

**ВЫПОЛНЕНИЕ МЕР
31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В
АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ
ПУТЕМ ПРИМЕНЕНИЯ
СПО СЗИ ОТ НСД «АККОРД-WIN64 К»**

ОКБ САПР

2021

1 Общие положения

В настоящем документе рассматривается выполнение мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения специального программного обеспечения «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.

1 Выполнение базового набора мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения СПО «Аккорд-Win64 К»

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СПО «Аккорд-Win64 К» (ТУ 26.20.40.140-091-37222406-2020).

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

Таблица 1 – Выполнение базового набора мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СПО «Аккорд-Win64 К»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			
1	ИАФ.0	Разработка политики и аутентификации	+ все	В комплексе разработана политика идентификации и аутентификации.	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
2	ИАФ.1	Идентификация и аутентификация пользователей и иницируемых ими процессов	+ 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 К. Руководство пользователя»; 2. п.п. 7.2-7.4 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
3	ИАФ.2	Идентификация и аутентификация устройств	+ все	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 К. Установка правил разграничения доступа. Программа ACED32».
4	ИАФ.3	Управление идентификаторами	+ 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 К. Установка правил разграничения доступа. Программа ACED32».
5	ИАФ.4	Управление средствами аутентификации	+ 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 времени действия пароля.	
6	ИАФ.5	Идентификация и аутентификация внешних пользователей	+ 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».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
7	ИАФ.7	Защита аутентификационной информации при передаче	+ 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».
		Управление доступом (УПД)			
8	УПД.0	Разработка политики управления доступом	+ все	В комплексе разработана политика управления доступом.	
9	УПД.1	Управление учетными записями пользователей	+ 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».
10	УПД.2	Реализация политик управления доступом	+ 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».
11	УПД.3	Доверенная загрузка	+ начиная со 2 класса защищенности автоматизированной системы управления	Выполняется при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМД3».	1. п.п. 1.1, 3.10 документа «Аккорд-АМД3. Руководство администратора».
12	УПД.4	Разделение полномочий (ролей) пользователей	+ 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 невозможно ограничить.	1. п. 7 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
13	УПД.5	Назначение минимально необходимых прав и привилегий	+ все	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».
14	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+ все	Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМД3».	1. п.п. 3.12.1 документа «Аккорд-АМД3. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
15	УПД.9	Ограничение числа параллельных сеансов доступа	+ в 1 классе защищенности автоматизированной системы управления	Для каждой учетной записи комплекса СПО СЗИ от НСД «Аккорд-Win64 К» возможен только один сеанс доступа.	
16	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+ все	Реализуется в утилите «ACED32», пункт меню <i>Программная среда/Гашение экрана/пауза в минутах.</i>	1. п. 7.6 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
17	УПД.11	Управление действиями пользователей до идентификации и аутентификации	+ 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».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
18	УПД.13	Реализация защищенного удаленного доступа	+ все	<p>Реализация защищенного удаленного доступа и контроля доступа из внешних информационных ресурсов возможна за счет включения подсистемы контроля имен общих ресурсов: в утилите AcSetup во вкладке Параметры\Дополнительные\Контроль: Включить подсистему контроля имен общих ресурсов.</p> <p>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 активирует процедуру контроля доступа к ресурсам данного компьютера из сети.</p> <p>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.</p>	1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке».
		Ограничение программной среды (ОПС)			
19	ОПС.0	Разработка политики ограничения программной среды	+ начиная со 2 класса защищенности автоматизированной системы управления	В СПО СЗИ от НСД «Аккорд-Win64 К» существует механизм настройки изолированной программной среды (ИПС).	
20	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ в 1 классе защищенности		1. п.п. 7.12 документа «Аккорд-Win64 К. Установка правил разграничения

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
			автоматизированной системы управления		доступа. Программа ACED32».
		Защита машинных носителей информации (ЗНИ)			
21	ЗНИ.0	Разработка политики защиты машинных носителей информации	+ все	СПО СЗИ от НСД «Аккорд-Win64 К» поддерживает политику защиты машинных носителей информации в части обеспечения контроля использования интерфейсов ввода (вывода) информации на машинные носители информации, контроля ввода (вывода) информации на машинные носители информации, контроля подключения машинных носителей информации, а также уничтожения (стирания) информации	
22	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ все	Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМД3».	
23	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ все	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.	1. п.п. 7.16 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
24	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	+ в 1 классе защищенности автоматизированной системы управления		
25	ЗНИ.7	Контроль подключения машинных носителей информации	+ все	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).	
26	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+ все	СПО СЗИ от НСД «Аккорд-Win64 К» включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.	1. п.п. 7.13 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Аудит безопасности (АУД)			
27	АУД.0	Разработка политики аудита безопасности	+ все	СПО СЗИ от НСД «Аккорд-Win64 К» поддерживает	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
				политику аудита безопасности в части обеспечения регистрации событий безопасности, защиты информации о событиях безопасности и анализа действий пользователей	
28	АУД.2	Анализ уязвимостей и их устранение	+ 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	АУД.4	Регистрация событий безопасности	+ 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. Возможны следующие значения детальности: <ul style="list-style-type: none"> • «Нет» - регистрация только входа/выхода из системы и событий НСД. • «Низкая» - регистрация входа/выхода из системы, попыток несанкционированного доступа, запуска исполняемых модулей, событий СЗИ. • «Средняя» - то же, что при низкой детальности, плюс операции доступа к файлам и каталогам. • «Высокая» - то же, что и при средней детальности плюс все файловые операции, включая параметры кома. • «Сбор статистики» - то же, что и при высокой детальности журнала, кроме того для пользователя не действуют установленные правила разграничения доступа. 	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».
30	АУД.6	Защита информации о событиях безопасности	+ все	Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
				<p>неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.</p> <p>Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам.</p>	
31	АУД.7	Мониторинг безопасности	+	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и очистку журнала.	<p>1. документ «Аккорд-Win64 К. Подсистема регистрации. Программы работы с журналами регистрации».</p> <p>2. п.п. 7.5 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».</p>
32	АУД.8	Реагирование на сбои при регистрации событий безопасности	+	Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМД3» за счет функции самотестирования.	1. п.п. 3.11 документа «Аккорд-АМД3. Руководство администратора».
33	АУД.9	Анализ действий пользователей	+	<p>СПО СЗИ от НСД «Аккорд-Win64 К» протоколирует работу о каждой сессии конкретного в отдельный файл.</p> <p>С помощью утилиты LOGVIEW и применением различных фильтров можно проанализировать работу каждого пользователя.</p>	<p>1. документ «Аккорд-Win64 К. Подсистема регистрации. Программы работы с журналами регистрации».</p> <p>2. п.п. 7.5 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».</p>
		Обеспечение целостности (ОЦП)			
34	ОЦП.0	Разработка политики обеспечения целостности	+	В комплексе реализована политика обеспечения целостности	
35	ОЦП.1	Контроль целостности программного обеспечения	+	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	1. п.п. 7.10 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
				<p>на других этапах контроля целостности, здесь применяется контроль с использованием хэш-функции.</p> <p>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 комплекса «Аккорд-Win64 К» средств защиты.</p>	
36	ОЦЛ.3	Ограничение по вводу информации в информационную (автоматизированную) систему	+ в 1 классе защищенности автоматизированной системы управления	Реализуется дискреционным и мандатным доступом к файлам документов.	1. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
37	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+ начиная со 2 класса защищенности автоматизированной системы управления	<p>С помощью СПО «Аккорд-Win64 К» возможно:</p> <ul style="list-style-type: none"> – 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 К. Установка правил разграничения доступа. Программа ACED32».
38	ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+ начиная со 2 класса защищенности автоматизированной системы управления	<p>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.</p> <p>При ошибочных действиях пользователя возникают предупреждения сначала от имени СЗИ «Аккорд», а потом будут дублироваться отказами системы.</p> <p>При превышении установленного количества попыток авторизации учетная запись пользователя блокируется.</p> <p>Фиксируется корректность алфавита ввода пароля (при использовании некорректных</p>	1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
				<p>символов на экране появляется сообщение).</p> <p>При превышении установленного количества попыток смены пароля учетная запись пользователя блокируется.</p> <p>Загрузка системы произойдет только после вмешательства Администратора БИ.</p>	
		Обеспечение доступности (ОДТ)			
39	ОДТ.0	Разработка политики обеспечения доступности	+ все	Комплекс поддерживает политики обеспечения доступности в части обеспечения резервного копирования конфигурации СЗИ от НСД и восстановления СЗИ от НСД из резервной копии.	
40	ОДТ.3	Контроль безотказного функционирования средств и систем	+ начиная со 2 класса защищенности автоматизированной системы управления	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».
41	ОДТ.4	Резервное копирование информации	+ все	<p>Комплексом обеспечивается периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов).</p> <p>Выполняется в утилите ACED32:</p> <p>Файл\Сохранить как – экспорт базы данных пользователей;</p> <p>Файл\Экспорт ПРД – экспорт ПРД пользователей.</p>	1. п.п. 7.15.1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
42	ОДТ.5	Обеспечение возможности восстановления информации	+ все	<p>Комплексом обеспечивается возможность восстановления информации (базы данных пользователей и списка контролируемых объектов) из резервных копий.</p> <p>Выполняется в утилите ACED32:</p> <p>Файл\Импорт базы – импорт базы данных пользователей;</p> <p>Файл\Импорт ПРД – импорт ПРД пользователей.</p>	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
43	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+ все	Комплекс обеспечивает защиту информационной (автоматизированной) системы и ее компонентов в	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
				части изоляции процессов в выделенной области памяти, защиты неизменяемых данных	
44	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+ все	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».
45	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 класса защищенности автоматизированной системы управления	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».
46	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+ 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».
47	ЗИС.33	Исключение доступа через общие ресурсы	+ в 1 классе защищенности автоматизированной системы управления	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».
48	ЗИС.38	Защита информации при использовании мобильных устройств	+ все	Обеспечивается контроль и мониторинг применения мобильных технических	1. п.п. 7.16 документа «Аккорд-Win64 К. Установка правил

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
				средств (съемных носителей информации) на предмет выявления их несанкционированного использования для доступа к объектам доступа ИС.	разграничения доступа. Программа ACED32».
		Реагирование на компьютерные инциденты (ИНЦ)			
49	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+ все	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 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.	
50	ИНЦ.1	Выявление компьютерных инцидентов	+ все		1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке»;
51	ИНЦ.2	Информирование о компьютерных инцидентах	+ все		2. Приложение 2 «Аккорд-Win64 К. Руководство администратора».
		Управление обновлениями программного обеспечения (ОПО)			
52	ОПО.0	Разработка политики управления обновлениями программного обеспечения	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения СЗИ от НСД.	
53	ОПО.4	Установка обновлений программного обеспечения	+ все	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».
		Обеспечение действий в нештатных ситуациях (ДНС)			
54	ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
55	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций	+ начиная со 2 класса защищенности автоматизированной системы управления	<p>Реализована функция сохранения резервной копии базы данных путем копирования резервной базы в папку Accord.x64 (файл accord.amz).</p> <p>Комплексом обеспечивается периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов).</p> <p>Выполняется в утилите ACED32:</p> <p>Файл\Сохранить как – экспорт базы данных пользователей;</p> <p>Файл\Экспорт ПРД – экспорт ПРД пользователей.</p>	1. п.п. 7.15 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
56	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+ все	<p>Комплексом обеспечивается возможность восстановления информации (базы данных пользователей и списка контролируемых объектов) из резервных копий.</p> <p>Выполняется в утилите ACED32:</p> <p>Файл\Импорт базы – импорт базы данных пользователей;</p> <p>Файл\Импорт ПРД – импорт ПРД пользователей.</p>	

2 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения СПО «Аккорд-Win64 К»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СПО «Аккорд Win64 К» (ТУ 26.20.40.140-091-37222406-2020).

Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СПО «Аккорд Win64 К»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
---	-------------	--	---	------------------	------------------------

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
		Управление доступом (УПД)			
1	УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам		<p>Администратор может настроить функцию предупреждения пользователя об НСД: в утилите AcSetup выбрать пункт меню Параметры\Дополнительные\Разное\Выводить на экран сообщения о НСД.</p> <p>Включение этого параметра означает, что сообщения об НСД будут выводиться сначала от имени СЗИ «Аккорд», а потом будут дублироваться отказами системы.</p> <p>При возникновении НСД СПО «Аккорд-Win64 К» генерирует код ошибки, передает его системным службам, и все отказы в доступе выводятся на уровне стандартного интерфейса ОС.</p>	1. п.п. 2.1.5 документа «Аккорд-Win64 К. Руководство по установке».
2	УПД.12	Управление атрибутами безопасности		<p>В процессе хранения и обработки информации сохраняются все необходимые атрибуты (метки) безопасности с помощью возможностей дискреционного и мандатного доступа.</p> <p>Метки конфиденциальности при настройке мандатного доступа при перемещении файлов сохраняются за счет назначения метки на папку (каталог).</p>	1. п.п. 7.11 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Ограничение программной среды (ОПС)			
3	ОПС.3	Управление временными файлами		<p>Реализуется за счет опции «Очищать файл подкачки».</p> <p>Данный флаг устанавливается в утилите AcSetup во вкладке Параметры\Дополнительные\Разное\Очищать файл подкачки.</p> <p>Включение этого параметра означает, что файл подкачки (виртуальная память ОС) будет очищен при завершении сеанса работы пользователя.</p>	1. п.п. Приложение 1 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32».
		Защита машинных носителей информации (ЗНИ)			
4	ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных		Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
		носителях информации		модуля доверенной загрузки «Аккорд-АМДЗ». Доступ к машинным носителям СВТ осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «Аккорд-АМДЗ».	
		Обеспечение целостности (ОЦЛ)			
5	ОЦЛ.2	Контроль целостности информации		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 К. Установка правил разграничения доступа. Программа ACED32».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
6	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		В СПО СЗИ от НСД «Аккорд-Win64 К» 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 К. Установка правил разграничения доступа. Программа ACED32».
7	ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами		При установке меток доступа информация об этом записывается в файл. Данные файл возможно установить на КЦ и есть возможность установить этот файл на КЦ.	1. п.п. 7.15.2 документа «Аккорд-Win64 К. Установка правил разграничения доступа. Программа ACED32»; 2. документ «Инструкция по созданию

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности автоматизированной системы управления	«Аккорд Win64 К»	Ссылки на документацию
					изолированной программной среды с использованием утилиты AcTskMng.
8	ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)		Обеспечивается при условии совместного использования СПО «Аккорд-Win64 К» и модуля доверенной загрузки «Аккорд-АМДЗ».	1. п.п. 3.14, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».

Итак, путем применения СПО «Аккорд-Win64 К» в автоматизированной системе управления выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 3, 4, 5, 7;

УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11, 13;

ОПС: 1;

ЗНИ: 2, 5, 6, 7, 8;

АУД: 2, 4, 6, 7, 8, 9;

ОЦЛ: 1, 3, 4, 5;

ОДТ: 3, 4, 5;

ЗИС: 1, 13, 21, 33, 38;

ИНЦ: 1, 2;

ОПО: 4;

ДНС: 4, 5;

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

УПД: 7, 12;

ОПС: 3;

ЗНИ: 4;

ОЦЛ: 2;

ЗИС: 12, 22, 37.

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