**Лабораторная Работа**

**На тему:**

**Настройка механизмов контроля входа**

**1. Теоретическое введение**

Настройка механизмов контроля входа осуществляется в несколько этапов, последовательность которых приведена в таблице 1.

*Таблица 1*

**Последовательность настройки механизмов контроля входа**

|  |  |
| --- | --- |
| Шаг | Процедура |
| Этап: Настройка параметров, общих для всех пользователей компьютера | |
| 1. | Указать имя пользователя, которое по умолчанию будет отображаться в диалоге запроса имени и пароля при входе пользователей в систему |
| 2. | Задать интервал времени, в течение которого пользователь, осуществляющий вход в систему, может начать ввод своего имени вместо имени, предлагаемого системой по умолчанию |
| 3. | Указать число попыток, которое отводится пользователю для правильного указания своего имени и пароля при входе в систему |
| 4. | Отредактировать системные файлы CONFIG.SYS и AUTOEXEC.BAT. |
| 5. | Определить требования к паролю пользователя: минимальную длину, период времени, на протяжении которого действителен текущий пароль, а также число старых паролей, информация о которых будет храниться системой |
| *Окончание табл. 1* | |
| Шаг | Процедура |
| Этап: Настройка параметров, индивидуальных для каждого пользователя компьютера | |
| 6. | Настроить параметры аутентификации пользователя, такие как: «Запрос пароля при входе», «Постоянный пароль» и «Автоввод пароля при входе в сеть» |
| 7. | Создать персональные версии системных файлов CONFIG.SYS и AUTOEXEC.BAT, если это необходимо |
| 8. | Установить значение параметра «Запрет работы при изменении конфигурации», с помощью которого можно разрешить или запретить вход пользователя в систему при изменении конфигурации компьютера |

### 1.1 Настройка общих параметров входа

Настройка общих параметров, связанных с работой системы защиты на этапе входа пользователей в систему, выполняется в окне управления общими параметрами. После установки системы Secret Net на компьютер, при входе пользователей в систему используются общие версии системных файлов CONFIG.SYS и AUTOEXEC.BAT. В дальнейшем, содержание этих файлов используется в качестве исходного содержания при формировании для каждого конкретного пользователя индивидуальных системных файлов. В том случае, когда для пользователей предполагается создавать персональные версии системных файлов, необходимо откорректировать общие системные файлы CONFIG.SYS и AUTOEXEC.BAT.

Для настройки общих параметров необходимо:

1. Вызвать на экран окно управления общими параметрами Secret Net:

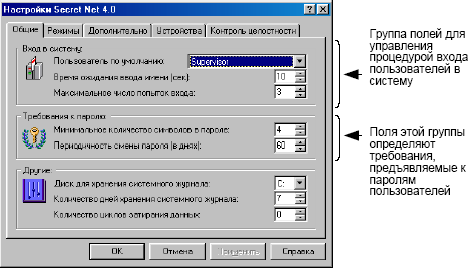


Рис. 14. Окно управления общими параметрами

1. Установить в поле с открывающимся списком «Пользователь по умолчанию» нужное имя пользователя. (Этот параметр не используется при входе пользователя в систему с предъявлением персонального идентификатора.) Если необходимо отказаться от автоматического ввода имени пользователя при входе в систему, выбрать в списке значение «Отсутствует».
2. В поле «Время ожидания ввода имени (сек)» задать интервал времени, в течение которого пользователь, осуществляющий вход в систему, может начать ввод своего имени вместо имени, предлагаемого системой по умолчанию и заданного параметром «Пользователь по умолчанию». По истечении этого интервала времени, если пользователь не начал ввод имени, система защиты автоматически перейдет к вводу пароля. Этот параметр может принимать значения от 0 до 40 секунд («0» – время ожидания ввода имени не ограничено).
3. В поле «Максимальное число попыток входа» указать число попыток, которое отводится пользователю для правильного указания своего имени и пароля при входе в систему. Если пользователь не смог правильно указать имя и пароль за отведенное число попыток - осуществляется блокировка компьютера. Этот параметр может принимать значения от 0 до 10 («0» – количество попыток не ограничено).
4. Нажать кнопку «ОК».

Для корректировки общих системных файлов необходимо:

1. Вызвать на экран окно управления общими параметрами Secret Net:
2. Активизировать диалог «Дополнительно».
3. В группе полей «Профили» выполнить одно из следующих действий:

подвести курсор мыши к строке таблицы, содержащей имя файла, и дважды нажать левую кнопку мыши;

выбрать строку с именем этого файла и нажать кнопку «Редактировать».

На экране появится окно текстового редактора SnEdit, в котором будет открыт выбранный для изменения файл.

1. Отредактировать нужным образом системный файл. Завершив редактирование, сохранить внесенные изменения и закрыть окно редактора SnEdit.
2. Нажать кнопку «ОК».

**1.2 Управление паролями**

#### 1.2.1 Настройка параметров пароля

Настройка параметров пароля, общих для всех пользователей компьютера, осуществляется в окне управления общими параметрами. В диалогах этого окна можно указать минимальное количество символов в пароле, периодичность смены паролей пользователей, а также определить требования к уникальности паролей пользователей.

Для настройки параметров необходимо:

1. Вызвать на экран окно управления общими параметрами Secret Net.
2. Определить минимальную длину пароля пользователя в поле «Минимальное количество символов в пароле». Этот параметр может принимать значения от 0 до 16 («0» означает - разрешено использование пустых паролей, т.е. паролей нулевой длины).

**Примечание.** Пользователю нельзя назначить пароль, количество символов в котором меньше числа, указанного в этом поле. При входе пользователя в систему, длина указанного им пароля сравнивается с этим значением. Если длина указанного пароля меньше установленной минимальной длины - пользователю предлагается сменить пароль.

1. Определить в поле «Периодичность смены пароля (в днях)» период времени, на протяжении которого действителен текущий пароль пользователя. Этот параметр принимает значения от 0 до 365 дней («0» означает - срок действия пароля не ограничен).
2. Активизировать диалог «Дополнительно».
3. Определить в поле «Число паролей, запоминаемое системой» число старых паролей каждого пользователя, информация о которых будет храниться системой. Этот параметр может принимать значения от 0 до 24 («0» означает, что пользователь при смене пароля может указать в качестве нового любой, в том числе свой текущий пароль).
4. Нажать кнопку «ОК».

#### 1.2.2 Правила определения пароля

При определении пароля необходимо соблюдать следующие правила:

1. Пароль может содержать только латинские символы, цифры и служебные символы (символы латинской раскладки клавиатуры). Запрещается использовать символы кириллицы, а также символ «пробел».
2. Разрешается использовать различные регистры клавиатуры (например, «Dog» или «dog»). При этом нужно помнить, что заглавные и строчные буквы воспринимаются как различные («Dog» и «dog» считаются разными паролями).
3. Длина пароля не может быть меньше установленной минимальной длины и не может превышать 16-ти символов.
4. Новый пароль не должен совпадать с теми старыми паролями пользователя, информация о которых хранится системой защиты.

### 1.3 Настройка индивидуальных параметров входа

Настройка параметров, связанных с аутентификацией пользователя на этапе входа в систему, выполняется в окне управления свойствами пользователя.

#### 1.3.1 Настройка параметров аутентификации пользователя

Для настройки параметров необходимо:

1. Вызвать на экран окно управления свойствами пользователя.
2. Установить выключатель «Запрос пароля», который позволяет разрешить или запретить пользователю входить в систему без предъявления пароля:

чтобы разрешить пользователю входить в систему без предъявления пароля необходимо удалить отметку из поля выключателя;

чтобы запретить пользователю входить в систему без пароля необходимо поставить отметку в поле выключателя.

1. Отметить поле «Постоянный пароль», чтобы отключить для пользователя режим устаревания пароля, который ограничивает срок действия текущего пароля пользователя.

Если поле не содержит отметки, срок действия пароля определяется общим параметром системы защиты «Периодичность смены пароля». По истечении заданного этим параметром числа дней, система защиты попросит пользователя сменить текущий пароль и запретит вход пользователя в систему по старому паролю.

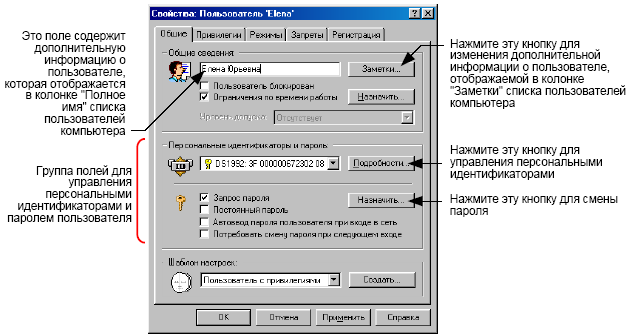


Рис. 15. Окно управления свойствами пользователей

Если имя и пароль пользователя в системе Secret Net, в сетях Novell NetWare и Microsoft Windows совпадают, регистрацию этого пользователя в сети можно упростить следующим образом:

1. Поставить отметку в поле «Автоввод пароля пользователя при входе в сеть», чтобы при подключении к сетям Novell NetWare и Microsoft Windows имя и пароль пользователя вводились автоматически.
2. Установить отметку в поле «Потребовать смену пароля при следующем входе», чтобы включить для пользователя этот режим смены пароля. При входе пользователя в систему на экран будет выведен диалог смены пароля.
3. Нажать кнопку «ОК».

#### 1.3.2 Смена пароля пользователя

Изменить пароль пользователя может только администратор безопасности компьютера или пользователь, который обладает привилегией на администрирование:

«Уровень 1» или выше из группы привилегий «Параметры своей работы» – для изменения своего пароля;

«Уровень 3» из группы привилегий «Параметры работы других пользователей» – для изменения паролей других пользователей компьютера.

Процедура смены пароля позволяет:

1. Сменить пароль пользователя в Secret Net;
2. При соблюдении определенных условий – одновременно сменить пароль пользователя в Secret Net, Windows и сетях;
3. Записать новый пароль в персональный идентификатор, если это необходимо.

Для смены пароля пользователя необходимо:

1. Вызвать на экран окно управления свойствами пользователя.
2. Нажать кнопку «Назначить» в группе полей «Персональные идентификаторы и пароль». На экране появится диалог смены пароля:

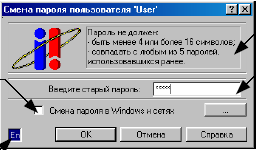


Рис. 16. Смена пароля пользователя

1. Настроить дополнительные параметры процедуры смены пароля, если это необходимо (см. ниже описание процедуры смены пароля в других службах).
2. Ввести текущий пароль в поле «Введите старый пароль» и нажать кнопку «ОК».
3. Ввести новый пароль в поле «Введите новый пароль» и нажать кнопку «ОК».
4. Повторно ввести тот же пароль в поле «Подтвердите пароль» и нажать кнопку «ОК».

Если оба значения нового пароля совпали и требования, предъявляемые к паролю, не были нарушены, смена пароля завершится успешно. Иначе появится сообщение об ошибке. В том случае, если пароль пользователя хранится в персональном идентификаторе, на экране появится запрос на предъявление идентификатора:

1. Предъявить персональный идентификатор. Если пользователю присвоено несколько идентификаторов – последовательно предъявите каждый из них. Новый пароль будет записан в персональные идентификаторы пользователя.

Рекомендуется записывать новый пароль во все имеющиеся у пользователя персональные идентификаторы. В том случае если для записи пароля предъявлен идентификатор eToken, который защищен нестандартным для Secret Net PIN-кодом, на экране появится запрос. Необходимо ввести PIN-код и нажать кнопку «OК».

Можно отказаться от записи нового пароля в один или несколько идентификаторов, нажав кнопку «Отмена» и выбрав вариант завершения процедуры в появившемся окне запроса:

* Нажав кнопку «Нет», можно продолжить процедуру смены пароля и назначить новый пароль пользователю без записи пароля в идентификаторы.

В этом случае после предъявления идентификатора (одного или нескольких) со старым паролем, например, при входе в систему, на экран будет выведен диалог запроса пароля для ввода нового пароля с клавиатуры.

Нажав кнопку «Да», если необходимо прервать процедуру смены пароля и восстановить старый пароль пользователя. На экране появится запрос на восстановление пароля в идентификаторе:

Предъявив персональный идентификатор. Если необходимо восстановить пароль в нескольких идентификаторах – последовательно предъявить каждый из них. Значение старого пароля будет восстановлено, и на экран будет выведено сообщение о результате выполнения операции.

Для отказа от восстановления старого пароля в одном или нескольких идентификаторах нажать кнопку «Отмена».

1. Закрыть окно управления свойствами пользователя.

Для того чтобы наряду с паролем в Secret Net одновременно изменить и другие пароли, необходимо, чтобы имя пользователя было во всех службах одним и тем же.

При смене администратором безопасности пароля любого пользователя компьютера необходимо указывать текущие пароли служб, в которых меняются пароли.

Для смены паролей пользователя в других службах необходимо:

* 1. Установить отметку в поле «Смена пароля в Windows и сетях» (или нажать кнопку «…»).

На экране появится диалог:

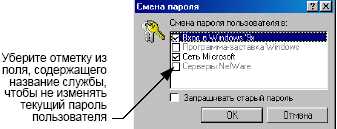


Рис. 17. Смена пароля пользователя

* 1. Определить параметры процедуры:

установить отметку в поле, содержащем название службы, для которой требуется изменить пароль;

в том случае если текущий пароль пользователя в Secret Net не совпадает с текущими паролями служб, в которых необходимо изменить пароль, поставить отметку в поле «Запрашивать старый пароль»;

нажать кнопку «ОК».

* 1. Выполнить шаги 4-7процедуры смены пароля.

В том случае, если текущий пароль пользователя в Secret Net совпадает с другими текущими паролями, пароль пользователя будет изменен без появления дополнительных сообщений на экране. Иначе на экране появится запрос на ввод текущего пароля службы:

* 1. Ввести текущий пароль службы, название которой указано в заголовке диалогового окна, и нажать кнопку «ОК».

Если пароль введен верно, произойдет смена пароля пользователя, иначе на экране появится сообщение об ошибке:

Для отказа от смены пароля пользователя в указанной службе нажать кнопку «Да».

Если требуется повторить попытку смены пароля в указанной службе, отметить поле «Попробовать еще раз с другим старым паролем», нажать кнопку «Да» и повторите ввод старого пароля в появившемся диалоге.

* 1. Указать старые пароли пользователя для остальных служб.

#### 1.3.3 Управление блокировкой пользователя

Для управления блокировкой пользователя необходимо:

1. Вызвать на экран окно управления свойствами пользователя.

**Внимание!** Вход пользователя в систему блокируется системой защиты автоматически, если пользователь:

осуществил попытку войти в систему в нерабочее время;

превысил число попыток, отводящихся ему для правильного указания своего имени и пароля при входе в систему;

своевременно не сменил свой пароль, несоответствующий заданным требованиям к паролям.

В этих случаях отметка автоматически устанавливается в поле выключателя «Пользователь блокирован». Чтобы разрешить вход пользователя в систему необходимо убрать отметку из поля выключателя.

1. В поле «Пользователь блокирован»:

установить отметку, чтобы запретить работу пользователя на компьютере;

удалить отметку, чтобы разрешить пользователю работать на компьютере.

1. Нажать кнопку «ОК».

**1.4 Управление персональными идентификаторами**

Персональный идентификатор пользователя – это аппаратное средство, предназначенное для идентификации пользователя и хранения необходимой служебной информации. В идентификаторе может храниться пароль пользователя, который считывается автоматически при предъявлении идентификатора для входа в систему.

Предъявить идентификатор – это означает, сделать его доступным системе для выполнения необходимых операций (например, чтения или записи). В зависимости от типа устройств эта процедура выполняется по-разному. Идентификатор Touch Memory необходимо приложить к считывателю так, чтобы между ними был надежный контакт, а идентификатор eToken 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 идентификатора. Во всех таких случаях система выведет на экран необходимые сообщения, рекомендациям которых необходимо следовать.

Каждому пользователю можно присвоить несколько идентификаторов разного или одного и того же типа. Нельзя присвоить один и тот же персональный идентификатор нескольким пользователям.

В системе предусмотрены следующие операции с идентификаторами:

инициализация свободного идентификатора;

присвоение идентификатора пользователю или удаление идентификатора из перечня идентификаторов пользователя;

запись пароля в идентификатор или удаление пароля из идентификатора.

При инициализации (форматировании) идентификатора из его памяти удаляется записанная ранее информация и производится разметка носителя информации. Таким образом, выполняется подготовка идентификатора для дальнейшего использования.

Инициализировать можно только идентификатор, который никому не принадлежит.

Для управления персональными идентификаторами необходимо:

1. Вызвать на экран окно управления свойствами пользователя.
2. В группе полей «Персональные идентификаторы и пароль» нажать кнопку «Подробности». На экране появится диалог для управления персональными идентификаторами пользователя.
3. Выполнить необходимые действия.
4. Нажать кнопку «ОК».
5. Закрыть окно управления свойствами пользователя.

Для инициализации персонального идентификатора необходимо:

1. В диалоге «Персональные идентификаторы» нажать на кнопку «Инициализировать…», если на компьютере установлено одно устройство идентификации.
2. Предъявить идентификатор. Если инициализация завершена успешно, появится сообщение об этом.
3. Нажать на кнопку «OK» в окне сообщения.

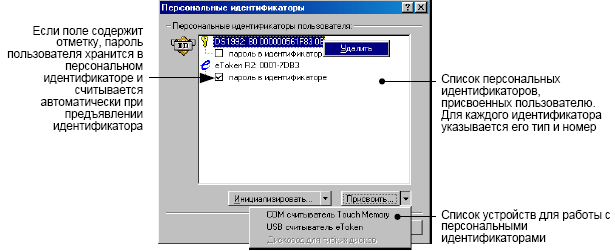


Рис. 18. Диалог «Персональные идентификаторы»

Следует помнить, что инициализировать можно только те идентификаторы, которые не принадлежат ни одному из пользователей.

Для присвоения идентификатора пользователю необходимо:

1. В диалоге «Персональные идентификаторы» нажать кнопку «Присвоить…», если на компьютере установлено одно устройство идентификации.
2. Предъявить идентификатор. Система может обнаружить ошибочный формат идентификатора и потребовать выполнить инициализацию персонального идентификатора. После инициализации повторить процедуру присвоения сначала.

При считывании информации из идентификатора система Secret Net проверяет, не используется ли этот идентификатор другим пользователем компьютера. Если идентификатор не используется другим пользователем, он присваивается данному пользователю, и в списке идентификаторов пользователя появится новая запись. Иначе на экране появится сообщение об ошибке, и предъявленный идентификатор не будет присвоен.

В том случае, если предъявлен идентификатор eToken, содержащий нестандартный PIN-код, на экране появится запрос на ввод PIN-кода.

Если требуется присвоить пользователю еще один персональный идентификатор необходимо повторить те же действия. Пользователю, которому присвоено несколько персональных идентификаторов, вход в систему разрешен по любому из них.

При присвоении идентификатора пароль пользователя не записывается в идентификатор автоматически. Если необходимо, чтобы пароль пользователя хранился в персональном идентификаторе и автоматически считывался при предъявлении идентификатора в момент входа пользователя в систему необходимо выполнить процедуру записи пароля в идентификатор.

Для записи пароля в идентификатор необходимо:

1. В диалоге «Персональные идентификаторы» установить отметку в соответствующем идентификатору поле «Пароль в идентификаторе». Появится запрос на предъявление идентификатора, в котором указан его учетный номер.
2. Предъявить идентификатор. Если предъявлен нужный идентификатор, на экране появится запрос пароля пользователя.
3. Ввести пароль и нажать кнопку «OK».

Если пароль указан правильно, он записывается в идентификатор. При этом отметка в поле «Пароль в идентификаторе» сохраняется.

Для удаления пароля из идентификатора необходимо:

1. В диалоге «Персональные идентификаторы» удалить отметку из соответствующего идентификатору поля «Пароль в идентификаторе». Появится запрос на предъявление идентификатора, в котором указан его учетный номер.
2. Предъявить идентификатор.

Если предъявлен нужный идентификатор, пароль будет из него удален. При этом отметка из поля «Пароль в идентификаторе» удаляется.

Для удаления персонального идентификатора необходимо:

1. В диалоге «Персональные идентификаторы» установить курсор на номер идентификатора, подлежащего удалению, вызвать контекстное меню и выбрать команду «Удалить».
2. Подтвердить свое решение в появившемся на экране окне запроса.

Идентификатор будет удален из списка.

### 1.5 Управление персональными системными файлами пользователя

После установки системы защиты на компьютер, при входе пользователей в систему выполняются общие версии системных файлов CONFIG.SYS и AUTOEXEC.BAT. Средства системы Secret Net позволяют создавать для пользователей персональные версии этих файлов.

Для создания персональных версий системных файлов необходимо:

1. Вызвать на экран окно управления свойствами пользователя.
2. Активизировать диалог «Режимы»:

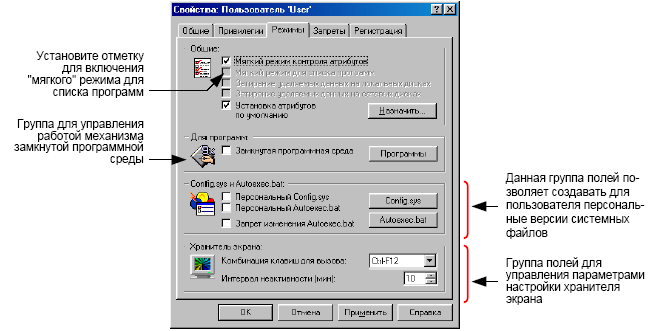


Рис. 19. Диалог «Режимы»

Выключатель «Персональный Config.sys» активен только тогда, когда компьютер оборудован устройством аппаратной поддержки системы защиты. Если данное устройство отсутствует – создать для пользователя персональный файл CONFIG.SYS нельзя.

1. Установить отметку в поле «Персональный Autoexec.bat» или «Персональный Config.sys», чтобы назначить пользователю персональные версии системных файлов.

На экране появится окно текстового редактора SnEdit, в котором будет отображаться содержание соответствующего файла. Если персональный системный файл пользователя еще не создан, в качестве его содержания будет предложено содержание общего системного файла.

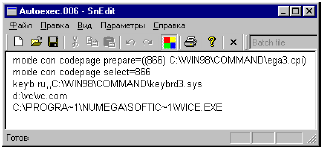


Рис. 20. Окно редактора SnEdit (редактирование файла autoexec.bat)

1. Отредактировать нужным образом системный файл. Завершив редактирование, сохранить внесенные изменения. Затем закрыть окно редактора SnEdit. Для редактирования персональных системных файлов используются кнопки «Config.sys» и «Autoexec.bat».

**Пояснение.** Персональные версии системных файлов хранятся на данном компьютере в каталоге C:\-SNET- под именами CONFIG.\*\*\* и AUTOEXEC.\*\*\* (где «\*\*\*» - регистрационный номер пользователя в системе Secret Net).

1. Установить отметку в поле «Запрет изменения Autoexec.bat», для запрета пользователю редактировать свой персональный командный файл. При этом попытка пользователя изменить содержание файла будет трактоваться как несанкционированное действие (НСД).
2. Нажать кнопку «ОК» в окне настройки свойств пользователя.

### 1.6 Запреты работы при изменении конфигурации компьютера

Средства системы Secret Net позволяют запретить работу пользователя в случае изменения аппаратной конфигурации компьютера, а также при изъятии из компьютера устройства аппаратной поддержки системы.

Вход пользователя, обладающего привилегией на работу с системой «Без ограничений по настройкам», не может быть заблокирован.

После того как соответствующие запреты введены в действие, при обнаружении факта изменения аппаратной конфигурации компьютера или изъятия устройства аппаратной поддержки доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран выводится предупреждающее сообщение, а загрузка компьютера прерывается. Системой Secret Net контролируется изменение следующих параметров:

тип процессора ( Pentium-II, Pentium-III и т.п.);

частота процессора в MHz;

версия операционной системы (DOS, Windows’9x);

размер оперативной памяти в Мб;

количество портов (LPT, COM, GAME);

количество устройств для чтения гибких дисков;

модель, версия и дата выпуска BIOS;

номер сетевой карты.

Для установки запретов необходимо:

* 1. Вызвать на экран окно управления свойствами пользователя.
  2. Активизировать диалог «Запреты».
  3. Установить отметку в поле:

«Запрет работы при изменении конфигурации».

«Запрет работы при изъятии аппаратной поддержки».

* 1. Нажать кнопку «OK».

**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.