ВЫПОЛНЕНИЕ МЕР

17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ

ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

ПУТЕМ ПРИМЕНЕНИЯ КОМПЛЕКСА

СЗИ ОТ НСД «ИНАФ»

ОКБ САПР
2021

1 Общие положения

В настоящем документе рассматривается выполнение мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе (автоматизированной системе) 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 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения ПАК СЗИ от НСД «ИНАФ»

В таблице № 1 представлено описание выполнения базового набора мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения комплекса «ИНАФ» (ТУ 4012-046-11443195-2015).

Выражение «все» в ячейках столбца «Уровни защищенности ПДн» означает, что рассматриваемая мера должна быть реализована в информационной системе с любым уровнем защищенности персональных данных.

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

Таблица 1 – Выполнение базового набора мер по защите информации 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения ПАК СЗИ НСД «ИНАФ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	Идентификация осуществляется по аппаратному идентификатору, аутентификация осуществляется паролю. Пароль пользователя временного действия длиной от 0 до 12 буквенно-цифровых символов. Пароль предъявляется 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».
2	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	В ИНАФ осуществляется идентификация стационарных устройств СВТ, при процедуре контроля целостности конфигурации технических средств СВТ.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ все	+ 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».
4	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+ все	+ 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».
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	Функция аутентификации обеспечивает исключение отображения для пользователя действительного значения аутентификационной информации за счет	1. п.п. 4.1.2 документа «ИНАФ. Руководство пользователя».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
					отображения вводимых символов аутентификационной информации условными знаками.	
6	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+ все	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	
		Управление доступом субъектов доступа к объектам доступа (УПД)				
7	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+ все	+ 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».
8	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+ все	+ все	Ролевой метод реализован в виде групп пользователей (Пользователи и Администраторы).	1. п.п. 3.6.1 документа «ИНАФ. Руководство администратора».
9	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+ все	+ 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 «Администраторы», то следующим шагом при загрузке будет отображено меню, которое определяет возможность	1. п.п. 3.6 документа «ИНАФ. Руководство администратора».
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим	+ все	+ все		

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		функционирование информационной системы			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.	
11	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+ все	+ 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».
12	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Для каждой учетной записи возможно инициировать только один сеанс работы.	
13	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+ начиная с 3 уровня защищенности ПДн	+ 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».
14	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+ начиная с 3 уровня защищенности ПДн	+ все	До проведения идентификации и аутентификации пользователю запрещены любые действия кроме ввода идентификационной и аутентификационной информации, предъявления аппаратного идентификатора,	1. п.п. 4.2 документа «ИНАФ. Руководство пользователя».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
					смены пользователя.	
15	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических устройств	+ все	+ 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».
16	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники[1]	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».
		Ограничение программной среды (ОПС)				
17	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	не входит в базовый набор мер	+ в 1 классе защищенности ИС	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	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 персональных данных (ЗНИ)				
18	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ начиная со 2 уровня защищенности ПДн	+ все	Доступ к машинным носителям СВТ осуществляется только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «ИНАФ»	
19	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на	не входит в базовый набор мер	+ начиная со 2 класса защищенности ИС	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

[1] Угроза доверенной загрузки может быть признана неактуальной в случае блокирования внешних интерфейсов системного блока компьютера, извлечения CD/DVD-приводов и пр. для исключения возможности произвести загрузку недоверенной ОС со сторонних носителей информации.

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		машинные носители персональных данных				«Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
20	ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	+ все	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 K» либо СПО «Аккорд-X K»).	1. п.п 3.2.2, 5.2 документа «Аккорд-X K. Руководство администратора»; 2. п.п. 7.13 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		Регистрация событий безопасности (РСБ)				
21	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+ все	+ все	Журнал регистрации событий содержит следующую информацию: – дата и время регистрации события; – идентификатор пользователя, совершившего событие; – тип события – в таблице выводится краткое описание события; – результат события. В случае совместного применения комплекса и СПО разграничения доступа имеется возможность регулирования детальности ведения журнала.	1. п.п. 3.14 документа «ИНАФ. Руководство администратора»; 2. Приложение 1 документа «ИНАФ. Руководство администратора».
22	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ все	+ все	При регистрации событий фиксируется исчерпывающий набор параметров: дата и время, идентификатор субъекта, идентификатор объекта, тип выполняемой операции, результат операции.	
23	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все	Комплекс обеспечивает сбор, запись и хранение следующих системных событий и действий пользователей: – В процессе работы ФПО регистрирует события безопасности: – начало сеанса	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
					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); – контроля целостности системного реестра (для ОС семейства Microsoft Windows)..	
24	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	не входит в базовый набор	+ 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.	
25	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+ начиная со 2 уровня защищенности ПДн	+ все	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и очистку журнала.	
26	РСБ.7	Защита информации о событиях безопасности	+ все	+ все	Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам (администраторам ИНАФ).	
		Контроль (анализ)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		защищенности персональных данных (АН3)				
27	АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ все	+ 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	АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения СЗИ от НСД.	
29	АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	Реализована функция самотестирования функционала СЗИ НСД перед стартом.	1. п.п. 3.18 документа «ИНАФ. Руководство администратора».
30	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	Комплекс обеспечивает контроль целостности структуры базы данных по контрольным суммам программных компонентов базы данных в процессе загрузки информационной системы.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
31	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	+ начиная со 2 уровня защищенности ПДн	+ все	Настраивается в Параметрах Пользователей: Параметры пароля включают в себя следующие поля: – «Кто может менять пароль» - установка этого параметра позволяет пользователю самому менять пароль после истечения времени действия, или смену пароля может осуществлять только администратор. – «Минимальная длина» - параметр определяет количество символов, контролируемое при создании и смене пароля. Нельзя ввести пароль меньшей длины. Если предполагается для авторизации пользователя использовать только	1. п.п. 3.6.2 документа «ИНАФ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
					идентификатор, то этот параметр нужно установить в 0 (пароль задавать не обязательно). По умолчанию длина пароля установлена равной 8 символам, максимальное допустимое значение - 12 символов. – «Время действия (дни)» - время действия пароля до смены в календарных днях: от 0 (смены пароля не требуется) до 366 дней. – «Попыток для смены» - количество попыток смены пароля: от 0 (не ограничено) до 5. Этот параметр определяет допустимое число попыток смены пароля, если пользователю разрешено самому выполнять такую операцию. Если за отведенное число попыток пароль не сменен корректно, выполняется перезагрузка компьютера. – «Алфавит пароля» - определяет набор символов, которые обязательно должны использоваться при вводе пароля. Например, если в алфавите заданы цифры и буквы, то нельзя ввести пароль, состоящий из одних цифр. При установке флага «Только генерировать» пароль будет генерироваться случайным образом из символов заданного алфавита при смене пароля пользователя.	
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
32	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».
33	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты	не входит в базовый набор мер	+ все	Реализована функция сохранения резервной копии конфигурации СЗИ НСД. Аппаратная часть комплекса СЗИ НСД «ИНАФ» имеет в составе внутреннего ПО функции резервного копирования на гибкий	1. п.п. 3.16 документа «ИНАФ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		информации, при возникновении нештатных ситуаций			магнитный диск и восстановления базы данных пользователей и списка контролируемых объектов.	
34	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ начиная 1 класса защищенности ИС	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К» либо СПО «Аккорд-Х К»).	1. п.п. 3.2.6, 3.2.7 документа «Аккорд-Х К. Руководство администратора»; 2. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Обеспечение доступности персональных данных (ОДТ)				
35	ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	+ на 1 уровне защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».
36	ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».
37	ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	По команде администратора комплексом обеспечивается возможность восстановления информации (базы данных пользователей и списка контролируемых объектов) с резервных машинных носителей информации (резервных копий).	
		Защита среды виртуализации (ЗСВ)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
38	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+ все	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К» либо СПО «Аккорд-Х К») либо СПО «Аккорд-В.».	1. п.п. 2.1.1, 2.1.2 документа «Аккорд-Х К. Руководство оператора (пользователя)»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора»; 3. п.п. 2.1.1, 2.1.2 документа «Аккорд-Win64 К. Руководство пользователя»; 4. п.п. 2.3.1, 2.3.2 документа «Аккорд-В. Руководство пользователя».
39	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+ все	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К» либо СПО «Аккорд-Х К»).	1. п.п. 3.2.6, 3.2.7, 3.2.10, 3.2.12 документа «Аккорд-Х К. Руководство администратора»; 2. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
40	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+ начиная с 3 уровня защищённости ПДн	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К») либо СПО «Аккорд-В.».	1. п.п. 5.3, 5.4 документа «Аккорд-В. Руководство администратора»; 2. документ «Аккорд-Win64 К. Подсистема регистрации. Программы работы с журналами регистрации».
41	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Обеспечивается при условии совместного применения комплекса с СПО «Аккорд-В.».	1. п.п. 3.7 документа «Аккорд-В. Руководство по установке».
42	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС		1. п.п. 5.2.4 документа «Аккорд-В. Руководство администратора».
43	ЗСВ.8	Резервное копирование данных, резервирование технических средств,	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС		1. п.п. 4 документа «Аккорд-В. Руководство по установке».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры				
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
44	ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы	+ на 1 уровне защищенности ПДн	+ начиная со 2 класса защищенности ИС	В «ИНАФ» реализован ролевой метод разграничения доступа. Пользователи делятся на «Администраторов» комплекса и «Пользователей».	1. п.п. 3.6.1 документа «ИНАФ. Руководство администратора».
45	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	не входит в базовый набор	+ 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. 7.11.1 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
46	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		персональных данных				
47	ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы	нет	+ в 1 классе защищенности ИС	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».
48	ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	нет	+ все	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. 7.16 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Выявление инцидентов и реагирование на них (ИНЦ)				
49	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищенности ПДн	нет	Комплекс обеспечивает возможность регистрации и сигнализации о любых событиях, относящихся к возможным нарушениям безопасности.	1. п.п. 3.14 документа «ИНАФ. Руководство администратора».

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения ПАК СЗИ НСД «ИНАФ»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения комплекса «ИНАФ» (ТУ 4012-046-11443195-2015).

Выражением «нет» выделены ячейки столбца «Уровни защищенности ПДн», которые относятся к требованиям, содержащимся только в 17-ом приказе ФСТЭК, и, следовательно, не относящимся к уровням защищенности ПДн.

Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения ПАК СЗИ НСД «ИНАФ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа	нет		Идентификация и аутентификация объектов файловой системы осуществляется на уровне идентификации поддерживаемых файловых систем. Комплекс поддерживает идентификацию и аутентификацию запускаемых и исполняемых модулей на уровне контроля целостности файлов ОС. Идентификация объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением осуществляется на уровне контроля целостности файлов реестра.	1. п.п. 3.13.2, 3.13.3 документа «ИНАФ. Руководство администратора».
		Управление доступом субъектов доступа к объектам доступа (УПД)				
2	УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных			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».
3	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее			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

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		хранения и обработки				«Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		Ограничение программной среды (ОПС)				
4	ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			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 персональных данных (ЗНИ)				
5	ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах			Доступ к машинным носителям СВТ осуществляется только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «ИНАФ».	
6	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных			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».
7	ЗНИ.7	Контроль подключения машинных носителей персональных данных				
		Регистрация событий безопасности (РСБ)				
8	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	нет		СЗИ от НСД «ИНАФ» протоколирует действия пользователей. С помощью раздела (вкладки) «Журнал» можно проанализировать работу каждого пользователя.	1. п.п. 3.14 документа «ИНАФ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
		Защита среды виртуализации (ЗСВ)				
9	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			Обеспечивается при условии совместного применения комплекса с СПО «Аккорд-В.».	1. п.п. 3.7 документа «Аккорд-В. Руководство по установке».
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
10	ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы			Комплекс обеспечивает контроль целостности структуры базы данных по контрольным суммам программных компонентов базы данных в процессе загрузки информационной системы.	1. п.п. 3.13 документа «ИНАФ. Руководство администратора».
11	ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы			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».
12	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			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	1. п.п. 4.1.2, 4.1.5 документа «ИНАФ. Руководство пользователя».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«ИНАФ»	Ссылки на документацию
					пользователя загрузка системы произойдет только после вмешательства администратора безопасности.	
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
13	ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами			Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К»).	1. п.п. 7.15.2 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32»; 2. документ «Инструкция по созданию изолированной программной среды с использованием утилиты AcTskMng».
14	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения			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».
15	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К»).	1. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
16	ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты	нет		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 восстановления информации с резервных машинных	1. п.п. 3.16, 3.18 документа «ИНАФ. Руководство администратора».

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

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

ИАФ: 1, 2, 3, 4, 5, 6;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 15, 17;

ОПС: 1;

ЗНИ: 2, 5, 8;

РСБ: 1, 2, 3, 4, 5, 7;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 3, 4, 5;

ЗСВ: 1, 2, 3, 6, 7, 8;

ЗИС: 1, 5, 15, 21, 30;

ИНЦ: 2;

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

ИАФ: 7;

УПД: 7, 12;

ОПС: 4;

ЗНИ: 4, 6, 7;

РСБ: 8;

ЗСВ: 5;

ОЦЛ: 2, 5, 8;

ЗИС: 6, 18, 19, 29.

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