Вопросы реализации требований к средствам сетевой защиты информации

ТБ ФОРУМ 2025. 12 февраля 2025 года
Актуальные вопросы защиты информации. XV Конференция

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

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

г. Королёв, Московская область

Средства сетевой защиты информации

Средства уровня сети

Средства уровня узлов

Противодействие

- **внедрению вредоносного ПО через сеть**
- **компьютерным атакам**
- **НСД к информации через сетевое взаимодействие**

Функционирование

- **работа на всех уровнях взаимодействия**
- **защищенность от возможности обхода, отключения и преодоления**
- **минимальное влияние на пропускную способность и производительность**
- **исключение возможности создания скрытых каналов в сети**

НПА

Методические документы

- **системы обнаружения вторжений**
- **межсетевые экраны**
- **средства защиты от DDoS**

Новые требования к средствам сетевой защиты информации

2023 г.

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

Типовая методика тестирования производительности и обеспечения бесперебойного функционирования многофункционального межсетевого экрана уровня сети

2025 г.

Требования по безопасности информации к средствам обнаружения и реагирования уровня узла

ГОСТ Р Защита информации. Информационный ресурс служебных баз данных. Общие положения

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

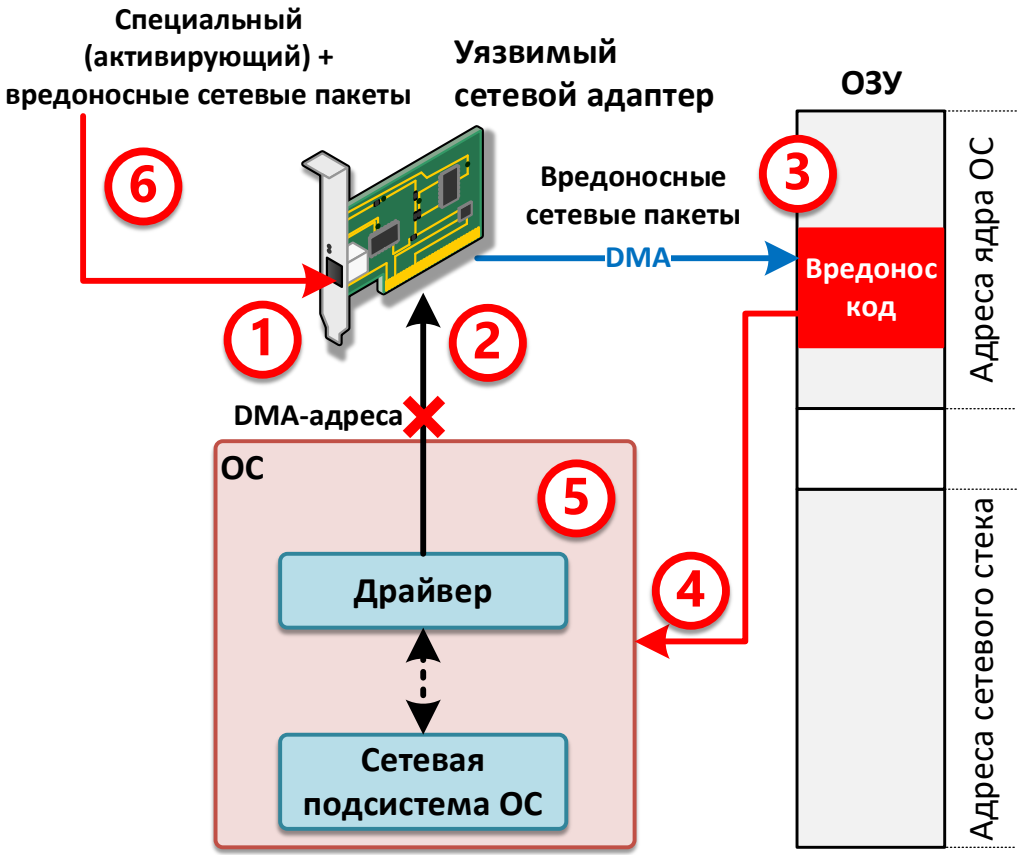
Обеспечение бесперебойного функционирования и восстановления

Тестирование и контроль целостности МЭ

Регистрация событий безопасности

Взаимодействие с иными средствами ЗИ

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

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]**

Реализация требований к аппаратной платформе. Доверенный сетевой адаптер

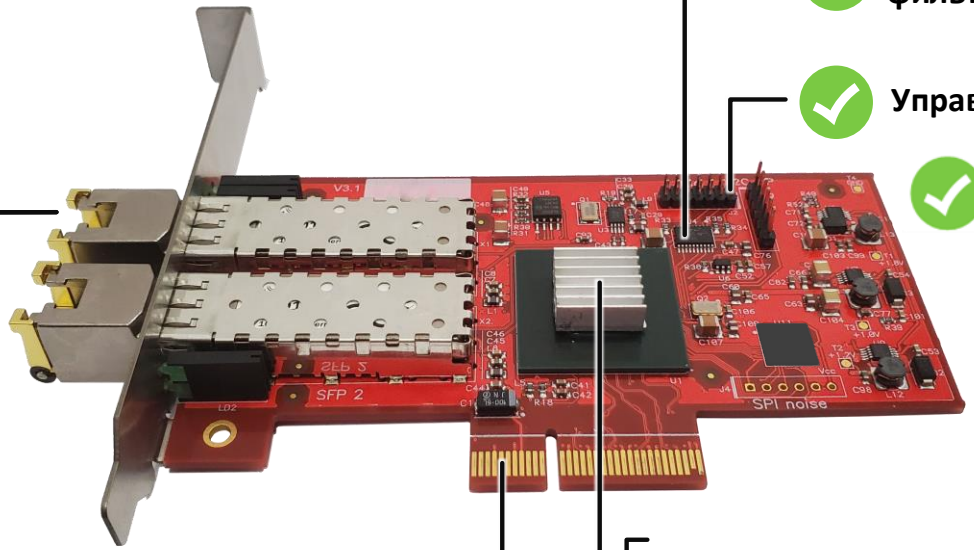
Показатель	Критерии	Реализация
Ограничение доступа к оперативной памяти (ОП)	доступ возможен только в разрешенном диапазоне адресов ОП	Доверенный сетевой адаптер
	доступ исключен к остальной (неразрешённой) части ОП	
Пакетная фильтрация	на основе сетевых адресов отправителей/получателей (IP-адресов)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

Доверенный сетевой адаптер «TrustNet»

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

Состояние работ по доверенному сетевому адаптеру

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

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**

Реализация требований к аппаратной платформе. Защита контура управления

Показатель	Критерии	Реализация
Защита контура управления	**недоступность интерфейса функций управления** со стороны пользователей (субъектов), осуществляющих передачу информационных потоков через МЭ	Решение и **элементы** защиты контура управления
	недоступность пользователям (субъектам), осуществляющим передачу информационных потоков через МЭ, **сетевого трафика управления МЭ**	

Интерфейс ФБ

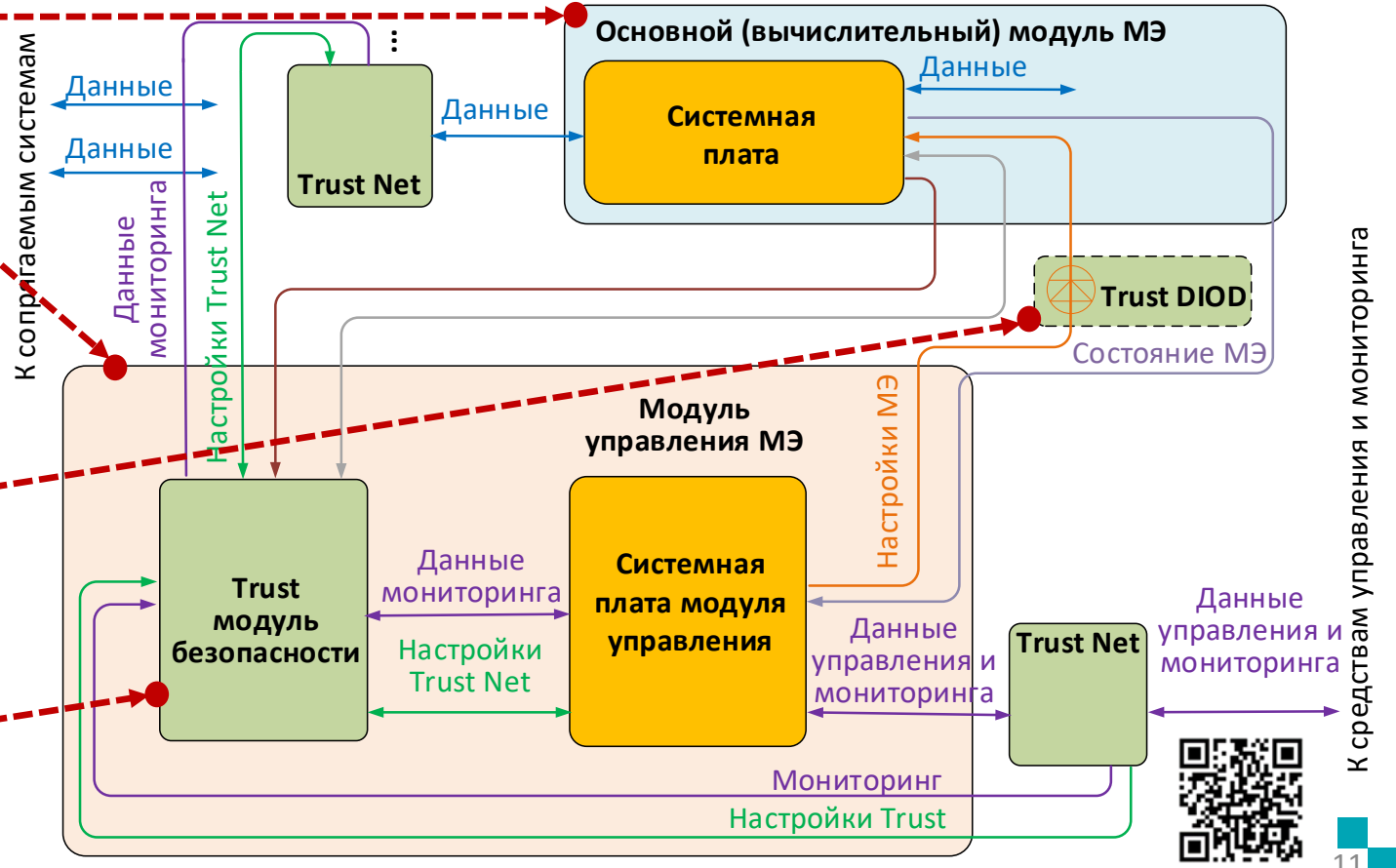
Однонаправленные средства

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 целостности встроенного ПО средствами **модуля безопасности**



Требования к производительности и бесперебойному функционированию МФМЭ уровня сети

Требования к производительности и обеспечению бесперебойного функционирования:

- **П. 14 «В формуляре подтвержденные сведения:**

1) о пропускной способности и задержках сетевых пакетов (кадров):

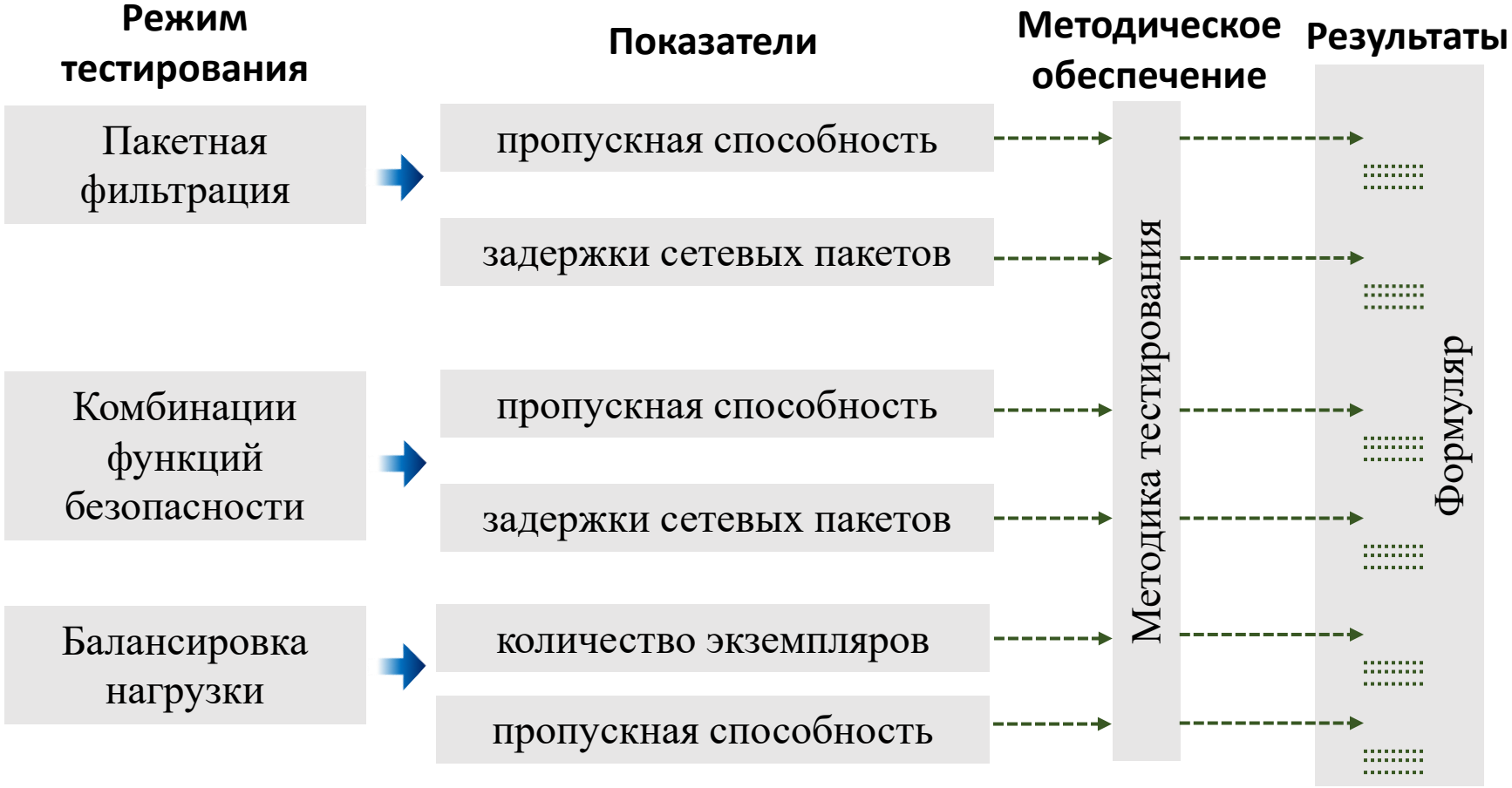
- ✓ в режиме пакетной фильтрации трафика (кадры 1518 байт и 64 байт)
- ✓ веб-трафика в определенных комбинациях функций безопасности

2) о количестве экземпляров МЭ **в режиме балансировки нагрузки** и их общей пропускной способности

3) о способах и средствах балансировки нагрузки;

- **П. 18 возможность работы в отказоустойчивом кластере**

Подтверждение сведений о производительности межсетевого экрана



Типовая методика тестирования производительности и обеспечения бесперебойного функционирования многофункционального межсетевого экрана уровня сети

- Общие положения;
- **Порядок тестирования производительности** МФМЭ;
- **Порядок тестирования** обеспечения **бесперебойного функционирования** МФМЭ;
- **Тесты производительности** МФМЭ;
- **Тесты** обеспечения **бесперебойного функционирования** МФМЭ;
- **Профили сетевого трафика**
- **Пример протокола** тестирования производительности и обеспечения бесперебойного функционирования МФМЭ.

Метод тестирования производительности МФМЭ

МЕТОД НАГРУЗОЧНОГО ТЕСТИРОВАННАЯ

Процесс определения и (или) подтверждения производительности ММЭ ***под нагрузкой, сопоставимой с реальными условиями эксплуатации***.

Нагрузка - сетевой трафик

Варьируемые параметры (способ тестирования)

Объем сетевого трафика

- ✓ увеличение объема (скорости)
- ✓ удержание
- ✓ замедление

Состав сетевого трафика

- ✓ Конкретный протокол
- ✓ Сочетание протоколов (профили трафика)

параметры МФМЭ уровня сети

- ✓ количество правил фильтрации
- ✓ режимы работы
- ✓ комбинации функций безопасности

Изменение объема сетевого трафика

Способ заключается в определении показателя, при которым отсутствуют ошибки по обработке сетевого трафике, а также при котором ММЭ способен выполнять заявленные функциональные возможности в полном объеме

Способ предполагает определение показателей производительности в несколько фаз

1. **фаза нарастания** – осуществляется постепенное увеличение скорости передачи сетевого трафика с целью достижения проверяемого показателя производительности;
2. **фаза удержания** – осуществляется удержание достигнутого показателя с целью подтверждения устойчивости ММЭ
3. **фаза замедления** – осуществляется замедление передачи сетевого трафика от проверяемого показателя с целью подтверждения корректного завершения обработки сетевого трафика

Состав сетевого трафика

***Определение типа сетевого трафика**, с использованием которого осуществляется тестирование производительности МФМЭ уровня сети*

Сетевой трафик, содержащий определенный протокол

Тестирование ММЭ в режиме пакетной фильтрации трафика, содержащего сетевые кадры размером 1518 байт и отдельно 64 байта

Профиль сетевого трафика, содержащий смесь сетевого трафика различного типа

Профили сетевого трафика

В проекте Методики приведены несколько профилей сетевого трафика, характерных для:

- ✓ среднестатистических ГИС;
- ✓ систем с активным видео/аудио- трафиком;
- ✓ систем с трафиком управления ТКО.

Перспективные профили сетевого трафика:

- ✓ для ГИС разных классов и масштабов;
- ✓ для ЗОКИИ в разных сферах деятельности;
- ✓ для систем ИСПДн;
- ✓ для АСУ ТП, использующих разные промышленные протоколы;
- ✓ для информационных систем общего пользования

Параметры МФМЭ уровня сети

Способ заключается в определении производительности ММЭ при разных параметрах настройки

Тестирование при увеличении количества правил фильтрации

В проекте документа предусмотрены вариации общего количества включенных правил фильтрации: 500, 1000, 2000

Тестирование в разных режимах работы ММЭ

Пакетная фильтрация сетевого трафика

Тесты с сетевыми кадрами размером

- 1518 байт
- 64 байт

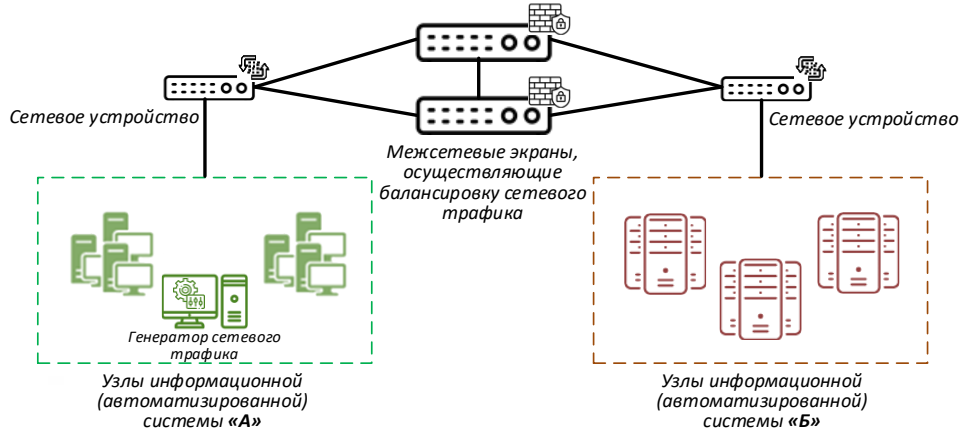
Комбинация включенный функций безопасности

- 6 и 5 классы защиты
- 4 класс защиты

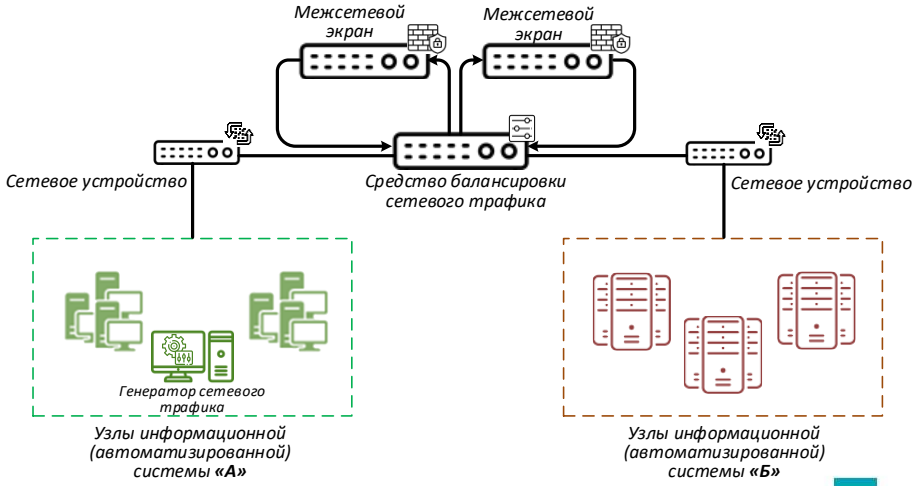
Параметры и режимы работы определены с учетом положений «Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети»

Тестирование балансировки сетевого трафика

Использование нескольких ММЭ, имеющих функциональную возможность балансировки сетевого трафика



Использование стороннего средства балансировки сетевого трафика (брокер)



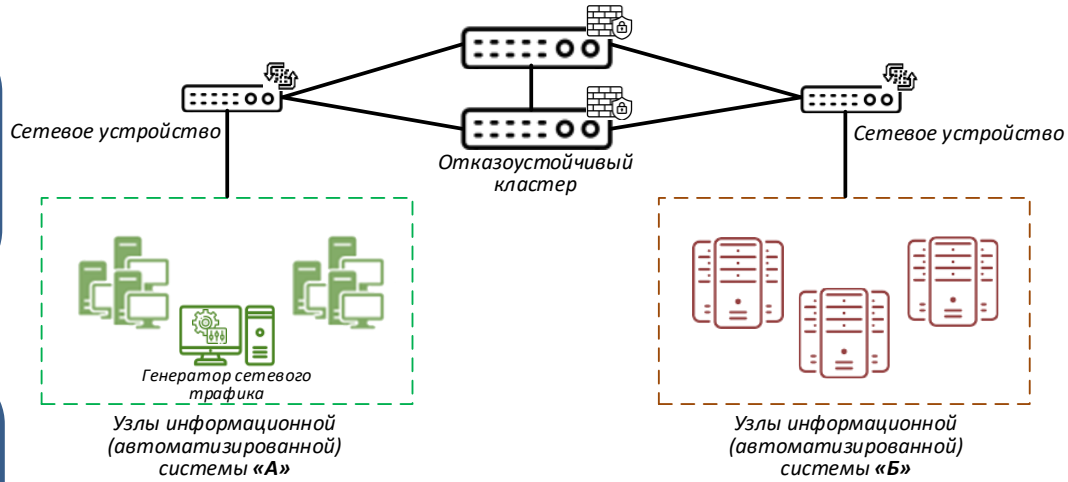
Тестирование работы в отказоустойчивом кластере

Организация отказоустойчивого кластера ММЭ путем **объединения нескольких ММЭ в одну логическую единицу сети**. При отказе одного ММЭ, другое **автоматически берет на себя все функции по обработке сетевого трафика** без прерывания сетевых сессий

Методы организация отказоустойчивого кластера:

Метод «активный/пассивный»
Основной ММЭ (активный) осуществляет обработку сетевого трафика, а резервный ММЭ (пассивный) находится в режиме ожидания и подключается только в случае отказа основного

Метод «активный/активный»
Один ММЭ осуществляет обработку сетевого трафика, а второй ММЭ осуществляет мониторинг состояния первого ММЭ, а также контролирует активные сетевые сессии



Состояние работ по разработке Методики тестирования производительности многофункциональных МЭ уровня сети

Создана рабочая группа

Разработан проект Методики

Получены и обработаны замечания / предложения, уточнен проект Методики

Апробация уточненного проекта Методики

Средства обнаружения и реагирования уровня узла (COP)

Программные средства, предназначенным для обнаружения на узлах информационной (автоматизированной) системы признаков вредоносного программного обеспечения и компьютерных атак, а также их нейтрализации.

мониторинг

обнаружение

реагирование

индикаторы

IoC **IoA**

правила

взаимодействие

Требования по безопасности информации к средствам обнаружения и реагирования уровня 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

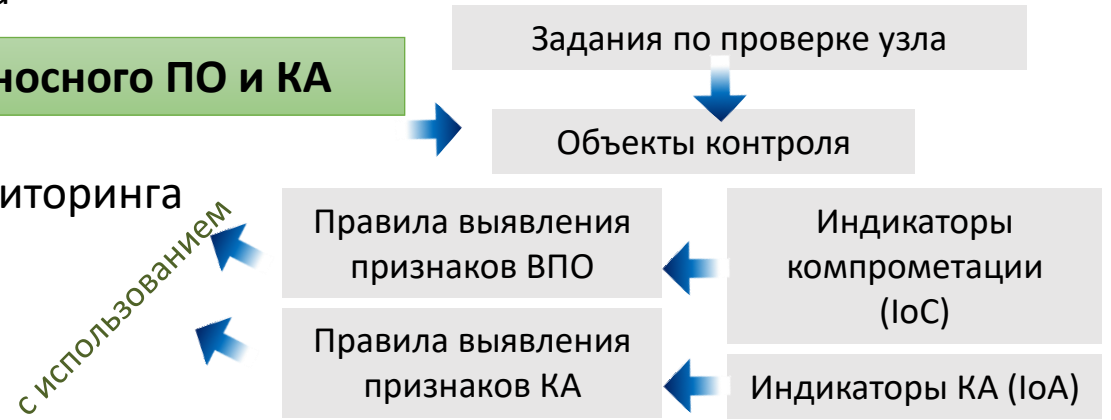
Требования по безопасности информации к средствам обнаружения и реагирования уровня узла (EDR)

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

Взаимодействие с иными средствами защиты информации

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»)

Анализ существующих решений
Выводы

высокий процент реализации по сбору данных мониторинга

вопросы по реализации правил на основе индикаторов атак

неполнота функционала реагирования

сложность определения границ изделия

Отсутствие интеграции с SIEM и «Песочницами» других производителей (замкнутость в собственной линейке)

Анализ существующих решений
Выводы

Перспективные задачи 2025-2026 годов	Разработка и сертификация по требованиям безопасности решений от различных производителей для 6, 5, 4 классов защиты в различных ценовых категориях
	Создание и поддержка в актуальном состояние различных информационных ресурсов, необходимых для функционирования средств, класса COP (EDR)
	Интеграция решений класса COP (EDR) со смежными системами различных производителей Интеграция с TI-платформами

ЦБИ Центр безопасности информации

ГОСТ Р Защита информации. Информационный ресурс служебных баз данных. Защита информации. Общие положения

ПРОБЛЕМА:

Средства ЗИ, предусматривающие использование служебных баз данных (СБД), **напрямую зависят от полноты и качества этих СБД**.

В связи с тем, что СБД существенно влияют на эффективность применения средств ЗИ в системах, должна обеспечиваться **независимая оценка СБД** при сертификации и поддержке безопасности

РЕШЕНИЕ:

- ✓ **Создание** производителями средств ЗИ **информационных ресурсов СБД** (ИР СБД)
- ✓ Обеспечение возможности **использования СБД разных производителей**
- ✓ **Стандартизация форматов** СБД

Служебные базы данных средств ЗИ

- База решающих правил
- База признаков ВПО
- База признаков уязвимостей
- База признаков КА и КИ
- База индикаторов компьютерных атак (IoC)
- База индикаторов компрометации (IoA)

Информационный ресурс служебных баз данных средств защиты информации

Внешний сегмент

Данные, размещаемые производителем (изготовителем):

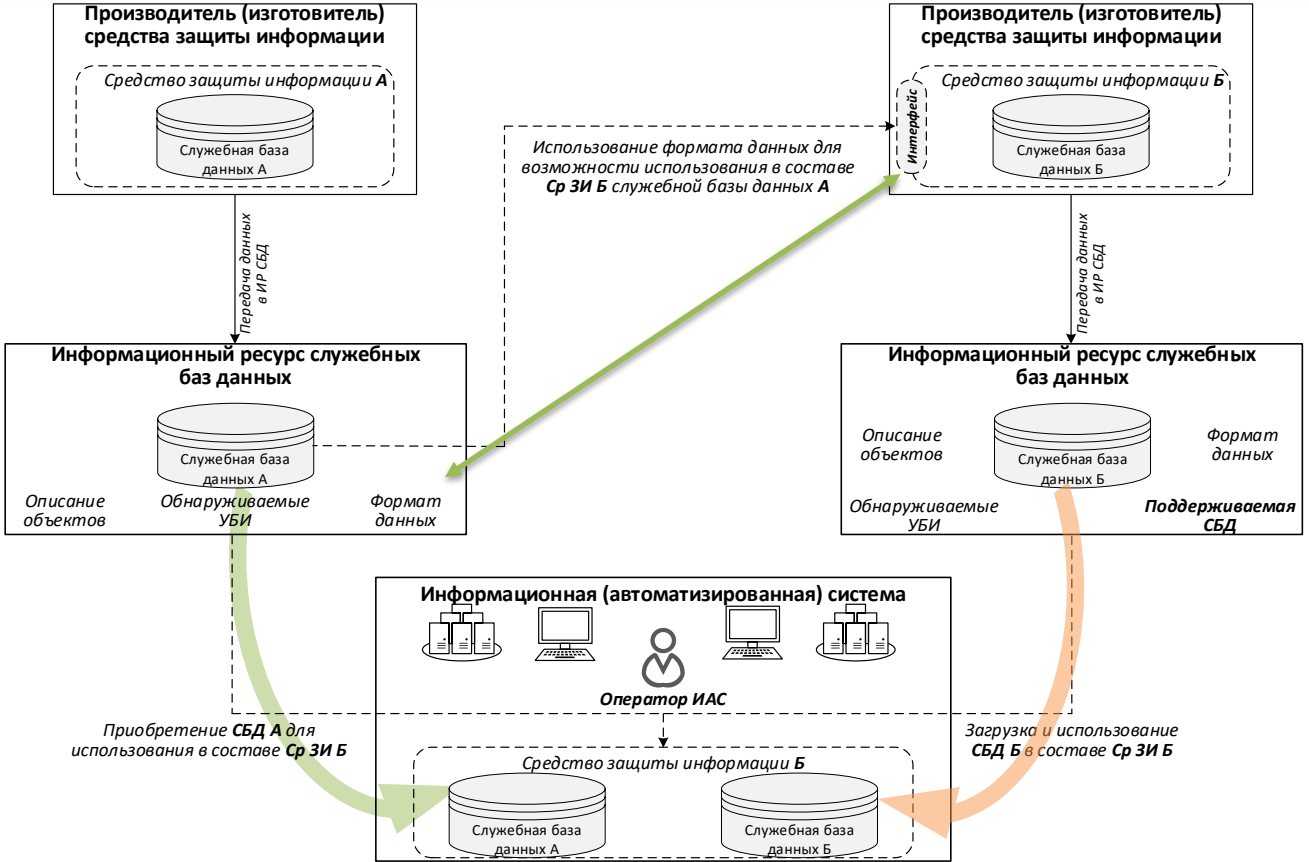
- СБД для загрузки в средство ЗИ;
- информация об объектах, входящих в состав СБД (*формат данных, описание объектов, доп. информация*);
- информация о возможности использования средством ЗИ дополнительных СБД;
- информация о результатах внешнего контроля

Внутренний сегмент

Данные, публикуемые производителем (изготовителем):

- описание процедуры представления обновлений СБД для проведения внешнего контроля;
- тесты, предназначенные для верификации объектов, входящих в состав СБД;
- тестовая изолированная среда для проведения внешнего контроля;
- протоколы внешнего контроля СБД

Использование в составе средств ЗИ дополнительных СБД



Вопросы реализации требований к средствам сетевой защиты информации

ТБ ФОРУМ 2025. 12 февраля 2025 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