ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
ОКБ АПР систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
37222406.26.20.40.140.080 34-ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа

«АККОРД-Х»

РУКОВОДСТВО ОПЕРАТОРА (ПОЛЬЗОВАТЕЛЯ)

37222406.26.20.40.140.080 34

Москва
2023

37222406.26.20.40.140.080 34

АННОТАЦИЯ

Настоящий документ является руководством оператора программно-аппаратного комплекса защиты информации от несанкционированного доступа «Аккорд-Х» (ТУ 26.20.40.140-080-37222406-2019), предназначен для конкретизации действий операторов (пользователей) при эксплуатации ПАК СЗИ НСД «Аккорд-Х» 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.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О КОМПЛЕКСЕ

1.1 Состав ПАК «Аккорд-X»

ПАК СЗИ НСД «Аккорд-X» (далее - ПАК «Аккорд-X», «Аккорд-X», комплекс «Аккорд-X», Комплекс) представляет собой комплекс программных и аппаратных средств, который предназначен для применения в СВТ типа IBM PC (автономных ПК, рабочих станциях ЛВС, терминальных серверах), функционирующих под управлением ОС семейства Linux (список поддерживаемых ОС см. в Формуляре на комплекс «Аккорд-X» (37222406.26.20.40.140.080 ФО)) с целью обеспечения защиты от несанкционированного доступа к информации при многопользовательском режиме эксплуатации.

ПАК «Аккорд-X» состоит из аппаратных и программных средств.

1.2 Аппаратные средства

Аппаратные средства ПАК «Аккорд-X» включают в себя:

- ***контроллер АМДЗ***, входящий в состав ПАК СЗИ НСД «Аккорд-АМДЗ» (ТУ 4012-038-11443195-2011, ТУ 26.20.40.140-079-37222406-2019, ТУ 4012-054-11443195-2013) - представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы СВТ (PC). Контроллер является универсальным, не требует замены при смене используемого типа операционной системы (ОС). В составе СЗИ НСД «Аккорд-АМДЗ» могут применяться специализированные контроллеры, имеющие шинный интерфейс PCI (5 В), PCI-X (3,3 В), PCI-Express (PCI-E), miniPCI, miniPCI-E, M.2;
- ***съемник информации с контактным устройством***, обеспечивающий интерфейс между контроллером Комплекса и персональным идентификатором пользователя. Съемник информации может быть:
  - внешним - соединительный провод находится вне корпуса СВТ (PC) и подключение осуществляется к задней планке контроллера (или к соответствующим портам СВТ);
  - внутренним - соединительный провод находится внутри корпуса СВТ (PC), подключение осуществляется с помощью разъема, находящегося на плате контроллера.

  Контактное устройство внешних съемников крепится в удобном для пользователя месте (на корпусе СВТ (PC), мониторе, рабочем столе и т.д.) при помощи клейкой основы. Крепление контактного устройства внутреннего съемника осуществляется обычно в отверстии, высверливаемом на резервной заглушке дисковода передней панели СВТ (PC), с помощью гайки либо пружинной или резиновой шайбы;

- ***персональный идентификатор пользователя–*** микропроцессорное устройство DS 199x («Touch memory»), ПАК «Персональный идентификатор ШИПКА», Рутокен Lite, Рутокен эцп 2.0, Рутокен 2151, JaCarta, ESMART Token. Каждый идентификатор обладает уникальным номером, который формируется технологически. Объем памяти, доступной для записи и чтения, зависит от типа идентификатора.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговариваются при поставке комплекса и указываются в документе «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Х». Формуляр» (37222406.26.20.40.140.080 ФО).

1.3 Программные средства

Специальное программное обеспечение «Аккорд-Х» включает в себя:

- ядро защиты – программы, реализующие защитные функции Комплекса;
- программы управления защитными функциями Комплекса (настройки Комплекса в соответствии с ПРД).

Более подробное описание компонентов СПО «Аккорд-Х» приведено в «Руководстве администратора» (37222406.26.20.40.140.080 90).

1.4 Назначение Комплекса

ПАК «Аккорд-Х» предназначен для обеспечения защиты от несанкционированного доступа к информации, обрабатываемой и хранимой в СВТ и АС, по требованиям Системы сертификации средств защиты информации № РОСС RU.0001.01.БИ00[1].

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД на основе:

- применения персональных идентификаторов пользователей;
- применения парольного механизма;
- блокировки загрузки операционной системы со съемных носителей информации;
- контроля целостности технических средств и программных средств и компонентов (файлов общего, прикладного ПО и данных) СВТ (АС);
- обеспечения режима доверенной загрузки установленных в СВТ (АС) операционных систем, использующих любую из файловых систем, поддерживаемых ПАК «Аккорд-АМДЗ»;

[1] *Данные об уровнях защищенности, обеспечиваемых Комплексом, приведены в ТУ 26.20.40.140-079-37222406-2019*

- реализации механизма разграничения доступа к ресурсам ПЭВМ (АС), в том числе к внешним устройствам, в соответствии с ПРД, установленными администратором безопасности информации (АБИ), атрибутами доступа и уровнем доступа пользователя;
- реализации дискреционного механизма и механизма разграничения доступа на основе иерархических меток и обеспечения управления потоками информации, исключая возможность ее несанкционированного переноса из объектов с меньшим уровнем конфиденциальности в объекты с большим уровнем;
- контроля целостности критичных с точки зрения информационной безопасности программ и данных (дисциплины защиты от несанкционированных модификаций). В программной части СЗИ НСД возможна проверка целостности программ и данных по индивидуальному списку для отдельного пользователя, или группы пользователей. Подсистема контроля целостности предусматривает как статический список (проверка выполняется однократно в начале сеанса), так и динамический список, проверка по которому выполняется перед каждой загрузкой контролируемого файла в оперативную память;
- создания изолированной программной среды, исключающей внедрение в систему вредоносных или неразрешенных АБИ программ;
- очистки оперативной памяти и памяти на внешних носителях;
- контроля печати, который позволяет контролировать процессы, документы, принтеры и автоматически маркировать распечатываемые листы специальными пометками, грифами и т.д.;
- управления процедурами ввода/вывода на отчуждаемые носители информации;
- механизма регистрации действий пользователей в системном журнале, доступ к которому предоставляется только АБИ.

1.5 Технические условия применения Комплекса

Для установки комплекса СЗИ НСД «Аккорд-X» требуется следующий минимальный состав технических и программных средств:

- IBM PC AT с центральным процессором архитектуры x86 (IA-32) или x86-64 (AMD64), с объемом динамической оперативной памяти (RAM) не менее 128 Мб, при наличии свободного разъема на материнской плате ПЭВМ, соответствующего типу специализированного контроллера АМДЗ;
- установленная на СВТ (PC) операционная система семейства Linux (список поддерживаемых ОС см. в Формуляре на комплекс «Аккорд-X» (37222406.26.20.40.140.080 ФО)).

В Н И М А Н И Е !

До начала установки комплекса «Аккорд-X» необходимо убедиться, что система входит в список поддерживаемых ОС.

При применении Комплекса следует помнить, что количество пользователей, регистрируемых на одной СВТ (РС), ограничено объемом энергонезависимой памяти контроллеров «Аккорд-АМДЗ» (подробнее см. документацию на «Аккорд-АМДЗ»).

Аппаратные средства, используемые в составе Комплекса, проверены на совместимость практически со всем доступным разработчику программно-аппаратным обеспечением СВТ (РС) как зарубежного, так и отечественного производства. Совместимость обеспечивается правильной установкой и настройкой Комплекса.

1.6 Организационные меры, необходимые для применения Комплекса

Для эффективного применения Комплекса и поддержания необходимого уровня защищенности СВТ (РС) и информационных ресурсов АС **необходимо**:

- наличие администратора безопасности информации (супервизора; далее по тексту – Администратор БИ) – 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(РС), эксплуатацию и контроль правильности использования СВТ(РС) с внедренным комплексом «Аккорд», в том числе, учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты Комплекса;
- разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета идентификаторов и отчуждаемых носителей пользователей и др.). Все разработанные учетные и объектовые документы должны быть согласованы, утверждены у руководства и доведены до сотрудников (пользователей). Это необходимо для того, чтобы План защиты организации (предприятия, фирмы и т.д.) и действия СБИ (администратора БИ) получили юридическую основу;
- физическая охрана СВТ (АС) и его ресурсов, в том числе проведение мероприятий по недопущению изъятия контроллера Комплекса;
- использование в СВТ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в Государственной системе защиты информации (ГСЗИ);
- периодическое тестирование средств защиты Комплекса.

Прием в эксплуатацию ПАК СЗИ «Аккорд» оформляется актом в установленном порядке, в формуляре на комплекс Администратором БИ делается соответствующая отметка.

2 ПОРЯДОК РАБОТЫ НА ЗАЩИЩЕННОМ СВТ

Процесс работы пользователя на СВТ, защищенном комплексом «Аккорд-Х», 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.

ВНИМАНИЕ!

Работа в ОС Linux с установленным комплексом «Аккорд-Х» отличается (от работы в ОС без комплекса «Аккорд-Х») только другой процедурой идентификации/аутентификации и возможными запретами на получение доступа к какому-либо объекту или файлу.

2.1 Выполнение контрольных процедур

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, программ и данных.

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

2.1.1 Процедура идентификации

В комплексе Аккорд-Х применяется двухуровневая идентификация (и аутентификация) пользователей - сначала средствами комплекса Аккорд-АМДЗ, затем средствами самого комплекса Аккорд-Х.

При загрузке СВТ, защищенного комплексом «Аккорд-Х», сразу после штатного BIOS управление перехватывает контроллер Аккорд-АМДЗ. Контроллер проводит необходимые контрольные процедуры, в том числе и идентификацию/аутентификацию пользователя. Эта процедура подробно описана в эксплуатационной документации на Аккорд-АМДЗ.

В случае успешного выполнения контрольных процедур Аккорд-АМДЗ происходит дальнейшая загрузка ОС. При этом на раннем этапе загружается

СПО комплекса Аккорд-X, и на экран выводится соответствующая информация (рисунок 1) (в случае какой-либо ошибки возникает паника ядра с указанием причины – превышен таймер ожидания БД, неправильная лицензия и т.п. – и дальнейшая загрузка ОС не осуществляется). После этого активируются и вступают в действие механизмы защиты, которые включены в данные о конфигурации модуля разграничения доступа (их может изменить Администратор БИ в ходе работы ОС с использованием утилиты acx-admin). Необходимо отметить, что для пользователя все указанные действия после Аккорд-АМДЗ могут быть невидимы - защитные механизмы не оказывают воздействия на быстродействие ОС, а экран с информацией о ходе начальной загрузки (рисунок 1) в зависимости от быстродействия СВТ может сменяться достаточно быстро.

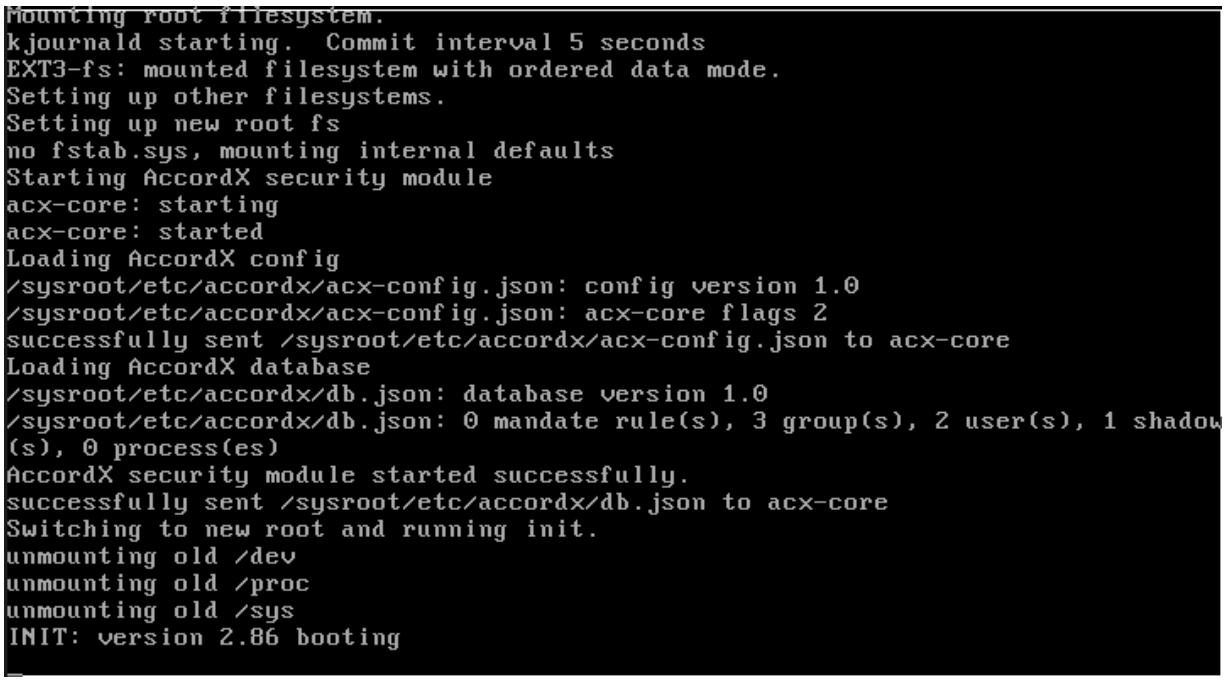

Рисунок 1 – Загрузка модуля разграничения доступа «Аккорд-X»

На заключительном этапе загрузки ОС выводится окно приветствия (стандартное окно входа в ОС, внешний вид отличается в различных дистрибутивах) и требование предъявить идентификатор (рисунок 2).

Рисунок 2 – Запрос идентификатора

2.1.2 Процедура аутентификации

После предъявления идентификатора в появившемся поле «Введите пароль» следует ввести соответствующий пароль пользователя, установленный для него в «Аккорд-X» (рисунок 3).

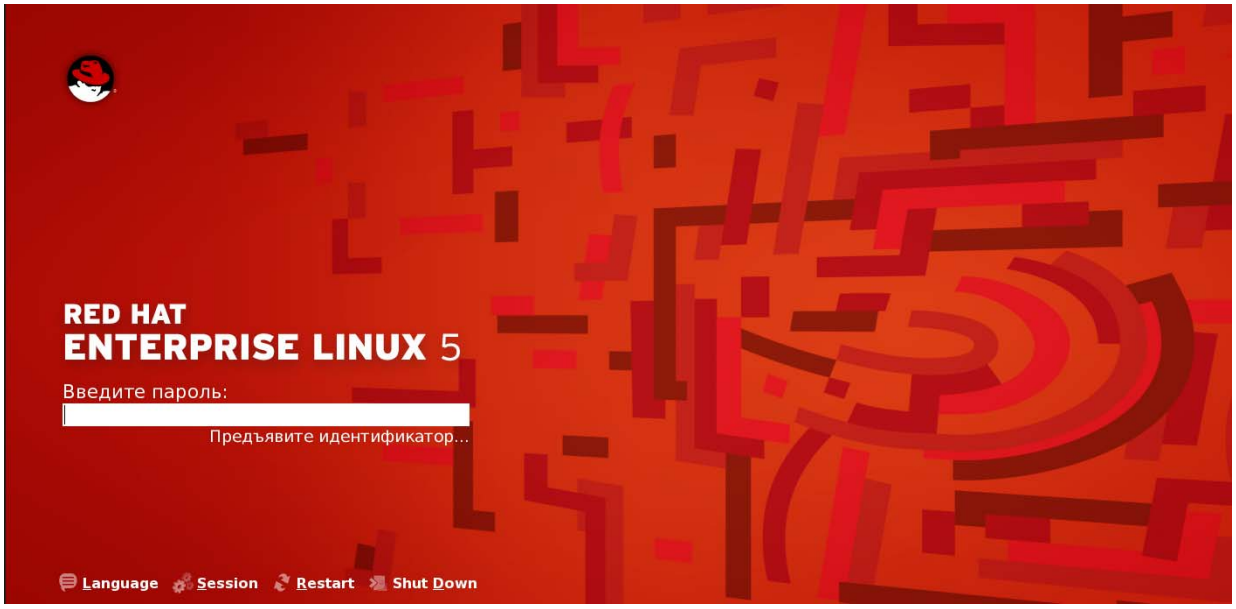

Рисунок 3 – Запрос пароля

В случае наличия пары идентификатор/пароль для пользователя в комплексе «Аккорд-X» процесс идентификации и аутентификации завершается успешно, при этом осуществляется стандартный вход в ОС.

Сразу после выполнения процедуры идентификации/аутентификации пользователя начинают работать соответствующие правила разграничения

доступа, которые ранее были заданы Администратором БИ конкретно для данного пользователя.

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.

Если нарушена целостность защищаемых файлов или проводилось несанкционированное изменение конфигурации технических средств СВТ[2], на экран выводится соответствующее сообщение, и дальнейшая загрузка ОС не производится. Загрузка будет возможна только для администратора.

В ходе загрузки ОС дополнительно может проводиться статический контроль целостности данных, поставленных на контроль Администратором БИ в комплексе «Аккорд-Х». Также во время обычной работы пользователя может выполняться динамический контроль целостности открываемых на выполнение файловых объектов. Все эти операции могут быть незаметными для пользователя (заметить их можно только по вторичным признакам - ошибка при входе в ОС, невозможность запуска приложения и т.д.). В случае возникновения каких-либо проблем необходимо обратиться к Администратору БИ (или см. «Руководство администратора» на Комплекс).

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 о необходимости обратиться к администратору.

Если пользователю дано право самостоятельной смены пароля, то при вводе просроченного пароля на экран выводится сообщение о необходимости сменить пароль. 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

---

[2] Параметры настройки см. в документе «Программно-аппаратный комплекс средств защиты информации от НСД для ПЭВМ (РС) «Аккорд-АМДЗ. Руководство администратора»

для смены пароля уменьшается на единицу. Если число попыток исчерпано, то выводится сообщение о необходимости обратиться к администратору.

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.

2.1.5 Проверка ограничения времени 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 соответствующее сообщение, 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 замкнутая 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.

2.3 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-Х» при этом не выводит.

3 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

В случае необходимости консультации АО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам:

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 762-17-72

или по адресам электронной почты: support@okbsapr.ru, help@okbsapr.ru.

Наш адрес в Интернете: http://www.okbsapr.ru/

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.

В случае выявления сбоев и ошибок в процессе эксплуатации изделия пользователь должен незамедлительно прекратить его использование и сообщить об этом ответственному лицу - администратору служба безопасности информации (СБИ) или администратор безопасности информации (АБИ).