ВЫПОЛНЕНИЕ МЕР

17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ

ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

ПУТЕМ ПРИМЕНЕНИЯ

ПАК СЗИ ОТ НСД СЕМЕЙСТВА «АККОРД-Х»

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 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 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения ПАК СЗИ от НСД «Аккорд-Х»

В таблице № 1 представлено описание выполнения базового набора мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения СЗИ НСД «Аккорд-Х».

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 ПАК СЗИ от НСД «Аккорд-Х»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	Идентификация и аутентификация осуществляется по имени пользователя, паролю и аппаратному идентификатору. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	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».
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	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. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	1. п.п. 3.10, 3.12 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ все	+ все	Управление идентификаторами учетных записей производится в консоли управления Аккорд-Х. (Управление Аккорд-Х возможно через толстый клиент, посредством веб-	1. п.п. 3.4.3 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.3 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					доступа, посредством командной строки). Возможные операции: создание, удаление, блокировка, редактирование свойств учетной записи; создание, присвоение, удаление аппаратных идентификаторов, присвоение уровня доступа. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	
4	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+ все	+ 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. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	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».
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	При вводе пароля (при авторизации в АМДЗ, при входе в ОС), пароль отображается звездочками. Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	
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. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		Управление доступом субъектов доступа к объектам доступа (УПД)				
7	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+ все	+ все	Управление учетными записями производится в консоли управления Аккорд-Х. Возможные операции с пользователями: создание, удаление, отключение (деактивация) учетной записи, редактирование свойств учетной записи; включение пользователей в группы. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	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».
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. 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».
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. Администратор СЗИ от НСД регистрирует в системе защиты других пользователей. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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».
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все		
11	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной	+ все	+ все	Параметр pam-retries (максимальное количество попыток выполнить login перед блокировкой). Выполняется за счет средств СПО «Аккорд-Х»,	1. п.п. 3.4.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		системе)			входящего в состав ПАК «Аккорд-Х».	
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	Ограничение многосессионности задается в файле конфигурации «Аккорд-Х». Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «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».
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	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). Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.4.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.9 документа «Аккорд-Х К. Руководство администратора».
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. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	1. п.п. 2.2 документа «Аккорд-Х. Руководство пользователя»; 2. п.п. 2.2 документа «Аккорд-Х К. Руководство пользователя».
15	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических устройств	+ все	+ все	Администратор должен описать всевозможные подключаемые устройства, на которых хранится и переносится информация (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	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.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					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. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	
16	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 наличия в составе комплекса СЗИ НСД модуля доверенной загрузки «Аккорд-АМДЗ» («Аккорд-Х» и «Аккорд-XL»). Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	1. п.п. 1.1, 3.10 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п 3.1 документа «Аккорд-АМДЗ. Руководство пользователя».
		Ограничение программной среды (ОПС)				
17	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	В СЗИ НСД существует механизм настройки изолированной программной среды (ИПС) путем установки и настройки мандатного механизма разграничения доступа с контролем процессов. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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 администартора».
		Защита машинных носителей персональных данных (ЗНИ)				
18	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ начиная со 2 уровня защищенности ПДн	+ все	Выполняется при условии наличия в составе комплекса СЗИ НСД модуля доверенной загрузки «Аккорд-АМДЗ» («Аккорд-Х» и «Аккорд-XL»): доступ к	

[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-Х»	Ссылки на документацию
					машинным носителям СВТ осуществляется, только после прохождения всех этапов доверенной загрузки, реализуемой СЗИ от НСД «Аккорд-АМДЗ». Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	
19	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных	не входит в базовый набор мер	+ начиная со 2 класса защищенности ИС	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. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
20	ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	+ начиная с 3 уровня защищенности ПДн	+ все	СЗИ НСД «Аккорд» включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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».
		Регистрация событий безопасности (РСБ)				
21	РСБ.1	Определение событий	+	+	Как для каталогов, так и для отдельных файлов, в	1. п.п. 4.4 документа «Аккорд-Х. Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		безопасности, подлежащих регистрации, и сроков их хранения	все	все	«Аккорд-Х» присутствует возможность установки опции регистрации в регистрационном журнале доступа к каталогу и его содержимому. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	администратора»; 2. п.п 4.4 документа «Аккорд-Х К. Руководство администратора».
22	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ все	+ все	Состав и содержание событий безопасности определяются для событий, которые связаны с функциональными возможностями комплекса (дискреционная и мандатная политика управления доступом, процедуры идентификации и аутентификации, контроль целостности). При регистрации событий фиксируется исчерпывающий набор параметров: дата и время, идентификатор субъекта, идентификатор объекта, тип выполняемой операции, результат операции и др. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 4.4, Приложение 3 документа «Аккорд-Х. Руководство администратора»; 2. п.п 4.4, Приложение 3 документа «Аккорд-Х К. Руководство администратора».
23	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все	Данные аудита хранятся в системной папке. Файлы журналов событий сохраняются в специальный файл и доступны к просмотру только администратору. Для удобства просмотра и анализа информации присутствует возможность фильтрации по одному или нескольким полям таблицы в acx-admin log. Ограничение времени хранения журналов обеспечивается ПО ОС. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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».
24	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в	не входит в базовый набор	+ все	Выполняется при условии наличия в составе комплекса СЗИ НСД модуля доверенной загрузки «Аккорд-АМДЗ» («Аккорд-Х» и «Аккорд-XL»).	1. п.п. 3.11 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти			Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х». Если заполнение журнала превышает 85%, при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если заполнение журнала превышает 95%, то загрузка для пользователя блокируется, и требуется вмешательство администратора.	
25	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+ Начиная со 2 уровня защищенности ПДн	+ все	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п 5.9 документа «Аккорд-Х К. Руководство администратора».
26	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 (аудита) предоставляется только уполномоченным должностным лицам. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 4.4, 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 4.4 документа «Аккорд-Х К. Руководство администратора».
		Контроль (анализ) защищенности персональных данных (АНЗ)				
27	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных	+ начиная с 3 уровня защищенности ПДн	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации.	1. п. 3 документа «Аккорд-Х. Руководство администратора»; 2. п. 3 документа «Аккорд-Х К. Руководство администратора»;

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		уязвимостей			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.	3. п. 6 документа «Аккорд-АМДЗ. Формуляр».
28	АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Обеспечивается средствами ОС.	
29	АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ все	Реализована функция самотестирования функционала СЗИ НСД. Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.1, 3.16 документа «Аккорд-АМДЗ. Руководство администратора».
30	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	Производится контроль целостности программных средств СЗИ НСД и отдельно назначенных объектов файловой системы. Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.10.1 документа «Аккорд-АМДЗ. Руководство администратора».
31	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения	+ начиная со 2 уровня защищенности ПДн	+ все	Настраивается в Параметрах Пользователей. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.4.3-3.4.5 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.3-3.2.5 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		доступа, полномочий пользователей в информационной системе				
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
32	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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. 2.1.1, 2.1.2 документа «Аккорд-Х. Руководство оператора (пользователя)»; 4. п.п. 2.1.1, 2.1.2 документа «Аккорд-Х К. Руководство оператора (пользователя)».
33	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	не входит в базовый набор мер	+ все	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. Выполняется за счет средств комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».
34	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ начиная 1 класса защищенности ИС	Реализуется дискреционным и мандатным доступом к файлам документов. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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».
		Защита среды виртуализации (ЗСВ)				
35	ЗСВ.1	Идентификация и	+	+	Функциональные	1. п.п. 2.1.1, 2.1.2

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	все	все	возможности ПАК «Аккорд-Х» и СПО «Аккорд-Х К» позволяют применять данные комплексы для обеспечения защиты от НСД к информации ПЭВМ типа IBM PC (автономных компьютерах, рабочих станциях ЛВС) и виртуальных машинах, функционирующих под управлением ОС семейства Linux, а также в автоматизированных системах (АС), построенных на их основе, в многопользовательском режиме. Комплексы «Аккорд-Х» и «Аккорд-Х К» позволяют выполнять процедуры И/А как на физических ПЭВМ, так и на виртуальных машинах. При применении «Аккорд-Х» и «Аккорд-Х К» на виртуальных машинах И/А в виртуальной среде, а именно, мера ЗСВ.1, обеспечивается за счет выполнения мер группы ИАФ (ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6).	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».
36	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+ все	+ все	Функциональные возможности ПАК «Аккорд-Х» и СПО «Аккорд-Х К» позволяют применять данные комплексы для обеспечения защиты от НСД к информации ПЭВМ типа IBM PC (автономных компьютерах, рабочих станциях ЛВС) и виртуальных машинах, функционирующих под управлением ОС семейства Linux, а также в автоматизированных системах (АС), построенных на их основе, в многопользовательском режиме. Комплексы «Аккорд-Х» и «Аккорд-Х К» позволяют управлять доступом как на физических ПЭВМ, так и в виртуальных машинах. При применении «Аккорд-Х» и «Аккорд-Х К» в виртуальных машинах управление доступом в	1. п.п. 3.2.6, 3.2.7, 3.2.10, 3.2.12 документа «Аккорд-Х К. Руководство администратора»; 2. п.п. 3.4.6, 3.4.7, 3.4.10, 3.4.13 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					виртуальной среде, а именно, мера ЗСВ.2, обеспечивается за счет выполнения мер группы УПД (УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.15, УПД.17 (УПД.17 выполняется при условии включения в состав комплекса модуля доверенной загрузки «Аккорд-АМДЗ»)).	
37	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+ начиная с 3 уровня защищенности ПДн	+ все	Обеспечивается средствами «Аккорд-KVM» при совместном применении последнего в совокупности с СПО «Аккорд-Х К».	1. п. 4 документа «Аккорд-KVM. Руководство администратора».
38	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Обеспечивается средствами «Аккорд-KVM» при совместном применении последнего в совокупности с СПО «Аккорд-Х К».	1. п. 3.10 документа «Аккорд-KVM. Руководство администратора».
39	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Обеспечивается средствами «Аккорд-KVM» при совместном применении последнего в совокупности с СПО «Аккорд-Х К».	1. п.п. 3.6, 3.7 документа «Аккорд-KVM. Руководство администратора».
		Обеспечение доступности персональных данных (ОДТ)				
40	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	С помощью комплекса «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».
41	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 «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»,	1. п.п. 3.14 документа «Аккорд-АМДЗ. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					входящего в состав ПАК «Аккорд-Х».	
42	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 «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 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 информации, функций по обработке информации и иных функций информационной системы	+ на 1 уровне защищенности ПДн	+ начиная со 2класса защищенности ИС	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.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+ все		Комплекс позволяет исключить несанкционированное использование USB-принтеров. Запрет (или использование) периферийных устройств регулируется посредством назначения пользователю (или группе пользователей) соответствующих правил разграничения доступа.	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
45	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Производится контроль целостности программных средств СЗИ НСД (по умолчанию) и всех компонентов. Возможен контроль целостности файлов других	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».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		подлежащих изменению в процессе обработки персональных данных			приложений, файлов с данными и пр. Выполняется за счет средств СПО «Аккорд-Х», а также комплекса «Аккорд-АМДЗ» входящих в состав ПАК «Аккорд-Х».	3. п.п. 3.10 документа «Аккорд-АМДЗ. Руководство администратора».
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	+ начиная с 1 класса защищенности ИС	В комплексе реализован механизм очистки памяти. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	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.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. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
		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 доступом к объектам, операции смены субъекта доступа, операции И/А.	1. Приложение 3 документа «Аккорд-Х. Руководство администратора»; 2. Приложение 3 документа «Аккорд-Х К. Руководство администратора».

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 ПАК СЗИ НСД «Аккорд-Х»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения комплекса ПАК СЗИ НСД «Аккорд-Х».

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 ПАК СЗИ от НСД «Аккорд-Х»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
		Идентификация и аутентификация субъектов и 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. Выполняется за счет средств комплекса «Аккорд-АМДЗ», а также СПО «Аккорд-Х», входящих в состав ПАК «Аккорд-Х».	1. п.п. 2.1.3 документа «Аккорд-Х. Руководство пользователя».
		Управление доступом субъектов доступа к объектам доступа (УПД)				
2	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			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»,	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».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					входящего в состав ПАК «Аккорд-Х».	
		Ограничение программной среды (ОПС)				
3	ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			Обеспечивается средствами ОС Linux (с помощью специального механизма swap).	
		Защита машинных носителей персональных данных (ЗНИ)				
4	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных			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. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
5	ЗНИ.7	Контроль подключения машинных носителей персональных данных				
		Регистрация событий безопасности (РСБ)				
6	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	нет		С помощью утилиты acx-admin log и применением различных фильтров можно проанализировать работу каждого пользователя. Выполняется за счет средств СПО «Аккорд-Х»,	1. п.п. 5.9 документа «Аккорд-Х. Руководство администратора»; 2. п.п 5.9 документа «Аккорд-Х К. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					входящего в состав ПАК «Аккорд-Х».	
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
7	ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы			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. Руководство администратора».
8	ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы			С помощью СЗИ от НСД «Аккорд» возможно выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации. Выполняется за счет средств СПО «Аккорд-Х», входящего в состав ПАК «Аккорд-Х».	1. п.п. 3.4.13 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.12 документа «Аккорд-Х К. Руководство администратора».
9	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			При превышении установленного количества попыток аутентификации пользователь блокируется. При этом в журнале комплекса отображается ошибка превышения количества некорректных попыток входа. Фиксируется корректность алфавита ввода пароля (при использовании некорректных символов на экране появляется сообщение). При превышении установленного количества попыток смены пароля пользователя	1. п.п. 3.4.2, Приложение 3 документа «Аккорд-Х. Руководство администратора»; 2. п.п. 3.2.2, Приложение 3 документа «Аккорд-Х К. Руководство администратора». 3. п.п. 2.1.4 документа «Аккорд-Х. Руководство пользователя».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Аккорд-Х»	Ссылки на документацию
					загрузка системы произойдет только после вмешательства Администратора БИ с использованием его идентификатора.	
		Защита среды виртуализации (ЗСВ)				
10	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			При условии совместного применения СПО «Аккорд-KVM» и ПАК «Аккорд-Х» (или «Аккорд-XL»), в состав которых входит модуль доверенной загрузки «Аккорд-АМДЗ», обеспечивается доверенная загрузка инфраструктуры виртуализации.	1. п.п. 1.1, 3.10 документа «Аккорд-АМДЗ. Руководство администратора»; 2. п.п 3.1 документа «Аккорд-АМДЗ. Руководство пользователя».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
11	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			Обеспечивается средствами ОС.	
12	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		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 информационной системе выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 3, 4, 5, 6;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 15, 17;

ОПС: 1;
ЗНИ: 2, 5, 8;
РСБ: 1, 2, 3, 4, 5, 7;
АНЗ: 1, 2, 3, 4, 5;
ОЦЛ: 1, 3, 6;
ЗСВ: 1, 2, 3, 6, 7;
ОДТ: 3, 4, 5;
ЗИС: 1, 5, 15, 21, 30;
ИНЦ: 2;
а также дополнительные (не включенные в базовый набор) меры:
ИАФ: 7;
УПД: 12;
ОПС: 4;
ЗНИ: 6, 7;
РСБ: 8;
ОЦЛ: 2, 5, 8;
ЗСВ: 5;
ЗИС: 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