



ТОП-5 проблемных требований ГОСТ Р 57580.1-2017

Диана Лейчук
руководитель направления аудитов

Аналитический центр, УЦСБ

Екатеринбург





1

«Проблемные» требования
ГОСТ Р 57580.1-2017



2

Как подготовиться
к аудиту?



3

Онлайн-сервис оценки
соответствия ГОСТ Р 57580

«ПРОБЛЕМНЫЕ» ТРЕБОВАНИЯ ГОСТ Р 57580.1-2017

01

Межсетевое
экранирование
во внутренней сети

02

Централизованный
сбор событий
безопасности

03

Обнаружение и
регистрация
инцидентов защиты
информации

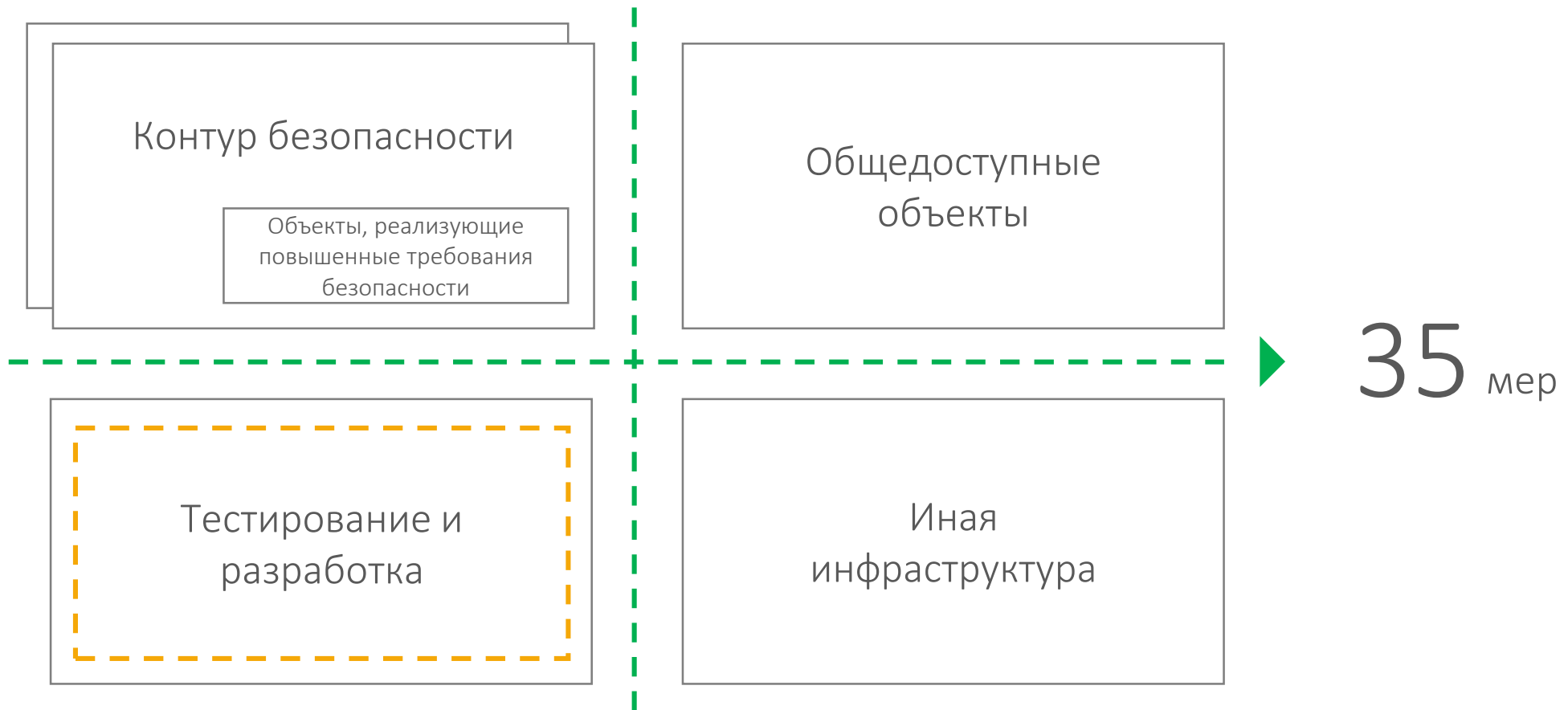
04

Требования по
контролю

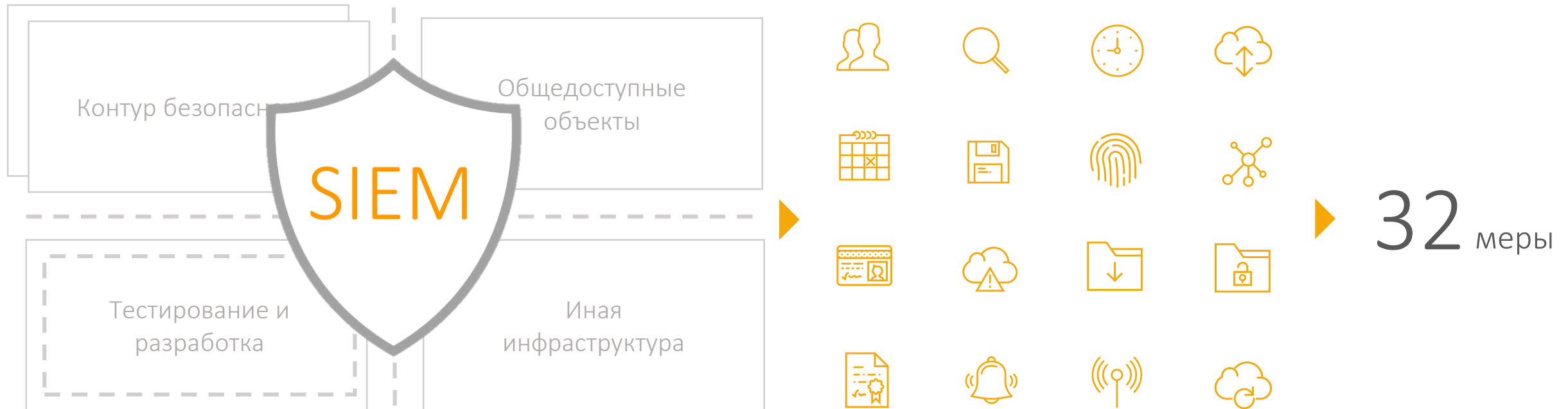
05

Учет
машинных
носителей
информации

01. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ ВО ВНУТРЕННЕЙ СЕТИ



02. ЦЕНТРАЛИЗОВАННЫЙ СБОР СОБЫТИЙ БЕЗОПАСНОСТИ

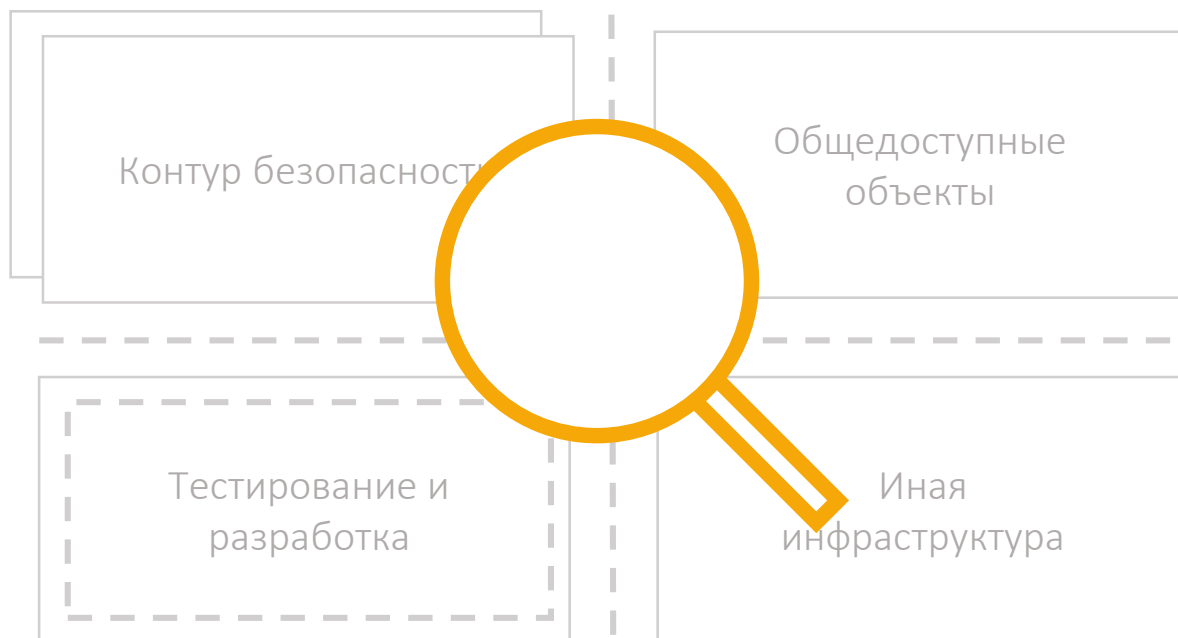


03. РЕГИСТРАЦИЯ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ



► 13 мер

04. ТРЕБОВАНИЯ ПО КОНТРОЛЮ



- Права логического доступа
- Действия администратора
- Размещение ресурсов доступа
- Состав разрешенного к использованию ПО
- Машинные носители информации

▶ 45 мер

05. УЧЕТ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Мера СЗИ		Уровень защиты информации		
		3	2	1
ПУИ.20	Учет и контроль использования машинных носителей информации, предназначенных для хранения информации конфиденциального характера	0	0	0

0 – организационная

Системы хранения данных тоже необходимо учитывать!



1

«Проблемные» требования
ГОСТ Р 57580.1-2017



2

Как подготовиться
к аудиту?



3

Онлайн-сервис оценки
соответствия ГОСТ Р 57580

КАК ПОДГОТОВИТЬСЯ К АУДИТУ?

- 01 Определить контуры безопасности
- 02 Определить объекты, входящие в область оценки
- 03 Сформировать «Положение о применимости ГОСТ Р 57580.1»
- 04 Провести самооценку и GAP-анализ
- 05 Разработать ОРД, настроить встроенные средства защиты





1

«Проблемные» требования
ГОСТ Р 57580.1-2017



2

Как подготовиться
к аудиту?



3

Онлайн-сервис оценки
соответствия ГОСТ Р 57580

Степень вовлеченности проверяемой организации	Местоположение аудитора	
	на местах	на расстоянии
взаимодействие людей	- проведение интервью - заполнение проверочных листов и вопросников с участием персонала проверяемой организации - проведение анализа документации с участием представителей проверяемой организации - осуществление представительных выборок	через интерактивные средства коммуникации: - проведение интервью - заполнение проверочных листов и вопросников - проведение анализа документации с участием представителей проверяемой организации
без взаимодействия людей	- проведение анализа документации - наблюдение за выполнением работы - посещение производственных подразделений - заполнение проверочных листов - осуществление представительных выборок	- проведение анализа документации - наблюдение за выполнением работы с помощью технических средств - анализ данных

ГОСТ Р 57580.2-2018

выбор конкретных источников свидетельств при проведении оценки соответствия осуществляет проверяющая организация (проверяющая группа) с учетом предложений проверяемой организации и обеспечения **максимальной достоверности оценки соответствия ЗИ**

01 Сервис «самооценки»

02 Сервис для дистанционного аудита

РЕЗУЛЬТАТЫ АУДИТА

- Отчет об аудите
- Числовые оценки соответствия с их обоснованием
- Заполненные листы сбора свидетельств
- Рекомендации по совершенствованию
- Копии документов на бумажных носителях, машинные носители информации с информацией, предоставляемой в качестве свидетельств проверяемой организацией
- Возможность использовать результаты аудита для подготовки к дальнейшим оценкам соответствия



ОНЛАЙН-СЕРВИС ДИСТАНЦИОННОЙ ОЦЕНКИ СООТВЕТСТВИЯ ГОСТ Р 57580

УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ | **USSC.RU**



Самостоятельная
оценка соответствия
и подготовка к аудиту



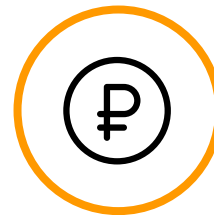
Шаблоны и справочники
выполнения мер
ГОСТ Р 57580



Выполнение требований
положений Банка России



Отчет по предварительному
аудиту для представления
в Банк России



Сокращение затрат на процедуру
оценки соответствия за счет
самостоятельной работы



online.ussc.ru

НАШИ ПРЕДЛОЖЕНИЯ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU



Оценка соответствия
требованиям ГОСТ Р 57580



Тестирование
на проникновение



Анализ уязвимостей
по ОУД



Анализ рисков ИБ



Онлайн-сервис
дистанционной оценки
соответствия ГОСТ Р 57580



Комплексные аудиты ИБ



Предварительный аудит
и приведение в соответствие
с требованиями регуляторов



Автоматизация процессов ИБ
в организации



СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?



Диана Лейчук

Руководитель направления аудитов,
Аналитический центр

dleichuk@ussc.ru

УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ | **USSC.RU**