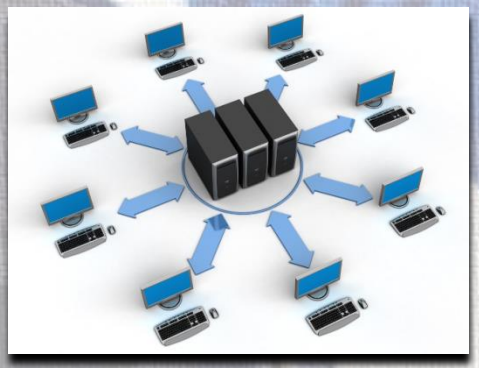
НОРМАТИВНАЯ ПРАВОВАЯ И МЕТОДИЧЕСКАЯ БАЗА В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

НАЧАЛЬНИК ОТДЕЛА
УПРАВЛЕНИЯ ФСТЭК РОССИИ
ПО СИБИРСКОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
СЕЛИФАНОВ ВАЛЕНТИН ВАЛЕРЬЕВИЧ

СИСТЕМЫ ЗИ ИС

Кто?

оператор ИС



Чем?

По каким требованиям?

Набор обязательных и компенсационных мер

ИНФОРМАЦИЯ

информация ограниченного доступа

ГТ,
Закон РФ «О гос. тайне»

Информация ограниченного доступа, не содержащая сведения, составляющие гос. тайну

Открытая информация – государственный информационный ресурс №8-ФЗ

Профессиональная тайна, различные ФЗ в отдельных направлениях

Персональные данные,
ФЗ «О персональных данных»

Коммерческая тайна,
ГК РФ ч. 4,
ФЗ «О коммерческой тайне»

Служебная тайна,
ПП РФ 1233

ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

Информационные (автоматизированные) системы различного назначения

- **обрабатывающие информацию ограниченного доступа (не ГТ)**
- **обрабатывающие информацию ограниченного доступа (ГТ)**
- **обрабатывающие общедоступную информацию**

- **КСИИ**
- **ПОО-И (АСУ ТП)**
- **ООИ**

СИСТЕМА ТРЕБОВАНИЙ В ОБЛАСТИ ТЗИ

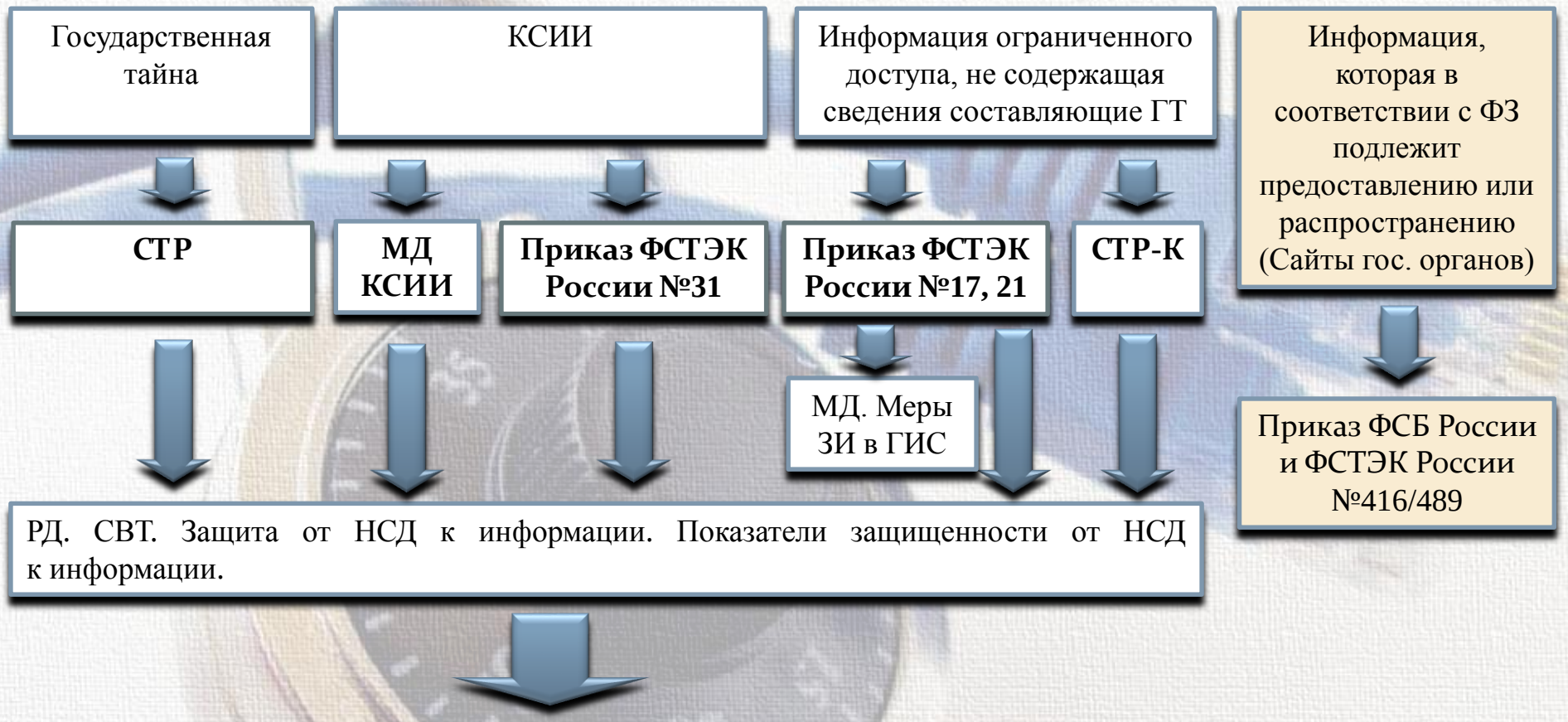
ФЗ или НПА, определяющий необходимость защиты

ПА или МД, НС или МС определяющий порядок работы

ПА ФОИВ или МД ФОИВ (ТЗ), определяющие требования к СЗИ

Программы и методики испытаний

СИСТЕМА ТРЕБОВАНИЙ В ОБЛАСТИ ТЗИ



СИСТЕМА ТРЕБОВАНИЙ В ОБЛАСТИ ТЗИ

Государственная тайна	КСИИ	Информация ограниченного доступа, не содержащая сведения составляющие ГТ	Информация, которая в соответствии с ФЗ подлежит предоставлению или распространению
СТР	Приказ ФСТЭК России №31	Приказы ФСТЭК России №17, 21	Приказ ФСБ России и ФСТЭК России №416/489

Требования к системам обнаружения вторжений
(Приказ ФСТЭК России №638, с 15 марта 2012 г.)

ПЗ 1 12

Требования к средствам антивирусной защиты
(Приказ ФСТЭК России №28, с 1 августа 2012 г.)

ПЗ 1 24

Требования к средствам доверенной загрузки
(Приказ ФСТЭК России №119, с 1 января 2014 г.)

ПЗ 1 10

Требования к средствам контроля съемных машинных носителей информации
(Приказ ФСТЭК России №87, с сентября 2014 г.)

ПЗ 1 10

Требования в области сертификации

ЭВОЛЮЦИЯ СИСТЕМЫ ТРЕБОВАНИЙ К СЗИ

Система РД НСД

- РД СВТ
- РД АС
- РД МЭ
- РД НДВ

- Управление доступом
- Регистрация и учет
- Обеспечение целостности
- Межсетевое экранирование

Система требований к СЗИ от НСД нового поколения

- Требования к средствам идентификации и аутентификации
- Требования к средствам управления доступом
- Требования к средствам разграничения доступа
- Требования к средствам управления потоками информации
- Требования к средствам контроля целостности
- Требования к средствам очистки памяти
- Требования к средствам межсетевого экранирования

- Требования к средствам защиты от несанкционированного вывода (ввода) информации (DLP – системы)
- Требования к средствам контроля и анализа защищенности
- Требования к средствам ограничения программной среды
- Требования к операционным системам
- Требования к системам управления базами данных
- Требования к средствам защиты среды виртуализации
- Требования к базовым системам ввода-вывода

СИСТЕМА ТРЕБОВАНИЙ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗИ

Система требований к оценке эффективности

ТЗ и ТП

- Нейтрализация актуальных угроз
- Выполнение требований к СЗИ

Программа и методика испытаний

Испытания

1. Формирование требований к системе ЗИ АСЗИ

- **Формирование требований к АС**
- **Разработка концепции АС**
- **Техническое задание**

2. Разработка системы ЗИ АСЗИ

- **Эскизный проект**
- **Технический проект**
- **Рабочая документация**

3. Внедрение системы ЗИ АСЗИ

- **Ввод в действие**
- **Аттестация АСЗИ**

4. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ

- **Сопровождение АС**

Формирование требований к АС (Приказ №17)

Определение угроз безопасности

- возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей
- анализа возможных уязвимостей информационной системы
- возможных способов реализации угроз безопасности информации
- последствий от нарушения свойств безопасности информации

Модель угроз безопасности информации

- описание информационной системы и ее структурно-функциональных характеристик
- описание угроз безопасности информации, включающее описание
  - возможностей нарушителей (модель нарушителя)
  - возможных уязвимостей информационной системы
  - способов реализации угроз безопасности информации
  - последствий от нарушения свойств безопасности информации

РАЗРАБОТКА МОДЕЛИ УГРОЗ

Модель угроз безопасности информации строиться с использованием методических документов ФСТЭК России

Базовая модель угроз безопасности ПДн при их обработке, в ИСПДн

http://bdu.fstec.ru/

Методика определения актуальных угроз безопасности ПДн при их обработке, в ИСПДн

Проект МД. Методика определения угроз безопасности информации в ИС.

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УБ ПДн, ПРИ ИХ ОБРАБОТКЕ В ИСПДн

Общие положения

Процесс определения угроз безопасности информации в ИС

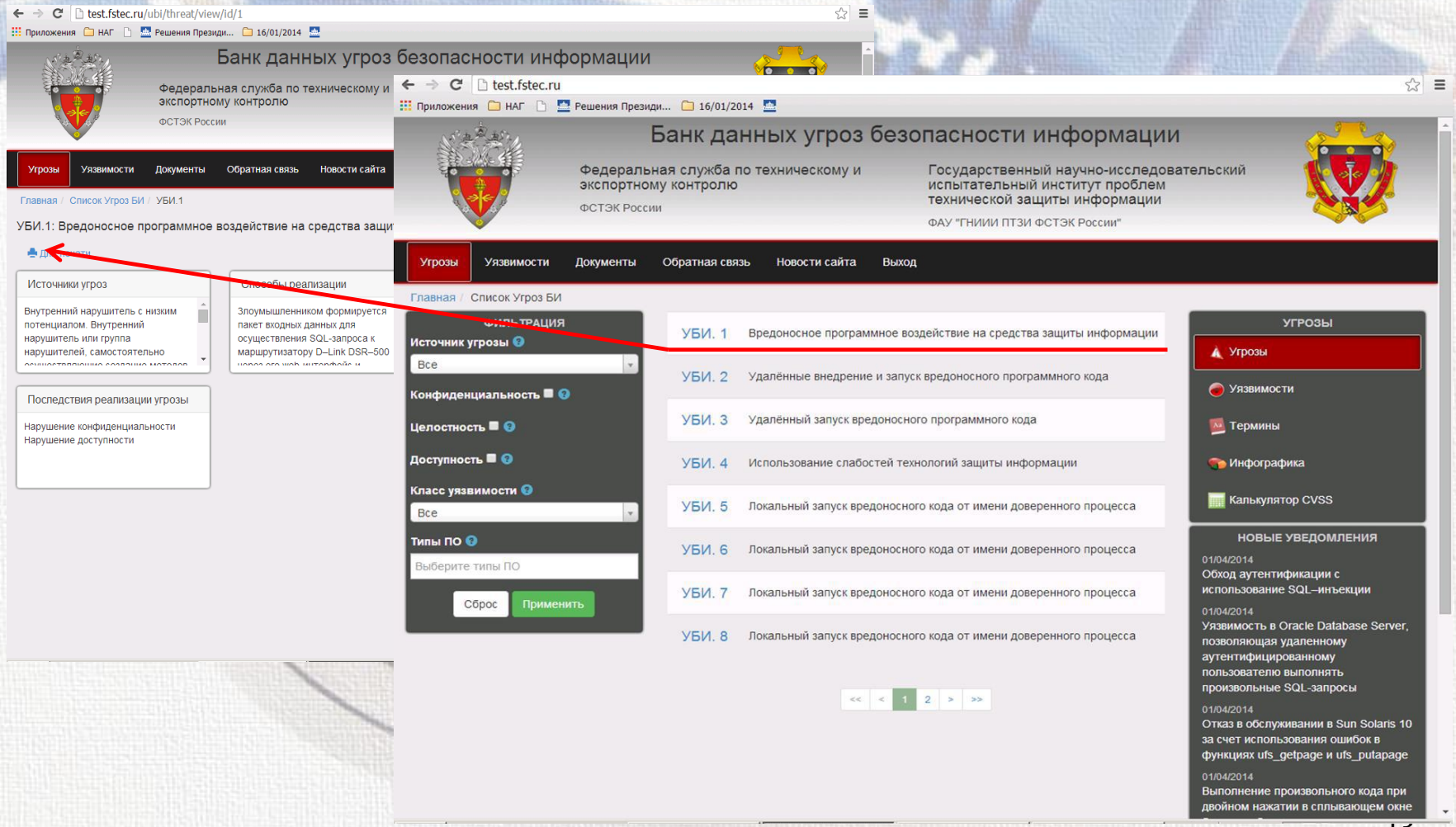
Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя)

Определение актуальных угроз безопасности информации в ИС

Приложение № 1	**Рекомендации по формированию экспертной группы и проведению экспертной оценки при определении угроз безопасности информации**
Приложение № 2	**Структура модели угроз безопасности информации**
Приложение № 3	**Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в ИС**

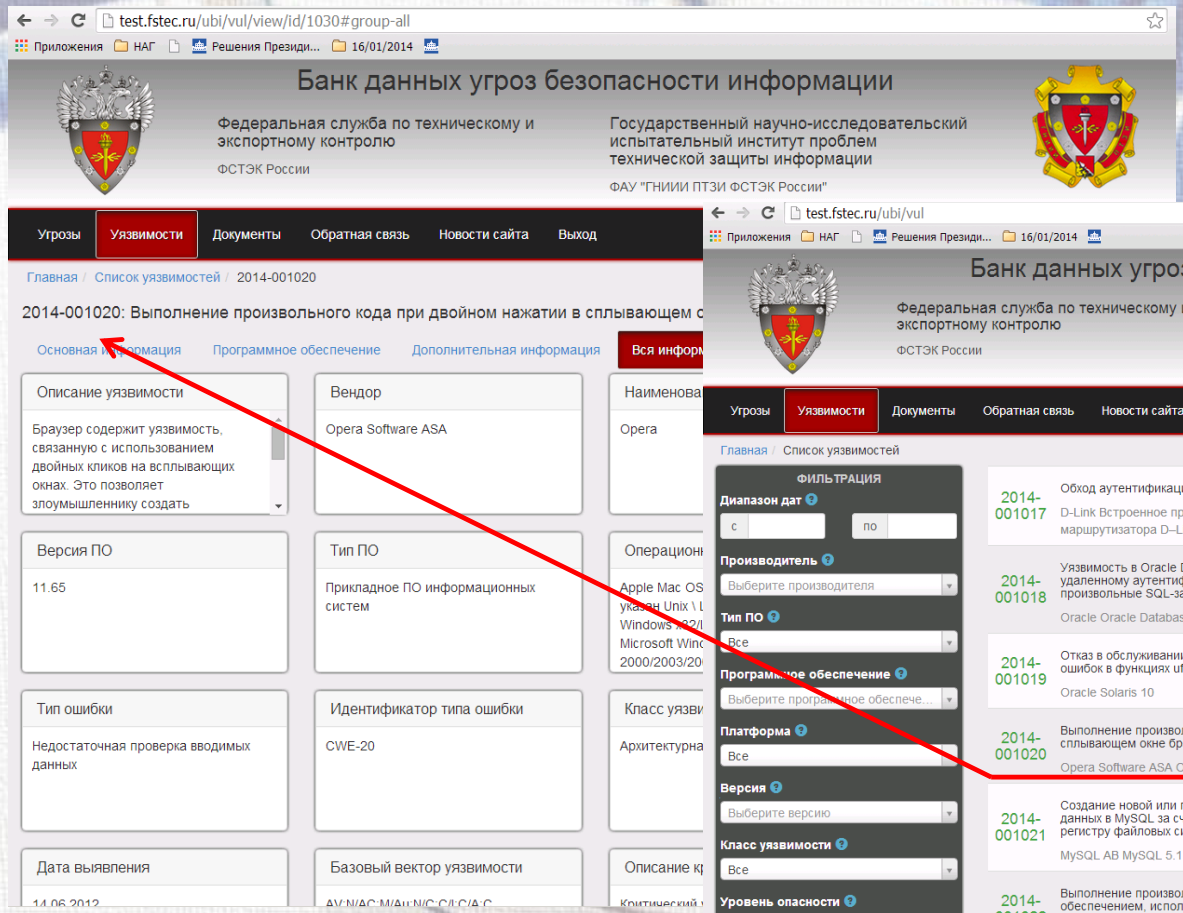
ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ

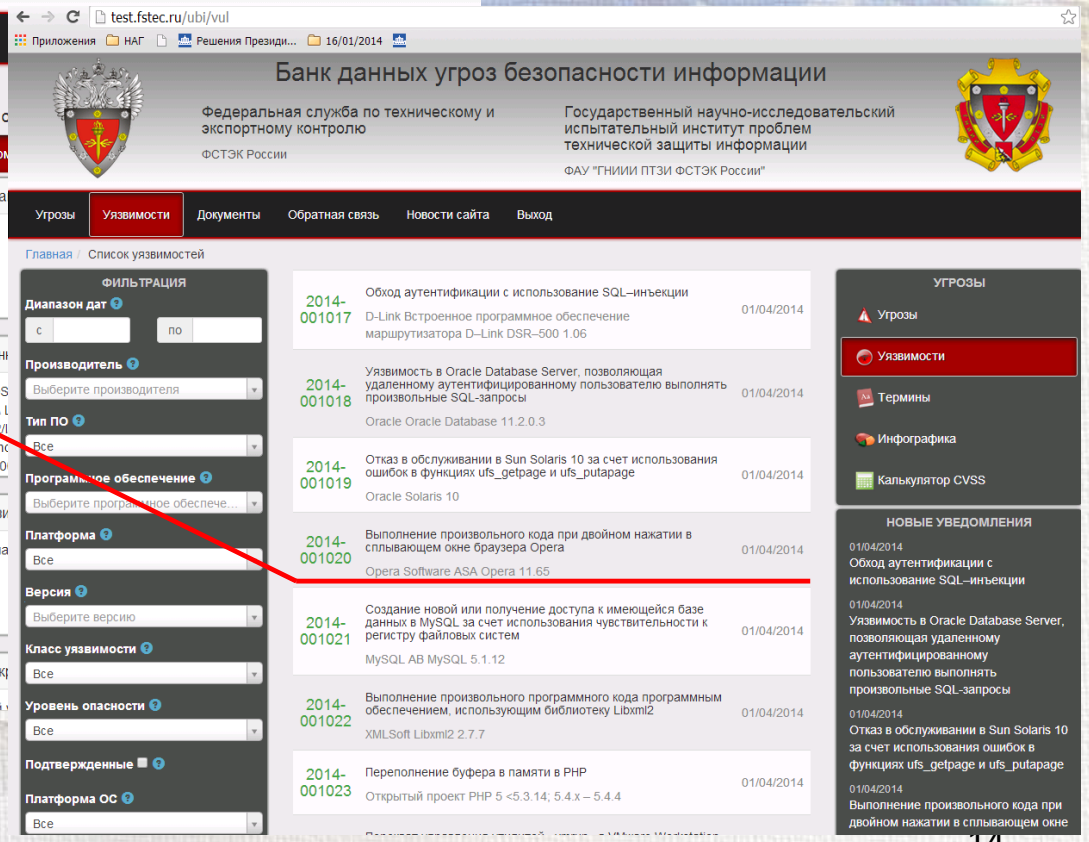
WEB-интерфейс открытого сегмента БДУ (подсистема «угрозы»)



ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ

WEB-интерфейс открытого сегмента БДУ (подсистема «уязвимости»)





АНАЛИЗ УЯЗВИМОСТЕЙ

РАЗРАБАТЫВАЕМЫЕ ДОКУМЕНТЫ

ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»

ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»

ГОСТ Р «Защита информации. Уязвимости информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей информационных систем»