ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-036 34 -ЛУ

# Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Win32» (версия 4.0)

# РУКОВОДСТВО ОПЕРАТОРА (ПОЛЬЗОВАТЕЛЯ)

**11443195.4012-036 34**

**Литера $О_1$**

# АННОТАЦИЯ

Руководство предназначено для конкретизации действий операторов (пользователей) при эксплуатации комплекса СЗИ НСД «Аккорд-Win32» v.4.0 (далее ПАК СЗИ НСД «Аккорд», комплекс «Аккорд» или комплекс) (ТУ 4012-036-11443195-2010) и содержит описание способов использования средств защиты комплекса, его интерфейса с пользователем в процессе обработки информации.

Перед эксплуатацией комплекса необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые организационные меры защиты, рекомендуемые в документации.

Применение защитных механизмов комплекса должно дополняться общими мерами технической безопасности, а также физической охраной СВТ и ее средств.

# СОДЕРЖАНИЕ

# 1. Назначение и краткая характеристика комплекса

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» v.4.0 предназначен для применения на ПЭВМ (рабочих станциях ЛВС) типа IBM PC, функционирующих под управлением ОС Windows NT/2000/XP/2003/Vista/2008/7/8/8.1 с целью обеспечения защиты от несанкционированного доступа (НСД) к СВТ и информационным ресурсам АС, обеспечения конфиденциальности информации, обрабатываемой и хранимой в СВТ при многопользовательском режиме эксплуатации.

Комплекс «Аккорд» под управлением операционной системы Windows обеспечивает:

- защиту от несанкционированного доступа к СВТ путем идентификации пользователей по не копируемым уникальным идентификаторам (DS 1992-1996 и ПСКЗИ ШИПКА) и их аутентификации[1] по индивидуальному паролю, вводимым с клавиатуры. При этом обеспечивается защита от раскрытия индивидуального пароля пользователя;
- блокировку загрузки с отчуждаемых носителей (FDD, CD ROM, ZIP Drive и др.) и прерывания контрольных процедур с клавиатуры;
- доверенную загрузку операционной системы (ОС) и защиту от несанкционированных модификаций программ и данных;
- создание и поддержку изолированной программной среды (ИПС), возможность реализации функционально замкнутых информационных систем на базе ПЭВМ;
- контроль целостности системных областей жестких дисков, программ и данных, а также конфигурации технических средств СВТ до загрузки ОС;
- защиту от внедрения разрушающих программных воздействий (РПВ): вирусов, закладок и т.д.;
- разграничение доступа пользователей к ресурсам СВТ в соответствии с уровнем их полномочий;
- управление потоками информации на основе принципов дискреционного и мандатного доступа;
- регистрацию контролируемых событий, т.ч. несанкционированных действий пользователей, в системном журнале, размещенном в энергонезависимой памяти контроллера комплекса. Доступ к журналу обеспечивается только администратору безопасности информации.
- возможность подключения криптографических средств защиты информации.

Для эффективного применения комплекса и поддержания необходимого уровня защищенности СВТ и информационных ресурсов **необходимы**:

---

[1] *Аутентификация - подтверждение подлинности*

- физическая охрана СВТ и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса СЗИ НСД;
- наличие администратора безопасности информации (супервизора) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в СВТ, эксплуатацию и контроль за правильным использованием СВТ с внедренным комплексом «Аккорд», в том числе, учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты комплекса. Более подробно обязанности администратора БИ по применению комплекса изложены в Руководстве администратора (11443195.4012-036 90).
- использование в СВТ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ;
- строгое выполнение обязанностей по обеспечению информационной безопасности каждым оператором (пользователем) СВТ, приведенных в приложении 1 к настоящему Руководству.

Комплекс «Аккорд-Win32» v.4.0 (ТУ 4012-036-11443195-2010) поставляется в программно-аппаратном исполнении в составе:

1) Комплекс СЗИ НСД «Аккорд-АМДЗ» в комплекте[1]:
   - контроллер «Аккорд» -1 шт.;
   - съёмник информации (контактное устройство) - 1 шт;
   - персональный идентификатор – по количеству пользователей СВТ;
2) Специальное ПО разграничения доступа в среде Windows NT/2000/XP/2003/Vista/2008/7/8/8.1 - СПО «Аккорд-Win32» v.4.0, размещаемое на жестком диске СВТ при установке комплекса.
3) Эксплуатационная документация[2].
4) Формуляр.

[1] тип контролера и его модификация, съемника информации, тип и количество персональных идентификаторов пользователей оговариваются при заказе комплекса в соответствии с требованиями Заказчика и указываются в формуляре.

[2] Поставляется на диске совместно с СПО разграничения доступа

# 2. Порядок работы на защищенной СВТ

Процесс работы пользователя на СВТ, защищенном комплексом «Аккорд», можно разделить на 3 этапа:

1) выполнение контрольных процедур;

2) работа пользователя в соответствии с функциональными обязанностями и правами доступа;

3) завершение работы и выход из системы.

## 2.1. Выполнение контрольных процедур[1)]

Контрольные процедуры делятся на обязательные, выполняемые при каждом запуске СВТ и необязательные, выполняемые при выполнении заданных условий.

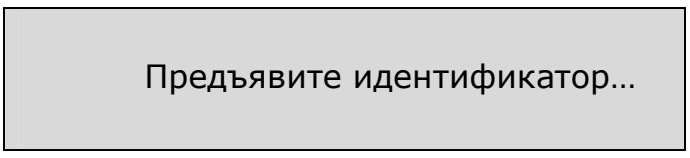
К обязательным процедурам относятся

- процедура идентификации;
- процедура аутентификации;
- проверка целостности аппаратуры СВТ, системной области диска и системных файлов;

К необязательным процедурам относится процедура смены пароля, выполняемая, когда время жизни пароля превысило установленный администратором БИ интервал времени и проверка ограничения на время входа в систему.

### 2.1.1. Процедура идентификации

При загрузке СВТ, защищенного комплексом «Аккорд», управление загрузкой перехватывает контроллер комплекса, загружается ACDOS и после старта драйвера контроллера на экран выводится сообщение на синем фоне:



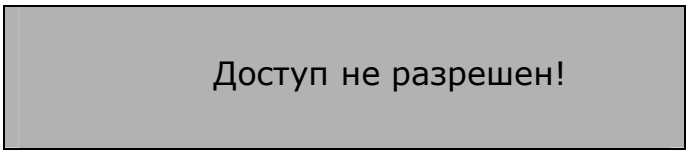

Окно остается на мониторе до момента контакта идентификатора пользователя и контактного устройства съемника информации. В правом нижнем углу выводится отсчет времени, отведенного для предъявления идентификатора пользователя. Если за отведенное время идентификатор не предъявлен, на экран выводится сообщение на красном фоне “Таймаут”. Возобновить процедуру идентификации можно только после перезагрузки СВТ.

---

[1)] Описание процедур в подразделе 2.1 соответствует описанию работы с DOS-контроллерами «Аккорд»

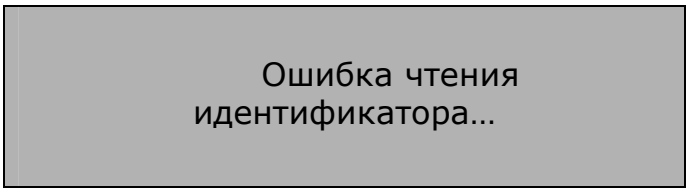
**Примечание:** В том случае, когда в качестве персонального идентификатора используется ПСКЗИ ШИПКА, на запрос идентификатора следует подключать устройство ШИПКА к USB-порту контроллера АМДЗ.

Если идентификатор не зарегистрирован в системе, то на экране появляется сообщение на красном фоне:




При успешном завершении процедуры идентификации происходит выполнение процедуры аутентификации (запрос пароля пользователя).

Если пользователь недостаточно плотно приложил ТМ-идентификатор к контактному устройству, то на экран в редких случаях может выводится сообщение (на красном фоне), сопровождаемое звуковым сигналом:



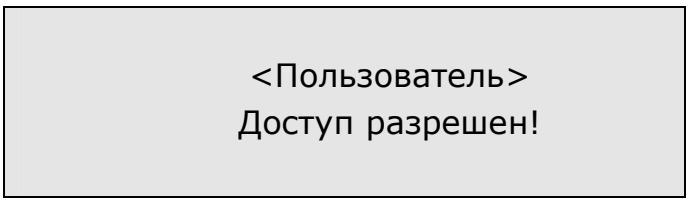

и пользователю предлагается повторить процедуру идентификации.

### 2.1.2. Процедура аутентификации

После идентификации пользователя, при условии, что ему при регистрации был задан пароль для входа в систему, на экран выводится сообщение на синем фоне:

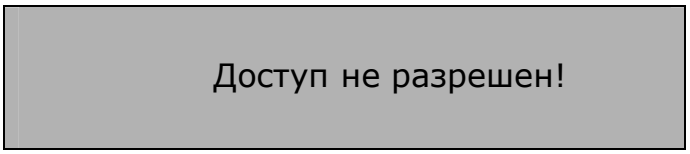

По этой команде необходимо набрать свой личный пароль, при этом символы пароля выводятся на экран в виде звездочек. Время, отведенное для ввода пароля, отображается в правом нижнем углу, так же как при запросе идентификатора.

Если процедура аутентификации успешно завершилась, на экран выводится надпись на зеленом фоне:



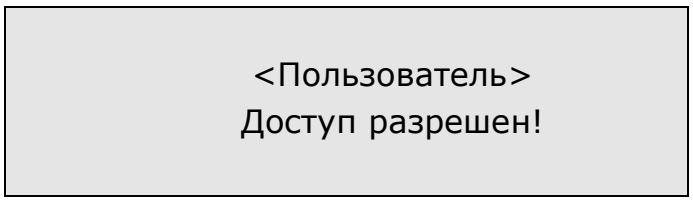
и происходит проверка целостности аппаратуры СВТ, системных файлов ОС, программ и данных, для которых установлен контроль целостности.

При неправильно введенном пароле на экран выводится надпись на красном фоне:




и пользователю предлагается снова пройти процедуры идентификации и аутентификации.

В случае если при регистрации пользователю не был назначен пароль, процедура аутентификации не выполняется, и на экран выводится надпись на зеленом фоне:



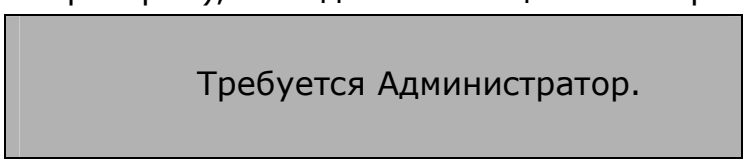

и происходит проверка целостности аппаратуры СВТ, системных файлов ОС, программ и данных, для которых установлен контроль целостности системных файлов с последующей загрузкой ОС.

### 2.1.3. Проверка целостности аппаратуры СВТ, системных областей, системных файлов, программ и данных

Данная процедура осуществляется до загрузки ОС и предназначена для исключения несанкционированных модификаций (случайных или злоумышленных) аппаратной и программной среды СВТ, системных областей и системных файлов ОС, обрабатываемых пользователем данных, если они поставлены на контроль целостности.

При проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным значением, хранящимся в контроллере «Аккорд»™. Эти данные заносятся при регистрации пользователя и могут меняться в процессе эксплуатации СВТ.

В случае если нарушена целостность защищаемых файлов или проводилась несанкционированное изменение конфигурации технических средств СВТ (параметры настройки см. в документе «Программно-аппаратный комплекс средств защиты информации от НСД для ПЭВМ (РС) «Аккорд-АМДЗ». Руководство администратора»), выводится сообщение на красном фоне:

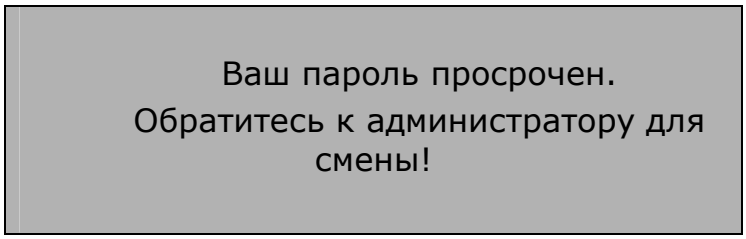


и загрузка ОС не производится. Загрузка будет возможна только для администратора. После идентификации Администратора на незначительное время выводится сообщение на оранжевом фоне:

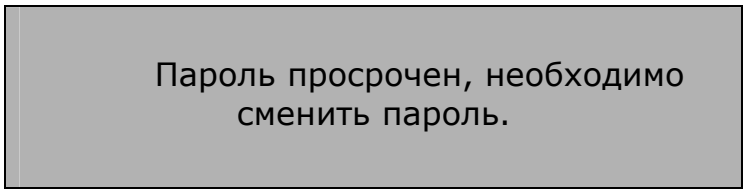

### 2.1.4. Смена пароля

Смена пароля происходит в случае, когда время действия пароля превысило отведенный интервал. Это время устанавливается администратором БИ при регистрации пользователя либо при последующем администрировании системы. По решению администратора БИ пользователю может предоставляться право самостоятельной смены пароля.

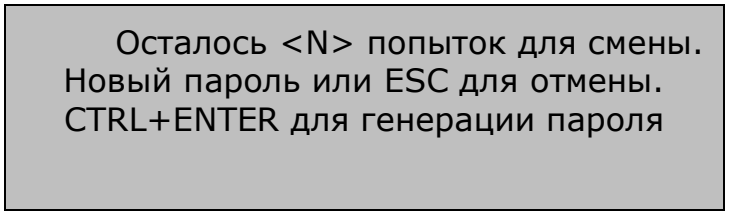
В случае, когда пользователь не имеет такого права, при вводе просроченного пароля на экран выводится сообщение на красном фоне:




Если пользователю дано право самостоятельной смены пароля, то при вводе просроченного пароля на экран выводится сообщение на оранжевом фоне:

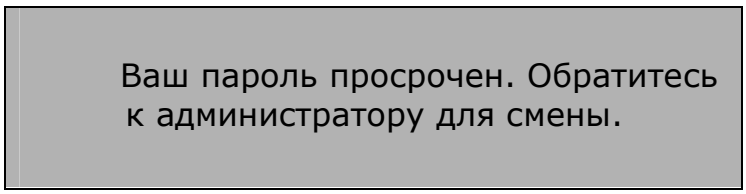



Затем на экран выводится сообщение на синем фоне:




где N – количество попыток для смены пароля (устанавливается администратором БИ).

При нажатии на любую клавишу выводится окно, в котором можно ввести новый пароль, после чего выполняется загрузка. При нажатии клавиши <Esc> смена пароля не выполняется, но при этом число попыток для смены пароля уменьшается на единицу. Если число попыток исчерпано, то выводится сообщение на красном фоне:

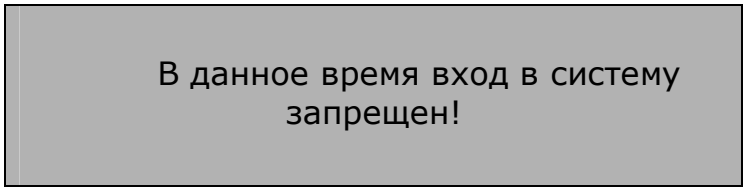



Пользователь может сменить пароль на новый во время любой из попыток, но при этом должен помнить: когда число попыток станет равным нулю, то загрузка системы произойдет только после вмешательства администратора БИ с использованием его идентификатора.

Комплекс «Аккорд» обеспечивает синхронизацию паролей при изменении, т. е. пароль, смененный в момент работы аппаратной части комплекса, автоматически (если в настройках комплекса выбрана опция «Синхронизировать с базой АМДЗ») сменится и в программной надстройке. Но совсем другой случай, если результаты процедуры идентификации/аутентификации пользователя используются для логина на контроллер домена. В этом случае менять пароль нужно только после начала сеанса пользователя. Необходимо на клавиатуре нажать комбинацию клавиш Ctrl-Alt-Del и в открывшемся окне выбрать команду «Смена пароля». После ввода нового пароля он изменится и на домене, и в программной части комплекса «Аккорд», и в базе пользователей аппаратной части СЗИ. Для этого необходимо разрешить пользователю менять пароль и в настройках комплекса выбрать опции «Синхронизация с базой АМДЗ» и «Синхронизация с базой пользователей NT».

### 2.1.5. Проверка ограничения на время входа в систему

Администратор может установить временной интервал (по дням недели с дискретностью 0.5 часа), в который загрузка данного СВТ данным пользователем запрещена. Если для пользователя установлены такие ограничения, то при попытке загрузки в неположенное время после процедуры идентификации/аутентификации и контроля целостности выводится сообщение на красном фоне:




и загрузка ОС не производится.

## 2.2. Работа пользователя в соответствии с функциональными обязанностями

После выполнения контрольных процедур выполняется загрузка операционной системы, и пользователь может приступить к работе, определяемой его функциональными обязанностями и правами доступа к ресурсам СВТ.

При регистрации пользователя для него создается функционально изолированная программная среда, которая позволяет контролировать права доступа пользователя к объектам доступа.

### 2.2.1. Проверка полномочий по доступу

Выполняется при запуске пользователем какой-либо программы или при попытке получить доступ к какому-либо ресурсу. Средствами комплекса «Аккорд» выполняется проверка полномочий пользователя, которая заключается в том, что в списке прав доступа пользователя осуществляется поиск описания данного ресурса.

Если в списке прав доступа пользователя разрешена работа с данной программой или файлом, то пользователь может легально работать в соответствии со своими функциональными обязанностями.

Если в списке прав доступа пользователя не разрешена работа с данной программой или файлом (или ограничен набор функций, которые может выполнить пользователь с данным ресурсом), то выводится стандартное сообщение операционной системы, например: «Файл не найден», «Невозможно удалить файл» и т. д.

### 2.2.2. Работа с хранителем экрана

**Принудительное гашение экрана**

В комплексе «Аккорд» процедура гашения экрана используется для временной блокировки компьютера по истечении установленной паузы в работе пользователя или с помощью «горячих» клавиш. Комбинацией клавиш <Ctrl><F12> пользователь может самостоятельно включить режим *«Screen-saver»* при кратковременном перерыве в работе. После включения хранителя экрана клавиатура и мышь блокируются.

**ВНИМАНИЕ!** В терминальном режиме, чтобы включить режим *«Screen-saver»* необходимо использовать комбинацию клавиш <Win><L>. После включения хранителя экрана клавиатура и мышь блокируются, на экране появляется сообщение «Предъявите идентификатор».

**Возобновление работы.**

Для возобновления работы на СВТ пользователь должен предъявить свой идентификатор и после того как система опознает его идентификатор как подлинный, режим *«Screen-saver»* отключается и можно продолжить работу.

## 2.3. Завершение работы и выход из системы

Завершение работы прикладных программ происходит в порядке, установленном для конкретного прикладного программного обеспечения, описанном в соответствующих руководствах. Никаких специфических окон или сообщений «Аккорд-Win32» при этом не выводит. Перед завершением работы ОС выводится окно с заголовком «Комплекс Аккорд» и остается на экране, пока монитор разграничения доступа не завершит корректно свою работу.

## 3. Сообщение программных средств комплекса и порядок действий пользователя по ним

При работе на СВТ, оснащенном комплексом «Аккорд», могут возникать ситуации, при появлении которых выдаются различные сообщения. Текст сообщений, причины их появления и методы устранения проблем приведены в таблице 1.

**Таблица 1 – Сообщения программных средств комплекса и методы их устранения.**

| Сообщение на экране | Причины появления сообщения | Порядок действий |
|---|---|---|
| «Ошибка чтения ТМ…» (на красном фоне) | ТМ-идентификатор был неправильно приложен к съемнику информации. | Снова приложить ТМ-идентификатор к съемнику информации после появления соответствующего запроса. |
| «В данное время вход в систему запрещен» | Для данного пользователя не разрешен вход в систему в данное время | Вызвать администратора БИ и уточнить разрешенное время работы |
| «Ваш пароль просрочен. Обратитесь к администратору для смены» (на красном фоне) | Окончилось время жизни пароля. Закончились все попытки смены пароля. | Вызвать администратора БИ. Изменить параметры пароля. |
| «Доступ не разрешен!» (на красном фоне) | Не зарегистрированный идентификатор. Не правильно введен пароль. В данное время работают временные ограничения. | Обратиться к администратору БИ для регистрации. Повторить процедуры идентификации / аутентификации. |
| «Требуется Администратор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне) | Несовпадение контрольных и текущих параметров аппаратной и программной частей системы. | Вызвать администратора БИ. Выявить и устранить причины изменения параметров. |
| «Проверить целостность объектов пользователя? (Y/N)» | Это сообщение означает, что администратор БИ установил пользователю опцию проверки целостности файлов, в соответствии с правилами настройки. | Пользователь должен осуществить выбор в соответствии со своими предпочтениями. (Рекомендуется периодически проводить проверку) |

| | | |
|---|---|---|
| «Обновить контрольные суммы объектов пользователя? (Y/N)» | Это сообщение появляется, если пользователю установлен режим пересчета контрольных сумм файлов после завершения задачи пользователя с подтверждением, в соответствии с правилами настройки. | Пользователь может записать новое значение КС. Для этого необходимо выбрать [Y] и после появления сообщения:<br>«Предъявите идентификатор, или ESC для отмены» нужно предъявить идентификатор. |
| «Не прошел логин в базу АМДЗ!» | Несоответствие версий ПО в АМДЗ и Windows. | Обновить ПО. |
| «Ошибка проверки объектов!» | Ошибка возникает, если объект, включенный в список контроля, недоступен. | Проверить правильность списка объектов контроля. |
| «Такую комбинацию символов недопустимо использовать в качестве пароля» | Это сообщение появляется в случае, если пользователь вводит комбинацию символов, которую легко подобрать (например, qwerty). | Ввести более сложную комбинацию символов. |
| «Отсутствует разрешение на смену пароля» | Это сообщение появляется, если у пользователя нет прав на смену пароля. | Попросить администратора дать пользователю права на самостоятельную смену пароля. |

## Приложение 1. Обязанности должностных лиц по обеспечению безопасности информации при выполнении работ на СВТ

### ОБЩИЕ ТРЕБОВАНИЯ

Все должностные лица (сотрудники) организации должны быть ознакомлены с этой инструкцией и своими обязанностями по обеспечению безопасности информации при выполнении ими работ на СВТ.

Персонал, допущенный к автоматизированной обработке конфиденциальной информации, обязан строго соблюдать установленные правила работы на автоматизированных рабочих местах и несет персональную ответственность за обеспечение безопасности информации при работе на технических средствах автоматизированной системы.

Установление личной ответственности сотрудников за поддержание уровня защищенности СВТ при обработке сведений, подлежащих защите по действующему законодательству, происходит путем:

- ознакомления с перечнем защищаемых сведений, организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- определения уровня полномочий в соответствии с его должностными обязанностями;
- получения от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

Мера ответственности персонала за выполнение действий, нарушающих политику безопасности, определяется нанесенным ущербом, наличием злого умысла и некоторыми субъективными факторами по усмотрению руководства учреждения (дисциплинарная, административная или уголовная).

Любое нарушение порядка и правил работы персоналом АС должно тщательно расследоваться, а к виновным должны применяться необходимые меры воздействия.

Все компоненты программного и аппаратного обеспечения системы должны использоваться персоналом ТОЛЬКО в служебных целях. Использование их в других целях ЗАПРЕЩАЕТСЯ.

Запрещается прием посетителей в помещениях, когда в них осуществляется обработка конфиденциальной информации на СВТ.

Пользователям ЗАПРЕЩАЕТСЯ самовольно изменять конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих мест и планом защиты. Исключением являются только те случаи, когда пользователь имеет права администратора (супервизора).

Все изменения конфигурации технических и программных средств осуществляются только на основании решения руководства организации

персоналом из числа инженеров, системных и прикладных программистов с участием администратора безопасности АС.

О случаях обнаружения непредусмотренных отводов кабелей и проводов, изменений алгоритмов функционирования технических и программных средств СВТ, нарушениях нормальной работы средств защиты, которые свидетельствуют о возможных попытках или фактах НСД к информации, необходимо немедленно ставить в известность администратора безопасности.

Любые изменения состава и конфигурации технических средств и программного обеспечения должны быть предварительно проанализированы на предмет их соответствия политике безопасности. Все добавляемые компоненты должны быть проверены на работоспособность, отсутствие вирусов и специальных вложений, а также отсутствие реализации опасных функций.

После изменения конфигурации СВТ в обязательном порядке должен производиться пересмотр существующих инструкций пользователей по обеспечению безопасности.

Категорически запрещается записывать и хранить конфиденциальную информацию на неучтенных гибких магнитных дисках, а также использовать гибкие магнитные диски с выявленными неисправностями.

## ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

В обязанности пользователей входит своевременный и точный ввод данных в систему и активизация процесса их обработки. Пользователи обладают правами доступа к системе и имеют возможность вводить и корректировать необходимую информацию. Они несут ответственность за содержание вводимой ими информации.

Пользователь (ответственный исполнитель работ) несет ответственность за сохранность и правильное использование получаемых в ходе выполнения работ машинных носителей и машинных документов с конфиденциальной информацией.

Степень конфиденциальности гибких магнитных дисков и машинных документов, получаемых в ходе автоматизированной обработки информации с помощью СВТ, определяется должностным лицом, выдавшим задание на автоматизированную обработку информации.

По окончании рабочего дня полученные во временное пользование гибкие магнитные диски (при необходимости и идентификаторы) должны быть возвращены в_____ (название подразделения, ответственного за хранение ГМД и идентификаторов).

Необходимо производить стирание с магнитных носителей конфиденциальной информации, не предназначенной для дальнейшего использования. Стирание информации производится допущенным к ее автоматизированной обработке должностным лицом под контролем администратора безопасности с отметкой в журнале учета стирания информации с магнитных машинных носителей.

После окончания обработки конфиденциальной информации и изъятия гибкого магнитного диска из дисковода необходимо выключить электропитание СВТ.

Ответственный за СВТ (АРМ) обязан проверять целостность и соответствие печатей в начале и по окончании рабочего дня.

Пользователям ЗАПРЕЩАЕТСЯ самовольно изменять конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих мест и планом защиты.