ЦБИ Центр безопасности информации

Практические подходы к реализации актуальных требований по защите данных в автоматизированных системах

Конференция РусКрипто’2025
19 марта 2025 года

Сидак Алексей Александрович, генеральный директор
Лузин Виктор Петрович, директор департамента
Василенко Владимир Васильевич, зам. генерального директора
Сидак Дарья Алексеевна, инженер
mail@cbi-info.ru

ООО «Центр безопасности информации» (ООО «ЦБИ»)
г. Королёв, Московская область

Уровни требований по защите информации

1 Информационная инфраструктура

Нормативные правовые акты	Национальные стандарты	Методические документы

2 Автоматизированные системы

Нормативные правовые акты	Национальные стандарты	Методические документы

3 Средства ЗИ и средства ОБИТ

Нормативные правовые акты	Национальные стандарты	Методические документы

Основные источники требований безопасности информации в ИАС

Нормативные правовые акты

Требования о ЗИ, не составляющей ГТ, содержащейся в ГИС

…

Методические документы

Меры защиты информации в ГИС

Организация управления уязвимостями

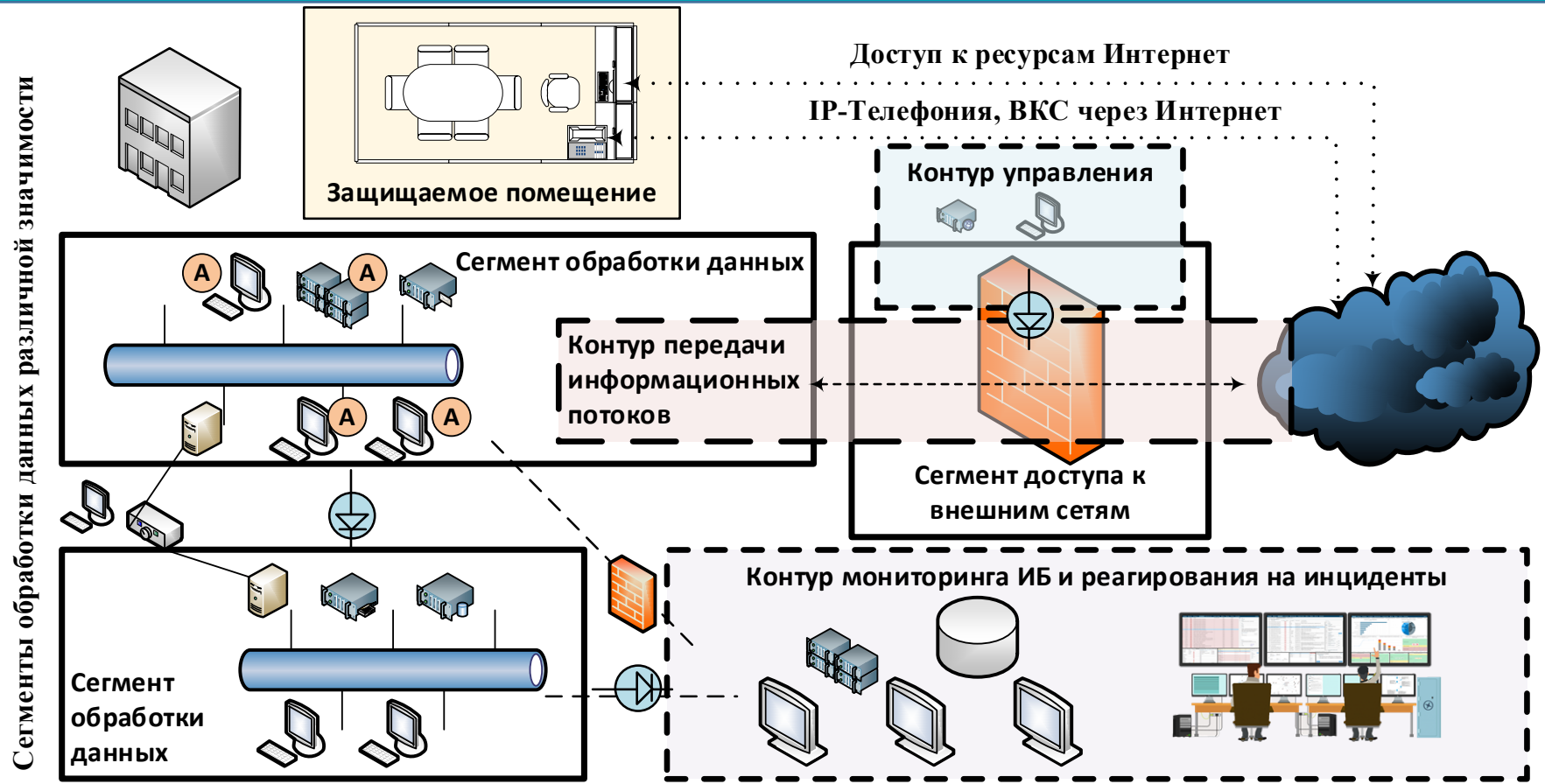
Тестирование обновлений

Национальные стандарты

ГОСТ Р 51583-2014 ЗИ. Порядок создания АСЗИ. Общие положения

ГОСТ Р 51624-2014 ЗИ. Порядок создания АСЗИ. Общие требования

Структуризация информационных автоматизированных систем



Требования к средствам ЗИ и средствам обеспечения БИТ

Нормативные правовые акты

САВЗ | СОВ | СДЗ | СКСНИ | ОС | СрЗ от ОвО | МЭ | МФМЭ

СУБД | Вирт. | Контейн. | СОР | Требования к уровням доверия

Методические документы

Профили защиты | Тестирование производительности МФМЭ

Национальные стандарты

Классификация, представление уязвимостей | Безопасная разработка | Регистрация событий безопасности | Функции Безопасности

Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла (EDR)

Уровни доверия

Управление доступом в средстве

Тестирование средства

Идентификация и аутентификация пользователей (администраторов) средства

Централизованное управление средством

Получение (сбор) данных мониторинга

Обнаружение признаков вредоносного ПО

Обнаружение признаков компьютерных атак

Реагирование

Обновление служебных баз данных

Регистрация событий безопасности

Взаимодействие с иными средствами ЗИ

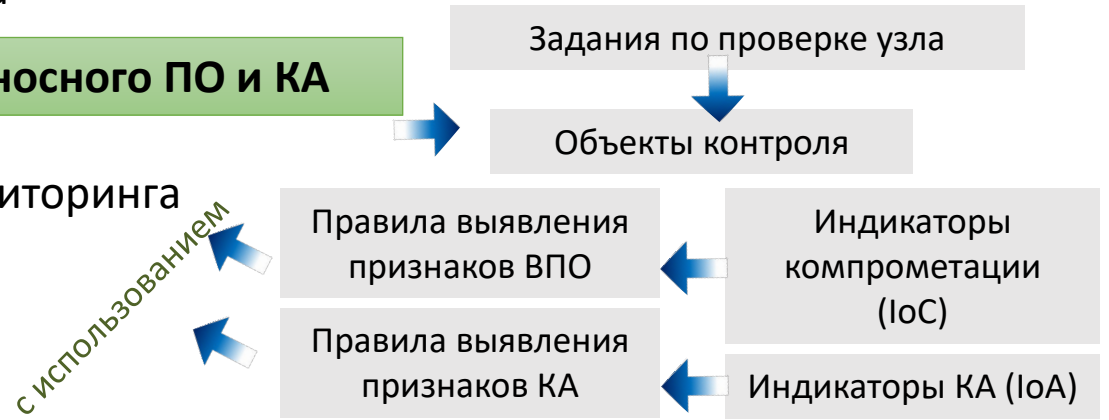
Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла (EDR)

1. Получение (сбор) данных мониторинга (~20 позиций)

- ✓ инвентаризационная информация узла
- ✓ сведения об операциях на узле
- ✓ сведения о вх./исх. трафике узла

2. Обнаружение признаков вредоносного ПО и КА

- ✓ анализ полученных данных мониторинга



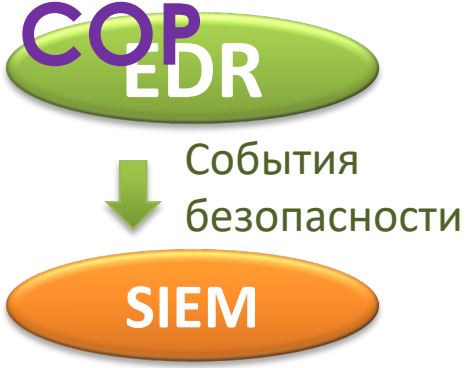
3. Реагирование (~20 позиций)

- ✓ уведомление
- ✓ блокирование
- ✓ завершение процессов
- ✓ отключение
- ✓ получение информации для доп. анализа

Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла (EDR)

6, 5, 4 класс защиты

Обеспечение **возможности передачи** зарегистрированных **событий безопасности в** сертифицированную **SIEM**

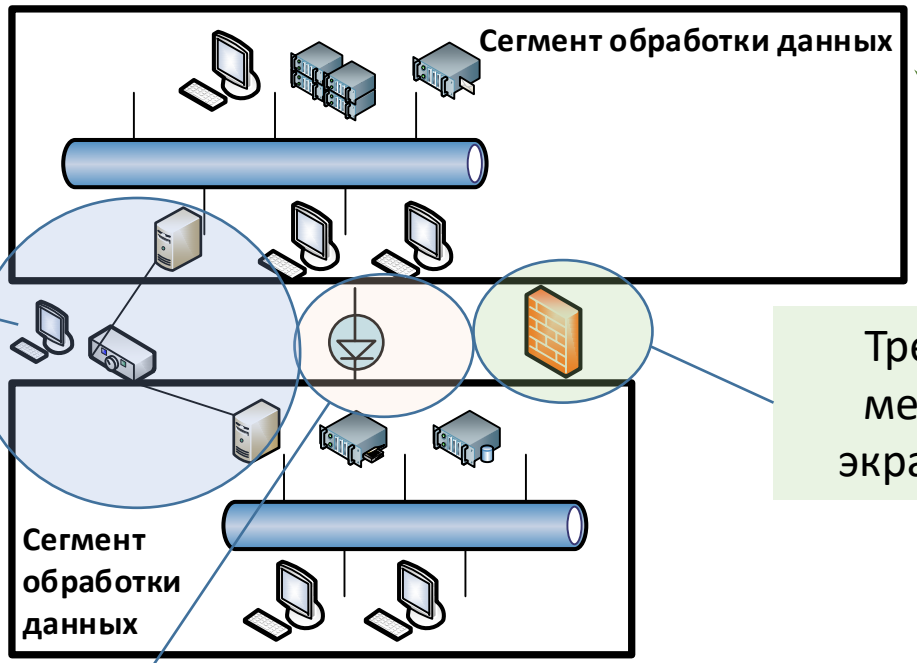


5, 4 класс защиты

Обеспечение взаимодействия с сертифицированной замкнутой системой (средой) предварительного выполнения программ («песочницей»)

Требования к защите при взаимодействии сегментов обработки данных разной значимости

Требования к защите от утечки данных по ТК при работе АРМ в разнокатегорийных сегментах



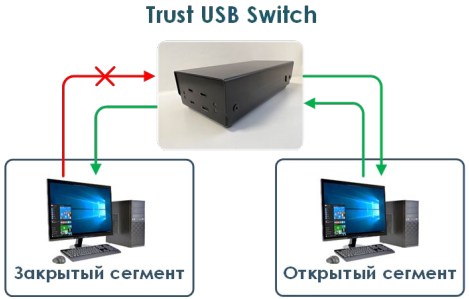
Требования к межсетевому экранированию

Требования к однонаправленной передаче

Реализация требований по однонаправленной передаче

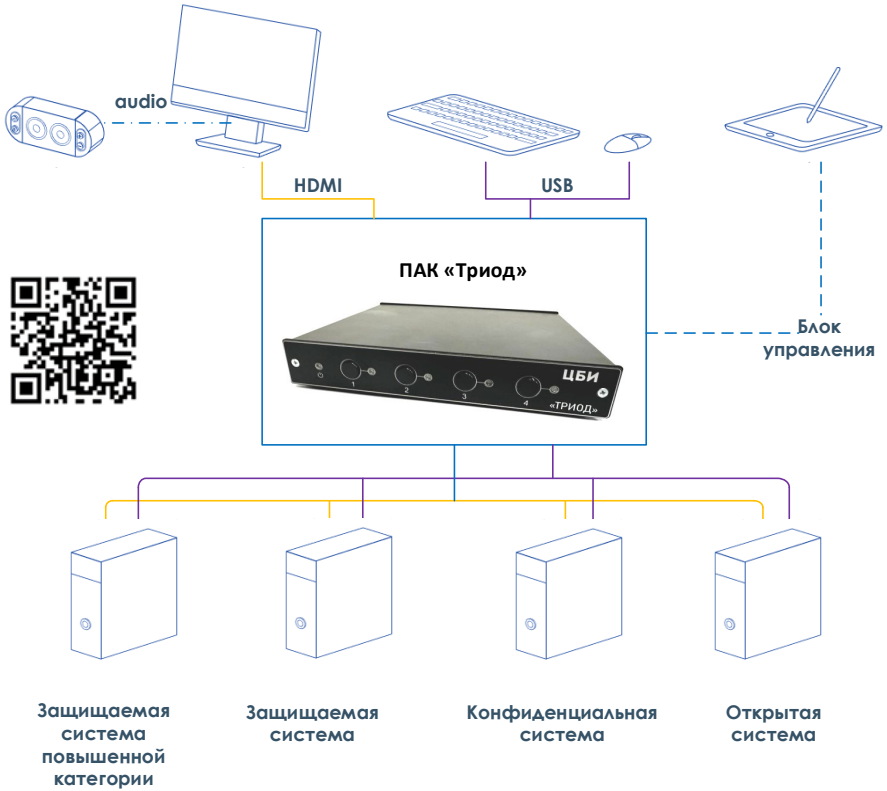
Защита от утечки информации между контурами обработки информации

Средство однонаправленной передачи информации (ДИОД-2С)



Переключатель машинного носителя для разных контуров

Реализация требований по защите данных при работе на АРМ в разнокатегорийных сегментах



Область применения:

- разнокатегорийные системы на одном рабочем месте
- выделенные и защищаемые помещения

Ключевые особенности:

- работа в **различных** автоматизированных системах
- удаленное подключение к СВТ (**до 300 метров**)
- **единые** средства отображения и звуковоспроизведения
- удобное современное устройство управления переключениями системных блоков
- **отсутствие** сигналов **ПЭМИН**

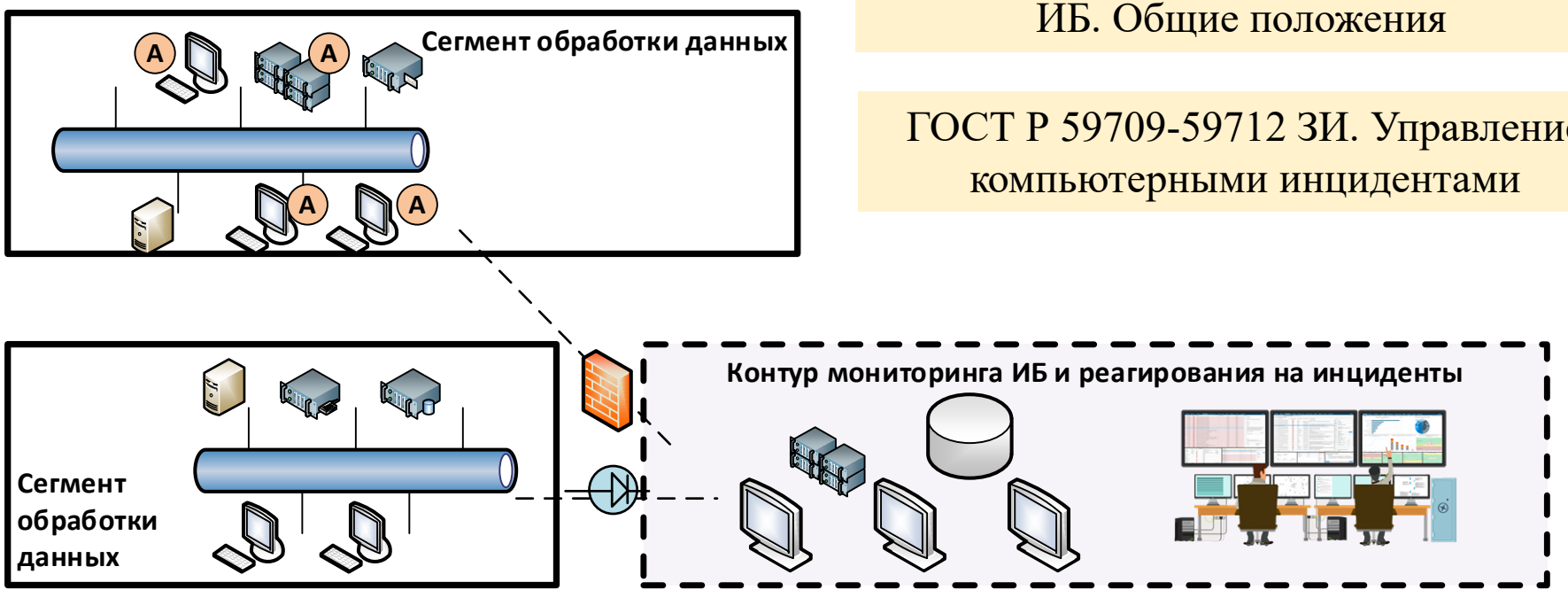
Контур мониторинга ИБ и реагирования на компьютерные инциденты

Требования о ЗИ, не составляющей ГТ, содержащейся в ГИС

Меры защиты информации в ГИС

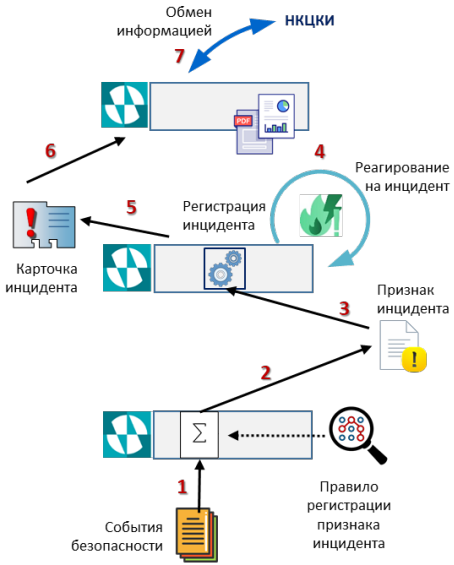
ГОСТ Р 59547-2021 ЗИ. Мониторинг ИБ. Общие положения

ГОСТ Р 59709-59712 ЗИ. Управление компьютерными инцидентами



Реализация требований к мониторингу ИБ и управлению инцидентами

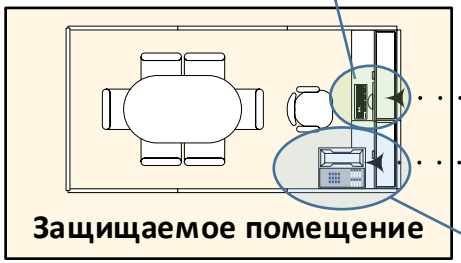
Средство взаимодействия с НКЦКИ (IS-система)	NeuroDAT SIEM IS
Центр управления инцидентами (IM-система)	NeuroDAT SIEM IM
Система мониторинга ИБ (SIEM-система)	NeuroDAT SIEM
Источники данных мониторинга	Агент NeuroDAT Коннекторы NeuroDAT
Инфраструктурные элементы	ДИОД СПЛИТ-22 ДИОД-2С



Доступ во внешние сети из защищаемых помещений

АРМ Интернет (ноутбук, моноблок, TV, системный блок)

АРМ Интернет ВКС



Доступ к ресурсам Интернет

IP-Телефония, ВКС через Интернет

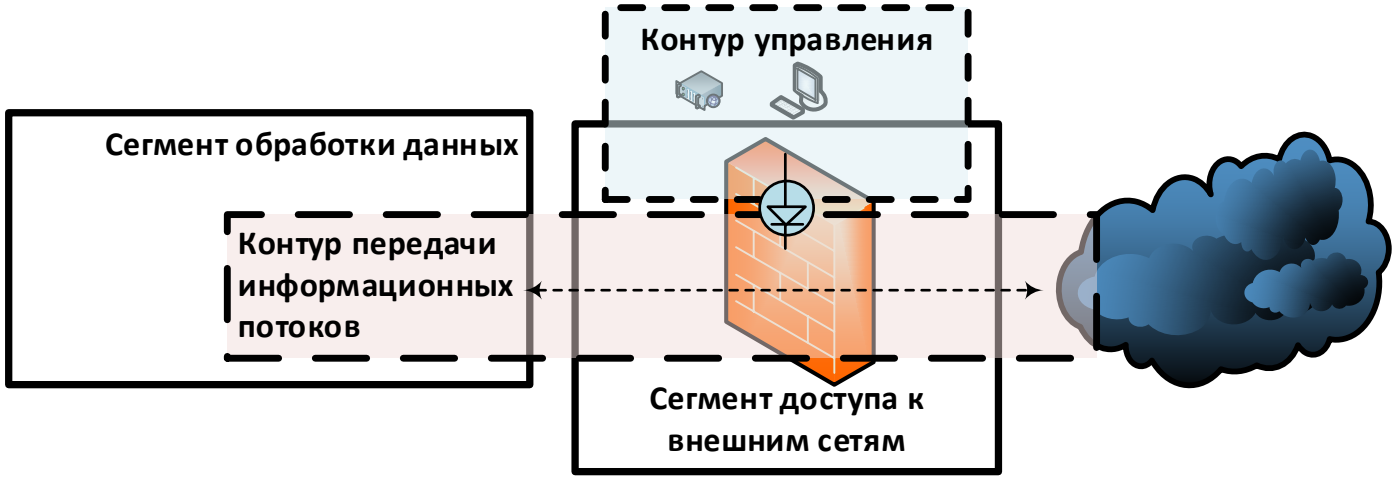
Защищенный IP-телефон (видеофон) «ТА Дозвон»

Требования к сегменту доступа к внешним сетям

Требования о ЗИ, не составляющей ГТ, содержащейся в ГИС

Меры защиты информации в ГИС

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети (утв. Приказом ФСТЭК России от 7 марта 2023 г. №44)



Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

Уровни доверия

Доверенная загрузка

Идентификация и аутентификация

Управление доступом в МЭ

Централизованное и удаленное управление

Фильтрация сетевого трафика

Обнаружение и блокирование КА

Обнаружение и блокирование ВПО

Режимы работы

Аппаратная платформа

Производительность

Обеспечение бесперебойного функционирования и восстановления

Тестирование и контроль целостности МЭ

Регистрация событий безопасности

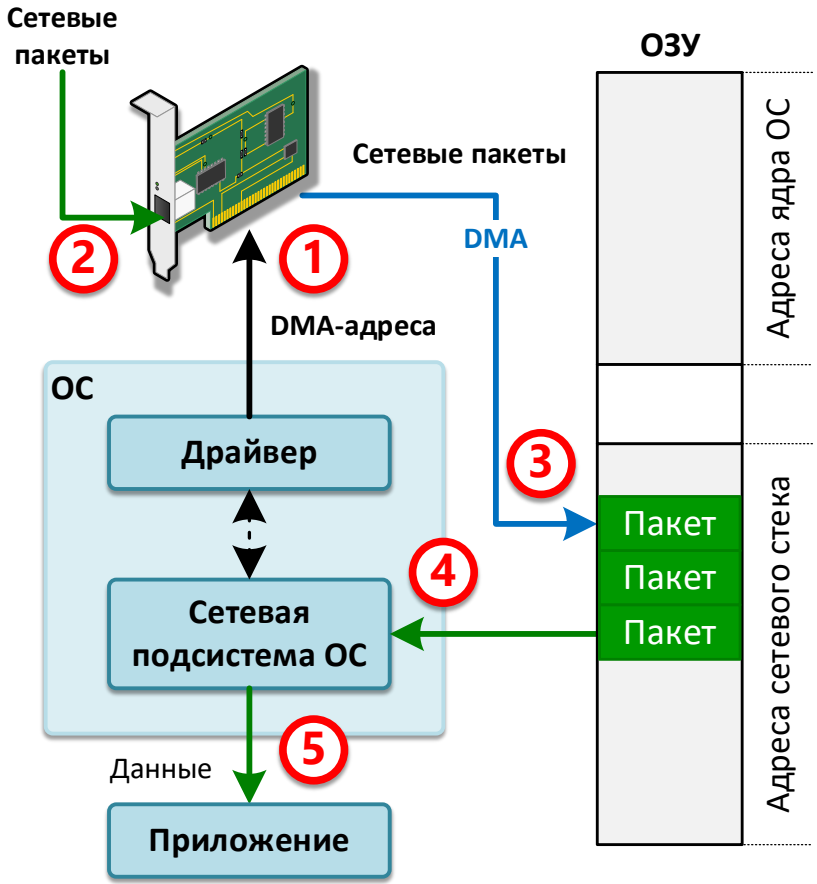
Взаимодействие с иными средствами ЗИ

Требования к аппаратной платформе МФМЭ уровня сети (п. 15 НПА)

Пункт **15** НПА **вступил в силу** с 1 января 2025 года

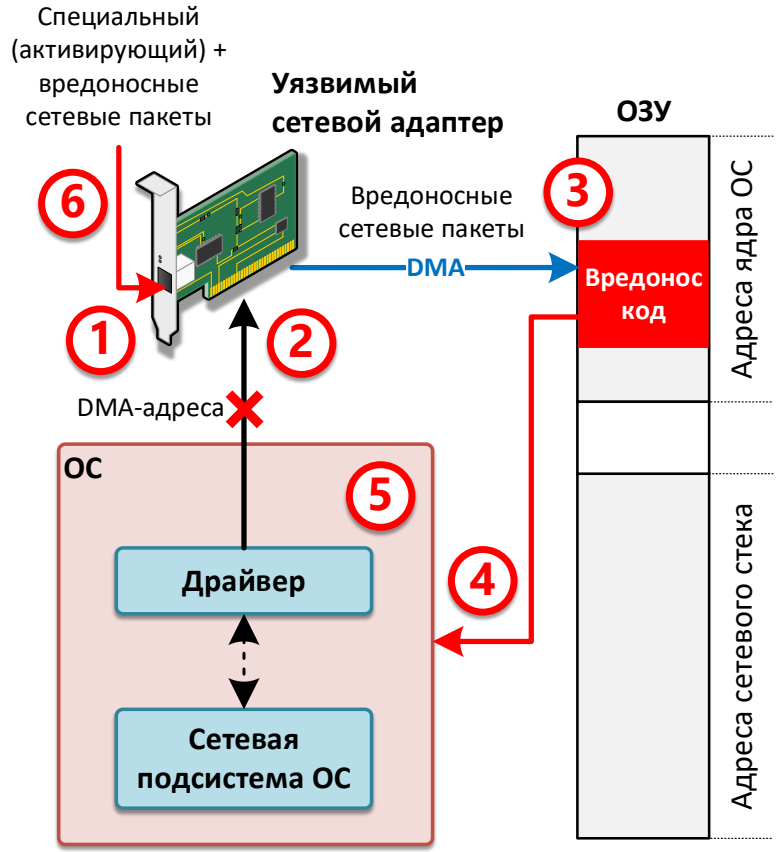
Ограничение доступа к оперативной памяти	15.1. **Аппаратная платформа** МЭ должна **ограничивать доступ через сетевые интерфейсы к оперативной памяти** только в разрешенном диапазоне адресов и **исключать возможность доступа** (как на чтение, так и на запись) **к остальной части оперативной памяти** аппаратной платформы **со стороны сетевого интерфейса**.
Пакетная фильтрация	15.2, 15.3 Аппаратная платформа должна содержать **компоненты, на аппаратном уровне реализующие пакетную фильтрацию** на основе сетевых адресов и физических адресов отправителей и получателей сетевого трафика
Защита контура управления	15.1 … должно быть доказано, что **субъектам …, осуществляющим передачу информационных потоков** через МЭ, **не может быть доступен интерфейс функций управления** МЭ **и сетевой трафик [управления]**

Типовая схема приема сетевых пакетов



1. Инициализация адресов ОЗУ для приема пакетов
2. Прием сетевого пакета сетевым адаптером
3. Запись сетевого пакета в ОЗУ по DMA-каналу
4. Чтение пакета из ОЗУ для обработки
5. Передача данных сетевого пакета приложению

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

Атака на программно-аппаратный межсетевой экран
Этап 1. Добавление разрешающего правила

Атака на программно-аппаратный межсетевой экран
Этап 2. Получение доступа к защищаемым данным

Подтвержденные результаты реализации угроз безопасности информации

- ✓ ***получение привилегированного доступа (выполнение шелл-кода)***
- ✓ ***компрометация учетных записей***
- ✓ ***изменение правил сетевой фильтрации межсетевого экрана***
- ✓ ***получение доступа к данным***

Реализация требований к аппаратной платформе. Доверенный сетевой адаптер

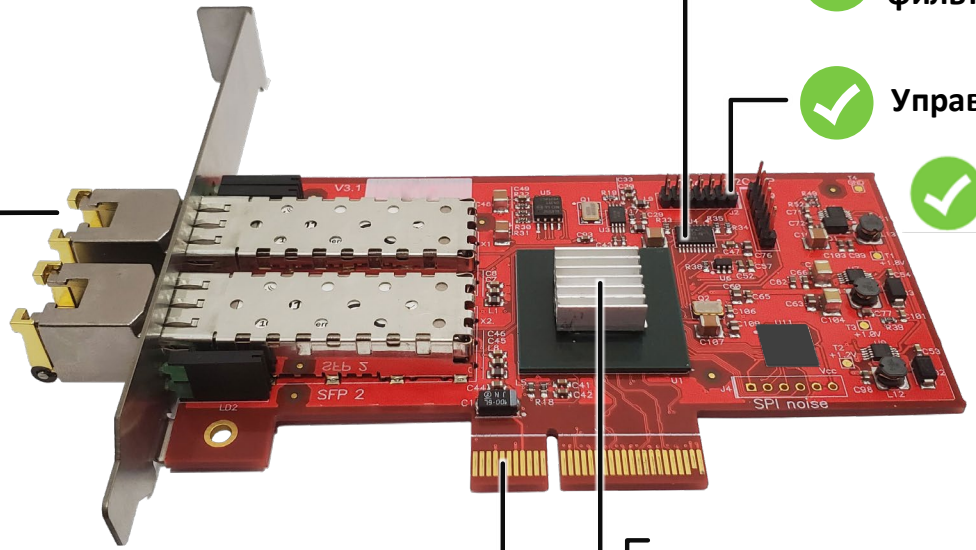
Показатель	Критерии	Реализация
Ограничение доступа к оперативной памяти (ОП)	доступ возможен только в разрешенном диапазоне адресов ОП	Доверенный сетевой адаптер
	доступ исключен к остальной (неразрешённой) части ОП	
Пакетная фильтрация	на основе сетевых адресов отправителей/получателей (IP-адресов)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

Доверенный сетевой адаптер «TRUST NET»

ЦБИ Центр безопасности информации

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

- ✓ Регистрация событий аппаратной фильтрации



- ✓ Хранение правил фильтрации
- ✓ Управление
- ✓ Изменение правил фильтрации сетевых пакетов без прерывания работы сетевого адаптера

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

- ✗ Управление
- ✗ Изменение встроенного ПО

Современные практики обеспечения высокой производительности

- *Сегментация сетевых пакетов (GSO, TSO, USO)*
- *Проверка контрольных сумм входящих пакетов (RX checksum offload)*
- *Вычисление контрольных сумм исходящих пакетов (TX checksum offload)*
- *Распределение обработки входящего трафика между несколькими ядрами ЦП (RSS)*
- *Обработка тегов VLAN (добавление и удаление) VLAN Offload*
- *Ускорение обработки сетевого трафика и повышение производительности сетевых приложений (DPDK, XDP)*

Состояние работ по доверенному сетевому адаптеру

Сертификация доверенного сетевого адаптера «TRUST NET» в системе сертификации ФСТЭК России **на заключительной стадии (документы на рассмотрении в ФСТЭК России)**

Образцы с различной производительностью

- с 2-мя сетевыми интерфейсами по 1 Гбит/с (разработан)
- с 2-мя сетевыми интерфейсами по 10 Гбит/с (разработан)
- с 2-мя сетевыми интерфейсами по 25 Гбит/с (в разработке)
- 100 Гбит/с (в разработке)

Образцы **взяты на тестирование** разработчиками МФМЭ уровня сети

infotecs КОД безопасности • • •

Образцы **включены разработчиками МФМЭ** уровня сети **в состав** своих **изделий**

ЦБИ Центр безопасности информации

Практические подходы к реализации актуальных требований по защите данных в автоматизированных системах

Конференция РусКрипто’2026. 19 марта 2025 года

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

г. Королев, Московской области
Ул. Ленинская, д. 11

: 8 (495) 580-52-18

: mail@cbi-info.ru