ВЫПОЛНЕНИЕ МЕР
31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ СПО «АККОРД-KVM»

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-KVM».

Функциональные возможности СПО «Аккорд-KVM» (СПО «Аккорд-KVM», СПО либо комплекс) позволяют применять его для защиты виртуальных инфраструктур, построенных на базе KVM и использующих библиотеку libvirt в качестве инструмента управления гипервизором.

Специальное программное обеспечение «Аккорд-KVM», устанавливаемое в ОС сервера, включает в себя:

– программный модуль accordkvm, отвечающий за контроль целостности виртуальных машин и их компонентов;

– программный модуль qemu, отвечающий за перехват старта виртуальных машин.

СПО «Аккорд-KVM» соответствует требованиям документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденным приказом ФСТЭК России от 2 июня 2020 г №76 по 4 уровню доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

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

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СПО «Аккорд-KVM» (ТУ 501410-073-37222406-2018).

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-KVM»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			
1	ИАФ.0	Разработка политики идентификации и аутентификации	+ все		
2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+ все	Обеспечивается средствами комплекса «Аккорд-Х К».	1. п.п. 3.10, 3.12 документа «Аккорд-АМДЗ. Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
					администратора»; 2. п.п. 3.2.9 документа «Аккорд-X K. Руководство администратора».
3	ИАФ.2	Идентификация и аутентификация устройств	+ все	Обеспечивается средствами модуля доверенной загрузки из состава ПАК «Аккорд-X» («Аккорд-XL»), а также за счет применения комплекса «Аккорд-X K».	1. п.п. 3.10, 3.12 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-X K. Руководство администратора».
4	ИАФ.3	Управление идентификаторами	+ все	Обеспечивается средствами комплекса «Аккорд-X K».	1. п.п. 3.2.3 документа «Аккорд-X K. Руководство администратора».
5	ИАФ.4	Управление средствами аутентификации	+ все		1. п.п. 3.2.2, 3.2.3 документа «Аккорд-X K. Руководство администратора».
6	ИАФ.5	Идентификация и аутентификация внешних пользователей	+ все		
7	ИАФ.7	Защита аутентификационной информации при передаче	+ все		
		Управление доступом (УПД)			
8	УПД.0	Разработка политики управления доступом	+ все	Обеспечивается средствами комплекса «Аккорд-X K».	
9	УПД.1	Управление учетными записями пользователей	+ все		1. п.п. 3.2.2, 3.2.3 документа «Аккорд-X K. Руководство администратора».
10	УПД.2	Реализация политик управления доступом	+ все		1. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-X K. Руководство администратора».
11	УПД.3	Доверенная загрузка	+ начиная со 2 класса защищенности автоматизированной системы управления	Мера УПД.3 выполняется при условии совместного применения «Аккорд-KVM» и ПАК «Аккорд-X» (или «Аккорд-XL») за счет наличия в составе комплекса модуля доверенной загрузки «Аккорд-АМДЗ».	1. п.п. 1.1, 3.10 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п 3.1 документа «Аккорд-АМДЗ. Руководство пользователя».
12	УПД.4	Разделение полномочий (ролей) пользователей	+ все	Обеспечивается средствами комплекса «Аккорд-X K».	1. п.п. 3.2.4-3.2.7 документа «Аккорд-X K. Руководство администратора».
13	УПД.5	Назначение минимально	+		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
		необходимых прав и привилегий	все		
14	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+ все		1. п.п. 3.2.9 документа «Аккорд-X K. Руководство администратора».
15	УПД.9	Ограничение числа параллельных сеансов доступа	+ начиная с 1 класса защищенности автоматизированной системы управления		1. п.п. 3.2.2 документа «Аккорд-X K. Руководство администратора».
16	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+ все		1. п.п. 3.2.9 документа «Аккорд-X K. Руководство администратора».
17	УПД.11	Управление действиями пользователей до идентификации и аутентификации	+ все		1. п.п. 2.2 документа «Аккорд-X K. Руководство пользователя».
		Ограничение программной среды (ОПС)			
18	ОПС.0	Разработка политики ограничения программной среды	+ начиная со 2 класса защищенности автоматизированной системы управления	Обеспечивается средствами комплекса «Аккорд-X K».	
19	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ начиная с 1 класса защищенности автоматизированной системы управления		1. п.п 3.2.7, 3.2.8, 5.2 документа «Аккорд-X K. Руководство пользователя».
		Защита машинных носителей информации (ЗНИ)			
20	ЗНИ.0	Разработка политики защиты машинных носителей информации	+ все	Обеспечивается средствами комплекса «Аккорд-X K».	
21	ЗНИ.2	Управление физическим доступом к машинным носителям информации	+ все	Обеспечивается средствами модуля доверенной загрузки из состава ПАК «Аккорд-X» («Аккорд-XL»), а также за счет применения комплекса «Аккорд-X K».	
22	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ все		1. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора».
23	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	+ начиная с 1 класса защищенности автоматизированной системы управления		
24	ЗНИ.7	Контроль подключения машинных носителей информации	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
25	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+ все		1. п.п 3.2.2, 5.2 документа «Аккорд-X K. Руководство администратора».
		Аудит безопасности (АУД)			
26	АУД.0	Разработка политики аудита безопасности	+ все	В комплексе реализована политика аудита безопасности в части регистрации событий безопасности и защиты событий безопасности информации.	
27	АУД.2	Анализ уязвимостей и их устранение	+ все	Обеспечивается за счет применения комплексов «Аккорд-X», «Аккорд-XL» (в составе которых имеется модуль доверенной загрузки) и «Аккорд-X K».	1. п. 3 документа «Аккорд-X. Руководство администратора»; 2. п. 3 документа «Аккорд-X K. Руководство администратора»; 3. п. 6 документа «Аккорд-АМДЗ. Формуляр».
28	АУД.4	Регистрация событий безопасности	+ все	СПО «Аккорд-KVM» в процессе работы производит регистрацию следующих событий безопасности: – о запуске и остановке СПО «Аккорд-KVM», а также сообщения о получении информации о режиме работы СПО «Аккорд-KVM»; – о создании базы данных; – о настройке режима работы СПО «Аккорд-KVM»; – об добавлении/удалении ВМ и её компонентов на контроль; – о проведении проверок целостности ВМ или её компонентов, в том числе о нарушениях целостности; – о включении ВМ; – о выключении ВМ; – об ошибках в СПО «Аккорд-KVM».	1. п. 4 документа «Аккорд-KVM. Руководство администратора».
29	АУД.6	Защита информации о событиях	+	Обеспечивается за счет	1. п.п. 4.4 документа

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
		безопасности	все	применения комплексов «Аккорд-X K».	«Аккорд-X K. Руководство администратора»;
30	АУД.7	Мониторинг безопасности	+ все	Для обеспечения возможности мониторинга работы СПО «Аккорд-KVM» с виртуальными машинами в СПО ведется журнал регистрации событий.	1. п. 4 документа «Аккорд-KVM. Руководство администратора».
31	АУД.8	Реагирование на сбои при регистрации событий безопасности	+ все	Обеспечивается средствами модуля доверенной загрузки из состава ПАК «Аккорд-X» («Аккорд-XL»), а также за счет применения комплекса «Аккорд-X K».	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».
32	АУД.9	Анализ действий пользователей	+ начиная с 1 класса защищенности автоматизированной системы управления	В журнале событий обеспечена возможность просмотра действий пользователя по настройке СПО «Аккорд-KVM» и результатов проверок целостности ВМ и её компонент в момент запуска или миграции.	1. п. 4 документа «Аккорд-KVM. Руководство администратора».
		Обеспечение целостности (ОЦЛ)			
33	ОЦЛ.0	Разработка политики обеспечения целостности	+ все	В комплексе реализована политика обеспечения целостности.	
34	ОЦЛ.1	Контроль целостности программного обеспечения	+ все	СПО «Аккорд-KVM» обеспечивает: – контроль целостности программных компонентов ВМ (файлов общего, прикладного ПО и данных), выполняемый до их запуска; – контроль целостности конфигурации ВМ, выполняемый до запуска ВМ.	1. п.п. 3.6, 3.7 документа «Аккорд-KVM. Руководство администратора».
35	ОЦЛ.3	Ограничение по вводу информации в информационную (автоматизированную) систему	+ начиная с 1 класса защищенности автоматизированной системы управления	Обеспечивается за счет применения комплексов «Аккорд-X K».	1. п.п. 3.2.6, 3.2.7 документа «Аккорд-X K. Руководство администратора».
36	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+ начиная со 2 класса защищенности автоматизированной системы управления		1. п.п. 3.2.12 документа «Аккорд-X K. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
37	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		1. п.п. 3.2.2, Приложение 3 документа «Аккорд-X K. Руководство администратора».
		Обеспечение доступности (ОДТ)			
38	ОДТ.0	Разработка политики обеспечения доступности	+ все	Обеспечивается за счет модуля доверенной загрузки из состава комплекса «Аккорд-X» или «Аккорд-XL».	
39	ОДТ.3	Контроль безотказного функционирования средств и систем	+ во 2 классе защищенности автоматизированной системы управления		1. п.п. 3.16 документа «Аккорд-АМДЗ. Руководство администратора».
40	ОДТ.4	Резервное копирование информации	+ все		1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».
41	ОДТ.5	Обеспечение возможности восстановления информации	+ все		
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
42	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+ все	Политика защиты информационной (автоматизированной) системы и ее компонентов обеспечивается за счет применения комплекса «Аккорд-X K».	
43	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+ все	Обеспечивается за счет применения комплекса «Аккорд-X K».	1. п.п. 3.2.4, 3.2.5 документа «Аккорд-X K. Руководство администратора».
44	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 класса защищенности автоматизированной системы управления	СПО «Аккорд-KVM» осуществляет контроль целостности виртуальной инфраструктуры и ее конфигурации.	1. п.п. 3.6, 3.7 документа «Аккорд-KVM. Руководство администратора».
45	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+ все	Обеспечивается за счет применения комплекса «Аккорд-X K».	1. п.п. 3.4.13 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора».
46	ЗИС.33	Исключение доступа через общие ресурсы	+ начиная с 1 класса защищенности автоматизированной системы управления		1. п.п. 3.4.2, 5.2 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.2, 5.2 документа «Аккорд-X K. Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
					администратора».
47	ЗИС.38	Защита информации при использовании мобильных устройств	+ все		1. п.п. 3.4.13 документа «Аккорд-X. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-X K. Руководство администратора».
48	ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+ все	Комплекс обеспечивает управление размещением и перемещением исполняемых виртуальных машин между контролируемыми СПО «Аккорд-KVM» серверами виртуализации путем контроля запуска ВМ.	1. п. 3.10 документа «Аккорд-KVM. Руководство администратора».
		Реагирование на компьютерные инциденты (ИНЦ)			
49	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+ все	Обеспечивается за счет применения комплекса «Аккорд-X K».	
50	ИНЦ.1	Выявление компьютерных инцидентов	+ все		1. Приложение 3 документа «Аккорд X K. Руководство администратора».
51	ИНЦ.2	Информирование о компьютерных инцидентах	+ все		
		Управление обновлениями программного обеспечения (ОПО)			
52	ОПО.0	Разработка политики управления обновлениями программного обеспечения	+ все	Обновление СПО «Аккорд-KVM» выполняется эксплуатирующей организацией в соответствии с ТУ на комплекс. В случае применения СПО «Аккорд-KVM» совместно с «Аккорд-X K», обновление «Аккорд-X K» также выполняется эксплуатирующей организацией в соответствии с ТУ на комплекс. В случае применения СПО «Аккорд-KVM» совместно с ПАК «Аккорд-X» или «Аккорд-XL» предусмотрена возможность обновления в том числе ПО (firmware) модуля доверенной загрузки,	
53	ОПО.4	Установка обновлений программного обеспечения	+ все		1. п. 3 документа «Аккорд-X K. Руководство администратора»; 2. п. 6 документа «Аккорд-KVM. Формуляр». 3. п. 6 документа «Аккорд-АМДЗ. Формуляр».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-KVM»	Ссылки на документацию
				который входит в состав ПАК «Аккорд-X» и ПАК «Аккорд-XL». Обновление прошивки модуля доверенной загрузки выполняется в сервисном центре Разработчика ПО.	
		Обеспечение действий в нештатных ситуациях (ДНС)			
54	ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+ все		
55	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций	+ начиная со 2 класса защищенности автоматизированной системы управления	Обеспечивается за счет модуля доверенной загрузки из состава комплекса «Аккорд-X» или «Аккорд-XL».	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».
56	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+ все		

3 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-KVM»

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 комплекса СПО «Аккорд KVM».

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 KVM»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	СПО «Аккорд KVM»	Ссылки на документацию
		Управление доступом (УПД)			
1	УПД.12	Управление атрибутами безопасности		Обеспечивается за счет применения комплекса «Аккорд-X К».	1. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-X К. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	СПО «Аккорд KVM»	Ссылки на документацию
		Ограничение программной среды (ОПС)			
2	ОПС.3	Управление временными файлами		Обеспечивается средствами ОС Linux (с помощью специального механизма swap).	
		Обеспечение целостности (ОЦЛ)			
3	ОЦЛ.2	Контроль целостности информации		Обеспечивается за счет применения комплекса «Аккорд-Х К».	1. п.п 2.1.2, 2.2, 3.2.2, 3.2.6, 3.2.8, 5.6, 5.7 документа «Аккорд-Х К. Руководство администратора».
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
4	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		Обеспечивается средствами ОС.	
	ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)		Обеспечивается за счет модуля доверенной загрузки из состава комплекса «Аккорд-Х» или «Аккорд-XL». Посредством комплекса «Аккорд-АМДЗ» возможно: – резервное копирование информации в соответствии с мерой ОДТ.4; – контроль безотказного функционирования технических средств ИС в соответствии с мерой ОДТ.3; – обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в соответствии с мерой ОДТ.5.	1. п.п. 3.14, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».

Итак, путем применения СПО «Аккорд-KVM» 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;

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, 39;
ИНЦ: 1, 2;
ОПО: 4;
ДНС: 4, 5;
а также дополнительные (не включенные в базовый набор) меры:
УПД: 12;
ОПС: 3;
ОЦЛ: 2;
ЗИС: 12, 37.

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