ВЫПОЛНЕНИЕ МЕР
31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ КОМПЛЕКСА КОМПЛЕКСА СЗИ ОТ НСД «ИНАФ»

ОКБ САПР
2021

1 Общие положения

В настоящем документе рассматривается выполнение мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения комплекса СЗИ НСД «ИНАФ».

ПАК СЗИ НСД «ИНАФ» (ПАК СЗИ НСД «ИНАФ», «ИНАФ», СЗИ НСД «ИНАФ» либо комплекс) обеспечивает защиту устройств и информационных ресурсов от НСД, идентификацию, аутентификацию пользователей, регистрацию их действий, контроль целостности файлов и областей жестких дисков при многопользовательском режиме их работы.

Комплекс «ИНАФ» используется на ПЭВМ с платформой HP Proliant BL460C G9, HP BL460 G8 Linux-ИНАФ, Lenovo x240 Compute Node и с установленной любой операционной системой, поддерживающей файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, QNX6, MINIX, Ext4, ReiserFS.

Применение комплекса «ИНАФ» возможно только при подключении к внутреннему разъему USB в ПЭВМ, при условии, что ПЭВМ имеет BIOS, сертифицированный на соответствие требованиям безопасности информации ФСТЭК России или ФСБ России.

ПАК СЗИ НСД «ИНАФ» состоит из:

– специализированного контроллера, который представляет собой среду функционирования для функционального программного обеспечения;
– функционального программного обеспечения, которое является ядром защиты комплекса, реализует функциональные требования безопасности комплекса и исполняется в резидентной операционной среде, предустановленной на специализированный контроллер.

2 Выполнение базового набора мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения СЗИ от НСД «ИНАФ»

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения комплекса ИНАФ» (ТУ 4012-046-11443195-2015).

Выражение «все» в ячейках столбца «Классы защищенности автоматизированной системы управления» означает, что рассматриваемая мера должна быть реализована в автоматизированной системе управления с любым классом защищенности.

Таблица 1 – Выполнение базового набора мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СЗИ от НСД «ИНАФ»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			
1	ИАФ.0	Разработка политики идентификации и аутентификации	+ все	В комплексе разработана политика идентификации и аутентификации.	
2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+ все	Функция идентификации и аутентификации обеспечивает идентификацию и аутентификацию пользователя с помощью специализированного контроллера «Инаф» и пароля пользователя временного действия длиной от 0 до 12 буквенно-цифровых символов при: – входе в систему; – допуске к средствам настройки и администрирования комплекса.	1. п.п. 3.5, 3.6 документа «ИНАФ. Руководство администратора»; 2. п.п. 4.1.1, 4.1.2 документа «ИНАФ. Руководство пользователя».
3	ИАФ.2	Идентификация и аутентификация устройств	+ все	В ИНАФ осуществляется идентификация стационарных устройств СВТ, при процедуре контроля целостности конфигурации технических средств СВТ.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
4	ИАФ.3	Управление идентификаторами	+ все	Управление идентификаторами учетных записей производится в административном режиме в разделе «Пользователи». Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных идентификаторов.	1. п.п. 3.6.4, 3.6.5 документа «ИНАФ. Руководство администратора».
5	ИАФ.4	Управление средствами аутентификации	+ все	Управление паролями и аппаратными идентификаторами учетных записей пользователей производится в административном режиме ИНАФ в разделе «Пользователи»	1. п.п. 3.6.4, 3.6.5 документа «ИНАФ. Руководство администратора».
6	ИАФ.5	Идентификация и аутентификация внешних пользователей	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
7	ИАФ.7	Защита аутентификационной информации при передаче	+ все	Функция аутентификации обеспечивает исключение отображения для пользователя действительного значения аутентификационной информации за счет отображения вводимых символов аутентификационной информации условными знаками.	1. п.п. 4.1.2 документа «ИНАФ. Руководство пользователя».
		Управление доступом (УПД)			
8	УПД.0	Разработка политики управления доступом	+ все	В комплексе разработана политика управления доступом.	
9	УПД.1	Управление учетными записями пользователей	+ все	Управление идентификаторами учетных записей производится в административном режиме в разделе «Пользователи». Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных идентификаторов.	1. п.п. 3.7, 3.8, 3.9 документа «ИНАФ. Руководство администратора».
10	УПД.2	Реализация политик управления доступом	+ все	Ролевой метод. Реализован в виде групп пользователей (Пользователи и Администраторы).	1. п.п. 3.6.1 документа «ИНАФ. Руководство администратора».
11	УПД.3	Доверенная загрузка	+ начиная со 2 класса защищенности автоматизированной системы	Комплекс обеспечивает исключение несанкционированного доступа к программным и техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.	1. п.п. 1.1, 3.13 документа «ИНАФ. Руководство администратора».
12	УПД.4	Разделение полномочий (ролей) пользователей	+ все	В памяти контроллера СЗИ от НСД «ИНАФ» хранятся имена пользователей и их полномочия. После прохождения процедуры И/А пользователей, встроенное ПО контроллера определяет дальнейший режим загрузки по результатам данной процедуры. Администрирование «ИНАФ» может проводить только пользователь, зарегистрированный группе «Администраторы» и имеющий абсолютные полномочия (супервизора). Если пользователь принадлежит к группе	1. п.п. 3.6 документа «ИНАФ. Руководство администратора».
13	УПД.5	Назначение минимально необходимых прав и привилегий	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
				«Администраторы», то следующим шагом при загрузке будет отображено меню, которое определяет возможность администрирования «ИНАФ» (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части ПЭВМ, просмотр системного журнала). Администратор безопасности информации вручную выставляет параметры безопасности, руководствуясь необходимыми нормативными и служебными документами. Если пользователь принадлежит к группе «Пользователи», то меню администрирования не отображается и происходит загрузка ОС в соответствии с полномочиями данного пользователя.	
14	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+ все	Параметр «Неудачных логинов» позволяет определять максимальное количество попыток входа в систему, заканчивающихся неудачей. При превышении допустимого лимита на экран выводится сообщение «Исчерпан лимит попыток ввода пароля или идентификатора» и загрузка становится невозможной. В таком случае необходимо перезагрузить компьютер и заново повторить операцию входа в систему.	1. п.п. 3.15.1 документа «ИНАФ. Руководство администратора».
15	УПД.9	Ограничение числа параллельных сеансов доступа	+ В 1 классе защищенности автоматизированной системы управления	Для каждой учетной записи возможно инициировать только один сеанс работы.	
16	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+ все	В комплексе имеется возможность установки параметра «Автоматическое выключение ЭВМ», то если по истечении заданного интервала времени (за данный интервал времени отвечает параметр «Таймаут для идентификатора») идентификатор пользователя не был предъявлен, ЭВМ автоматически выключается.	1. п.п. 3.15.1 документа «ИНАФ. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
17	УПД.11	Управление действиями пользователей до идентификации и аутентификации	+ все	До проведения идентификации и аутентификации пользователю запрещены любые действия кроме ввода идентификационной и аутентификационной информации, предъявления аппаратного идентификатора, смены пользователя.	1. п.п. 4.2 документа «ИНАФ. Руководство пользователя».
		Ограничение программной среды (ОПС)			
18	ОПС.0	Разработка политики ограничения программной среды	+ во 2 классе защищенности автоматизированной системы управления	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	
19	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ в 1 классе защищенности автоматизированной системы управления		1. п.п 3.2.7, 3.2.8, 5.2 документа «Аккорд-X K. Руководство пользователя»; 2. п.п. 7.12 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		Защита машинных носителей информации (ЗНИ)			
20	ЗНИ.0	Разработка политики защиты машинных носителей информации	+ все	ПАК СЗИ от НСД «ИНАФ» поддерживает политику защиты машинных носителей информации.	
21	ЗНИ.2	Управление физическим доступом к машинным носителям информации	+ все	Доступ к машинным носителям СВТ осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «ИНАФ».	
22	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	1. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора»; 2. п.п. 7.16 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
23	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	+ начиная с 1 класса защищенности автоматизированной системы управления		
24	ЗНИ.7	Контроль подключения машинных носителей информации	+ все		
25	ЗНИ.8	Уничтожение (стирание) информации на	+ все	Обеспечивается при условии совместного	1. п.п 3.2.2, 5.2 документа «Аккорд-X K. Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
		машинных носителях информации		применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	администратора»; 2. п.п. 7.13 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		Аудит безопасности (АУД)			
26	АУД.0	Разработка политики аудита безопасности	+ все	СЗИ от НСД «ИНАФ» поддерживает политику аудита безопасности в части обеспечения регистрации событий безопасности, защиты информации о событиях безопасности и анализа действий пользователей.	
27	АУД.2	Анализ уязвимостей и их устранение	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации. Обновление ПО (firmware) комплекса выполняется в сервисном центре Разработчика ПО.	1. п. 6 документа «ИНАФ. Формуляр».
28	АУД.4	Регистрация событий безопасности	+ все	Комплекс обеспечивает сбор, запись и хранение следующих системных событий и действий пользователей: – В процессе работы ФПО регистрирует события безопасности: – начало сеанса пользователя; – прохождение процедуры идентификации/аутентификации пользователем; – создание журнала системных событий и действий пользователей; – изменение полномочий пользователей; – нарушения целостности, выявленные в рамках: – контроля целостности аппаратуры ПЭВМ; – контроля целостности отдельных файлов и программ; – контроля целостности системных областей жестких дисков (секторов);	1. п.п. 3.14 документа «ИНАФ. Руководство администратора»; 2. Приложение 1 документа «ИНАФ. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
				– контроля целостности системного реестра (для ОС семейства Microsoft Windows).	
29	АУД.6	Защита информации о событиях безопасности	+ все	Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам (администраторам ИНАФ).	
30	АУД.7	Мониторинг безопасности	+ все	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и очистку журнала.	
31	АУД.8	Реагирование на сбои при регистрации событий безопасности	+ все	Если заполнение журнала превышает 85%, при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если заполнение журнала превышает 95%, то загрузка для пользователя блокируется, и требуется вмешательство администратора.	
32	АУД.9	Анализ действий пользователей	+ начиная с 1 класса защищенности автоматизированной системы	СЗИ от НСД «ИНАФ» протоколирует действия пользователей. С помощью раздела (вкладки) «Журнал» можно проанализировать работу каждого пользователя.	
		Обеспечение целостности (ОЦЛ)			
33	ОЦЛ.0	Разработка политики обеспечения целостности	+ все	В комплексе реализована политика обеспечения целостности.	
34	ОЦЛ.1	Контроль целостности программного обеспечения	+ все	С помощью «ИНАФ» производится контроль целостности системных областей жестких дисков, программ и данных, конфигурации технических средств ПЭВМ, а также программных средств СЗИ НСД.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
35	ОЦЛ.3	Ограничение по вводу информации в информационную (автоматизированную) систему	+ начиная с 1 класса защищенности автоматизированной системы управления	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	1. п.п. 3.2.6, 3.2.7 документа «Аккорд-X K. Руководство администратора»; 2. п.п. 7.11 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
36	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+ начиная со 2 класса защищенности автоматизированной системы управления	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К» либо СПО «Аккорд-Х К»).	1. п.п. 3.2.12 документа «Аккорд-Х К. Руководство администратора; 2. п.п. 5.2, 7.13 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
37	ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+ начиная со 2 класса защищенности автоматизированной системы управления	При превышении установленного количества попыток аутентификации загрузка ОС прерывается, ПЭВМ блокируется. Фиксируется корректность алфавита ввода пароля (при использовании некорректных символов на экране появляется сообщение). При превышении установленного количества попыток смены пароля пользователя загрузка системы произойдет только после вмешательства администратора безопасности.	1. п.п. 4.1.2, 4.1.5 документа «ИНАФ. Руководство пользователя».
		Обеспечение доступности (ОДТ)			
38	ОДТ.0	Разработка политики обеспечения доступности	+ все	Комплекс поддерживает политику обеспечения доступности в части обеспечения резервного копирования конфигурации СЗИ от НСД и восстановления СЗИ от НСД из резервной копии.	
39	ОДТ.3	Контроль безотказного функционирования средств и систем	+ во 2 классе защищенности автоматизированной системы управления	Обеспечивается контроль работоспособности, правильности функционирования программного обеспечения средств защиты информации посредством функции самотестирования функционала СЗИ НСД перед стартом.	1. п.п. 3.18 документа «ИНАФ. Руководство администратора».
40	ОДТ.4	Резервное копирование информации	+ все	Комплексом обеспечиваться периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов) на резервные машинные носители информации.	1. п.п. 3.16 документа «ИНАФ. Руководство администратора».
41	ОДТ.5	Обеспечение возможности восстановления информации	+ все	По команде администратора комплексом обеспечивается возможность восстановления информации (базы данных	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
				пользователей и списка контролируемых объектов) с резервных машинных носителей информации (резервных копий).	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
42	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+ все	Комплекс обеспечивает защиту информационной (автоматизированной) системы и ее компонентов в части реализации разделения функций по управлению системой и защиты неизменяемых данных.	
43	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+ все	В «ИНАФ» реализован ролевой метод разграничения доступа. Пользователи делятся на «Администраторов» комплекса и «Пользователей».	1. п.п. 3.6.1 документа «ИНАФ. Руководство администратора».
44	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 класса защищенности автоматизированной системы	Производится контроль целостности программных средств СЗИ НСД (по умолчанию) и всех компонентов. Возможен контроль целостности файлов других приложений, файлов с данными и пр.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
45	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К» либо СПО «Аккорд-X K»).	1. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора»; 2. п.п. 7.11.1 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
46	ЗИС.33	Исключение доступа через общие ресурсы	+ начиная с 1 класса защищенности автоматизированной системы управления	Комплекс обеспечивает очистку баз данных при необходимости передаче устройства «ИНАФ» в другое подразделение, где есть собственный администратор БИ и иной состав пользователей либо при утере идентификатора администратора. Для этого в комплексе реализована функция форматирования баз данных контроллера.	1. п.п. 3.17 документа «ИНАФ. Руководство администратора».
47	ЗИС.38	Защита информации при использовании мобильных устройств	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа	1. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора»;

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
				(СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	2. п.п. 7.16 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
48	ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+ все	Обеспечивается при условии совместного применения комплекса с СПО «Аккорд-В.».	1. п.п. 3.7 документа «Аккорд-В. Руководство по установке».
		Реагирование на компьютерные инциденты (ИНЦ)			
49	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+ все	Комплекс обеспечивает возможность регистрации и сигнализации о любых событиях, относящихся к возможным нарушениям безопасности. Комплекс обеспечивает возможность регистрации и сигнализации о любых событиях, относящихся к возможным нарушениям безопасности.	
50	ИНЦ.1	Выявление компьютерных инцидентов	+ все		1. п.п. 3.14 документа «ИНАФ. Руководство администратора».
51	ИНЦ.2	Информирование о компьютерных инцидентах	+ все		
		Управление обновлениями программного обеспечения (ОПО)			
52	ОПО.0	Разработка политики управления обновлениями программного обеспечения	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения СЗИ от НСД.	
53	ОПО.4	Установка обновлений программного обеспечения	+ все		1. п. 6 документа «ИНАФ. Формуляр».
		Обеспечение действий в нештатных ситуациях (ДНС)			
54	ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+ все	Комплексом обеспечиваться периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов) на резервные машинные носители информации. По команде администратора комплексом обеспечивается возможность восстановления информации (базы данных пользователей и списка контролируемых объектов) с резервных машинных носителей информации (резервных копий).	
55	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций	+ начиная со 2 класса защищенности автоматизированной системы управления		1. п.п. 3.16 документа «ИНАФ. Руководство администратора».
56	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
		нештатных ситуаций			

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения комплекса «ИНАФ»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения комплекса «ИНАФ» (ТУ 4012-046-11443195-2015).

Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения комплекса «ИНАФ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
		Управление доступом (УПД)			
1	УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам		Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K»).	1. п.п. 2.1.5 документа «Аккорд-Win64 K. Руководство по установке».
2	УПД.12	Управление атрибутами безопасности		Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	1. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-X K. Руководство администратора»; 2. п.п. 7.11 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		Ограничение программной среды (ОПС)			
3	ОПС.3	Управление временными файлами		Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K»). Функция «Очищать файл подкачки».	1. п.п. Приложение 1 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		Защита машинных носителей			

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
		информации (ЗНИ)			
4	ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации		Доступ к машинным носителям СВТ осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «ИНАФ».	
		Обеспечение целостности (ОЦЛ)			
5	ОЦЛ.2	Контроль целостности информации		Комплекс обеспечивает контроль целостности структуры базы данных по контрольным суммам программных компонентов базы данных в процессе загрузки и динамически в процессе работы информационной системы.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
6	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K»).	1. п.п. 7.12 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
7	ЗИС.14	Использование неперезаписываемых машинных носителей информации		Комплекс обеспечивает загрузку и исполнение программного обеспечения со специальных носителей информации (CH, выполненные в форм-факторе USB), доступных только для чтения.	1. п.п. 1.1 документа «ИНАФ. Руководство администратора».
8	ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами		Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K»).	1. п.п. 7.15.2 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32»; 2. документ «Инструкция по созданию изолированной программной среды с использованием утилиты AcTskMng».
9	ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)		Посредством комплекса возможно: – резервное копирование информации в соответствии с мерой ОДТ.4; – контроль безотказного функционирования технических средств ИС в соответствии с мерой ОДТ.3; – обеспечение возможности	1. п.п. 3.16, 3.18 документа «ИНАФ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«ИНАФ»	Ссылки на документацию
				восстановления информации с резервных машинных носителей информации (резервных копий) в соответствии с мерой ОДТ.5.	

Итак, путем применения комплекса «ИНАФ» в автоматизированной системе управления выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 3, 4, 5, 7;

УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11;

ОПС: 1;

ЗНИ: 2, 5, 6, 7, 8;

АУД: 2, 4, 6, 7, 8, 9;

ОЦЛ: 1, 3, 4, 5;

ОДТ: 3, 4, 5;

ЗИС: 1, 13, 21, 33, 38, 39;

ИНЦ: 1, 2;

ОПО: 4;

ДНС: 4, 5;

а также дополнительные (не включенные в базовый набор) меры:

УПД: 7, 12;

ОПС: 3;

ЗНИ: 4;

ОЦЛ: 2;

ЗИС: 12, 14, 22, 37.

ОКБ САПР
www.okbsapr.ru
okbsapr@okbsapr.ru
Россия, 115114, Москва, 2-ой Кожевнический переулок, д. 12
Тел.: +7 (495) 994-72-62