Кубарев Алексей Валентинович

Требования безопасности информации к межсетевым экранам и операционным системам

Действующие требования, предъявляемые к операционным системам и к межсетевым экранам

Утвержден решением
председателя Государственной
технической комиссии при
Президенте Российской
Федерации от 30 марта 1992 г.

Руководящий документ
Средства вычислительной техники
Защита от несанкционированного доступа к информации
Показатели защищенности от несанкционированного доступа к информации

Москва, 1992 г.

Утверждено решением
председателя Государственной
технической комиссии при
Президенте Российской
Федерации от 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.

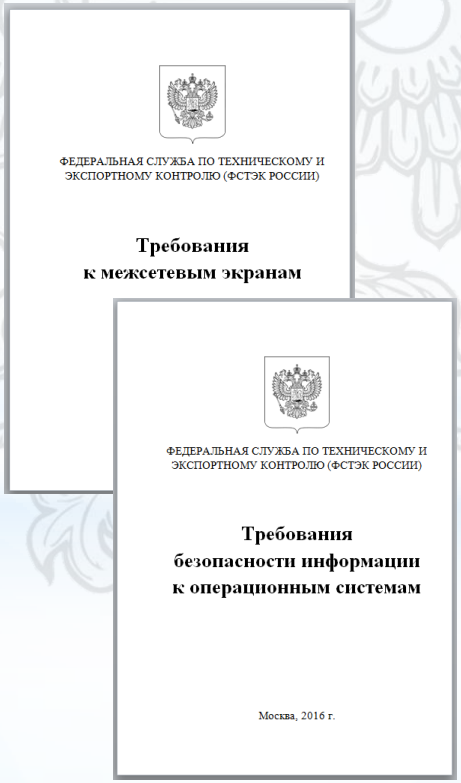
Разработка Требований к межсетевым экранам

Опыт разработчиков межсетевых экранов и операционных систем

Современные угрозы безопасности информации

Современные операционные системы и межсетевые экраны

Требования к СОВ, САВЗ, СДЗ и СКСМНИ

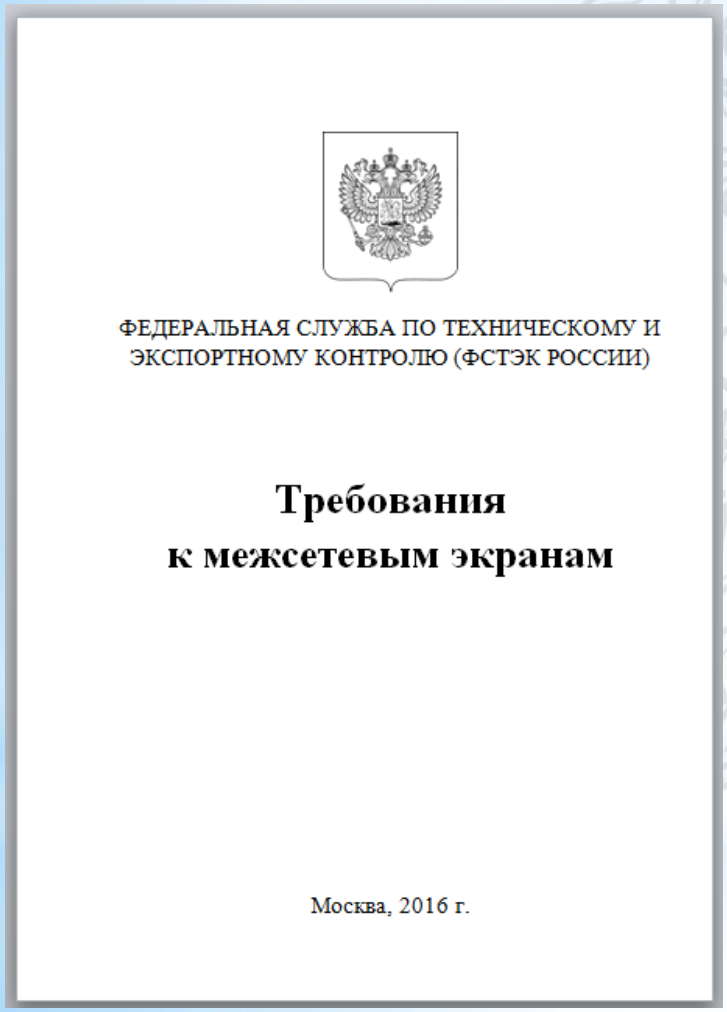


ГОСТ Р ИСО/МЭК 15408

Опыт организаций по защите информации

Зарубежные требования к межсетевым экранам и операционным системам

Введение в действие Требований к межсетевым экранам



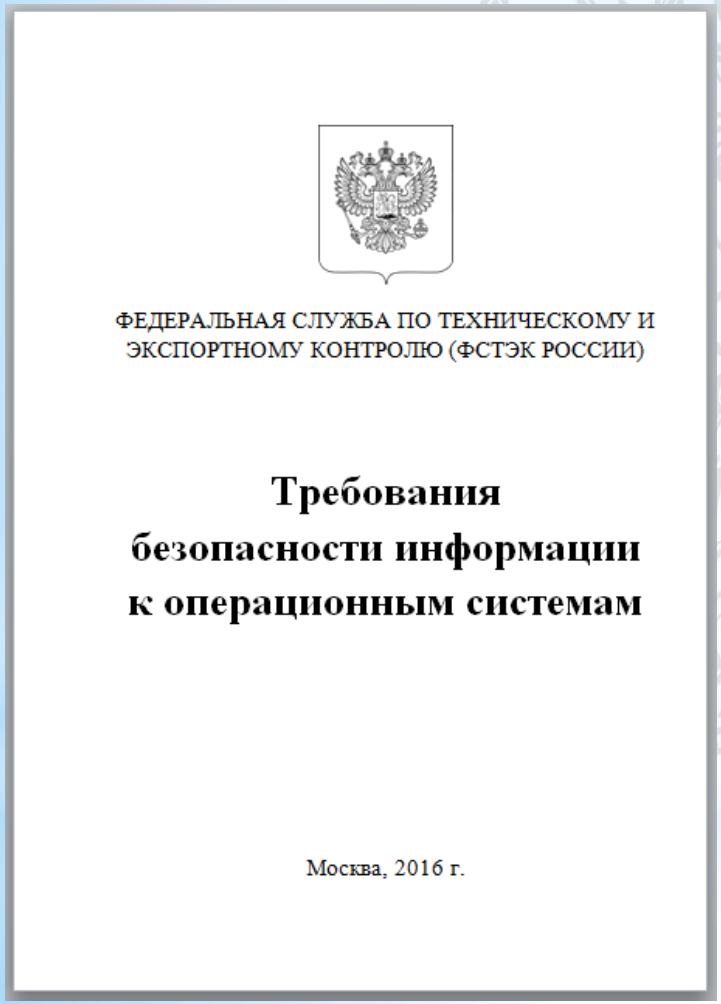
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК РОССИИ)

Требования к межсетевым экранам

Москва, 2016 г.

Утверждены	**приказом ФСТЭК России от 9 февраля 2016 г. № 9**
Зарегистрированы Минюстом России	**25 марта 2016 г., регистрационный № 41564**
Вступают в силу	**с 1 декабря 2016 г.**

Введение в действие Требований безопасности информации к операционным системам



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК РОССИИ)

Требования безопасности информации к операционным системам

Москва, 2016 г.

Утверждены — **приказом ФСТЭК России от 19 августа 2016 г. № 119**

Проходят процедуру регистрации в Минюсте России

Вступают в силу — **с 1 июня 2017 г.**

Структура и назначение Требований

СОДЕРЖАНИЕ

Требования предназначены для:

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

Классификация межсетевых экранов и операционных систем

Классы защиты СЗИ	Классы защищенности ГИС	Уровни 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			

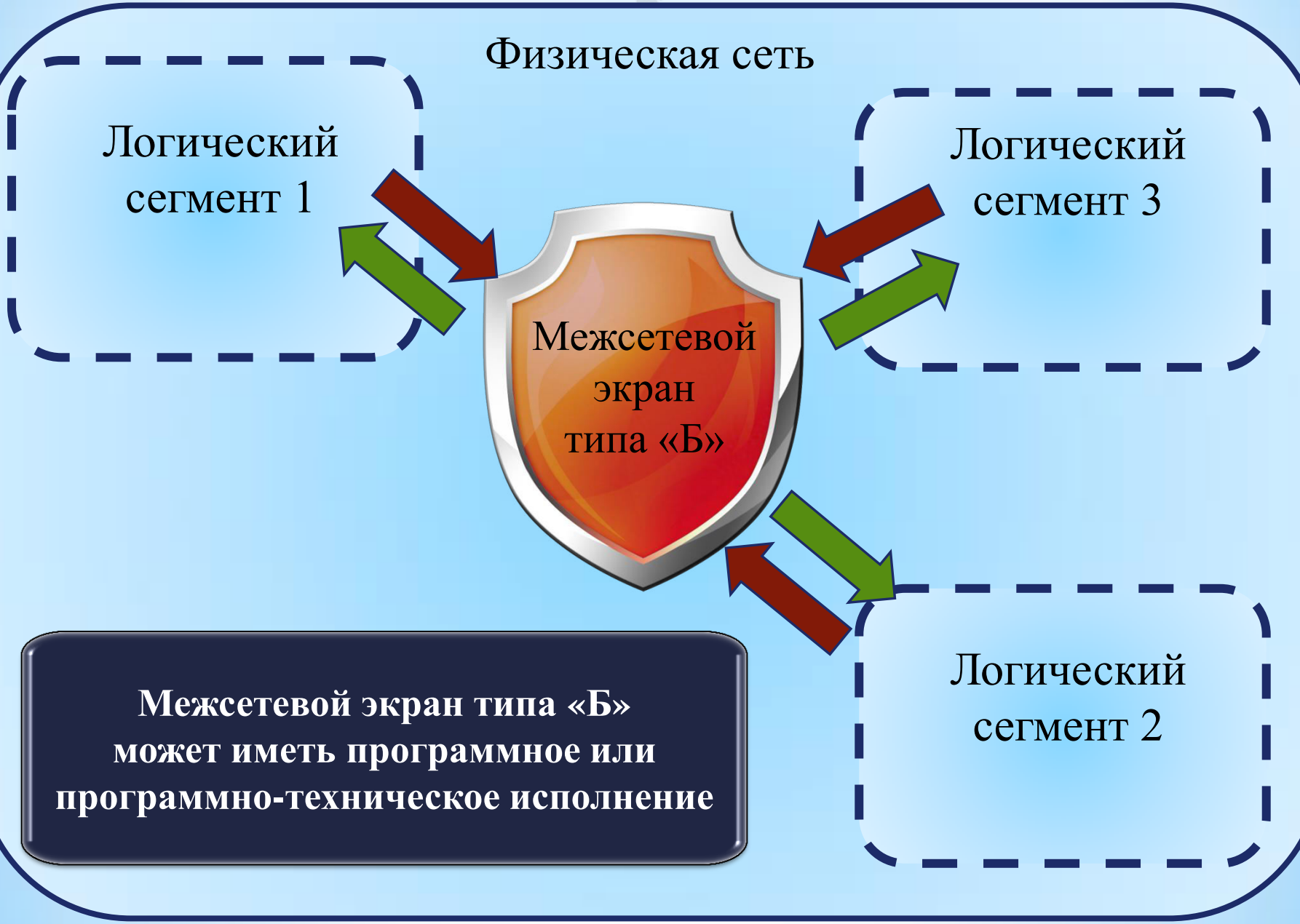
Типизация межсетевых экранов

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»

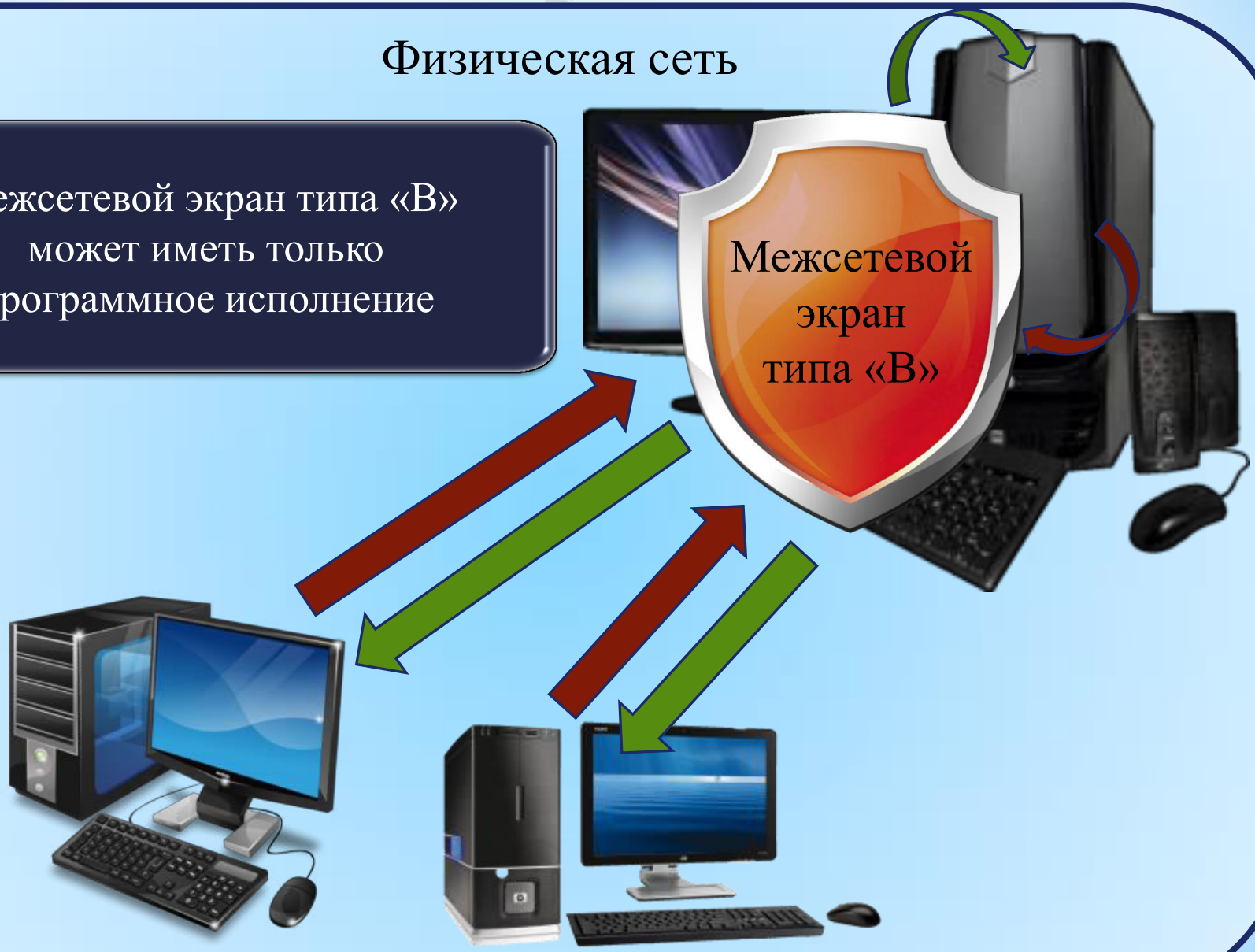


Межсетевой экран типа «Б» может иметь программное или программно-техническое исполнение

Межсетевые экраны типа «В»

Физическая сеть

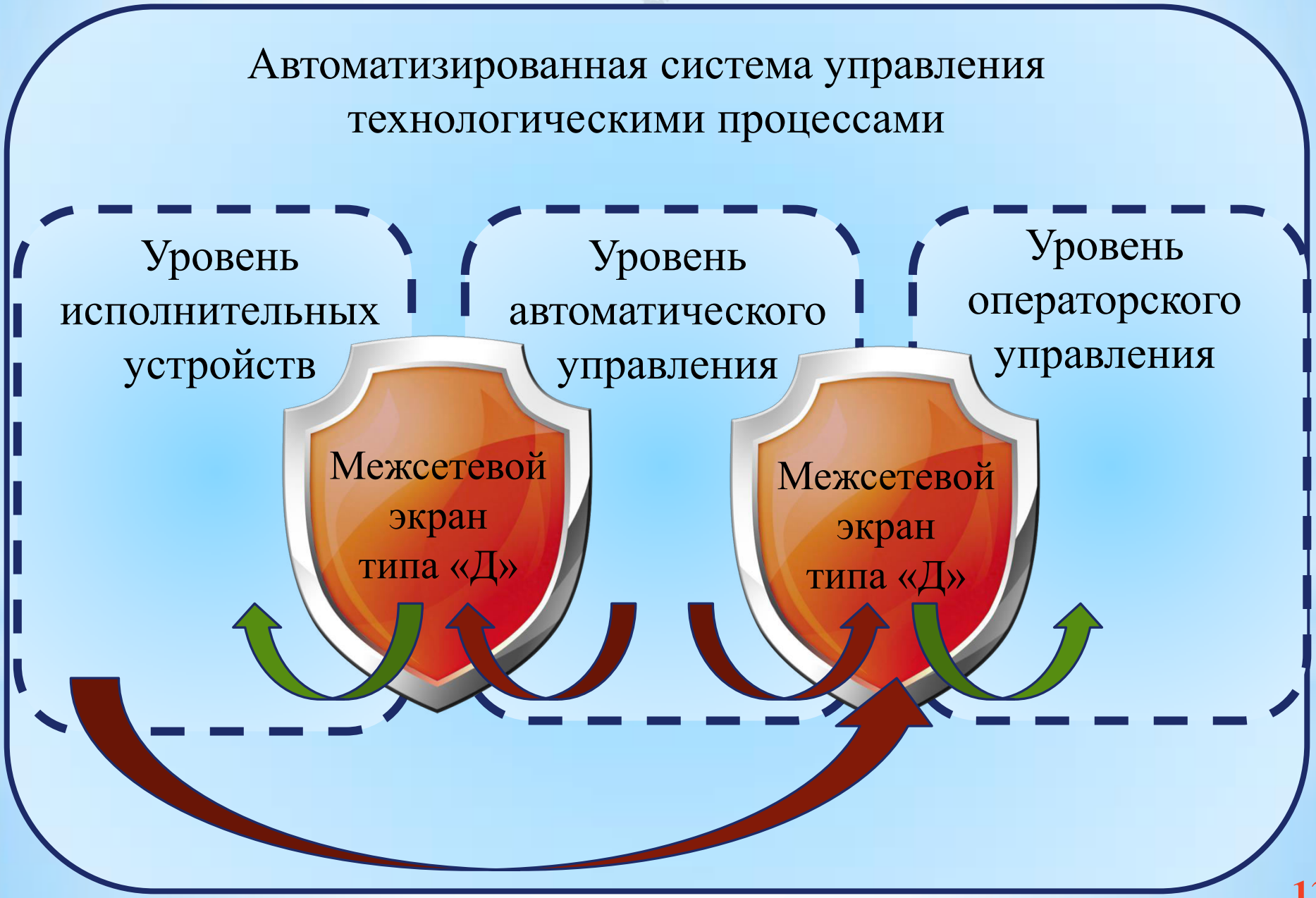
Межсетевой экран типа «В» может иметь только программное исполнение



Межсетевые экраны типа «Г»

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

Межсетевые экраны типа «Д»



Типизация операционных систем

Тип	
А	- общего назначения
Б	- встраиваемая
В	- реального времени

Операционные системы типа «А»

Операционные системы типа «Б»

Операционные системы типа «В»

Функции безопасности, реализуемые операционными системами

Функция безопасности	Руководящий документ, 1992 г.	Требования к операционным системам, 2016 г.
Управление доступом	Имеется	Усилено
Идентификация и аутентификация	Имеется	Усилено
Регистрация событий безопасности (аудит)	С 5 класса	С 6 класса, усилено
Оповещение о критичных видах событий безопасности	Отсутствует	Имеется
Сохранение и восстановление штатного режима функционирования при сбоях и ошибках, обеспечение доступности	С 3 класса, частично	Имеется, усилено
Ограничение программной среды	Отсутствует	Имеется
Фильтрация сетевых потоков	Отсутствует	Имеется
Изоляция процессов	Имеется	Усилено
Очистка остаточной информации и защита от выполнения произвольного кода	С 5 класса	С 6 класса, усилено
Контроль целостности компонентов	Имеется	Усилено
Маркирование документов	С 4 класса	С 6 класса, усилено

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
Приоритезация информационных потоков	Отсутствует	Имеется
Администрирование	Имеется	Усилено
Взаимодействие с другими СЗИ	Отсутствует	Имеется

Требования доверия, предъявляемые к средствам защиты информации (1)

Требование доверия	Руководящие документы, 1992 г. и 1997 г.	Требования, 2016 г.
Описание архитектуры безопасности	Частично	Имеется
Функциональная спецификация с полной аннотацией	Частично	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	Частично	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 средствам защиты информации (2)

Требование доверия	Руководящие документы, 1992 г. и 1997 г.	Требования, 2016 г.
Полное независимое тестирование	Имеется	Имеется
Анализ уязвимостей	Отсутствует	Имеется
Верификация формальной модели	Частично	Имеется
Полное отображение представления реализации функциональных возможностей безопасности	Частично	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	Только для ГТ	Имеется

Информационное сообщение ФСТЭК России

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И
ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

от 28 апреля 2016 г. № 240/24/1986

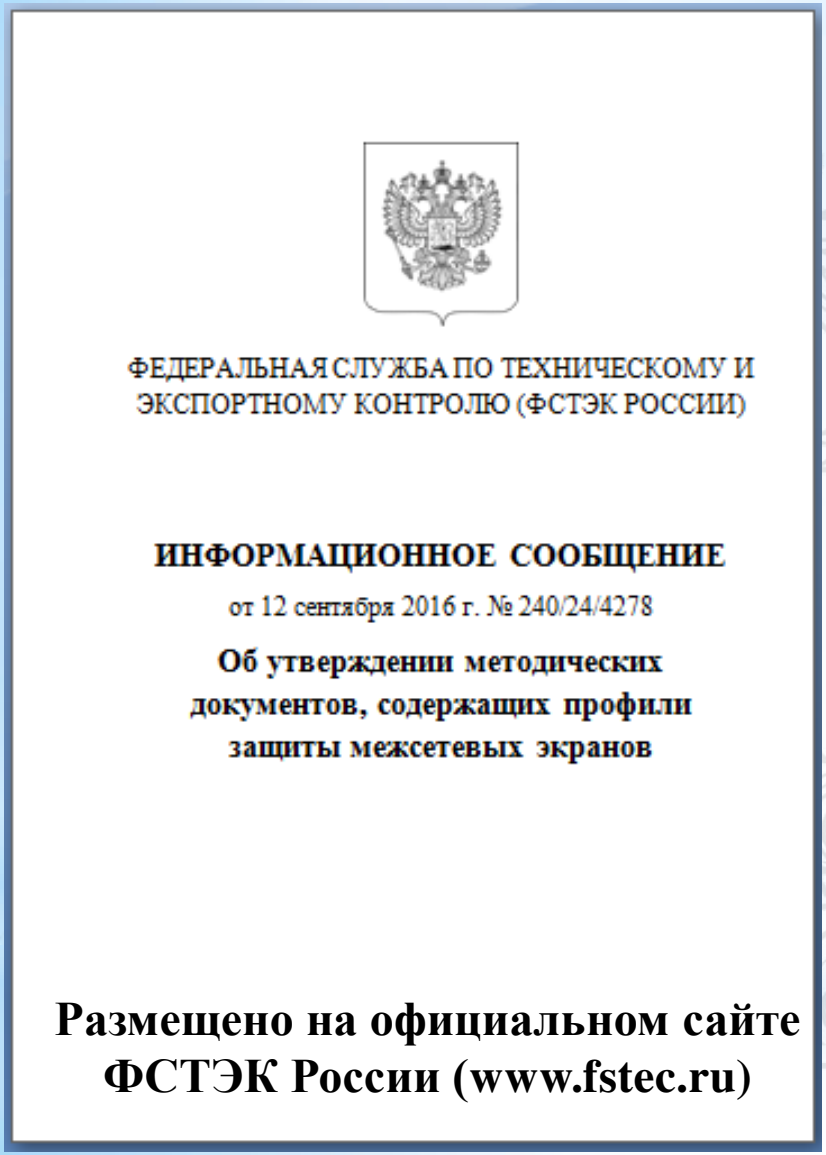
**Об утверждении
Требований к межсетевым экранам**

Размещено на официальном сайте ФСТЭК России (www.fstec.ru)

в разделе «Документы. Информационные и аналитические материалы»

- Сведения об утверждении Требований и регистрации приказа
- Область применения Требований
- Для кого предназначены
- Типизация межсетевых экранов
- Классификация межсетевых экранов
- Сведения о порядке применения Требований
- Сведения об обеспечении Требованиями

Информационное сообщение ФСТЭК России



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК РОССИИ)

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

от 12 сентября 2016 г. № 240/24/4278

Об утверждении методических документов, содержащих профили защиты межсетевых экранов

Размещено на официальном сайте ФСТЭК России (www.fstec.ru)

в разделе «Документы. Информационные и аналитические материалы»

- Сведения об утверждении методических документов
- Область применения методических документов
- Для кого методические документы предназначены
- Спецификация методических документов
- Сведения об обеспечении Требованиями

Порядок применения Требований к межсетевым экранам

С 01.07.16

В ФСТЭК России **не принимаются** к рассмотрению **заявки на сертификацию** межсетевых экранов на соответствие иным требованиям

До 01.12.16

Возможна установка межсетевых экранов, сертифицированных на соответствие иным требованиям, **на объекты информатизации**

Возможны производство и поставка межсетевых экранов, соответствующих иным требованиям

С 01.12.16

Разрабатываемые, производимые и поставляемые межсетевые экраны **должны соответствовать Требованиям**

Сертификация, а также инспекционный контроль серийного производства межсетевых экранов будут осуществляться только на соответствие Требованиям

Применение сертификатов соответствия межсетевых экранов иным требованиям

Решения на сертификацию межсетевых экранов и операционных систем на соответствие иным требованиям **будут аннулированы**

Сертификаты соответствия межсетевых экранов и операционных систем, производимых серийно, иным требованиям **будут аннулированы**

Сертификация межсетевых экранов и операционных систем, имеющих действующие сертификаты соответствия иным требованиям будет проводиться **в форме инспекционного контроля**

Продление сертификатов соответствия межсетевых экранов и операционных систем, эксплуатируемых на объектах информатизации, иным требованиям **будет осуществляться по упрощенной схеме**

Кубарев Алексей Валентинович

Спасибо за внимание !

Требования безопасности информации к межсетевым экранам и операционным системам