УТВЕРЖДЕН

СЮИК.00042-02 34 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ЗАЩИТЫ ПЭВМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА "БАРЬЕР"

Руководство оператора

СЮИК.00042-02 34 01

Листов 45

2004

АННОТАЦИЯ

Настоящий программный документ содержит сведения, необходимые для работы с программно-аппаратным комплексом защиты информации от несанкционированного доступа "Барьер" (ПАК "Барьер"). В документе излагаются сведения о порядке и последовательности действий при установке программной части ПАК "Барьер"на ПЭВМ – программы паролирования, выполняющей функции управления ПАК "Барьер" до загрузки операционной системы (ОС), и входа в систему.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Программа паролирования используется в процессе работы ПАК "Барьер" и обеспечивает проверку состояния адаптера, идентификацию и аутентификацию пользователя, предоставление пользователю доступа к разрешенным для него ресурсам ПЭВМ, контроль целостности контролируемых ресурсов.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Программа паролирования выполняется до загрузки ОС путем загрузки ее в память программой расширения BIOS.

2.2. Для работы программы необходима автономная ПЭВМ, имеющая следующие эксплуатационные параметры:

- процессор, совместимый с Intel Pentium, с тактовой частотой – не менее 100 МГц;
- оперативное запоминающее устройство (ОЗУ) с объем памяти не менее 32 Мбайт;
- накопители на жестких магнитных дисках (НЖМД) IDE – не более 4 шт;
- количество логических дисков – не более 10;
- накопитель на гибких магнитных дисках (при необходимости).

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

Процесс инсталляции программы паролирования представляет собой последовательность действий, которую должен выполнить пользователь, имеющий права администратора, для установки программной части ПАК "Барьер" на ПЭВМ.

3.1. Подготовка к процессу инсталляции

Перед инсталляцией программы паролирования, необходимо тщательно ознакомиться с настоящим документом для получения полного представления о требованиях, предъявляемых к рабочему месту пользователя, и непосредственно к процессу инсталляции.

3.1.1. Удостовериться, что ПЭВМ удовлетворяет всем требованиям, указанным в документе руководство по эксплуатации СЮИК.305817.002 РЭ.

3.1.2. Проверить наличие в комплекте поставки платы адаптера имеющей номер СЮИК.020004.002 (либо СЮИК.020004.002 PCI).

3.1.3. Настроить BIOS SETUP ПЭВМ и сформировать логические разделы на НЖМД в соответствии с требованиями, приведенными в приложениях 1, 2.

3.1.4 Подготовить следующие данные для каждого пользователя:

- фамилия, имя, отчество пользователя;
- статус пользователя: Администратор безопасности, Администратор ключей, Пользователь;
- список логических дисков, подлежащие шифрованию;
- список доступных логических дисков;
- список контролируемых файлов;
- пароль доступа к ресурсам ПЭВМ в соответствии с требованиями приложения 3.

3.2. Процесс инсталляции

Приступать к инсталляции программы следует после проведения подготовки, описанной в п. 3.1.

3.2.1. Установить плату адаптера в разъем материнской платы ПЭВМ, в соответствии с документом руководство по эксплуатации СЮИК.305817.002 РЭ. Перед инсталляцией программы необходимо убедиться в том, что ПЭВМ готова к работе и включить питание. После завершения внутреннего теста ПЭВМ и отображения соответствующей служебной информации на экране монитора начнет выполняться встроенное программное обеспечение адаптера. На экране отобразится сообщение, представляющее собой начальное меню инсталляции (рис. 1).

Рис. 1

3.2.2. Выбрать пункт меню "Вход в систему". При этом управление передается загрузчику ОС и осуществляется загрузка.

3.2.3. После загрузки ОС обнаружит новое устройство – Барьер PCI. При этом необходимо установить в дисковод ГМД, содержащий драйвер устройства, из комплекта поставки.

3.2.4. Далее следовать указаниям мастера установки драйверов для новых устройств, который произведет копирование файлов драйверов в свои системные папки. После копирования на экране монитора отобразится сообщение, предлагающее произвести перезагрузку ПЭВМ.

3.2.5 Произвести перезагрузку ПЭВМ. Дождаться отображения на экране сообщения (рис. 1).

3.2.6 При помощи манипулятора типа "мышь" или клавиши "Tab" клавиатуры ПЭВМ выбирается пункт меню "**Инсталляция**". Выбор подтверждается нажатием клавиши "Enter" или левой клавиши манипулятора

типа "мышь". При этом на экране монитора отображается сообщение (рис. 2).

Рис. 2

В случае выбора пункта меню "**Вход в систему**" управление передается системному загрузчику ПЭВМ, который произведет загрузку операционной системы (ОС) ПЭВМ, при этом инсталляция будет отменена.

В течение времени отображения сообщения (см. рис. 2) происходит предварительная настройка платы адаптера. По завершении предварительной настройки на экране отобразится сообщение (рис. 3).

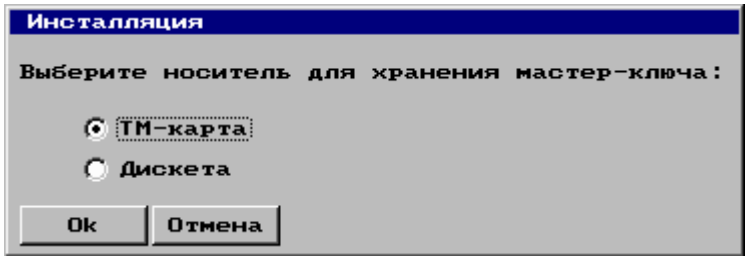

Рис. 3

3.2.7. Необходимо выбрать носитель, на который будет записан мастер-ключ для долговременного хранения, и нажать кнопку "Ок" для продолжения процесса инсталляции.

В случае нажатия кнопки "Отмена" инсталляция прерывается, и управление передается системному загрузчику ПЭВМ.

После нажатия кнопки "Ок" на экране монитора отобразится сообщение (рис. 4), предлагающее установить в считыватель ТМ-карту или дискету в зависимости от выбранного носителя. При выборе в качестве носителя дискеты следует использовать ГМД.

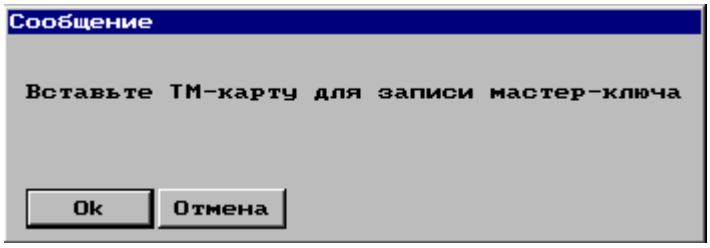

Рис. 4

3.2.8. Далее установить выбранный сменный носитель в считыватель (или дисковод) и нажать кнопку "Ок". При этом происходит запись мастер-ключа на выбранный носитель, в результате на экране монитора отобразится основное меню инсталляции (рис. 5).

В случае нажатия кнопки "Отмена" инсталляция прерывается, и управление передается системному загрузчику ПЭВМ.

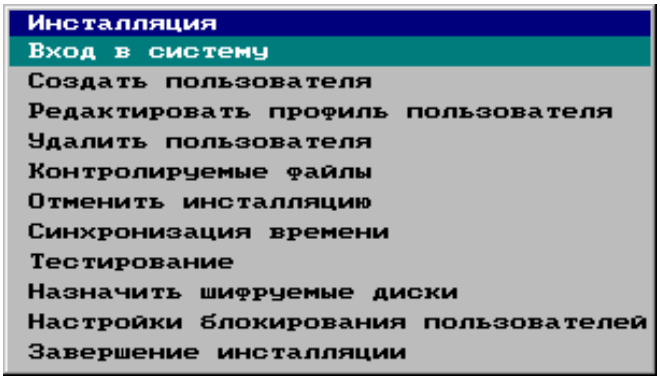

Рис. 5

3.2.9. В меню инсталляции (см. рис. 5) выбирается пункт "Создать пользователя", при этом на экране монитора ПЭВМ отобразится окно с формой "Формирование профиля пользователя" (рис. 6). Для эксплуатации ПАК "Барьер" с использованием шифрования дисков необходимо наличие не менее двух пользователей – Администратора безопасности и Администратора ключей.

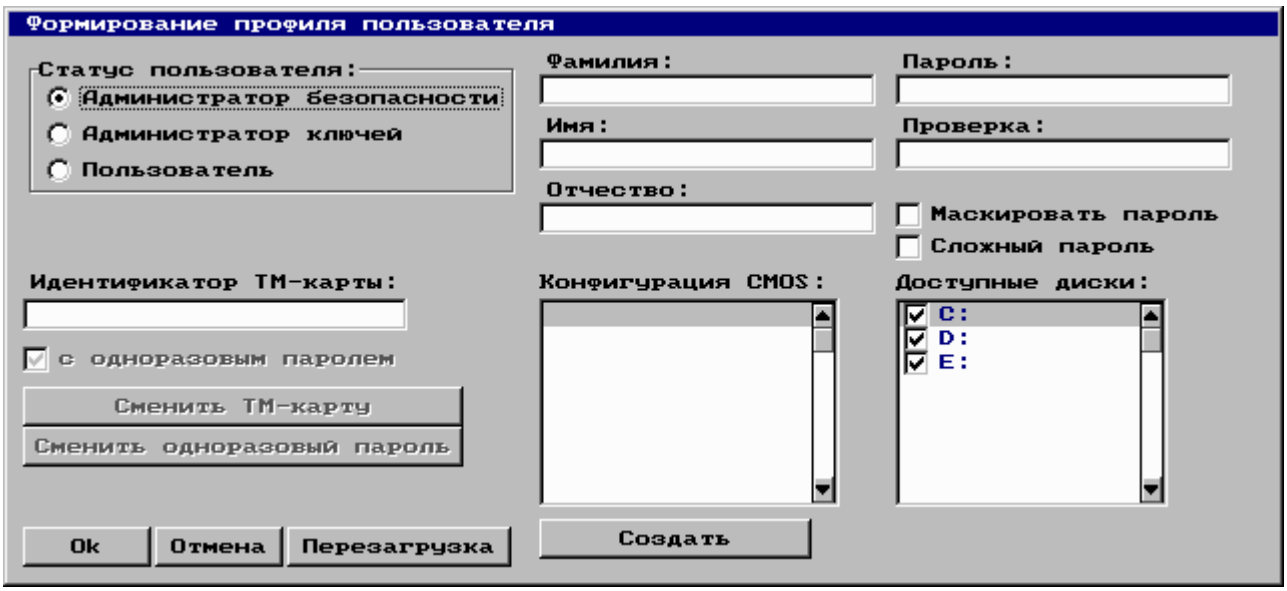

Рис. 6

3.2.10. В группе "Статус пользователя" следует выбрать тип пользователя

"Администратор безопасности".

3.2.11. В соответствующих полях ввести фамилию, имя и отчество пользователя, для которого создается профиль.

3.2.12. В поле "Пароль" ввести пароль, минимальная длина которого должна составлять 8 символов, для доступа данного пользователя к закрепленной за ним конфигурации ПЭВМ. Требования к системе ведения паролей, а также методика определения необходимой длины пароля представлены в приложении 3.

3.2.13. Для исключения возможности подсматривания посторонними лицами вводимого пароля устанавливается отметка в поле "Маскировать пароль" и вводимый пароль будет отображаться символами "*".

3.2.14. В поле "Проверка" повторно ввести пароль для исключения ошибки ввода пароля.

3.2.15. Отметка в поле "Сложный пароль" позволяет контролировать сложность устанавливаемого пароля.

3.2.16. В списке "Доступные диски" установить отметки напротив доступных для данного пользователя логических дисков. Не отмеченные логические диски регистрируемому пользователю не будут доступны

3.2.17. Для создания образа текущей аппаратной конфигурации ПЭВМ (конфигурации CMOS) и закрепления ее за регистрируемым пользователем необходимо нажать кнопку "Создать". На экране монитора отображается поле для ввода наименования конфигурации ПЭВМ, соответствующей регистрируемому пользователю. Ввести любое словесное обозначение и нажать ввод.

3.2.18. При необходимости изменения текущей конфигурации ПЭВМ следует нажать кнопку "Перезагрузка". При этом произойдет сохранение уже введенных параметров пользователя и перезагрузка ПЭВМ. Во время перезагрузки войти в системные настройки BIOS и установить требуемую для данного пользователя конфигурацию ПЭВМ и затем сохранить настройки. После повторной перезагрузки на экране монитора вновь отобразится окно "Формирование профиля пользователя" (см. рис. 6), с ранее введенными

параметрами пользователя.

3.2.19. Завершается формирование профиля для регистрируемого пользователя нажатием кнопки "Ок". При этом на экране монитора ПЭВМ отображается сообщение (рис. 7).

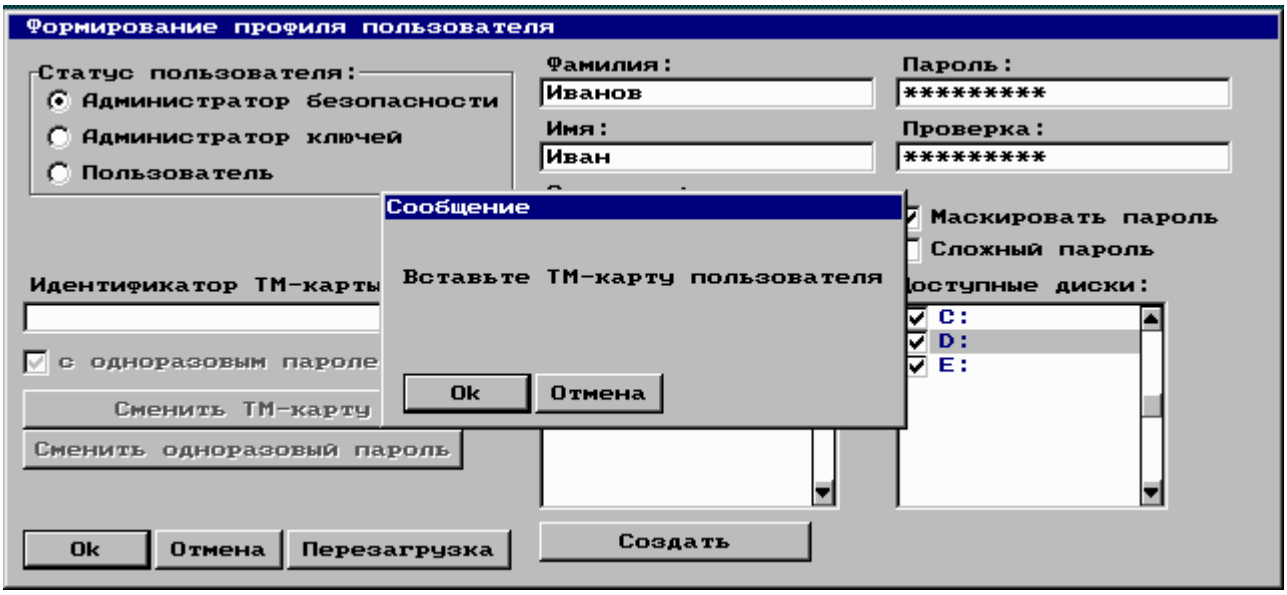

Рис. 7

3.2.20. Установить в считыватель личный идентификатор пользователя (ТМ-карту) для его регистрации и нажать кнопку "Ок". При этом произойдет сохранение профиля для пользователя. По завершении процесса записи профиля на экране монитора ПЭВМ отображается сообщение (рис. 8).

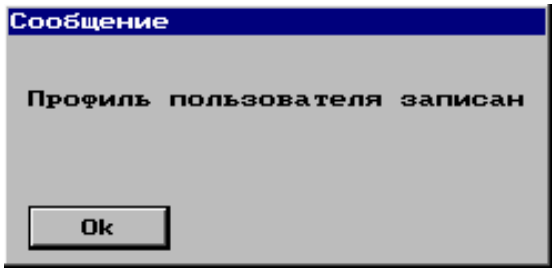

Рис. 8

3.2.21. Нажать кнопку "Ок". При этом произойдет выход в основное меню инсталляции (см. рис. 5).

3.2.22. При необходимости повторить пп.3.2.9 – 3.2.21 для пользователей со статусами: "Администратор ключей", "Пользователь".

3.2.23. Для использования контроля целостности файлов выбрать пункт

меню "Контролируемые файлы" и подтвердить выбор. В результате на экране монитора ПЭВМ отобразится окно редактирования списка контролируемых файлов (рис. 9), списки файлов могут отличаться от изображенных на рис. 9.

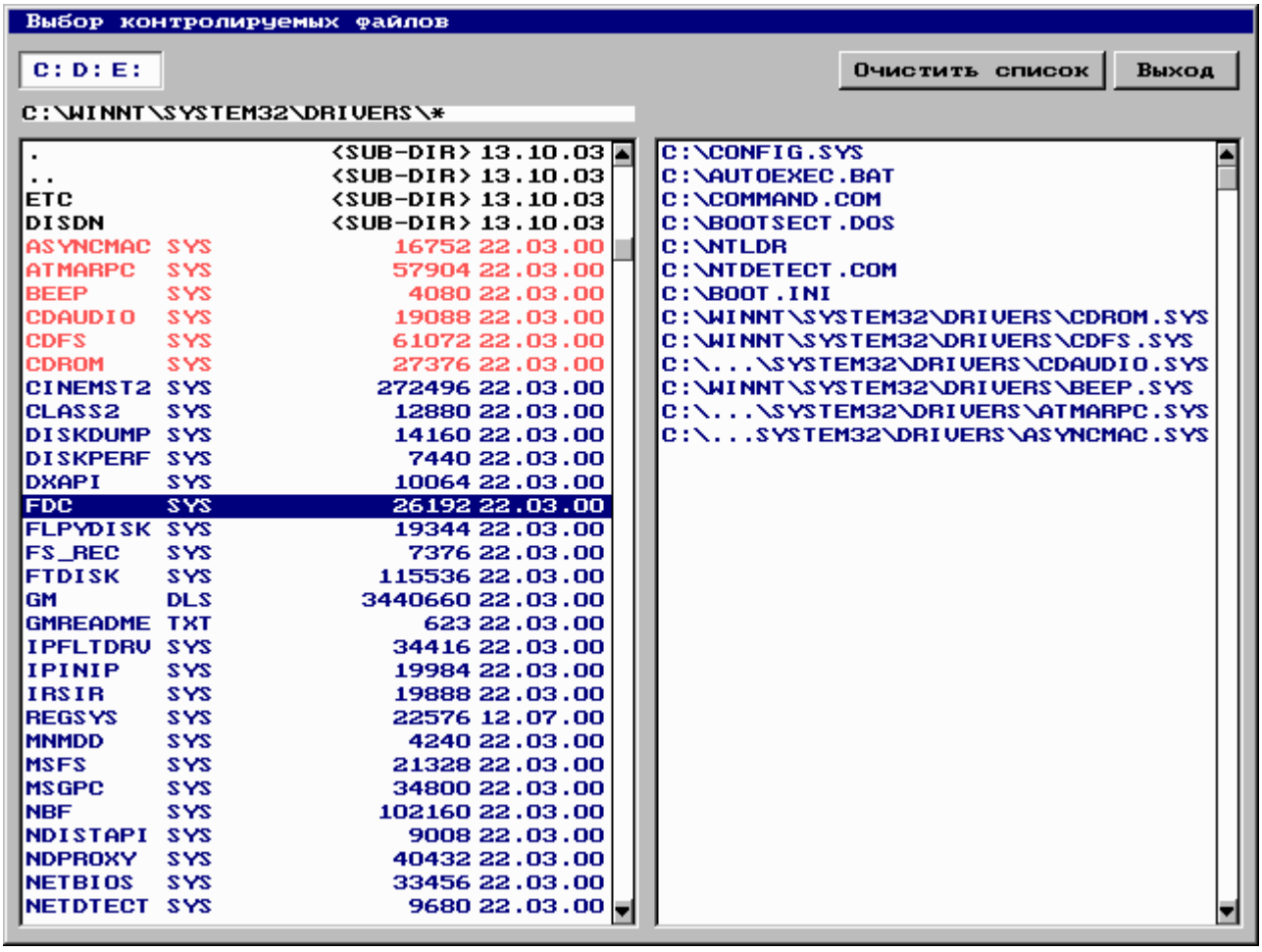

Рис. 9

3.2.24. В левой колонке отображается список файлов на текущем логическом диске. Выбор логического диска осуществляется в левом верхнем окошке окна редактирования списка. В правой колонке отображается список файлов, подлежащих контролю. Добавление файлов в список правой колонки осуществляется нажатием на выбранном файле в левой колонке клавиши "Enter" или двойным щелчком левой клавиши манипулятора типа "мышь". При этом цвет отображения имени файла изменяется на красный. Удаление файлов из списка контролируемых производится нажатием клавиши "DEL" на выбранном файле в правой колонке. Если необходимо очистить список контролируемых файлов, следует нажать кнопку "Очистить список".

3.2.25. Произвести выбор и добавление необходимых файлов в список контролируемых. При нажатии кнопки "Выход" на экране отобразится сообщение (рис. 10).

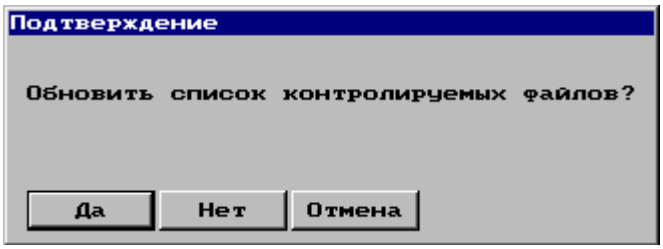

Рис. 10

3.2.26. При нажатии кнопки "Да" будут пересчитаны и сохранены значения функции хэширования для выбранных файлов. Затем произойдет выход в основное меню инсталляции (см. рис. 5).

3.2.27. Выбрать пункт меню "Синхронизация времени" в основном меню инсталляции (см. рис. 5) и подтвердить выбор. В результате на экране отобразится сообщение (рис. 11). Значения времени могут отличаться от изображенных на рис. 11.

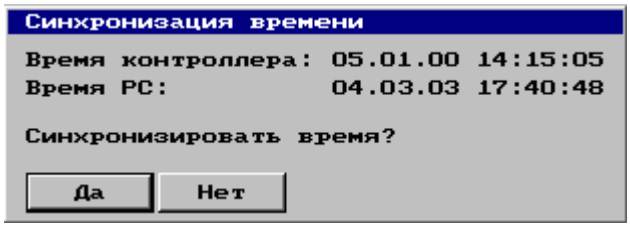

Рис. 11

3.2.28. При нажатии кнопки "Да" произойдет запись (синхронизация) системного времени ПЭВМ в адаптер и выход программы в основное меню инсталляции (см. рис. 5).

3.2.29.Для назначения возможности шифрования дисков выбрать пункт меню "Шифруемые диски" и подтвердить выбор. В результате на экране монитора ПЭВМ отобразится окно (рис. 12). Количество дисков в списке может отличаться от изображенного на рис. 12.

3.2.30. В списке "Шифруемые диски" установить отметки возле обозначений логических дисков, которые должны быть зашифрованы. Логические

диски, возле обозначений которых отметки будут сняты, шифроваться не будут. Логические диски остаются зашифрованными на протяжении всего срока службы ПЭВМ с установленным ПАК "Барьер". Расшифрование их производится при деинсталляции ПАК из состава ПЭВМ.

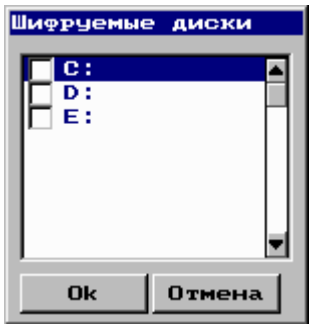

Рис. 12

3.2.31. При нажатии кнопки "Ок" произойдет сохранение информации о назначенных для шифрования логических дисках и выход в основное меню инсталляции (см. рис. 5). При необходимости отказа от изменения назначения шифруемых дисков используется кнопка "Отмена".

3.2.32. Выбрать пункт меню "Завершение инсталляции" в основном меню инсталляции (см. рис. 5) и подтвердить выбор. В результате на экране монитора ПЭВМ отобразится сообщение (рис. 13).

Рис. 13

3.2.33. Установить в считыватель ТМ-карту администратора безопасности и произвести перезагрузку ПЭВМ.

3.2.34. После перезагрузки, в случае, если были назначены шифруемые диски, на экран монитора выводится сообщение (рис. 14), отображающее процесс шифрования дисков .

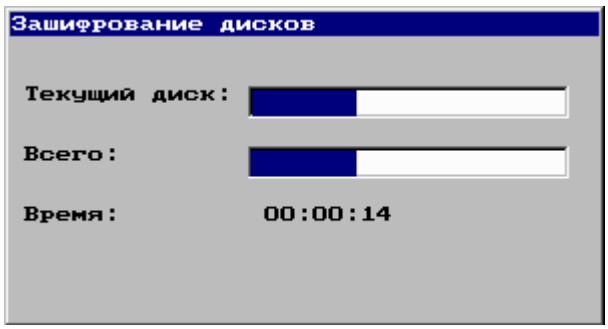

Рис. 14

3.2.35. По завершении процесса шифрования логических дисков на экране монитора отобразится сообщение (рис. 15).

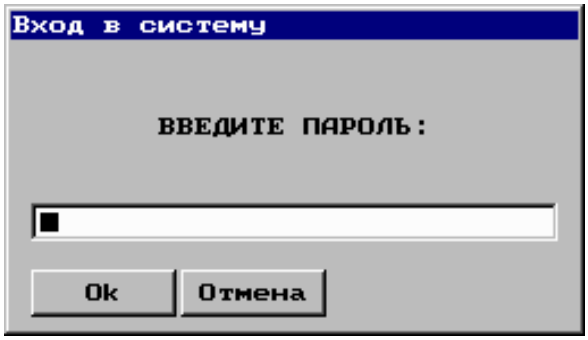

Рис. 15

3.2.36. На этом инсталляция считается завершенной.

4. ОРГАНИЗАЦИЯ РАБОЧЕГО ПРОЦЕССА НА ПЭВМ

Перед использованием ПЭВМ, с установленным ПАК "Барьер", пользователь обязан получить у администратора безопасности персональную карту-ключ пользователя и пароль доступа. При необходимости оговаривается график работы пользователя на ПЭВМ.

Процесс работы пользователя на ПЭВМ, защищенной ПАК "Барьер" разделяется на следующие этапы:

1) начало сеанса работы в системе;
2) работа пользователя в соответствии с функциональными обязанностями;
3) завершение сеанса работы.

В процессе работы для управления доступны следующие клавиши и сочетания клавиш клавиатуры ПЭВМ:

– "**Tab**", "**Shift**"+"**Tab**", манипулятор типа "**мышь**" – для выбора пунктов меню или установки курсора в поле ввода данных или поле выбора режима/действия;
– "**Enter**", левая клавиша манипулятора "**мышь**" – для подтверждения сделанного выбора или нажатия кнопки на отображаемых сообщениях-диалогах.

4.1. Начало сеанса работы в системе

4.1.1. Установить в считыватель карту-ключ со статусом "Пользователь" и включить питание ПЭВМ.

4.1.2. Далее, дождаться появления на экране сообщения (рис. 16).

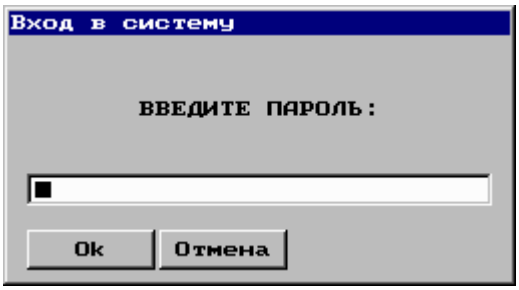

Рис. 16

4.1.3. Ввести пароль для доступа к конфигурации ПЭВМ, закрепленной за пользователем, чья карта-ключ установлена в считыватель. Нажать кнопку "Ок". При этом если пароль был введен с ошибкой, пользователю будет предоставлено еще две попытки ввода пароля. После истечения трех попыток, вход в систему блокируется, с выдачей соответствующего сообщения.

4.1.4. При успешном вводе пароля на экране отобразится сообщение **"Проверка целостности контролируемых файлов"**. Данное сообщение отображает процесс проверки целостности назначенных на контроль файлов.

4.1.5. При обнаружении файлов с нарушением целостности содержимого, на экране отображается сообщение **"Нарушена целостность файлов. Необходимо перезагрузить компьютер"**. При этом доступ к ПЭВМ запрещается.

4.1.6. По нормальному завершению процесса проверки целостности файлов, управление передается системному загрузчику BIOS ПЭВМ для загрузки ОС.

4.2. Работа пользователя в соответствии с функциональными обязанностями

4.2.1. После выполнения процедур начало сеанса работы выполняется загрузка ОС, и пользователь может приступить к работе, определяемой его функциональными обязанностями.

4.2.2. При инсталляции ПАК "Барьер" создается функционально замкнутая программная среда, которая позволяет контролировать права доступа пользователя к объектам доступа.

4.3. Завершение сеанса работы

4.3.1. Завершение сеанса работы в ОС осуществляется стандартными средствами ОС.

5. РАБОТА В РЕЖИМЕ АДМИНИСТРИРОВАНИЯ

Режим администрирования доступен пользователю, имеющему статус "Администратор" – как администратору безопасности, так и администратору ключей. Пользователю, имеющему статус "Пользователь" этот режим недоступен.

Вход в систему Администратора осуществляется согласно п. 4.1 при установленной в считыватель ТМ-карты Администратора. При входе в систему Администратора на экране монитора ПЭВМ отображается меню администрирования (см. рис. 17).

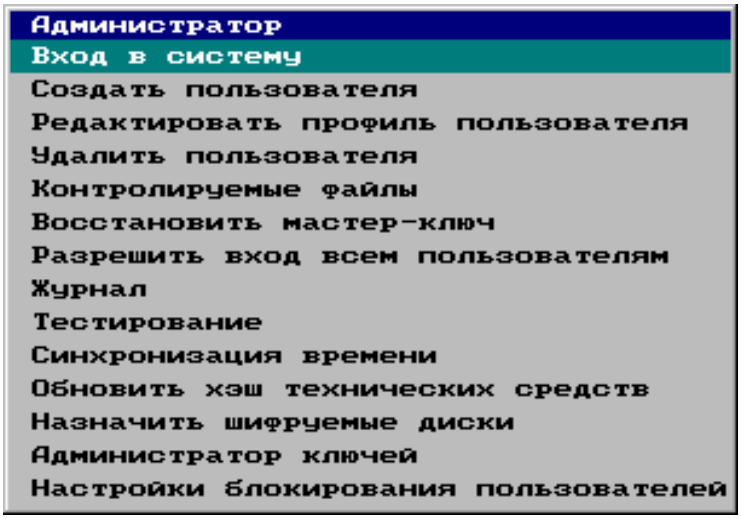

Рис. 17

5.1. Назначение пунктов меню администратора

5.1.1. Пункт меню "Вход в систему"

Пункт меню "Вход в систему" предназначен для передачи управления загрузчику ОС для ее загрузки.

5.1.1.1. Выбрать пункт меню "Вход в систему". После подтверждения выбора на экране монитора отобразится сообщение, отражающее процесс проверки целостности контролируемых файлов (рис. 18). Имена файлов могут отличаться от изображенных на рисунке.

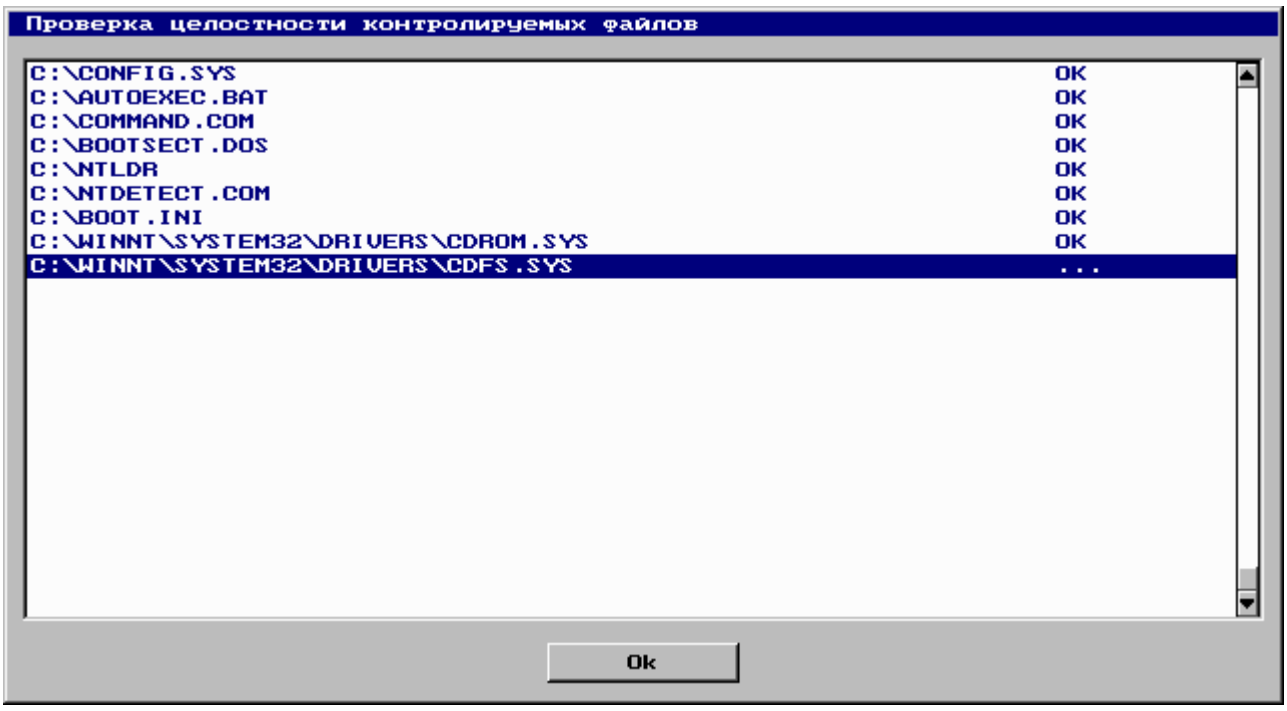

Рис. 18

5.1.1.2. По успешном завершении процесса проверки целостности файлов, управление передается системному загрузчику для загрузки ОС.

5.1.1.3. При обнаружении файлов с нарушением целостности содержимого, на экране отображается сообщение (рис. 19). Имена файлов могут отличаться от изображенных на рис. 23. При этом нажатие кнопки "Ок" приведет к загрузке ОС.

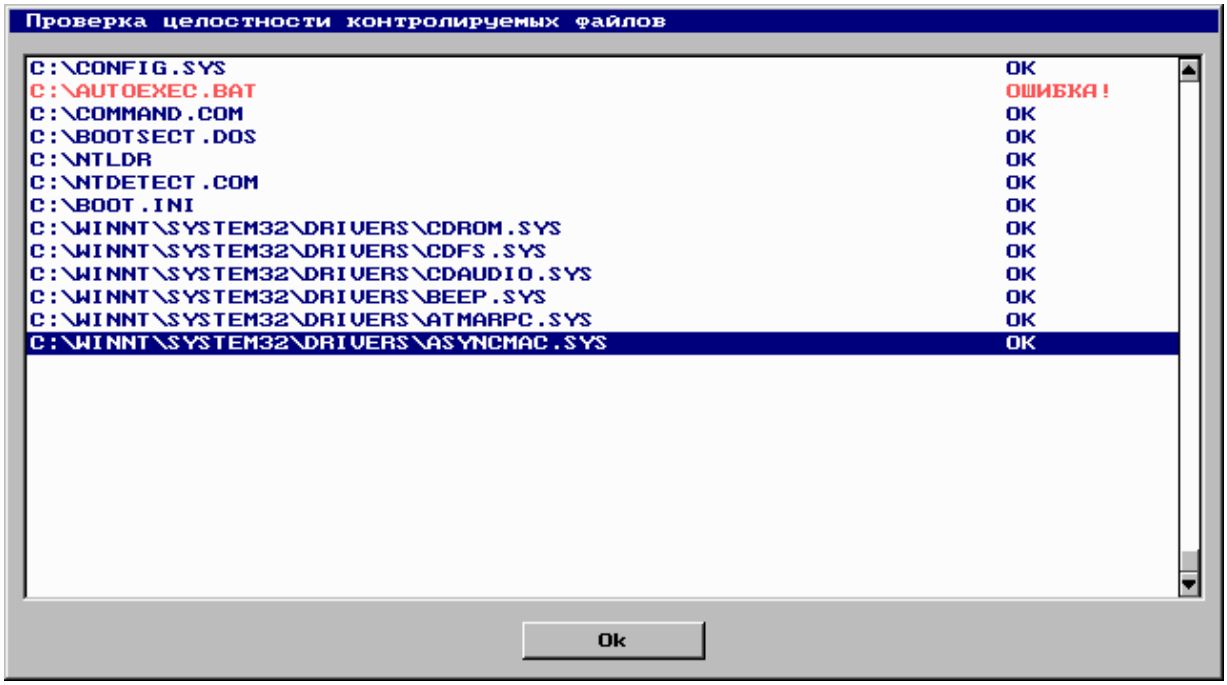

Рис. 19

5.1.2. Пункт меню "Создать пользователя"

Пункт меню "Создать пользователя" позволяет создать профиль нового пользователя и добавить его в систему. Работа с этим пунктом описана в пп. 3.2.9 – 3.2.20.

5.1.3. Пункт меню "Редактировать профиль пользователя"

Позволяет отредактировать профиль уже существующего в системе пользователя.

5.1.3.1. При выборе пункта меню "Редактировать профиль пользователя" и подтверждении выбора, на экране монитора отобразится окно (рис. 20). Количество и имена пользователей могут отличаться от изображенных на рис. 20.

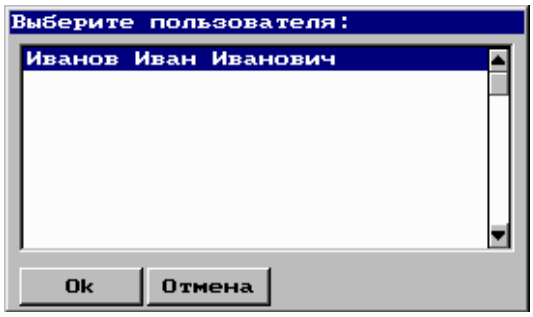

Рис. 20

5.1.3.2. В отображенном окне (см. рис. 20) необходимо выбрать имя пользователя, профиль которого требуется изменить и нажать кнопку "Ок". На экране монитора отобразится окно "Формирование профиля пользователя" (см. рис. 6). Поля данной формы будут заполнены параметрами профиля выбранного пользователя и становятся доступными кнопки "Сменить ТМ-карту" и "Сменить одноразовый пароль".

5.1.3.3. Далее необходимо внести требуемые изменения в соответствующие поля формы. Для изменения пароля доступа пользователя необходимо ввести пароль и проверку в соответствующие поля. Если поля ввода пароля и проверки остаются пустыми, то текущее значение пароля для редактируемого пользователя не изменяется.

5.1.3.4. Для замены ТМ-карты пользователя необходимо нажать кнопку

"Сменить ТМ-карту" и на экране отобразится сообщение (рис. 21).

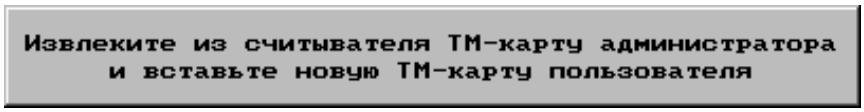

Рис. 21

5.1.3.5. Далее необходимо извлечь из считывателя ТМ-карту Администратора, а затем установить новую ТМ-карту, которая будет закреплена за выбранным Пользователем. При этом на экране отобразится сообщение (рис. 22).

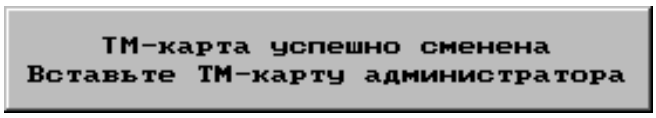

Рис. 22

5.1.3.6. Затем необходимо извлечь карту Пользователя и установить в считыватель извлеченную ранее ТМ-карту Администратора. На экране монитора отобразится окно "Формирование профиля пользователя" (см. рис. 6), и в поле "Идентификатор ТМ-карты" отобразится значение идентификатора новой ТМ-карты, закрепленной за редактируемым Пользователем.

5.1.3.7. Для замены одноразового пароля на ТМ-карте Пользователя следует нажать кнопку "Сменить одноразовый пароль" и на экране отобразится сообщение (рис. 23).

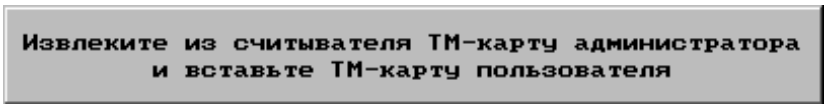

Рис. 23

5.1.3.8. Затем необходимо извлечь из считывателя ТМ-карту Администратора и установить ТМ-карту Пользователя. При этом на экране отобразится сообщение (рис. 24).

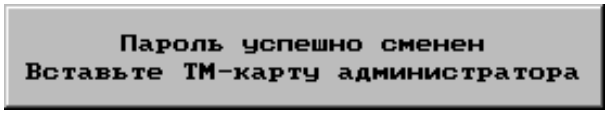

Рис. 24

5.1.3.9. Далее необходимо извлечь карту Пользователя и установить в

считыватель извлеченную ранее ТМ-карту Администратора. При этом на экране монитора отобразится окно "Формирование профиля пользователя" (см. рис. 6).

5.1.3.10. При смене ТМ-карты пользователя возможно отображение на экране монитора следующих сообщений:

- "**ТМ-карта уже используется**" – в считыватель установлена ТМ-карта, которая уже используется в данной системе;
- "**ТМ-карта мастер-ключа**" – в считыватель установлена ТМ-карта, на которой сохранен мастер-ключ данной системы;
- "**ТМ-карта не вставлена**" – из считывателя была изъята ТМ-карта Администратора, но не была установлена новая ТМ-карта Пользователя;
- "**Невозможно записать одноразовый пароль в ТМ-карту**" – в считыватель установлена ТМ-карта, которая была использована более чем на 8-ми системах;
- "**Ошибка обмена с контроллером**" – внутренняя ошибка адаптера.

5.1.3.11. При смене одноразового пароля на ТМ-карте возможно отображение на экране монитора следующих сообщений:

"**Неверная ТМ-карта**" – в считыватель установлена ТМ-карта, не соответствующая пользователю, для которого меняется одноразовый пароль;

"**ТМ-карта не вставлена**" – из считывателя была изъята ТМ-карта Администратора, но не была установлена новая ТМ-карта Пользователя.

При отображении на экране любого из вышеуказанных сообщений необходимо выполнить действия описанные в разделе 6.

5.1.3.12. По завершении процесса редактирования профиля пользователя нажать кнопку "Ок" и на экране отобразится сообщение (см. рис. 8).

5.1.3.13. Нажать кнопку "Ок". На экране отобразится меню администрирования (см. рис. 17).

5.1.4. Пункт меню "Удалить пользователя"

Пункт меню "Удалить пользователя" предназначен для удаления из системы

уже существующих пользователей.

5.1.4.1. При выборе пункта меню "Удалить пользователя"и подтверждении выбора, на экране отобразится окно (см. рис. 20).

5.1.4.2. В изображенном окне выбирается имя пользователя, которого необходимо удалить из системы, и нажимается кнопка "Ок". На экране монитора отобразится запрос на подтверждение удаления пользователя.

5.1.4.3. При подтверждении удаления, пользователь будет удален из системы и на экране отобразится меню администрирования (см. рис. 17).

5.1.4.4. В случае отмены подтверждения удаления, пользователь не будет удален из системы и на экране отобразится меню администрирования (см. рис. 17).

5.1.5. Пункт меню "Контролируемые файлы"

5.1.5.1. Пункт меню "Контролируемые файлы" предназначен для редактирования списка файлов, подлежащих контролю на целостность до загрузки ОС. При выборе пункта и подтверждении выбора, на экране монитора отобразится окно редактирования списка контролируемых файлов (см. рис. 9).

5.1.5.2. Работа с пунктом меню "Контролируемые файлы" описана в пп. 3.2.24-3.2.25.

5.1.5.3. По завершении процесса редактирования списка контролируемых файлов, нажимается кнопка "Выход" и на экране отображается сообщение (см. рис. 10).

5.1.5.4. Для выхода из пункта меню "Контролируемые файлы" с сохранением всех сделанных изменений в списке контролируемых файлов следует нажать кнопку "Да". Если содержимое некоторых файлов было изменено с разрешения Администратора и необходимо обновить результат функции хэширования для этих файлов, то также следует нажать кнопку "Да".

5.1.5.5. Для выхода из пункта меню "Контролируемые файлы" без сохранения изменений в списке, сделанных Администратором, нажимается

кнопка "Нет".

5.1.5.6. Для отмены выхода и возврата в режим редактирования списка контролируемых файлов, следует нажать кнопку "Отмена".

5.1.5.7. При выходе из пункта меню "Контролируемые файлы" на экране монитора отобразится меню администрирования (см. рис. 17).

5.1.6. Пункт меню "Восстановить мастер-ключ"

Для восстановления мастер-ключа после его уничтожения при вскрытии корпуса необходимо установить в устройство считывания носитель, на который был записан ключ во время инсталляции ПАК "Барьер".

5.1.6.1. При выборе пункта меню "Восстановить мастер-ключ" и подтверждении выбора, на экране монитора отобразится сообщение (рис. 25).

В зависимости от типа носителя, который использовался для сохранения мастер-ключа, на экране может отобразиться предложение установить дискету.

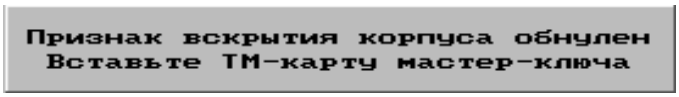

Рис. 25

5.1.6.2. Далее необходимо установить требуемый носитель с мастер-ключом (для ТМ-карты предварительно необходимо извлечь из считывателя ТМ-карту Администратора).

5.1.6.3. В случае успешного восстановления мастер-ключа с внешнего носителя на экране монитора отобразится соответствующее сообщение.

5.1.6.4. Для продолжения следует нажать кнопку "Ок" в появившемся окне сообщения. При этом на экране отобразится меню администрирования (см. рис. 17).

Если во время выполнения действий по восстановлению мастер-ключа корпус ПЭВМ вскрыт, то будет выдано соответствующее предупреждение (рис. 26). Необходимо закрыть корпус ПЭВМ и нажать кнопку "Ок". Для отмены процесса восстановления мастер-ключа нажать кнопку "Отмена".

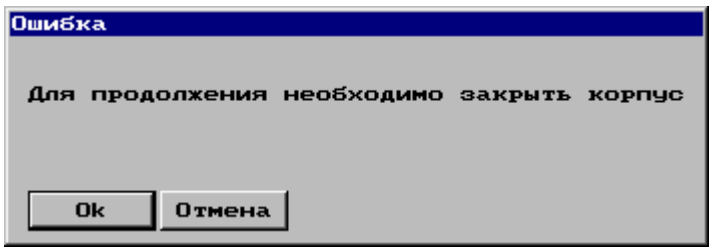

Рис. 26

5.1.6.5. При восстановлении мастер-ключа возможно отображение на экране следующего сообщения:

"**Неверный носитель**" – установленный носитель, не содержит мастер-ключ или мастер-ключ соответствует другому комплексу. В этом случае необходимо установить требуемый носитель.

5.1.7. Пункт меню "Разрешить вход всем пользователям"

Пункт меню "Разрешить вход всем пользователям" предназначен для отмены запрета входа в систему для пользователей, не имеющих статуса "Администратора". Запрет входа в систему для обычных пользователей возникает в следующих ситуациях, которые являются критическими с точки зрения безопасности системы:

- было произведено вскрытие корпуса;
- была нарушена целостность одного или нескольких контролируемых файлов;
- была нарушена целостность технических средств ПЭВМ;
- для входа в систему была использована ТМ-карта, не зарегистрированная в данной системе.

5.1.7.1. При выборе пункта меню "Разрешить вход всем пользователям" и подтверждении выбора, на экране отобразится сообщение (рис. 27).

5.1.7.2. Для продолжения нажать кнопку "Ок" на экране отобразится меню администрирования (см. рис. 17).

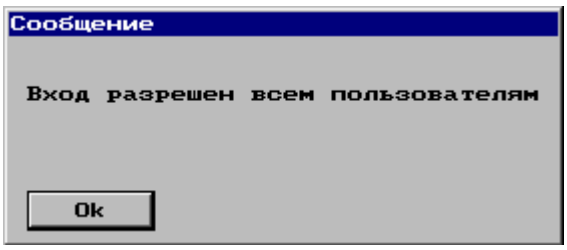

Рис. 27

5.1.8. Пункт меню "Журнал"

Пункт меню "Журнал" предназначен для просмотра журнала аудита событий, происходящих в ПЭВМ, защищенной ПАК "Барьер".

5.1.8.1. При выборе пункта меню "Журнал" и подтверждении выбора, на экране монитора отобразится окно журнала (рис. 28).

5.1.8.2. Для отображения всех записей журнала из выбранного источника (по умолчанию – "ППЗУ адаптера") нажать кнопку "Ок". В результате на экране монитора отобразится окно (рис. 29).

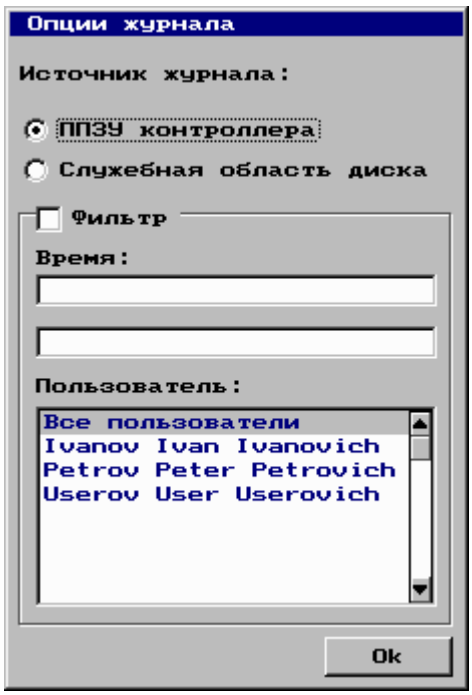

Рис. 28

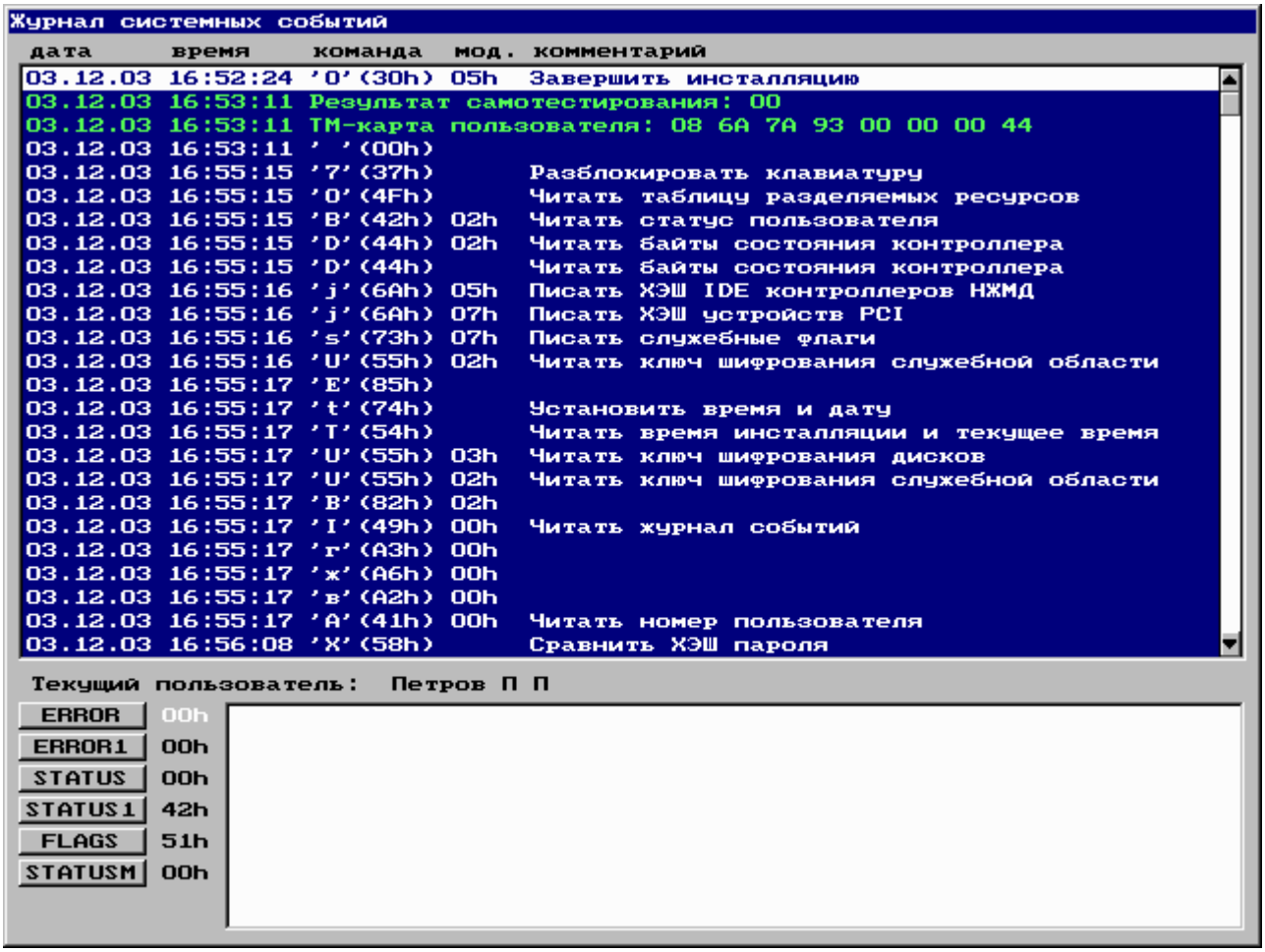

Рис. 29

5.1.8.3. Для отображения сообщений журнала аудита соответствующих некоторому критерию необходимо установить отметку в поле "Фильтр" и выбрать признак, по которому будет осуществляться выборка и отображение записей.

5.1.8.4. Существуют следующие признаки выборки записей журнала:

– "**Время**": производится выборка записей, удовлетворяющих условию временного диапазона, задаваемого в полях "Время". При заполнении обеих строк временного диапазона, производится выборка записей, начиная со времени, указанного в первой строке и до времени, указанного во второй строке. Если задается первая строка, а вторая остается пустой, то просматривается диапазон, начиная с указанного значения и до конца журнала. Если задается вторая строка, то просматривается диапазон с начала журнала и до указанного значения. Время задается в следующем формате:

"ДД.ММ.ГГГГ чч:мм:сс",

где **ДД** – число месяца, **ММ** – месяц, **ГГГГ** – год;

чч – часы, **мм** – минуты, **сс** – секунды.

– "**Пользователь**": производится выборка записей, совершенных во время нахождения в системе определенного пользователя. Выборка осуществляется по всем пользователям, либо по выбранному из списка пользователю.

5.1.8.5. Пример результата выборки записей (см рис. 29). Основную часть окна занимает список событий (на синем фоне). Зеленым цветом отображены успешные события входа в систему и внутреннего тестирования ПАК "Барьер". Красным цветом отображаются события с нарушениями: использование незарегистрированной в системе ТМ-карты, подбор пароля пользователя, ошибки внутреннего тестирования. Белым цветом отображаются команды, которыми обменивается система с платой ПАК "Барьер".

5.1.8.6. Под списком событий отображается имя пользователя, который находился в системе в момент данного (выделенного курсором) события.

5.1.8.7. Слева внизу расположен набор кнопок, отвечающих за расшифровку содержимого внутренних регистров ПАК "Барьер". При нажатии на любую кнопку, содержимое системных флагов адаптера с подробными комментариями отображается справа от кнопок (на белом фоне).

5.1.8.8. Кнопка "Экспорт" предназначена для записи журнала системных событий на дискету. При нажатии этой кнопки на экране отобразится сообщение, предлагающее установить дискету для сохранения журнала аудита: **"Вставьте диск для записи журнала"**. Следует установить в дисковод чистую дискету и нажать кнопку "Ок". Отобразится одно из следующих сообщений:

– **"Журнал сохранен"** – в случае успешной записи на дискету;

– **"Ошибка диска"** – в случае невозможности сохранить журнал на дискету.

5.1.8.9. Выход из просмотра журнала аудита событий в меню администрирования осуществляется нажатием клавиши "Esc" на клавиатуре ПЭВМ или кнопки "Выход".

5.1.9. Пункт меню "Тестирование"

Пункт меню "Тестирование" предназначен для запуска процедуры тестирования адаптера и отображения его результатов.

5.1.9.1. При выборе пункта меню "Тестирование" и подтверждении выбора, адаптеру подается команда на запуск внутреннего тестирования. По истечении некоторого времени, необходимого для завершения процесса тестирования, на экране отобразится сообщение (рис. 30).

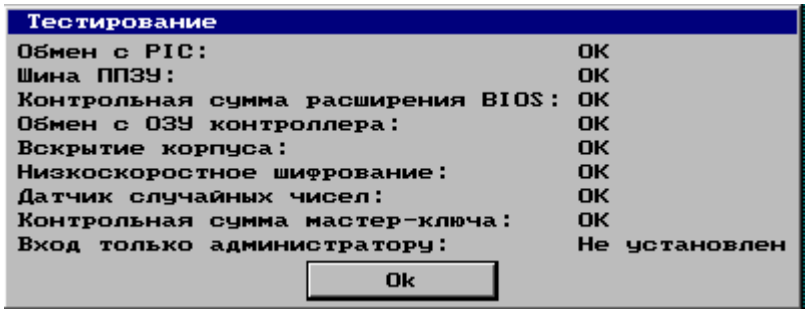

Рис. 30

5.1.9.2. После анализа результатов внутреннего тестирования, для выхода в меню администрирования (см. рис. 17), следует нажать кнопку "Ок".

5.1.10. Пункт меню "Синхронизация времени"

Пункт меню "Синхронизация времени" предназначен для проведения синхронизации времени между системными часами ПЭВМ и внутренними часами адаптера. Работа с пунктом меню "Синхронизация времени" аналогична работе с соответствующим пунктом в меню инсталляции, описанной в пп. 3.2.27-3.2.28.

5.1.11. Пункт меню "Обновить хэш технических средств"

Пункт меню "Обновить хэш технических средств" предназначен для контроля состава технических средств путем перерасчета значений функций хеширования идентифицирующей информации технических средств из состава ПЭВМ при изменении аппаратной конфигурации ПЭВМ.

При этом на экране отобразится сообщение об успешном завершении обновления значений функций хэширования.

5.1.12. Пункт меню "Назначить шифруемые диски"

Пункт меню "Назначить шифруемые диски" предназначен для назначения признаков шифрования логическим дискам (разделам) на НЖМД, установленным в данной ПЭВМ. Работа с данным пунктом аналогична работе с соответствующим пунктом в меню инсталляции, описанной в пп. 3.2.29–3.2.31.

5.1.13. Пункт меню "Администратор ключей"

Пункт меню "Администратор ключей" предназначен для доступа к меню администратора ключей, позволяющий в частности, осуществить деинсталляцию ПАК "Барьер". Для доступа к данному меню следует в начале получить доступ к ПЭВМ пользователем, имеющим статус "Администратор безопасности". Затем действовать в соответствии с пп. 5.1.13.1–5.1.13.4.

5.1.13.1. Выбрать и подтвердить выбор пункта меню "Администратор ключей". На экране отобразится сообщение (рис. 31).

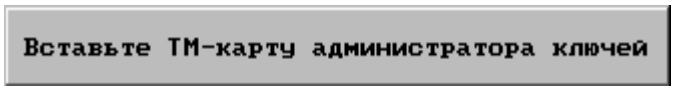

Рис. 31

5.1.13.2. Извлечь из считывателя ТМ-карту администратора безопасности. Затем, установить в считыватель ТМ-карту администратора ключей. На экране монитора отобразится меню администратора ключей (рис. 32).

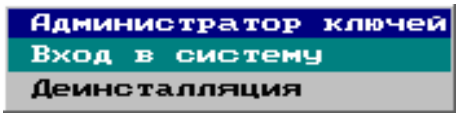

Рис. 32

5.1.13.3. Пункт "Вход в систему" данного меню полностью соответствует аналогичному пункту в меню администрирования (см. рис. 17).

5.1.13.4. При выборе пункта "Деинсталляция" меню администратора ключей (рис. 32) и подтверждении выбора, на экране монитора отобразится сообщение, запрашивающее подтверждение на проведение деинсталляции. При подтверждении запроса процесс деинсталляции будет продолжен. В случае

отрицательного ответа произойдет выход в меню администратора ключей (см. рис. 32).

При продолжении процесса деинсталляции будут уничтожены служебные области, которые необходимы для функционирования ПАК "Барьер" на данной ПЭВМ и восстановление первоначальной (с учетом текущих изменений) конфигурации ПЭВМ. Далее произойдет передача управления системному загрузчику ОС и будет осуществлена ее загрузка.

На этом процесс деинсталляции считается завершенным.

5.1.14. Пункт меню "Настройки блокировки пользователей"

Пункт меню "Настройки блокировки пользователей" предназначен для выбора условий блокирования входа в систему пользователей со статусом "Пользователь" (установка признака "Вход только администратору") при выполнении критических событий.

5.1.14.1. При выборе пункта меню "Настройки блокировки пользователей" и подтверждении выбора, на экране отобразится сообщение (рис. 33).

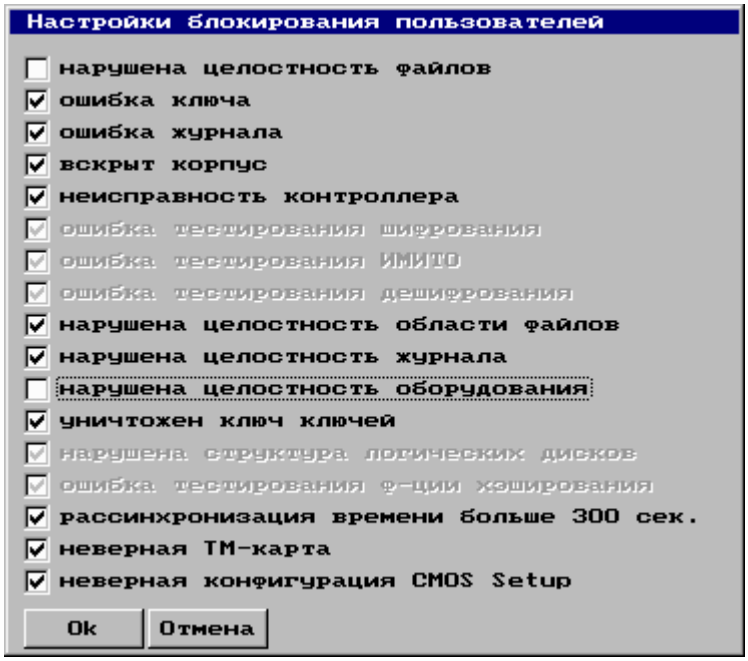

Рис. 33

5.1.14.2. Установка отметки напротив строки, описывающей критическое событие, приведет при его возникновении, к установке признака "Вход только

администратору" и блокировке входа в систему для пользователей со статусом "Пользователь".

5.1.14.3. Снятие отметки напротив строки с описанием события приведет только к регистрации критического события в журнале аудита, и блокирование входа в систему для пользователей со статусом "Пользователь" производится не будет.

6. СООБЩЕНИЯ ОПЕРАТОРУ

6.1. При эксплуатации ПАК "Барьер" возможна выдача соответствующих сообщений приведенных в таблице 1.

Таблица 1 – Перечень сообщений при работе ПАК "Барьер"

Текст сообщения	Описание события	Порядок действия
1 ТМ-карта уже используется	В считыватель установлена ТМ-карта, которая уже используется в данной системе ПЭВМ	Установить необходимую ТМ-карту
2 ТМ-карта мастер-ключа	В считыватель установлена ТМ-карта, на которой сохранен мастер-ключ данной системы ПЭВМ	Установить свободную ТМ-карту
3 Ошибка записи	Произошла ошибка при записи мастер-ключа в ТМ-карту.	Установить другую необходимую ТМ-карту и возобновить запись
4 ТМ-карта не вставлена	Из считывателя была изъята ТМ-карта администратора, но не была установлена новая ТМ-карта пользователя	Установить необходимую ТМ-карту
5 Невозможно записать одноразовый пароль в ТМ-карту	В считыватель установлена ТМ-карта, которая была использована более чем на восьми системах	Установить необходимую ТМ-карту
6 Неверная ТМ-карта	В считыватель установлена ТМ-карта, не соответствующая пользователю, для которого меняется одноразовый пароль	Установить необходимую ТМ-карту
7 Ошибка обмена с адаптером	Внутренняя ошибка адаптера	Сообщить администратору
8 Пароль должен быть не меньше 8 символов	Введен пароль меньше 8 символов	Ввести пароль, длиной больше или равной 8 символов
9 Неверный пароль	Попытка входа в систему с неверным паролем	Ввести правильный пароль

Продолжение таблицы 1

Текст сообщения	Описание события	Порядок действия
10 Такой пароль уже существует	Введен пароль установленный для другого пользователя	Ввести новый пароль
11 Доступ в систему запрещен	Три раза введен неверный пароль. Система блокирована, вход разрешен только администратору	Перегрузить ПЭВМ и повторить ввод соответствующего пароля
12 Неверный IDE диск 0	Инсталляция начата на машине с другим диском	Провести инсталляцию заново
13 Нарушена структура логических дисков	Была изменена структура дисков после начала инсталляции	Провести инсталляцию заново
14 Проверка не совпадает с паролем	При создании или редактировании пользователя в форме "Формирование профиля пользователя" пароль в поле "проверка" не совпадает с ранее введенным	Ввести правильный пароль
15 Не все поля заполнены	При создании пользователя в форме "Формирование профиля пользователя" не все поля заполнены	Необходимо заполнить все поля в форме
16 Необходимо наличие АБ и АК	Завершение инсталляции без создания двух администраторов: администратора безопасности и администратора ключей	Создать администратора безопасности (АБ) и администратора ключей (АК)
17 Ошибка диска	При записи мастер-ключа на дискету или чтении с дискеты	Повторить запись или чтение
18 Был вскрыт корпус	Произведено вскрытие корпуса ПЭВМ	Закрыть корпус, восстановить мастер-ключ
19 Уничтожен мастер-ключ	При уничтожении мастер-ключа в случае вскрытия корпуса или при неисправности контроллера	Закрыть корпус, восстановить мастер-ключ

Продолжение таблицы 1

Текст сообщения	Описание события	Порядок действия
20 Для продолжения необходимо закрыть корпус	Открыт корпус ПЭВМ	Закрыть корпус и повторить инсталляцию
21 Ошибка записи ключа	Возможно неисправность контроллера	Повторить инсталляцию
22 Ошибка: последний диск должен быть не меньше 2 цилиндров	Не выполнены требования приложения 2 по формированию логических разделов НЖМД	Выполнить формирование логических разделов НЖМД в соответствии с требованиями приложения 2
23 Мастер-ключ не восстановлен	При восстановлении мастер-ключа не удалось восстановить мастер-ключ, неверный носитель	Повторить восстановление мастер-ключа используя правильный носитель
24 Ошибка ключа шифрования служебной области	Уничтожен мастер-ключ	Восстановить мастер-ключ, разрешить вход всем пользователям
25 Ошибка ключа шифрования дисков	Уничтожен мастер-ключ	Восстановить мастер-ключ, разрешить вход всем пользователям
26 Нарушена целостность технических средств	Изменены PCI или IDE устройства	Обновить хэш оборудования, разрешить вход всем пользователям
27 Работа с журналом событий невозможна. Необходима деинсталляция	Нарушена структура системного журнала на диске	Деинсталлировать систему защиты
28 Нарушена целостность области журнала	Нарушена структура системного журнала на диске	Деинсталлировать систему защиты

Продолжение таблицы 1

Текст сообщения	Описание события	Порядок действия
29 Не могу расшифровать диски. Продолжить деинсталляцию?	При деинсталляции из-за уничтоженного мастер-ключа невозможно расшифровать зашифрованные диски	Продолжить деинсталляцию, но при этом содержание дисков будет потеряно, либо вернуться и попытаться восстановить мастер-ключ
30 Неверный носитель	ТМ-карта или дискета, установленная для считывания мастер-ключа, не содержит нужный для данной системы мастер-ключ	Установить необходимую ТМ-карту или дискету
31 Рассинхронизация времени адаптера и ПЭВМ больше допустимой	Разница во времени контроллера и ПЭВМ больше допустимой	Выполнить синхронизацию времени, разрешить вход всем пользователям
32 Нарушена целостность файлов. Необходимо перезагрузить компьютер	Нарушена целостность файлов	Перезагрузить компьютер
33 Контроллер неисправен	Внутренняя ошибка контроллера	Перезагрузить ПЭВМ, заново провести инсталляцию. Если произведенные действия не привели к положительному результату – обратиться к разработчику ПАК "Барьер"
34 Ошибка тестирования функции шифрования	Выводится при невыполнении функции самотестировании шифрования	
35 Ошибка тестирования функции ИМИТО	Выводится при невыполнении функции самотестировании ИМИТО	
36 Ошибка тестирования функции дешифрования	Выводится при невыполнении функции самотестировании шифрования	
37 Ошибка тестирования функции хэша	Выводится при невыполнении функции самотестировании хэша	

ПРИЛОЖЕНИЕ 1

ТРЕБОВАНИЯ К НАСТРОЙКАМ BIOS SETUP

В приложении приводятся требования и рекомендации по настройке конфигурации ПЭВМ (BIOS SETUP) для начального запуска по включению питания.

В таблице 2 приведены опции, значение которых обязательно должно быть установлено в конфигурации ПЭВМ.

Таблица 2

Наименование опции настройки	Состояние
Boot Sector Virus Protection (Anti-Virus Protection, Virus Warning)	Disabled
Halt On	All Errors
Quick Boot (Quick Power On Self Test)	Enabled

Для ограничения доступа к настройкам BIOS пользователя со статусом "Пользователь" рекомендуется, при конфигурировании профиля пользователя, установить пароль на доступ к настройкам BIOS. Данный пароль не будет использоваться для доступа к настройкам, поэтому его можно нигде не хранить и, соответственно, не производить смену пароля. Для пользователей со статусом "Администратор" данная настройка не требуется.

Остальные опции в настройке конфигурации ПЭВМ устанавливаются по умолчанию, либо по усмотрению администратора.

ПРИЛОЖЕНИЕ 2

ТРЕБОВАНИЯ К ЛОГИЧЕСКИМ РАЗДЕЛАМ НЖМД

Логические разделы на НЖМД, установленном в ПЭВМ, защищаемой ПАК "Барьер" рекомендуется создавать утилитами fdisk или Partition Magic.

Требования к логическим разделам, предназначенным для шифрования средствами ПАК "Барьер":

– тип файловой системы – любой;

– размер раздела – не более 2 Гбайт.

Требования к логическим разделам, предназначенным для хранения файлов с данными и контроля их целостности средствами ПАК "Барьер":

– тип файловой системы – FAT16, FAT32, NTFS;

– размер раздела – любой.

Требования к логическим разделам, предназначенным для хранения файлов с контролем их целостности и шифрования средствами ПАК "Барьер":

– тип файловой системы – FAT16, FAT32, NTFS:

– размер раздела – не более 2 Гбайт.

Размер последнего раздела не может быть меньше 14 Мбайт.

Общее количество логических дисков на всех НЖМД, установленных в ПЭВМ не должно превышать 10.

Минимальный размер последнего логического раздела на НЖМД – не менее двух цилиндров (14 Мбайт).

Для правильного функционирования ПАК "Барьер" ОБЯЗАТЕЛЬНО выполнения приведенных выше требований.

ПРИЛОЖЕНИЕ 3

ТРЕБОВАНИЯ К ПАРОЛЯМ

Порядок ведения (ввода, изменения, удаления/блокирования) паролей должен быть изложен в соответствующих инструкциях по формированию и ведению паролей.

Общие требования к паролям пользователей

Общие требования к паролям пользователей следующие:

- идентификатор (имя) и пароль должны выдаваться каждому пользователю администратором безопасности под роспись в «карточке учета паролей»;
- полномочия каждого пользователя, дающие ему право доступа к информации, должны быть подтверждены администратором безопасности;
- при входе в систему идентификатор и пароль вводятся самим пользователем; при троекратной подряд ошибке ввода пароля осуществляется автоматическое блокирование системы с регистрацией факта ошибки в журнале аудита;
- пароли пользователей должны периодически меняться администратором безопасности в сроки, предусмотренные регламентом;
- пароль должен иметь длину не менее восьми символов, в состав которых должны входить буквы латинского алфавита, цифры и специальные знаки (подчеркивание, тильда и др.); ввод паролей, не отвечающих этим требованиям, блокируется системой;
- пароли должны отличаться друг от друга не менее чем тремя символами и не должны иметь более двух повторяющихся символов;
- пользователям запрещается передавать свои индивидуальные пароли

друг другу и записывать пароль на чём-либо;

– пользователь должен помнить свой пароль; если после длительного перерыва в работе (например, после отпуска, болезни) пользователь забыл свой пароль, он может получить его у администратора безопасности.

Требования к системе ведения паролей

Процедура системы ведения паролей должна быть тщательно отработана администратором безопасности и пользователями:

– пароль должен вводиться администратором безопасности согласно требованиям инструкций по формированию и ведению паролей;
– запрещается осуществлять ввод пароля в присутствии посторонних лиц;
– должна быть предусмотрена процедура смены паролей в случае несанкционированного доступа к информации и в других нештатных ситуациях;
– при компрометации пароля необходимо срочно принять меры по смене пароля;
– периодичность смены пароля должна быть ежемесячная (в первый рабочий понедельник каждого месяца смена паролей производится для всех пользователей);
– смену паролей пользователей осуществляет администратор безопасности.

Требования к пользователю при работе с паролем

Пользователь обязан:

– выполнять требования эксплуатационной документации на встроенные средства защиты информации при работе со своим паролем;
– сохранять пароль в тайне и следить за конфиденциальностью ввода пароля с клавиатуры;
– в неясных или нештатных случаях обращаться за помощью к администратору безопасности,

Требования к администратору безопасности при работе с паролями

Администратор безопасности обязан:

- своевременно формировать и выдавать пароли пользователям и обеспечивать установку паролей в систему;
- обеспечивать разработку необходимых инструкций по формированию и ведению паролей, определяющих процедуры ввода, изменения, удаления, и блокирования паролей пользователей, а также порядок контроля над действиями пользователей при работе в сети;
- в совершенстве знать используемую систему защиты информации, механизмы аутентификации, владеть процедурами установки и смены паролей, знать политику безопасности организации по учетным записям пользователей (паролям);
- следить, чтобы каждый пользователь знал свои права и обязанности при работе в сети, владел навыками работы с паролем;
- вести систему учета паролей каждого пользователя в его именной «карточке учета паролей» (производить смену паролей всех пользователей не реже одного раза в месяц);
- применять необходимые меры защиты в нештатных ситуациях, докладывать своему руководству при нарушении работы сети или ее сбоях.

Прочие требования по организации ведения паролей

- пользователь должен быть ознакомлен с перечисленными выше требованиями и предупрежден об ответственности за невыполнение своих обязанностей, а также за разглашение паролей;
- ответственность за своевременное формирование и распределение (выдачу) паролей пользователям возлагается на администратора безопасности;

- конверты с паролями должны быть опечатаны, при необходимости может быть заведена резервная копия «карточки учета паролей» каждого пользователей (на случай утраты основной);
- внеплановая смена (блокирование) личного пароля любого пользователя в случае прекращения его полномочии (увольнение, переход на другую работу и т.п.), либо компрометирующих действий должна производиться немедленно после окончания последнего санкционированного сеанса работы данного пользователя. Необходимо производить внеплановую смену паролей всех пользователей при фактах возникновения несанкционированного доступа;
- в случае компрометации личного пароля хотя бы одного пользователя должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля (вплоть до смены паролей всех пользователей);
- в случае компрометации (разглашения) пароля пользователя должно проводиться служебное расследование.

Методика определения необходимой длины пароля

Оценка необходимой длины пароля требуется для того, чтобы правильно выбрать период действия (смены) паролей. Данный период действия паролей определяется вероятностью подбора пароля, при этом предполагается, что подбор пароля осуществляется непрерывным тестированием ПЭВМ в течение определенного периода времени.

Взаимосвязь между длиной пароля и периодом времени для его подбора в результате непрерывного тестирования ПЭВМ определяется формулой Андерсона:

$$4{,}32 \times 10^4 \times \mathrm{K} \times \left(\frac{\mathrm{M}}{\mathrm{P}} \right) \le \mathrm{A}^{\mathrm{Z}} \qquad (1),$$

где К – количество попыток подбора пароля в минуту $\left(\frac{1}{мин}\right)$;

М – период времени непрерывного тестирования ПЭВМ для подбора пароля в месяцах (*месяц*);

Р – заданная вероятность подбора пароля;

А – количество символов, из которых составляется пароль (базовая длина алфавита);

z – длина пароля.

Формула (1) позволяет определить необходимую длину пароля, если задана вероятность подбора пароля при непрерывном тестировании ПЭВМ в течение какого-либо определенного промежутка времени.

Данная задача решается следующим образом.

Пусть заданная вероятность подбора пароля в результате месячного непрерывного тестирования ПЭВМ не должна превышать 0,0001 ($P \le 0{,}0001$).

Для составления пароля используется английский алфавит ($A = 26$).

Длина пароля ($z = 8$).

Выясним соответствие длины пароля и заданных условий по его подбору, при этом будем полагать, что время на одну попытку подбора пароля составляет 5 секунд (то есть, что $K = 60/5 = 12$).

Имеем:

$$4{,}32 \times 10^4 \times 12 \times \left(\frac{1}{0{,}0001}\right) \le 26^8$$

или

$$5{,}2 \times 10^9 \le 208{,}8 \times 10^9$$

То есть, длина пароля с 8 символов достаточна для выполнения заданных условий, а именно – если будет выбран пароль длиной в 8 символов, то в течение месяца при осуществлении непрерывных попыток его подбора вероятность подбора будет не выше 0,0001.

Задача может быть сформулирована по-другому, а именно пусть требуется вычислить вероятность подбора пароля при осуществлении непрерывных попыток его подбора в течение месяца при следующих условиях:

$K = 12 \left(\frac{1}{мин} \right)$;

M = 1 (*мес.*);

A = 26 (символов);

z =8 (символов).

Подставив данные значения в формулу (1), получим:

$$4,\ 10^4 \times 12 \times \left(\frac{1}{P} \right) \le 208,8 \times 10^9$$

или

$$0,00052 \times 10^9 \times \left(\frac{1}{P} \right) \le 208,8 \times 10^9$$

то есть, вероятность подбора пароля не превысит $2,5 \times 10^{-6}$.

Если при составлении пароля использовать буквы русского алфавита (прописные и строчные), буквы латинского алфавита (прописные и строчные), цифры и спецсимволы, то базовая длина алфавита составит A = 161 символ.

Пароль, в котором используется хотя бы одна цифра, спецсимвол, а также буквы различных алфавитов или регистров, называется сложным.

В этом случае вероятность подбора пароля при осуществлении непрерывных попыток его подбора в течение месяца не превысит $2,5 \times 10^{-14}$.

Таким образом, при использовании сложного пароля вероятность его подбора крайне низка и, кроме того, исключается возможность его подбора методом "словаря".

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

№ изм.	*Подп.*	*Дата*