ВЫПОЛНЕНИЕ МЕР

17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ

ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

ПУТЕМ ПРИМЕНЕНИЯ КОМПЛЕКСА

СЗИ НСД «АККОРД-АМДЗ»

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 «Аккорд-АМДЗ».

ПАК СЗИ НСД «Аккорд-АМДЗ» (ПАК СЗИ НСД «Аккорд-АМДЗ», СЗИ от НСД «Аккорд--АМДЗ» либо комплекс) предназначен для использования на ПЭВМ (ПК) типа IBM PC и обеспечивает защиту устройств и информационных ресурсов от НСД, идентификацию и аутентификацию пользователей, регистрацию их действий, контроль целостности файлов и областей жестких дисков ПЭВМ при многопользовательском режиме их работы.

Доверенная загрузка выполняется для любых операционных систем (ОС), поддерживающих файловые системы: поддерживающей файловые системы:

– FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, Ext4, ReiserFS (ТУ 4012-038-11443195-2011);

– FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, Ext4, ReiserFS (ТУ 4012-054-11443195-2013);

– FAT12, FAT16, FAT32, NTFS, Ext2, Ext3 Ext4, FreeBSD UFS/UFS2, QNX4, QNX6, XFS (ТУ 26.20.40.140-079-37222406-2019).

ПАК СЗИ НСД «Аккорд-АМДЗ» состоит из:

– специализированного контроллера (далее по тексту – контроллер) с предустановленной на этапе изготовления резидентной операционной средой (специализированное программное обеспечение – СПО, которое не реализует функциональные требования безопасности комплекса и представляет собой среду функционирования для функционального программного обеспечения);

– функционального программного обеспечения, реализующего функциональные требования безопасности в соответствии с требованиями документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013) и «Профиль защиты средства доверенной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ» (ФСТЭК России, 2013) и исполняется в резидентной операционной среде.

2 Выполнение базового набора мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения комплекса СЗИ НСД «Аккорд-АМДЗ»

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 «Аккорд-АМДЗ» (ТУ 26.20.40.140-079-37222406-2019, ТУ 4012-054-11443195-2013, ТУ 4012-038-11443195-2011).

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 комплекса СЗИ НСД «Аккорд-АМДЗ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	В ПАК СЗИ от НСД «Аккорд-АМДЗ» идентификация осуществляется по аппаратному идентификатору, аутентификация осуществляется паролю.	1. п.п. 3.2 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п. 3.1.1, 3.1.2 документа «Аккорд-АМДЗ. 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 ПАК СЗИ от НСД «Аккорд-АМДЗ» осуществляется идентификация стационарных устройств СВТ, при процедуре контроля целостности конфигурации технических средств СВТ.	1. п.п. 3.10, 3.12 документа «Аккорд-АМДЗ. Руководство администратора».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ все	+ все	Управление идентификаторами учетных записей производится в административном режиме АМДЗ в разделе «Пользователи». Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных идентификаторов.	1. п.п. 3.2 документа «Аккорд-АМДЗ. 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 АМДЗ в разделе «Пользователи».	1. п.п. 3.2 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	При вводе пароля (при авторизации в АМДЗ), пароль отображается звездочками.	1. п.п. 3.1.2 документа «Аккорд-АМДЗ. Руководство пользователя».
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 К», СПО «Аккорд-Х К») либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ».	
		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 учетными записями производится в административном режиме АМДЗ в разделе «Пользователи». Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных идентификаторов. Возможно задание временных ограничений на доступ пользователей к АМДЗ в соответствии с установленным для них режимом работы.	1. п.п. 3.3 документа «Аккорд-АМДЗ. 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 АМДЗ.	1. п.п. 3.3.1 документа «Аккорд-АМДЗ. Руководство администратора».
9	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+ все	+ все	В памяти контроллера АМДЗ хранятся имена пользователей и их полномочия. После прохождения процедуры ИА пользователей, встроенное ПО контроллера определяет дальнейший режим	1. п.п. 3.3.2, 3.3.3 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все	загрузки по результатам данной процедуры. Администрирование АМДЗ 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 администрирования АМДЗ (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	Комплекс «Аккорд-АМДЗ» обеспечивает блокирование персонального идентификатора, с которого предпринимаются попытки доступа, при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему.	1. п.п. 3.12.1 документа «Аккорд-АМДЗ. 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.	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
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 сторожевого таймера – времени, которое предоставляется пользователю для предъявления идентификатора и пароля. Также 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. 3.12.4, 3.12.1 документа «Аккорд-АМДЗ. 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, смены пользователя.	1. п.п. 3.2 документа «Аккорд-АМДЗ. Руководство 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 К», СПО «Аккорд-Х К») либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора»; 3. п.п. 7.16 документа «Аккорд-Win64 К. 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, 3.10 документа «Аккорд-АМДЗ. Руководство администратора».

[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	«Аккорд-АМДЗ»	Ссылки на документацию
					Функционирование подсистемы безопасности доверенной загрузки тесно связано с результатами выполнения процедур в других подсистемах СДЗ, например: – в случае заполнения журнала регистрации событий на 95% в подсистеме аудита, осуществляется блокировка загрузки ОС; – при превышении числа попыток идентификации/аутентификации в подсистеме идентификации и аутентификации осуществляется блокировка загрузки ОС; – при нарушении целостности СДЗ при выполнении процедур подсистемы самотестирования осуществляется блокировка загрузки ОС; – при нарушении целостности загружаемой программной среды и состава аппаратных компонентов в подсистеме контроля целостности осуществляется блокировка загрузки ОС.	
		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 К», СПО «Аккорд-Х К») либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.7, 3.4.8, 5.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.7, 3.2.8, 5.2 документа «Аккорд-Х К. Руководство пользователя»; 3. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Защита машинных носителей персональных данных (ЗНИ)				
18	ЗНИ.2	Управление доступом к	+ начиная со 2	+ все	Доступ к машинным носителям СВТ	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		машинным носителям персональных данных	уровня защищенности ПДн		осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «Аккорд-АМДЗ».	
19	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных	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», СПО «Аккорд-X K») либо при применении ПАК «Аккорд-X», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.13 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора»; 3. п.п. 7.16 документа «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», СПО «Аккорд-X K») либо при применении ПАК «Аккорд-X», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.2, 5.2 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.2, 5.2 документа «Аккорд-X K. Руководство администратора»; 3. 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 Аккорд-АМДЗ содержит следующую информацию: – дата и время регистрации события; – имя пользователя, совершившего событие; – тип операции – в таблице выводится краткое описание события; – результат события. В случае совместного применения комплекса и СПО разграничения доступа имеется возможность регулирования детальности ведения	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
					журнала.	
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: – начало сеанса пользователя; – прохождение процедуры аутентификации пользователя; – осуществление контроля целостности аппаратуры ПЭВМ; – осуществление контроля целостности отдельных файлов и программных средств ПЭВМ; – осуществление контроля целостности системных областей жестких дисков (секторов); – осуществление контроля целостности системного реестра (для ОС семейства Microsoft Windows); – создание журнала системных событий и действий пользователей; – изменение полномочий пользователей.	
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.	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».
25	РСБ.5	Мониторинг (просмотр, анализ)	+	+	Комплекс обеспечивает просмотр администратору	1. п.п. 3.11, 3.14.3 документа

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		результатов регистрации событий безопасности и реагирование на них	начиная со 2 уровня защищенности ПДн	все	зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и очистку журнала.	«Аккорд-АМДЗ. Руководство администратора».
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 АМДЗ).	
		Контроль (анализ) защищенности персональных данных (АНЗ)				
27	АНЗ.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) модуля доверенной загрузки выполняется в сервисном центре Разработчика ПО.	1. п. 6 документа «Аккорд-АМДЗ. Формуляр».
28	АНЗ.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	АНЗ.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. 3.16 документа «Аккорд-АМДЗ. Руководство администратора».
30	АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	С помощью «Аккорд-АМДЗ» производится контроль целостности системных областей жестких дисков, программ и данных, конфигурации технических средств ПЭВМ, а также программных средств СЗИ НСД. В комплексе обеспечивается регистрация событий безопасности, связанных с изменением состава технических средств,	1. п.п. 3.10 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п. 3.1 документа «Аккорд-АМДЗ. Руководство пользователя».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
					программного обеспечения и средств защиты информации.	
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 для авторизации пользователя предполагается использовать только идентификатор, этот параметр нужно установить равным 0 (пароль задавать необязательно). 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» -	1. п.п. 3.3.2-3.3.5 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
					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 «Аккорд-АМДЗ» производится контроль целостности системных областей жестких дисков, программ и данных, конфигурации технических средств ПЭВМ, а также программных средств СЗИ НСД.	1. п.п. 3.10 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п. 3.1 документа «Аккорд-АМДЗ. Руководство пользователя».
33	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	не входит в базовый набор мер	+ все	Реализована функция сохранения резервной копии конфигурации СЗИ НСД. Аппаратная часть комплекса СЗИ НСД «Аккорд-АМДЗ» имеет в составе внутреннего ПО функции резервного копирования на гибкий магнитный диск и восстановления базы данных пользователей и списка контролируемых объектов.	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».
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», СПО «Аккорд-Х К») либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.6, 3.4.7 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.6, 3.2.7 документа «Аккорд-Х К. Руководство администратора»; 3. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		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. 3.16 документа «Аккорд-АМДЗ. 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. 3.14 документа «Аккорд-АМДЗ. 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)				
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», СПО «Аккорд-Х К»), СПО «Аккорд-В.» либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ».	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-Х. Руководство оператора (пользователя)»; 4. п.п. 3.4.3 документа «Аккорд-Х. Руководство администратора». 5. п.п. 2.1.1, 2.1.2 документа «Аккорд-Win64 К. Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
						пользователя»; 6. 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», СПО «Аккорд-Х К»), либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.2.6, 3.2.7, 3.2.10, 3.2.12 документа «Аккорд-Х К. Руководство администратора»; 2. п.п. 3.4.6, 3.4.7, 3.4.10, 3.4.13 документа «Аккорд-Х. Руководство администратора»; 3. 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, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС		1. п.п. 4 документа «Аккорд-В. Руководство по установке».
		Защита информационной системы, ее средств, систем связи и передачи				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		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 «Аккорд-АМДЗ» реализован ролевой метод разграничения доступа. Пользователи делятся на «Администраторов» комплекса и «Пользователей».	1. п.п. 3.3.1 документа «Аккорд-АМДЗ. 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 К», СПО «Аккорд-Х К») либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ». Возможно исключение несанкционированного использования USB-принтеров – регулируется посредством назначения пользователю (или группе пользователей) соответствующих правил разграничения доступа.	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора»; 3. п.п. 7.11.1 документа «Аккорд-Win64 К. 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 персональных данных	+ 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. 3.10 документа «Аккорд-АМДЗ. Руководство администратора».
47	ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные	нет	+ в 1 классе защищенности ИС	Комплекс обеспечивает очистку баз данных при необходимости передаче компьютера в другое подразделение, где есть собственный администратор БИ и иной состав пользователей либо при утере идентификатора администратора. Для этого в комплексе реализована	1. п. 4 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		общие для пользователей ресурсы информационной системы			функция аппаратной очистки баз данных.	
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 K», СПО «Аккорд-X K») либо при применении ПАК «Аккорд-X», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.13 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора»; 3. п.п. 7.16 документа «Аккорд-Win64 K. 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 фиксацию операций с доступом к объектам, операции смены субъекта доступа, операции И/А.	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора»; 2. Приложение 1 документа «Аккорд-АМДЗ. Руководство пользователя».

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 СЗИ НСД «Аккорд-АМДЗ»

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 «Аккорд-АМДЗ» (ТУ 26.20.40.140-079-37222406-2019, ТУ 4012-054-11443195-2013, ТУ 4012-038-11443195-2011).

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 СЗИ НСД «Аккорд-АМДЗ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	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. 1.1, 3.10.3 документа «Аккорд-АМДЗ. 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),			Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО	1. п.п. 3.4.6, 3.4.7, 5.2 документа «Аккорд-X. Руководство администратора»;

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		связанных с информацией в процессе ее хранения и обработки			«Аккорд-Win64 K», СПО «Аккорд-X K») либо при применении ПАК «Аккорд-X», в состав которого сходит «Аккорд-АМДЗ».	2. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-X K. Руководство администратора»; 3. п.п. 7.11 документа «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 «Аккорд-АМДЗ».	
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», СПО «Аккорд-X K») либо при применении ПАК «Аккорд-X», в состав которого сходит «Аккорд-АМДЗ».	1. п.п. 3.4.13 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора»; 3. 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)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
8	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	нет		СЗИ от НСД «Аккорд» протоколирует действия пользователей. С помощью раздела (вкладки) «Журнал» можно проанализировать работу каждого пользователя.	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».
		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. 3.10.2 документа «Аккорд-АМДЗ. 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», СПО «Аккорд-Х К») либо при применении ПАК «Аккорд-Х», в состав которого сходит «Аккорд-АМДЗ». С помощью «Аккорд-Х» возможно выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации. С помощью СПО «Аккорд-Win64 К» возможно: – выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации и	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.12 документа «Аккорд-Х К. Руководство администратора; 3. п.п. 5.2, 7.13 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
					реагирование на них; – выявление фактов неправомерного вывода на печать документов, содержащих защищаемую информацию, и реагирование на них.	
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 пользователь блокируется. Фиксируется корректность алфавита ввода пароля (при использовании некорректных символов на экране появляется сообщение). При превышении установленного количества попыток смены пароля пользователя выполняется перезагрузка компьютера.	1. п.п. 3.2.2, 3.12.1 документа «Аккорд-АМДЗ. Руководство администратора».
		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 K»). При установке меток доступа информация об этом записывается в файл. Данные файл возможно установить этот файл на КЦ.	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».
14	ЗИС.19	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».
15	ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае	нет		Посредством комплекса возможно: – резервное копирование информации в соответствии с мерой ОДТ.4; – контроль безотказного функционирования технических средств ИС в соответствии с мерой	1. п.п. 3.14, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-АМДЗ»	Ссылки на документацию
		возникновении отказов (сбоев) в системе защиты информации информационной системы			ОДТ.3; – обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в соответствии с мерой ОДТ.5.	

Итак, путем применения комплекса «Аккорд-АМДЗ» 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;

ОЦЛ: 2, 5, 8;

ЗСВ: 5;

ЗИС: 6, 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