Международный ТБ ФОРУМ Технологии и Безопасность

ЦБИ Центр безопасности информации

Состояние работ по реализации требований, предъявляемых к аппаратной платформе и производительности многофункциональных межсетевых экранов уровня сети

ТБ ФОРУМ 2024. 14 февраля 2024 года
Актуальные вопросы защиты информации. XIV Конференция

Сидак Алексей Александрович
Генеральный директор
sidak@cbi-info.ru

ООО «Центр безопасности информации» (ООО «ЦБИ»)

г. Королёв, Московская область

Эволюция требований к межсетевым экранам

2023 г.

НПА. Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

Утв. Приказом ФСТЭК России от 7 марта 2023 г. №44

2016 г.

НПА. Требования к межсетевым экранам

Тип А | Тип Б | Тип В | Тип Г | Тип Д

МД. Профили защиты

1997 г.

РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации

Конструкционные принципы построения нового типа МЭ

Композиционность: реализация функционала сразу нескольких типов средств защиты информации

МЭ | СОВ | САВЗ | «Песочница» | СДЗ

→ ***UTM-решение***

Платформенность: доверенная аппаратная платформа; реализация части функций безопасности

→ ***NGFW-решение***

Эксплуатационная технологичность: обеспечение потребности в производительности и отказоустойчивости

→ ***Востребованное решение российскими операторами***

Требования к аппаратной платформе МЭ

НПА. Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети **(пункт 15)**

Ограничение доступа к оперативной памяти

Пакетная фильтрация

Защита контура управления

Пункт 15 вступает в силу с 1 января 2025 года

Приказ ФСТЭК России от 7 марта 2023 г. № 44

Информационное сообщение ФСТЭК России

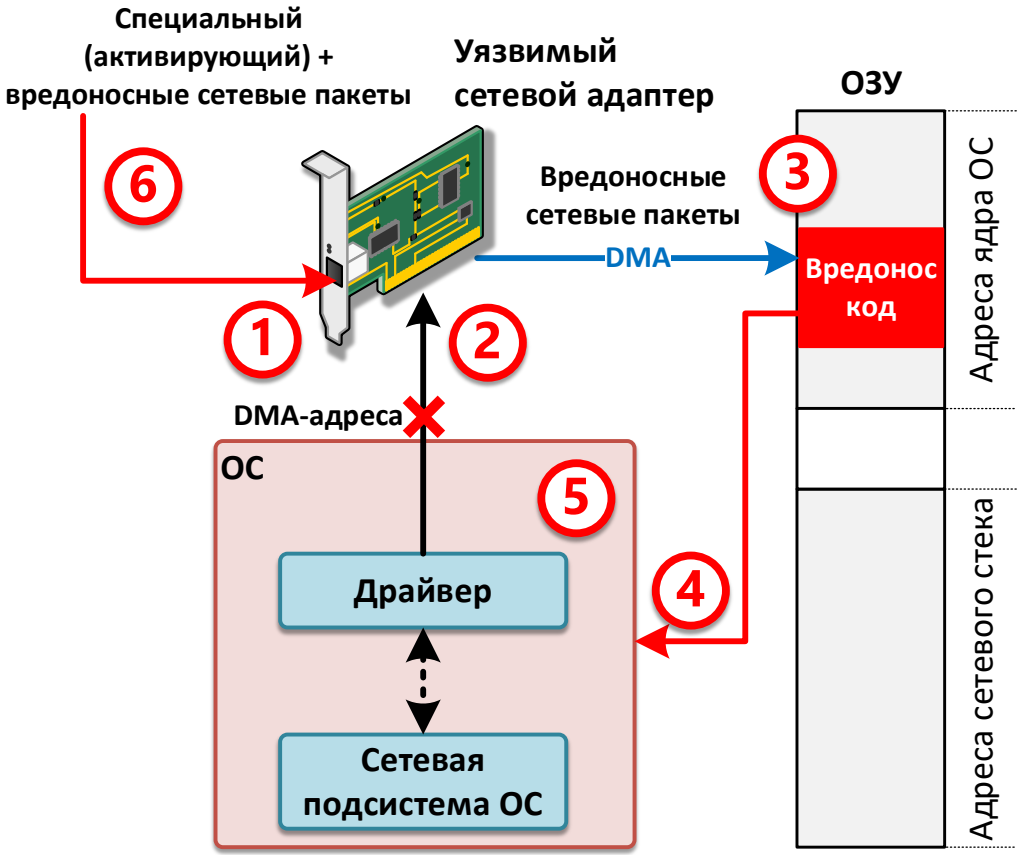
Требования к аппаратной платформе

Показатель	Критерии	Потребность в реализации
Ограничение доступа к оперативной памяти (ОП)	доступ возможен только в разрешенном диапазоне адресов ОП	
	доступ исключен к остальной (неразрешённой) части ОП	?!
Пакетная фильтрация	на основе сетевых адресов отправителей/получателей (IP-адресов)	
	на основе физических адресов отправителей/получателей (MAC-адресов)	

Реализация требований к аппаратной платформе. Доверенный сетевой адаптер

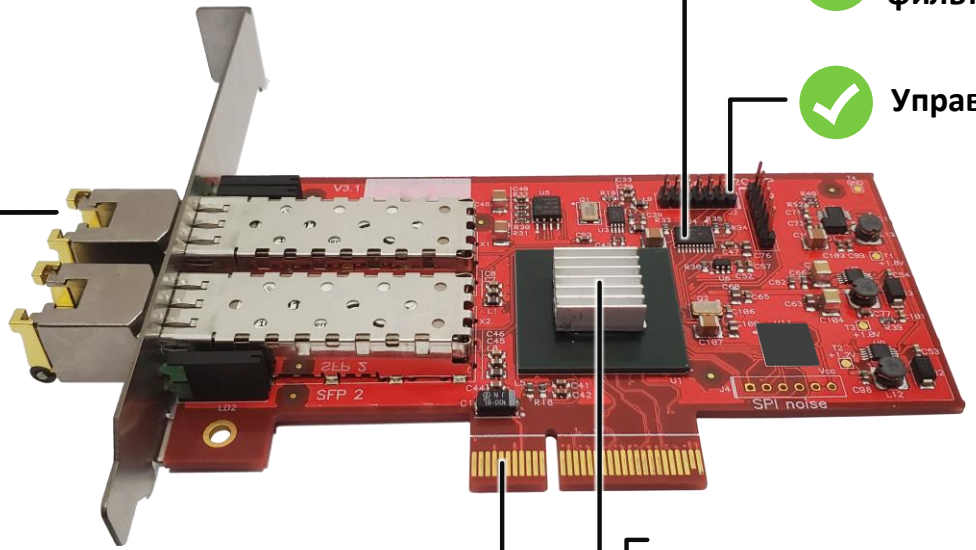
Показатель	Критерии	Реализация
Ограничение доступа к оперативной памяти (ОП)	доступ возможен только в разрешенном диапазоне адресов ОП	Доверенный сетевой адаптер
	доступ исключен к остальной (неразрешённой) части ОП	
Пакетная фильтрация	на основе сетевых адресов отправителей/получателей (IP-адресов)	
	на основе физических адресов отправителей/получателей (MAC-адресов)	

Результаты экспериментов с недоверенным сетевым адаптером



1. Прием активирующего и вредоносных пакетов
2. Игнорирование DMA-адресов от драйвера
3. Запись вредоносного кода в область ОЗУ ядра ОС
4. Выполнение вредоносного кода
5. Нарушение безопасности функционирования ОС
6. Возможность получения нарушителем полного доступа к данным и функциям

Доверенный сетевой адаптер «TrustNet»



- ✗ Управление
- ✗ Изменение встроенного ПО
- ✓ Фильтрация сетевых пакетов

- ✓ Хранение правил фильтрации
- ✓ Управление

- ✓ Контроль целостности встроенного ПО
- ✓ Контроль обращений к ОЗУ

- ✗ Управление
- ✗ Изменение встроенного ПО

Состояние работ по доверенному сетевому адаптеру

Доверенный сетевой **адаптер** «TRUST NET» **разработан**

Модуль уровня ядра «**Драйвер** доверенного сетевого адаптера «TRUST NET» для ОС Linux» прошел проверку и **включен в состав** сертифицированной операционной системы **«Astra Linux Special Edition»**

Подана **заявка на сертификацию** Доверенного сетевого адаптера «TRUST NET» в системе сертификации ФСТЭК России

Ведется разработка образцов с большей производительностью

Требования к аппаратной платформе

Показатель	Критерии	Потребность в реализации
Защита контура управления	недоступность интерфейса функций управления со стороны пользователей, осуществляющих передачу информационных потоков через МЭ	?!
	недоступность пользователям, осуществляющим передачу информационных потоков через МЭ, сетевого трафика, поступающего в МЭ от пользователей, осуществляющих управление МЭ	

Реализация требований к аппаратной платформе. Элементы обеспечения физической однонаправленности

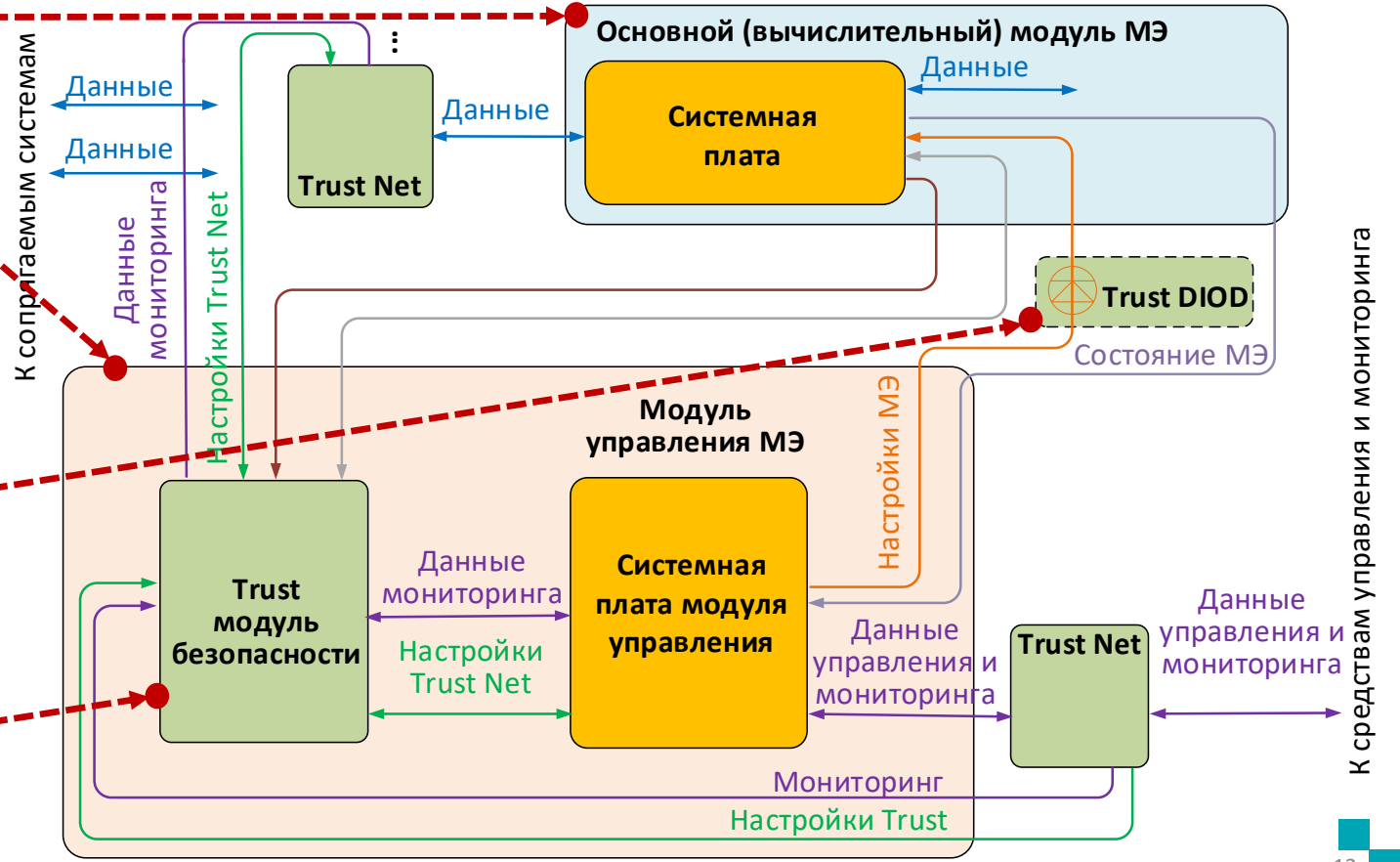
Показатель	Критерии	Реализация
Защита контура управления	недоступность интерфейса функций управления со стороны пользователей, осуществляющих передачу информационных потоков через МЭ	Элементы защиты контура управления
	недоступность пользователям, осуществляющим передачу информационных потоков через МЭ, сетевого трафика, поступающего в МЭ от пользователей, осуществляющих управление МЭ	

Реализация требований к аппаратной платформе. Элементы защиты контура управления

аппаратное **разделение** модуля управления и вычислительного модуля

применение средств **однонаправленной** передачи правил в вычислительный модуль

контроль модуля управления и вычислительного модуля



Подтверждение сведений о производительности межсетевого экрана

Состояние работ по разработке Методики тестирования производительности многофункциональных МЭ уровня сети

Создана рабочая группа

Разработан проект Методики

Получены замечания / предложения от участников рабочей группы

Ведется обработка замечаний / предложений, уточнение проекта Методики

Состояние работ по реализации требований, предъявляемых к аппаратной платформе и производительности многофункциональных межсетевых экранов уровня сети

ТБ ФОРУМ 2024. 14 февраля 2024 года

ООО «Центр безопасности информации» (ООО «ЦБИ»)

г. Королев, Московская область, ул. Ленинская, д. 11

: 8 (495) 580-52-18

: info@cbi-info.ru

ЦБИ Центр безопасности информации