Утвержден
СЮИК.467458.001 РЭ-ЛУ

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

Руководство по эксплуатации

СЮИК.467458.001 РЭ

Содержание

Настоящее руководство по эксплуатации (РЭ) распространяется на комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа "Барьер" (ПАК "Барьер") – устройство, выполняющее функции защиты информационных ресурсов ПЭВМ от несанкционированного доступа (НСД).

Данный документ является объединенным эксплуатационным документом, удостоверяющим гарантированные изготовителем основные параметры и технические характеристики ПАК "Барьер" и содержащим сведения по эксплуатации и ремонту.

Руководство по эксплуатации содержит руководство пользователя (раздел 3) и руководство администратора (раздел 4).

Руководство по эксплуатации адресовано специалистам, которые занимаются организацией защиты информации на предприятии и имеют знания в области защиты информации программными методами.

Руководство по эксплуатации описывает следующее:

- принцип работы ПАК "Барьер";
- порядок хранения и транспортирования ПАК "Барьер";
- порядок монтажа и ввода в эксплуатацию ПАК "Барьер";
- описание аварийных ситуаций.

При записи в документе не допускаются записи карандашом, смывающимися чернилами и подчистки.

Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет лицо, ответственное за эксплуатацию ПЭВМ. После подписи проставляют фамилию и инициалы ответственного лица (вместо подписи допускается проставлять его личный штамп).

1 Описание и работа комплекса программно-аппаратного защиты ПЭВМ от несанкционированного доступа "Барьер"

1.1 Назначение

1.1.1 ПАК "Барьер" предназначен для защиты информации ограниченного распространения при ее обработке на автономной ПЭВМ, работающей с ОС семейства MS Windows 98/NT/2000/XP/2003.

1.1.2 Разделение полномочий (распределение ролей) субъектов, зарегистрированных в ПАК "Барьер", осуществляется согласно их статусам следующим образом:

– "администратор безопасности" – субъект доступа (пользователь), имеющий широкие полномочия при работе в системе;

– "администратор ключей" – субъект доступа (пользователь), имеющий ограниченные полномочия при работе в системе (имеет право только на вход в систему совместно с администратором безопасности для осуществления процедур смены ключей или деинсталляции ПАК "Барьер");

– "пользователь" – субъект доступа, имеющий право работать только с определенными для него при инсталляции ПАК "Барьер" доступными ресурсами.

Разделение полномочий субъектов, зарегистрированных в ПАК "Барьер", осуществляется администратором безопасности.

1.1.3 ПАК "Барьер" обеспечивает выполнение следующих функций:

а) идентификацию и аутентификацию субъектов, зарегистрированных в ПАК "Барьер", по карте-ключу (ТМ-карте), содержащей персональный идентификатор пользователя, и паролю соответственно. При этом осуществляется блокирование несанкционированного доступа к настройкам BIOS ПЭВМ, защита ресурсов ПЭВМ от подбора идентификаторов карт-ключей, блокирование доступа к ресурсам ПЭВМ при извлечении карты-ключа из считывателя во время начальной загрузки ОС и в процессе работы ПЭВМ;

б) смену ключевой информации в случае дискредитации ключей. Процедура смены ключей реализуется после совместного входа в систему администратора безопасности и администратора ключей;

в) контроль целостности состава PCI- и IDE-устройств ПЭВМ, контроль настроек BIOS ПЭВМ;

г) контроль целостности логических дисков и файлов на накопителе на жестком магнитном диске (НЖМД). Защиту содержимого логических дисков и файлов от несанкционированного изменения. При этом для защиты данных на НЖМД используется режим гаммирования согласно ГОСТ 28147-89 и функция хеширования согласно СТБ 1176.1-99;

д) контроль времени и блокирование работы ПЭВМ во время начальной загрузки при расхождении времени более чем на пять минут между значениями системных часов ПЭВМ и внутренних часов реального времени адаптера ПАК "Барьер";

е) разделение полномочий субъектов, зарегистрированных в ПАК "Барьер", на основе аутентификационных данных, выполнение установки настроек BIOS ПЭВМ и подключение доступных логических дисков в соответствии с данными, сохраненными в учетной записи пользователя при регистрации. Разделение полномочий осуществляется администратором безопасности на уровне доступа к средствам администрирования;

ж) хранение загрузчика ОС и таблицы логических дисков в защищенном виде, восстановление их на НЖМД после успешной идентификации и аутентификации любого из пользователей и уничтожение сразу после загрузки ОС (после прохождения успешной идентификации и аутентификации администратора ключей восстановление загрузчика ОС и таблицы логических дисков на НЖМД не происходит);

з) хранение ключевой информации в зашифрованном виде в области памяти ПАК "Барьер",

недоступной системным и специальным программным средствам ОС. Шифрование ключевой информации выполняется в соответствии с ГОСТ 28147-89 в режиме простой замены;

и) защиту данных на НЖМД путем их хранения в зашифрованном виде в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью. Доступ к данным на НЖМД осуществляется расшифрованием их в оперативном запоминающем устройстве (ОЗУ) ПЭВМ в процессе работы ОС;

к) автоматическое выполнение самодиагностики адаптера ПАК "Барьер";

л) контроль вскрытия корпуса и уничтожение критически важной информации (ключей шифрования) в случае обнаружения факта вскрытия корпуса;

м) аудит и протоколирование событий безопасности в защищенном журнале. Каждая запись журнала должна иметь следующий формат: время записи, тип записи, имя субъекта, зарегистрированного в ПАК "Барьер", текст записи;

н) просмотр записей журнала аудита администратором безопасности с использованием встроенных средств, включая организацию поиска и фильтрацию отображаемых данных;

о) блокирование работы ПЭВМ в случае выхода из строя аппаратных узлов ПАК "Барьер";

п) соответствие ПАК "Барьер" требованиям по электромагнитной совместимости и электромагнитному воздействию на конструктивные элементы ПЭВМ согласно СТБ ГОСТ Р 51317.4.3-2001, СТБ ГОСТ Р 51317.4.5-2001 и СТБ ГОСТ Р 51318.22-2001 (класс Б).

1.2 Основные сведения об изделии и технические данные

1.2.1 Основные сведения

Наименование изделия: Комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа "Барьер"

Обозначение изделия **СЮИК.467458.001**

Дата изготовления _____

Изготовитель _Республика Беларусь ЗАО "НТЦ КОНТАКТ"

220034 г. Минск, ул. Первомайская, 17, ком. 1к_____

наименование и почтовый адрес предприятия-изготовителя

Заводской номер _____

1.2.2 Технические характеристики

1.2.2.1 ПАК "Барьер" имеет следующие технические характеристики:

- габаритные размеры – не более 135×125×20 мм;
- габаритные размеры печатной платы ПАК "Барьер" – не более 120×100×20 мм;
- масса – не более 0,5 кг;
- напряжения питания – плюс 3,5 В, плюс 5 В, плюс 12 В, минус 12 В;
- постоянное запоминающее устройство (ПЗУ) ПАК "Барьер" имеет объем памяти не менее 96 Кбайт;
- ОЗУ ПАК "Барьер" имеет объем памяти не менее 2 Кбайта;
- тип используемой шины ПЭВМ – PCI;
- количество хранимых профилей пользователей – 8;
- средняя наработка на отказ – не менее 10000 ч;
- среднее время восстановления работоспособности – не более 30 мин без учета времени доставки заменяемого элемента потребителю и времени доставки ПАК "Барьер" от потребителя на территорию предприятия-изготовителя и обратно;
- срок службы – не менее 10 лет.

1.2.3 Сведения о содержании драгоценных материалов и цветных металлов

1.2.3.1 Сведения о содержании драгоценных металлов в ПАК "Барьер" приведены в таблице 1.

Таблица 1

Наименование изделия	Золото	Серебро	Платина	Палладий
Комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа "Барьер"	0,17 мг	–	–	–
Примечание – Сведения являются справочными. Фактическое содержание драгоценных материалов определяется после их списания на основе сведений предприятий по переработке вторичных, драгоценных материалов.				

1.3 Комплектность

1.3.1 Состав ПАК "Барьер" приведен в таблице 2.

Таблица 2

Обозначение изделия	Наименование изделия	Коли-чество (шт.)	Заводской номер	Приме-чание
СЮИК.467458.001	Адаптер ПАК "Барьер"	1		
DS1402D-DR8	Считыватель карты-ключа	1		
DS1992L	Карта-ключ	4		
ИО102-14	Датчик вскрытия корпуса	1		
	Драйвер устройства для ОС Windows 98/NT/2000/XP/2003	1		ГМД или компакт-диск
СЮИК.467458.001 ВЭ	Комплект эксплуатационной документации согласно ведомости	1		
СЮИК.320305.001	Упаковка	1		
Примечание – Количество поставляемых карт-ключей и датчиков вскрытия корпуса может быть увеличено по требованию заказчика.				

1.4 Устройство и работа

1.4.1 Устройство

1.4.1.1 ПАК "Барьер" состоит из следующих элементов:

а) адаптера, представляющего собой плату, которая содержит всю аппаратную часть ПАК "Барьер" за исключением считывателя карт-ключей;

б) считывателя карт-ключей, представляющего собой аппаратное устройство, которое подключается к портам адаптера и предназначено для организации операций обменов с картой-ключом. В качестве данного устройства применяется устройство типа DS1402D-DR8;

в) карт-ключей, используемых для хранения в защищенном виде идентификационной информации субъектов, зарегистрированных в ПАК "Барьер";

г) датчика вскрытия корпуса;

д) специального программного обеспечения (ПО), состоящего из:

1) программного обеспечения микроконтроллеров, обеспечивающего выполнение команд, поступающих от ПЭВМ, внутреннее тестирование и управление элементами, входящими в состав ПАК "Барьер";

2) программного обеспечения, выполняемого на ПЭВМ до загрузки ОС, работающего как расширитель базовой системы ввода-вывода (BIOS) и обеспечивающего выполнение следующих функций:

– конфигурирование системы защиты ПЭВМ;

– проверку целостности аппаратных и программных средств ПЭВМ;

– проверку вводимого пароля и сопоставление его с соответствующей идентификационной информацией субъекта, зарегистрированного в ПАК "Барьер";

– возможность создания защищенных разделов на жестких магнитных дисках ПЭВМ для шифрования информации пользователей;

– удаление загрузочных секторов и таблицы распределения логических дисков;

3) драйверов ПАК "Барьер" для ОС семейства MS Windows 98/NT/2000/XP/2003, представляющих собой программы, обеспечивающие взаимодействие ПАК "Барьер" с ОС.

1.4.1.2 В состав платы адаптера ПАК "Барьер" входят следующие элементы:

- центральный процессор;
- PIC-микроконтроллер;
- последовательная память;
- параллельная память;
- PCI-контроллер;
- программируемая логическая интегральная схема (ПЛИС);
- датчик случайной числовой последовательности (ДСЧП);
- блок часов реального времени.

1.4.1.3 Центральный процессор состоит из арифметико-логического устройства, блока регистров, встроенной памяти данных, логики прерываний, таймеров и портов ввода-вывода. Он предназначен для управления работой узлов адаптера и вычисления криптографических преобразований, приема и выполнения команд управления с ПЭВМ. Центральный процессор также выполняет операции обмена информацией с картой-ключом: проверку наличия карты-ключа в считывателе, чтение и запись информации на карту-ключ.

1.4.1.4 PIC-микроконтроллер предназначен для хранения критически важной информации, которая уничтожается при попытке несанкционированного вскрытия корпуса ПЭВМ. К такой информации относятся ключи шифрования и загружаемая информация о функционировании адаптера. PIC-микроконтроллер имеет автономное электропитание и способен функционировать при выключенном питании ПЭВМ.

PIC-микроконтроллер соединен с датчиком вскрытия корпуса и часами реального времени ПАК "Барьер" и обеспечивает регистрацию сигналов датчиков вскрытия корпуса ПЭВМ и запись даты и времени регистрации в журнал аудита.

1.4.1.5 Последовательная память представляет собой перепрограммируемое постоянное запоминающее устройство (ППЗУ), обеспечивающее энергонезависимое хранение части информации, требующей изменения в процессе эксплуатации адаптера. Последовательная память используется также для хранения оперативной части журнала аудита.

1.4.1.6 Параллельная память представляет собой ОЗУ объемом 8 Кбайт, предназначена для загрузки в нее программы расширения BIOS и используется для хранения результатов выполнения некоторых команд ПЭВМ.

1.4.1.7 PCI-контроллер обеспечивает взаимодействие ПАК "Барьер" с ПЭВМ посредством операций обмена информацией между шиной PCI ПЭВМ и адаптером.

1.4.1.8 ПЛИС предназначена для согласования сигналов между отдельными элементами платы адаптера по временам и уровню.

1.4.1.9 ДСЧП предназначен для формирования случайных числовых последовательностей, используемых в работе ПЭВМ, и включает в себя генератор шума, компаратор напряжения и схемы сопряжения с центральным процессором.

1.4.1.10 Датчик вскрытия корпуса ПЭВМ предназначен для фиксирования момента вскрытия корпуса ПЭВМ и выдачи сигналов на PIC-микроконтроллер для уничтожения критически важной информации.

1.4.1.11 Блок часов реального времени предназначен для контроля отсчета времени и выдачи его значения элементам адаптера по их запросу. Данный блок обеспечивает формирование меток времени в протоколах работы адаптера и синхронизацию часов ПЭВМ.

1.4.2 Принцип работы

1.4.2.1 При включении питания системного блока ПЭВМ на адаптер подается напряжение питания и происходит его самотестирование, после чего ожидается установка карты-ключа в считыватель. После установки карты-ключа считывается ее идентификатор и сравнивается с перечнем допустимых идентификаторов из таблицы, хранящейся в ППЗУ адаптера. Если идентификатор не зарегистрирован, то его значение заносится в журнал аудита. При совпадении считанного идентификатора с любым из перечня допустимых определяется номер субъекта, зарегистрированного в ПАК "Барьер", и разрешается включение питания системного блока ПЭВМ. Также при включении питания ПЭВМ запускается на выполнение программа POST (BIOS). Данная программа передает управление программе-расширению BIOS для обеспечения загрузки в ОЗУ ПЭВМ из ППЗУ адаптера программы паролирования, которая осуществляет разграничение прав доступа, паролирование, контроль целостности программного и аппаратного обеспечения, администрирование и т.д. После загрузки программы паролирования осуществляется контроль целостности загруженного модуля и передача ему управления. При обнаружении нарушения целостности контролируемого ПО или оборудования производится вывод сообщения об ошибке, работа ПЭВМ блокируется и устанавливается признак "Вход только администратору безопасности".

В том случае, если при прохождении процедуры идентификации идентификатор карты-ключа не был опознан, происходит блокирование ПЭВМ.

1.4.2.2 Программа паролирования, являющаяся основным компонентом специального программного обеспечения ПАК "Барьер", выполняющегося до загрузки ОС. Данная программа производит процедуру аутентификации зарегистрированного в ПАК "Барьер" субъекта после ввода им пароля с клавиатуры. Значения символов, составляющих пароль, на экране монитора не отображаются. При введении пароля действуют правила: максимальная длина пароля – 255 символов, минимальная длина – 8 символов. Далее программа паролирования вычисляет значение функции хэширования от введенного пароля и передает ее в адаптер для сравнения. Если введен

верный пароль, то субъекту, зарегистрированному в ПАК "Барьер", будут предоставлены определенные для него ресурсы и права на выполнение команд, соответствующих его статусу, и будет установлена выбранная аппаратная конфигурация ПЭВМ. При этом субъект, имеющий статус "администратор ключей", имеет право на вход в систему совместно с администратором безопасности.

Субъекту, зарегистрированному в ПАК "Барьер", предоставляются всего три попытки ввода пароля. Если пароль введен неверно три раза, работа ПЭВМ блокируется.

После успешного завершения процедуры аутентификации осуществляется зашифрование логических дисков, которые не были зашифрованы при предыдущем сеансе работы, проводится контроль целостности файлов, указанных при процедуре инсталляции, и далее – загрузка ОС.

1.4.2.3 Все параметры, определяющие права каждого из пользователей, устанавливаются при инсталляции ПАК "Барьер" и могут быть изменены лишь администратором безопасности при помощи средств администрирования ПАК "Барьер".

1.4.2.4 Загрузка ОС выполняется после окончания работы программы паролирования, при этом управление ПЭВМ передается программе расширения BIOS. Программа расширения BIOS очищает оперативную память ПЭВМ (прописывает нули) по адресам, в которых работала программа паролирования.

1.4.2.5 Сразу после загрузки ОС драйвер ПАК "Барьер" уничтожает загрузчик ОС на НЖМД. Восстановление загрузчика ОС, хранящегося в защищенном виде в памяти адаптера ПАК "Барьер", осуществляется программой паролирования при очередном сеансе работы пользователя после успешного выполнения процедур идентификации и аутентификации.

1.4.2.6 Во время работы ОС ПАК "Барьер" взаимодействует с драйвером устройства. Драйвер принимает запросы на выполнение криптографических преобразований и направляет их в ПАК "Барьер", который производит их обработку и выдает результат.

1.5 Средства измерения, инструмент и принадлежности

1.5.1 Специальных измерительных приборов, необходимых для работы и настройки ПАК "Барьер" и выполнения работ по техническому обслуживанию, не требуется.

1.6 Маркировка

1.6.1 На плату ПАК "Барьер" нанесена маркировка, содержащая следующие данные:

- товарный знак предприятия-изготовителя ПАК "Барьер";
- наименование и обозначение ПАК "Барьер";
- заводской номер ПАК "Барьер" по системе нумерации предприятия-изготовителя.

1.7 Упаковка

1.7.1 Все составные компоненты ПАК "Барьер" и эксплуатационный документ РЭ, помещены в запаянный полиэтиленовый мешок. В полиэтиленовый мешок вложен упаковочный лист.

2 Использование по назначению

2.1 Эксплуатационные ограничения

2.1.1 Для функционирования ПАК "Барьер" необходимы совместимая ПЭВМ, работающая под управлением ОС семейства MS Windows 98/NT/2000/XP/2003, поддерживающей любую из файловых систем FAT12, FAT16, FAT32, NTFS, и инсталляционный комплект дисков, содержащий драйвер устройства.

В состав ПЭВМ должны входить:

- процессор, совместимый с Intel Pentium, с тактовой частотой не менее 100 МГц;
- ОЗУ емкостью не менее 32 Мбайт;
- материнская плата, имеющая свободный PCI слот;
- не более четырех НЖМД, имеющих интерфейс IDE. Объем каждого НЖМД должен быть не более 120 Гбайт, кроме того, в конце первого физического диска должно быть свободное пространство размером не менее 1 цилиндра (7 Мбайт). Количество логических дисков – не более 24, при этом все логические диски не должны содержать сбойных секторов;
- накопитель на гибких магнитных дисках (НГМД) 3,5".

В случае невозможности обеспечения вышеуказанных требований следует обратиться к разработчику ПАК "Барьер".

2.1.2 Максимальное количество субъектов, которые могут быть зарегистрированы в ПАК "Барьер" – 8.

2.1.3 Для одного пользователя количество файлов, подлежащих контролю, должно быть не более 2048.

2.1.4 Если в ПЭВМ установлено несколько НЖМД, то в Windows 98/NT/2000/XP/2003 обозначения логических дисков должны соответствовать следующим требованиям:

- логические диски обозначаются латинскими буквами;
- обозначения логических дисков начинаются с латинской буквы "C", и далее следуют по порядку в латинском алфавите.

2.1.5 На ПЭВМ с установленным ПАК "Барьер" **ЗАПРЕЩАЕТСЯ** пользоваться утилитами, осуществляющими изменение структуры логических дисков на НЖМД.

2.1.6 Для работы на защищенной ПЭВМ пользователь должен быть зарегистрирован в ПАК "Барьер", для чего ему необходимо определить:

- имя, под которым пользователь будет работать в системе;
- персональный идентификатор пользователя (карта-ключ);
- пароль и возможность его смены (при необходимости);
- права пользователя;
- перечень программных средств, которые подлежат контролю на целостность;
- дополнительные меры безопасности (время жизни пароля, период времени, когда пользователю разрешен вход в систему).

После процедуры регистрации, выполняемой администратором безопасности, пользователь получает персональный идентификатор, о чем делается соответствующая запись в реестре учета носителей информации за подписью пользователя.

2.1.7 Для эксплуатации и эффективного применения средства защиты ПАК "Барьер", поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов требуется:

- физическая охрана ПЭВМ и ее средств;
- наличие субъектов, выполняющих роли (обязанности) администратора безопасности и администратора ключей;
- учет персональных идентификаторов пользователей (карт-ключей);
- периодическое тестирование средства защиты ПАК "Барьер".

2.1.8 Условия эксплуатации ПАК "Барьер":

– температура окружающего воздуха от плюс 5 до плюс 40 °С;

– относительная влажность окружающего воздуха до 80 % при температуре окружающего воздуха плюс 25 °С;

– атмосферное давление от 84 до 107 кПа (630 до 800 мм рт.ст).

2.2 Подготовка комплекса программно-аппаратного защиты ПЭВМ от несанкционированного доступа "Барьер" к использованию

2.2.1 Перед началом работы необходимо внимательно изучить настоящее РЭ.

2.2.2 ПАК "Барьер" обеспечивает электрическую, механическую и пожарную безопасность персонала в соответствии с требованиями СТБ МЭК 60950-1-2003 и ГОСТ 25861-83.

2.2.3 Подключать и отключать любые внешние устройства ПЭВМ необходимо только в выключенном состоянии.

2.2.4 Необходимо удостовериться, что в наличии имеется драйвер устройства ПАК "Барьер".

2.2.5 Необходимо удостовериться в наличии платы адаптера ПАК "Барьер" СЮИК.467458.001.

2.2.6 Необходимо убедиться в отсутствии механических повреждений платы адаптера.

2.2.7 Подготовку ПАК "Барьер" к использованию следует проводить при отключенной сети питания.

2.2.8 Установку платы ПАК "Барьер" в ПЭВМ производить в соответствии с рисунком 1 в следующем порядке:

– отключить ПЭВМ от сети питающего напряжения;

– снять кожух системного блока ПЭВМ;

– установить плату ПАК "Барьер" в свободный PCI-разъем на материнской плате ПЭВМ;

– к вилке J2 платы ПАК "Барьер" подключить шлейф датчика вскрытия корпуса;

– к вилке J4 платы ПАК "Барьер" подключить считыватель карт-ключей;

– установить перемычку J3 на плате ПАК "Барьер";

– установить датчик вскрытия корпуса согласно 2.2.8;

– закрыть кожух системного блока ПЭВМ;

– провести инсталляцию ПАК "Барьер" в соответствии с 2.3.

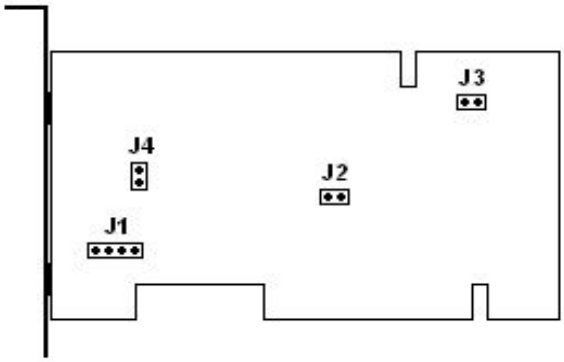

Рисунок 1

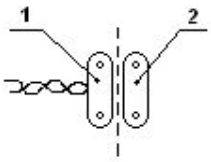

Рисунок 2

2.2.9 Установку датчика вскрытия корпуса производить в соответствии с рисунком 2 следующим образом:

– выбрать место для установки двух элементов датчика таким образом, чтобы при закрытии

корпуса оба элемента датчика находились в непосредственной близости друг от друга на расстоянии не более 1 см. Один элемент датчика (поз. 1) устанавливается в корпусе системного блока, а другой (поз. 2) – на съемной крышке корпуса системного блока;

– установить элемент датчика, содержащий геркон (поз. 1), в корпусе системного блока ПЭВМ и закрепить его при помощи клея или дополнительных стоек и винтов. При использовании нескольких датчиков элементы датчика, содержащие геркон, соединяются последовательно;

– установить элемент датчика, содержащий магнит (поз. 2), на съемной крышке корпуса системного блока ПЭВМ и закрепить его при помощи клея или винтов.

2.3 Программная инсталляция комплекса программно-аппаратного защиты ПЭВМ от несанкционированного доступа "Барьер"

2.3.1 Подготовка к процессу инсталляции

2.3.1.1 Процесс инсталляции ПО представляет собой последовательность действий, осуществляемых пользователем, которым является администратор безопасности, для установки программной части ПАК "Барьер" на ПЭВМ.

2.3.1.2 Перед тем, как проводить инсталляцию, необходимо тщательно ознакомиться с настоящим документом для получения полного представления о требованиях непосредственно к процессу инсталляции.

2.3.1.3 Необходимо удостовериться, что ПЭВМ удовлетворяет всем требованиям, указанным в 2.1.

2.3.1.4 Необходимо четко сформулировать следующие параметры для каждого субъекта, который будет зарегистрирован в ПАК "Барьер":

– фамилия, имя, отчество;
– статус (администратор безопасности, администратор ключей, пользователь);
– пароли доступа к системе;
– список доступных каждому конкретному пользователю логических дисков;
– список логических дисков, подлежащих шифрованию;
– список контролируемых файлов.

2.3.2 Процесс инсталляции

2.3.2.1 После проведения подготовки, описанной в 2.3.1, можно приступить к инсталляции программного обеспечения ПАК "Барьер".

При инсталляции такие операции, как регистрация пользователя со статусом "пользователь" согласно 2.3.2.27, а также операции, описывающие процессы выбора контролируемых файлов согласно 2.3.2.31– 2.3.2.34 и назначение шифруемых дисков в соответствии с 2.3.2.39 – 2.3.2.41, могут выполняться при необходимости.

Установка драйвера устройства для **Windows 98/NT/2000/XP/2003** выполняется согласно 2.3.2.5 – 2.3.2.12. Установка драйвера устройства для **Windows NT** выполняется согласно 2.3.2.4.1.

2.3.2.2 Для управления процессом инсталляции доступны следующие клавиши и сочетания клавиш:

– "**Tab**", "**Shift+Tab**" клавиатуры ПЭВМ, манипулятор типа "**мышь**" – для выбора пунктов меню или установки курсора в поле ввода данных или поле выбора режима или действия;

– "**Enter**", левая клавиша манипулятора типа "мышь" – для подтверждения сделанного выбора или нажатия кнопки на отображаемых сообщениях-диалогах;

– "**Left Shift** + **Right Shift**" – для смены английской раскладки клавиатуры на русскую, и наоборот. При этом, если устанавливается раскладка для русского языка, бордюр экрана окрашивается в синий цвет.

Перемещение по пунктам меню производится с помощью клавиш "**Tab**", "**Shift+Tab**" или при помощи манипулятора типа "мышь". При нажатии клавиши "Enter" или при нажатии левой

клавиши манипулятора типа "мышь" подтверждается выбор пункта меню.

2.3.2.3 Для начала процесса инсталляции программной части ПАК "Барьер" необходимо включить питание ПЭВМ. После завершения внутреннего теста ПЭВМ и отображения соответствующей служебной информации на экране монитора отобразится сообщение, представляющее собой начальное меню инсталляции в соответствии с рисунком 3.

Рисунок 3

2.3.2.4 При помощи указателя манипулятора типа "мышь" или клавиши "Tab" клавиатуры выбрать пункт меню "**Вход в систему**" и подтвердить выбор нажатием клавиши "Enter" или левой клавиши манипулятора типа "мышь". При этом управление будет передано системному загрузчику BIOS ПЭВМ для загрузки ОС.

2.3.2.4.1 Для **Windows NT** установка драйвера ПАК "Барьер", размещенного на ГМД, выполняется следующим образом:

– после загрузки ОС необходимо вставить в дисковод ГМД из комплекта поставки, который содержит драйвер устройства;

– в меню "Пуск" операционной системы выбрать пункт "Выполнить" и в появившемся окне ввести строку "**a:\winnt\barpci.bat**";

– нажать кнопку "Ок" или клавишу "Enter", после чего ОС произведет копирование файлов драйверов в свои системные папки. По окончании копирования на экране монитора отобразится сообщение, предлагающее произвести перезагрузку ПЭВМ;

– выполнить перезагрузку ПЭВМ;

– далее выполнение инсталляции продолжить в соответствии с 2.3.2.12.

Аналогичным образом выполняется установка драйвера, размещенного на компакт-диске.

2.3.2.5 Во время загрузки ОС MS Windows™ будет обнаружено новое устройство, при этом на экране монитора отобразится запрос мастера установки устройств в соответствии с рисунком 4.

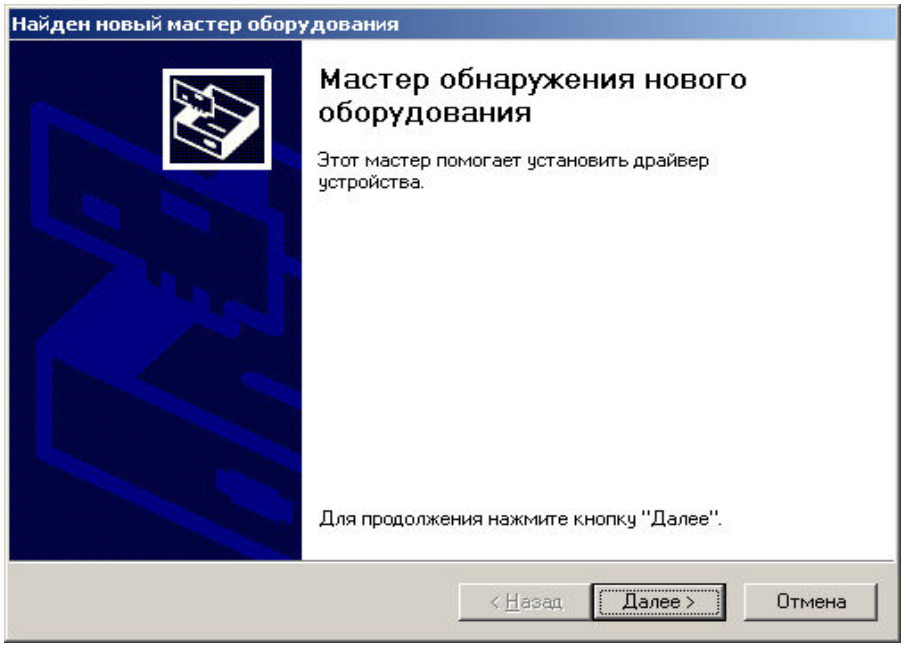

Рисунок 4

2.3.2.6 Нажать кнопку "Далее". При этом на экране отобразится сообщение в соответствии с рисунком 5.

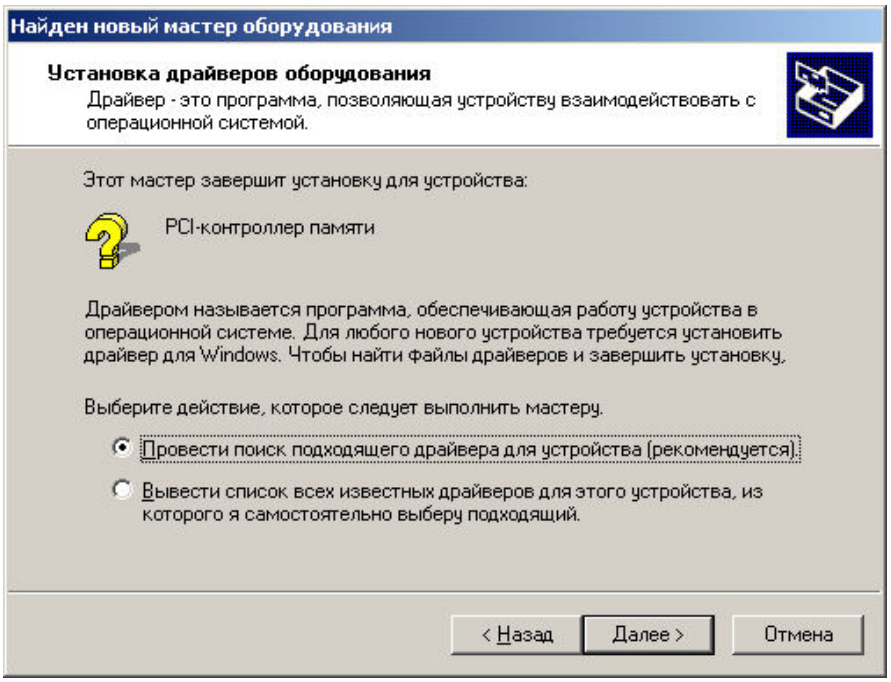

Рисунок 5

2.3.2.7 Выбрать действие для мастера установки нового устройства: "Провести поиск подходящего драйвера для устройства". Нажать кнопку "Далее". При этом на экране монитора отобразится сообщение в соответствии с рисунком 6.

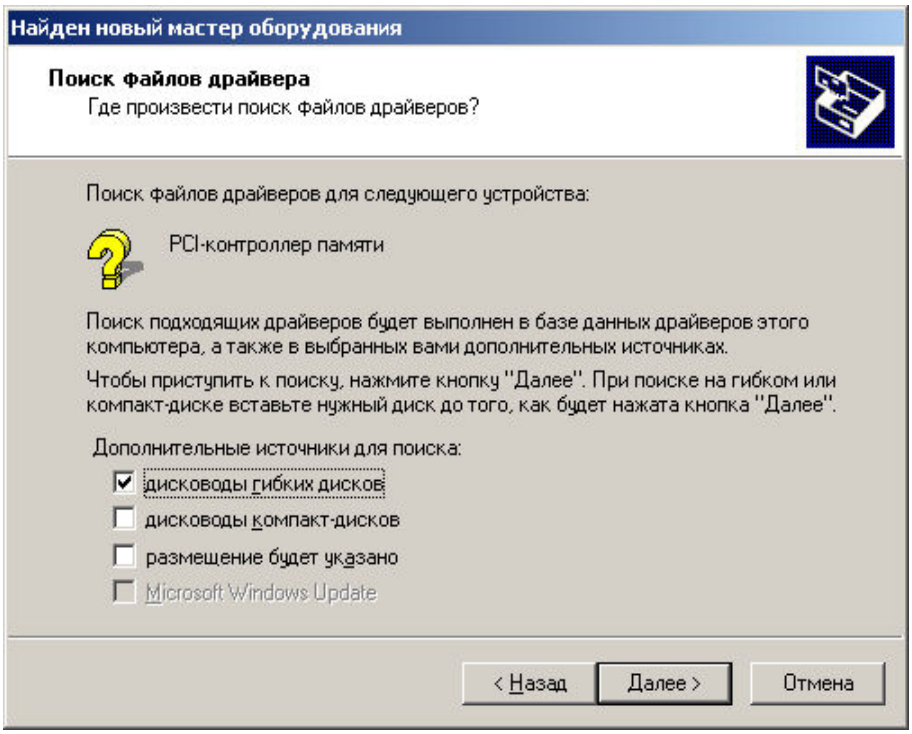

Рисунок 6

2.3.2.8 Выбрать источник для поиска драйвера: "дисководы гибких дисков", остальные источники отключить (снять отметки). Вставить в НГМД дискету из комплекта поставки. Нажать кнопку "Далее". После обнаружения на дискете необходимых файлов, на экране монитора отобразится сообщение в соответствии с рисунком 7.

2.3.2.9 Нажать кнопку "Далее". При этом ОС произведет копирование файлов драйверов в свои системные папки. По окончании копирования на экране монитора отобразится сообщение в

соответствии с рисунком 8.

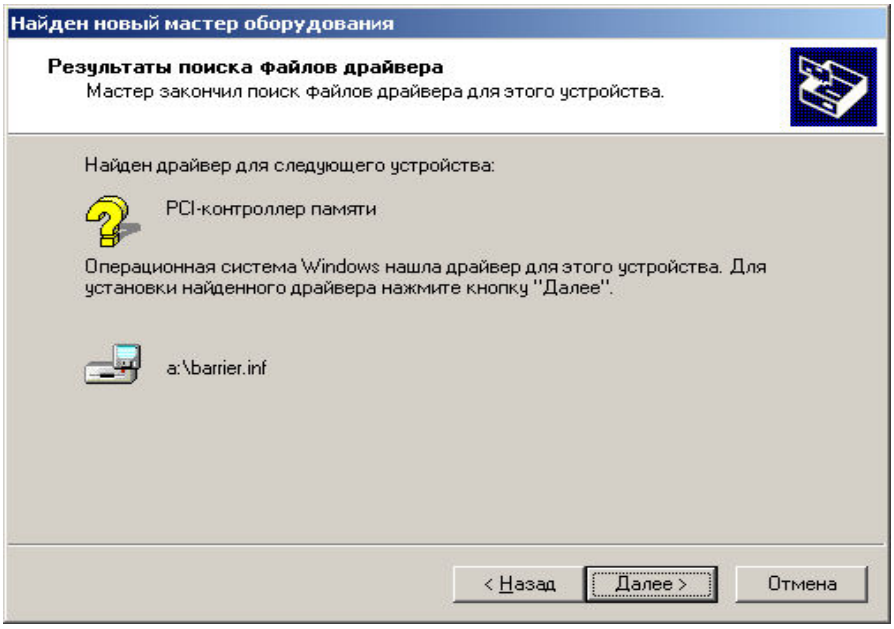

Рисунок 7

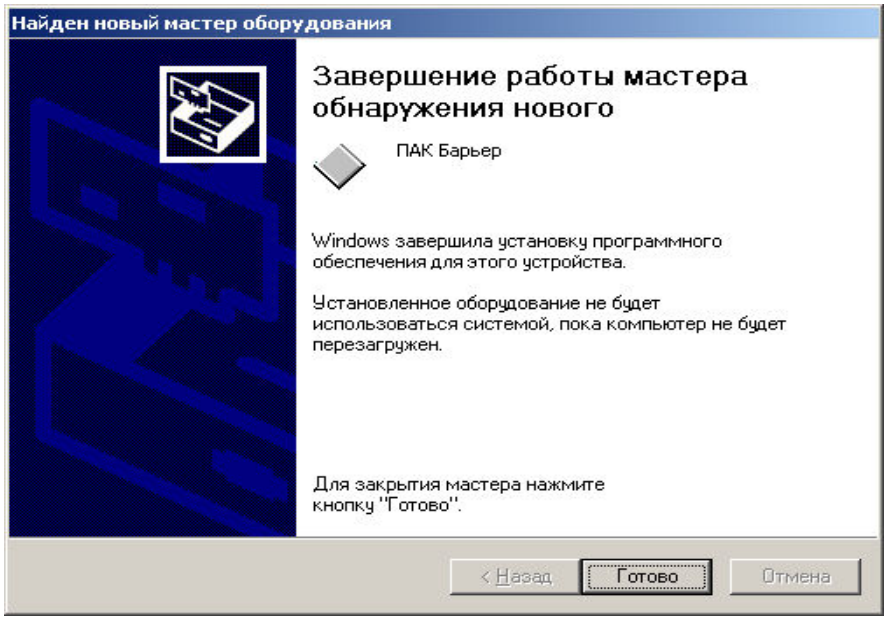

Рисунок 8

2.3.2.10 Нажать кнопку "Готово". При этом на экране монитора ПЭВМ отобразится сообщение в соответствии с рисунком 9.

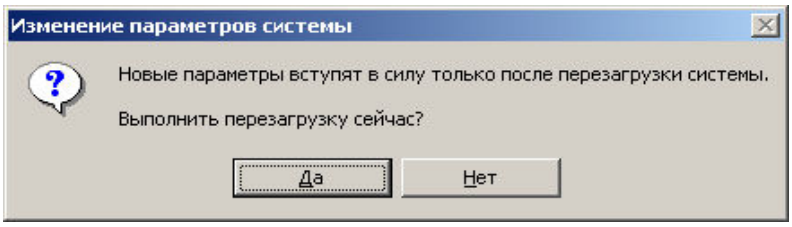

Рисунок 9

2.3.2.11 Подтвердить выполнение перезагрузки нажатием кнопки "Да".

2.3.2.12 После перезагрузки ПЭВМ на экране монитора отобразится начальное меню инсталляции в соответствии с рисунком 3.

2.3.2.13 Выбрать пункт меню "**Инсталляция**" и подтвердить выбор нажатием клавиши "Enter" или левой клавиши манипулятора типа "мышь". При этом на экране монитора ПЭВМ отобразится сообщение в соответствии с рисунком 10, предлагающее установить в считыватель

карту-ключ для сохранения на ней мастер-ключа.

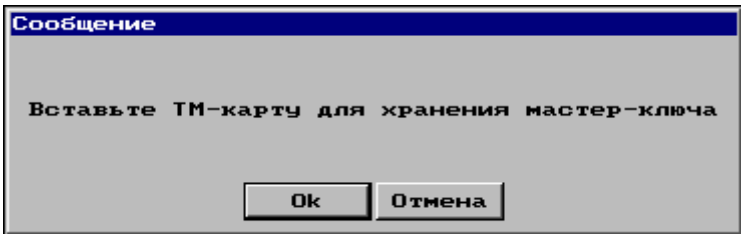

Рисунок 10

2.3.2.14 В случае нажатия кнопки "Отмена" инсталляция прерывается и управление передается системному загрузчику ПЭВМ. Для продолжения инсталляции необходимо установить карту-ключ в считыватель и нажать кнопку "Ок". При этом произойдет запись мастер-ключа. После завершения процесса записи ключа на экране монитора отобразится сообщение в соответствии с рисунком 11.

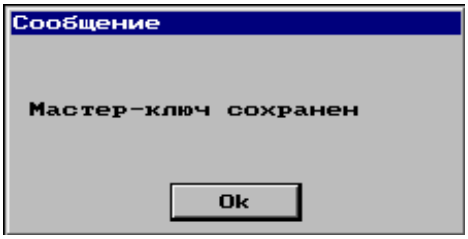

Рисунок 11

2.3.2.15 Нажать кнопку "Ок". При этом на экране монитора отобразится основное меню инсталляции в соответствии с рисунком 12.

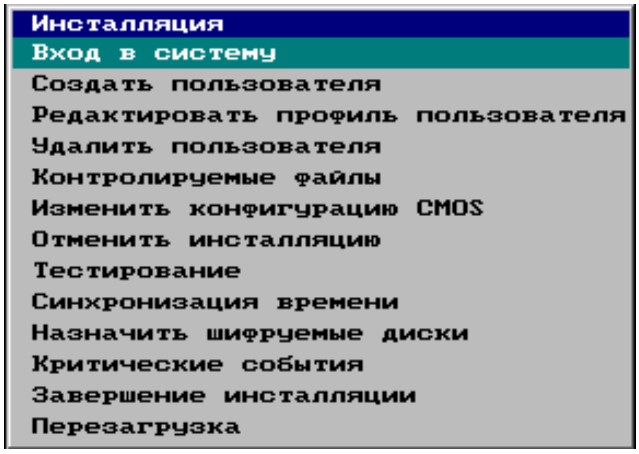

Рисунок 12

2.3.2.16 Для регистрации какого-либо субъекта в ПАК "Барьер" выбрать пункт "**Создать пользователя**" и подтвердить выбор. При этом на экране монитора отобразится окно в соответствии с рисунком 13.

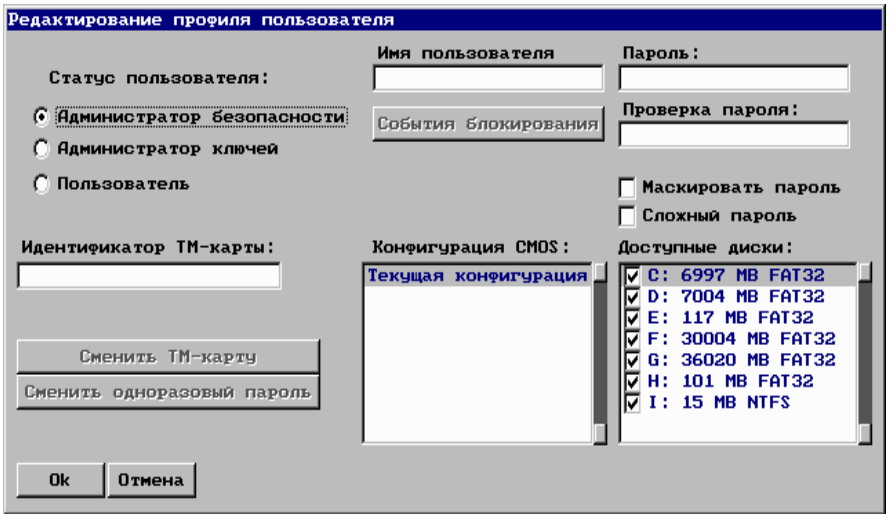

Рисунок 13

2.3.2.17 Если для регистрируемого субъекта необходимо изменить текущую конфигурацию ПЭВМ (настройки BIOS), следует перезагрузить ПЭВМ. Во время перезагрузки установить системные настройки BIOS, в соответствии с технической документацией на системную плату ПЭВМ, в необходимой регистрируемому субъекту конфигурации. После перезагрузки на экране отобразится меню инсталляции в соответствии с рисунком 12, при этом выбрать пункт "**Создать пользователя**" в соответствии с 2.3.2.16.

2.3.2.18 Вначале необходимо создать профиль субъекта, имеющего статус "администратор безопасности", для чего в группе "**Статус пользователя**" следует выбрать тип пользователя "администратор безопасности".

2.3.2.19 В поле "**Имя пользователя**" ввести имя пользователя (наименование учетной записи), для которого создается профиль.

2.3.2.20 Для исключения возможности просмотра посторонними лицами вводимого пароля на экране монитора необходимо установить отметку в поле "**Маскировать пароль**". При этом вместо символов вводимого пароля будут отображаться символы "*".

2.3.2.21 В поле "**Пароль**" с клавиатуры ПЭВМ ввести пароль для доступа данного пользователя к закрепленной за ним конфигурации ПЭВМ. Минимальная длина пароля – 8 символов, максимальная – 255 символов. Для корректной работы ПАК "Барьер" совместно с ОС Windows имена и пароли создаваемых пользователей должны соответствовать именам и паролям пользователей, зарегистрированных в ОС Windows. Рекомендации по выбору пароля приведены в приложении А.

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

2.3.2.23 В списке "**Доступные диски**" установить отметки напротив доступных для данного пользователя логических дисков. Логические диски, напротив обозначений которых отметки будут сняты, данному пользователю доступны не будут.

2.3.2.24 Список "**Конфигурация CMOS**" отображает список доступных конфигураций (настроек BIOS ПЭВМ). Выбранная конфигурация закрепляется за регистрируемым пользователем.

2.3.2.25 При необходимости изменить текущую конфигурацию CMOS (настройки BIOS ПЭВМ), которая будет закреплена за регистрируемым пользователем, следует воспользоваться пунктом меню "**Изменить конфигурацию CMOS**" до начала процесса создания профиля нового пользователя. После изменения настроек BIOS ПЭВМ, при редактировании профиля пользователя, в списке "Конфигурация CMOS" следует выбрать пункт "Текущая конфигурация".

2.3.2.26 Для завершения формирования профиля для данного пользователя необходимо нажать кнопку "Ок". При этом на экране монитора ПЭВМ отобразится сообщение в соответствии с рисунком 14.

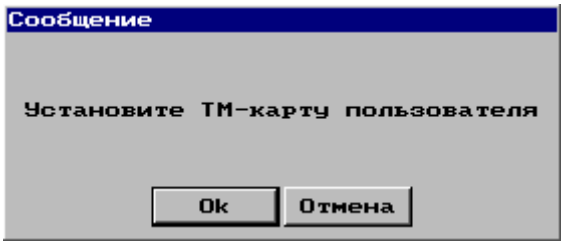

Рисунок 14

2.3.2.27 Установить в считыватель личный идентификатор пользователя (карту-ключ). Затем нажать кнопку "Ок".

В случае возникновения после нажатия кнопки "Ок" ошибки, на экране монитора ПЭВМ будет выдано соответствующее предупреждение в соответствии с рисунком 15.

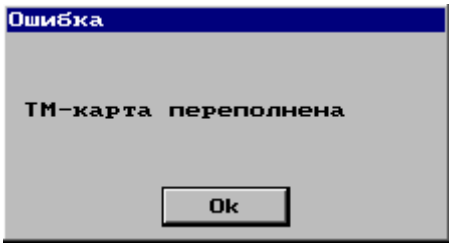

Рисунок 15

При этом необходимо проверить, не используется ли установленная карта-ключ в качестве идентификатора ранее зарегистрированного пользователя либо для хранения мастер-ключа, а также правильно ли подключен считыватель.

При переполнении карты-ключа, в случае если она была до этого зарегистрирована восемь раз, пользователю будет предложено очистить её внутреннюю память, при этом на экране монитора будет выдано соответствующее предупреждение в соответствии с рисунком 16.

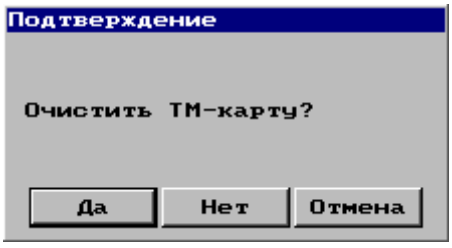

Рисунок 16

При успешном завершении всех операций на экране монитора отобразится сообщение в соответствии с рисунком 17.

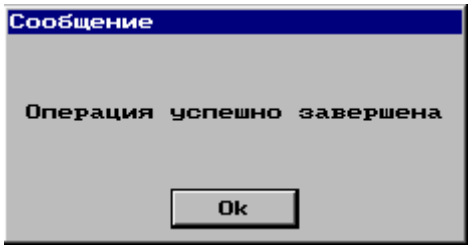

Рисунок 17

2.3.2.28 Нажать кнопку "Ок". При этом, если была выбрана текущая конфигурация CMOS, на экране монитора отобразится сообщение для ввода наименования текущей конфигурации и закрепления ее за регистрируемым пользователем в соответствии с рисунком 18.

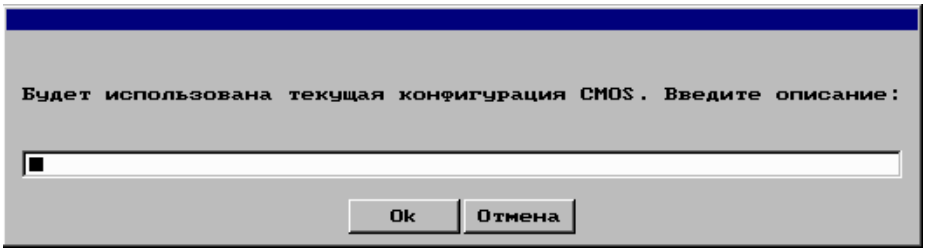

Рисунок 18

Необходимо ввести любое словесное обозначение и нажать клавишу "Enter" на клавиатуре ПЭВМ. При этом произойдет сохранение профиля для данного пользователя. По завершении процесса записи профиля на экране отобразится сообщение в соответствии с рисунком 19.

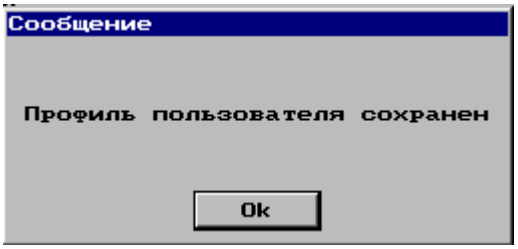

Рисунок 19

2.3.2.29 Нажать кнопку "Ок". При этом произойдет выход в основное меню инсталляции в соответствии с рисунком 12.

2.3.2.30 При необходимости повторить 2.3.2.16 – 2.3.2.29 для регистрации в ПАК "Барьер" субъектов, имеющих статус "пользователь". Данные пункты необходимо повторить и при создании профиля для субъекта, имеющего статус "администратор ключей", однако для него не устанавливается список "**Доступные диски**".

2.3.2.31 Пункт "**Контролируемые файлы**" выполняется при необходимости для любого пользователя. Выбрать пункт меню "Контролируемые файлы" и подтвердить выбор. При этом на экране монитора отобразится окно редактирования списка контролируемых файлов в соответствии с рисунком 20.

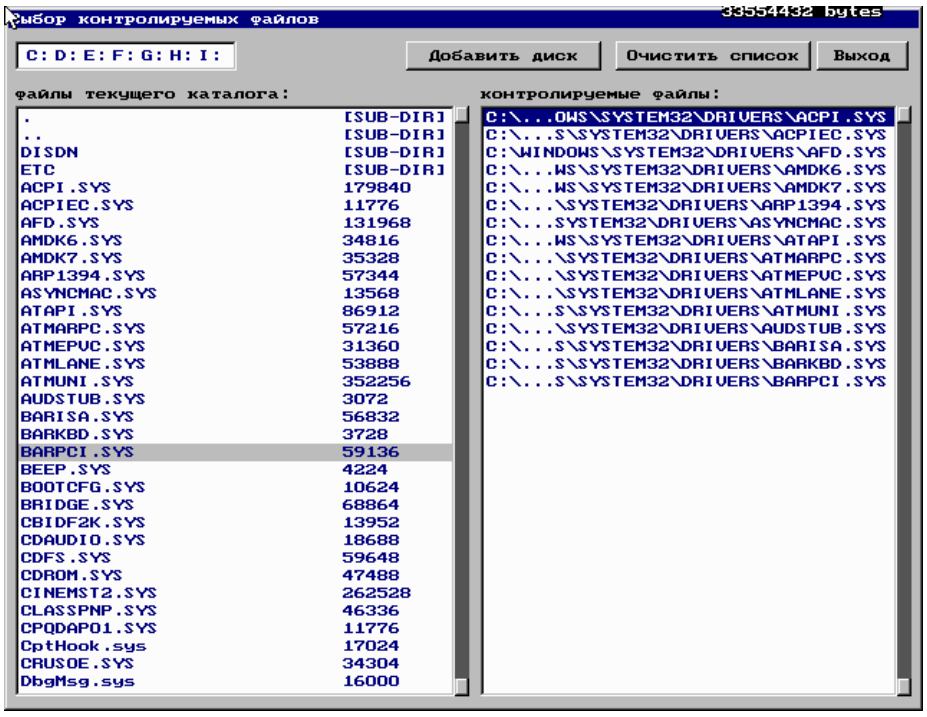

Рисунок 20

2.3.2.32 В левой колонке отображается список файлов и папок на текущем логическом диске. Выбор логического диска осуществляется в левом верхнем поле 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. Добавление папки в список контролируемых производится нажатием комбинации клавиш "**Ctrl** + **Enter**" на выбранной папке в левой колонке. При этом в список контролируемых добавляются все файлы, содержащиеся в выбранном каталоге и во всех его подкаталогах. Прервать рекурсивный поиск файлов в подкаталогах можно, нажав клавишу "**Esc**". Удаление файла из списка контролируемых производится нажатием клавиши "**Delete**" на клавиатуре ПЭВМ на выбранном файле в правой колонке. Кнопка "**Очистить список**" служит для очищения списка файлов, подлежащих контролю. При нажатии кнопки **"Добавить диск"** в список для контроля добавляется текущий выбранный логический диск. Контроль диска осуществляется посекторно, без учёта файловой системы.

2.3.2.33 Произвести выбор и добавление необходимых файлов в список контролируемых. Нажать кнопку "**Выход**". При этом на экране монитора отобразится сообщение в соответствии с рисунком 21.

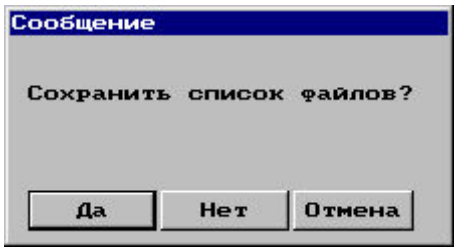

Рисунок 21

2.3.2.34 Нажать кнопку "Да". При этом будут пересчитаны и сохранены значения функций хэширования для выбранных файлов. При выполнении данной операции на экране монитора будет отображаться сообщение в соответствии с рисунком 22.

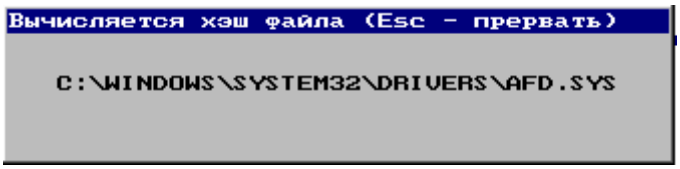

Рисунок 22

После завершения произойдет выход в основное меню инсталляции (см. рисунок 12).

2.3.2.35 Пункт "**Изменить конфигурацию CMOS**" выполняется при необходимости изменения текущей конфигурации CMOS для регистрируемого пользователя. При выборе данного пункта и подтверждении выбора на экране монитора отображается сообщение в соответствии с рисунком 23.

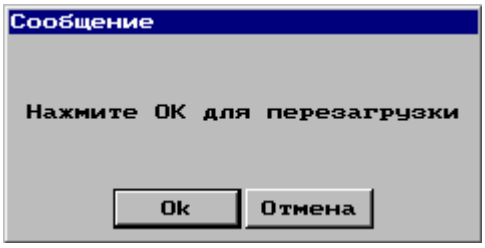

Рисунок 23

2.3.2.36 Нажать кнопку "Ок". При этом произойдет перезагрузка ПЭВМ. Во время перезагрузки следует войти в настройки BIOS ПЭВМ и произвести необходимые изменения в конфигурации CMOS. Затем выйти с сохранением изменений, при этом произойдет автоматическая перезагрузка ПЭВМ.

После повторной перезагрузки на экране монитора отобразится меню инсталляции (см. рисунок 12). При этом необходимо выбрать пункт меню "Создать пользователя" в соответствии с 2.3.2.16 и начать создание учетной записи для нового пользователя.

2.3.2.37 Выбрать пункт меню "**Синхронизация времени**" и подтвердить выбор. При этом на экране монитора отобразится сообщение в соответствии с рисунком 24. Значения времени могут отличаться от изображенных на рисунке 24.

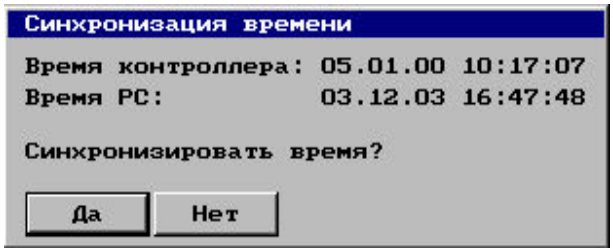

Рисунок 24

2.3.2.38 Нажать кнопку "Да". При этом произойдет запись (синхронизация) системного времени ПЭВМ в адаптер ПАК "Барьер". Затем произойдет выход в основное меню инсталляции (см. рисунок 12).

2.3.2.39 Пункт "**Назначить шифруемые диски**" выполняется при необходимости для любого пользователя. Выбрать пункт меню "Назначить шифруемые диски" и подтвердить выбор. При этом на экране монитора отобразится сообщение в соответствии с рисунком 25. Количество дисков в списке может отличаться от изображенных на рисунке 25.

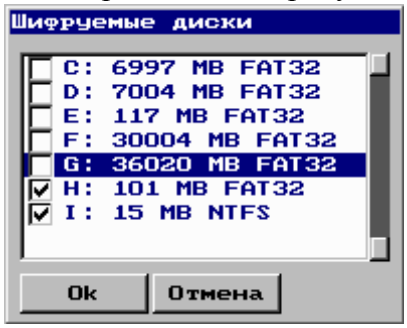

Рисунок 25

2.3.2.40 В списке "Шифруемые диски" установить отметки напротив обозначений логических дисков, которые должны быть зашифрованы. Логические диски, напротив обозначений которых отметки будут сняты, шифроваться не будут.

2.3.2.41 Нажать кнопку "Ок". При этом происходит сохранение информации о назначенных для шифрования логических дисках и выход в основное меню инсталляции (см. рисунок 12).

2.3.2.42 Выбрать пункт меню "**Завершение инсталляции**" и подтвердить выбор. При этом на экране монитора отобразится сообщение в соответствии с рисунком 26.

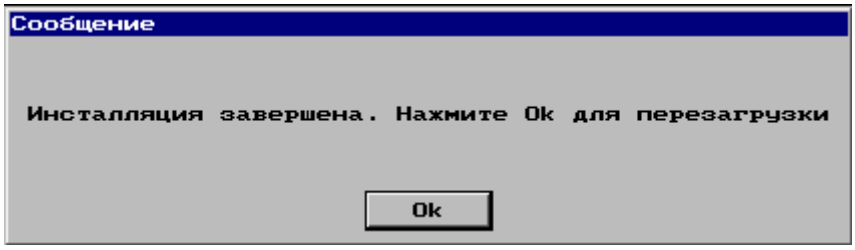

Рисунок 26

2.3.2.43 Установить в считыватель карту-ключ администратора безопасности и произвести перезагрузку ПЭВМ. После перезагрузки на экране монитора отобразится сообщение в соответствии с рисунком 27.

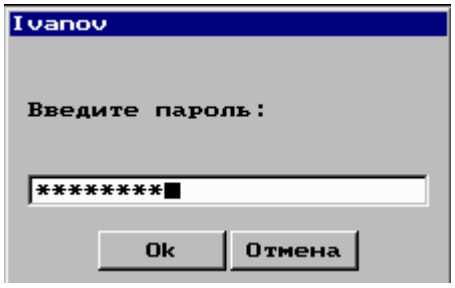

Рисунок 27

2.3.2.44 После ввода правильного пароля пользователя, в случае, если были назначены шифруемые диски, на экране монитора отобразится сообщение-запрос на подтверждение зашифрования каждого диска в соответствии с рисунком 28:

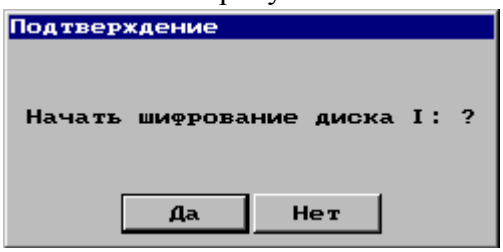

Рисунок 28

Для продолжения процесса зашифрования необходимо нажать кнопку "Да". При этом на экране монитора появится окно в соответствии с рисунком 29, на котором отображается процесс зашифрования дисков.

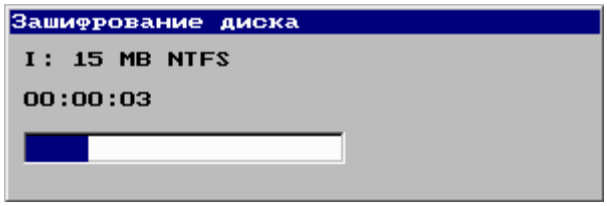

Рисунок 29

2.3.2.45 После завершения шифрования всех дисков инсталляция ПАК "Барьер" на ПЭВМ считается завершенной.

2.3.2.46 При выполнении инсталляции возможно отображение на экране монитора ПЭВМ следующих сообщений:

- "Продолжение инсталляции невозможно";
- "Для продолжения необходимо закрыть корпус";
- "Ошибка записи";
- "Ошибка".

При отображении на экране монитора любого из вышеуказанных сообщений необходимо выполнить соответствующие действия, описанные в разделе 14.

2.4 Использование комплекса программно-аппаратного защиты ПЭВМ от несанкционированного доступа "Барьер"

2.4.1 Ограничение прав доступа

2.4.1 ПАК "Барьер" предназначен для эксплуатации в составе ПЭВМ и применяется для обработки и хранения информации ограниченного распространения. При этом на ПЭВМ осуществляется локальная обработка данных без передачи информации за пределы области действия средств обеспечения безопасности.

2.4.1.2 Организация ограничения прав доступа осуществляется путем:

а) создания групп (классов) пользователей;

б) наделения каждой группы пользователей определенными правами;

в) генерации паролей для каждого субъекта, зарегистрированного в ПАК "Барьер";

г) идентификации и аутентификации субъектов, зарегистрированных в ПАК "Барьер"; при входе в систему до загрузки ОС;

д) предоставления пользователю работы только с заранее определенными для него логическими дисками.

2.4.1.3 В системе допустимы три группы субъектов доступа**:**

- администратор безопасности;
- администратор ключей;
- пользователь.

Администратор безопасности – пользователь системы, имеющий доступ ко всем ресурсам ПЭВМ, за исключением чтения (изменения) ключевой информации других групп пользователей, и выполняющий функции администрирования.

Администратор ключей – пользователь системы, имеющий право только на вход в систему совместно с администратором безопасности для осуществления процедур смены ключей или деинсталляции ПАК "Барьер".

Пользователь – самостоятельный пользователь, который работает только с определенными для него при инсталляции доступными ресурсами и конфигурацией, имеет доступ на чтение только личных и общих ключей.

2.4.1.4 Ограничение прав доступа к ресурсам ПЭВМ организовано при помощи системы контроля допустимости исполнения команд. При установленной защите система контроля анализирует статус текущего пользователя и момент времени исполнения команды (работает расширение BIOS ПАК "Барьер" или работает ОС).

2.4.2 Разделение ресурсов

2.4.2.1 Разделение ресурсов между пользователями осуществляется на уровне логических дисков. За каждым из пользователей закрепляется один или несколько логических дисков. После успешного завершения процедуры идентификации и аутентификации пользователь получает доступ к информации, объем которой устанавливается для него администратором безопасности.

2.4.2.2 Логические диски, закрепляемые за пользователями, могут быть зашифрованы. Они остаются зашифрованными на протяжении всего срока службы ПЭВМ, на которой установлен ПАК "Барьер", и расшифровываются при деинсталляции ПАК "Барьер" или в любой момент по желанию администратора безопасности.

2.4.3 Контроль целостности

2.4.3.1 Включение питания ПЭВМ инициирует процесс самотестирования адаптера, который проверяет систему контроля вскрытия корпуса. Данная система регистрирует факт вскрытия корпуса, время и количество вскрытий с момента сброса последнего признака вскрытия.

2.4.3.2 Далее вычисляются значения функции хэширования для технических средств ПЭВМ и сравниваются с эталонными значениями, сохраненными в ППЗУ ПАК "Барьер" при инсталляции. При обнаружении нарушения целостности технических средств ПЭВМ вход в систему становится доступным только администратору безопасности.

2.4.3.3 Кроме того вычисляются значения функции хэширования для критически важных файлов, целостность которых также необходимо контролировать. Перечень критически важных файлов устанавливается администратором безопасности. Вычисленные значения функции хэширования сравниваются с эталонными значениями, которые хранятся в зашифрованном виде в служебной области диска. При обнаружении нарушения целостности критически важных файлов вход в систему становится возможен только для администратора безопасности, для остальных пользователей вход в систему блокируется.

2.4.4 Датчик случайной числовой последовательности

2.4.4.1 Реализованный в адаптере датчик случайной числовой последовательности служит для получения случайной последовательности байт, которые используются в качестве ключей.

2.4.4.2 Доступ к генератору случайной последовательности разрешен для всех категорий пользователей, то есть любой прикладной процесс может получать из адаптера последовательность случайных чисел.

2.4.5 Формирование ключей, их хранение и смена

2.4.5.1 Генерация ключей и их запись в ППЗУ и ОЗУ PIC-микроконтроллер происходит на этапе инсталляции.

2.4.5.2 В ППЗУ ПАК "Барьер" все ключи хранятся в зашифрованном виде согласно ГОСТ 28147-89. При запросе прикладного процесса необходимый ключ расшифровывается внутри адаптера при помощи ключа, хранящегося в PIC- микроконтроллер.

2.4.5.3 При вскрытии корпуса ПЭВМ ключ в PIC- микроконтроллер уничтожается. Восстановление данного ключа доступно с помощью средств администрирования ПАК "Барьер" при наличии карты-ключа, содержащей копию мастер-ключа, сохранённую при инсталляции.

2.4.5.4 Смена ключей возможна только после двойного входа администратора безопасности совместно с администратором ключей с применением средств администрирования ПАК "Барьер".

2.4.6 Порядок использования средств администрирования

2.4.6.1 Все средства администрирования ПАК "Барьер" находятся в программе паролирования, загрузка которой в память ПЭВМ осуществляется программой расширения BIOS при входе в систему пользователя со статусом администратора безопасности.

2.4.6.2 Функции администрирования предназначены для выполнения следующих действий:

– просмотра журналов системных событий и контроля нарушения целостности критически важных файлов;
– комплексного тестирования ПАК "Барьер";
– смены ключей ПАК "Барьер" (функция может выполняться только после осуществления процедуры двойного входа администратора безопасности и администратора ключей);
– изменения профиля пользователя (перераспределение конфигураций CMOS, изменение доступных логических дисков пользователей);
– изменения списка контролируемых файлов;
– изменения списка шифруемых дисков.

2.4.7 Световая индикация

2.4.7.1 На крепежную планку адаптера выведены два светодиода. Свечение зеленого светодиода указывает на блокирование ПЭВМ на момент выполнения служебных функций адаптера и кратковременного отсутствия карты-ключа в считывающем устройстве.

2.4.7.2 Совместно с непрерывно горящим зеленым светодиодом возможно свечение красного. Непрерывное свечение красного светодиода указывает на то, что ПЭВМ заблокирована в результате попытки несанкционированного доступа. Серии вспышек красного светодиода с равными интервалами указывает на неисправность адаптера в случае неуспешного завершения самотестирования. При этом количество вспышек в серии указывает на причину неисправности.

Возможны следующие варианты индикации состояния адаптера красным светодиодом (количество вспышек в серии), при этом зеленый светодиод светится непрерывно:

– одна вспышка – ошибка обмена данными с PIC- микроконтроллером;
– две вспышки – ошибка энергонезависимой памяти (ППЗУ) адаптера;
– четыре вспышки – ошибка контрольной суммы контролируемых объектов;
– восемь вспышек – ошибка переписывания расширения BIOS в ОЗУ.

2.4.7.3 Количество вспышек, равное сумме некоторых из перечисленных вариантов,

указывает на наличие нескольких ошибочных ситуаций. Например, подсчитано девять вспышек. Представив число девять, как сумму значений из приведенного выше перечня вариантов, получаем: 9 = 1 + 8, что указывает на неисправность PIC-микроконтроллера (один) и нарушение работы ОЗУ (восемь).

2.5 Действия в экстремальных условиях

2.5.1 На случай стихийного бедствия (пожар, затопление помещения и т.п.) должны быть разработаны и утверждены руководством предприятия специальные инструкции, в которых предусматривается порядок вызова администрации, должностных лиц, очередность и порядок спасения имущества.

2.5.2 В случае возгорания ПЭВМ немедленно обесточить цепи питания и принять меры по ликвидации очага возгорания имеющимися средствами пожаротушения.

3 Организация рабочего процесса на защищенной ПЭВМ

3.1 Начало процесса

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

а) начало сеанса работы в системе;

б) работа пользователя в соответствии с функциональными обязанностями;

в) завершение сеанса работы.

3.1.2 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 типа "**мышь**" – для подтверждения сделанного выбора или нажатия кнопки на отображаемых сообщениях-диалогах.

3.2 Начало сеанса работы в системе

3.2.1 Необходимо получить у администратора безопасности карту-ключ пользователя и установить ее в считыватель.

3.2.2 Включить питание ПЭВМ.

3.2.3 Дождаться появления на экране монитора сообщения в соответствии с рисунком 27.

3.2.4 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. При ошибке будет выдаваться сообщение в соответствии с рисунком 30.

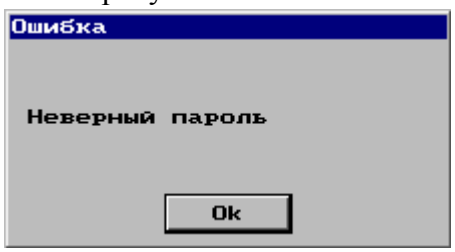

Рисунок 30

После истечения трех попыток ввода пароля вход в систему блокируется с выдачей сообщения в соответствии с рисунком 31.

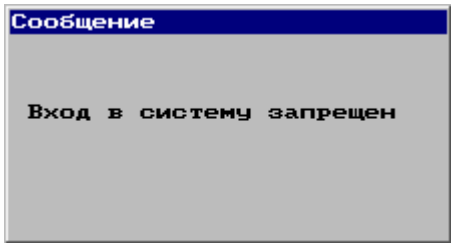

Рисунок 31

3.2.5 При успешном вводе пароля пользователя в случае, если были заданы контролируемые файлы, на экране монитора отобразится сообщение, показывающее процесс проверки целостности назначенных на контроль файлов, в соответствии с рисунком 32.

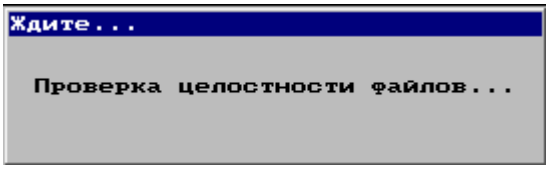

Рисунок 32

3.2.6 При обнаружении файлов с нарушением целостности содержимого, на экране монитора отображается сообщение в соответствии с рисунком 33. При нажатии кнопки "ОК" будет отображаться сообщение в соответствии с рисунком 34.

При этом доступ к ПЭВМ запрещается для всех пользователей, кроме администратора безопасности.

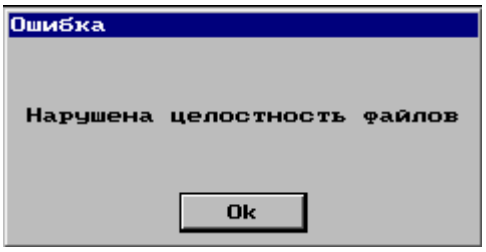

Рисунок 33

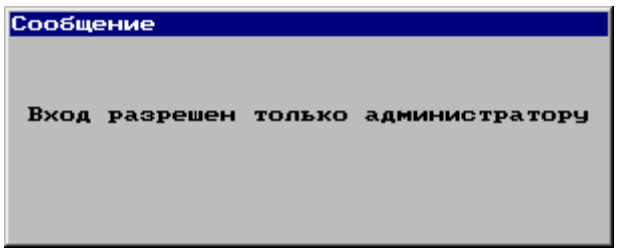

Рисунок 34

3.2.7 При успешном завершении процесса проверки целостности файлов управление передается системному загрузчику BIOS ПЭВМ для загрузки ОС и дальнейшей работы в установленном порядке.

3.3 Работа пользователя в соответствии с функциональными обязанностями

3.3.1 После выполнения процедуры "начало сеанса работы в системе" выполняется загрузка ОС и пользователь может приступить к работе, определяемой его функциональными обязанностями. Во время загрузки ОС Windows в считывателе должна находиться карта-ключ пользователя, при этом загрузка профиля пользователя осуществляется автоматически. Если в процессе загрузки ОС Windows карта-ключ извлекается из считывателя, на экране монитора появляется сообщение, предлагающее вставить идентификатор пользователя в считыватель. После установки карты-ключа пользователя в считыватель загрузка ОС Windows продолжается.

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

3.3.3 В процессе работы ОС Windows карта-ключ пользователя должна находиться в считывателе, в противном случае работа ПЭВМ блокируется. Для возобновления работы пользователю необходимо установить в считыватель карту-ключ.

3.4 Завершение сеанса работы

3.4.1 Завершение сеанса работы пользователем осуществляется в соответствии с правилами, определяемыми для установленной на ПЭВМ операционной системы.

3.4.2 Если ОС автоматически не выключит ПЭВМ, необходимо выключить питание ПЭВМ вручную.

3.4.3 На этом сеанс работы пользователя считается завершенным.

4 Работа в режиме администрирования

4.1 Назначение режима администрирования

4.1.1 Режим администрирования доступен пользователю, имеющему статус "администратор безопасности". Пользователю, имеющему статус "пользователь" и администратору ключей данный режим недоступен.

Вход в систему администратора безопасности осуществляется согласно 3.2 при использовании соответствующей карты-ключа и пароля.

4.1.2 При входе в систему администратора безопасности на экране монитора отображается меню администратора безопасности в соответствии с рисунком 35.

Все последующие действия, выполняемые администратором безопасности по редактированию системы, относятся к субъектам, имеющим статус "пользователь" и "администратор ключей".

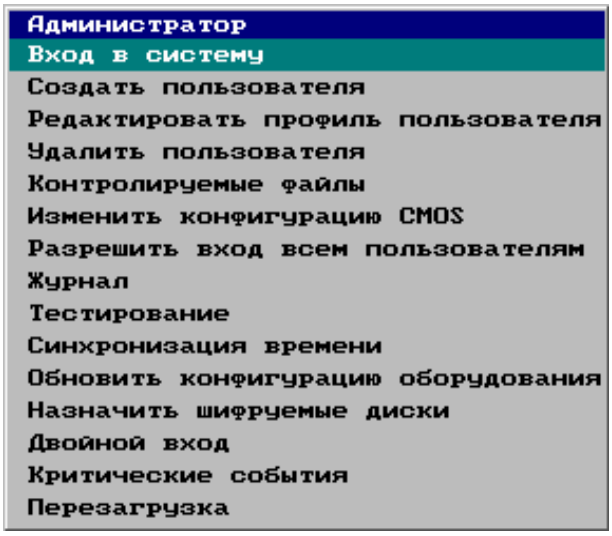

Рисунок 35

Меню администратора безопасности содержит следующие пункты:

– "Вход в систему" – предназначен для передачи управления загрузчику ПЭВМ и загрузки ОС;

– "Создать пользователя" – предназначен для создания профиля нового пользователя и добавления его в систему;

– "Редактировать профиль пользователя" – предназначен для редактирования профиля пользователя, уже существующего в системе;

– "Удалить пользователя" – предназначен для удаления из системы уже существующих пользователей;

– "Контролируемые файлы" – предназначен для редактирования списка файлов, подлежащих контролю на целостность до загрузки ОС;

– "Изменить конфигурацию CMOS" – предназначен для изменения текущей конфигурации CMOS (настроек BIOS ПЭВМ) и используется при необходимости перед выполнением пунктов меню "Создать пользователя" и "Редактировать профиль пользователя";

– "Разрешить вход всем пользователям" – предназначен для отмены блокировки входа в систему пользователям, имеющим статус "пользователь" после аварийных ситуаций;

– "Журнал" – предназначен для просмотра журнала аудита событий, происходящих в ПЭВМ, защищенной ПАК "Барьер";

– "Тестирование" – предназначен для выполнения внутреннего тестирования платы адаптера ПАК "Барьер" и отображения результата тестирования;

– "Синхронизация времени" – предназначен для выполнения синхронизации времени

системных часов ПЭВМ и внутренних часов платы адаптера;

– "Обновить конфигурацию оборудования" – предназначен для обновления списка оборудования, входящего в состав ПЭВМ;

– "Назначить шифруемые диски" – предназначен для назначения логических дисков, подлежащих шифрованию;

– "Двойной вход" – предназначен для удаления программной части ПАК "Барьер" из ПЭВМ либо для смены служебных ключей системы. Может выполняться только после осуществления процедуры двойного входа администратора безопасности совместно с администратором ключей;

– "Критические события" - предназначен для выбора событий, при которых будет блокироваться вход для пользователей.

– "Перезагрузка" – предназначен для корректной перезагрузки ПЭВМ.

4.2 Пункт "Вход в систему"

4.2.1 При выборе пункта "Вход в систему" и подтверждении выбора запускается на выполнение процесс проверки целостности контролируемых файлов, если таковые были заданы. На экране монитора ПЭВМ при этом отображается сообщение в соответствии с рисунком 36.

4.2.2 В случае обнаружения файлов с нарушением целостности на экране монитора ПЭВМ отображается сообщение в соответствии с рисунком 37. При этом доступ в систему запрещается для всех пользователей, имеющих статус "пользователь". После просмотра списка с поврежденными файлами, администратор безопасности может продолжить загрузку ОС нажатием кнопки "Ок".

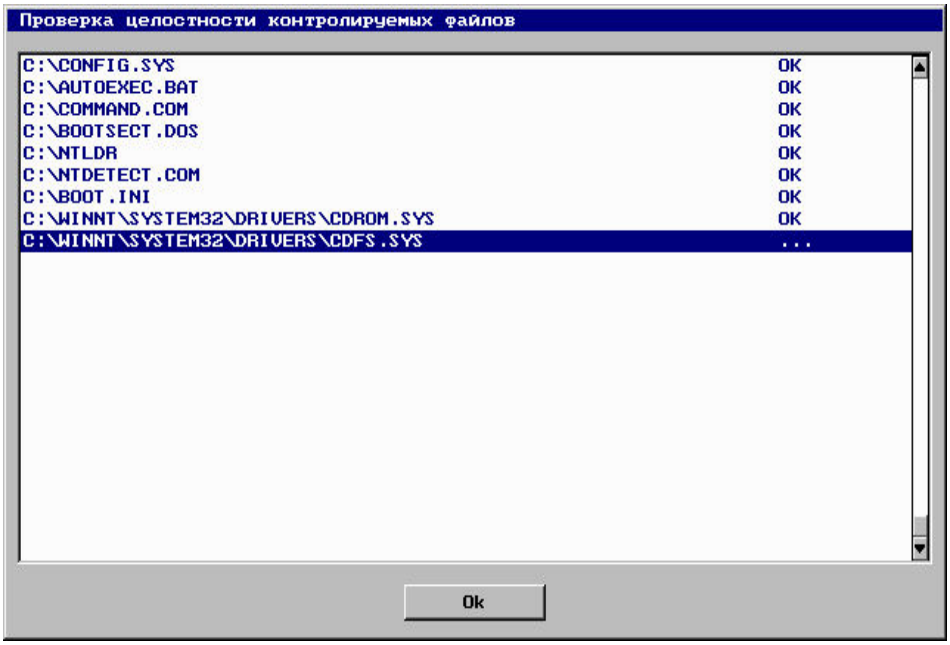

Рисунок 36

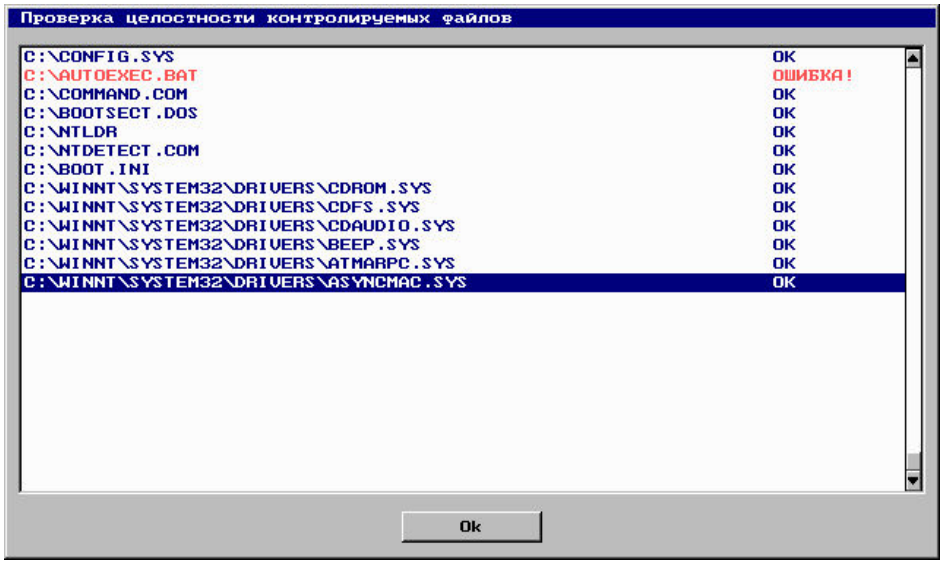

Рисунок 37

4.2.3 После завершения процесса проверки целостности файлов управление передается системному загрузчику BIOS ПЭВМ для загрузки ОС.

4.2.4 После загрузки ОС администратор безопасности может приступить к работе, определяемой его функциональными обязанностями.

4.3 Пункт "Создать пользователя"

4.3.1 Пункт "Создать пользователя" позволяет создать учетную запись нового пользователя и добавить его в систему. Работа с данным пунктом описана в 2.3.2.16 – 2.3.2.29.

4.4 Пункт "Редактировать профиль пользователя"

4.4.1 При выборе пункта "Редактировать профиль пользователя" и подтверждении выбора, на экране монитора отобразится сообщение в соответствии с рисунком 38.

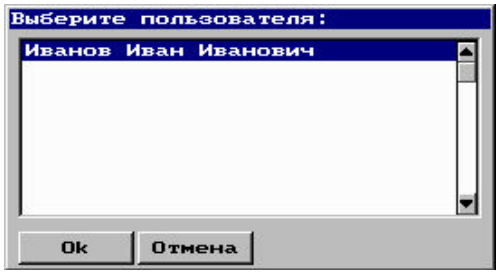

Рисунок 38

4.4.2 В изображенном окне необходимо выбрать имя пользователя, профиль которого требуется изменить. Затем нажать кнопку "Ок". При этом на экране монитора отобразится сообщение в соответствии с рисунком 13. Поля данной формы должны быть заполнены параметрами профиля выбранного пользователя, после чего становится доступной кнопка "Сменить ТМ-карту".

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

4.4.4 Для замены карты-ключа пользователя необходимо нажать кнопку "Сменить ТМ-карту". При этом на экране монитора отобразится сообщение, в соответствии с рисунком 39.

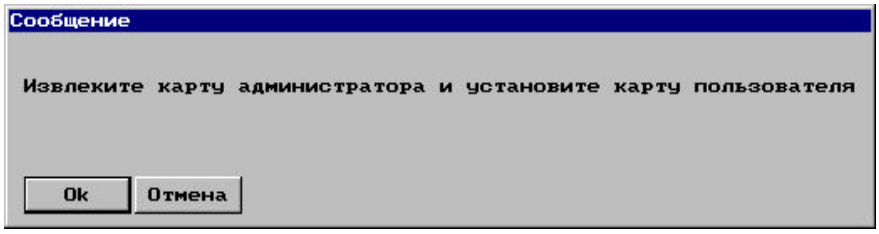

Рисунок 39

4.4.5 Необходимо извлечь из считывателя карту-ключ администратора безопасности и затем установить новую карту-ключ, которая будет закреплена за данным пользователем. Далее нажать кнопку "Ок". При этом на экране монитора отобразится сообщение в соответствии с рисунком 40.

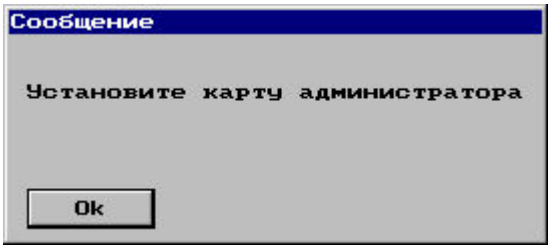

Рисунок 40

4.4.6 Необходимо извлечь карту пользователя, установить в считыватель извлеченную ранее карту-ключ администратора безопасности и нажать кнопку "Ок". При этом на экране монитора ПЭВМ отобразится форма редактирования профиля пользователя (см. рисунок 13) и в поле "Идентификатор ТМ-карты" отобразится идентификатор новой карты-ключа, закрепленной за редактируемым пользователем.

4.4.7 При смене карты-ключа пользователя возможно отображение на экране монитора следующих сообщений:

– "**ТМ-карта уже используется**" – в считыватель установлена карта-ключ, которая уже используется в данной системе;

– "**ТМ-карта мастер-ключа**" – в считыватель установлена карта-ключ, на которой сохранен мастер-ключ данной системы;

– "**ТМ-карта не вставлена**" – из считывателя была изъята карта-ключ администратора безопасности, но не была установлена новая карта-ключ пользователя;

– "**Ошибка обмена с контроллером**" – внутренняя ошибка аппаратуры ПАК "Барьер".

При отображении на экране монитора одного из вышеуказанных сообщений необходимо вернуть в считыватель карту-ключ администратора безопасности и повторить операцию с другой картой-ключом, выполнив соответствующие действия, описанные в разделе 14.

4.4.8 Для изменения конфигурации CMOS, закрепленной за редактируемым пользователем, необходимо следовать действиям, описанным в 2.3.2.24 – 2.3.2.25.

4.4.9 По завершении процесса редактирования профиля пользователя (см. рисунок 13) необходимо нажать кнопку "Ок". При этом на экране монитора отобразится сообщение в соответствии с рисунком 19.

4.4.10 Нажать кнопку "Ок". При этом на экране монитора отобразится меню администратора безопасности в соответствии с рисунком 35.

4.5 Пункт "Удалить пользователя"

4.5.1 При выборе пункта "Удалить пользователя" и подтверждении выбора на экране монитора отобразится сообщение в соответствии с рисунком 38.

4.5.2 В изображенном окне следует выбрать имя пользователя, которого необходимо удалить из системы, и нажать кнопку "Ок". При этом на экране монитора отобразится запрос на подтверждение удаления пользователя в соответствии с рисунком 41.

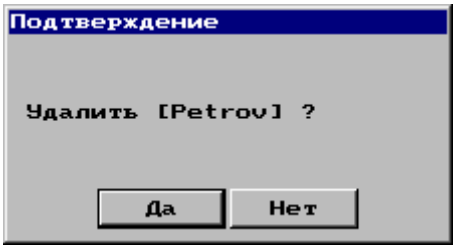

Рисунок 41

4.5.3 В случае подтверждения удаления, пользователь будет удален из системы. При этом на экране монитора отобразится меню администратора безопасности в соответствии с рисунком 35.

4.5.4 В случае отмены подтверждения удаления, пользователь не будет удален из системы. При этом на экране монитора отобразится меню администратора безопасности в соответствии с рисунком 35.

4.6 Пункт "Контролируемые файлы"

4.6.1 При выборе пункта "Контролируемые файлы" и подтверждении выбора на экране монитора отобразится окно редактирования списка контролируемых файлов в соответствии с рисунком 20.

4.6.2 Работа с данным пунктом согласно 2.3.2.31-2.3.2.32..

4.6.3 По завершении процесса редактирования списка контролируемых файлов необходимо нажать кнопку "Выход" (см. рисунок 20). При этом на экране монитора отобразится сообщение в соответствии с рисунком 21.

4.6.4 Для выхода из данного пункта меню с сохранением всех сделанных изменений в списке контролируемых файлов необходимо нажать кнопку "Да".

4.6.5 Для выхода из данного пункта меню без сохранения изменений в списке, сделанных администратором безопасности, необходимо нажать кнопку "Нет".

4.6.6 Для отмены выхода и возврата в режим редактирования списка контролируемых файлов необходимо нажать кнопку "Отмена".

4.6.7 При выходе из данного пункта на экране монитора отобразится меню администратора безопасности в соответствии с рисунком 35.

4.7 Пункт "Изменить конфигурацию CMOS"

4.7.1 При выборе пункта "Изменить конфигурацию CMOS" и подтверждении выбора на экране монитора отобразится сообщение в соответствии с рисунком 23.

4.7.2 Работа с данным пунктом производится согласно 2.3.2.35 – 2.3.2.36.

4.8 Пункт "Разрешить вход всем пользователям"

4.8.1 Пункт "Разрешить вход всем пользователям" позволяет пользователям работать с соответствующими ресурсами системы и снимает запрет входа в систему для пользователей, не имеющих статуса "администратор безопасности", и администратора ключей. Запрет входа в систему возникает в следующих ситуациях, которые являются критическими с точки зрения безопасности системы:

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

4.8.2 При выборе данного пункта меню и подтверждении выбора на экране монитора отобразится сообщение в соответствии с рисунком 42.

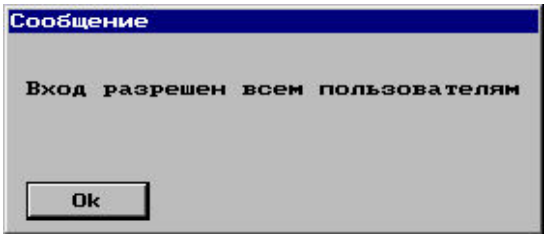

Рисунок 42

4.8.3 Для продолжения необходимо нажать кнопку "Ок". При этом на экране монитора отобразится меню администратора безопасности в соответствии с рисунком 35.

4.9 Пункт "Журнал"

4.9.1 При выборе пункта "Журнал" и подтверждении выбора на экране монитора ПЭВМ отобразится сообщение в соответствии с рисунком 43.

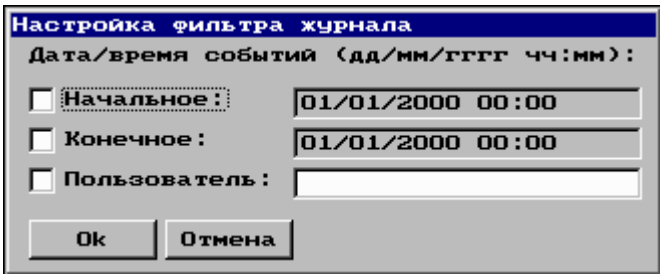

Рисунок 43

4.9.2 Для отображения всех записей журнала необходимо нажать кнопку "Ок". При этом на экране монитора отобразится сообщение в соответствии с рисунком 44.

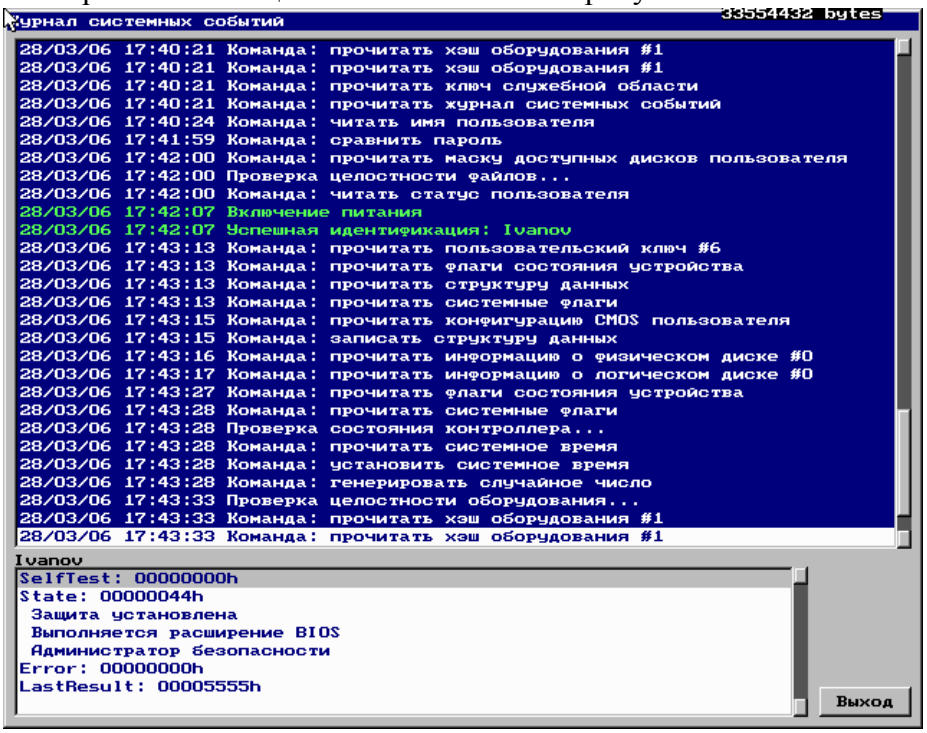

Рисунок 44

4.9.3 Для фильтрации отображаемых сообщений журнала аудита необходимо установить начальное и конечное состояние временного диапазона и выбрать пользователя, для которого будет осуществляться выборка и отображение записей.

4.9.4 Признаки фильтрации записей журнала аудита следующие:

– "Начальное" – состояние начала временного диапазона осуществления выборки и отображения записей;

– "Конечное" – состояние окончания временного диапазона осуществления выборки и отображения записей;

– "Пользователь" – выборка записей действий, совершенных во время нахождения в системе определенного пользователя, выбранного из списка пользователей.

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 времени и до конца журнала. Если задается вторая строка, то просматривается диапазон, начиная с начала журнала и до указанного времени. Время задается в следующем формате:

"дд/мм/гггг чч:мм",

где дд – число месяца, мм – месяц, гггг – год,

чч – часы, мм – минуты.

4.9.5 Пример результата выборки записей, изображенный на экране монитора в окне "Журнал системных событий", представлен на рисунке 44. Основную часть окна (на синем фоне) занимает список событий. Зеленым цветом отображены успешные события входа в систему и внутреннего тестирования ПАК "Барьер". Красным цветом отображаются события с такими нарушениями, как использование незарегистрированной в системе карты-ключа, подбор пароля пользователя, ошибки внутреннего тестирования ПАК "Барьер". Белым цветом отображаются команды, которыми обменивается система с ПАК "Барьер".

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

4.9.7 Выход из просмотра журнала аудита событий в меню администратора безопасности осуществляется нажатием кнопки "Выход" или клавиши "Esc" на клавиатуре ПЭВМ.

4.10 Пункт "Тестирование"

4.10.1 При выборе пункта "Тестирование" и подтверждении выбора ПАК "Барьер" подает команду на запуск внутреннего тестирования. По истечении некоторого времени, необходимого для проведения тестирования, на экране монитора отобразится сообщение в соответствии с рисунком 45.

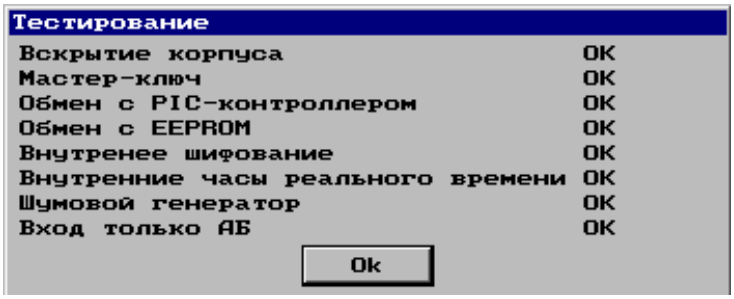

Рисунок 45

4.10.2 После анализа результатов внутреннего тестирования, для выхода в меню администратора безопасности, необходимо нажать кнопку "Ок". При этом на экране монитора отобразится меню администратора безопасности в соответствии с рисунок 35.

4.11 Пункт "Синхронизация времени"

4.11.1 Пункт "Синхронизация времени" предназначен для проведения синхронизации времени между системными часами ПЭВМ и внутренними часами ПАК "Барьер".

4.11.2 Работа с данным пунктом согласно 2.3.2.37-2.3.2.38.

4.12 Пункт "Обновить конфигурацию оборудования"

4.12.1 Пункт меню "Обновить конфигурацию оборудования" предназначен для обновления в

системе информации о конфигурации аппаратного состава ПЭВМ и используется в следующих случаях:

– осуществлено изменение набора плат расширения, устанавливаемых в PCI-разъемы на системной плате ПЭВМ;

– осуществлено изменение набора IDE-устройств (приводы CD-ROM).

ВНИМАНИЕ! Если необходимо сменить НЖМД, следует произвести деинсталляцию системы защиты, замену НЖМД, а затем – повторную инсталляцию.

4.12.2 При выборе пункта "Обновить конфигурацию оборудования" и подтверждении выбора произойдет обновление списка оборудования ПЭВМ, при этом на экране монитора отобразится сообщение в соответствии с рисунком 46.

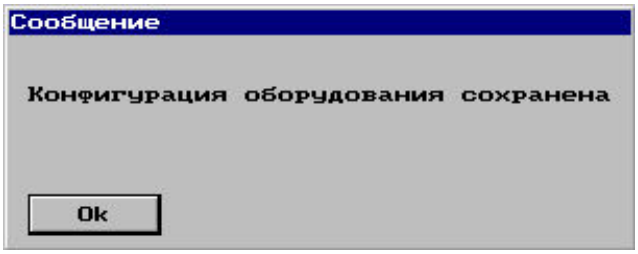

Рисунок 46

4.12.3 Нажать кнопку "Ок". При этом на экране монитора отобразится меню администратора безопасности в соответствии с рисунок 35.

4.13 Пункт "Назначить шифруемые диски"

4.13.1 Пункт меню "Назначить шифруемые диски" предназначен для выбора логических дисков (разделов), подлежащих шифрованию.

4.13.2 Работа с данным пунктом проводится в соответствии 2.3.2.39 – 2.3.2.41.

4.14 Пункт "Двойной вход"

4.14.1 При выборе пункта "**Двойной вход**" и подтверждении выбора на экране монитора ПЭВМ отобразится сообщение в соответствии с рисунком 47, предлагающее установить в считыватель карту-ключ второго администратора (администратора ключей) и ввести его пароль.

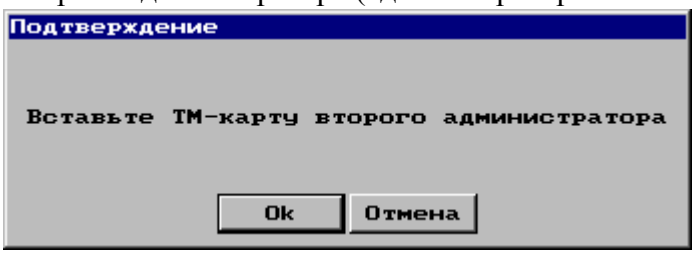

Рисунок 47

4.14.2 При успешной аутентификации администратора ключей на экране монитора отобразится меню в соответствии с рисунком 48.

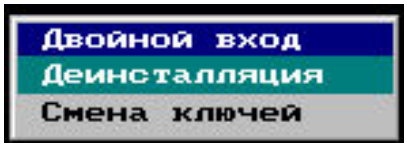

Рисунок 48

4.14.3 При выборе пункта "**Деинсталляция**" и подтверждении выбора на экране отобразится сообщение в соответствии с рисунком 49. При подтверждении запроса процесс деинсталляции будет продолжен. В случае отрицательного ответа произойдет выход в меню администратора безопасности в соответствии с рисунок 35.

При продолжении процесса деинсталляции будут уничтожены служебные области, которые были необходимы для функционирования ПАК "Барьер" на данной ПЭВМ, и произойдет восстановление первоначальной (с учетом текущих изменений) конфигурации ПЭВМ. Затем произойдет передача управления системному загрузчику BIOS ПЭВМ и будет осуществлена загрузка ОС. На этом процесс деинсталляции считается завершенным.

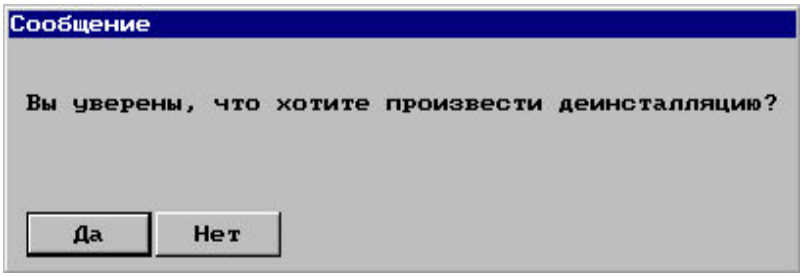

Рисунок 49

4.14.4 Пункт "**Смена ключей**" предназначен для смены служебных ключей системы. При выборе пункта "Смена ключей" на экране монитора появляется сообщение в соответствии с рисунком 56. После подтверждения запроса на смену служебных ключей происходят процессы проверки состояния дисков и генерации ключей дисков, при этом ранее зашифрованные диски расшифровываются. На экране монитора последовательно возникают сообщения в соответствии с рисунками 50 – 52.

ВНИМАНИЕ! если процесс смены ключей будет прерван, дальнейшая работа с ПАК "Барьер" станет невозможна.

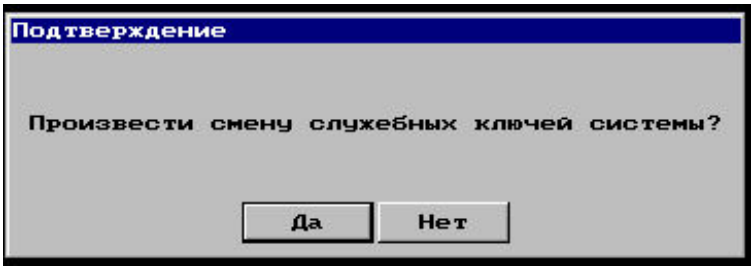

Рисунок 50

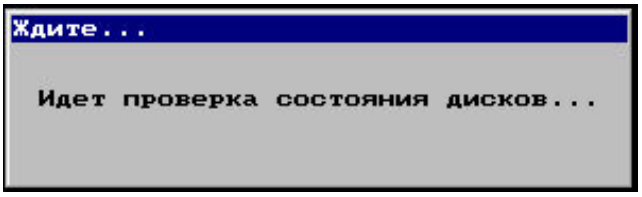

Рисунок 51

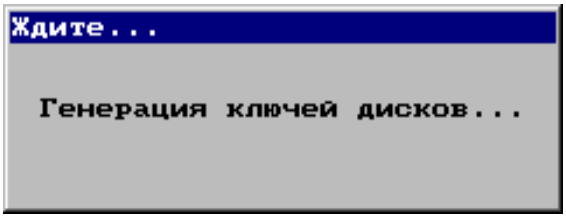

Рисунок 52

После завершения процесса генерации ключей на экране монитора ПЭВМ отобразится сообщение, предлагающее сохранить новый мастер-ключ. Необходимо извлечь карту-ключ администратора ключей из считывателя, установить в него карту-ключ для хранения мастер-ключа и нажать кнопку "Ок". С этого момента начинает осуществляться запись мастер-ключа и на экране монитора отобразится сообщение в соответствии с рисунком 53.

Рисунок 53

Процессы автоматической генерации и записи ключей могут занять несколько минут.

После завершения процесса записи мастер-ключа на экране монитора ПЭВМ отобразится сообщение в соответствии с рисунком 11. Необходимо нажать кнопку "ОК" извлечь из считывателя карту-ключ с сохраненным мастер-ключом, вставить в считыватель карту-ключ администратора ключей и перезагрузить ПЭВМ.

4.15 Восстановление мастер-ключа

4.15.1 В случае уничтожения мастер-ключа при включении ПЭВМ на экране монитора отобразится сообщение в соответствии с рисунком 54.

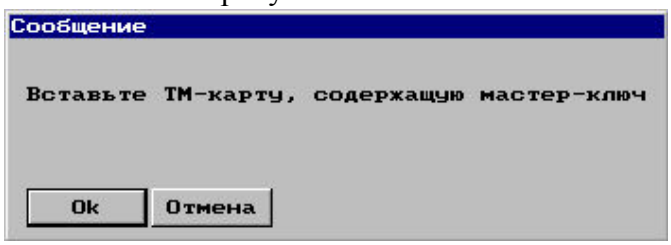

Рисунок 54

4.15.2 Необходимо установить карту-ключ, содержащую мастер-ключ, и нажать кнопку "Ок". При этом произойдет считывание мастер-ключа с носителя и восстановление его во внутренней памяти адаптера ПАК "Барьер".

4.15.3 В случае успешного восстановления мастер-ключа на экране монитора отобразится сообщение в соответствии с рисунком 55.

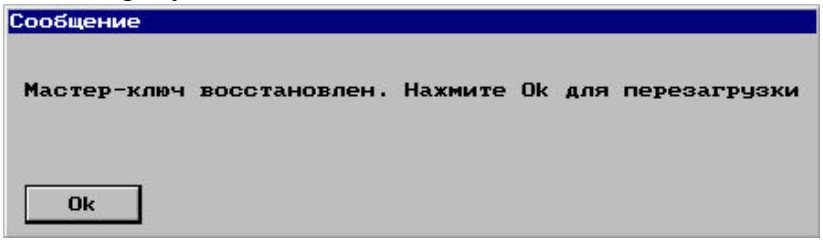

Рисунок 55

4.15.4 После перезагрузки ПЭВМ рабочий процесс выполняется в обычном режиме.

4.15.5 При восстановлении мастер-ключа возможно отображение на экране монитора следующих сообщений:

– "Не удалось восстановить мастер-ключ";
– "Необходимо закрыть корпус".

При отображении на экране монитора ПЭВМ вышеуказанных сообщений необходимо выполнить соответствующие действия, описанные в разделе 14.

5 Техническое обслуживание

5.1 ПАК "Барьер" в процессе эксплуатации является необслуживаемым изделием.

6 Текущий ремонт

6.1 ПАК "Барьер" не требует текущих ремонтов. В случае нарушения работоспособности необходимо обратиться к изготовителю ПАК "Барьер".

7 Хранение

7.1 ПАК "Барьер" не содержит в своем составе веществ и материалов, опасных для жизни и здоровья человека и окружающей среды, и не требует принятия специальных мер предосторожности при хранении.

7.2 ПАК "Барьер" хранят в упаковке изготовителя в складских помещениях.

7.3 Не допускается хранение ПАК "Барьер" совместно с испаряющимися жидкостями, кислотами и другими веществами, которые могут вызвать коррозию.

7.4 Условия хранения ПАК "Барьер" – 1 (Л) по ГОСТ 15150-69:

– температура окружающего воздуха в помещении хранения от плюс 5 до плюс 40 ^{0}С;

– относительная влажность окружающего воздуха – не более 80 % при температуре окружающего воздуха плюс 25 ^{0}С.

Гарантийный срок хранения ПАК "Барьер" – не более 24 мес.

8 Транспортирование

8.1 ПАК "Барьер" не содержит в своем составе веществ и материалов, опасных для жизни и здоровья человека и окружающей среды, и не требует принятия специальных мер предосторожности при транспортировании. Транспортирование ПАК "Барьер" производится в подборной таре любым видом транспорта на любое расстояние в соответствии с правилами перевозок, действующими на каждом виде транспорта.

8.2 Способ крепления упакованных ПАК "Барьер" при транспортировании должен предотвращать их перемещение.

8.3 Условия транспортирования ПАК "Барьер" по ГОСТ 21552-84 Е:

– температура окружающего воздуха от минус 50 до плюс 50 °С;

– относительная влажность окружающего воздуха – не более 98 % при температуре окружающего воздуха плюс 25 °С;

– атмосферное давление от 84 до 107 кПа

8.4 В транспортных средствах, где перевозится ПАК "Барьер", не должно быть паров кислот, щелочей и других химически активных веществ, пары или газы которых могут вызвать коррозию.

9 Утилизация

9.1 ПАК "Барьер" не содержит в своем составе ядовитых и вредных веществ и материалов, опасных для жизни и здоровья человека, а также представляющих опасность для окружающей среды, и не требует специальных мер предосторожности при утилизации.

9.2 Утилизацию ПАК "Барьер" проводят после окончания срока службы и заключения комиссии о нецелесообразности дальнейшей эксплуатации ПАК "Барьер".

9.3 Мероприятия по подготовке и отправке на утилизацию разрабатываются по распоряжению руководителя предприятия в соответствии с порядком утилизации, установленным на предприятии.

9.4 Все мероприятия по подготовке и отправке технических средств ПАК "Барьер" на утилизацию должны производиться при полном отключении этих средств от сети электропитания.

9.5 При подготовке ПАК "Барьер" к утилизации следует соблюдать меры безопасности, предусмотренные для монтажных и механических работ. Для подготовки к утилизации следует провести демонтаж ПАК "Барьер" с целью извлечения узлов с электронными компонентами, которые содержат драгоценные металлы, и извлечения деталей, изготовленных из цветных металлов.

10 Ресурсы, сроки службы и хранения, гарантии изготовителя

10.1 Ресурсы, сроки службы и хранения

Ресурсные показатели долговечности для ПАК "Барьер" не устанавливаются.

Средний срок службы до списания (полный) – не менее 10 лет.

Ресурс изделия до первого ремонта – наработка на отказ не менее 10000 ч в течение срока службы 10 лет, в том числе срок хранения – 2 года в отапливаемых и вентилируемых складах, хранилищах с кондиционированием воздуха в упаковке изготовителя.

Указанные ресурсы, сроки службы и хранения действительны при соблюдении потребителем требований настоящего РЭ.

10.2 Гарантии изготовителя

Изготовитель гарантирует соответствие ПАК "Барьер" требованиям ТУ BY 100037461.004-2005 при соблюдении пользователем правил и условий эксплуатации, хранения, транспортирования и монтажа, установленной документацией на ПАК "Барьер".

Гарантийный срок службы ПАК "Барьер" – **12 мес.** с момента ввода изделия в эксплуатацию в пределах гарантийного срока хранения.

При отсутствии отметки о дате ввода в эксплуатацию гарантийный срок отсчитывается с даты упаковки, указанной в свидетельстве об упаковывании настоящего РЭ.

Гарантийный срок хранения ПАК "Барьер" – **24 мес.** с момента приемки на предприятии-изготовителе.

Гарантийное обслуживание ПАК "Барьер" осуществляется за счет изготовителя по договору между изготовителем или другой организацией, имеющей с изготовителем соответствующее соглашение, и потребителем.

Потребитель лишается права на гарантийное обслуживание при нарушении условий эксплуатации ПАК "Барьер".

11 Свидетельство об упаковывании

Комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа "Барьер"

СЮИК.467458.001 № _____
заводской номер

Упакован(а)_____ЗАО "НТЦ КОНТАКТ"_____
наименование или код изготовителя

согласно требованиям, предусмотренным в действующей технической документации.

_____ _____ _____
должность личная подпись расшифровка подписи

_____
год, месяц, число

12 Свидетельство о приемке

Комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа "Барьер"
ТУ BY 100037461.004-2005

СЮИК.467458.001 № _____
заводской номер

изготовлен(а) и принят(а) в соответствии с обязательными требованиями государственных стандартов, действующей технической документации и признан (а) годным(ой) для эксплуатации.

Начальник ОТК

МП _____ _____
личная подпись расшифровка подписи

_____
год, месяц, число

13 Движение изделия при эксплуатации

13.1 Движение изделия при эксплуатации

Сведения о движении ПАК "Барьер" должны заноситься в таблицу 3.

Таблица 3

Дата установки	Где установлено	Дата снятия	Наработка		Причина снятия	Подпись лица проводившего установку
			с начала эксплуатации	после последнего ремонта		

14 Аварийные ситуации

14.1 При работе на ПЭВМ, защищенной ПАК "Барьер", возможна выдача на экран монитора соответствующих сообщений, приведенных в таблице 4.

Таблица 4 – Перечень сообщений

Текст сообщения	Описание события	Порядок действия
Продолжение инсталляции невозможно	Сообщение выводится после сообщения с указанием ошибки	Устранить ошибку, повторить инсталляцию снова
Для продолжения необходимо закрыть корпус системного блока	Во время инсталляции или при восстановлении мастер-ключа не закрыт корпус системного блока	Закрыть корпус системного блока и повторить операцию
Ошибка записи	1 Произошла ошибка записи мастер-ключа на выбранный носитель. 2 Возможно, неисправен адаптер.	1 Установить другой носитель (выбранного типа) и повторить операцию. 2 Повторить инсталляцию.
Необходимо создать администратора	Попытка завершить инсталляцию без создания учетной записи пользователя со статусом "администратор"	Создать учетную запись пользователя со статусом "администратор" и завершить инсталляцию
Вход разрешен только администратору	Произошло событие, нарушившее установленную политику безопасности	Сообщить о событии администратору безопасности
Неверный пароль	Попытка входа в систему с неверным паролем	Ввести верный пароль и повторить вход
Минимальная длина пароля 8 символов	Введен пароль меньше 8 символов	Ввести пароль длиной больше или равный 8 символам
Такой пароль уже существует	Введен пароль, установленный для другого пользователя	Ввести новый пароль
Подтверждение не совпадает с паролем	Пароль в поле "Подтверждение" не совпадает с паролем в поле "Пароль"	Ввести правильный пароль
Ошибка	Ошибка при получении идентификатора карты-ключа	Сменить карту-ключ в считывателе
Уничтожен мастер-ключ	Уничтожен мастер-ключ в случае вскрытия корпуса системного блока или неисправности адаптера	Закрыть корпус системного блока, восстановить мастер ключ
Не удалось восстановить мастер-ключ	Попытка восстановить мастер-ключ с неверного носителя	Повторить операцию по восстановлению, используя правильный носитель
Продолжение работы невозможно. Доступ в систему запрещен	Выполнен отказ от выполнения процедуры восстановления мастер-ключа	Произвести перезагрузку ПЭВМ и восстановить мастер-ключ
Нарушена целостность IDE устройств	Изменен состав IDE-устройств	Обновить конфигурацию оборудования, разрешить вход всем пользователям
Нарушена целостность PCI устройств	Изменен состав PCI-устройств	Обновить конфигурацию оборудования, разрешить вход всем пользователям

Окончание таблицы 4

Текст сообщения	Описание события	Порядок действия
Ошибка контроллера	Внутренняя ошибка платы адаптера ПАК "Барьер"	Сообщить в сервисный центр
Слишком много файлов	Количество файлов, отмеченных для контроля целостности слишком велико	Удалить из списка наименее значимые файлы
Ошибка поиска	Аппаратная ошибка НЖМД при считывании каталога файлов	Заменить НЖМД, повторить инсталляцию заново
Ошибка сохранения списка	Сбой при записи списка файлов в энергонезависимую память адаптера	Повторить сохранение списка файлов
Ошибка загрузки списка файлов	Сбой при чтении списка файлов из энергонезависимой памяти адаптера	Повторить чтение списка файлов
Ошибка CRC ключа шифрования диска	Сбой при считывании ключа шифрования диска из памяти ПАК "Барьер"	Перезагрузить ПЭВМ и выполнить повторную загрузку ОС
ТМ-карта уже используется	В считыватель установлена карта-ключ, которая уже используется в данной системе ПЭВМ	Установить необходимую карту-ключ
ТМ-карта не вставлена	Из считывателя была изъята карта-ключ администратора, но не была установлена новая карта-ключ пользователя	Установить необходимую карту-ключ
ТМ-карта мастер-ключа	В считыватель установлена карта-ключ, на которой сохранен мастер-ключ данной системы ПЭВМ	Вставить свободную карту-ключ
Неверная ТМ-карта	В считыватель установлена карта-ключ, не соответствующая пользователю, для которого меняется одноразовый пароль	Установить необходимую карту-ключ
Ошибка диска	При записи мастер-ключа на диск или чтении	Повторить запись или чтение
Доступ в систему запрещен	Введен 3 раза неверный пароль. Система блокирована, вход разрешен только администратору безопасности	Перегрузить ПЭВМ и повторить ввод соответствующего пароля
Рассинхронизация времени адаптера и ПЭВМ больше допустимой	Разница во времени адаптера и ПЭВМ больше допустимой	Выполнить синхронизацию времени, разрешить вход всем пользователям

Приложение А

(справочное)

Правила формирования паролей

А.1 Общие требования к паролям пользователей

Порядок ведения (ввода, изменения, удаления/блокирования) паролей должен быть изложен в соответствующих инструкциях организации.

Общие требования к паролям следующие:

– ответственность за своевременное формирование и распределение (выдачу) паролей пользователям возлагается на администратора безопасности;

– идентификатор (имя) и пароль должны выдаваться каждому пользователю администратором безопасности под роспись в "карточке учета паролей";

– конверты с паролями должны быть опечатаны;

– при необходимости может быть заведена резервная копия "карточки учета паролей" каждого пользователя (на случай утраты основной);

– при входе в систему идентификатор и пароль вводятся самим пользователем;

– пароли пользователей должны периодически меняться администратором безопасности в сроки, предусмотренные политикой безопасности организации.

– пароль должен иметь длину не менее восьми символов, в состав которых должны входить буквы латинского алфавита, цифры и специальные знаки (подчеркивание, тильда и др.);

– 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;

– пользователь должен помнить свой пароль; если после длительного перерыва в работе (отпуск, болезнь) пользователь забыл свой пароль, он обязан получить его у администратора безопасности;

– пользователь должен быть предупрежден об ответственности за невыполнение своих обязанностей и за разглашение паролей;

– внеплановая смена (блокирование) личного пароля любого пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.), либо компрометирующих действий должна производиться немедленно после окончания последнего санкционированного сеанса работы данного пользователя. Также необходимо производить внеплановую смену паролей всех пользователей при фактах 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.

А.2 Требования к системе ведения паролей

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

– пароль должен назначаться 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 выявления факта 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.

А.3 Обязанности пользователя при работе с паролем

Пользователь обязан:

– выполнять требования эксплуатационной документации на встроенные средства защиты информации;

– сохранять пароль в тайне и следить за конфиденциальностью ввода пароля с клавиатуры;

– в нештатных ситуациях обращаться за помощью к администратору безопасности.

А.4 Обязанности администратора 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 на ПЭВМ;

– в совершенстве знать используемую систему защиты информации, механизмы аутентификации, владеть процедурами установки и смены паролей в соответствии с политикой безопасности организации;

– следить, чтобы каждый пользователь знал свои права и обязанности при работе на ПЭВМ, владел навыками работы с паролем;

– вести учет 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 ПЭВМ или ее сбоях.

А.5 Методика определения необходимой длины пароля

Выбор необходимой длины пароля требуется для того, чтобы правильно определить период действия (смены) паролей. 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:

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

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

M – период времени непрерывного тестирования ПЭВМ для подбора пароля в месяцах;

P – заданная вероятность подбора пароля;

A – 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 К = 60/5 = 12).

Имеем:

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

или

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

Значит длина пароля, равная восьми символам, достаточна для выполнения заданных условий, а именно – если будет выбран пароль длиной в восемь 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:

$К = 12 \left(\frac{1}{мин} \right)$;

M = 1 (*мес.*);

A = 26 (символов);

z =8 (символов).

Подставив данные значения в формулу (1), получим:

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

или

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

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".

Приложение Б

(справочное)

Перечень принятых сокращений

В настоящем руководстве по эксплуатации приняты следующие сокращения:

ДСЧП – датчик случайной числовой последовательности
НСД – несанкционированный доступ
ОЗУ – оперативное запоминающее устройство
ОС – операционная система
ПАК "Барьер" – комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа "Барьер"
ПЗУ – постоянное запоминающее устройство
ПЛИС – программируемая логическая интегральная схема
ПО – программное обеспечение
ППЗУ – перепрограммируемое постоянное запоминающее устройство
ПЭВМ – персональная электронно-вычислительная машина
РЭ – руководство по эксплуатации

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводи-тельного докум. и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннули-рованных					