

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

**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 «Аккорд-МКТ».

Модуль доверенной загрузки «Аккорд-МКТ» (МДЗ «Аккорд-МКТ», «Аккорд-МКТ», МДЗ либо комплекс) представляет собой программное средство доверенной загрузки ЭВМ на базе процессоров с архитектурой x86_64, которое встраивается в базовую систему ввода-вывода и осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, а также не препятствует доступу к информационным ресурсам в случае успешного контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы.

МДЗ «Аккорд-МКТ» состоит из:

- специального программного обеспечения средства доверенной загрузки уровня БСВВ «Аккорд-МКТ» (далее по тексту – СПО «Аккорд-МКТ»), которое обеспечивает выполнение функциональных требований безопасности и является объектом оценки при сертификации.
- БСВВ и базы данных МДЗ «Аккорд-МКТ» составляют среду функционирования СПО «Аккорд-МКТ».

МДЗ «Аккорд-МКТ» встраивается на этапе производства ЭВМ и функционирует в их составе.

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

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-МКТ» (ТУ 26.20.40.140-082-37222406-2019, ТУ 501410-071-37222406-2016).

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 МДЗ «Аккорд-МКТ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	<p>Комплекс обеспечивает:</p> <ul style="list-style-type: none"> – идентификацию и аутентификацию пользователей при входе в систему по уникальному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры; – идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования МДЗ «Аккорд-МКТ» по уникальному идентификатору пользователя и по паролю 0 до 12 буквенно-цифровых символов, введенных с клавиатуры. <p>Комплекс способен прервать процесс открытия сеанса после превышения, установленного администратором МДЗ значения, неуспешных попыток аутентификации пользователя. После прерывания процесса открытия сеанса МДЗ предлагает пользователю выполнить перезагрузку ПЭВМ.</p>	<p>1. п.п. 4.2.2 документа «Аккорд-МКТ. Руководство администратора»;</p> <p>2. п.п. 4.1.2 документа «Аккорд-МКТ. Руководство пользователя».</p>
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 МДЗ осуществляется идентификация стационарных устройств СВТ при процедуре контроля целостности конфигурации технических средств СВТ.	<p>1. п.п. 4.10 документа «Аккорд-МКТ. Руководство администратора»;</p> <p>2. п.п. 4.1.4 документа «Аккорд-МКТ. Руководство пользователя».</p>
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ все	+ все	Управление идентификаторами учетных записей производится в рамках выполнения процедур создания пользователя и группы, модификации пользователя и группы, а также удаления пользователя и группы.	1. п.п. 4.2.2, 4.3.4, 4.12.1 документа «Аккорд-МКТ. 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	+ все	+ все	<p>Управление идентификаторами производится в административном режиме МДЗ в разделе «Пользователи».</p> <p>Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных</p>	1. п.п. 4.2.3, 4.12.1 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		аутентификации			идентификаторов.	
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 отображения вводимых символов аутентификационной информации условными знаками.	1. п.п. 4.1.3 документа «Аккорд-МКТ. 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» либо СПО «Аккорд-X К»).	
		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 МДЗ 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 МКТ в соответствии с установленным для них режимом работы.	1. п.п. 4.3-4.9 документа «Аккорд-МКТ. 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. 4.3.2, 4.3.3 документа «Аккорд-МКТ. Руководство администратора».
9	УПД.4	Разделение полномочий (ролей) пользователей,	+ все	+ все	После прохождения процедуры ИА пользователей, МДЗ определяет дальнейший режим загрузки по	1. п.п. 4.3 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		администраторов и лиц, обеспечивающих функционирование информационной системы			результатам данной процедуры. Администрирование МДЗ может проводить только пользователь, зарегистрированный в 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 МДЗ (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.	
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все	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 обеспечивает блокирование персонального идентификатора, с которого предпринимаются попытки доступа, при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему.	1. п.п. 4.12.1 документа «Аккорд-МКТ. 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	1. п.п. 4.12.1 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
					не был предъявлен, ЭВМ автоматически выключается.	
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. 4.2 документа «Аккорд-МКТ. 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 («Аккорд-Win64 К» либо «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».
16	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники ¹	+ начиная с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС	Комплекс обеспечивает блокировку загрузки операционной системы МДЗ при выявлении попыток загрузки нештатной операционной системы, при превышении числа неудачных попыток аутентификации пользователя, нарушении целостности МДЗ, загружаемой программной среды, при попытках обхода МДЗ, при критичных типах сбоев и ошибок.	1. п.п. 1.1, 4.10 документа «Аккорд-МКТ. 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 («Аккорд-Win64 К» либо «Аккорд-Х К»).	1. п.п. 3.2.7, 3.2.8, 5.2 документа «Аккорд-Х К. Руководство пользователя»; 2. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Защита машинных носителей				

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	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		персональных данных (ЗНИ)				
18	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ начиная с 2 уровня защищенности ПДн	+ все	Доступ к машинным носителям СВТ осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой МДЗ.	
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 («Аккорд-Win64 К» либо «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».
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		1. п.п 3.2.2, 5.2 документа «Аккорд-Х К. Руководство администратора»; 2. п.п. 7.13 документа «Аккорд-Win64 К. 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 точное время регистрации события; – имя пользователя, совершившего событие; – тип операции; – результат события. В случае совместного применения комплекса и СПО разграничения доступа имеется возможность регулирования детальности ведения журнала.	1. п.п. 4.11 документа «Аккорд-МКТ. Руководство администратора»; 2. п.п. 6.1.4 документа «Модуль доверенной загрузки «Аккорд-МКТ». Задание по безопасности».
22	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих	+ все	+ все	При регистрации событий фиксируется исчерпывающий набор параметров: дата и время, идентификатор субъекта, идентификатор объекта, тип выполняемой операции, результат	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		регистрации			операции.	
23	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все	Комплекс обеспечивает выполнение следующих функций безопасности: – регистрация и учет выполнения функций безопасности СДЗ; – сигнализация о событиях, связанных с нарушением безопасности; – начало сеанса пользователя; – прохождение процедуры аутентификации пользователя; – осуществление контроля целостности; – осуществление процедур самоконтроля; – создание журнала системных событий и действий 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	Комплекс обеспечивает реагирование на сбои при регистрации событий безопасности. Если заполнение журнала превышает 85%, при загрузке МДЗ «Аккорд-МКТ» 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 с 2 уровня защищенности ПДн	+ все	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности. Регистрируется дата совершения события, тип события и результат.	
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).	
		Контроль (анализ) защищенности персональных данных (АНЗ)				
27	АНЗ.1	Выявление, анализ уязвимостей информационной	+ все	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений	1. п. 6 документа «Аккорд-МКТ. Формуляр».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		системы и оперативное устранение вновь выявленных уязвимостей			программного обеспечения средств защиты информации. Обновление ПО «Аккорд-МКТ» выполняется в сервисном центре Разработчика ПО.	
28	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Комплекс обеспечивает возможность 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 МДЗ, проверки целостности хранимого выполняемого кода и параметров МДЗ.	1. п.п. 4.16 документа «Аккорд-МКТ. Руководство администратора».
30	АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	Комплекс обеспечивает контроль целостности состава и параметров аппаратной части ПЭВМ, целостность системных областей и файлов на жестком диске.	1. п.п. 4.10 документа «Аккорд-МКТ. Руководство администратора».
31	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	Настраивается в Параметрах Пользователей: Параметры пароля включают в себя следующие поля: – «Минимальная длина» - параметр определяет количество символов, контролируемое при создании и смене пароля. Нельзя ввести пароль меньшей длины. Если предполагается для авторизации пользователя использовать только 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	1. п.п. 4.3.2 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
					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.	
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
32	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС	Комплекс обеспечивает целостность программной среды и контроль аппаратного обеспечения СВТ.	1. п.п. 4.10 документа «Аккорд-МКТ. Руководство администратора».
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	Комплекс поддерживает резервное копирование на отчуждаемый носитель и восстановления базы данных пользователей и списка контролируемых объектов.	1. п.п. 4.14 документа «Аккорд-МКТ. 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 («Аккорд-Win64 К» либо «Аккорд-X К»).	1. п.п. 3.2.6, 3.2.7 документа «Аккорд-X 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	+ 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 комплексом перед стартом.	1. п.п. 4.16 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		отказавших средств и их тестирование				
36	ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	+ начиная с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС	Комплекс поддерживает возможность резервного копирования на отчуждаемый носитель базы данных пользователей и списка контролируемых объектов.	1. п.п. 1.1, 4.14, 4.16 документа «Аккорд-МКТ. Руководство администратора».
37	ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала	+ начиная с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС	Комплекс поддерживает возможность восстановления (путем копирования с отчуждаемого носителя) резервной базы данных пользователей и списка контролируемых объектов.	
		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.».	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		1. п.п. 3.2.6, 3.2.7, 3.2.10, 3.2.12 документа «Аккорд-Х К. Руководство администратора»; 3. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
40	ЗСВ.3	Регистрация событий безопасности в	+ начиная с 3 уровня	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО	1. п.п. 5.3, 5.4 документа «Аккорд-В. Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		виртуальной инфраструктуре	защищенности ПДн		«Аккорд-Win64 К») либо СПО «Аккорд-В.».	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 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 с 2 класса защищенности ИС	В МДЗ «Аккорд-МКТ» реализован ролевой метод разграничения доступа. Пользователи делятся на «Администраторов» комплекса и «Пользователей».	1. п.п. 4.3 документа «Аккорд-МКТ. Руководство администратора».
45	ЗИС.5	Запрет несанкционированной удаленной	не входит в базовый набор	+ все	Обеспечивается при условии совместного применения комплекса с СПО	1. п.п. 3.2.12 документа «Аккорд-Х К. Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств			разграничения доступа («Аккорд-Win64 К» либо «Аккорд-Х К»).	администратора»; 2. 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 с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС	Производится контроль целостности системных областей и файлов на жестком диске.	1. п.п. 4.10 документа «Аккорд-МКТ. 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 общие для пользователей ресурсы информационной системы	нет	+ в 1 классе защищенности ИС	СДЗ обеспечивает недоступность информационного содержания ресурсов СВТ, использовавшихся в процессе работы СДЗ программным обеспечением и данными СДЗ, после завершения работы СДЗ путем его очистки. Конструктивные особенности СДЗ обеспечивают недоступность ресурсов средства доверенной загрузки из программной среды СВТ после завершения работы средства доверенной загрузки.	1. п.п. 5.1.1, 6.1.10 документа «Модуль доверенной загрузки «Аккорд-МКТ». Задание по безопасности».
48	ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	нет	+ все	Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа («Аккорд-Win64 К» либо «Аккорд-Х К»).	1. 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».
		Выявление инцидентов и реагирование на них (ИНЦ)				
49	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищенности	нет	«Аккорд-МКТ» осуществляет регистрацию и учет следующих системных событий и действий пользователей:	1. п.п. 6.1.4 документа «Модуль доверенной загрузки «Аккорд-МКТ». Задание по

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
			ПДн		<ul style="list-style-type: none"> – начало сеанса пользователя; – прохождение процедуры аутентификации пользователем; – осуществление контроля целостности аппаратуры ЭВМ; – осуществление контроля целостности отдельных файлов и программ; – 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. 	безопасности».

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 МДЗ «Аккорд-МКТ»

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-МКТ» (ТУ 26.20.40.140-082-37222406-2019, ТУ 501410-071-37222406-2016).

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 МДЗ «Аккорд-МКТ»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		Идентификация и аутентификация субъектов и				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		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 осуществляется на уровне контроля целостности файлов ОС. Идентификация объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением осуществляется на уровне контроля целостности отдельных файлов и программных средств ЭВМ, в том числе и файлов реестра.	1. п.п. 1.1, 4.10.3 документа «Аккорд-МКТ. 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 («Аккорд-Win64 К»).	1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке».
3	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К», СПО «Аккорд-X К»).	1. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-X К. Руководство администратора»; 2. 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	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		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 К»). Функция «Очищать файл подкачки».	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			Доступ к машинным носителям СВТ осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой МДЗ.	
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 К», СПО «Аккорд-X К»).	1. п.п 3.2.12 документа «Аккорд-X К. Руководство администратора»; 2. 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		МДЗ «Аккорд-МКТ» протоколирует действия пользователей. С помощью раздела (вкладки) «Журнал» можно проанализировать работу каждого пользователя.	1. п.п. 4.11 документа «Аккорд-МКТ. Руководство администратора».
		Защита среды				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
		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. 4.10 документа «Аккорд-МКТ. 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-X К»).	1. п.п. 3.2.12 документа «Аккорд-X 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			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	1. п.п. 4.3.2, 4.12.1, Приложение 3 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	МДЗ «Аккорд-МКТ»	Ссылки на документацию
					<p>выполнить перезагрузку и заново повторить операцию входа в систему.</p> <p>Параметр «Число неверных попыток аутентификации» задает максимальное количество неудачных попыток аутентификации пользователя, при превышении которого происходит блокировка загрузки ОС, а СВТ начинает перезагрузку.</p> <p>Фиксируется корректность алфавита ввода пароля (при использовании некорректных символов на экране появляется сообщение).</p> <p>При превышении установленного количества попыток смены пароля пользователя выполняется перезагрузка компьютера.</p>	
		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			<p>Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К»).</p> <p>При установке меток доступа информация об этом записывается в файл. Данные файл возможно установить этот файл на КЦ.</p>	<p>1. п.п. 7.15.2 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32»;</p> <p>2. документ «Инструкция по созданию изолированной программной среды с использованием утилиты AcTskMng».</p>
14	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			<p>Обеспечивается при условии совместного применения комплекса с СПО разграничения доступа (СПО «Аккорд-Win64 К»).</p>	<p>1. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».</p>
15	ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту	нет		<p>Посредством комплекса возможно:</p> <ul style="list-style-type: none"> – резервное копирование информации в соответствии с мерой ОДТ.4; – контроль безотказного функционирования технических средств ИС в соответствии с мерой ОДТ.3; 	<p>1. п.п. 1.1, 4.14, 4.16 документа «Аккорд-МКТ. Руководство администратора».</p>

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

Итак, путем применения комплекса «Аккорд-МКТ» 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, 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