ВЫПОЛНЕНИЕ МЕР 17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ ЗАЩИЩЕННОГО ТЕРМИНАЛА «M-TRUST ТЕРМИНАЛ»

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 защищенного терминала «m-TrusT Терминал».

Защищённый терминал на базе микрокомпьютера «m-TrusT» (далее – защищенный терминал, «m-TrusT Терминал» либо комплекс) представляет собой СВТ в едином корпусе, предназначенное для организации защищенного канала передачи данных при подключении к терминальным серверам обработки данных в критических информационных структурах.

В «m-TrusT Терминал» ОС полностью хранится в памяти микрокомпьютера и доступна в режиме «только чтение».

Функциональность защищённого терминала такова, что пользователь может работать на нем, как на обычном ПК, но при этом посредством криптографических механизмов обеспечивается защита критичной информации и высокий уровень вычислительной мощности.

Защищённый терминал на базе микрокомпьютера «m-TrusT» построен на базе новой Гарвардской архитектуры, что обеспечивает высокий уровень вирусного иммунитета. Встроенный резидентный компонент безопасности создаёт доверенную среду функционирования криптографии и позволяет поддерживать высокий уровень конфиденциальности. Подключение к серверам обработки данных по защищенному каналу связи и использование встроенного аппаратного блока неизвлекаемого ключа обеспечивает простоту использования с соблюдением всех требований регулятора.

Наличие встроенного ПО «Аккорд-МКТ» и «Аккорд-Х К» обеспечивает доверенную загрузку ОС и разграничение доступа пользователей, а также регистрацию событий, контроль целостности и контроль подключения машинных носителей.

Аппаратная платформа терминала имеет производительный процессор – RK3399, совместима с последними версиями ядра Linux и поддерживает интерфейсы USB 3.0 и USB Type-C, что обеспечивает высокий уровень вычислительной мощности при относительно низком энергопотреблении.

Ресурсы терминала позволяют обеспечить среду функционирования криптографии, позволяющую сертифицировать вариант исполнения СКЗИ (может быть различным) на «m-TrusT» на класс КС3.

Также возможны:

– реализация поддержки sd-карт;
– реализация блока защиты от инвазивных атак.

Удаленный доступ с защищенного терминала на базе «m-TrusT» может осуществляться с помощью встроенных средств, выбранных на этапе заказа:

– Citrix ICA;
– Virtual Network Computing (VNC);
– Free RDP.

Основная функциональность «m-TrusT Терминала»:

– идентификация и аутентификация пользователя;
– контроль целостности ПО;
– доверенная загрузка ОС;
– защита от несанкционированной модификации программ и данных;

– «вирусный иммунитет»;
– защита информации при ее передаче по каналам связи (опционально);
– исключение доступа через общие ресурсы;
– доверенный сеанс связи пользователя с удаленными ресурсами;
– регистрация действий пользователя.

2 Выполнение базового набора мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения «m-TrusT Терминал»

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

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.

Таблица 1 – Выполнение базового набора мер по защите информации 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения «m-TrusT Терминал»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	Выполняются входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.1.2, 4.1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
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		1. см. п.п. 4.10.1, 4.10.2 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора». 2. см. п.п. 4.1.4 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение,	+ все	+ все		1. см. документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		уничтожение идентификаторов				Администратора» п.п. 4.2.
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		1. см. п.п. 4.2 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все		1. см. п.п. 4.1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
6	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+ все	+ все	Выполняется входящим в состав СРД «Аккорд-Х К».	
		Управление доступом субъектов доступа к объектам доступа (УПД)				
7	УПД.1	Управление учетными записями пользователей	+ все	+ все	Выполняются входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.3.2, 4.3.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». 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		1. см. п.п. 4.3.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
9	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной	+ все	+ все		1. см. п.п. 4.3.4, 4.3.5 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		системы				
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 системе)	+ все	+ все		1. см. п.п. 4.3.2, 4.3.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
12	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	не входит в базовый набор мер	+ в 1 классе защищенности ИС	При необходимости реализации данной меры необходимо использовать ту ОС, для которой данная меры выполняется. Например, из списка поддерживаемых m-TrusT ОС – это Astra Linux.	
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	Выполняется входящим в состав СРД «Аккорд-Х К».	1. см. п.п. 4.2.9 документа «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Х К». Руководство администратора».
14	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+ начиная с 3 уровня защищенности ПДн	+ все	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
15	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные связи	+ все	+ все	Выполняется входящим в состав СКЗИ.	1. см. п.п. 1, 2.2, 2.6, 9 документа «Микрокомпьютер m-TrusT. Технические условия».
16	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических устройств	+ все	+ все	Выполняется входящим в состав СРД «Аккорд-Х К».	1. 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	«m-TrusT Терминал»	Ссылки на документацию
17	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники[1]	+ начиная со 2 уровня защищённости ПДн	+ начиная со 2 класса защищенности ИС	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 1.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
		Ограничение программной среды (ОПС)				
18	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	не входит в базовый набор мер	+ в 1 классе защищённости ИС	Выполняется за счет архитектуры микрокомпьютера «m-TrusT», входящего в состав комплекса.	1. см. п.п. 2.2, 2.9 документа «Микрокомпьютер m-TrusT. Технические условия».
19	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	+ начиная со 2 уровня защищённости ПДн	+ начиная со 2 класса защищенности ИС	Выполняется в варианте реализации «Центр-TrusT».	
20	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+ на 1 уровне защищенности ПДн	+ все		
		Защита машинных носителей персональных данных (ЗНИ)				
21	ЗНИ.2	Управление доступом к машинным носителям персональных	+ начиная с 2 уровня защищенности	+ все	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.1.4 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство

[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	«m-TrusT Терминал»	Ссылки на документацию
		данных	ПДн			Пользователя». 2. см. п.п. 4.10.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
22	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	Выполняется входящим в состав СРД «Аккорд-Х К».	1. см. п.п. 4.2.12 документа «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Х К»,.
23	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	+ все	+ все		1. п.п 3.2.2, 5.2 документа «Аккорд-Х К. Руководство администратора».
		Регистрация событий безопасности (РСБ)				
24	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+ все	+ все	Выполняются входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
25	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ все	+ все		
26	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все		
27	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и	не входит в базовый набор мер	+ все	Выполняются входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
28	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+ начиная со 2 уровня защищенности ПДн	+ все		
29	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	не входит в базовый набор мер	+ все	Выполняется входящей в состав собственной системой времени, предварительно настроенной пользователем или синхронизированной с внешним источником.	
30	РСБ.7	Защита информации о событиях безопасности	+ все	+ все	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
		Антивирусная защита (АВЗ)				
31	АВЗ.1	Реализация антивирусной защиты	+ все	+ все	Выполняется за счет архитектуры микрокомпьютера «m-TrusT», входящего в состав комплекса.	
		Контроль (анализ) защищенности персональных данных (АНЗ)				
32	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ все	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации. Обновление ПО выполняется в сервисном центре Разработчика ПО.	
33	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Выполняются входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	
34	АНЗ.3	Контроль работоспособности, параметров	+ начиная с 3 уровня	+ все		1. см. п.п. 4.1, 4.16 документа «Модуль доверенной загрузки

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		настройки и правильности функционирования программного обеспечения и средств защиты информации	защищенности ПДн			«Аккорд-МКТ». Руководство Администратора».
35	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все		1. см. п.п. 4.10 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
36	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	+ начиная со 2 уровня защищенности ПДн	+ все	Выполняется входящим в состав СРД «Аккорд-Х К».	1. см. п.п. 4.3.2, 4.3.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
37	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.10 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
38	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	не входит в базовый набор мер	+ все	Выполняется за счет архитектуры микрокомпьютера «m-TrusT», входящего в состав комплекса.	1. см. п.п. 4.14 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
39	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ начиная 1 класса защищенности ИС	Выполняется входящим в состав СРД «Аккорд-Х К».	1. п.п. 3.2.6, 3.2.7 документа «Аккорд-Х К. Руководство администратора».
		Обеспечение доступности персональных данных (ОДТ)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
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	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. п.п. 4.16 документа «Аккорд-МКТ. Руководство администратора».
41	ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	+ начиная с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС		1. см. п.п. 4.14.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
42	ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала	+ начиная с 2 уровня защищенности ПДн	+ начиная с 2 класса защищенности ИС		1. см. п.п. 4.14.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». 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 персональных данных, функций по обработке персональных данных и иных функций информационной системы	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
44	ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к	+ все	+ все	Выполняется за счет СКЗИ, входящего в состав микрокомпьютера «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи				
45	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	не входит в базовый набор мер	+ все	Выполняется входящим в состав платформы СРД «Аккорд-Х К».	1. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
46	ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Выполняется за счет СКЗИ, входящего в состав «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
47	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Выполняется входящими в состав датчиком случайных чисел, за счет особенностей архитектуры комплекса, а также сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.1.4 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя». 2. см. п.п. 4.10.2, 4.10.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
48	ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+ начиная с 3 уровня защищенности ПДн	+ все	Выполняется за счет СКЗИ, входящего в состав «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
49	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	нет	+ в 1 классе защищенности ИС	Выполняется за счет архитектуры комплекса. Также обеспечивается за счет средств СДЗ уровня BIOS «Аккорд-МКТ», входящего в состав платформы.	1. п.п. 5.1.1, 6.1.10 документа «Модуль доверенной загрузки «Аккорд-МКТ». Задание по безопасности».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		информационной системы				
50	ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	нет	+ начиная со 2 класса защищенности ИС	Выполняется за счет СКЗИ, входящего в состав микрокомпьютера «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
51	ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	нет	+ все	Выполняется входящим в состав СРД «Аккорд-Х К».	1. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
		Выявление инцидентов и реагирование на них (ИНЦ)				
52	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищённости ПДн	нет	Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
		Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)				
53	УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	+ начиная с 3 уровня защищенности ПДн	нет	Выполняется в варианте реализации «Центр-TrusT».	

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 «m-TrusT Терминал»

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 «m-TrusT Терминал».

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 «m-TrusT Терминал»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	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		Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. п.п. 1.1, 4.10.3 документа «Аккорд-МКТ. Руководство администратора».
		Защита машинных носителей персональных данных (ЗНИ)				
2	ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах			Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.1.4 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя». 2. см. п.п. 4.10.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
3	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных			Выполняется входящим в состав СРД «Аккорд-Х К».	1. см. п.п. 4.2.12 документа «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Х К».
4	ЗНИ.7	Контроль подключения машинных носителей персональных данных				
		Регистрация событий безопасности (РСБ)				
5	РСБ.8	Обеспечение возможности просмотра и анализа	нет		Выполняется входящим в состав сертифицированным	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		информации о действиях отдельных пользователей в информационной системе			СДЗ уровня BIOS «Аккорд-МКТ».	Руководство Администратора».
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
6	ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы			Выполняется входящим в состав сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. п.п. 4.10 документа «Аккорд-МКТ. Руководство администратора».
7	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			Выполняется входящим в состав СРД «Аккорд-Х К».	1. п.п. 3.2.12 документа «Аккорд-Х К. Руководство администратора.
8	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях			Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. п.п. 4.3.2, 4.12.1, Приложение 3 документа «Аккорд-МКТ. Руководство администратора».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
9	ЗИС.4	Обеспечение доверенных канала, маршрута между			Выполняется за счет СКЗИ, входящего в состав комплекса.	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«m-TrusT Терминал»	Ссылки на документацию
		администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
10	ЗИС.14	Использование устройств терминального доступа для обработки персональных данных			Выполняется за счет наличия встроенных клиентов удаленного рабочего стола.	1. см. п. 4 документа «Автоматизированное рабочее место «m-TrusT Терминал». Руководство по быстрому старту».
11	ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			Выполняется за счет архитектуры комплекса	
12	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			Выполняется за счет архитектуры микрокомпьютера «m-TrusT», входящего в состав комплекса.	
13	ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем	нет		Микрокомпьютер m-TrusT, на базе которого выполнен терминал, предназначен для использования в средах различных ОС.	
14	ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы	нет		Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. п.п. 1.1, 4.14, 4.16 документа «Аккорд-МКТ. Руководство администратора».

Итак, путем применения «m-TrusT Терминал» в информационной системе выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 3, 4, 5, 6;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 13, 15, 17;

ОПС: 1, 2, 3;

ЗНИ: 2, 5, 8;

РСБ: 1, 2, 3, 4, 5, 6, 7;

АВЗ: 1;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 3, 4, 5;

ЗИС: 1, 3, 5, 11, 15, 20, 21, 22, 30;

ИНЦ: 2;

УКФ: 2;

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

ИАФ: 7;

ЗНИ: 4, 6, 7;

РСБ: 8;

ОЦЛ: 2, 5, 8;

ЗИС: 4, 14, 16, 19, 26, 29.

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