ВЫПОЛНЕНИЕ МЕР 239-ГО ПРИКАЗА ФСТЭК ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПУТЕМ ПРИМЕНЕНИЯ КРИПТОШЛЮЗОВ FIN-TRUST

ОКБ САПР
2021

1 Общие положения

В настоящем документе рассматривается выполнение мер 239-го Приказа ФСТЭК по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации путем применения криптошлюзов «fin-TrusT» (далее по тексту – «fin-TrusT» либо комплекс).

Устройство «fin-TrusT», представляет собой криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации на базе защищенного микрокомпьютера «m-TrusT». С помощью криптошлюзов «fin-TrusT» защищаются коммуникации между подразделениями и офисами банков, банком и процессинговым центром, процессинговым центром и банкоматами. Выполняются требования законодательства, блокируются уязвимости во взаимодействии в финансовой сфере.

Линейка криптошлюзов fin-TrusT включает:

– «fin-TrusT банкомат» – криптошлюз в технологическом корпусе для установки в банкоматы с возможностью поддержки двух и более операторов мобильной сети Интернет.

– «fin-TrusT офис» – криптошлюз в корпусе одноюнитового сервера для установки в бэк- или фронт-офис до 50 абонентских устройств.

– «fin-TrusT центр» – сервер VPN для установки в ЦОД или серверную стойку головного отделения.

«Fin-TrusT банкомат» поддерживает одновременную работу нескольких независимых каналов связи. К примеру, могут быть подключены два коннектора Ethernet от различных провайдеров и/или два LTE-модема различных операторов связи. Это позволяет продолжить работу даже при отказе одного из каналов, что повышает отказоустойчивость и является актуальной задачей именно для банкоматов.

В зависимости от архитектуры сети в качестве ответной части решения может использоваться такое же устройство в исполнении в стойку (если требуется небольшое количество подключений и ресурсы сервера VPN избыточны) или обыкновенный сервер VPN, стоимость которого ощутимо выше.

Криптошлюз функционирует прозрачно для пользователя, не добавляя никаких действий в его привычный набор действий.

Каждый микрокомпьютер «m-TrusT» является точкой сбора информационных и/или управляющих сигналов от ПКО, их шифрования для передачи по каналам связи, а также приема зашифрованных сигналов из каналов связи и их расшифровкой.

Наличие собственной ОС и вычислительных ресурсов позволяет обеспечить достаточную для защиты сетевого взаимодействия производительность (возможна защищенная передача видеосигнала с камер без ощутимого снижения качества изображения) и высокий уровень защищенности.

Наличие датчика случайных чисел и размещение ПО в памяти с физически устанавливаемым доступом read only (только чтение) в защищенных микрокомпьютерах «m-TrusT» исключает вредоносное воздействие на ПО и обеспечивает неизменность среды функционирования средств криптографической защиты информации. Ресурсы «m-TrusT» позволяют обеспечить СФК, позволяющую сертифицировать вариант исполнения СКЗИ на «m-TrusT» на класс КС3. Помимо Новой гарвардской архитектуры защищенность платформы обеспечивается РКБ и СДЗ, сертифицированным ФСТЭК России.

Встроенное по умолчанию в fin-TrusT СКЗИ – DCrypt от компании ТСС – сертифицировано ФСБ России России в исполнениях на «m-TrusT» на классы КС2 и КС3.

2 Выполнение базового набора мер, определенных 239-ым Приказом ФСТЭК России по обеспечению безопасности значимых объектов критической информационной инфраструктуры, путем применения криптошлюзов «fin-TrusT»

В таблице № 1 представлено описание выполнения базового набора мер 239-го Приказа ФСТЭК по обеспечению безопасности значимых объектов критической информационной инфраструктуры путем применения криптошлюзов «fin-TrusT».

Выражение «все» в ячейках столбца «Категория значимости» означает, что рассматриваемая мера должна быть реализована для объектов критической информационной инфраструктуры с любой категорией значимости.

Таблица 1 – Выполнение базового набора мер по защите информации 239-го Приказа ФСТЭК по обеспечению безопасности значимых объектов критической информационной инфраструктуры путем применения криптошлюзов «fin-TrusT»

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
		Идентификация и аутентификация (ИАФ)			
1	ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+ все	Подсистемы идентификации и аутентификации и администрирования СДЗ «Аккорд-МКТ», входящего в состав «fin-TrusT», обеспечивают выполнение любых непротиворечивых правил и процедур идентификации и аутентификации.	
2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+ все	Выполняются входящим в состав продукта 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 идентификации	+ 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	1. см. п.п. 4.1.3 документа «Модуль доверенной загрузки

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
				сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	«Аккорд-МКТ». Руководство Пользователя».
		Управление доступом (УПД)			
8	УПД.0	Регламентация правил и процедур управления доступом	+ все	Подсистемы администрирования и блокировки загрузки СДЗ «Аккорд-МКТ» и подсистема администрирования СРД «Аккорд-Х К», установленных в «fin-TrusT», а также СКЗИ из состава «fin-TrusT» в совокупности с ОС, средствами которой обеспечивается реализация мер группы УПД, обеспечивают выполнение любых непротиворечивых правил и процедур управления доступом.	
9	УПД.1	Управление учетными записями пользователей	+ все	Выполняются входящим в состав продукта 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 категории значимости		1. см. п.п. 1.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
12	УПД.4	Разделение полномочий (ролей) пользователей	+ все		1. п.п. 4.3 документа «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	+ при 1 категории значимости	При необходимости реализации данной меры необходимо использовать ту ОС, для которой данная меры 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 микрокомпьютера «m-TrusT» 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

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
					администратора».
17	УПД.11	Управление действиями пользователей до идентификации и аутентификации	+ все	Выполняется входящим в состав продукта сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
18	УПД.13	Реализация защищенного удаленного доступа	+ все	Выполняются входящим в состав продукта СКЗИ.	1. см. п.п. 1, 2.2, 2.6, 9 документа «Микрокомпьютер m-TrusT. Технические условия».
19	УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+ все		
		Ограничение программной среды (ОПС)			
20	ОПС.0	Регламентация правил и процедур ограничения программной среды	+ начиная со 2 категории значимости	Архитектура платформы «m-TrusT» из состава продукта «fin-TrusT» обеспечивает выполнение любых непротиворечивых правил и процедур ограничения программной среды.	
21	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ при 1 категории значимости	Выполняется за счет архитектуры комплекса.	1. см. п.п. 2.2, 2.9 документа «Микрокомпьютер m-TrusT. Технические условия».
		Аудит безопасности (АУД)			
22	АУД.0	Регламентация правил и процедур аудита безопасности	+ все	Подсистема аудита СДЗ «Аккорд-МКТ», входящего в состав «fin-TrusT», в совокупности с собственной системой времени микрокомпьютера «m-TrusT» и СКЗИ обеспечивают выполнение любых непротиворечивых правил и процедур аудита безопасности.	
23	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.	
24	АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+ все	Выполняется входящей в состав «m-TrusT» собственной системой времени, предварительно настроенной пользователем или синхронизированной с внешним источником.	
25	АУД.4	Регистрация событий безопасности	+ все	Выполняется входящим в состав продукта сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
26	АУД.5	Контроль и анализ сетевого трафика	+ при 1 категории значимости	Выполняются входящим в состав продукта СКЗИ.	1. см. п.п. 1, 2.2, 2.6, 9 документа «Микрокомпьютер m-TrusT. Технические условия».
27	АУД.6	Защита информации о событиях безопасности	+ все	Выполняются входящим в состав продукта сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.11 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
28	АУД.7	Мониторинг безопасности	+ все		
29	АУД.8	Реагирование на сбои при регистрации событий безопасности	+ все		
30	АУД.9	Анализ действий отдельных пользователей	+ при 1 категории значимости		
		Антивирусная защита (АВЗ)			
31	АВЗ.0	Регламентация правил и процедур антивирусной защиты	+ все	Архитектура платформы «m-TrusT» из состава продукта «fin-TrusT» обеспечивает выполнение любых непротиворечивых правил и процедур антивирусной защиты	
32	АВЗ.1	Реализация антивирусной защиты	+ все	Выполняется за счет архитектуры комплекса.	
		Обеспечение целостности (ОЦЛ)			
33	ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+ все	Подсистемы контроля целостности и администрирования СДЗ «Аккорд-МКТ», входящего в состав «fin-TrusT», обеспечивают выполнение любых непротиворечивых правил и процедур обеспечения целостности.	
34	ОЦЛ.1	Контроль целостности программного обеспечения	+ все	Выполняются входящим в состав продукта сертифицированным СДЗ уровня BIOS «Аккорд-МКТ».	1. см. п.п. 4.10.2, 4.10.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
35	ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	+ при 1 категории значимости		1. см. п.п. 4.3.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
36	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+ начиная со 2 категории значимости		1. см. п.п. 4.1.3 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Пользователя».
37	ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+ начиная со 2 категории значимости		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

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
					Администратора».
		Обеспечение доступности (ОДТ)			
38	ОДТ.0	Регламентация правил и процедур обеспечения доступности	+ все	Архитектура комплекса обеспечивает выполнение непротиворечивых правил и процедур обеспечения доступности.	
39	ОДТ.1	Использование отказоустойчивых технических средств	+ начиная со 2 категории значимости	Выполняется за счет возможности одновременной работы нескольких независимых каналов связи (могут быть подключены два коннектора Ethernet от различных провайдеров и/или два LTE-модема различных операторов связи).	
40	ОДТ.3	Контроль безотказного функционирования средств и систем	+ начиная со 2 категории значимости	Выполняется за счет средств СДЗ «Аккорд-МКТ», входящего в состав «fin-TrusT».	1. п.п. 4.16 документа «Аккорд-МКТ. Руководство администратора».
41	ОДТ.4	Резервное копирование информации	+ все		1. см. п.п. 4.10.2, 4.14 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
42	ОДТ.5	Обеспечение возможности восстановления информации	+ все		
43	ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+ все	Выполняется за счет архитектуры платформы «m-TrusT», входящей в состав продукта.	
		Защита технических средств и систем (ЗТС)			
44	ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+ все	За счет архитектуры комплекса обеспечивается выполнение непротиворечивых правил и процедур защиты технических средств и систем.	
45	ЗТС.3	Управление физическим доступом	+ все	Выполняется за счет наличия возможности контроля и управления физическом доступом путем организации передачи видеосигнала с камер видеонаблюдения без снижения качества изображения.	

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
46	ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+ все	Подсистемы администрирования и контроля целостности СДЗ «Аккорд-МКТ», входящего в состав «fin-TrusT», а также СКЗИ из состава «fin-TrusT» и архитектура комплекса обеспечивают выполнение непротиворечивых правил и процедур 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.2	Защита периметра информационной (автоматизированной) системы	+ все	Выполняется за счет: – Новой гарвардской архитектуры микрокомпьютера «m-TrusT», – РКБ, встроенного в основной аппаратный блок микрокомпьютера «m-TrusT», СКЗИ, входящего в состав комплекса.	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
49	ЗИС.6	Управление сетевыми потоками	+ все	Выполняется за счет СКЗИ, входящего в состав комплекса.	
50	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 категории значимости	Выполняется входящими в состав платформы «m-TrusT» и 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».
51	ЗИС.16	Защита от спама	+ начиная со 2 категории значимости	Выполняется за счет архитектуры платформы «m-TrusT», входящей в состав продукта.	
52	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».
53	ЗИС.20	Обеспечение доверенных канала, маршрута	+ все		
54	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».
55	ЗИС.27	Обеспечение подлинности	+	Выполняется за счет	1. см. п.п. 2.2 документа

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
		сетевых соединений	начиная со 2 категории значимости	СКЗИ, входящего в состав комплекса.	«Микрокомпьютер m-TrusT. Технические условия».
56	ЗИС.32	Защита беспроводных соединений	+ все	Выполняется за счет СКЗИ, входящего в состав комплекса.	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
57	ЗИС.33	Исключение доступа через общие ресурсы	+ в 1 категории значимости	Выполняется за счет архитектуры микрокомпьютера «m-TrusT» и РКБ, встроенного в основной аппаратный блок микрокомпьютера «m-TrusT».	
58	ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+ все	Выполняется за счет СКЗИ, входящего в состав комплекса.	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
59	ЗИС.35	Управление сетевыми соединениями	+ все		
60	ЗИС.38	Защита информации при использовании мобильных устройств	+ все	Выполняется за счет выполнения мер ИАФ.1, ИАФ.7, УПД.2, УПД.13, АУД.4, АУД.7, АВЗ.1, ОЦЛ.1.	
		Реагирование на компьютерные инциденты (ИНЦ)			
61	ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+ все	Подсистема аудита СДЗ «Аккорд-МКТ», входящего в состав «fin-TrusT», в совокупности с собственной системой времени микрокомпьютера «m-TrusT» и СКЗИ обеспечивают выполнение любых непротиворечивых правил и процедур аудита безопасности.	
62	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».
63	ИНЦ.2	Информирование о компьютерных инцидентах	+ все		
		Управление обновлениями программного обеспечения (ОПО)			
64	ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+ все	Применение ОС, средствами которой обеспечивается реализация мер группы ОПО, обеспечивают выполнение любых непротиворечивых правил и процедур управления обновлениями	

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
				программного обеспечения.	
65	ОПО.2	Контроль целостности обновлений программного обеспечения	+ все	Выполняется входящим в состав микрокомпьютером «m-TrusT».	
66	ОПО.4	Установка обновлений программного обеспечения	+ все		
		Обеспечение действий в нештатных ситуациях (ДНС)			
67	ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+ все	Архитектура комплекса и «Аккорд-МКТ», входящий в состав «fin-TrusT», обеспечивают выполнение непротиворечивых правил и процедур обеспечения действий в нештатных ситуациях.	
68	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций	+ во 2 категории значимости	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».
69	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+ все		

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 239-ым приказом ФСТЭК России по обеспечению безопасности значимых объектов критической информационной инфраструктуры, путем применения криптошлюзов «fin-TrusT»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 239-го приказа ФСТЭК по обеспечению безопасности значимых объектов критической информационной инфраструктуры путем применения криптошлюзов «fin-TrusT».

Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 239-го приказа ФСТЭК по обеспечению безопасности значимых объектов критической информационной инфраструктуры путем применения криптошлюзов «fin-TrusT»

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию

№	Усл. обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости	«fin-TrusT»	Ссылки на документацию
		Обеспечение целостности (ОЦЛ)			
1	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)			
2	ОДТ.7	Кластеризация информационной системы (автоматизированной) системы		Выполняется за счет наличия варианта исполнения m-TrusT «в стойку».	
		Защита технических средств и систем (ЗТС)			
3	ЗТС.1	Защита информации от утечки по техническим каналам		Выполняется за счет архитектуры комплекса.	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
4	ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем		Микрокомпьютер «m-TrusT», на базе которого выполнены криптошлюзы «fin-TrusT», предназначен для использования в средах различных ОС.	
5	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		Выполняется за счет архитектуры платформы.	
6	ЗИС.17	Защита информации от утечек		Выполняется за счет входящего в состав СКЗИ	1. см. п.п. 2.2 документа «Микрокомпьютер m-TrusT. Технические условия».
7	ЗИС.25	Контроль передачи видеоинформации		Выполняется за счет наличия возможности защищенной передачи видеосигнала с камер без ощутимого снижения качества изображения.	
8	ЗИС.31	Защита от скрытых каналов передачи информации		Выполняется за счет архитектуры комплекса.	

Итак, путем применения «fin-TrusT» в рамках обеспечения безопасности значимых объектов критической информационной инфраструктуры выполняются следующие меры, включенные в базовый набор мер обеспечения безопасности значимого объекта для соответствующей категории значимости:
ИАФ: 1, 2, 3, 4, 5, 7;
УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, 14;
ОПС: 1;
АУД: 2, 3, 4, 5, 6, 7, 8, 9;
АВЗ: 1;
ОЦЛ: 1, 3, 4, 5;
ОДТ: 1, 3, 4, 5, 6;
ЗТС: 3;
ЗИС: 1, 2, 6, 13, 16, 19, 20, 21, 27, 32, 33, 34, 35, 38;

ИНЦ: 1, 2;
ОПО: 2, 4;
ДНС: 4, 5;
а также дополнительные (не включенные в базовый набор) меры:
ОЦЛ: 2;
ОДТ: 7;
ЗТС: 1;
ЗИС: 10, 12, 17, 25, 31.

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