USSC

Как проводится аудит по ГОСТ Р 57580.2-2018?

Сергей Борисов

Анастасия Заведенская

График проведения вебинаров

№	Дата	Название
1	15.04	Требования Банка России по информационной безопасности некредитных финансовых организаций
2	22.04	Требования Банка России по информационной безопасности кредитных финансовых организаций
3	29.04	Анализ уязвимостей по требованиям к ОУД4
4	20.05	Обзор требований ГОСТ Р 57580.1-2017
5	17.06	Как проводится аудит по ГОСТ Р 57580.2-2018?
6	08.07	Онлайн-сервис оценки соответствия ГОСТ Р 57580.2-2018
7	15.07	Биометрия в финансовых организациях
8	19.08	Пентесты для финансовых организаций
9	16.09	Требования к средствам криптографической защиты информации в финансовых организациях

Ведущие пятого выпуска

Сергей Борисов

Заместитель руководителя по ИБ
обособленного подразделения УЦСБ
г. Краснодар

Блог: https://sborisov.blogspot.com

Анастасия Заведенская

Аналитик
Аналитический центр УЦСБ
г. Екатеринбург

План

- [ ] Выбор проверяющей организации
- [ ] Область проверки
- [ ] Возможные результаты аудита
- [ ] Сроки прохождения аудита
- [ ] Рекомендации

Цели аудита

Объективная и независимая оценка выбора и реализации требований ГОСТ Р 57580.1-2017

Определение организационных и технических мер для:

- приведения в соответствие требованиям ГОСТ Р 57580.1-2017 и Положений Банка России
- повышения уровня защищенности информации

Выбор проверяющей организации

Кто может провести аудит?

Лицензиаты ФСТЭК России на деятельность по технической защите конфиденциальной информации как минимум по одному виду работ и услуг:

- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации
- проектирование в защищенном исполнении средств и систем информатизации
- установка, монтаж, наладка, испытание, ремонт средств защиты информации

Кто может провести аудит?

Организации, обладающие необходимым уровнем компетенции

НАПРИМЕР

- Имеют опыт аудита на соответствие комплекса стандартов СТО БР ИББС, Положению Банка России № 382-П

- Наличие в штате специалистов, обладающих соответствующей квалификацией и сертификатами:

  Certified Information Systems Auditor (CISA)

  Certified Information Systems Security Professional (CISSP)

  Certified Information Security Manager (CISM)

Выбор проверяющей организации

Кого **нельзя** привлекать к аудиту?

- Организации, являющиеся зависимыми от проверяемой организации
- Организации, осуществлявшие или осуществляющие оказание услуг проверяемой организации в области реализации информатизации и защиты информации (в части внедрения и/или сопровождения систем, средств, процессов информатизации и защиты информации, включенных в область аудита), и организации от них зависимые

План

- [x] Выбор проверяющей организации
- [ ] Область проверки
- [ ] Возможные результаты аудита
- [ ] Сроки прохождения аудита
- [ ] Рекомендации

Область оценки соответствия

- Совокупность объектов информатизации, включая автоматизированные системы (АС) и приложения, используемые для выполнения бизнес-процессов и или технологических процессов, связанных с предоставлением финансовых и банковских услуг, а также услуг по осуществлению переводов денежных средств

- Область оценки соответствия должна совпадать с областью применения

  ГОСТ Р 57580.1

- Количество и выборку проверяемых подразделений, объектов информатизации, АС и средств вычислительной техники, входящих в область оценки соответствия, определяет аудитор самостоятельно с учетом предложений проверяемой организации

Положение о применимости

Технологии, не используемые в проверяемой организации

Нет необходимости для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей

Определены компенсирующие меры при невозможности технической реализации мер защиты информации и (или) в случае отсутствия экономической целесообразности

Свидетельства

Инструментальные средства сбора свидетельств полноты реализации мер защиты информации

Документы и иные материалы в бумажном или электронном виде относящиеся к обеспечению защиты информации

Устные высказывания сотрудников проверяемой организации в процессе интервьюирования

Результаты наблюдений аудиторов за процессами и деятельностью сотрудников

Параметры конфигураций и настроек технических объектов информатизации и средств защиты информации

Направления оценки соответствия

ГОСТ Р 57580.1, раздел 7 Система защиты информации

- процесс 1 «Обеспечение защиты информации при управлении доступом»
- процесс 2 «Обеспечение защиты вычислительных сетей»
- процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»
- процесс 4 «Защита от вредоносного кода»
- процесс 5 «Предотвращение утечек информации»
- процесс 6 «Управление инцидентами защиты информации»
- процесс 7 «Защита среды виртуализации»
- процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

ГОСТ Р 57580.1, раздел 8 Организация и управление защитой информации

ГОСТ Р 57580.1, раздел 9 Защита информации на этапах жизненного цикла

Направления оценки соответствия

ГОСТ Р 57580.1, раздел 7 Система защиты информации

ГОСТ Р 57580.1, раздел 8 Организация и управление защитой информации

- направление 1 «Планирование процесса системы защиты информации»
- направление 2 «Реализация процесса системы защиты информации»
- направление 3 «Контроль процесса системы защиты информации»
- направление 4 «Совершенствование процесса системы защиты информации»

ГОСТ Р 57580.1, раздел 9 Защита информации на этапах жизненного цикла

Направления оценки соответствия

ГОСТ Р 57580.1, раздел 7 Система защиты информации

ГОСТ Р 57580.1, раздел 8 Организация и управление защитой информации

ГОСТ Р 57580.1, раздел 9 Защита информации на этапах жизненного цикла

- Этап «Создания (модернизации)»
- Этап «Ввода в эксплуатацию»
- Этап «Эксплуатации (сопровождения)»
- Этап «Эксплуатации (сопровождения) и снятия с эксплуатации»

План

- [x] Выбор проверяющей организации
- [x] Область проверки
- [ ] Возможные результаты аудита
- [ ] Сроки прохождения аудита
- [ ] Рекомендации

Оценки

ГОСТ Р 57580.1, раздел 7 Система защиты информации

Емзи	Вербальный показатель
1	Мера выбрана (при предъявлении свидетельств выбора)
0	Мера не выбрана (при отсутствии свидетельств выбора)

ГОСТ Р 57580.1, раздел 8 Организация и управление защитой информации

Емоу	Вербальный показатель
1	Мера реализуется в полном объеме
0,5	Мера реализуется не в полном объеме
0	Мера полностью не реализуется

ГОСТ Р 57580.1, раздел 9 Защита информации на этапах жизненного цикла

Емас	Вербальный показатель
1	Мера на этапах жизненного цикла реализуется в полном объеме
0,5	Мера на этапах жизненного цикла реализуется не в полном объеме
0	Мера на этапах жизненного цикла полностью не реализуется

USSC

ГОСТ Р 57580.1, раздел 7 Система защиты информации

$$\text{Епзи}_i\ (\text{Еппзи}_i) = \frac{\sum_{j=1}^{N} \text{Емзи}_j}{N}$$

Оценки

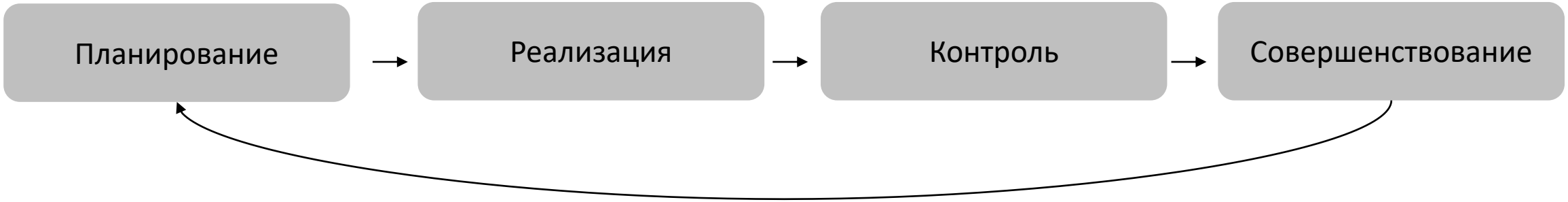
ГОСТ Р 57580.1, раздел 7 Система защиты информации

НАПРИМЕР

Наименование процесса системы ЗИ/направления ЗИ	Оценка, характеризующая выбор ОТМ системы ЗИ $Епзи_i$
Процесс 1 «Обеспечение ЗИ при управлении доступом»	0,57
Процесс 2 «Обеспечение защиты вычислительных сетей»	0,53
Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»	0,26
Процесс 4 «Защита от вредоносного кода»	0,81
Процесс 5 «Предотвращение утечек информации»	0,86
Процесс 6 «Управление инцидентами защиты информации»	0,29
Процесс 7 «Защита среды виртуализации»	0,68
Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»	0,70

ГОСТ Р 57580.1, раздел 8 Организация и управление защитой информации

$$Еп_i = \frac{\sum_{n=1}^{F} Емоу_n}{F} \qquad Ер_i = \frac{\sum_{j=1}^{P} Емоу_j}{P} \qquad Ек_i = \frac{\sum_{k=1}^{S} Емоу_k}{S} \qquad Ес_i = \frac{\sum_{m=1}^{Q} Емоу_m}{Q}$$



Оценки

ГОСТ Р 57580.1, раздел 8 Организация и управление защитой информации

НАПРИМЕР

Наименование процесса системы ЗИ/направления ЗИ	ЕПЗИi	Оценка по направлениям ЗИ системы			
		Планирование ЕПi	Реализация ЕРi	Контроль ЕКi	Совершенствование ЕСi
Процесс 1	0,57	0,60	0,95	0,79	1,00
Процесс 2	0,53	0,40	0,90	0,79	1,00
Процесс 3	0,26	0,40	0,90	0,79	1,00
Процесс 4	0,81	0,60	0,95	0,79	1,00
Процесс 5	0,86	0,30	0,90	0,79	1,00
Процесс 6	0,29	0,60	0,95	0,79	1,00
Процесс 7	0,68	0,20	0,90	0,79	1,00
Процесс 8	0,70	0,00	0,75	0,79	1,00

ГОСТ Р 57580.1, раздел 9 Защита информации на этапах жизненного цикла

$$E_{AC} = \frac{\sum_{j=1}^{L} Емас_j}{L}$$

Оценки

ГОСТ Р 57580.1, раздел 9 Защита информации на этапах жизненного цикла

НАПРИМЕР

Наименование процесса системы ЗИ/направления ЗИ	ЕПЗИi	Оценка по направлениям ЗИ системы			
		Планирование ЕПi	Реализация ЕРi	Контроль ЕКi	Совершенствование ЕСi
Процесс 1	0,57	0,60	0,95	0,79	1,00
Процесс 2	0,53	0,40	0,90	0,79	1,00
Процесс 3	0,26	0,40	0,90	0,79	1,00
Процесс 4	0,81	0,60	0,95	0,79	1,00
Процесс 5	0,86	0,30	0,90	0,79	1,00
Процесс 6	0,29	0,60	0,95	0,79	1,00
Процесс 7	0,68	0,20	0,90	0,79	1,00
Процесс 8	0,70	0,00	0,75	0,79	1,00
Применение организационных и технических мер защиты информации на этапах жизненного цикла					0,65

Оценка соответствия

$$E_i = \frac{Епзи_i + (0,2Еп_i + 0,4Ер_i + 0,25Ек_i + 0,15Ес_i)}{2}$$

$$R = \frac{\sum_{i=1}^{T} E_i + E_{AC}}{T + 1} - 0,01Z$$

Оценка процесса (итоговая оценка)	Уровень соответствия
E (R) = 0	Нулевой
0 < E (R) <= 0,5	Первый
0,5 < E (R) <= 0,7	Второй
0,7 < E (R) <= 0,85	Третий
0,85 < E (R) <= 0,9	Четвертый
0,9 < E (R) <= 1	Пятый

Оценка соответствия

НАПРИМЕР

Наименование процесса системы ЗИ/направления ЗИ	ЕПЗИi	Оценка по направлениям ЗИ системы				Качественная оценка уровня соответствия процесса	Числовое значение оценки соответствия процесса системы ЗИ Ei
		ЕПi	ЕРi	ЕКi	ЕСi		
Процесс 1	0,57	0,60	0,95	0,79	1,00	третий	0,71
Процесс 2	0,53	0,40	0,90	0,79	1,00	второй	0,66
Процесс 3	0,26	0,40	0,90	0,79	1,00	второй	0,52
Процесс 4	0,81	0,60	0,95	0,79	1,00	третий	0,83
Процесс 5	0,86	0,30	0,90	0,79	1,00	третий	0,81
Процесс 6	0,29	0,60	0,95	0,79	1,00	второй	0,57
Процесс 7	0,68	0,20	0,90	0,79	1,00	третий	0,71
Процесс 8	0,70	0,00	0,75	0,79	1,00	второй	0,67
Применение организационных и технических мер защиты информации на этапах жизненного цикла							0,65
Количество выявленных нарушений, Z							2
Итоговая оценка соответствия, R							0,66

Основные нарушения

- Осуществление логического доступа под учетными записями неопределенного целевого назначения
- Осуществление логического доступа под коллективными неперсонифицированными учетными записями
- Наличие незаблокированных учетных записей уволенных работников
- Отсутствие разграничения логического доступа
- Несанкционированное предоставление пользователям административных прав
- Несанкционированное предоставление пользователям прав логического доступа
- Хранение паролей субъектов доступа в открытом виде
- Передача аутентификационных данных в открытом виде по каналам и линиям связи
- Отсутствие регистрации персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации
- Отсутствие разграничения физического доступа в помещения, в которых расположены объекты доступа
- Несанкционированный физический доступ посторонних лиц в помещения, в которых расположены объекты доступа
- Отсутствие логической сетевой изоляции внутренних вычислительных сетей и сети Интернет и/или беспроводных сетей
- Передача информации конфиденциального характера с использованием сети Интернет, телекоммуникационных каналов и/или линий связи, не контролируемых проверяемой организацией, в открытом виде
- Наличие в контролируемой зоне финансовой организации незарегистрированных точек беспроводного доступа, имеющих подключение к локальной вычислительной сети финансовой организации
- Использование нелицензионного ПО
- Отсутствие применения средств защиты от воздействия вредоносного кода
- Обработка информации конфиденциального характера с использованием неучтенных МНИ
- Отсутствие гарантированного стирания информации конфиденциального характера с МНИ
- Отсутствие реагирования на инциденты

Что вы получаете на выходе?

- Отчет об аудите
- Числовые оценки соответствия с их обоснованием
- Заполненные листы сбора свидетельств
- Перечень выявленных нарушений
- Рекомендации по совершенствованию
- Копии документов на бумажных носителях, машинные носители информации с информацией, предоставляемой в качестве свидетельств проверяемой организацией

План

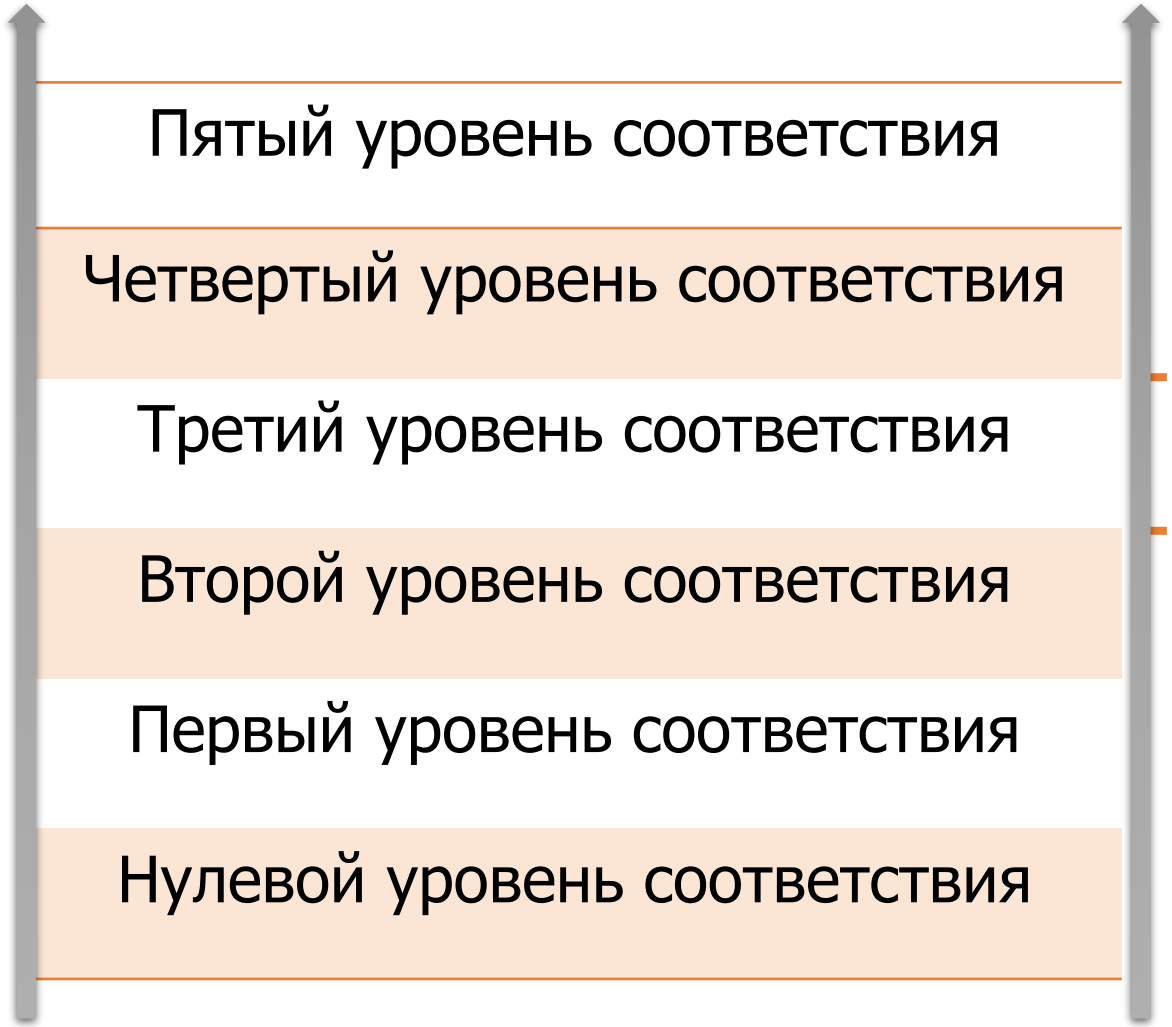
- [x] Выбор проверяющей организации
- [x] Область проверки
- [x] Возможные результаты аудита
- [ ] Сроки прохождения аудита
- [ ] Рекомендации

Когда необходимо провести аудит?

USSC

683-П	Все кредитные финансовые организации	Реализация усиленного или стандартного уровня защиты Проведение оценки соответствия уровню защиты Обеспечить уровень соответствия не ниже третьего Обеспечить уровень соответствия не ниже четвертого	с 01.01.2021 с 01.01.2023
684-П	Некредитные финансовые организации	Реализация усиленного или стандартного уровня защиты Проведение оценки соответствия уровню защиты Обеспечить уровень соответствия не ниже третьего Обеспечить уровень соответствия не ниже четвертого	с 01.01.2021 с 01.01.2022 с 01.07.2023
672-П	Участники платежной системы Банка России	Реализация усиленного или стандартного уровня защиты Проведение оценки соответствия уровню защиты Обеспечить уровень соответствия не ниже четвертого	с 06.04.2019 с 01.07.2021 с 01.01.2023

Когда необходимо провести аудит?



	683-П	684-П	672-П
> 0,85	к 01.01.2023	к 01.07.2023	к 01.01.2023
> 0,7	к 01.01.2021	к 01.01.2022	

Временные затраты

Очное обследование
Производится сбор информации о действующей IT-структуре, интервьюирование работников, анализируется выполнение ГОСТ Р 57580.1

Согласование
Согласование результатов оценки соответствия с проверяемой организацией

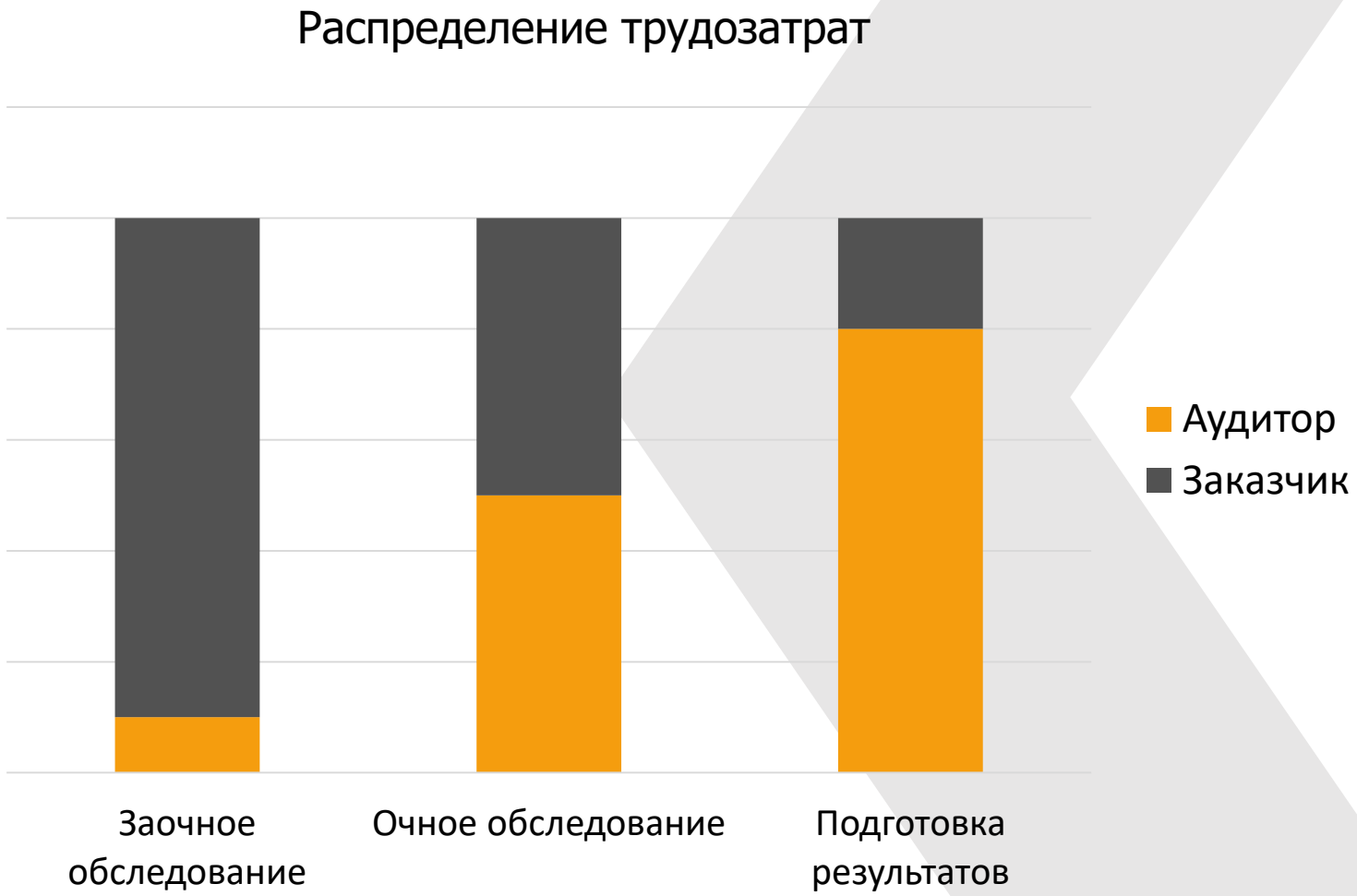
Заочное обследование
Подготовка, заполнение опросных листов, анализ исходных данных

Формирование отчета и свидетельств
Подготавливается отчет по форме ГОСТ Р 57580.2-2018, разрабатываются рекомендации по приведению в соответствие, заполняются листы сбора свидетельств

Хранение отчета проверяемой организацией*

Ресурсные затраты

- Представители ИТ-подразделения
- Представители ИБ-подразделения
- Владельцы систем



План

- [x] Выбор проверяющей организации
- [x] Область проверки
- [x] Возможные результаты аудита
- [x] Сроки прохождения аудита
- [ ] Рекомендации

Как подготовиться к аудиту?

USSC

Разработать модель угроз и нарушителя, определить контуры безопасности

Провести самооценку и GAP-анализ

Сформировать «положение о применимости»

Разработать ОРД, «донастроить» встроенные средства защиты

Провести инвентаризацию объектов информатизации и АС, входящих в область оценки

Подготовить сотрудников к возможному интервьюированию, ознакомить с внутренними ОРД

Чем можно руководствоваться?

USSC

НАПРИМЕР

- Рекомендации Банка России СТО БР ИББС
- Рекомендации в информационных письмах Банка России
- Методики ФСТЭК России
- Вендоры подготовили таблицы с описанием своих средств защиты информации и их соответствия мерам ГОСТ Р 57580.1
- Серия вебинаров УЦСБ «Безопасность финансовых организаций»

Варианты проведения аудита

1. Предварительная оценка соответствия требованиям ГОСТ Р 57580.1 (без оформления опросных листов и свидетельств аудита в соответствии с ГОСТ Р 57580.2)

2. Оценка соответствия требованиям ГОСТ Р 57580.1-2017 (с оформлением опросных листов и свидетельств аудита в соответствии с ГОСТ Р 57580.2)

3* Дистанционная оценка соответствия требованиям ГОСТ Р 57580.1 с использованием онлайн-сервиса в соответствии с методологией ГОСТ Р 57580.2 (без выезда аудиторов на объекты проверяемой организации с дистанционной проверкой предоставленных свидетельств аудита)

План

- [x] Выбор проверяющей организации
- [x] Область проверки
- [x] Возможные результаты аудита
- [x] Сроки прохождения аудита
- [x] Рекомендации

Наши предложения для финансовых организаций

USSC

Оценка соответствия требованиям ГОСТ Р 57580

Тестирование на проникновение

Анализ уязвимостей по ОУД

Онлайн-сервис дистанционной оценки соответствия ГОСТ Р 57580

Комплексные аудиты

Предварительный аудит и приведение в соответствие с требованиями регуляторов

О компании

Опыт

Специалисты компании УЦСБ выполняют проекты в области информационной безопасности более 10 лет

Сертификации

Проектная команда - сотрудники с высшим профессиональным образованием по направлению подготовки 090100 «Информационная безопасность», имеющие сертификаты:

- Certified Information Systems Auditor (CISA);
- Certified Information Systems Security Professional (CISSP);
- Certified Information Security Manager (CISM);
- Cisco Certified Internetwork Expert (CCIE);
- Ethical Hacking and Penetration Testing (CEH);
- Computer Hacking Forensic Investigator (CHFI);
- Offensive Security Certified Professional (OSCP);
- Offensive Security Certified Expert (OSCE)

О компании

Уральский центр систем безопасности (УЦСБ) – компания-эксперт в области безопасного использования информационных технологий. С 2007 года компания непрерывно развивается, наращивает компетенции и выполняет все более сложные проекты.

Компетенции

- **Информационные технологии**
- **Комплексы инженерно-технических средств охраны**
- **Анализ защищенности**
- **Сервисное обслуживание**
- **Информационная безопасность**
- **Информационные инфраструктуры**
- **Безопасность промышленных систем автоматизации и управления**

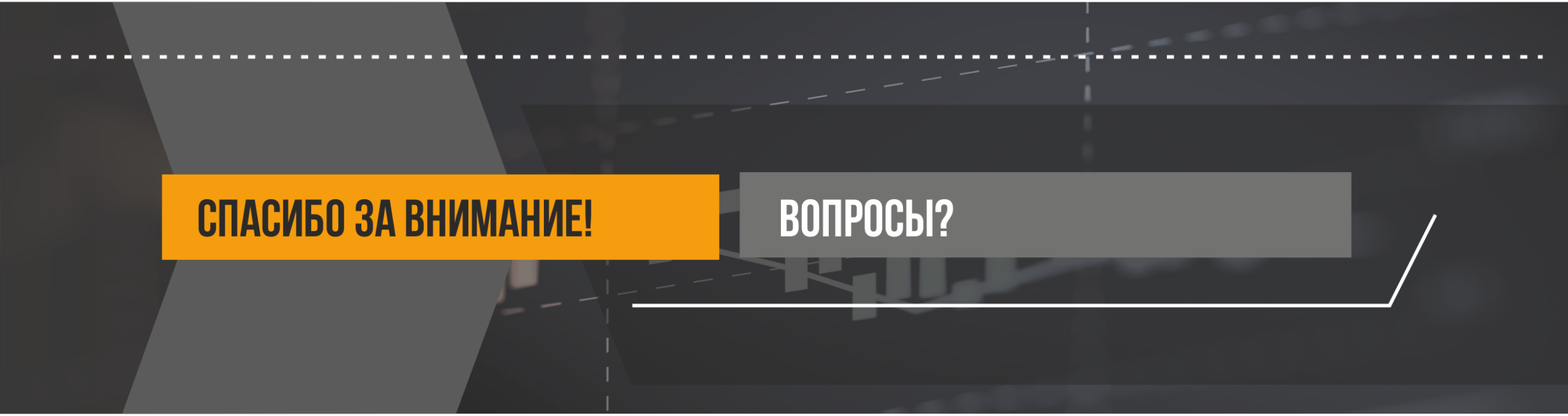
USSC.RU

620100, г. Екатеринбург, ул. Ткачей, д. 6
620100, г. Екатеринбург, ул. Ткачей, д. 23

Тел.: +7 (343) 379-98-34,
e-mail: info@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

USSC



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Борисов Сергей

Обособленное подразделение в г. Краснодар

sborisov@ussc.ru

Заведенская Анастасия

Аналитический центр

azavedenskaya@ussc.ru