ВЫПОЛНЕНИЕ МЕР

17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ

ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

ПУТЕМ ПРИМЕНЕНИЯ СПО СЗИ ОТ НСД

«АККОРД-WIN64 K»

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 системы защиты информации от несанкционированного доступа «Аккорд-Win64 К» (СПО СЗИ от НСД «Аккорд-Win64 К», СПО «Аккорд-Win64 К», СПО или комплекс).

СПО СЗИ от НСД «Аккорд-Win64 К» предназначено для применения на ПЭВМ (автономных компьютерах, рабочих станциях ЛВС) и виртуальных машинах, функционирующих под управлением 32 и 64-битных операционных систем семейства Microsoft Windows, в системах терминального доступа, построенных на базе терминальных служб сетевых операционных систем Windows и программного обеспечения Citrix XenApp/XenDesktop версии 7.16, а также в АС, построенных на их основе, в многопользовательском режиме эксплуатации.

СПО может функционировать в СВТ под управлением:

- 64-битных ОС:
  - Windows Server 2012 Enterprise Edition R2;
  - Windows 10 Professional;
  - Windows Server 2016 Enterprise Edition;
  - Windows Server 2019;
- 32-битных ОС:
  - Windows 10 Professional.

2 Выполнение базового набора мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения СПО «Аккорд-Win64 К»

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-Win64 К» (ТУ 26.20.40.140-091-37222406-2020).

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.

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 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-Win64 К»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	Идентификация пользователя производится по логину пользователя или, опционально, по уникальному аппаратному персональному идентификатору пользователя, а аутентификация – по клавиатурному паролю. Длина пароля, задаваемая администратором, определяет стойкость процедур идентификации и аутентификации.	1. п.п. 2.1.1, 2.1.2 документа «Аккорд-Win64 K. Руководство пользователя»; 2. п.п. 7.2-7.4 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
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 СПО СЗИ от НСД «Аккорд-Win64 К» идентификация терминалов, ЭВМ и узлов сети ЭВМ осуществляется по логическим именам. Идентификация внешних устройств и внешних носителей информации производится по Vid, Pid, Sn и типу носителя.	1. п.п. 7.10.1, 7.11.1 Приложение 1 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ все	+ все	Управление идентификаторами учетных записей производится с помощью утилиты ACED32. Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; присвоение, удаление аппаратных идентификаторов.	1. п.п. 7.2-7.4 документа «Аккорд-Win64 K. 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	+ все	+ все	Управление паролями и аппаратными идентификаторами учетных записей пользователей производится с помощью утилиты ACED32. Возможные операции: создание пароля, генерация пароля программой, смена пароля, запись данных в идентификатор, установка	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
		средств аутентификации			времени действия пароля.	
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	При вводе пароля (при входе в ОС, при доступе к модулям СПО СЗИ от НСД), пароль отображается звездочками.	1. п.п. 2.1.2 документа «Аккорд-Win64 К. Руководство пользователя».
6	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+ все	+ все	Идентификация и аутентификация осуществляется по имени пользователя, паролю и аппаратному идентификатору.	1. п.п. 2.1.1, 2.1.2 документа «Аккорд-Win64 К. Руководство пользователя»; 2. п.п. 7.2-7.4 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		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 с помощью утилиты ACED32. Возможные операции с пользователями: создание, удаление, отключение (деактивация) учетной записи, редактирование свойств учетной записи; включение пользователей в группы.	1. п. 5 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
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	Доступ субъектов доступа к ресурсам разграничивается в рамках настройки дискреционного и мандатного доступа. Ролевой метод реализован в виде групп пользователей.	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	Пользователь, установивший систему защиты, обладает всеми полномочиями администрирования (управления) системы защиты и всеми правами по доступу к ресурсам, причем эти права и полномочия в дальнейшем	1. п. 7 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-Win64 К»	Ссылки на документацию
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все	невозможно ограничить. Гл. администратор регистрирует в системе защиты других пользователей. При этом он может делегировать зарегистрированному пользователю все или часть своих полномочий на администрирование СПО СЗИ от НСД «Аккорд-Win64 К». Полномочия на управление СПО СЗИ от НСД «Аккорд-Win64 К» устанавливаются в разделе «Привилегии Администраторов», вкладка «Команды» утилиты ACED32.	1. п. 5, 7 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
11	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+ все	+ все	Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «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 информационной системы	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Для каждой учетной записи комплекса СПО СЗИ от НСД «Аккорд-Win64 К» возможен только один сеанс доступа.	
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	Реализуется в утилите «ACED32», пункт меню *Программная среда/Гашение экрана/пауза в минутах*.	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	До проведения идентификации и аутентификации пользователю запрещены любые действия кроме ввода идентификационной и аутентификационной информации, предъявления аппаратного идентификатора, смены пользователя.	1. п.п. 2.2 документа «Аккорд-Win64 К. Руководство пользователя».
15	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через	+ все	+ все	Реализация защищенного удаленного доступа и контроля доступа из внешних информационных ресурсов возможна за счет включения подсистемы	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-Win64 К»	Ссылки на документацию
		внешние информационно-телекоммуникационные связи			контроля имен общих ресурсов: в утилите AcSetup во вкладке Параметры\Дополнительные\Контроль: Включить подсистему контроля имен общих ресурсов. Установка данного параметра активирует процедуру контроля заданных в редакторе ПРД общих ресурсов, т.е. устройств, папок и файлов данного компьютера, предоставленных в общий доступ пользователям сети и активизирует процедуру контроля доступа к ресурсам данного компьютера из сети. Параметр «Контроль имен общих ресурсов» регламентирует выделение ресурсов данного компьютера в общий доступ с фиксированными именами, а флаг «Контроль доступа к общим ресурсам» включает драйвер, который разрешает или запрещает доступ из внешней сети к ресурсам компьютера на время сеанса работы конкретного пользователя.	
16	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических устройств	+ все	+ все	Контроль использования съемных носителей информации настраивается в утилите ACED32 в разделе «Редактирование правил разграничение доступа»/ «Атрибуты доступа к объектам»/ «Устройства».	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	Мера УПД.17 выполняется при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМДЗ».	1. п.п. 1.1, 3.10 документа «Аккорд-АМДЗ. Руководство администратора».
		Ограничение программной среды (ОПС)				

[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-Win64 К»	Ссылки на документацию
18	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	В СПО СЗИ от НСД «Аккорд-Win64 К» существует механизм настройки изолированной программной среды (ИПС).	1. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения доступа. 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 использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «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	Комплекс позволяет однозначно идентифицировать все имеющиеся в системе устройства, диски и носители информации как по внутренним именам операционной системы, так и по логическим, и задать для них правила доступа. С помощью утилиты ACED32 администратор СПО имеет возможность составить для пользователя список разрешённых устройств (диски, принтеры, файлы устройств и т.п.) и задать права доступа к ним. Для USB-устройств и SD карт список разрешенных устройств формируется на основании их уникальных идентификационных параметров (серийных номеров, классов и типов).	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	+ все	+ все	СПО СЗИ от НСД «Аккорд-Win64 К» включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления	1. п.п. 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-Win64 К»	Ссылки на документацию
		передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания			удаленных данных.	
		Регистрация событий безопасности (РСБ)				
22	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+ все	+ все	Во время каждого сеанса работы пользователя ведется журнал регистрации событий, в котором отображаются действия пользователя, прикладного и системного ПО. Детальность ведения журнала регулируется значением поля «Детальность журнала» в окне параметров пользователя. Регистрация осуществляется в следующем порядке: для каждого пользователя виртуальной инфраструктуры администратор ОО должен установить уровень детальности журнала низкий, средний, высокий; – для любого уровня детальности в журнале отражаются: – параметры регистрации пользователя; – доступ к устройствам; – запуск задач; – попытки нарушения правил доступа; – изменения правил доступа (в частности, изменение паролей); – срабатывание блокировки экрана; – попытки разблокировать экран другим идентификатором. – для среднего уровня детальности в журнале отражаются дополнительно все попытки доступа к	1. документ «Аккорд-Win64 К. Подсистема регистрации. Программы работы с журналами регистрации». 2. п.п. 7.5 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-Win64 К»	Ссылки на документацию
					защищаемым дискам, каталогам и отдельным файлам, а также попытки изменения некоторых системных параметров. Например, даты, времени и др.; – для высокого уровня детальности в журнале отражаются дополнительно все попытки доступа к содержимому защищаемых каталогов.	
23	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ все	+ все	Журнал событий СПО содержит следующую информацию: – дата и точное время регистрации события; – детальность журнала, установленная на момент регистрации события; – имя рабочей станции; – тип операции. В таблице выводится краткая аббревиатура, характеризирующая тип операции; – объект доступа. В таблице выводится полное наименование объекта доступа. Объектом доступа может быть файл, каталог, устройство. Если событием является изменение прав доступа, то в этом поле должны отображаться новые права доступа; – результат события. В ОО регистрируются как положительные, так и отрицательные результаты завершения событий. При отрицательном завершении в качестве результата регистрируется несанкционированный доступ или ошибка доступа; – имя процесса. Это программа, осуществляющая доступ к объекту в момент регистрации события. Для удобства просмотра и анализа в ОО присутствует возможность фильтрации по одному или нескольким полям таблицы.	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
24	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все	Данные аудита хранятся в системной папке C:\ACCORDx64 файлы журналов событий сохраняются в специальный файл *LOW и доступны к просмотру только администратору комплекса через утилиту LOGVIEW. Предоставляется возможность просмотра, вывода на печать и архивации журнала регистрации событий изделия. Журнал отображается в виде таблицы. Каждая строка таблицы соответствует одному событию, зарегистрированному в журнале.	
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 использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «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	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и очистку журнала.	
27	РСБ.7	Защита информации о событиях безопасности	+ все	+ все	Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий. Доступ к записям аудита и функциям управления механизмами регистрации	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
					(аудита) предоставляется только уполномоченным должностным лицам.	
		Контроль (анализ) защищенности персональных данных (АН3)				
28	АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ все	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации. Обновление СПО выполняется эксплуатирующей организацией в соответствии с ТУ и п. 2.1 документа «Руководство по установке» на комплекс.	1. п.п. 2.1 документа «Аккорд-Win64 К. Руководство по установке».
29	АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения СЗИ от НСД	
30	АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ все	Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМДЗ».	1. п.п. 3.1, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».
31	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	Производится контроль целостности средств защиты информации по контрольным суммам всех компонентов средств защиты информации динамически в процессе работы системы. Контроль целостности изделия реализуется: – проверкой целостности назначенных для контроля пользовательских программ и данных; — механизмом создания изолированной программной среды, запрещающей запуск привнесенных программ.	1. п.п. 7.10 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-Win64 К»	Ссылки на документацию
32	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 о 2 уровня защищенности ПДн	+ все	Настраивается в Параметрах Пользователей/Параметры пароля в утилите в утилите ACED32: Параметры пароля включают в себя: – «Длина пароля» - минимальная длина пароля – 0 (пароль задавать не обязательно), максимальная - 12 символов. – «Время действия» - время действия пароля до смены: от 0 (нет смены пароля) до 366 дней. – «Попыток для смены» - количество попыток смены пароля: от 0 (бесконечное) до 5. – «Кто может менять пароль» - установка прав на смену пароля (только администратор или администратор и пользователь). – «Дополнительные параметры»: «Биометрические данные, с качеством (%)» - этот флаг устанавливается в случае применения биометрической идентификации по отпечатку пальца или сосудистому руслу руки (см. раздел «Особенности работы утилиты «Настройка идентификаторов СЗИ Аккорд» Руководства по установке) и определяет процент совпадения предъявляемых биометрических данных с установленным эталонным значением. – «Алфавит для пароля» - определяет набор символов, из которых может состоять пароль пользователя. Если установлен флаг в одном или нескольких полях, то наличие хотя бы одного символа данной последовательности обязательно при вводе пароля. При установке флага «Только генерировать» пароль будет генерироваться случайным образом из	1. п.п. 7.3, 7.4 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-Win64 К»	Ссылки на документацию
					символов заданного алфавита при смене пароля пользователя..	
		Обеспечение целостности информационной 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	В комплексе «Аккорд-Win64 К» предусмотрен динамический контроль целостности исполняемых модулей (задач). Этот контроль выполняется при каждом запуске контролируемого модуля, независимо от того, выполняется ли эта операция пользователем, или операционной системой. Как и на других этапах контроля целостности, здесь применяется контроль с использованием хэш-функции. Дополнительно в комплексе «Аккорд-Win64 К» предусмотрен динамический контроль целостности монитора разграничения доступа. Этот контроль выполняется периодически и обеспечивает дополнительный уровень защиты от случайных или преднамеренных покушений на отключение комплексе «Аккорд-Win64 К» средств защиты.	1. п.п. 7.10 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
34	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 базы данных путем копирования резервной базы в папку Accord.x64 (файл accord.amz).	1. п.п. 7.15 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
35	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Реализуется дискреционным и мандатным доступом к файлам документов.	1. 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-Win64 К»	Ссылки на документацию
		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 использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМДЗ» за счет функции самотестирования.	1. п.п. 3.16 документа «Аккорд-АМДЗ. 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	Комплексом обеспечивается периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов). Выполняется в утилите ACED32: Файл\Сохранить как – экспорт базы данных пользователей; Файл\Экспорт ПРД – экспорт ПРД пользователей.	1. п.п. 7.15.1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
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	Комплексом обеспечивается возможность восстановления информации (базы данных пользователей и списка контролируемых объектов) из резервных копий. Выполняется в утилите ACED32: Файл\Импорт базы – импорт базы данных пользователей; Файл\Импорт ПРД – импорт ПРД пользователей.	
		Защита среды виртуализации (ЗСВ)				
39	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в	+ все	+ все	В комплексе обеспечивается идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной	1. п.п. 2.1.1, 2.1.2 документа «Аккорд-Win64 К. Руководство пользователя»;

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
		том числе администраторов управления средствами виртуализации			инфраструктуре.	
40	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+ все	+ все	В комплексе обеспечивается управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре.	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 защищённости ПДн	+ все	Регистрация осуществляется в следующем порядке: – для каждого пользователя виртуальной инфраструктуры администратор ОО должен установить уровень детальности журнала низкий, средний, высокий; – для любого уровня детальности в журнале отражаются: – параметры регистрации пользователя; – доступ к устройствам; – запуск задач; – попытки нарушения правил доступа; – изменения правил доступа (в частности, изменение паролей); – срабатывание блокировки экрана; – попытки разблокировать экран другим идентификатором. – для среднего уровня детальности в журнале отражаются дополнительно все попытки доступа к защищаемым дискам, каталогам и отдельным файлам, а также попытки изменения некоторых системных параметров. Например, даты, времени и др.; — для высокого уровня детальности в журнале отражаются дополнительно все попытки доступа к содержимому защищаемых каталогов.	1. документ «Аккорд-Win64 К. Подсистема регистрации. Программы работы с журналами регистрации».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
42	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Комплекс обеспечивает выполнение контроля целостности виртуальной инфраструктуры.	1. п.п. 7.10 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
43	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	Имеется возможность разделения функций по управлению информационной системой посредством создания отдельных групп пользователей с возможностью задания для каждой группы отдельных прав по управлению комплексом (задается в программе ACED32).	1. п.п. 7 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
44	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	Возможно исключение несанкционированного использования USB-принтеров – регулируется посредством назначения пользователю (или группе пользователей) соответствующих правил разграничения доступа.	1. п.п. 7.11.1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
45	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 СПО и всех компонентов. Возможен контроль целостности файлов других приложений, файлов с данными и пр.	1. п.п. 7.10 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-Win64 К»	Ссылки на документацию
46	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	Имеется возможность исключения доступа через общие ресурсы за счет установки параметров: «Удаление файлов с очисткой» в дополнительных опциях пользователя. (При удалении файлы сразу очищаются в корзине). «Число проходов при очистке файлов» – этим параметром задается количество циклов заполнения случайными данными области на жестком диске, занимаемой удаляемым файлом. «Очищать файлы, начиная с уровня» - параметр работает при включенном механизме мандатного доступа, когда требуется очищать остаточную информацию для файлов с определенного уровня конфиденциальности. «Очищать файл подкачки» – включение этого параметра означает, что файл подкачки (виртуальная память ОС) будет очищен при завершении сеанса работы пользователя.	1. п.п. Приложение 1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
47	ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	нет	+ все	Обеспечивается контроль и мониторинг применения мобильных технических средств (съемных носителей информации) на предмет выявления их несанкционированного использования для доступа к объектам доступа ИС.	1. п.п. 7.16 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Выявление инцидентов и реагирование на них (ИНЦ)				
48	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищенности ПДн	нет	Комплекс обеспечивает фиксацию операций с файлами и каталогами, ключами реестра, событий хранителя экрана и проверки файлов, Имеется возможность установки параметров 1. «Выводить на экран сообщения о НСД» - сообщения об НСД будут	1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке»; 2. Приложение 2 «Аккорд-Win64 К. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Win64 К»	Ссылки на документацию
					выводиться сначала от имени СЗИ «Аккорд», а потом будут дублироваться отказами системы. В обычном режиме СЗИ «Аккорд» генерирует код ошибки, передает его системным службам, и все отказы в доступе выводятся на уровне стандартного интерфейса ОС. 2. «Мягкий режим. В этом режиме при обращении к запрещенному (недоступному) ресурсу системой «Аккорд» выводится сообщение об НСД, если включен параметр «Выводить на экран сообщения о НСД», попытка НСД заносится в журнал регистрации событий, но выполнение операции не прерывается.	

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-Win64 К»

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 Win64 К» (ТУ 26.20.40.140-091-37222406-2020).

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.

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 Win64 К»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд Win64 К»	Ссылки на документацию
		Идентификация и аутентификация субъектов и				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд Win64 K»	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 объектов осуществляется по полному абсолютному пути в файловой системе. Для объектов файловой системы возможно использование контроля целостности. Идентификация и аутентификация объектов систем управления базами данных не поддерживается.	1. п.п. 7.10 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
		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			Администратор может настроить функцию предупреждения пользователя об НСД: в утилите AcSetup выбрать пункт меню Параметры\Дополнительные\Разное\Выводить на экран сообщения о НСД. Включение этого параметра означает, что сообщения об НСД будут выводиться сначала от имени СЗИ «Аккорд», а потом будут дублироваться отказами системы. При возникновении НСД СПО «Аккорд-Win64 K» генерирует код ошибки, передает его системным службам, и все отказы в доступе выводятся на уровне стандартного интерфейса ОС.	1. п.п. 2.1.5 документа «Аккорд-Win64 K. Руководство по установке».
3	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			В процессе хранения и обработки информации сохраняются все необходимые атрибуты (метки) безопасности с помощью возможностей дискреционного и мандатного доступа. Метки конфиденциальности при настройке мандатного доступа при перемещении	1. п.п. 7.11 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд Win64 K»	Ссылки на документацию
					файлов сохраняются за счет назначения метки на папку (каталог).	
		Ограничение программной среды (ОПС)				
4	ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			Реализуется за счет опции «Очищать файл подкачки». Данный флаг устанавливается в утилите AcSetup во вкладке Параметры\Дополнительные\Разное\Очищать файл подкачки. Включение этого параметра означает, что файл подкачки (виртуальная память ОС) будет очищен при завершении сеанса работы пользователя.	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			Обеспечивается при условии совместного использования СПО «Аккорд-Win64 K» и модуля доверенной загрузки «Аккорд-АМДЗ». 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			Комплекс позволяет однозначно идентифицировать все имеющиеся в системе устройства, диски и носители информации как по внутренним именам операционной системы, так и по логическим, и задать для них правила доступа. С помощью утилиты ACED32 администратор СПО имеет возможность составить для пользователя список разрешённых устройств (диски, принтеры, файлы	1. п.п. 7.16 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
7	ЗНИ.7	Контроль подключения машинных носителей персональных данных				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд Win64 K»	Ссылки на документацию
					устройств и т.п.) и задать права доступа к ним. Для USB-устройств и SD карт список разрешенных устройств формируется на основании их уникальных идентификационных параметров (серийных номеров, классов и типов).	
		Регистрация событий безопасности (РСБ)				
8	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	нет		СПО СЗИ от НСД «Аккорд-Win64 K» протоколирует работу о каждой сессии конкретного в отдельный файл. С помощью утилиты LOGVIEW и применением различных фильтров можно проанализировать работу каждого пользователя.	1. п.п. 7.5 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32»; 2. документ «Аккорд-Win64 K. Подсистема регистрации. Программы работы с журналами регистрации».
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
9	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. 7.10 документа «Аккорд-Win64 K. 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 исключение неправомерной передачи информации из информационной			С помощью СПО «Аккорд-Win64 K» возможно: – выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации и реагирование на них; — выявление фактов неправомерного вывода на печать документов, содержащих защищаемую информацию, и реагирование на них.	1. п.п. 5.2, 7.13 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд Win64 K»	Ссылки на документацию
		системы				
11	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях			Администратор может настроить функцию предупреждения пользователя при его доступе к информационным ресурсам: в утилите AcSetup выбрать пункт меню Параметры\Дополнительные\Разное\Выводить на экран сообщения о НСД. При ошибочных действия пользователя возникают предупреждения сначала от имени СЗИ «Аккорд», а потом будут дублироваться отказами системы. При превышении установленного количества попыток авторизации учетная запись пользователя блокируется. Фиксируется корректность алфавита ввода пароля (при использовании некорректных символов на экране появляется сообщение). При превышении установленного количества попыток смены пароля учетная запись пользователя блокируется. Загрузка системы произойдет только после вмешательства Администратора БИ.	1. п.п. 2.1.5 документа «Аккорд-Win64 K. Руководство по установке».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
12	ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с			При установке меток доступа информация об этом записывается в файл. Данный файл возможно установить 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».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд Win64 K»	Ссылки на документацию
		иными информационными системами				
13	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			В СПО СЗИ от НСД «Аккорд-Win64 K» осуществляется изоляция процессов (выполнение программ) в выделенной области памяти. Изоляция процессов (выполнение программ) в выделенной области памяти должна обеспечивать недоступность областей памяти, используемых процессами (программами), выполняемыми от имени одного пользователя, для процессов (программ), исполняемых от имени другого пользователя. Изоляция процессов (выполнение программ) в выделенной области памяти реализуется в средствах вычислительной техники, определенных оператором, и как минимум должна включать изоляцию процессов, связанных с выполнением функций безопасности средств защиты информации.	1. п.п. 7.12 документа «Аккорд-Win64 K. Установка правил разграничения доступа. Программа ACED32».
14	ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы	нет		Обеспечивается при условии совместного использования СПО «Аккорд-Win64 K» и модуля доверенной загрузки «Аккорд-АМДЗ».	1. п.п. 3.14, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».

Итак, путем применения СПО «Аккорд-Win64 K» 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, 7;
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;
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