советник отдела управления
ФСТЭК России

Кубарев Алексей Валентинович

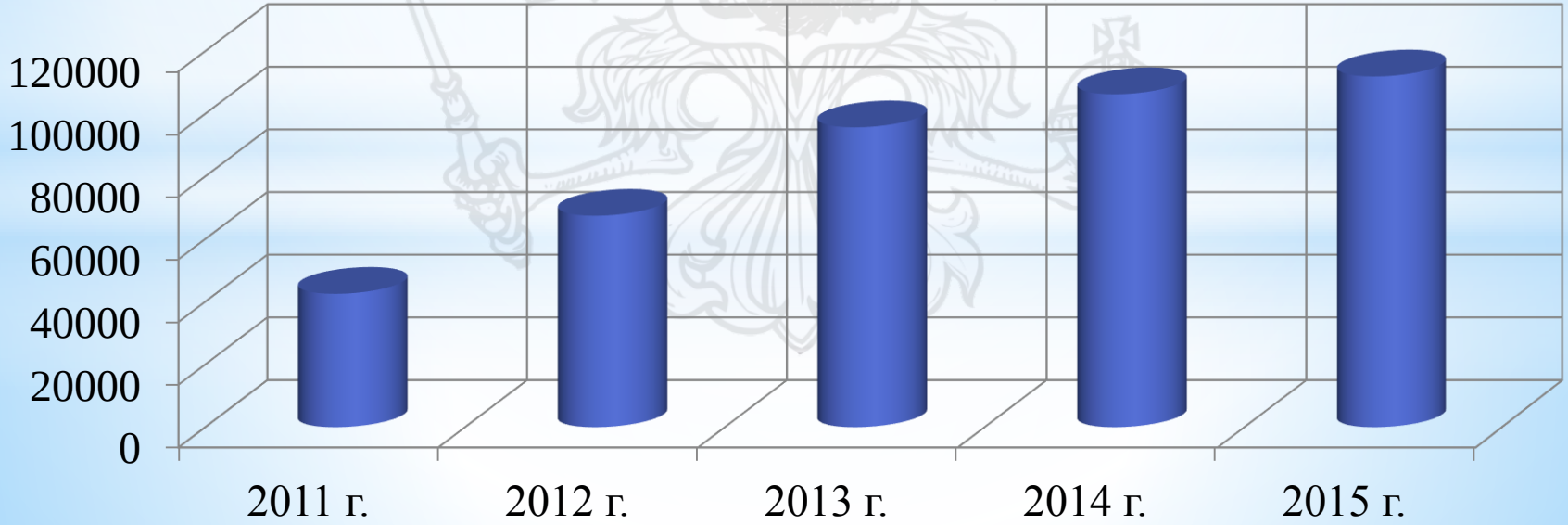
# Совершенствование требований по защите информации, предъявляемых к межсетевым экранам

# Востребованность межсетевых экранов

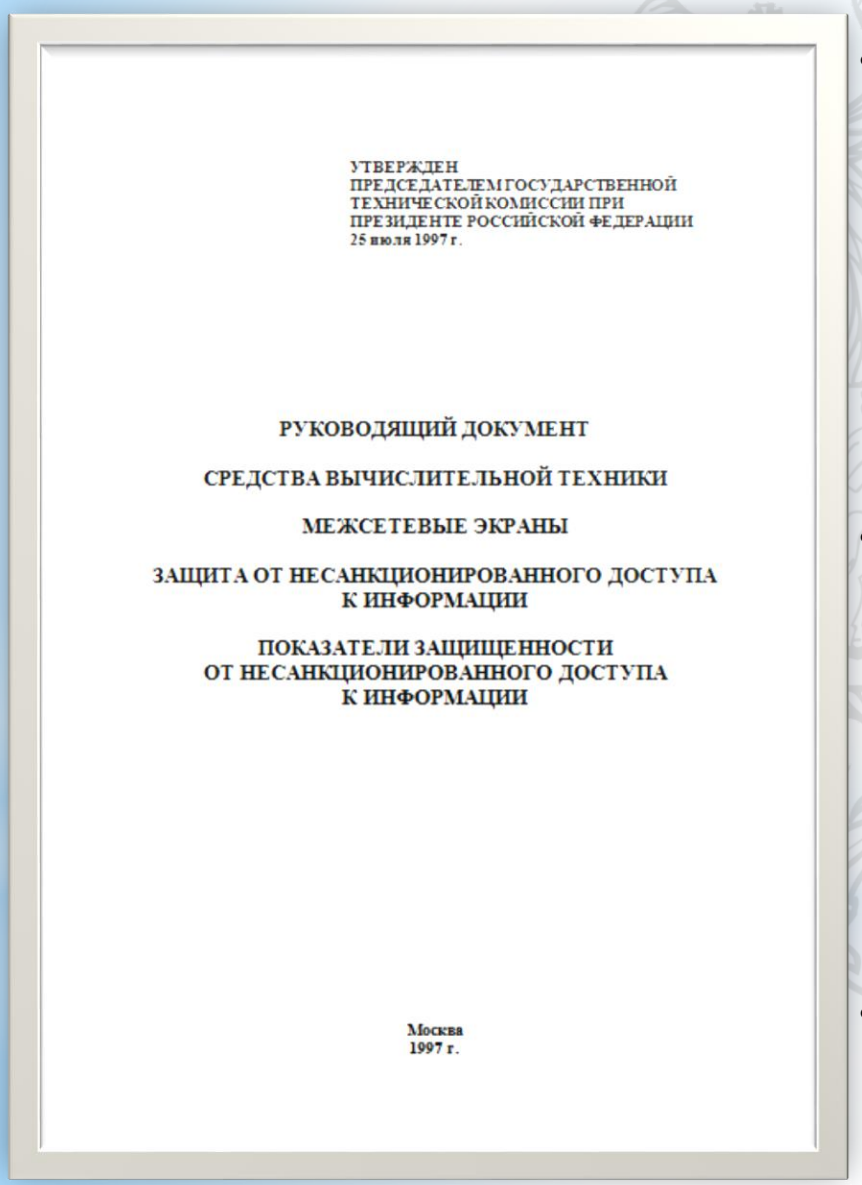
## Сертифицированные средства защиты информации


## Разработчики и производители средств защиты информации


## Произведено сертифицированных межсетевых экранов



# Действующие требования к межсетевым экранам



УТВЕРЖДЕН
ПРЕДСЕДАТЕЛЕМ ГОСУДАРСТВЕННОЙ
ТЕХНИЧЕСКОЙ КОМИССИИ ПРИ
ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
25 июля 1997 г.

РУКОВОДЯЩИЙ ДОКУМЕНТ

СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

МЕЖСЕТЕВЫЕ ЭКРАНЫ

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
К ИНФОРМАЦИИ

ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ
ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
К ИНФОРМАЦИИ

Москва
1997 г.

- **устанавливает классификацию межсетевых экранов (5 классов) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности (12 показателей: 9 по функциям и 3 по свидетельствам) и совокупности описывающих их требований;**
- **предназначен для заказчиков и разработчиков межсетевых экранов, а также вычислительных сетей, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от несанкционированного доступа к информации;**
- **устанавливает соответствие классов межсетевых экранов классам автоматизированных систем.**

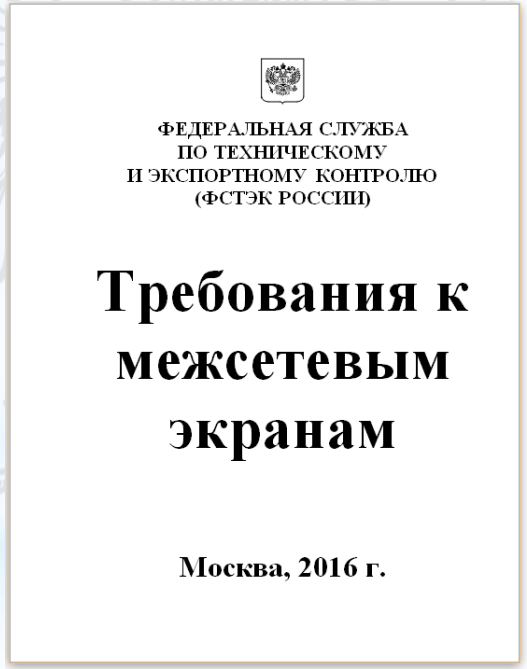
# Разработка Требований к межсетевым экранам

Опыт разработчиков межсетевых экранов

Современные угрозы безопасности информации

Современные технологии межсетевого экранирования

Требования к СОВ, САВЗ, СДЗ и СКСМНИ




ГОСТ Р ИСО/МЭК 15408

Опыт организаций по защите информации

Зарубежные требования к межсетевым экранам

# Структура и назначение Требований к межсетевым экранам

СОДЕРЖАНИЕ


I. Общие положения

II. Общие требования к межсетевым экранам

III. Требования к функциям безопасности межсетевых экранов:

a. требования к составу функций безопасности межсетевых экранов и сред, в которых эти средства функционируют;

b. требования к составу функциональных возможностей межсетевых экранов, обеспечивающих реализацию функций безопасности;

c. требования к реализации функциональных возможностей межсетевых экранов;

d. требования доверия к безопасности межсетевых экранов.


**Требования предназначены для:**

- **разработчиков межсетевых экранов;**
- **производителей межсетевых экранов;**
- **заявителей на сертификацию межсетевых экранов**
- **испытательных лабораторий средств защиты информации;**
- **органов по сертификации средств защиты информации.**

# Общие угрозы безопасности, нейтрализацию которых должен обеспечивать межсетевой экран

## Внешние

- Несанкционированный доступ к информации, содержащейся в информационной системе
- Отказ в обслуживании информационной системы
- Вызов нарушения функционирования межсетевого экрана
- Несанкционированное получение сведений о сети и её узлах

## Внутренние

- Несанкционированная передача информации из информационной системы
- Отказ в обслуживании информационной системы
- Вызов нарушения функционирования межсетевого экрана

# Классификация межсетевых экранов

| Классы защиты межсетевого экрана | Классы защищенности ГИС | Классы защищенности ИСПД | Классы защищенности АСУ ТП |
|---|---|---|---|
| 6 | 3, 4 | 3, 4 | 3 |
| 5 | 2 | 2 | 2 |
| 4 | 1 | 1 | 1 |
| 3 | Применяются в информационных системах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну | | |
| 2 | | | |
| 1 | | | |

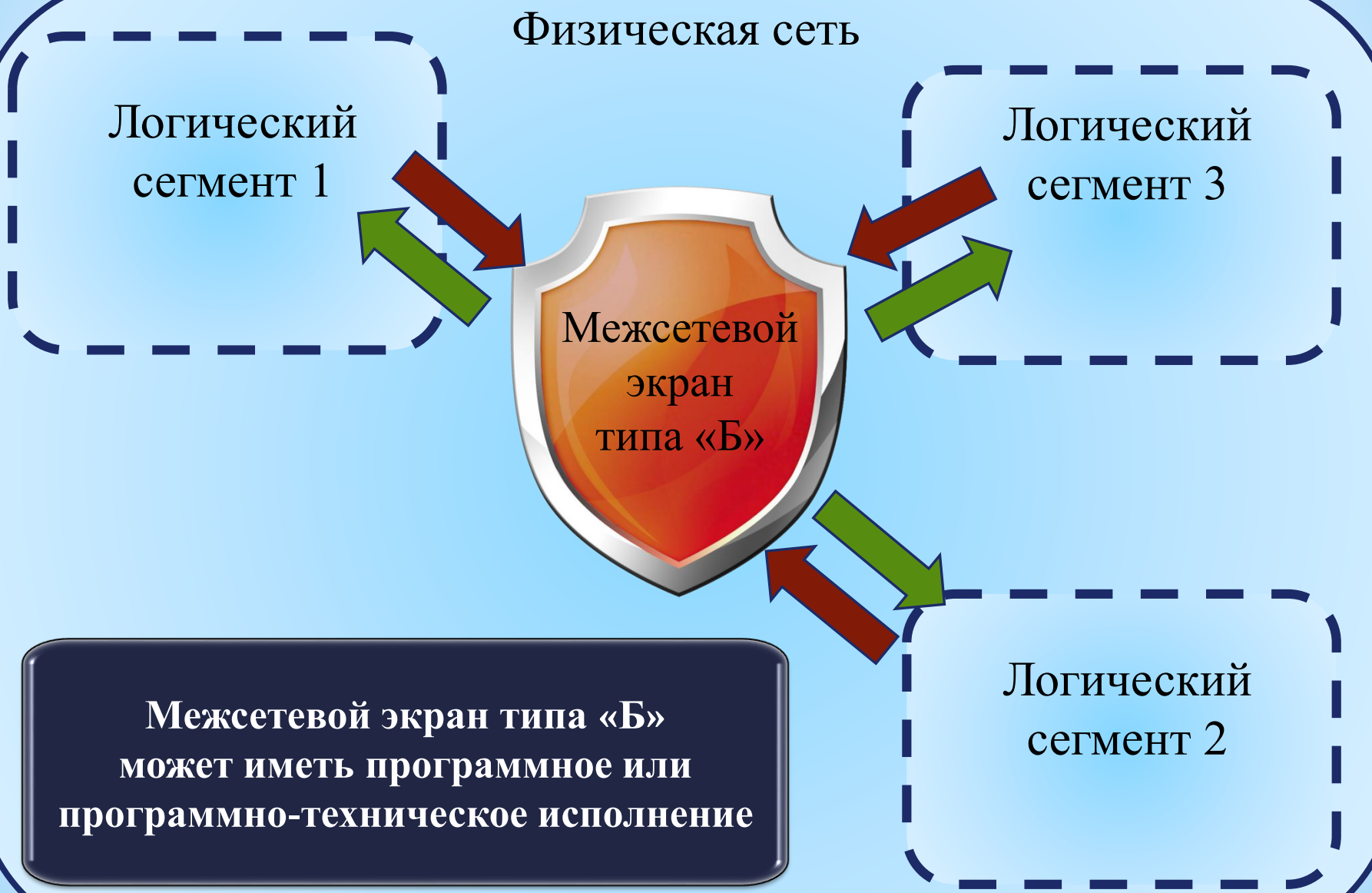
# Типизация межсетевых экранов

| Тип | |
|---|---|
| А | - уровня сети |
| Б | - уровня логических границ сети |
| В | - уровня узла |
| Г | - уровня веб-сервера |
| Д | - уровня промышленной сети |

# Межсетевые экраны типа «А»

**Межсетевой экран типа «А» может иметь только программно-техническое исполнение**

# Межсетевые экраны типа «Б»

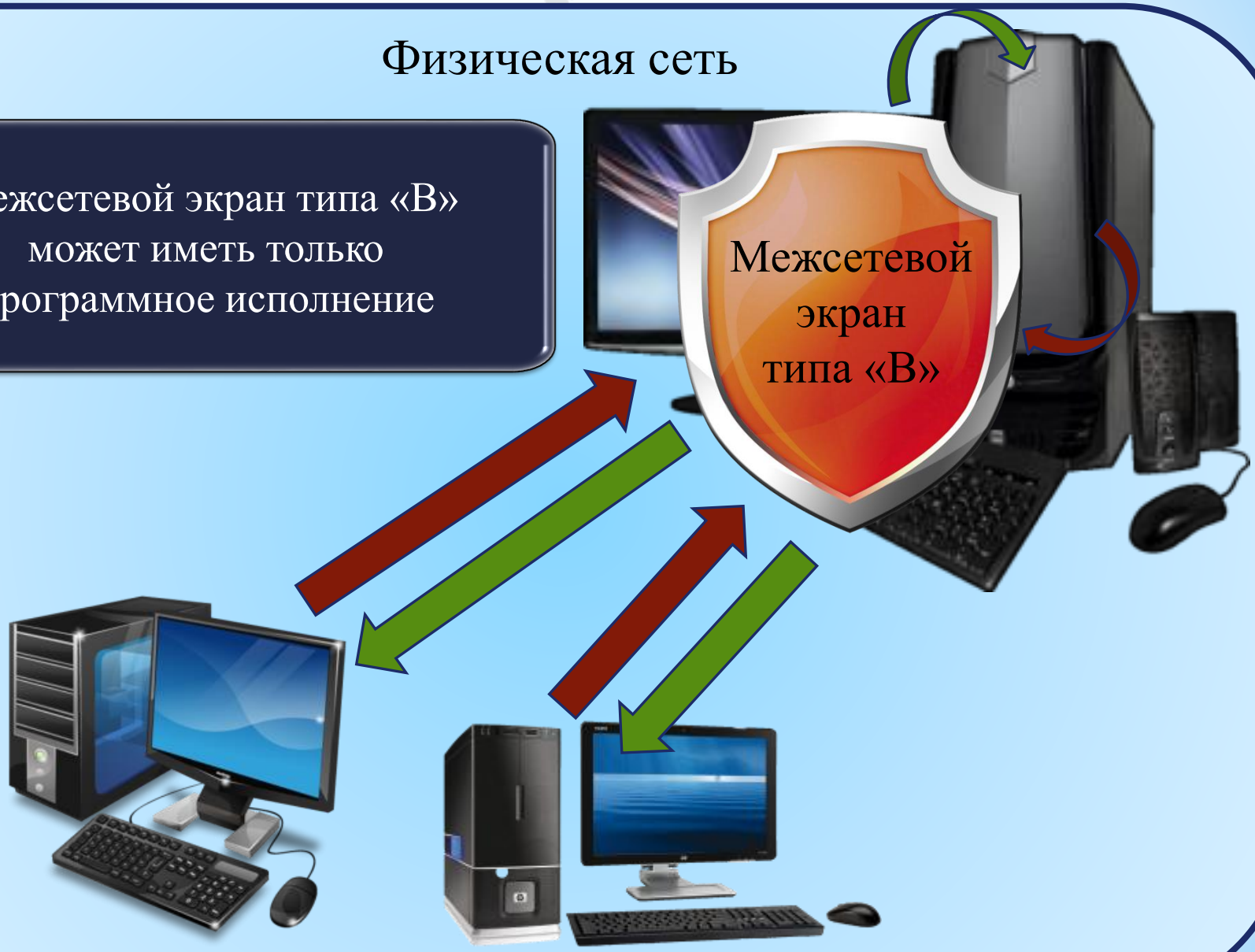



**Межсетевой экран типа «Б» может иметь программное или программно-техническое исполнение**

# Межсетевые экраны типа «В»

Физическая сеть

Межсетевой экран типа «В» может иметь только программное исполнение



# Межсетевые экраны типа «Г»

Веб-сервер

Физическая сеть

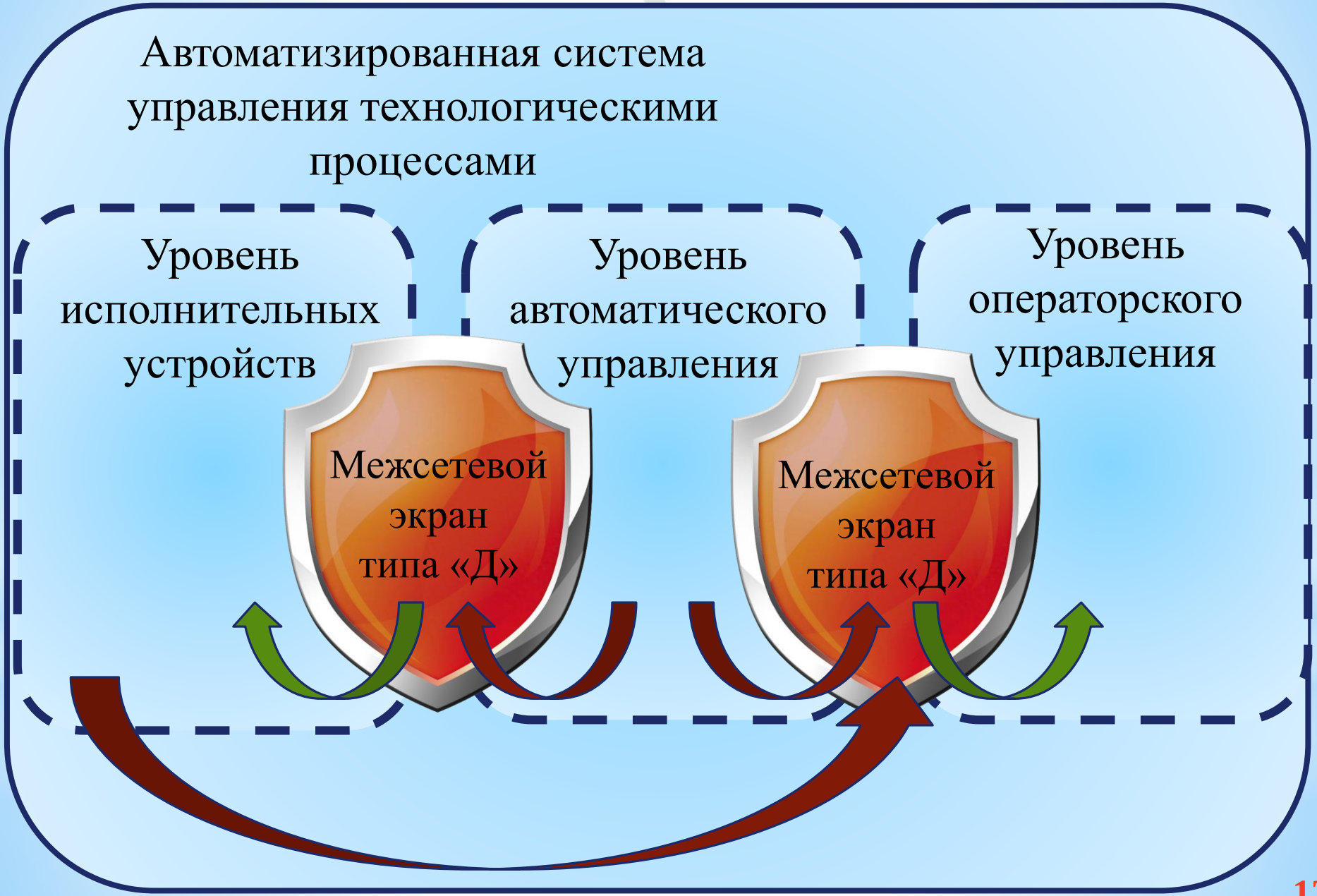

Гипертекст

Гипертекст

Внешние сети

**Межсетевой экран типа «Г» может иметь программное или программно-техническое исполнение**

# Межсетевые экраны типа «Д»



# Функции безопасности, реализуемые межсетевыми экранами

| Функция безопасности | Руководящий документ, 1997 г. | Требования к межсетевым экранам, 2016 г. |
|---|---|---|
| Контроль и фильтрация | Имеется | Усилено |
| Идентификация и аутентификация | С 3 класса | С 6 класса, усилено |
| Регистрация событий безопасности (аудит) | Имеется | Усилено |
| Оповещение о критичных видах событий безопасности | Отсутствует | Имеется |
| Сохранение и восстановление штатного режима функционирования при сбоях и ошибках | В части восстановления | Имеется, усилено |
| Тестирование межсетевого экрана | Имеется | Усилено |
| Проверка целостности программного обеспечения и конфигурации (параметров) межсетевого экрана | Имеется | Усилено |
| Преобразование сетевых адресов | Со 2 класса | С 4 класса, усилено |
| Маскирование наличия межсетевого экрана | Отсутствует | Имеется |
| Приоритизация информационных потоков | Отсутствует | Имеется |
| Администрирование | Имеется | Усилено |
| Взаимодействие с другими СЗИ | Отсутствует | Имеется |

# Требования доверия, предъявляемые к межсетевым экранам (1)

| Требование доверия | Руководящий документ, 1997 г. | Требования к межсетевым экранам, 2016 г. |
|---|---|---|
| Описание архитектуры безопасности | Отсутствует | Имеется |
| Функциональная спецификация с полной аннотацией | Отсутствует | Имеется |
| Архитектурный проект | Частично | Имеется |
| Руководства пользователя и администратора, формуляр | Частично | Имеется |
| Подготовительные процедуры | Частично | Имеется |
| Средства управления авторизацией | Частично | Имеется |
| Охват управления конфигурацией представления реализации | Отсутствует | Имеется |
| Процедуры поставки | Отсутствует | Имеется |
| Идентификация мер безопасности | Отсутствует | Имеется |
| Определенная разработчиком модель жизненного цикла | Отсутствует | Имеется |
| Задание по безопасности | Отсутствует | Имеется |
| Анализ покрытия | Отсутствует | Имеется |
| Тестирование: базовый проект | Имеется | Имеется |
| Правила по безопасной настройке | Имеется | Имеется |

# Требования доверия, предъявляемые к межсетевым экранам (2)

| Требование доверия | Руководящий документ, 1997 г. | Требования к межсетевым экранам, 2016 г. |
|---|---|---|
| Полное независимое тестирование | Имеется | Имеется |
| Анализ уязвимостей | Отсутствует | Имеется |
| Полная функциональная спецификация | Отсутствует | Имеется |
| Полное отображение представления реализации функциональных возможностей безопасности | Отсутствует | Имеется |
| Базовый модульный проект | Отсутствует | Имеется |
| Поддержка генерации, процедуры приемки и автоматизация | Отсутствует | Имеется |
| Базовое устранение недостатков | Отсутствует | Имеется |
| Полностью определенные инструментальные средства разработки | Отсутствует | Имеется |
| Усиленный методический анализ (уязвимостей) | Отсутствует | Имеется |
| Процедуры обновления программного обеспечения | Отсутствует | Имеется |
| Анализ влияния обновлений на безопасность | Отсутствует | Имеется |
| Контроль отсутствия НДВ | Отсутствует | Имеется |

# Общие требования к межсетевым экранам

Отсутствие каналов внеполосного доступа

Применение мер, направленных снижение вероятности возникновения в средстве уязвимостей и других недостатков

Постоянный поиск и устранение уязвимостей заявителем

Дополнительные требования к среде функционирования программных межсетевых экранов

Проверка применения правил фильтрации по всем атрибутам и режимам фильтрации

Оценка соответствия аппаратных средств и всего программного обеспечения , функционирующего на них (в том числе, микропрограммного, общисистемного и иного)

Оценка соответствия только программного обеспечения, реализующего функции безопасности, и исключение возможности использования иного программного обеспечения при сертификации

советник отдела управления
ФСТЭК России

Кубарев Алексей Валентинович

# Спасибо за внимание !

## Совершенствование требований по защите информации, предъявляемых к межсетевым экранам