).

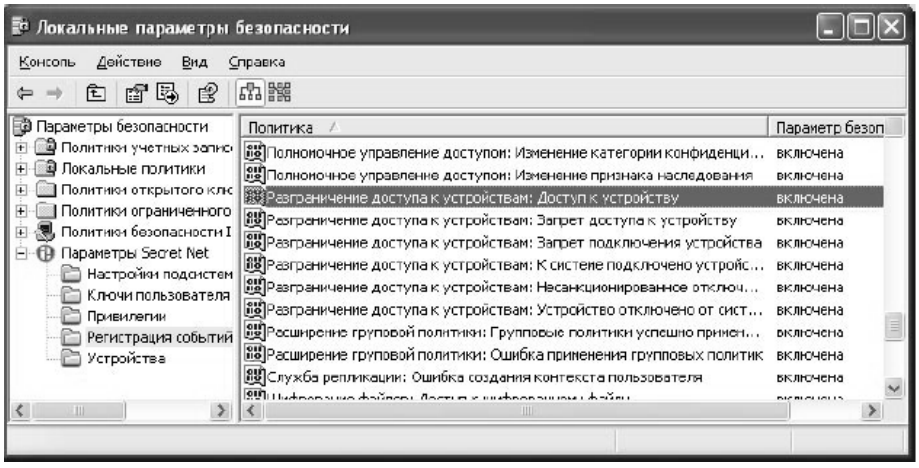

Рис. 9 - Список регистрируемых событий.

По умолчанию регистрация всех событий включена.

3. Для включения или отключения регистрации события вызовите контекстное меню для элемента списка и активируйте в нем команду "Свойства"(рис. 10).

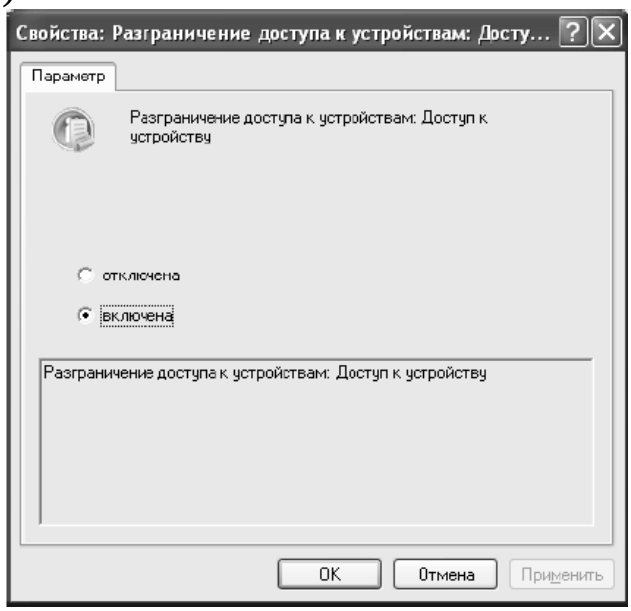

Рис. 10 - Редактирование параметров аудита.

4. Отметьте поле "включена" или "отключена" в зависимости от того, требуется или не требуется регистрировать данное событие.

5. Нажмите кнопку "OK".

Таким образом можно настроить регистрацию всех событий происходящих в системе.

Для настройки параметров журнала Secret Net:

1. Откройте параметры Secret Net в консоли локальной политики безопасности.

2. Перейдите к группе параметров "Настройки подсистем".

В правой части окна появится список настраиваемых параметров защитных механизмов системы Secret Net 5.0.

3. В списке параметров выберите элемент "Журнал: политика перезаписи событий" и вызовите окно настройки его свойств (рис. 11).

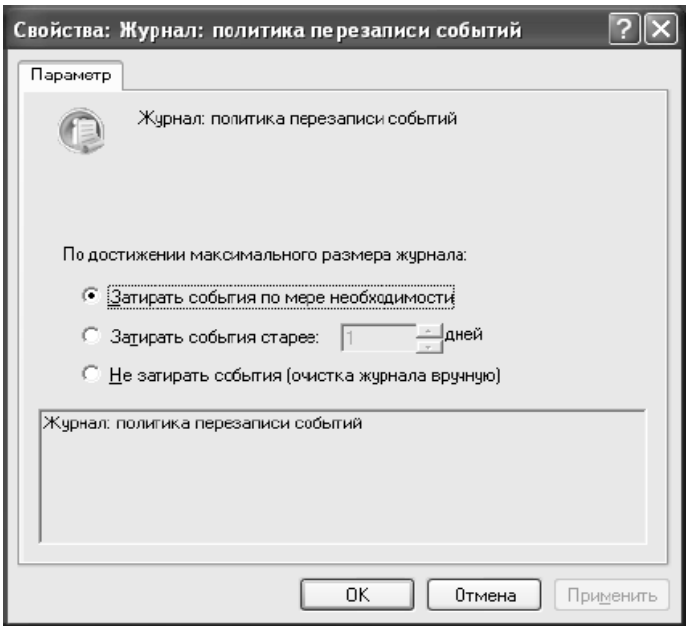

Рис. 11 - Редактирование времени затирания событий

4. Выберите способ очистки журнала при его переполнении (если размер журнала достигает максимального значения). Для этого установите отметку в одном из следующих полей:

- Затирать события по мере необходимости:

При переполнении журнала система автоматически удаляет из журнала необходимое количество самых старых записей.

- Затирать события старее: <…> дней:

При переполнении журнала система автоматически удаляет записи, время хранения которых превысило заданный период. Новые записи не будут добавляться, если журнал достиг максимального размера, и в нем нет записей старше заданного периода. Длительность периода хранения записей указывается в поле справа. Диапазон ввода значений: от 1 до 365 дней.

- Не затирать события:

После достижения максимального размера записи хранятся в журнале. Новые события в журнале не регистрируются. Журнал можно очистить только “вручную” с помощью программы просмотра журналов системы защиты. Очистка должна выполняться периодически, чтобы не допустить переполнения журнала, т. к. это

может привести к нарушениям в работе и вызвать блокировку компьютера.

5. Нажмите кнопку "OK" в диалоговом окне настройки.

3.3. Установка запретов сетевых интерфейсов.

Для работы с конфиденциальной информацией иногда требуется отключить доступ к сети для гарантирования конфиденциальности и не распространяемости защищаемых данных.

Для запретов сетевых интерфейсов необходимо:

- Открыть «Панель управления», выбрать оснастку «Локальная политика безопасности».
- Среди параметров выбрать «Параметры Secret Net». Устройства.

Для просмотра полного списка устройств (рис. 12) нажмите кнопку на панели инструментов.

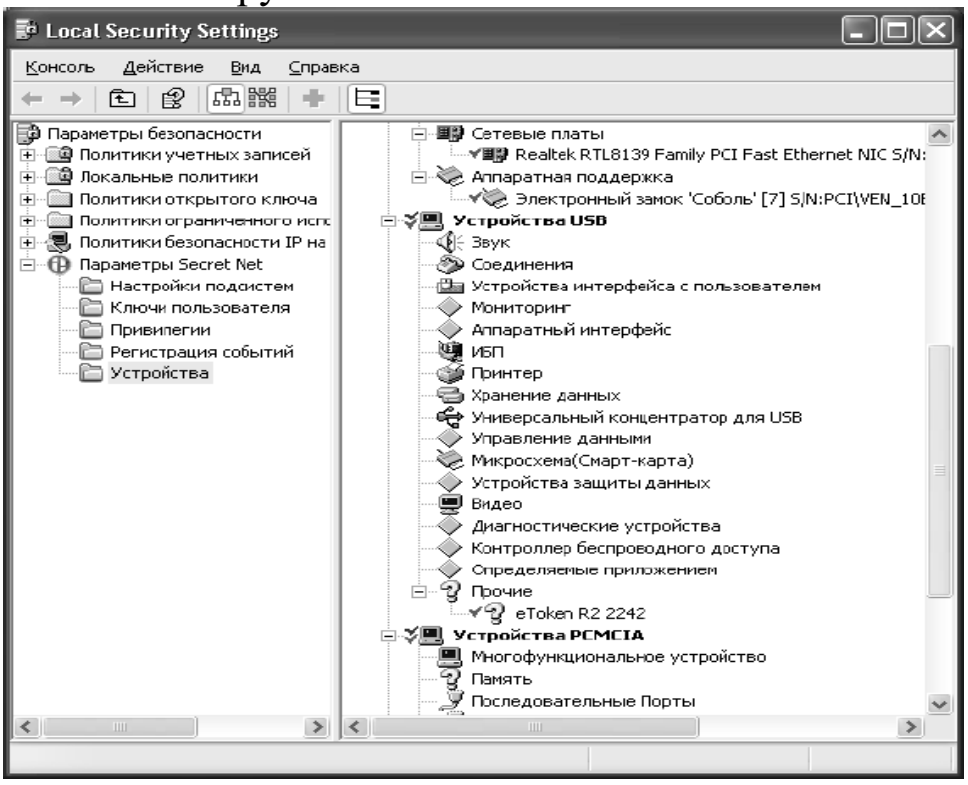

Рис. 12 - Список подключённых устройств

Полный список содержит как устройства, зафиксированные в локальной базе данных, так и те устройства, которые могут

подключаться пользователями. Среди представленных устройств выбрать класс устройств «Сетевые платы»

Параметры контроля объектов могут быть унаследованы от вышестоящих объектов или заданы явно. Так, если требуется установить ограничения не для одного а для нескольких устройств, то проще установить запрет для всей группы, в которую входят данные устройства.

- Выберите в списке устройство (объект), для которого необходимо изменить параметры контроля, и вызовите окно его свойств (рис. 13).

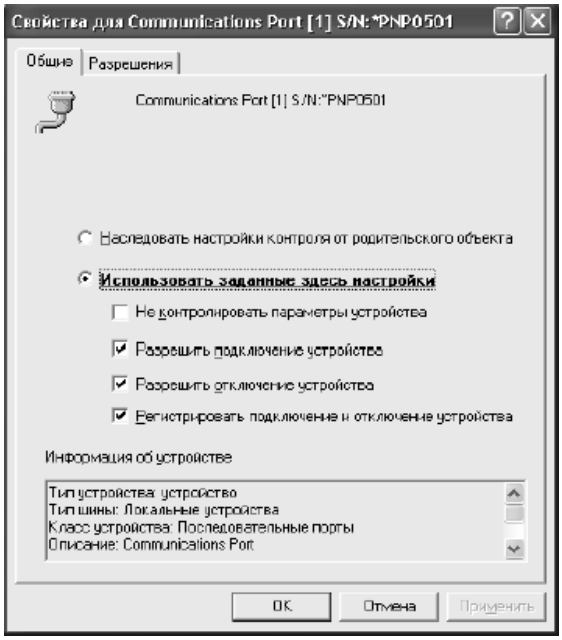

Рис. 13 - Свойства доступа к сетевым платам.

Здесь можно установить Разрешения для действий совершаемых с устройством. Так же если нужно унаследовать настройки группы, то нужно установить 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 настройте параметры политики контроля.
- Для завершения настройки параметров контроля данного устройства нажмите кнопку "OK".

3.4. Назначение персональных идентификаторов.

Для присвоения персонального идентификатора пользователю необходимо:

1. Открыть «Панель управления»
2. Выбрать *Администрирование» → Управление компьютером*.
3. Выбрать пользователя, которому присваиваем идентификатор и вызвать его свойства.
4. Среди вкладок выбрать “Secret Net”
5. В диалоге "Secret Net 5", функционирующем в режиме "Идентификатор", нажмите кнопку "Присвоить…".

На экране появится первый диалог (рис. 14).

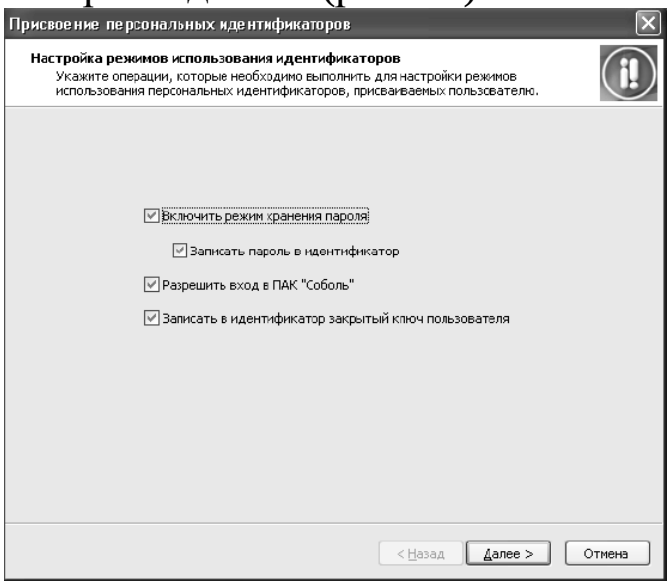

Рис. 14 - Начало присвоения идентификатора

Диалог предназначен для настройки режимов использования присваиваемого идентификатора. В нем расположены выключатели для задания операций, которые должны быть выполнены в процессе присвоения идентификатора.

6. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".

В зависимости от выбранных операций будет выполнен переход:

- к первому действию пункта 7 — если выбраны операции "Запись пароля в идентификатор" и/или "Разрешить вход в ПАК "Соболь";

- ко второму действию пункта 7 — если выбрана операция "Записать в идентификатор закрытый ключ пользователя, не выбраны операции "Запись пароля в идентификатор" и "Разрешить вход в ПАК "Соболь" и у пользователя уже есть закрытый ключ.

7. Ввод данных

На этом шаге вводятся данные, необходимые для выполнения операций, выбранных в пункте 5. Такими данными являются пароль пользователя и закрытый ключ, хранящийся в другом идентификаторе. Если пользователь не имеет закрытого ключа, а была выбрана операция "Записать в идентификатор закрытый ключ пользователя", в пункте 8 будет выполнена генерация ключа и его запись в присваиваемый идентификатор.

На экране появится диалог мастера, отображающий ход выполнения операций ввода данных. Если на предыдущем шаге была выбрана операция "Записать пароль в идентификатор" и/или "Разрешить вход в ПАК "Соболь", на экране появится диалог для ввода пароля пользователя (рис. 15).

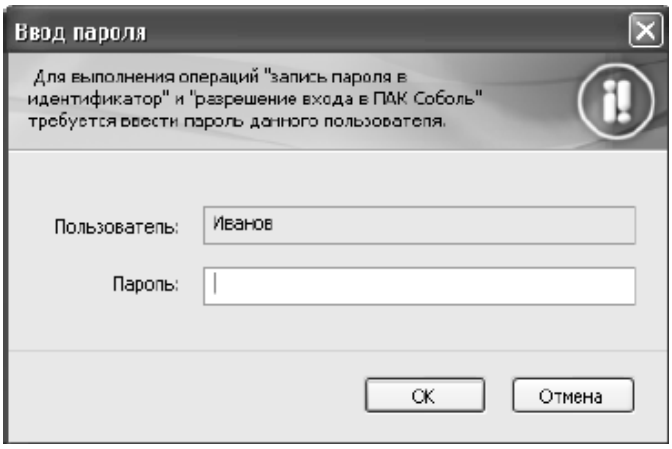

Рис. 15 - Диалог для ввода пароля пользователя

7.1. Введите пароль пользователя и нажмите кнопку"OK".

Если операция записи закрытого ключа не предусмотрена, на этом пункт 7 завершается.

7.2. предусмотрен ввод закрытого ключа, после успешного ввода пароля автоматически появится приглашение предъявить идентификатор, содержащий закрытый ключ пользователя (рис. 16).

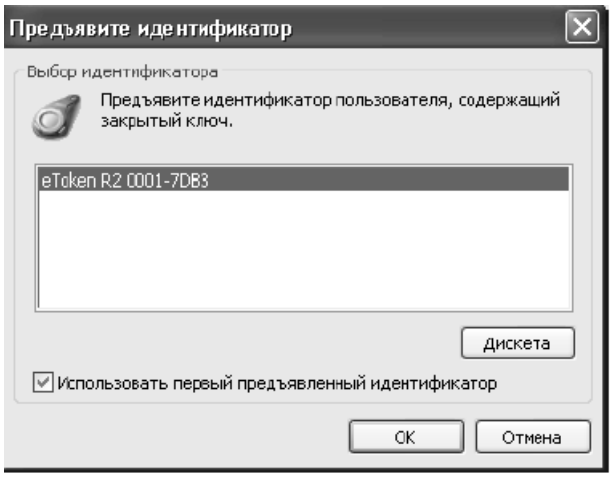

Рис. 16 - Диалог предъявления идентфикатора

8. Запись данных

На этом шаге выполняются операции, выбранные при настройке режимов использования идентификатора, а также сохранение информации в базе данных Secret Net 5.0. Операции выполняются при условии, что на шаге 2 были введены все необходимые для этого данные. На экране появится приглашение предъявить присваиваемый пользователю идентификатор.

8.1. Предъявите идентификатор и не нарушайте контакта со считывателем до завершения всех операций.

Начнется последовательное выполнение всех выбранных в пункте 5 операций. Ход их выполнения отображается в диалоге мастера. В нем представлен полный список всех возможных операций и их статус. По мере успешного выполнения очередной операции ее статус меняется со значения "Выполняется" назначение "Выполнено". Операции, не предусмотренные для выполнения, имеют статус "Не выполнялось".

После успешного завершения всех операций статус каждой из них должен иметь значение "Выполнено".

9. Для завершения работы мастера нажмите кнопку "Готово" в диалоге с результатами выполненных операций.

3.5. Назначение прав доступа к файлам.

Полномочное разграничение доступа применяется для обеспечения контролируемого доступа к информации и, тем самым, ограничения её несанкционированного распространения.

Каждому уровню соответствуют свои права доступа. В Secret Net 5.0 используются 3 уровня допуска:

- Отсутствует – Отсутствуют права доступа к конфиденциальной информации.
- Конфиденциальный - Разрешается доступ к ресурсам с категорией "конфиденциальный".
- Строго конфиденциальный - Разрешается доступ к ресурсам с категорией "конфиденциальный" и "строго конфиденциальный".

Одновременно с уровнем допуска пользователю могут предоставляться привилегии:

- Управление категориями конфиденциальности;
- Печать конфиденциальных документов.

Привилегии могут быть предоставлены только тем пользователям, которым установлен уровень допуска "Конфиденциальный" или "Строго конфиденциальный".

Пользователь, не обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше своего уровня допуска. Пользователь, наделенный привилегией "Управление категориями конфиденциальности", может выполнять следующие действия:

- повысить категорию конфиденциальности каталогов и файлов, но не выше своего уровня допуска;
- понизить категорию конфиденциальности каталогов и файлов, категория конфиденциальности которых не выше его уровня;
- настраивать параметр “Автоматически присваивать новым файлам”, выбирать режим работы каталогов, категория конфиденциальности которых не выше его уровня допуска.

Для ресурсов используются 3 категории конфиденциальности:

- Не конфиденциально;
- Конфиденциально;

- Строго конфиденциально.

После того как каталогу присвоена категория конфиденциальности, доступ к содержащимся в нем файлам смогут осуществить только те пользователи, для которых установлен соответствующий уровень допуска к конфиденциальной информации.

Для назначения уровня допуска и привилегий:

1. Открыть *Панель управления → «Администрирование → Управление компьютером.*
2. Выберите пользователя, откройте окно настройки его свойств, перейдите к диалогу "Secret Net 5" в режиме "Доступ"(рис. 17).

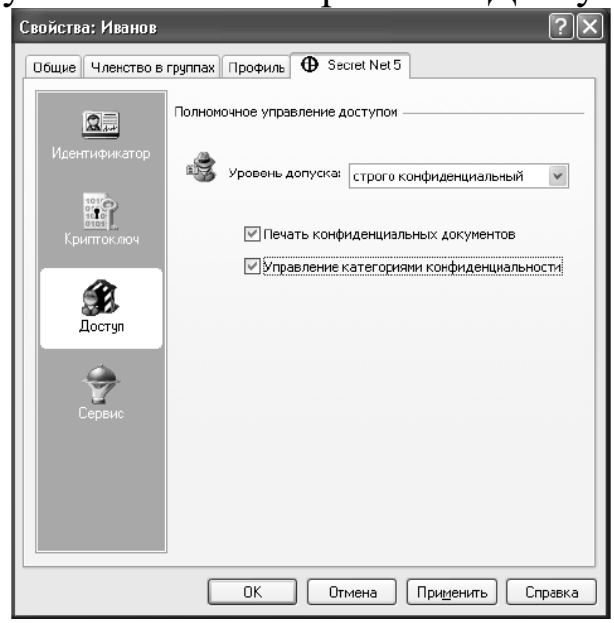

Рис. 17 - Редактирование полномочий пользователя

3. Установите уровень допуска пользователя в одноименном поле.
4. Предоставьте или отмените привилегии пользователя.
5. Нажмите кнопку "OK".

3.6. Шифрование файлов с помощью закрытого ключа.

Прежде чем начать шифрование каталогов и файлов необходимо осуществить загрузку ключевой информации с выданного пользователю персонального идентификатора:

- Вызовите контекстное меню пиктограммы Secret Net 5.0, находящейся в системной области панели задач Windows, и

активируйте команду “Загрузить ключи”. В появившемся окне предложат предъявить персональный идентификатор.

- Предъявите персональный идентификатор для считывания закрытого ключа.
- Как только ключ считается пиктограмма “Secret Net” изменит свой вид и можно будет производить шифрование файлов.

Для открытия диалога "Secret Net":

- Вызовите программу Проводник.
- Вызовите контекстное меню каталога или файла, над которым вы собираетесь выполнить операцию, и активируйте команду “Свойства”.
- В появившемся на экране окне "Свойства” перейдите к диалогу "Secret Net"(рис. 18).

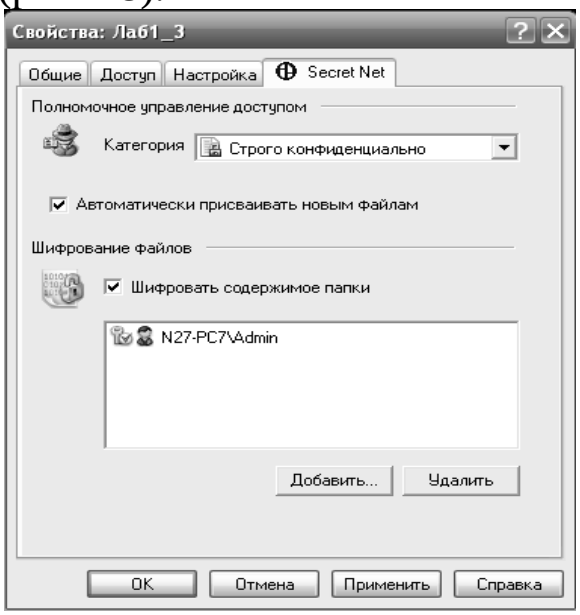

Рис. 18 - Диалог шифрования каталога

Операции с шифрованными ресурсами выполняются с помощью элементов интерфейса, размещенных в секции «Шифрование файлов». В секции имеется выключатель «Шифровать содержимое папки» (для каталога) или "Файл зашифрован" (для файла). У зашифрованного каталога (файла) в поле выключателя есть отметка, у незашифрованного каталога (файла) ее нет.

1. Установите отметку в поле выключателя "Шифровать содержимое папки".

В списке появится строка с именем текущего пользователя. При необходимости отредактируйте список пользователей, которым разрешен доступ к шифрованному каталогу.

2. Нажмите кнопку “ОК”.

На экране появится диалог настроек шифрования каталога.

3. Установите отметку в поле выключателя:

- "зашифровать существующие в каталоге файлы" — чтобы зашифровать все файлы, за исключением скрытых и системных;
- "шифровать скрытые и системные файлы" — если требуется зашифровать находящиеся в каталоге скрытые и системные файлы.

4. Нажмите кнопку “ОК”. Произведётся шифрование файла

3.7. Назначение уровня конфиденциальности файлам.

1. В программе "Проводник" найдите нужный каталог или файл.

2. Вызовите контекстное меню для ярлыка каталога или файла и активируйте в меню команду "Свойства". На экране появится диалоговое окно настройки свойств каталога или файла.

3. Перейдите к диалогу "Secret Net"(рис. 19).

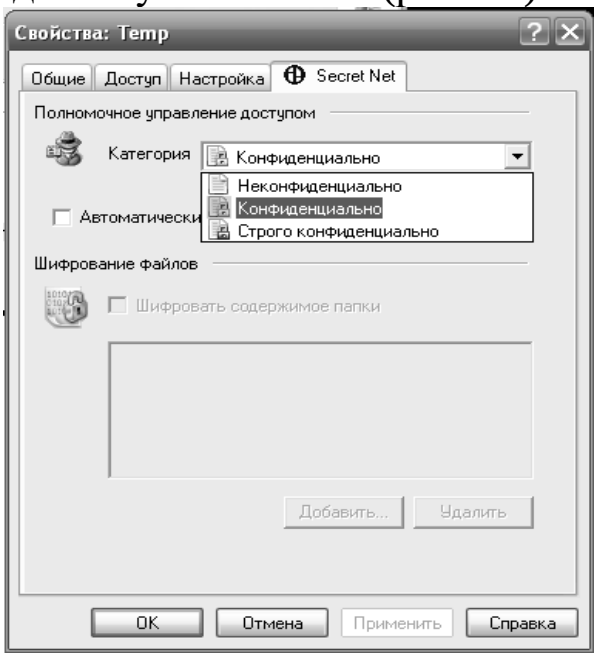

Рис. 19 - Свойства доступа к файлам

4. В разделе полномочное управление доступом в графе «Категория» выберите «Конфиденциально» или «Строго конфиденциально». Появится диалог параметров конфиденциальности (рис. 20).

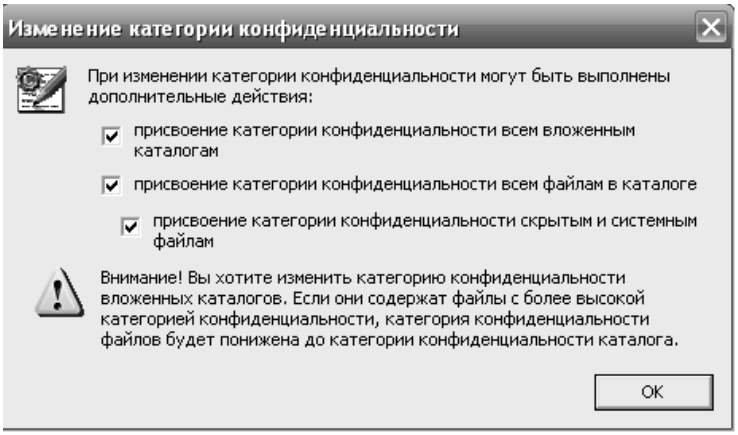

Рис. 20 - Параметры конфиденциальности файла

5. В появившихся пунктах установите отметки по необходимости.

6. Нажмите кнопку «ОК»

3.8. Создание и инициализация дискеты как идентификатора.

1. Выберите *Пуск →Панель управления →Управление компьютером*.

2. В появившимся окне выберите пользователей и перейдите к вкладке SecretNet.

3. В режиме «Идентификатор» выберите «Присвоить». На экране появится диалог присвоения идентификатора (см. рис. 14).

4. Появится приглашение предъявить персональный идентификатор (рис. 16).

5. Нажмите кнопку «Дискета» и вставьте дискету в дисковод.

6. Для завершения работы мастера нажмите кнопку "Готово" в диалоге с результатами выполненных операций.

Диалог мастера закроется и в списке появится новый идентификатор пользователя (рис. 21).

Рис. 21 - Новый идентификатор пользователя

7. Для инициализации дискеты выберите кнопку «Инициализировать» и в появившемся окне выберите «Дискета» и вставьте её в дисковод для считывания.

3.9. Создание ключа на дискете и редактирование времени смены ключей и их срока действия.

- Выберите *Пуск →Панель управления →Управление компьютером*
- В появившимся окне выберите пользователей и перейдите к вкладке SecretNet.
- Перейдите в режим «Криптоключ» (рис. 22).

Рис. 22 - Диалог работы с криптоключами пользователя

- Нажмите кнопку «Выдать». В появившемся окне выберите «Игнорировать старый закрытый ключ пользователя» если на дискете нет уже готового закрытого ключа. Введите в поле слово "продолжить" (без кавычек) и нажмите кнопку "Далее >".
- На экране появится диалог Мастера, отображающий ход выполнения операций, и приглашение предъявить идентификаторы (рис. 23).

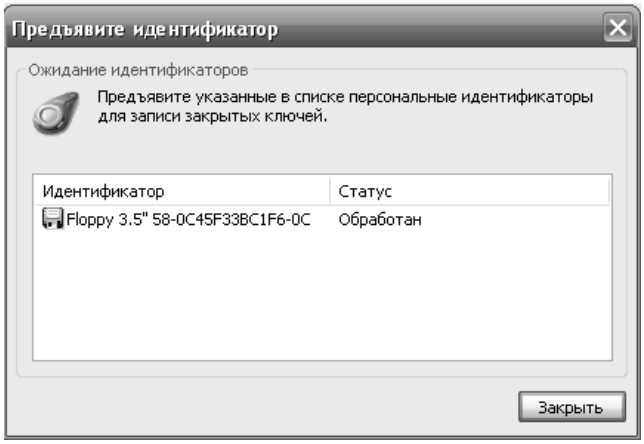

Рис. 23 - Окно предъявления идентификатора

- Предъявите дискету. После успешной записи ключа в очередной идентификатор, его статус принимает значение "Обработан". Если во время записи произошла ошибка, статус соответствующего идентификатора примет значение "Ошибка записи".
- Нажмите кнопку "Готово". Диалог Мастера закроется и в диалоге "Secret Net 5" появятся ведения о ключах пользователя.
- Для редактирования времени смены ключей и их срока действия выберите в «Панели инструментов» откройте оснастку «Локальная политика безопасности».
- Откройте узел "Параметры Secret Net" и выберите папку "Ключи пользователя".В правой части появится список параметров ключей и их значения, установленные по умолчанию (рис. 30).

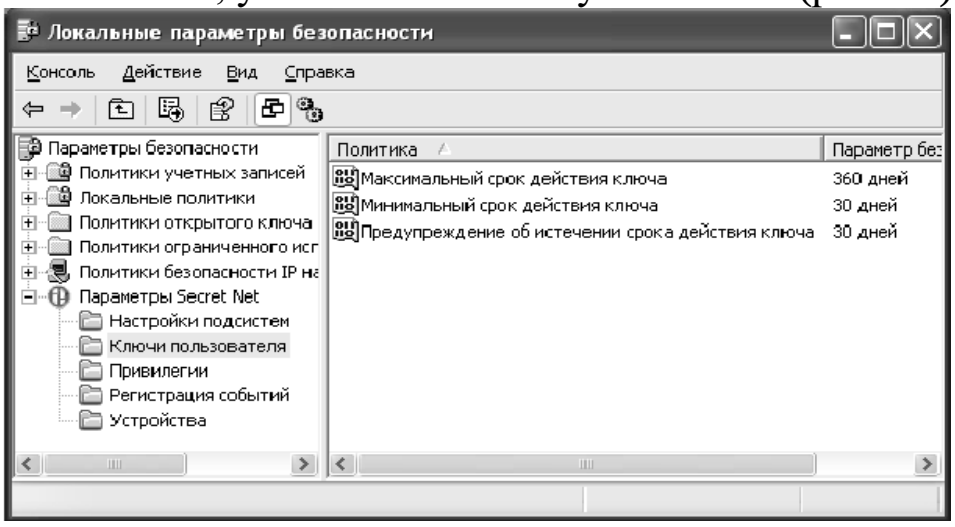

Рис. 24 - Редактирования времени смены ключей

- Вызовите контекстное меню для строки с названием настраиваемого параметра и активируйте в нем команду "Свойства". Появится диалог, предназначенный для установки значения параметра (рис. 25).
- Установите нужное значение и нажмите кнопку "ОК".

3.10. Копирование ключа с дискеты на iButton.

1. Выберите в оснастке "Управление компьютером" пользователя, откройте окно его свойств и в диалоге "Secret Net 5" перейдите в режим "Криптоключ".

2. Нажмите кнопку "Копировать". Появится диалог предъявления идентификатора (рис. 25).

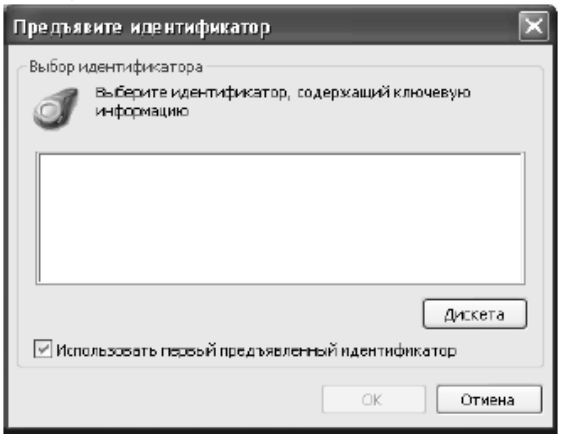

Рис. 25 - Окно предъявления идентификатора

3. Вставьте дискету с ключами в дисковод и нажмите кнопку "Дискета".

4. В диалоге появится информация о дискете (рис. 33).

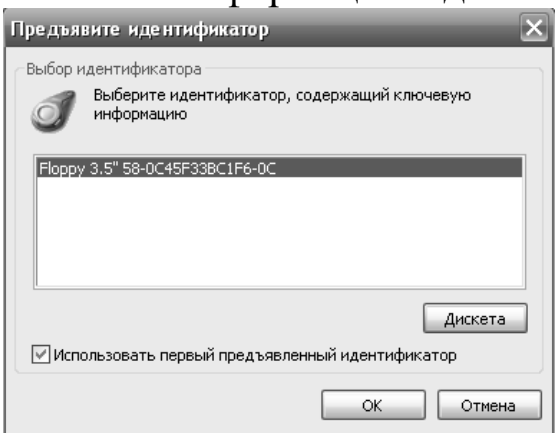

Рис. 26 - Информация по предъявленной дискете

5. Нажмите кнопку "OK".

Ключ будет считан с дискеты и на экране появится диалог со списком идентификаторов пользователя, не содержащих ключа (в данном случае такими идентификатором является iButton).

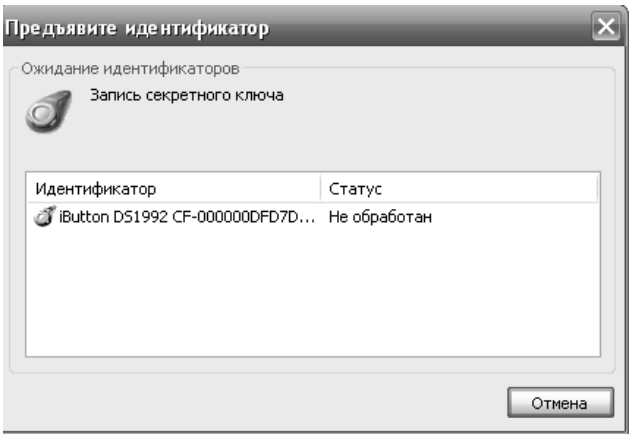

Рис. 27 - Идентификаторы не содержащие ключей

6. Предъявите идентификатор.
7. Нажмите кнопку "Закрыть".

Чтобы проверить, что ключ скопировался, перейдите в диалоге "Secret Net 5" в режим "Идентификатор" и в списке идентификаторов пользователя убедитесь в наличии отметки о хранении ключа.

3.11. Добавление задачи контроля прикладных программ.

Целью данного этапа настройки является построение в модели данных списка всех остальных задач (помимо ресурсов Windows и Secret Net 5.0). Используется для этого специальное средство — механизм генерации задач. Задачи создаются на основании сведений об установленных на компьютере программных продуктах. Для задач контроля целостности используются сведения MS Installer, а для замкнутой программной среды — ярлыки меню "Пуск" ОС Windows.

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

1. Выберите «Пуск», затем «Secret Net» - программу «Контроль программ и данных».
2. Выберите в меню «Сервис» команду «Генератор задач» (рис. 28).

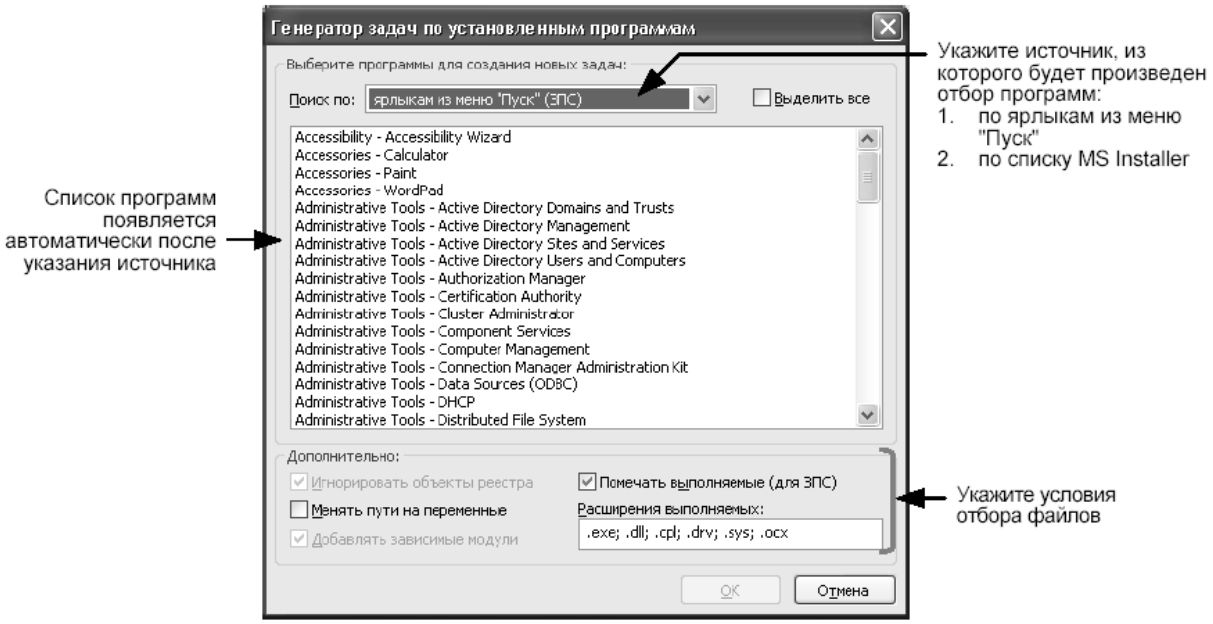

Рис. 28 - Генератор задач контроля программ

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

Укажите в поле "Поиск по" — из какого списка должны выбираться программы.

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

Таблица 4. - Пояснение условий отбора

Условие	Пояснение
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 переменных окружения ОС Windows.
Добавлять зависимые модули	К ресурсам добавляются зависимые модули.

5. Нажмите кнопку "ОК". Начнется процесс генерации и появится сообщение об успешном его завершении.

6. Нажмите кнопку "ОК" в окне сообщения.

В модель данных будут добавлены новые задачи(рис. 29).

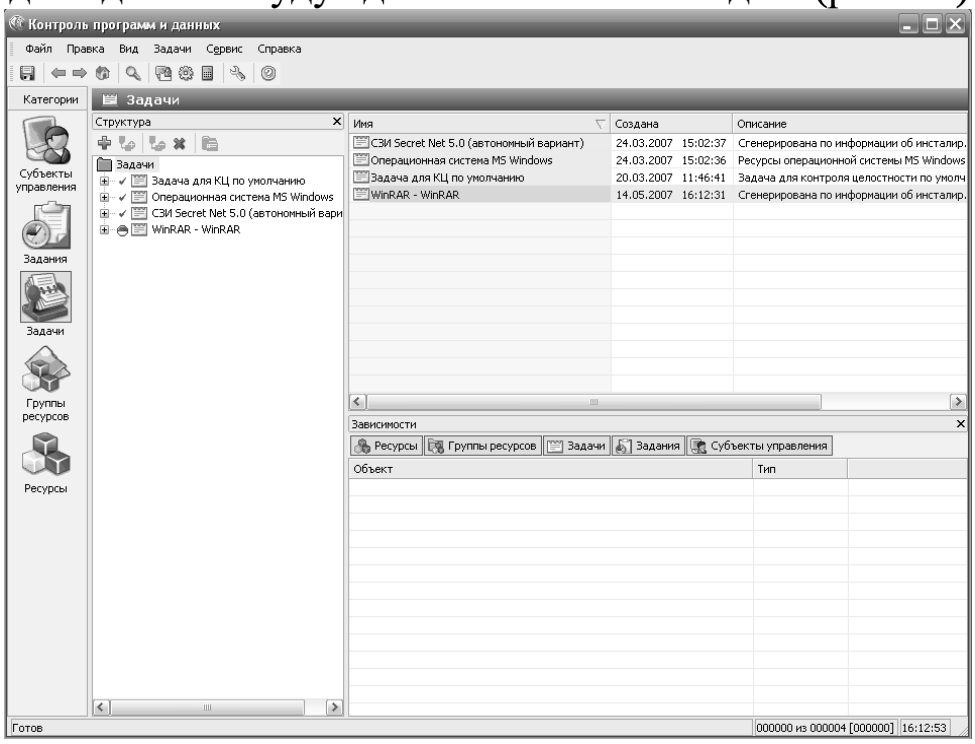

Рис. 29 - Добавление новых задач в модель

3.12. Формирование заданий и включение в них задач

Цель данного этапа — сформировать задания на основе задач, созданных на предыдущем этапе. Для заданий контроля целостности должна быть выполнена настройка, в которой указываются:

- методы и алгоритмы контроля защищаемых ресурсов;
- реакция системы в случаях нарушения целостности контролируемых ресурсов;
- перечень событий, регистрируемых в журнале;
- расписание, в соответствии с которым должна проводиться проверка.

Настройка выполняется в соответствии с планом, разработанным при составлении требований к защитным механизмам.

Для формирования задания:

1. Активируйте ярлык категории "Задания" на панели категорий.
2. Выберите в меню команду "Задания | Создать задание".

Появится диалог выбора типа задания (КЦ или ЗПС) (рис. 30).

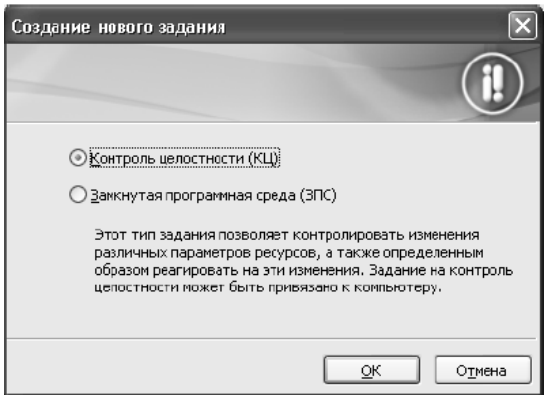

Рис. 30 - Выбор задания

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

Если выбрана замкнутая программная среда, появится диалог назначения имени заданию.

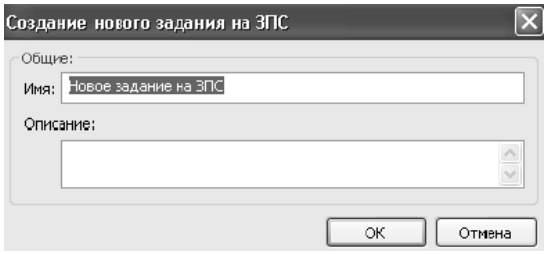

Рис. 31 - Назначение имени заданию

Если выбран контроль целостности, появится диалог создания нового задания на КЦ.

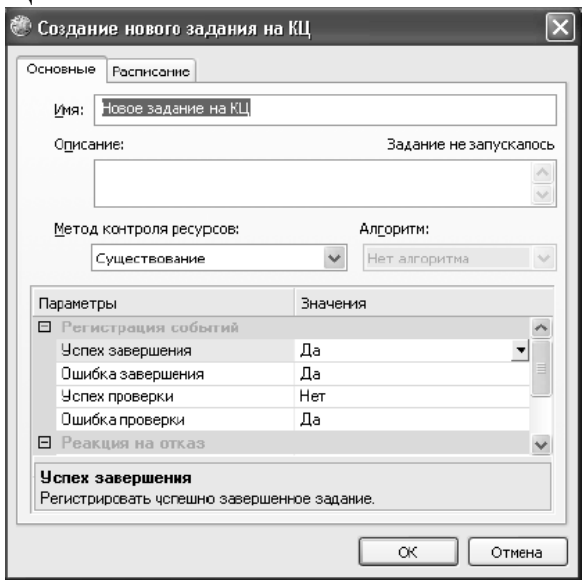

Рис. 32 - Создание задания на контроль целостности

4. Если была выбрана замкнутая программная среда, введите имя задания, его краткое описание и нажмите кнопку "OK". Если был выбран контроль целостности, перейдите к следующему пункту процедуры.

5. Введите имя и краткое описание задания.

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

Предусмотрено 4 метода показанных в таблице 5.

Таблица 5. - Методы контроля ресурсов

Метод контроля	Что проверяется
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.

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

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 событие регистрировалось. Предусмотрена регистрация 4-х событий (таблица 6).

Таблица 6. - Описание регистрируемых событий

Событие	Описание события
Успех завершения	Обработка задания контроля завершено успешно.
Ошибка завершения	Обнаружено нарушение целостности при обработке задания.
Успех проверки	Проверка целостности ресурса завершена успешно.
Ошибка проверки	Нарушение целостности ресурса.

8. Настройте реакцию системы на отказ. Для этого выделите в столбце "Параметры" строку "Действие", а в столбце "Значения" выберите нужный вариант. Предусмотренные варианты представлены в таблице 7.

Таблица 7. - Описание реакций системы

Реакция	Пояснение
Игнорировать	Реакция системы на отказ 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.

9. Перейдите к диалогу "Расписание" и составьте расписание контроля в соответствии с требованиями к заданию (рис. 33).

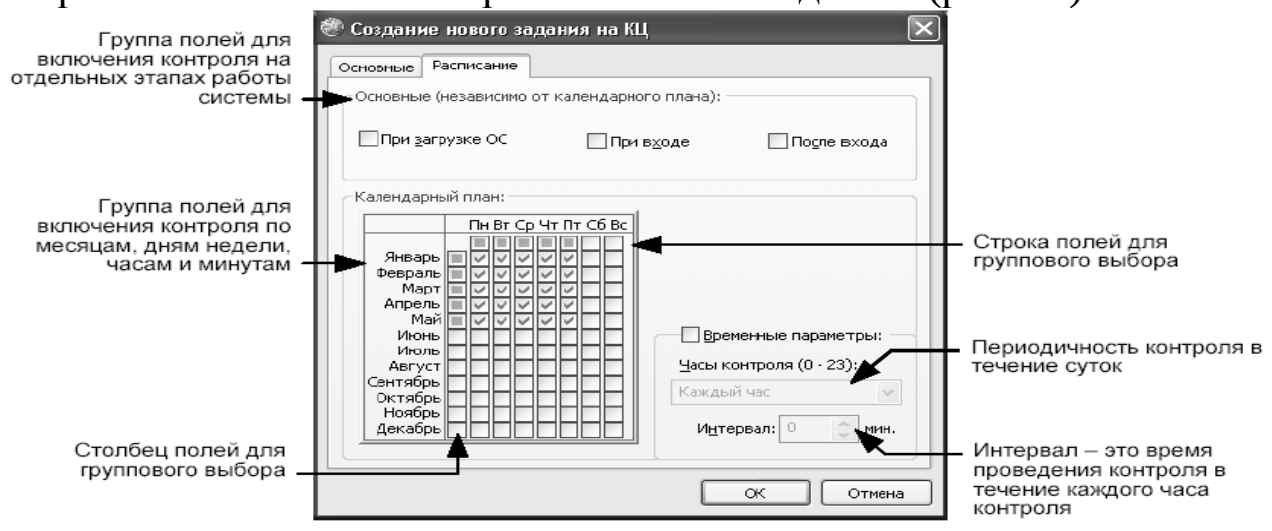

Рис. 33 - Составление нового расписании на контроль целостности

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.

10. Нажмите кнопку "OK".

В дополнительном окне структуры появится новое задание контроля целостности, не связанное с субъектами.

11. Активируйте ярлык категории "Задания" на панели категорий.

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 (рис. 34).

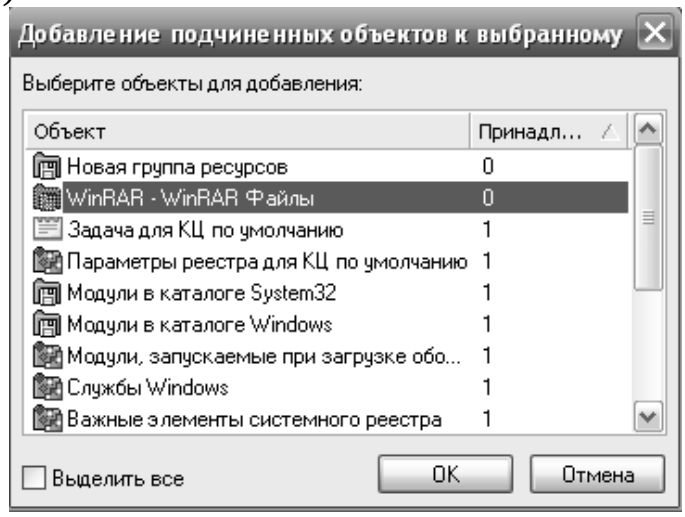

Рис. 34 - Каталог выбора объектов

В диалоге представлен список всех задач и групп ресурсов, еще не включенных в данное задание.

12. Выберите задачи, которые следует включить в задание.

13. Нажмите кнопку "OK".

Выбранные задачи будут включены в задание.

4. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ.

1. Создать трех пользователей (user1, user2, user3) и назначить им права доступа:

User 1 – имеет права администратора, имеет персональный идентификатор на iButton с записанным на него криптографическим ключом. Обладает максимальным уровнем доступа, способен назначать уровень доступа другим пользователям, может шифровать файлы с помощью своего ключа. Способен свободно читать файлы других пользователей. Назначает уровень конфиденциальности файлам. Идентификация по электронному ключу.

User 2 – способен запускать программы «Excel» и «Word», может просматривать содержимое всех папок на компьютере, записывать может только в одну папку, назначенную администратором. Также пользователь способен читать файлы зашифрованные пользователем User 1. Идентификация по дискете.

User 3 – способен запускать только программы «Блокнот» и «Paint», способен записывать файлы только в одну папку, назначенную администратором. Не может в входить папки диска. Запрещены съёмные диски. Идентификация по паролю.

2. Проверить назначенные пользователям полномочия. Привести скриншоты работающих режимов.

3. Зашифровать файл пользователем User 1 и попытаться прочитать его пользователями User2 и User3. Привести скриншоты результатов.

4. Попытаться получить доступ пользователем User3к программам в закрытой программной среде. Привести скриншоты результатов.

5. СОДЕРЖАНИЕ ОТЧЁТА.

1. Титульный лист.
2. Цель работы.
3. Задание на лабораторную работу.
4. Ход работы.
5. Выводы по работе.

6. ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Назовите основные возможности системы Secret Net.
2. Охарактеризуйте персональный идентификатор и работу с ним.
3. Назовите и кратко охарактеризуйте основные средства управления Secret Net.
4. Назовите и охарактеризуйте функции аппаратных средств системы Secret Net.
5. Каким образом происходит назначение прав пользователям?
6. Какие механизмы замкнутой программной среды реализуются средствами Secret Net?
7. Опишите механизм распределения и хранения ключей пользователей.

7. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационная безопасность офиса. Выпуск 1. Технические средства защиты информации [Текст]: учеб. пособие / : ТИД «ДС», 2003, 216 с.
2. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст]: учеб.пособие/ Платонов В.В.: Академия, 2006, 416 с.
3. Черкесов, Г.А. Надежность аппаратно-программных комплексов[Текст]: учеб.пособие/ Г.А.Черкесов, С.-Петербург,: Питер, 2004, 510 с.
4. Руководство по администрированию системы Secret Net [электронный ресурс] : инстр. по прим. / «Информзащита», 2006, 219с.