ВЫПОЛНЕНИЕ МЕР 239-ГО ПРИКАЗА ФСТЭК ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПУТЕМ ПРИМЕНЕНИЯ СПЕЦИАЛИЗИРОВАННЫХ МИКРОКОМПЬЮТЕРОВ «M-TRUST»

ОКБ САПР

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 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 № 239, 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 239-ым приказом ФСТЭК России по обеспечению безопасности значимых объектов критической информационной инфраструктуры, путем применения специализированных микрокомпьютеров «m-TrusT»

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

Таблица 1. Соответствие m-TrusT техническим мерам Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239

Обозн. и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие m-TrusT требованиям ФСТЭК	Примечание
I. Идентификация и аутентификация (ИАФ)			Меры ИАФ.0. ИАФ.3, ИАФ.4 являются организационными. Мера ИАФ.6 – необязательная.
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	
ИАФ.2	Идентификация и аутентификация устройств	+	
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	
ИАФ.7	Защита аутентификационной информации при передаче	+	
II. Управление доступом (УПД)			Меры УПД.0, УПД.4, УПД.5 являются организационными. Меры УПД.7, УПД.8, УПД.12 – необязательные.
УПД.1	Управление учетными записями пользователей	*	Не имеет пользователей т. к. обычно работает в автоматическом режиме
УПД.2	Реализация модели управления доступом	*	Управление доступом осуществляется ключевой системой
УПД.3	Доверенная загрузка	+	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	
УПД.9	Ограничение числа параллельных сеансов доступа	*	Ограничивается ключевой системой
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	
УПД.13	Реализация защищенного удаленного доступа	+	Защита удаленного доступа обеспечивается СКЗИ
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	
III. Ограничение программной среды (ОПС)			Меры ОПС.0 и ОПС.2 являются организационными. Мера ОПС.3 – необязательная.
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+	

IV. Защита машинных носителей информации (ЗНИ)			Меры ЗНИ.0 - ЗНИ.2 являются организационными. Меры ЗНИ.3 и ЗНИ.4 – необязательные.
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. В системе обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.7	Контроль подключения съемных машинных носителей информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	-	
V. Аудит безопасности (АУД)			Меры АУД.0 – АУД.2, АУД.10 и АУД.11 являются организационными.
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	Обеспечивается собственной системой времени
АУД.4	Регистрация событий безопасности	+	
АУД.5	Контроль и анализ сетевого трафика	-	
АУД.6	Защита информации о событиях безопасности	+	
АУД.7	Мониторинг безопасности	+	
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	
АУД.9	Анализ действий отдельных пользователей	-	
VI. Антивирусная защита (АВЗ)			Меры АВЗ.0 и АВЗ.5 являются организационными.
АВЗ.1	Реализация антивирусной защиты	+	
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	-	Электронная почта и внешние сервисы не используются
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	-	
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	-	Не требуется

VII. Предотвращение вторжений (компьютерных атак) (СОВ)			Мера СОВ.0 является организационной.
СОВ.1	Обнаружение и предотвращение компьютерных атак	**	Обеспечивается внешними средствами СОВ
СОВ.2	Обновление базы решающих правил	**	Обеспечивается внешними средствами СОВ
VIII. Обеспечение целостности (ОЦЛ)			Мера ОЦЛ.0 является организационной. Меры ОЦЛ.2 и ЗНИ.6 – необязательные.
ОЦЛ.1	Контроль целостности программного обеспечения	+	
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	+	
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+	
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+	
IX. Обеспечение доступности (ОДТ)			Меры ОТД.0 – ОТД.2 являются организационными. Мера ОТД.7 – необязательная.
ОДТ.4	Резервное копирование информации	**	В соответствии с политикой информационной безопасности
ОДТ.5	Обеспечение возможности восстановления информации	**	В соответствии с политикой информационной безопасности
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	Обеспечивается архитектурой
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	-	
X. Защита технических средств и систем (ЗТС)			Меры ЗТС.0, ЗТС.2 – ЗТС.5 являются организационными. Меры ЗТС.1 и ЗТС.6 – необязательные.
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			Меры ЗИС.0 – ЗИС.5, ЗИС.8 являются организационными. Меры ЗИС.7, ЗИС.9 – ЗИС.12, ЗИС14, ЗИС.15, ЗИС.17, ЗИС.18, ЗИС.22 – ЗИС.26, ЗИС.28 – ЗИС.31, ЗИС.36, ЗИС.37 – необязательные.
ЗИС.6	Управление сетевыми потоками	+	Обеспечивается ключевой системой
ЗИС.13	Защита неизменяемых данных	+	
ЗИС.16	Защита от спама	+	

ЗИС.19	Защита информации при ее передаче по каналам связи	+	
ЗИС.20	Обеспечение доверенных канала, маршрута	+	
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	
ЗИС.27	Обеспечение подлинности сетевых соединений	+	
ЗИС.32	Защита беспроводных соединений	+	
ЗИС.33	Исключение доступа через общие ресурсы	+	
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	
ЗИС.35	Управление сетевыми соединениями	+	
ЗИС.38	Защита информации при использовании мобильных устройств	+	
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	-	
XII. Реагирование на компьютерные инциденты (ИНЦ)			Все меры этой группы – организационные.
XIII. Управление конфигурацией (УКФ)			Все меры этой группы – организационные.
XIV. Управление обновлениями программного обеспечения (ОПО)			Меры ОПО.0, ОПО.1 и ОПО.3 являются организационными.
ОПО.2	Контроль целостности обновлений программного обеспечения	+	
ОПО.4	Установка обновлений программного обеспечения	+	
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)			Все меры этой группы – организационные.
XVI. Обеспечение действий в нештатных ситуациях (ДНС)			Все меры этой группы – организационные.
XVII. Информирование и обучение персонала (ИПО)			Все меры этой группы – организационные.

* - при использовании в ИС без СКЗИ мера осуществляется установкой СПО СЗИ

** - при использовании в ИС при установке СПО СЗИ

Таблица 2. Применение m-TrusT для защиты значимых объектов КИИ

Обозн. и номер меры	Меры обеспечения безопасности
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.27	Обеспечение подлинности сетевых соединений

ЗИС.32	Защита беспроводных соединений
ЗИС.33	Исключение доступа через общие ресурсы
ЗИС.35	Управление сетевыми соединениями