ВЫПОЛНЕНИЕ МЕР 31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ СПЕЦИАЛИЗИРОВАННЫХ МИКРОКОМПЬЮТЕРОВ «M-TRUST»

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 специализированных микрокомпьютеров «m-TrusT».

Специализированные микрокомпьютеры «m-TrusT» (ТУ 26.20.40.140-083-37222406-2019) представляют собой одноплатные компьютеры Новой гарвардской архитектуры с общим назначением – платформа для СЗИ (в том числе, СКЗИ), коммутируемых с различными техническими средствами объектов КИИ, АСУ ТП и др.

Конструктивно микрокомпьютеры «m-TrusT» включают в себя док-станцию (интерфейсную плату), которая стационарно включается в состав технического средства, и подключаемого к ней универсального по своему аппаратному исполнению модуля – мезонина («m» в названии микрокомпьютера – это именно «мезонин»).

Исполнения, в том числе, состав интерфейсов док-станции могут существенно различаться, так как ее задача – коммутация с различными техническими средствами – от локомотивов до банкоматов, от газовых счетчиков до терминалов управления АЭС.

В зависимости от задачи, на платформе «m-TrusT» создаются различные средства защиты – криптошлюза, терминалы СКУД, межсетевые экраны и мн. др. Эти продукты могут выпускаться как разработчиком «m-TrusT», так и другими вендорами, иметь различные торговые названия и функциональные характеристики. В настоящем документе приведены возможности выполнения мер Приказа ФСТЭК № 31, характеризующие именно платформу, то есть универсальные для всех изделий на ней. Возможности выполнения мер конкретными изделиями могут быть шире, чем возможности платформы, но все возможности платформы релевантны для всех изделий, построенных на ней.

Ресурсы «m-TrusT» позволяют обеспечить среду функционирования криптографии (СФК), позволяющую сертифицировать вариант исполнения СКЗИ на «m-TrusT» на класс КС3. Помимо Новой гарвардской архитектуры защищенность платформы обеспечивается РКБ и СДЗ уровня BIOS («Аккорд-МКТ»), сертифицированным ФСТЭК России.

Основными особенностями микрокомпьютеров «m-TrusT» являются:

- Новая гарвардская архитектура, обеспечивающая «вирусный иммунитет»;
- аппаратная поддержка реализации доверенной загрузки;
- функциональная замкнутость среды;
- аппаратное обеспечение целостности;
- аппаратное резидентное решение по неизвлекаемости ключа;
- аппаратный ДСЧ.

2 Выполнение базового набора мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения специализированных микрокомпьютеров «m-TrusT»

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения специализированных микрокомпьютеров «m-TrusT».

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

Таблица 1 – Выполнение базового набора мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения специализированных микрокомпьютеров «m-TrusT»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			
1	ИАФ.0	Разработка политики идентификации и аутентификации	+ все	Подсистемы идентификации и аутентификации и администрирования СДЗ «Аккорд-МКТ», установленного в «m-TrusT», позволяют реализовать любую непротиворечивую политику идентификации и аутентификации.	
2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+ все	Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1 см. п.п. 4.1.2, 4.1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
3	ИАФ.2	Идентификация и аутентификация устройств	+ все		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».
4	ИАФ.3	Управление идентификаторами	+ все		1. см. п.п. 4.2 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
5	ИАФ.4	Управление средствами аутентификации	+ все		1. см. п.п. 4.2 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
6	ИАФ.5	Идентификация и аутентификация внешних пользователей	+ все	Выполняется входящим в состав платформы СРД «Аккорд-Х К».	
7	ИАФ.7	Защита аутентификационной информации при передаче	+ все	Выполняется входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
		Управление доступом (УПД)			
8	УПД.0	Разработка политики управления доступом	+ все	Подсистемы администрирования и блокировки загрузки СДЗ «Аккорд-МКТ» и	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
				подсистема администрирования СРД «Аккорд-Х К», установленных в «m-TrusT», а также СКЗИ из состава «m-TrusT» в совокупности с ОС, средствами которой обеспечивается реализация мер группы УПД, позволяют реализовать любую непротиворечивую политику управления доступом.	
9	УПД.1	Управление учетными записями пользователей	+ все	Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.3.2, 4.3.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
10	УПД.2	Реализация политик управления доступом	+ все		1. см. п.п. 4.3.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
11	УПД.3	Доверенная загрузка	+ начиная со 2 класса защищенности автоматизированной системы управления		1. см. п.п. 1.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
12	УПД.4	Разделение полномочий (ролей) пользователей	+ все		1. см. п.п. 4.3.4, 4.3.5 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
13	УПД.5	Назначение минимально необходимых прав и привилегий	+ все		
14	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+ все		1. см. п.п. 4.3.2, 4.3.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
15	УПД.9	Ограничение числа параллельных сеансов доступа	+ в 1 классе защищенности автоматизированной системы управления	При необходимости реализации данной меры необходимо использовать ту ОС, для которой данная мера выполняется. Например, из списка поддерживаемых m-TrusT ОС – это Astra Linux.	
16	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+ все	Выполняется входящим в состав платформы 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».
17	УПД.11	Управление действиями пользователей до идентификации и аутентификации	+ все	Выполняется входящим в состав платформы сертифицированным	1. см. п.п. 1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
				СДЗ уровня BIOS «Аккорд-МКТ».	Пользователя».
18	УПД.13	Реализация защищенного удаленного доступа	+ все	Выполняется входящим в состав платформы СКЗИ.	1. см. п.п. 1, 2.2, 2.6, 9 документа «Микрокомпьютер m-TrusT. Технические условия».
		Ограничение программной среды (ОПС)			
19	ОПС.0	Разработка политики ограничения программной среды	+ начиная со 2 класса защищенности автоматизированной системы управления	Архитектура платформы «m-TrusT» позволяет реализовать любую непротиворечивую политику ограничения программной среды.	
20	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ в 1 классе защищенности автоматизированной системы управления	Выполняется за счет архитектуры комплекса.	1. см. п.п. 2.2, 2.9 документа «Микрокомпьютер m-TrusT. Технические условия».
		Защита машинных носителей информации (ЗНИ)			
21	ЗНИ.0	Разработка политики защиты машинных носителей информации	+ все	Подсистема блокировки загрузки СДЗ «Аккорд-МКТ» и подсистема управления доступом СРД «Аккорд-Х К», установленных в «m-TrusT», позволяют реализовать любую непротиворечивую политику защиты машинных носителей информации.	
22	ЗНИ.2	Управление физическим доступом к машинным носителям информации	+ все	Выполняется входящим в состав платформы 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».
23	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ все	Выполняется входящим в состав платформы СРД «Аккорд-Х К».	1. см. п.п. 4.2.12 документа «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Х К».
24	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	+ в 1 классе защищенности автоматизированной системы управления		
25	ЗНИ.7	Контроль подключения машинных носителей информации	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
26	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+ все		1. п.п 3.2.2, 5.2 документа «Аккорд-X K. Руководство администратора».
		Аудит безопасности (АУД)			
27	АУД.0	Разработка политики аудита безопасности	+ все	Подсистема аудита СДЗ «Аккорд-МКТ», установленного в «m-TrusT», в совокупности с собственной системой времени микрокомпьютера «m-TrusT» позволяют реализовать любую непротиворечивую политику аудита безопасности.	
28	АУД.2	Анализ уязвимостей и их устранение	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации. Обновление ПО выполняется в сервисном центре Разработчика ПО.	
29	АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+ все	Выполняется входящей в состав собственной системой времени, предварительно настроенной пользователем или синхронизированной с внешним источником.	
30	АУД.4	Регистрация событий безопасности	+ все	Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
31	АУД.6	Защита информации о событиях безопасности	+ все		
32	АУД.7	Мониторинг безопасности	+ все		
33	АУД.8	Реагирование на сбои при регистрации событий безопасности	+ все		
21	АУД.9	Анализ действий пользователей	+ начиная с 1 класса защищенности автоматизированной системы		
		Антивирусная защита (АВЗ)			
34	АВЗ.0	Разработка политики антивирусной защиты	+ все	Архитектура платформы «m-TrusT» позволяет реализовать любую непротиворечивую	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
				политику антивирусной защиты.	
35	АВЗ.1	Реализация антивирусной защиты	+ все	Выполняется за счет архитектуры комплекса.	
		Обеспечение целостности (ОЦЛ)			
36	ОЦЛ.0	Разработка политики обеспечения целостности	+ все	Подсистемы контроля целостности и администрирования СДЗ «Аккорд-МКТ», установленного в «m-TrusT», позволяют реализовать любую непротиворечивую политику обеспечения целостности.	
37	ОЦЛ.1	Контроль целостности программного обеспечения	+ все	Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.10.2, 4.10.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
38	ОЦЛ.3	Ограничение по вводу информации в информационную (автоматизированную) систему	+ начиная с 1 класса защищенности автоматизированной системы управления	Выполняется входящим в состав платформы СРД «Аккорд-Х К».	1. п.п. 3.2.6, 3.2.7 документа «Аккорд-Х К. Руководство администратора».
39	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+ начиная со 2 класса защищенности автоматизированной системы управления		1. п.п. 3.2.12 документа «Аккорд-Х К. Руководство администратора.
40	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	Выполняются входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя». 2. см. п.п. 4.2.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
		Обеспечение доступности (ОДТ)			
41	ОДТ.0	Разработка политики обеспечения доступности	+ все	Подсистема администрирования СДЗ «Аккорд-МКТ», установленного в «m-TrusT», а также архитектура комплекса позволяют реализовать любую непротиворечивую политику обеспечения доступности.	
42	ОДТ.3	Контроль безотказного функционирования средств и систем	+ во 2 классе защищенности	Выполняется входящим в состав платформы сертифицированным	1. п.п. 4.16 документа «Аккорд-МКТ. Руководство администратора».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
			автоматизированной системы управления	СДЗ уровня BIOS «Аккорд-МКТ».	
43	ОДТ.4	Резервное копирование информации	+ все		1. см. п.п. 4.10.2, 4.14 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
44	ОДТ.5	Обеспечение возможности восстановления информации	+ все		
45	ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+ все	Выполняется за счет архитектуры комплекса.	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
46	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+ все	Подсистемы администрирования и контроля целостности СДЗ «Аккорд-МКТ», установленного в «m-TrusT», а также СКЗИ из состава «m-TrusT» и архитектура комплекса позволяют реализовать любую непротиворечивую политику защиты информационной (автоматизированной) системы и ее компонентов.	
47	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+ все	Выполняется входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
48	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 класса защищенности автоматизированной системы управления	Выполняется входящими в состав платформы 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».
49	ЗИС.16	Защита от спама	+ начиная со 2 класса защищенности автоматизированной системы управления	Выполняется за счет архитектуры комплекса.	
50	ЗИС.19	Защита информации при ее передаче по каналам связи	+ все	Выполняется за счет СКЗИ, входящего в состав комплекса.	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
51	ЗИС.20	Обеспечение доверенных канала, маршрута	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
52	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+ все	Выполняется входящим в состав платформы СРД «Аккорд-Х К».	1. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
53	ЗИС.27	Обеспечение подлинности сетевых соединений	+ начиная со 2 класса защищенности автоматизированной системы управления	Выполняется за счет СКЗИ, входящего в состав «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
54	ЗИС.31	Защита от скрытых каналов передачи информации	+ в 1 классе защищенности автоматизированной системы управления	Выполняется за счет архитектуры комплекса.	
55	ЗИС.32	Защита беспроводных соединений	+ все	Выполняется за счет СКЗИ, входящего в состав «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
56	ЗИС.33	Исключение доступа через общие ресурсы	+ в 1 классе защищенности автоматизированной системы управления	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».
57	ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+ все	Выполняется за счет СКЗИ, входящего в состав «m-TrusT».	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
58	ЗИС.38	Защита информации при использовании мобильных устройств	+ все	Выполняется входящим в состав СРД «Аккорд-Х К».	1. п.п 3.2.12 документа «Аккорд-Х К. Руководство администратора».
		Реагирование на компьютерные инциденты (ИНЦ)			
59	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+ все	Подсистема аудита позволяет реализовать любую непротиворечивую политику реагирования на компьютерные инциденты.	
60	ИНЦ.1	Выявление компьютерных инцидентов	+ все	Выполняется входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
61	ИНЦ.2	Информирование о компьютерных инцидентах	+ все		
		Управление обновлениями программного обеспечения (ОПО)			
62	ОПО.0	Разработка политики управления обновлениями программного обеспечения	+ все	Применение ОС, средствами которой обеспечивается реализация мер группы ОПО, позволяют реализовать любую непротиворечивую	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
				политику управления обновлениями программного обеспечения.	
63	ОПО.2	Контроль целостности обновлений программного обеспечения	+ все	Выполняются за счет наличия возможности обновления ПО встроенной ОС.	
64	ОПО.4	Установка обновлений программного обеспечения	+ все		
		Обеспечение действий в нештатных ситуациях (ДНС)			
65	ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+ все	Выполняется входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	
66	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций	+ начиная со 2 класса защищенности автоматизированной системы управления		1. п.п. 1.1, 4.14, 4.16 документа «Аккорд-МКТ. Руководство администратора».
67	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+ все		

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения специализированных микрокомпьютеров «m-TrusT»

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 специализированных микрокомпьютеров «m-TrusT».

Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения специализированных микрокомпьютеров «m-TrusT»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
1	ИАФ.6	Двусторонняя аутентификация		Выполняется входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ» и ОС.	
		Управление доступом (УПД)			
2	УПД.12	Управление атрибутами безопасности		Выполняется входящим в состав платформы СРД «Аккорд-Х К».	1. п.п. 3.2.6, 3.2.7, 5.2 документа «Аккорд-Х К. Руководство администратора».
		Защита машинных носителей информации (ЗНИ)			
3	ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации		Выполняется входящим в состав платформы 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».
		Обеспечение целостности (ОЦЛ)			
4	ОЦЛ.2	Контроль целостности информации		Выполняется входящим в состав платформы сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.10.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
		Обеспечение доступности (ОДТ)			
5	ОДТ.7	Кластеризация информационной (автоматизированной) системы		Выполняется за счет наличия варианта исполнения m-TrusT «в стойку».	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
6	ЗИС.6	Управление сетевыми потоками		При необходимости реализации данной меры необходимо использовать ту ОС, для которой данная меры выполняется. Например, из списка поддерживаемых m-TrusT ОС – это Astra Linux.	
7	ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем		m-TrusT предназначен для использования в средах различных ОС.	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	«m-TrusT»	Ссылки на документацию
8	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		Выполняется за счет архитектуры платформы.	
9	ЗИС.17	Защита информации от утечек			
10	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. Выполняется 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» в автоматизированной системе управления выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 3, 4, 5, 7;

УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11, 13;

ОПС: 1;

ЗНИ: 2, 5, 6, 7, 8;

АУД: 2, 3, 4, 6, 7, 8, 9;

АВЗ: 1;

ОЦЛ: 1, 3, 4, 5;

ОДТ: 3, 4, 5, 6;

ЗИС: 1, 13, 16, 19, 20, 21, 27, 31, 32, 33, 34, 38;

ИНЦ: 1, 2;

ОПО: 2, 4;

ДНС: 4, 5;

а также дополнительные (не включенные в базовый набор) меры:
ИАФ: 6;
УПД: 12;
ЗНИ: 4;
ОЦЛ: 2;
ОДТ: 7;
ЗИС: 6, 10, 12, 17, 37.

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