ВЫПОЛНЕНИЕ МЕР
31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ ПАК СЗИ ОТ НСД СЕМЕЙСТВА «АККОРД-Х»

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 системы защиты информации от несанкционированного доступа «Аккорд-Х».

Программно-аппаратный комплекс «Аккорд-Х» обеспечивает выполнение положений документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) и функциональных требований, установленных в Технических условиях ТУ 26.20.40.140-080-37222406-2019.

Аппаратные средства ПАК «Аккорд-Х» включают в себя:

– контроллер АМДЗ, входящий в состав ПАК СЗИ НСД «Аккорд-АМДЗ» (ТУ 4012-038-11443195-2011, ТУ 26.20.40.140-079-37222406-2019, ТУ 4012-054-11443195-2013);
– съемник информации с контактным устройством;
– персональный идентификатор пользователя.

Программные средства ПАК «Аккорд-Х» включают в себя специальное программное обеспечение «Аккорд-Х»:

– ядро защиты – программы, реализующие защитные функции «Аккорд-Х»;
– программы управления защитными функциями (настройки «Аккорд-Х» в соответствии с ПРД).

В ядро защиты входят:

– монитор разграничения доступа – МРД (модуль ядра Linux acx-core.ko);
– подсистема идентификации и аутентификации (PAM-модули pam_acx_local.so и др.);
– подсистема контроля печати (фильтр подсистемы печати Linux CUPS - pstops);
– модуль реализации статического контроля целостности объектов ОС (acx-integrity-controller).

Различают следующие типы СЗИ от НСД семейства «Аккорд Х»:

– ПАК СЗИ от НСД «Аккорд-Х» / «Аккорд-XL» - применяется для защиты от НСД автоматизированных рабочих мест и серверов.
– ПАК СЗИ от НСД «Аккорд-Х К» применяется для защиты от НСД автоматизированных рабочих мест и серверов, и отличается от предыдущего типа СЗИ тем, что способ реализации процедур контроля целостности у данного типа СЗИ программный.
– ПАК СЗИ от НСД «Аккорд-Х К» (Virtual Edition) применяется для защиты от НСД в ВМ.

2 Выполнение мер базового набора мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения ПАК СЗИ от НСД «Аккорд-Х»

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения СЗИ НСД «Аккорд-Х».

Выражение «все» в ячейках столбца «Классы защищенности автоматизированной системы управления» означает, что рассматриваемая мера должна быть реализована в автоматизированной системе 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 ПАК СЗИ от НСД «Аккорд-Х»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			
1	ИАФ.0	Разработка политики идентификации и аутентификации	+ все	В комплексе разработана политика идентификации и аутентификации.	
2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+ все	Комплекс «Аккорд-Х» позволяет однозначно идентифицировать все имеющиеся в системе устройства, как по внутренним именам операционной системы, так и по логическим, и задает для них правила разграничения доступа.	1. п.п. 2.1.1, 2.1.2 документа «Аккорд-Х К. Руководство оператора (пользователя)»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора»; 3. п.п. 2.1.1, 2.1.2 документа «Аккорд-Х. Руководство оператора (пользователя)»; 4. п.п. 3.4.3 документа «Аккорд-Х. Руководство администратора».
3	ИАФ.2	Идентификация и аутентификация устройств	+ все	Управление идентификаторами учетных записей производится в консоли управления Аккорд-Х. (Управление Аккорд-Х возможно через толстый клиент, посредством веб-доступа, посредством командной строки) Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных идентификаторов, присвоение уровня доступа.	1. п.п. 3.10, 3.12 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора».
4	ИАФ.3	Управление идентификаторами	+ все	Управление паролями и аппаратными идентификаторами учетных записей пользователей производится в консоли управления Аккорд-Х.	1. п.п. 3.4.3 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.3

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
				Возможные операции: создание пароля, генерация пароля программой, смена пароля, запись данных в идентификатор, установка времени действия пароля.	документа «Аккорд-Х К. Руководство администратора».
5	ИАФ.4	Управление средствами аутентификации	+ все	Управление паролями и аппаратными идентификаторами учетных записей пользователей производится в консоли управления Аккорд-Х. Возможные операции: создание пароля, генерация пароля программой, смена пароля, запись данных в идентификатор, установка времени действия пароля.	1. п.п. 3.4.2, 3.4.3 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.2, 3.2.3 документа «Аккорд-Х К. Руководство администратора».
6	ИАФ.5	Идентификация и аутентификация внешних пользователей	+ все	Идентификация и аутентификация осуществляется по имени пользователя, паролю и аппаратному идентификатору.	
7	ИАФ.7	Защита аутентификационной информации при передаче	+ все	При вводе пароля (при авторизации в АМДЗ, при входе в ОС), пароль отображается звездочками.	
		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 в консоли управления Аккорд-Х. Возможные операции с пользователями: создание, удаление, отключение (деактивация) учетной записи, редактирование свойств учетной записи; включение пользователей в группы.	1. п.п. 3.4.2, 3.4.3 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.2, 3.2.3 документа «Аккорд-Х К. Руководство администратора».
10	УПД.2	Реализация политик управления доступом	+ все	Доступ субъектов доступа к ресурсам разграничивается в рамках настройки дискреционного и мандатного доступа.	1. п.п. 3.4.6, 3.4.7, 5.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-Х К. Руководство администратора».
11	УПД.3	Доверенная загрузка	+ начиная со 2 класса защищенности автоматизированной системы управления	Мера УПД.3 выполняется при условии наличия в составе комплекса СЗИ НСД модуля доверенной загрузки «Аккорд-АМДЗ» («Аккорд-Х» и «Аккорд-XL»).	1. п.п. 1.1, 3.10 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п 3.1

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
					документа «Аккорд-АМДЗ. Руководство пользователя».
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. Администратор СЗИ от НСД регистрирует в системе защиты других пользователей.	1. п.п. 3.2.4-3.2.7 документа «Аккорд-Х К. Руководство администратора»; 2. п.п. 3.4.4-3.4.7 документа «Аккорд-Х. Руководство администратора».
13	УПД.5	Назначение минимально необходимых прав и привилегий	+ все		
14	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+ все	Параметр pam-retries (максимальное количество попыток выполнить login перед блокировкой).	1. п.п. 3.4.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора».
15	УПД.9	Ограничение числа параллельных сеансов доступа	+ начиная с 1 класса защищенности автоматизированной системы управления	Ограничение многосессионности задается в файле конфигурации «Аккорд-Х».	1. п.п. 3.4.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.2 документа «Аккорд-Х К. Руководство администратора».
16	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+ все	PAM-модули «Аккорд-Х» можно использовать для блокировки сессии пользователей при включении штатного хранителя экрана в ОС Linux. Для этого PAM-модуль нужно аналогичным образом прописать для приложений типа gnome-screensaver или аналогичных (в зависимости от установленного приложения-скринсейвера).	1. п.п. 3.4.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора».
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-Х. Руководство пользователя»; 2. п.п. 2.2 документа «Аккорд-Х К. Руководство пользователя».
		Ограничение программной среды (ОПС)			

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
18	ОПС.0	Разработка политики ограничения программной среды	+ начиная со 2 класса защищенности автоматизированной системы управления	В СЗИ НСД существует механизм настройки изолированной программной среды (ИПС).	
19	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ начиная с 1 класса защищенности автоматизированной системы управления		1. п.п. 3.4.7, 3.4.8, 5.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.7, 3.2.8, 5.2 документа «Аккорд-Х К. Руководство пользователя».
		Защита машинных носителей информации (ЗНИ)			
20	ЗНИ.0	Разработка политики защиты машинных носителей информации	+ все	Комплекс 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.	
21	ЗНИ.2	Управление физическим доступом к машинным носителям информации	+ все	Обеспечивается при условии применения ПАК «Аккорд-Х» («Аккорд-XL»), в состав которого входит «Аккорд-АМДЗ», либо совместного применения комплекса с СЗИ НСД «Аккорд-АМДЗ». Доступ к машинным носителям СВТ осуществляется только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «Аккорд-АМДЗ».	
22	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ все	Администратор должен описать всевозможные подключаемые устройства (идентифицируя их, желательно, по UUID) и задать для каждого из них свою точку монтирования (например, в каталоге /mnt/diskA, /mnt/diskB и т.п.). После чего для каждого пользователя можно задать права в рамках дискреционной политики доступа Аккорд-Х на доступ к этим точкам монтирования, а для точек	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
				монтирования можно задать мандатные метки с уровнем конфиденциальности или добавить некоторые объекты в списки контроля целостности – всё зависит от решаемых задач по контролю за внешними носителями информации.	
23	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	+ начиная с 1 класса защищенности автоматизированной системы управления	Администратор должен описать всевозможные подключаемые устройства (идентифицируя их, желательно, по UUID) и задать для каждого из них свою точку монтирования (например, в каталоге /mnt/diskA, /mnt/diskB и т.п.). После чего для каждого пользователя можно задать права в рамках дискреционной политики доступа Аккорд-Х на доступ к этим точкам монтирования, а для точек монтирования можно задать мандатные метки с уровнем конфиденциальности или добавить некоторые объекты в списки контроля целостности – всё зависит от решаемых задач по контролю за внешними носителями информации.	
24	ЗНИ.7	Контроль подключения машинных носителей информации	+ все	Администратор должен описать всевозможные подключаемые устройства (идентифицируя их, желательно, по UUID) и задать для каждого из них свою точку монтирования (например, в каталоге /mnt/diskA, /mnt/diskB и т.п.). После чего для каждого пользователя можно задать права в рамках дискреционной политики доступа Аккорд-Х на доступ к этим точкам монтирования, а для точек монтирования можно задать мандатные метки с уровнем конфиденциальности или добавить некоторые объекты в списки контроля целостности – всё зависит от решаемых задач по контролю за внешними носителями информации.	
25	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+ все	СЗИ НСД «Аккорд» включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.	1. п.п. 3.4.2, 5.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.2, 5.2 документа «Аккорд-Х К.

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
					Руководство администратора».
		Аудит безопасности (АУД)			
26	АУД.0	Разработка политики аудита безопасности	+ все	Комплекс поддерживает политику аудита безопасности в части обеспечения регистрации событий безопасности, защиты информации о событиях безопасности и анализа действий пользователей.	
27	АУД.2	Анализ уязвимостей и их устранение	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации. Обновление ПО разграничения доступа выполняется эксплуатирующей организацией в соответствии с ТУ и п. 3 документа «Руководство администратора» на комплекс. В комплексе предусмотрена возможность обновления в том числе ПО (firmware) модуля доверенной загрузки, который входит в состав ПАК «Аккорд-Х» и ПАК «Аккорд-XL». Обновление прошивки модуля доверенной загрузки выполняется в сервисном центре Разработчика ПО.	1. п. 3 документа «Аккорд-Х. Руководство администратора»; 2. п. 3 документа «Аккорд-Х К. Руководство администратора»; 3. п. 6 документа «Аккорд-АМДЗ. Формуляр».
28	АУД.4	Регистрация событий безопасности	+ все	Как для каталогов, так и для отдельных файлов, в «Аккорд-Х» присутствует возможность установки опции регистрации в регистрационном журнале доступа к каталогу и его содержимому.	1. п.п. 4.4, 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п 4.4, 5.9 документа «Аккорд-Х К. Руководство администратора».
29	АУД.6	Защита информации о событиях безопасности	+ 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	1. п.п. 4.4, 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 4.4 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
				функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам.	
30	АУД.7	Мониторинг безопасности	+ все	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности.	1. п.п. 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п 5.9 документа «Аккорд-Х К. Руководство администратора».
31	АУД.8	Реагирование на сбои при регистрации событий безопасности	+ все	Обеспечивается при условии применения ПАК «Аккорд-Х» («Аккорд-XL»), в состав которого входит «Аккорд-АМДЗ», либо совместного применения комплекса с СЗИ НСД «Аккорд-АМДЗ».	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».
32	АУД.9	Анализ действий пользователей	+ начиная с 1 класса защищенности автоматизированной системы управления	С помощью утилиты acx-admin log и применением различных фильтров можно проанализировать работу каждого пользователя.	1. п.п. 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п 5.9 документа «Аккорд-Х К. 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	Комплекс обеспечивает контроль целостности средств защиты информации по контрольным суммам всех компонентов средств защиты информации динамически в процессе работы системы. В частности, комплекс должен обеспечивать контроль целостности файлов программ и данных.	1. п.п. 3.4.8, 5.7 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.8, 5.7 документа «Аккорд-Х К. Руководство администратора».
35	ОЦЛ.3	Ограничение по вводу информации в информационную (автоматизированную) систему	+ начиная с 1 класса защищенности автоматизированной системы управления	Реализуется дискреционным и мандатным доступом к файлам документов.	1. п.п. 3.4.6, 3.4.7 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.6, 3.2.7 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-X»	Ссылки на документацию
36	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+ начиная со 2 класса защищенности автоматизированной системы управления	С помощью СЗИ от НСД «Аккорд» возможно выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации.	1. п.п. 3.4.13 документа «Аккорд-X. Руководство администратора»; 2. п.п. 3.2.12 документа «Аккорд-X K. Руководство администратора».
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	При превышении установленного количества попыток аутентификации пользователь блокируется. При этом в журнале комплекса отображается ошибка превышения количества некорректных попыток входа.	1. п.п. 3.4.2, Приложение 3 документа «Аккорд-X. Руководство администратора»; 2. п.п. 3.2.2, Приложение 3 документа «Аккорд-X K. Руководство администратора».
		Обеспечение доступности (ОДТ)			
38	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.	
39	ОДТ.3	Контроль безотказного функционирования средств и систем	+ во 2 классе защищенности автоматизированной системы управления	Обеспечивается при условии применения ПАК «Аккорд-X» («Аккорд-XL»), в состав которого входит «Аккорд-АМДЗ», либо совместного применения комплекса с СЗИ НСД «Аккорд-АМДЗ». Обеспечивается контроль работоспособности, правильности функционирования программного обеспечения средств защиты информации посредством функции самотестирования функционала СЗИ НСД перед стартом.	1. п.п. 3.16 документа «Аккорд-АМДЗ. Руководство администратора».
40	ОДТ.4	Резервное копирование информации	+ все	Комплексом «Аккорд-АМДЗ» (по команде администратора) обеспечиваться периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов) на резервные машинные носители информации.	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
				Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	
41	ОДТ.5	Обеспечение возможности восстановления информации	+ все	Комплексом «Аккорд-АМДЗ» (по команде администратора) обеспечивается возможность восстановления информации (базы данных пользователей и списка контролируемых объектов) с резервных машинных носителей информации (резервных копий). Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
42	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+ все	Комплекс обеспечивает защиту информационной (автоматизированной) системы и ее компонентов в части изоляции процессов в выделенной области памяти, защиты неизменяемых данных.	
43	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+ все	Пользователь, установивший систему защиты, обладает всеми полномочиями администрирования (управления) системы защиты и всеми правами по доступу к ресурсам. Администратор СЗИ от НСД регистрирует в системе защиты других пользователей.	1. п.п. 3.4.3, 3.4.4 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.3, 3.2.4 документа «Аккорд-Х К. Руководство администратора».
44	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 класса защищенности автоматизированной системы управления	Производится контроль целостности программных средств СЗИ НСД (по умолчанию) и всех компонентов. Возможен контроль целостности файлов других приложений, файлов с данными и пр.	1. п.п. 3.4.8, 5.7 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.8, 5.7 документа «Аккорд-Х К. Руководство администратора». 3. п.п. 3.10 документа «Аккорд-АМДЗ. Руководство администратора».
45	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+ все	Комплекс позволяет исключить несанкционированное использование USB-	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
				принтеров. Запрет (или использование) периферийных устройств регулируется посредством назначения пользователю (или группе пользователей) соответствующих правил разграничения доступа.	администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
46	ЗИС.33	Исключение доступа через общие ресурсы	+ начиная с 1 класса защищенности автоматизированной системы управления	В комплексе реализован механизм очистки памяти.	1. п.п. 3.4.2, 5.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.2, 5.2 документа «Аккорд-Х К. Руководство администратора».
47	ЗИС.38	Защита информации при использовании мобильных устройств	+ все	При применении в ИС комплекса «Аккорд-Х» или «Аккорд-Х К» 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. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
48	ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+ все	Обеспечивается при совместном применении с СПО «Аккорд-KVM».	1. п. 3.10 документа «Аккорд-KVM. Руководство администратора».
		Реагирование на компьютерные инциденты (ИНЦ)			
49	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+ все	Комплекс обеспечивает фиксацию операций с доступом к объектам, операции смены субъекта доступа, операции И/А.	
50	ИНЦ.1	Выявление компьютерных инцидентов	+ все		1. Приложение 3 документа «Аккорд-Х. Руководство администратора»; 2. Приложение 3 документа «Аккорд-Х К. 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 ПО разграничения доступа выполняется эксплуатирующей организацией в соответствии с ТУ и п. 3 документа	
53	ОПО.4	Установка обновлений программного обеспечения	+ все		1. п. 3 документа «Аккорд-Х. Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
				«Руководство администратора» на комплекс. В комплексе предусмотрена возможность обновления в том числе ПО (firmware) модуля доверенной загрузки, который входит в состав ПАК «Аккорд-Х» и ПАК «Аккорд-XL». Обновление прошивки модуля доверенной загрузки выполняется в сервисном центре Разработчика ПО.	администратора»; 2. п. 3 документа «Аккорд-Х К. Руководство администратора»; 3. п. 6 документа «Аккорд-АМДЗ. Формуляр».
		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	Комплексом «Аккорд-АМДЗ» (по команде администратора) обеспечиваться периодическое резервное копирование информации (базы данных пользователей и списка контролируемых объектов) на резервные машинные носители информации. Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	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	Реализована функция сохранения резервной копии конфигурационных файлов СЗИ НСД «Аккорд-АМДЗ». Аппаратная часть комплекса СЗИ НСД «Аккорд-АМДЗ» имеет в составе внутреннего ПО функции резервного копирования и восстановления базы данных пользователей и списка контролируемых объектов.	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения ПАК СЗИ НСД «Аккорд-Х»

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 ПАК СЗИ НСД «Аккорд-Х».

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 ПАК СЗИ от НСД «Аккорд-Х»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
		Управление доступом (УПД)			
1	УПД.12	Управление атрибутами безопасности		В ПАК «Аккорд-Х» и СПО «Аккорд-Х К» реализованы мандатный и дискреционный механизмы разграничения доступа. Посредством данных механизмов разграничения доступа комплексы «Аккорд-Х» и «Аккорд-Х К» обеспечивают обновление, назначение, изменение и сохранение меток безопасности (меток доступа). Изменение атрибутов безопасности (меток доступа) возможно только авторизованными пользователям или процессами. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.4.6, 3.4.7, 5.2 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-Х К. Руководство администратора».
		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		Комплекс позволяет осуществлять контроль целостности на уровне файлов БД и СУБД.	1. п.п. 2.1.2, 2.2, 3.4.2, 3.4.8, 5.6, 5.7 документа «Аккорд-Х. Руководство администратора»; 2. п.п 2.1.2, 2.2, 3.2.2, 3.2.6, 3.2.8, 5.6, 5.7 документа «Аккорд-Х К.

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«Аккорд-Х»	Ссылки на документацию
					Руководство администратора».
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
4	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		Обеспечивается средствами ОС.	
5	ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)		Посредством комплекса 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 ПАК СЗИ НСД «Аккорд-Х» в автоматизированной системе управления выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности автоматизированной 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