

**ВЫПОЛНЕНИЕ МЕР
17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ
ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ
ПУТЕМ ПРИМЕНЕНИЯ СПО «АККОРД-В.»**

**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 специального программного обеспечения «Аккорд-В.».

СПО «Аккорд-В.» состоит из специального программного обеспечения «Аккорд-В.», которое обеспечивает выполнение функциональных требований безопасности и является объектом оценки при сертификации, в состав которого входят 3 программных компонента:

- сервис регистрации событий;
- программное обеспечение (ПО) управления изделием;
- агенты защиты ESXi серверов.

СПО «Аккорд-В.» соответствует требованиям документов «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденных приказом ФСТЭК России от 2 июня 2020 г №76 по 2 уровню доверия.

2 Выполнение базового набора мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения СПО «Аккорд-В.»

В таблице № 1 представлено описание выполнения базового набора мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения СПО «Аккорд-В.» (ТУ 26.20.40.140-086-37222406-2020).

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 СПО «Аккорд-В.»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей,	+ все	+ все	В СПО «Аккорд-В.» реализован механизм идентификации	1. п.п. 2.3.1, 2.3.2 документа «Аккорд-В. Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		являющихся работниками оператора			аутентификации администратора безопасности при входе на ESXi сервера. Идентификация и аутентификация осуществляется по имени пользователя, паролю. Идентификация пользователей осуществляется по имени и идентификатору (например, ПИ «ШИПКА»).	пользователя»; 2. п. 3.7.1 документа «Аккорд-В. Руководство администратора».
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	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	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	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.2-7.4 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
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		
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	При вводе пароль отображается символами.	1. п. 3.7.1 документа «Аккорд-В. Руководство администратора».
6	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+ все	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 2.1.1, 2.1.2 документа «Аккорд-Win64 К. Руководство пользователя».
		Управление доступом субъектов доступа к объектам доступа (УПД)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
7	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+ все	+ все	В СПО «Аккорд-В.» регистрируются администратор безопасности информации, а также системные учетные записи для подсистемы регистрации событий.	1. п. 3, 6 документа «Аккорд-В. 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	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
9	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+ все	+ все	СПО «Аккорд-В.» обеспечивает разделение на администратора безопасности информации и системных пользователей. Также обеспечивается разделение должностных обязанностей в рамках роли администратора безопасности информации.	1. п.п. 3.5.2 документа «Аккорд-В. Руководство по установке»; 2. п. 3, 6 документа «Аккорд-В. Руководство администратора».
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все		
11	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+ все	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	1. п.п. 3.12.1 документа «Аккорд-АМДЗ. Руководство администратора».
12	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Для каждой учетной записи комплекса СПО СЗИ от НСД «Аккорд-В.» возможен только один сеанс доступа.	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		информационной системы				
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	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п. 7.6 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
14	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+ начиная с 3 уровня защищенности ПДн	+ все	Пользователь может приступить к работе только после выполнения контрольных процедур.	1. п.п. 2.4 документа «Аккорд-В. Руководство пользователя».
15	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные связи	+ все	+ все	Доступ администратора безопасности к ESXi-серверам обеспечивается по защищенному протоколу SSH.	1. п.п. 3.6.3 документа «Аккорд-В. Руководство по установке»; 2. п.п. 5.5.1 документа «Аккорд-В. Руководство администратора».
16	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических устройств	+ все	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п. 7.16 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
17	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники ¹	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	СПО «Аккорд-В.» осуществляет доверенную загрузку VM инфраструктуры виртуализации VMware vSphere. В совокупности с СЗИ НСД «Аккорд-АМД3» обеспечивается доверенная загрузка всей инфраструктуры виртуализации.	1. п.п. 3.7 документа «Аккорд-В. Руководство по установке». 2. п.п. 1.1, 3.10 документа «Аккорд-АМД3. Руководство администратора».
		Ограничение программной среды (ОПС)				
18	ОПС.1	Управление запуском (обращениями) компонентов	не входит в базовый набор мер	+ в 1 классе защищенности ИС	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО	1. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа».

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-В.»	Ссылки на документацию
		программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения			«Аккорд-Win64 К».	Программа ACED32».
		Защита машинных носителей персональных данных (ЗНИ)				
19	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ начиная со 2 уровня защищенности ПДн	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	
20	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 СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.16 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
21	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		1. п.п. 7.13 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Регистрация событий безопасности (РСБ)				
22	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+ все	+ все	СПО «Аккорд-В.» в процессе работы производит регистрацию следующих событий безопасности: – о запуске и остановке СПО «Аккорд-В.», а также	1. п.п. 5.3, 5.4 документа «Аккорд-В. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
23	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	<p>сообщения о получении информации о режиме работы СПО «Аккорд-В.»;</p> <ul style="list-style-type: none"> – о настройке режима работы СПО «Аккорд-В.»; – об добавлении/удалении ВМ и её компонентов на контроль; – о проведении проверок целостности ВМ или её компонентов, в том числе о нарушениях целостности; – о включении и выключении ВМ; – о блокировании и разблокировании ВМ; – о работе с виртуальными папками Virtual Folders; – о работе с сессией; – о включении, выключении, перезагрузке, переходе в режим энергосбережения (suspend режим) ВМ; – о включении, выключении, перезагрузке, переходе в режим энергосбережения (suspend режим) vApp; – о миграции ВМ; – о клонировании ВМ; – об изменении конфигурации ВМ; – о работе со снапшотами; – о включении, выключении, переключении, работе в режиме обслуживания (maintenance mode) хостов ESXi серверов; – об изменении конфигурации ESXi серверов (сетевых настроек, работы firewall, запуска, останова или перезапуска сервисов, работы с ролями и разрешениями); – об ошибках в СПО «Аккорд-В.». 	
24	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в	+	+	В СПО «Аккорд-В.» обеспечено централизованное автоматизированное управление сбором, записью	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		течение установленного времени хранения			и хранением информации о событиях безопасности. Сбор событий выполняется с vCenter и агентов «Аккорд-В.» на ESXi.	
25	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	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».
26	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+ начиная со 2 уровня защищенности ПДн	+ все	Для того чтобы начать работу с журналом регистрации событий, необходимо запустить с правами администратора ярлык «LogViewer-V.» на АРМ с установленным сервисом регистрации событий.	1. п.п. 5.3, 5.4 документа «Аккорд-В. Руководство администратора».
27	РСБ.7	Защита информации о событиях безопасности	+ все	+ все	Доступ к записям аудита и функциям управления механизмами аудита предоставляется только уполномоченным должностным лицам.	
		Контроль (анализ) защищенности персональных данных (АНЗ)				
28	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ все	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения защиты информации. Обновление СПО выполняется эксплуатирующей организацией в соответствии с Формуляром и п. 3 документа «Руководство по установке» на комплекс.	1. п. 3 документа «Аккорд-В. Руководство по установке». 2. п.п. 6.2 документа «Аккорд-В. Формуляр».
29	АНЗ.2	Контроль установки обновлений программного обеспечения,	+ все	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения.	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		включая обновление программного обеспечения средств защиты информации				
30	АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	1. п.п. 3.1, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».
31	АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	В СПО реализован механизм контроля целостности оборудования ВМ, а также BIOS и MBR ВМ, выполняемого до их запуска.	1. п. 5.2.4, 5.2.5 документа «Аккорд-В. Руководство администратора».
32	АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	+ начиная с 2 уровня защищенности ПДн	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.3, 7.4 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Обеспечение целостности информационно й системы и персональных данных (ОЦЛ)				
33	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	СПО «Аккорд-В.» обеспечивает контроль целостности BIOS и MBR включаемых ВМ, файлов, содержащих параметры настройки виртуальных машин, а также системных и пользовательских файлов внутри ВМ.	1. п. 5.2.4, 5.2.5 документа «Аккорд-В. Руководство администратора».
34	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты	не входит в базовый набор мер	+ все	СПО «Аккорд-В.» обеспечивает создание резервных копий баз данных агентов СПО «Аккорд-В.» на ESXi серверах.	1. п. 5.5.2 документа «Аккорд-В. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		информации, при возникновении нештатных ситуаций				
35	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К.».	1. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Обеспечение доступности персональных данных (ОДТ)				
36	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 при условии совместного применения СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМД3».	1. п.п. 3.16 документа «Аккорд-АМД3. Руководство администратора».
37	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	СПО «Аккорд-В.» обеспечивает создание резервных копий баз данных агентов СПО «Аккорд-В.» на ESXi серверах.	1. п. 4 документа «Аккорд-В. Руководство по установке».
38	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	СПО «Аккорд-В.» обеспечивает восстановление резервных копий баз данных агентов СПО «Аккорд-В.» на ESXi серверах.	1. п. 5.5.2 документа «Аккорд-В. Руководство администратора».
		Защита среды виртуализации (ЗСВ)				
39	ЗСВ.1	Идентификация и аутентификация субъектов доступа и	+ все	+ все	В СПО «Аккорд-В.» реализован механизм идентификации и аутентификации	1. п.п. 2.3.1, 2.3.2 документа «Аккорд-В. Руководство пользователя»;

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации			администратора безопасности при входе на ESXi сервера. Идентификация пользователей осуществляется по имени и идентификатору (например, ПИ «ШИПКА»).	2. п. 3.7.1 документа «Аккорд-В. Руководство администратора».
40	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 СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
41	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+ начиная с 3 уровня защищенности ПДн	+ все	СПО «Аккорд-В.» в процессе работы производит регистрацию следующих событий безопасности: – о запуске и остановке СПО «Аккорд-В.», а также сообщения о получении информации о режиме работы СПО «Аккорд-В.»; – о настройке режима работы СПО «Аккорд-В.»; – об добавлении/удалении ВМ и её компонентов на контроль; – о проведении проверок целостности ВМ или её компонентов, в том числе о нарушениях целостности; – о включении и выключении ВМ; – о блокировании и разблокировании ВМ; – о работе с виртуальными папками Virtual Folders; – о работе с сессией; – о включении, выключении, перезагрузке, переходе в режим энергосбережения (suspend режим) ВМ; – о включении, выключении, перезагрузке, переходе в режим энергосбережения (suspend режим) vApp; – о миграции ВМ;	1. п.п. 5.3, 5.4 документа «Аккорд-В. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
					<ul style="list-style-type: none"> – о клонировании VM; – об изменении конфигурации VM; – о работе со снапшотами; – о включении, выключении, переподключении, работе в режиме обслуживания (maintenance mode) хостов ESXi серверов; – об изменении конфигурации ESXi серверов (сетевых настроек, работы firewall, запуска, останова или перезапуска сервисов, работы с ролями и разрешениями); – об ошибках в СПО «Аккорд-В.». <p>Сбор событий выполняется с vCenter и агентов «Аккорд-В.» на ESXi.</p>	
42	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	<p>СПО обеспечивает управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации в части контроля запуска виртуальных машин на ESXi с установленным агентами из состава СПО «Аккорд-В.».</p> <p>Управление перемещением виртуальных машин (контейнеров) путем контроля запуска виртуальной машины предусматривает ограничение запуска перемещаемых виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы) на СВТ с установленным СПО «Аккорд-В.».</p>	1. п.п. 3.7 документа «Аккорд-В. Руководство по установке».
43	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	СПО обеспечивает выполнение контроля целостности оборудования VM, а также BIOS и MBR VM, выполняемого до их запуска.	1. п.п. 5.2.4 документа «Аккорд-В. Руководство администратора».
44	ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	СПО «Аккорд-В.» обеспечивает восстановление резервных копий баз данных агентов СПО «Аккорд-В.» на ESXi серверах.	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	«Аккорд-В.»	Ссылки на документацию
		обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры				
		Защита информационно й системы, ее средств, систем связи и передачи данных (ЗИС)				
45	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 СПО «Аккорд-В.» регистрируются администратор безопасности информации, а также системные учетные записи для подсистемы регистрации событий.	1. п. 3, 6 документа «Аккорд-В. Руководство администратора».
46	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 СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.11.1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
47	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Производится контроль целостности BIOS и MBR включаемых ВМ, файлов, содержащих параметры настройки виртуальных машин, а также системных и пользовательских файлов внутри ВМ.	1. п.п. 5.2.4 документа «Аккорд-В. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		данных				
48	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	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. Приложение 1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
49	ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	нет	+ все	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.16 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Выявление инцидентов и реагирование на них (ИНЦ)				
50	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищенности ПДн	нет	Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К». Сервис регистрации событий осуществляет сбор событий инфраструктуры VMware vSphere, а также событий агентов «Аккорд-В.» на ESXi.	1. п.п. 1.2 документа «Аккорд-В. Руководство по установке»; 2. Приложение 1 документа «Аккорд-В. Руководство администратора»; 3. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке»; 4. Приложение 2 документа «Аккорд-Win64 К. 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 СПО «Аккорд-В.»

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 СПО «Аккорд-В.» (ТУ 26.20.40.140-086-37222406-2020).

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.

Выражением «нет» выделены ячейки столбца «Классы защищенности ИС», которые относятся к требованиям, содержащимся только в 21-ом приказе ФСТЭК, и, следовательно, не относящимся к классам защищенности ИС.

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 СПО «Аккорд-В.»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	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 ОС. Комплекс поддерживает идентификацию и аутентификацию запускаемых и исполняемых модулей на уровне контроля целостности файлов ОС ВМ.	
		Управление доступом субъектов доступа к объектам доступа (УПД)				
2	УПД.7	Предупреждение пользователя при его входе в информационную систему о том,			Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
3	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				1. п.п. 7.11 документа «Аккорд-Win64 К. 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 СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. Приложение 1 документа «Аккорд-Win64 К. 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			Обеспечивается при условии совместного использования СПО «Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
6	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных			Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.16 документа «Аккорд-Win64 К. 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		В утилите просмотра журнала регистрации событий «LogViewer-V.» предусмотрена возможность ведения статистики по полученным событиям. Выводится статистика по количеству, типам и результатам полученных событий.	1. п.п. 5.3, 5.4 документа «Аккорд-В. Руководство администратора».
		Обеспечение целостности информационно й системы и персональных данных (ОЦЛ)				
9	ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы			Обеспечивается при условии совместного применения СПО «Аккорд-В.» и СПО «Аккорд-Win64 К».	1. п.п. 7.10 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
10	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				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		исключение неправомерной передачи информации из информационной системы				
11	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке».
		Защита среды виртуализации (ЗСВ)				
12	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			В СПО обеспечивается доверенная загрузка всех элементов инфраструктуры виртуализации.	1. п.п. 3.7 документа «Аккорд-В. Руководство по установке».
		Защита информационно й 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 СПО «Аккорд-В.» и 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 среды с использованием утилиты AcTskMng».
14	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				1. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
15	ЗИС.29	Перевод информационной системы или ее	нет		Обеспечивается при условии совместного использования СПО	1. п.п. 3.14, 3.16 документа «Аккорд-АМДЗ. Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-В.»	Ссылки на документацию
		устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновения отказов (сбоев) в системе защиты информации информационной системы			«Аккорд-В.» и СЗИ НСД «Аккорд-АМДЗ».	администратора».

Итак, путем применения СПО «Аккорд-В.» 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, 13, 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