Кафедра: Информационные Технологии

Лабораторная Работа

На тему: **Настройка механизмов контроля и регистрации**

**Москва, 2008 год**

**1. Контроль целостности**

Контроль целостности – функция системы защиты, которая предназначена для слежения за изменением параметров заданных ресурсов. Система Secret Net контролирует целостность каталогов, файлов, элементов системного реестра.

Контролируются следующие параметры:

целостность содержимого ресурса;

права доступа и владения;

атрибуты DOS;

существование ресурса.

Для организации контроля целостности необходимо определить список ресурсов, подлежащих контролю, и сформировать задание на контроль, в котором указать:

тип контролируемых данных;

алгоритм выполнения;

реакцию системы на результаты контроля;

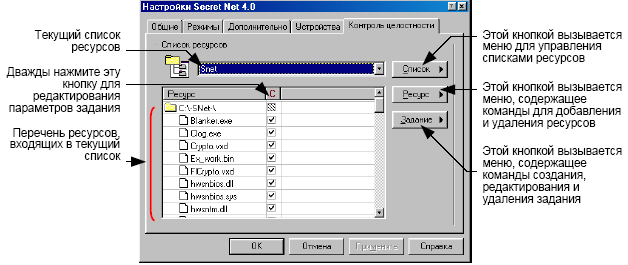
расписание проведения контроля.

Для настройки механизма контроля целостности необходимо:

Вызвать на экран окно настройки общих параметров.

Активизировать диалог «Контроль целостности».

Группа полей «Список ресурсов» содержит название списка ресурсов и перечень ресурсов, представленный в виде таблицы. Каждая строка этой таблицы содержит в столбце «Ресурс» имя ресурса и полный путь к нему. Заголовки остальных столбцов содержат пиктографические обозначения заданий на контроль целостности. Отметки, установленные в столбцах, указывают, какое задание назначено для контроля целостности ресурса.



**Рис. 32. Диалог «Контроль целостности»**

Выбрать в поле с открывающимся списком название списка ресурсов, настройку которого необходимо выполнить, или создать новый список ресурсов.

Выполнить необходимые действия.

Нажать кнопку «ОК».

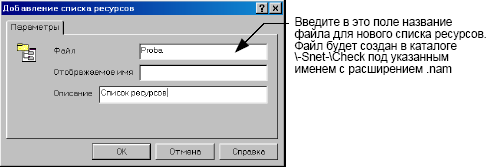
Большинство изменений в настройках диалога будет записано в базу данных контроля целостности только после сохранения общих параметров. Однако результат выполнения некоторых операций записывается в базу данных немедленно, и не может быть отменен при закрытии окна управления общими параметрами.

**1.1 Создание списка ресурсов**

Для создания списка ресурсов необходимо:

Нажать кнопку «Список >«.

Активизировать команду «Добавить». На экране появится диалог создания списка ресурсов:



**Рис. 33. Добавление нового списка ресурсов**

Ввести в поле «Файл» название файла, в котором будет храниться создаваемый список ресурсов.

Ввести в поле «Отображаемое имя» название списка, которое будет отображаться в перечне имеющихся списков ресурсов.

Поле «Отображаемое имя» необходимо оставить пустым, если название списка должно совпадать с названием файла. В этом случае программа автоматически заполнит это поле значением, указанным в поле «Файл».

Если это необходимо, ввести дополнительную информацию о создаваемом списке ресурсов в текстовом поле «Описание».

Нажать кнопку «ОК».

Новый список ресурсов будет создан и его название добавится в перечень имеющихся списков ресурсов.

**1.2 Изменение свойств списка ресурсов**

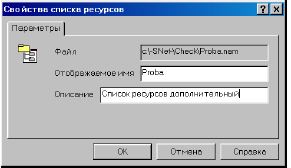
Для изменения свойств необходимо:

Выбрать в поле с открывающимся списком название списка ресурсов.

Нажать кнопку «Список >«.

Активизировать команду «Свойства».

На экране появится диалог «Свойства списка ресурсов»:



**Рис. 34. Свойства списка ресурсов**

Отредактировать содержание полей «Отображаемое имя» и «Описание».

Нажать кнопку «ОК».

**1.3 Удаление списка ресурсов**

Для удаления списка ресурсов необходимо:

Выбрать в поле с открывающимся списком название удаляемого списка ресурсов.

Нажать кнопку «Список>«.

Активизировать команду «Удалить».

Подтвердить удаление текущего списка ресурсов в окне запроса.

Подтвердив удаление списка невозможно отменить удаление, закрыв окно управления общими параметрами без сохранения изменений.

**1.4 Управление составом списка ресурсов**

Управление составом списка ресурсов осуществляется с помощью команд меню кнопки «Ресурс»:

«Удалить» – для удаления одного или нескольких ресурсов из списка;

«Добавить/Удалить» – для удаления или добавления ресурсов в список.

Для удаления ресурса из списка необходимо:

Выбрать в таблице диалога «Контроль целостности» ресурс, который требуется удалить.

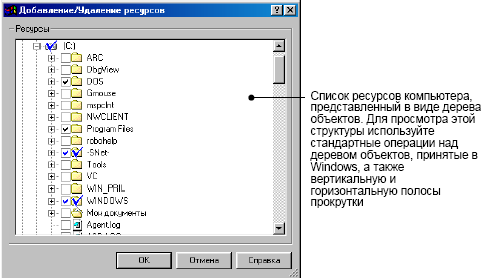
Нажать кнопку «Ресурс>«.

Активизировать команду «Удалить».

Подтвердить удаление ресурса в окне запроса.

Для изменения состава списка:

Нажать кнопку «Ресурс>« и выбрать в меню команду «Добавить/Удалить». На экране появится диалог для корректировки текущего списка ресурсов:



**Рис. 35. Добавление (удаление) ресурсов**

Откорректировать список ресурсов:

С помощью команд контекстного меню

Подведя курсор к имени диска или каталога, нажать правую кнопку мыши и активизировать в появившемся контекстном меню команду:

«Отметить вложенные ресурсы» – чтобы добавить в список файлы и подкаталоги первого уровня иерархии;

«Отметить все вложенные ресурсы» – чтобы добавить в список все вложенные файлы и подкаталоги;

«Очистить вложенные ресурсы» – если требуется исключить из списка подкаталоги и файлы первого уровня иерархии;

«Очистить все вложенные ресурсы» – для исключения из списка всех вложенных подкаталогов и файлов.

Вручную

Чтобы добавить ресурс – установить отметку слева от имени ресурса;

Чтобы исключить ресурс из списка – удалить отметку слева от имени ресурса.

Нажать кнопку «ОК».

**1.5 Формирование задания на контроль целостности**

Задания на контроль целостности формируются для каждого списка ресурсов. Для списка ресурсов можно составить одно или несколько заданий и в дальнейшем управлять ими (включать и выключать, изменять параметры). Для каждого задания формируется расписание, в соответствии с которым будет проводиться контроль целостности.

Для формирования задания необходимо:

Выбрать в поле с открывающимся списком название списка ресурсов.

Нажать кнопку «Задание>«.

Активизировать команду «Добавить».

Настроить общие параметры задания в диалоге «Общие».

Составить расписание контроля в диалоге «Расписание».

Нажать кнопку «ОК».

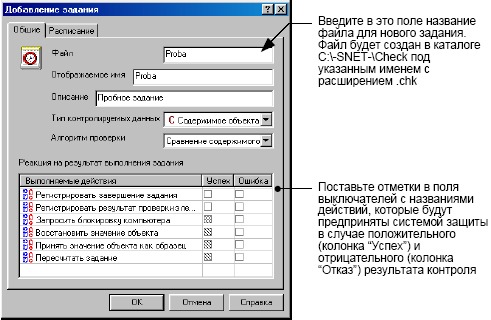
Программа возвратится к диалогу «Контроль целостности». В таблице диалога появится новый столбец, соответствующий сформированному заданию на контроль целостности для текущего списка ресурсов.

Нажать кнопку «ОК» или «Применить» в окне настройки общих параметров.

Для настройки общих параметров задания необходимо:

Активизировать диалог «Общие» (если активен другой диалог).

На экране появится диалог:



**Рис. 36. Диалог «Общие» (задание на контроль целостности)**

Ввести в поле «Файл» название файла, в котором будет храниться создаваемое задание.

Ввести в поле «Отображаемое имя» название задания, которое будет отображаться в списке заданий на контроль целостности.

Если оставить поле «Отображаемое имя» пустым, то название списка будет совпадать с названием файла. В этом случае программа автоматически заполнит это поле значением, указанным в поле «Файл».

Если это необходимо, ввести дополнительную информацию о задании в текстовом поле «Описание».

Выбрать в открывающемся списке поля «Тип контролируемых данных»:

содержимое объекта (С) – чтобы создать задание на контроль целостности содержимого ресурсов;

атрибуты объекта (А) – чтобы создать задание на контроль установленных для ресурсов атрибутов DOS;

список доступа (S) – для создания задания на контроль установленных для ресурсов атрибутов Secret Net;

существование объектов (P) – если необходимо создать задание на контроль существования ресурсов.

Для контроля целостности содержимого ресурсов - указать алгоритм контроля в поле «Алгоритм проверки».

Полный перечень алгоритмов контроля для всех типов контролируемых данных представлен в таблице ниже.

Алгоритмы контроля атрибутов объекта, списка доступа и существования объекта определяются автоматически.

*Таблица 1*

**Алгоритмы контроля**

|  |  |
| --- | --- |
| Название | Характеристика |
| Сравнение содержимого | Проверка целостности содержимого ресурсов. Скорость выполнения – средняя, надежность – высокая |
| Проверка содержимого CRC-7 | Проверка целостности содержимого ресурсов. Скорость выполнения – высокая, надежность – низкая, дополнительных аппаратных средств не требуется |
| Проверка содержимого Имитовставка | Проверка целостности содержимого объектов. Скорость выполнения – средняя, надежность – высокая, требуется дополнительное аппаратное средство для хранения секретного ключа |
| Проверка содержимого Хэш | Проверка целостности содержимого ресурсов. Скорость выполнения – средняя, надежность – высокая |
| Проверка содержимого ЭЦП | Проверка целостности содержимого ресурсов Скорость выполнения – низкая, надежность – высокая |
| Сверка атрибутов | Проверка атрибутов файлов, даты создания и т.п. |
| Проверка прав доступа | Проверка прав доступа пользователей к ресурсам |
| Проверка существования | Проверка наличия ресурса |

Определить в таблице «Реакция на результат выполнения задания» действия, которые будут предприняты системой защиты в зависимости от результатов контроля в случае успеха и в случае неудачи (отказа):

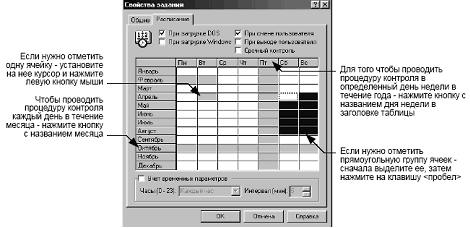
*Таблица 2*

**Реакция на результат выполнения задания**

|  |  |
| --- | --- |
| Регистрировать завершение задания | Результаты выполнения задания регистрируются в журнале безопасности |
| Регистрировать результат проверки элементов | Результаты контроля каждого элемента задания (ресурса) регистрируются в журнале безопасности |
| Запросить блокировку компьютера | При нарушении целостности, компьютер будет заблокирован, если в настройках свойств пользователя задан параметр «Запрет работы при нарушении целостности» |
| Восстановить значение объекта | При нарушении целостности контролируемых ресурсов текущие значения контролируемых параметров (атрибуты объекта, список доступа, содержимое объекта при выполнении сравнения содержимого) устанавливаются равными эталонным значениям |
| Принять значение объекта как образец | При нарушении целостности контролируемых ресурсов новые значения контролируемых параметров, полученные в ходе проверки, становятся эталонными |
| Пересчитать задание | Однократно выполняется пересчет задания. Полученные новые значения контролируемых параметров становятся эталонными. |

Для составления расписания:

Активизируйте диалог «Расписание». На экране появится следующий диалог:



**Рис. 37. Диалог «Расписание» (задание на контроль целостности)**

Активизируйте специальные режимы контроля целостность ресурсов, установив отметки в поля выключателей верхней части диалога:

При загрузке DOS – процедура контроля проводится при загрузке DOS;

При использовании данного режима:

недопустимы символы кириллицы в названиях списка ресурсов, путей и имен файлов в перечне ресурсов, названиях заданий;

длина полного пути ресурса не должна превышать 128 символов;

имя ресурса и название задания не должно превышать 8 символов;

запрещается использовать режим для сетевых ресурсов и элементов системного реестра;

данный режим разрешается использовать только для следующих типов контролируемых данных: «Содержимое объекта» (алгоритм «имитовставка»), «Список доступа».

При загрузке Windows – процедура контроля целостности осуществляется при загрузке графической среды ОС Windows 9x;

При смене пользователя – процедура контроля проводится при повторном входе в систему без перезагрузки компьютера;

При выходе пользователя – процедура контроля проводится после завершения каждого сеанса работы пользователя;

Срочный контроль – проведение одноразового контроля немедленно после сохранения параметров задания.

Сформируйте календарный график проведения контроля. Чтобы определить дни проведения контроля необходимо выделить соответствующие ячейки таблицы. Для того чтобы снять отметки нужно повторить те же действия еще раз.

Если расписание контроля целостности составляется без учета временных параметров - контроль будет осуществляться не менее одного раза в те дни, которые заданы календарным графиком.

Если дополнительно требуется определить периодичность проведения контроля в течение суток, установите отметку в поле «Учет временных параметров». При этом станут доступными для изменений поля нижней части диалога.

Если календарный график задан, контроль будет осуществляться в указанное время в соответствии с графиком, иначе – ежедневно в указанное время.

Указать в поле «Часы (0-23)» периодичность проведения контроля в течение суток.

Выбрать из раскрывающегося списка значение периодичности контроля. Например, «Каждые 4 часа», что означает – «проводить контроль каждый четвертый час суток», контроль будет проводиться в 0, 3, 7, 11, и т.д.

Часы контроля можно задать, указав конкретные значения. Например, если ввести с клавиатуры следующую строку «2, 7-9, 16-18, 21», то контроль будет проведен в 2, 7, 8, 9, 16, 17, 18 и 21 час. Следует иметь в виду, что отсчет начинается с нулевого часа.

Указать в поле «Интервал (мин.)» периодичность проведения контроля в течение каждого заданного часа контроля.

Параметр может принимать значения от 0 до 59 минут. Так, например, если контроль должен проводиться в 7 часов, а в поле «Интервал» указано значение 10, то процедура контроля первый раз выполнится в 7 часов 0 минут, а затем будет повторяться каждые 10 минут в течение этого часа. Если указано значение «0», то периодичность проведения контроля не задана и контроль выполняется в начале часа один раз.

Нажмите кнопку «ОК».

**1.6 Управление заданиями**

После того как для списка ресурсов сформированы задания на контроль целостности можно удалить задание, включить и отключить задание для отдельных входящих в него ресурсов, а также редактировать параметры задания.

Столбцы таблицы ресурсов, начиная со второго, соответствуют заданиям контроля целостности. Заголовки столбцов одновременно являются и кнопками. Пиктограммы кнопок-заголовков соответствуют типам контролируемых данных:

С – содержимое объекта;

А – атрибуты объекта;

S – список доступа;

Р – существование объекта;

Выключатели таблицы определяют состояние задания для ресурса: выполняется оно, не выполняется или оно не применимо.

Для изменения параметров задания необходимо:

Выбрать список ресурсов, для которого необходимо изменить задание на контроль целостности.

Нажать кнопку «Задание>«, выберите в появившемся меню название задания, затем команду «Свойства». Или дважды нажать в заголовке таблицы кнопку с пиктограммой задания, параметры которого необходимо изменить.

Изменить параметры задания в диалоге «Общие»:

сведения о задании в полях «Отображаемое имя» и «Описание»;

действия, которые будут предприняты системой защиты в зависимости от результатов контроля, в таблице «Реакция на результат выполнения задания».

При изменении свойств задания значения полей «Файл», «Тип контролируемых данных» и «Алгоритм проверки» изменить нельзя.

Составить расписание проведения контроля в диалоге «Расписание».

Нажать кнопку «ОК».

Новые параметры задания будут записаны в базу данных контроля целостности только после сохранения общих параметров системы.

Нажать кнопку «ОК» или «Применить» в окне настройки общих параметров.

Для удаления задания необходимо:

Выбрать в поле с открывающимся списком название списка ресурсов, из которого необходимо удалить задание на контроль целостности.

Нажать кнопку «Задание>«.

Выбрать в появившемся меню название задания, затем команду «Удалить».

Подтвердить свое решение в появившемся окне запроса.

Для управления заданиями необходимо:

Чтобы включить (активировать) для ресурса задание необходимо установить отметку в поле выключателя на пересечении строки, содержащей информацию о ресурсе, и столбца, соответствующего заданию.

Чтобы отключить для ресурса задание необходимо удалить отметку из поля выключателя на пересечении строки, содержащей информацию о ресурсе, и столбца, соответствующего заданию.

**1.7 Пересчет контролируемых параметров**

Пересчет эталонных значений контролируемых параметров (контрольных сумм, атрибутов и др.) может потребоваться при изменении состава списка контролируемых ресурсов, изменении содержимого или атрибутов ресурсов, входящих в список.

Для пересчета контрольных сумм необходимо:

Выбрать список ресурсов.

Откорректировать список ресурсов.

Нажать кнопку «OK» или «Применить» в окне управления общими параметрами. В результате выполненных действий для всех заданий на контроль целостности данного списка ресурсов будут пересчитаны контролируемые параметры и приняты в качестве эталонных.

Для пересчета контрольных сумм необходимо:

Выбрать в поле с открывающимся списком название списка ресурсов.

Нажать кнопку «Задание>«, выберите в появившемся меню название задания, затем команду «Свойства». Или дважды нажать в заголовке таблицы кнопку с пиктограммой задания.

В таблице «Реакция на результат выполнения задания» диалога «Общие» поставить отметку в поле «Пересчитать задание».

Активизировать диалог «Расписание» и отметить поле «Срочный контроль».

Нажать кнопку «ОК».

Нажать кнопку «OK» или «Применить» в окне управления общими параметрами.

Пересчет параметров ресурсов, контролируемых данным заданием, выполняется немедленно. Новые значения параметров принимаются в качестве эталонных.

**2. Регистрация событий**

Работа механизма регистрации событий определяется следующими настройками:

параметрами настройки журнала безопасности;

индивидуальным режимом регистрации событий для каждого пользователя.

**2.1 Настройка параметров журнала безопасности**

Для настройки параметров необходимо:

Вызвать на экран окно управления общими параметрами.

Активизировать диалог «Общие».

Выбрать в поле «Диск для хранения системного журнала» имя локального логического диска, на котором будет накапливаться журнал событий. По умолчанию предлагается диск [С:]. Если для ведения журнала выбран диск, отличный от диска [C:], на нем создается каталог -SNET-.

Если ядро системы защиты не обнаружит заданный диск, журнал будет накапливаться на диске [C:]. Если диск, на котором накапливается системный журнал, переполнен, доступ всех пользователей к компьютеру блокируется, за исключением пользователя, являющегося администратором по умолчанию (обладающего привилегией «Без ограничений по настройкам»).

Указать в поле «Количество дней хранения системного журнала» срок хранения записей в журнале событий. По истечении указанного числа дней записи автоматически удаляются из журнала. Этот параметр может принимать значения от 0 до 365 дней («0» означает - срок хранения записей журнала не ограничен).

Нажать кнопку «ОК».

**2.2 Настройка режима регистрации событий для пользователя**

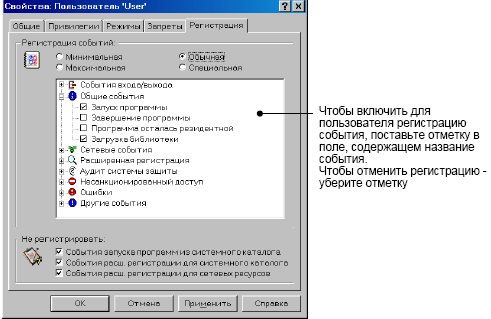
Для каждого пользователя компьютера может быть составлен персональный перечень событий, которые будут регистрироваться в журнале безопасности после идентификации пользователя.

Для настройки режима:

Вызвать на экран окно управления свойствами пользователя.

Активизировать диалог «Регистрация»:

Группа полей «Регистрация событий» позволяет определить для пользователя перечень регистрируемых событий. События, регистрируемые для пользователя в данный момент, имеют отметку слева от названия события. В системе Secret Net предусмотрены три стандартных режима регистрации событий: обычная, минимальная и максимальная регистрация. В режиме специальной регистрации (переключатель «Специальная») перечень регистрируемых событий не соответствует ни одному из стандартных режимов регистрации.



**Рис. 38. Диалог «Регистрация»**

Определить режим регистрации событий.

Чтобы определить перечень событий, регистрируемых при специальной регистрации, используйте выключатели списка событий.

Чтобы определить перечень программ, необходимых пользователю для повседневной работы (например, при формировании списка программ, разрешенных пользователю для запуска), необходимо включить регистрацию событий «Запуск программы» и «Загрузка библиотеки» из списка событий, входящих в состав группы «Общие события».

Для регистрации попыток доступа к файлам, которым присвоены дополнительные атрибуты «Аудит чтения» и «Аудит записи», необходимо включить регистрацию событий «Чтение из файла» и «Запись в файл», входящих в группу «Расширенная регистрация».

Чтобы установить для пользователя один из стандартных режимов, поставьте отметку в поле «Минимальная», «Обычная» или «Максимальная».

Группа выключателей «Не регистрировать» позволяет исключить из регистрации некоторые события. Необходимо установить отметку в поле:

«События запуска программ из системного каталога», чтобы во время работы данного пользователя запретить регистрацию событий, состоящих в запуске программ из системного каталога ОС Windows (\SYSTEM);

«События расш. регистрации для системного каталога», чтобы запретить регистрацию событий, относящихся к группе событий расширенной регистрации, для системного каталога ОС Windows (\SYSTEM);

«События расш. регистрации для сетевых ресурсов», чтобы запретить регистрацию событий, относящихся к группе событий расширенной регистрации, во время работы пользователя со всеми доступными ему сетевыми ресурсами.

Нажать кнопку «ОК».

**Список литературы**

1. Система защиты информации Secret Net 4.0 автономный вариант для Windows 9x. Принципы построения. М: ЗАО НИП «Информзащита», 2003.

2. Система защиты информации Secret Net 4.0 автономный вариант для Windows 9x. Руководство пользователя. М: ЗАО НИП «Информзащита», 2003.