USSC

Онлайн-сервис оценки соответствия требованиям ГОСТ Р 57580

Диана Лейчук
Анастасия Краснова

План

1. Кратко об оценке соответствия по ГОСТ Р 57580
2. Варианты проведения оценки соответствия
3. Демонстрация онлайн-сервиса

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 (683-П, 684-П, 672-П)
- повышения уровня защищенности информации

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

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?

USSC

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

Когда необходимо провести аудит?

		683-П	684-П	672-П
Пятый уровень соответствия				
Четвертый уровень соответствия	≥ 0,85	к 01.01.2023	к 01.07.2023	к 01.01.2023
Третий уровень соответствия	≥ 0,7	к 01.01.2021	к 01.01.2022	
Второй уровень соответствия				
Первый уровень соответствия				
Нулевой уровень соответствия				

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)»

Направления оценки соответствия

ГОСТ Р 57580.1, раздел 7 Система защиты информации

341 мера

ГОСТ Р 57580.1, раздел 8
Организация и управление защитой информации

37 мер (оценка по каждому из процессов из раздела 7)

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

28 мер

---

406 мер

План

1. Кратко об оценке соответствия по ГОСТ Р 57580
2. Варианты проведения оценки соответствия
3. Демонстрация онлайн-сервиса

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)

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)

Методы проведения аудита

ГОСТ Р ИСО 19011-2012

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

Методы проведения аудита

ГОСТ Р ИСО 19011-2012

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

Временные затраты (очный аудит)

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

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*

Заочное обследование
Подготовка, заполнение опросных листов, анализ исходных данных

Устранение несоответствий
«донастройка» средств защиты, сбор дополнительных свидетельств, внедрение организационных мер

Согласование
Согласование результатов оценки соответствия с проверяемой организацией

Временные затраты (дистанционный аудит)

Заочное обследование
Производится анализ предоставленной информации, интервьюирование работников, анализируется выполнение ГОСТ Р 57580.1

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

Хранение отчета проверяемой организацией*

Сбор и заполнение данных*
Подготовка, заполнение опросных листов

Устранение несоответствий
«донастройка» средств защиты, сбор дополнительных свидетельств, внедрение организационных мер

Согласование*
Согласование результатов оценки соответствия с проверяемой организацией

* выполняется представителями проверяемой организации

Свидетельства

- 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
- Инструментальные средства сбора свидетельств полноты реализации мер защиты информации

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
- Возможность использовать результаты аудита для подготовки к дальнейшим оценкам соответствия

План

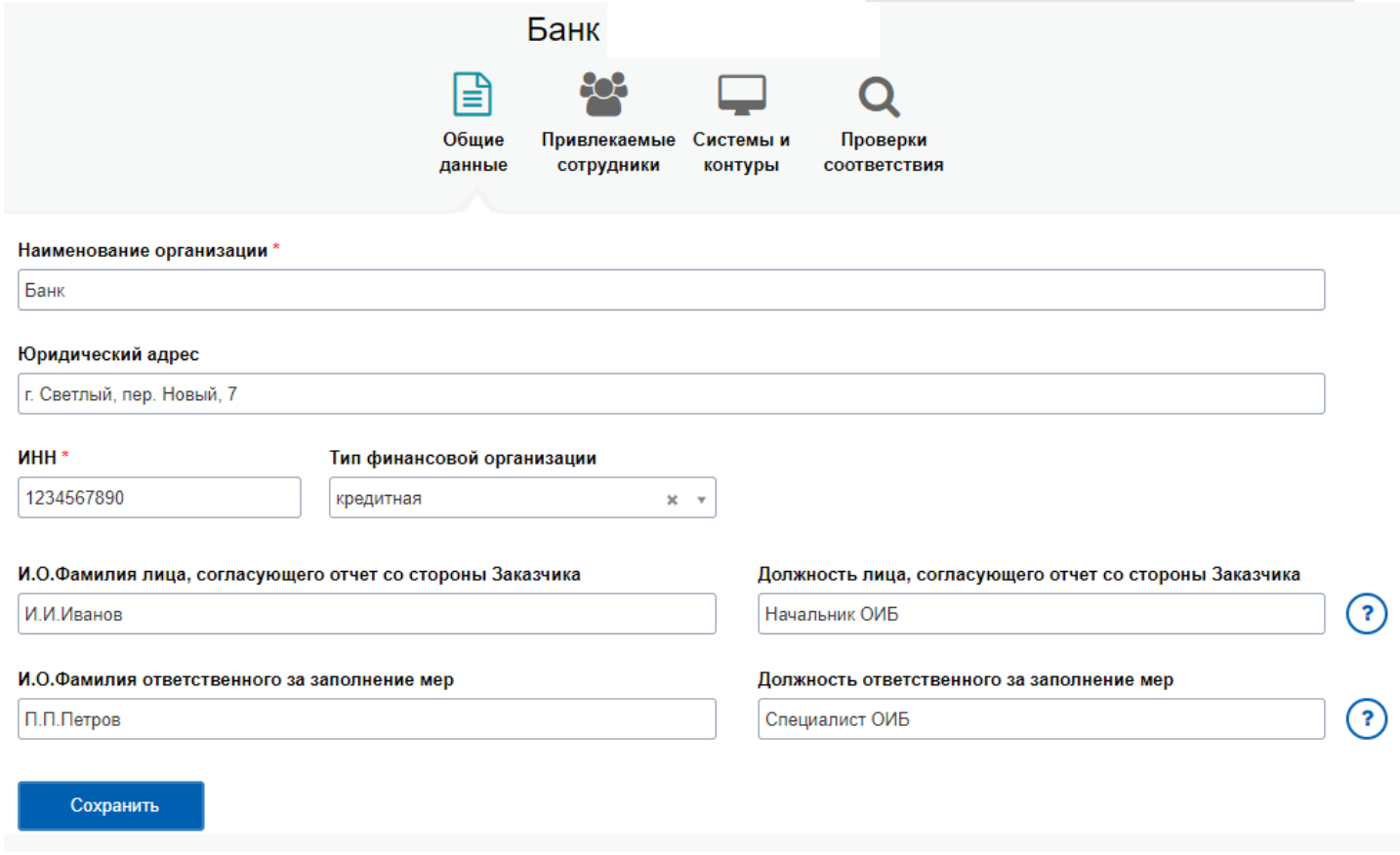
1. Кратко об оценке соответствия по ГОСТ Р 57580
2. Варианты проведения оценки соответствия
3. Демонстрация онлайн-сервиса

Этапы работы в онлайн-сервисе

1. Работа Заказчика в онлайн-сервисе
2. Работа аудитора в онлайн-сервисе
3. Согласование результатов аудита Заказчиком
4. Вывод итоговых документов в бумажном виде

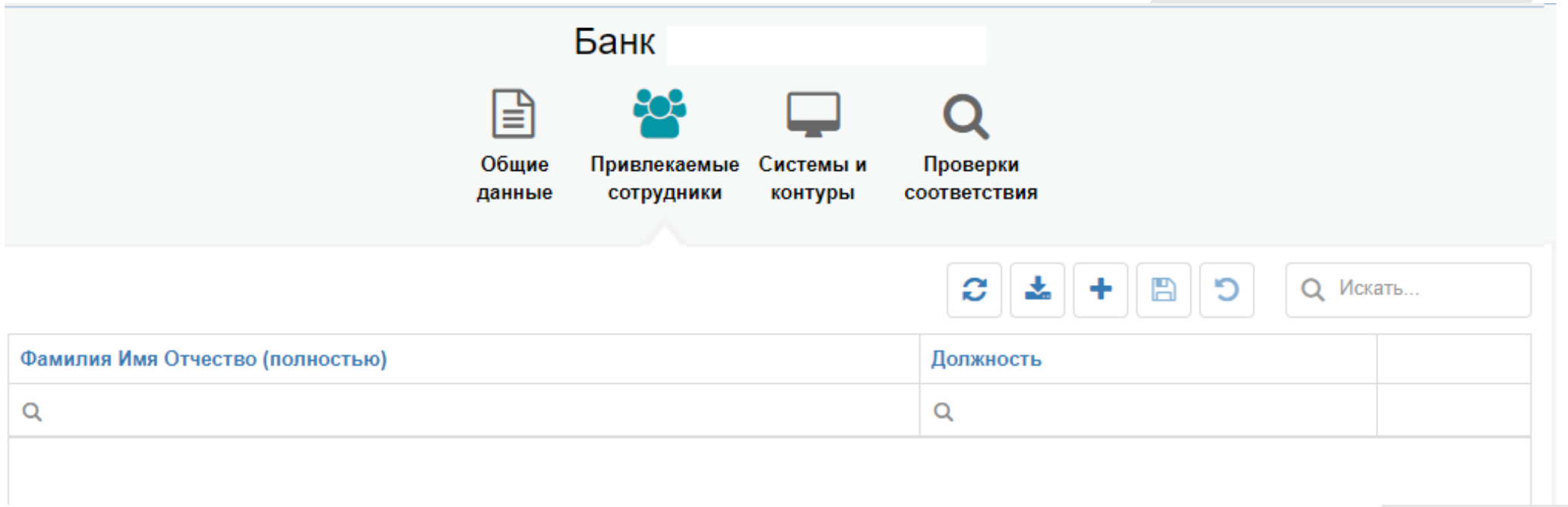
Работа представителя Заказчика в сервисе

1. Создание и заполнение карточки организации - общей информации:
   - об организации
   - привлекаемых сотрудниках – согласующих лицах
   - перечень систем
   - уровень защиты информации



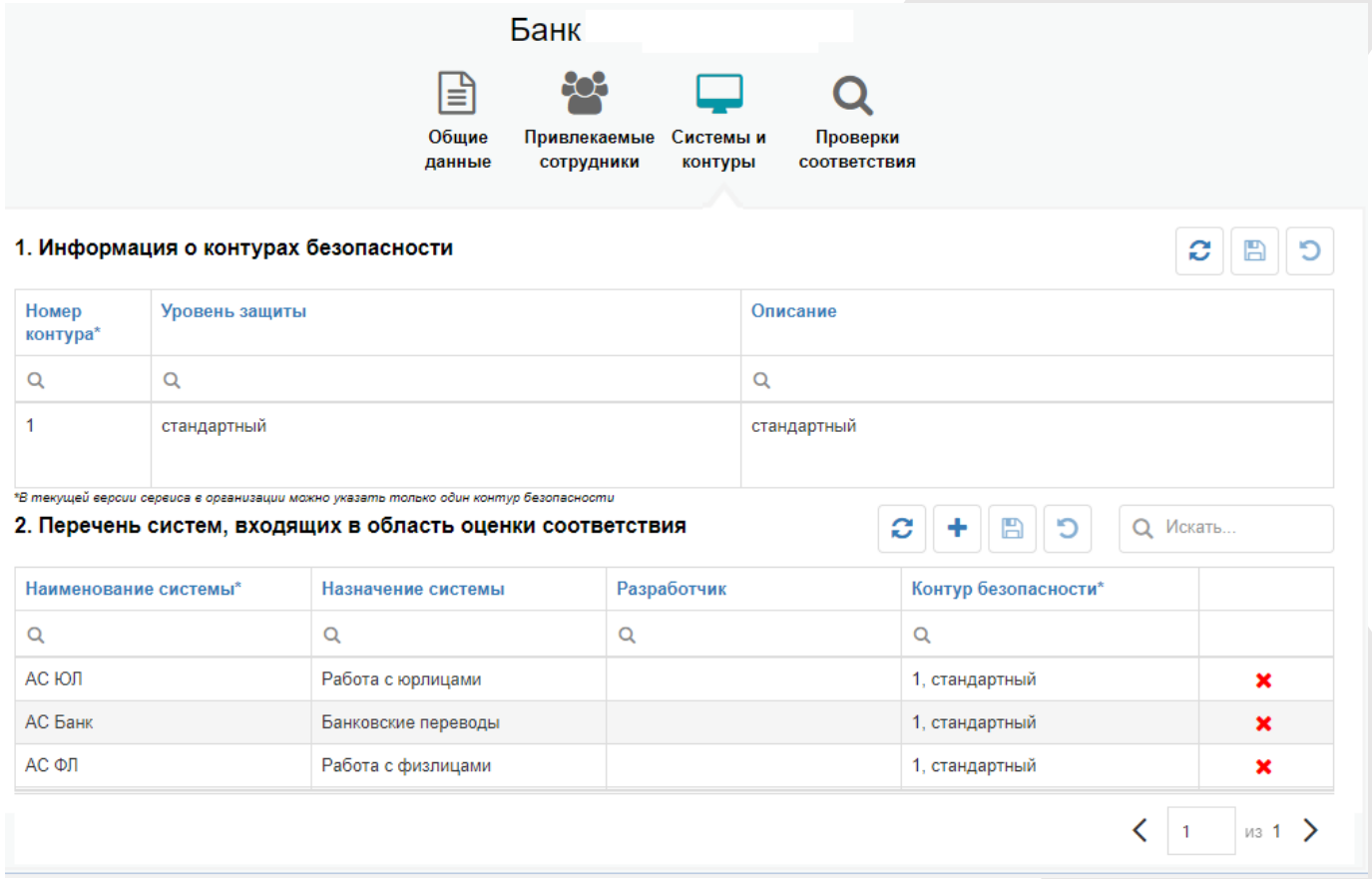
Работа представителя Заказчика в сервисе

1. Создание и заполнение карточки организации - общей информации:
   - об организации
   - привлекаемых сотрудниках – согласующих лицах
   - перечень систем
   - уровень защиты информации



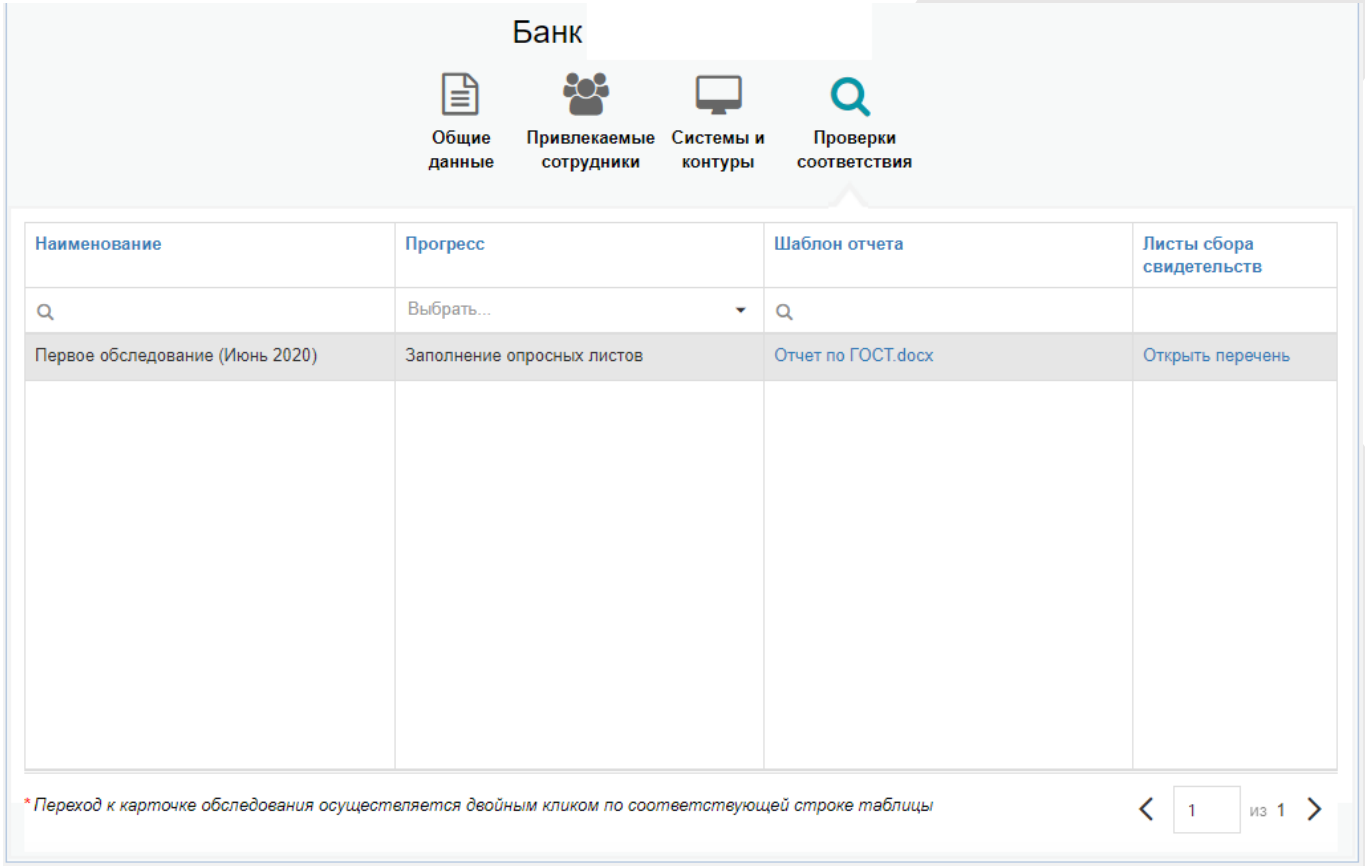
Работа представителя Заказчика в сервисе

1. Создание и заполнение карточки организации - общей информации:
   - об организации
   - привлекаемых сотрудниках – согласующих лицах
   - перечень систем
   - уровень защиты информации



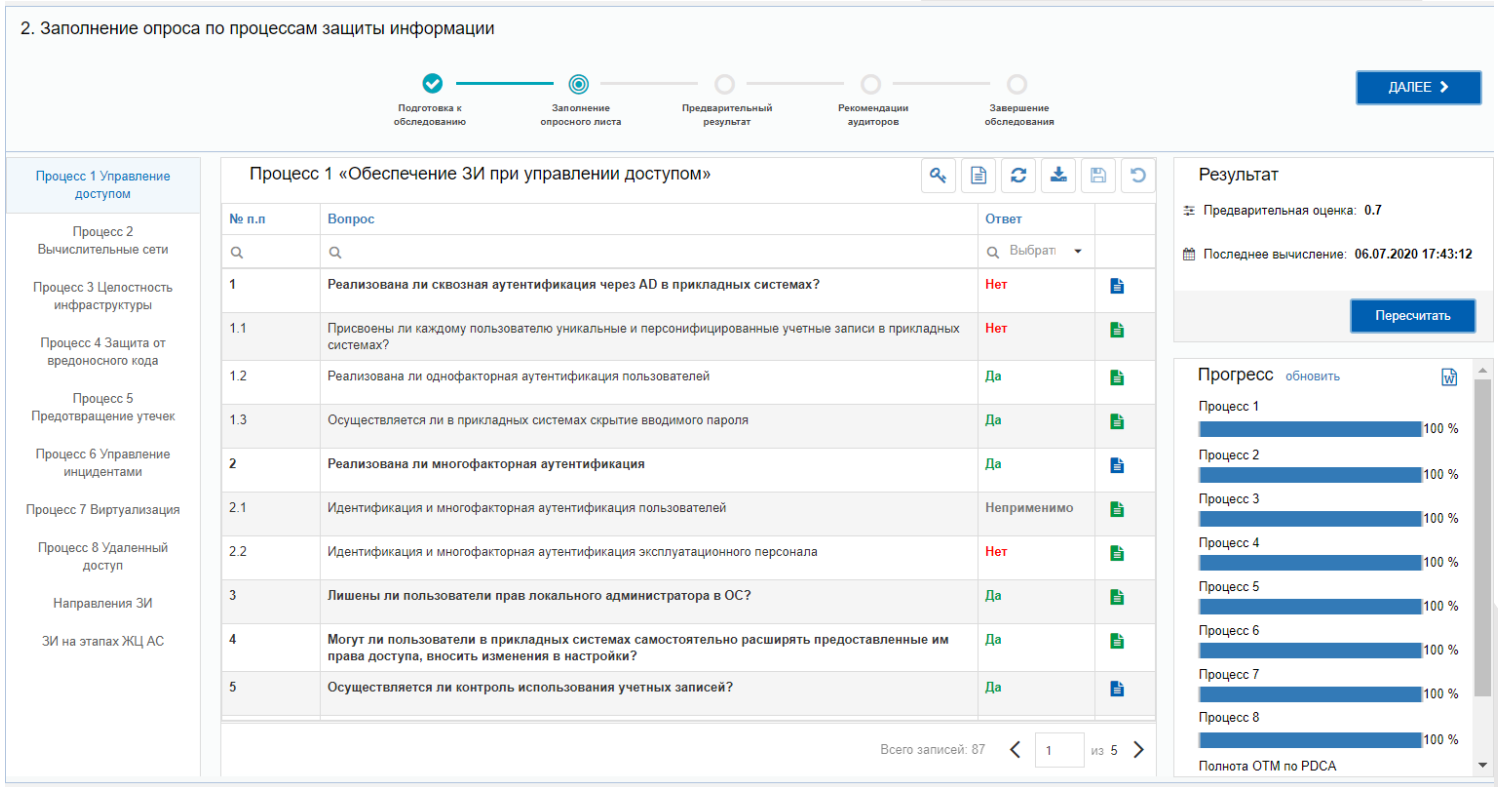
Работа представителя Заказчика в сервисе

1. Создание и заполнение карточки организации
2. Создание и заполнение карточки обследования:
   - заполнение вопросов-фильтров
   - заполнение реализации мер из ГОСТ Р 57580.1-2017
   - прикрепление свидетельств



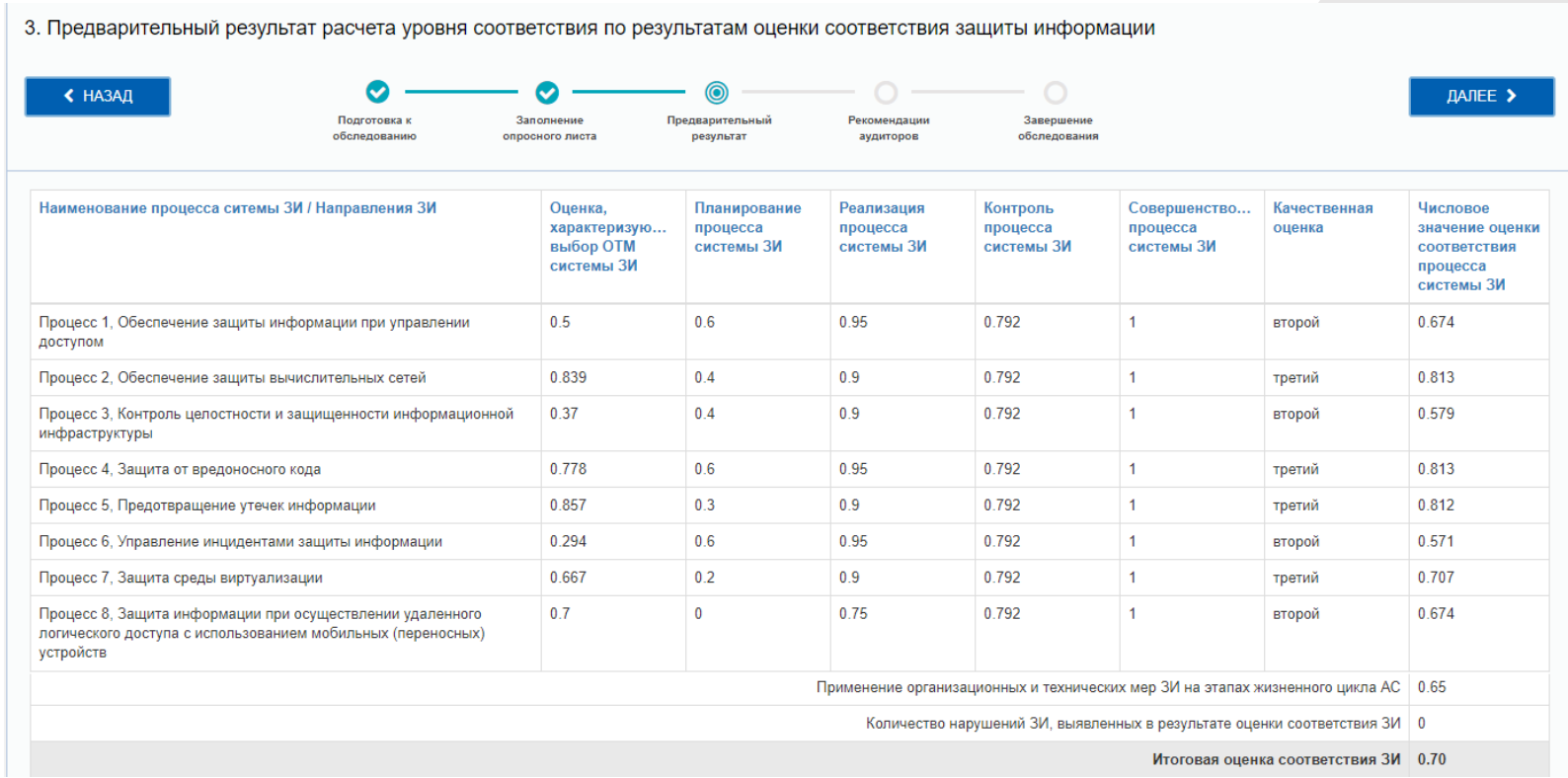
Работа представителя Заказчика в сервисе

1. Заполнение карточки организации
2. Заполнение карточки обследования:
   - заполнение вопросов-фильтров
   - заполнение реализации мер из ГОСТ Р 57580.1-2017
   - прикрепление свидетельств



Работа представителя Заказчика в сервисе

1. Заполнение карточки организации
2. Заполнение карточки обследования
3. Просмотр предварительного результата и отчетных документов



3. Предварительный результат расчета уровня соответствия по результатам оценки соответствия защиты информации

НАЗАД

Подготовка к обследованию — Заполнение опросного листа — Предварительный результат — Рекомендации аудиторов — Завершение обследования

ДАЛЕЕ

Наименование процесса ситемы ЗИ / Направления ЗИ	Оценка, характеризую... выбор ОТМ системы ЗИ	Планирование процесса системы ЗИ	Реализация процесса системы ЗИ	Контроль процесса системы ЗИ	Совершенство... процесса системы ЗИ	Качественная оценка	Числовое значение оценки соответствия процесса системы ЗИ
Процесс 1, Обеспечение защиты информации при управлении доступом	0.5	0.6	0.95	0.792	1	второй	0.674
Процесс 2, Обеспечение защиты вычислительных сетей	0.839	0.4	0.9	0.792	1	третий	0.813
Процесс 3, Контроль целостности и защищенности информационной инфраструктуры	0.37	0.4	0.9	0.792	1	второй	0.579
Процесс 4, Защита от вредоносного кода	0.778	0.6	0.95	0.792	1	третий	0.813
Процесс 5, Предотвращение утечек информации	0.857	0.3	0.9	0.792	1	третий	0.812
Процесс 6, Управление инцидентами защиты информации	0.294	0.6	0.95	0.792	1	второй	0.571
Процесс 7, Защита среды виртуализации	0.667	0.2	0.9	0.792	1	третий	0.707
Процесс 8, Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств	0.7	0	0.75	0.792	1	второй	0.674
						Применение организационных и технических мер ЗИ на этапах жизненного цикла АС	0.65
						Количество нарушений ЗИ, выявленных в результате оценки соответствия ЗИ	0
						Итоговая оценка соответствия ЗИ	**0.70**

Работа представителя Заказчика в сервисе

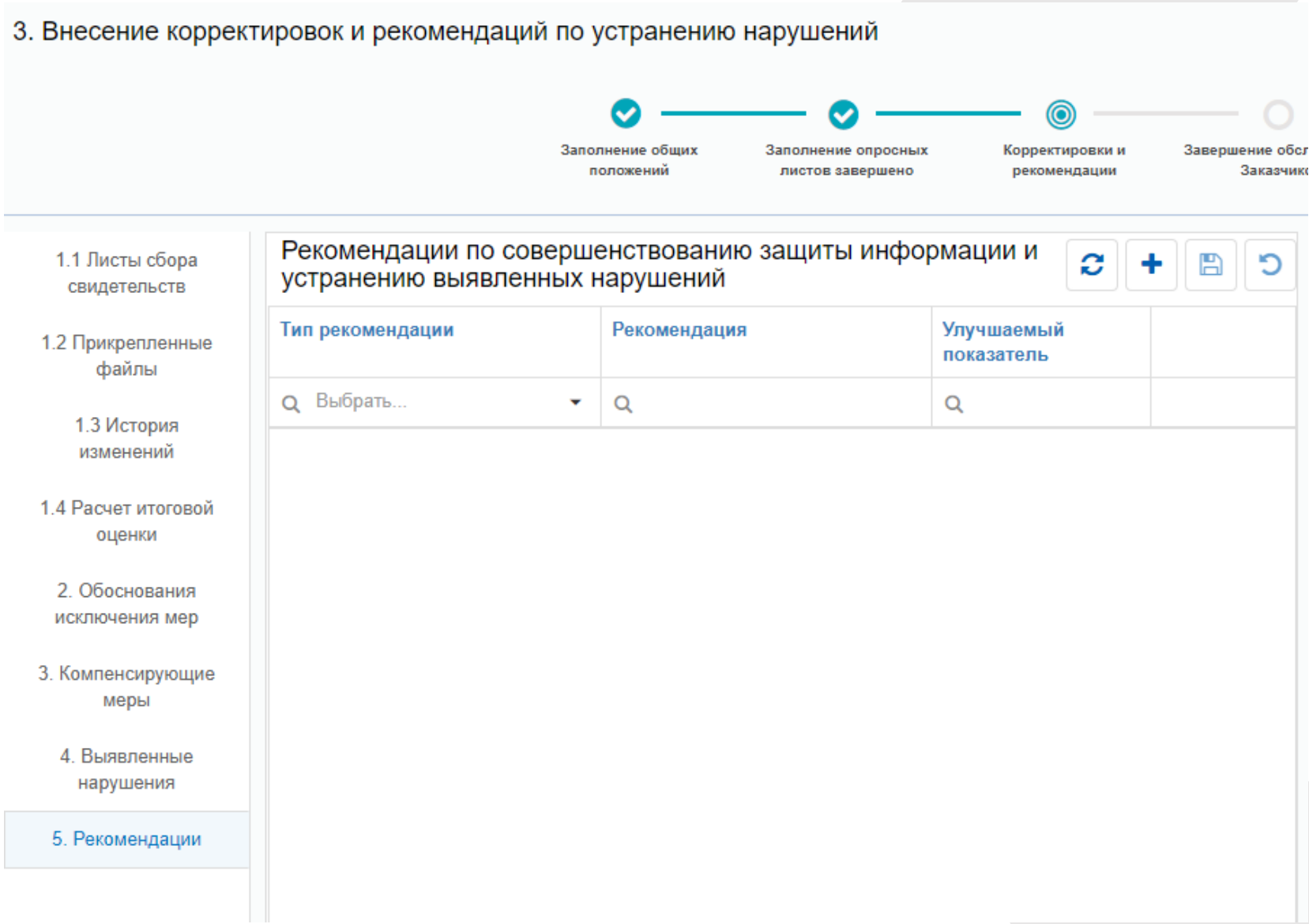
1. Заполнение карточки организации
2. Заполнение карточки обследования
3. Просмотр предварительного результата
4. Отправка на проверку аудитору

Этапы работы в онлайн-сервисе

1. Работа Заказчика в онлайн-сервисе
2. Работа аудитора в онлайн-сервисе
3. Согласование результатов аудита Заказчиком
4. Распечатка итоговых документов в бумажном виде

Работа аудитора в сервисе

- проверка собранной информации
- корректировка числовых оценок/ свидетельств/ описания реализации мер

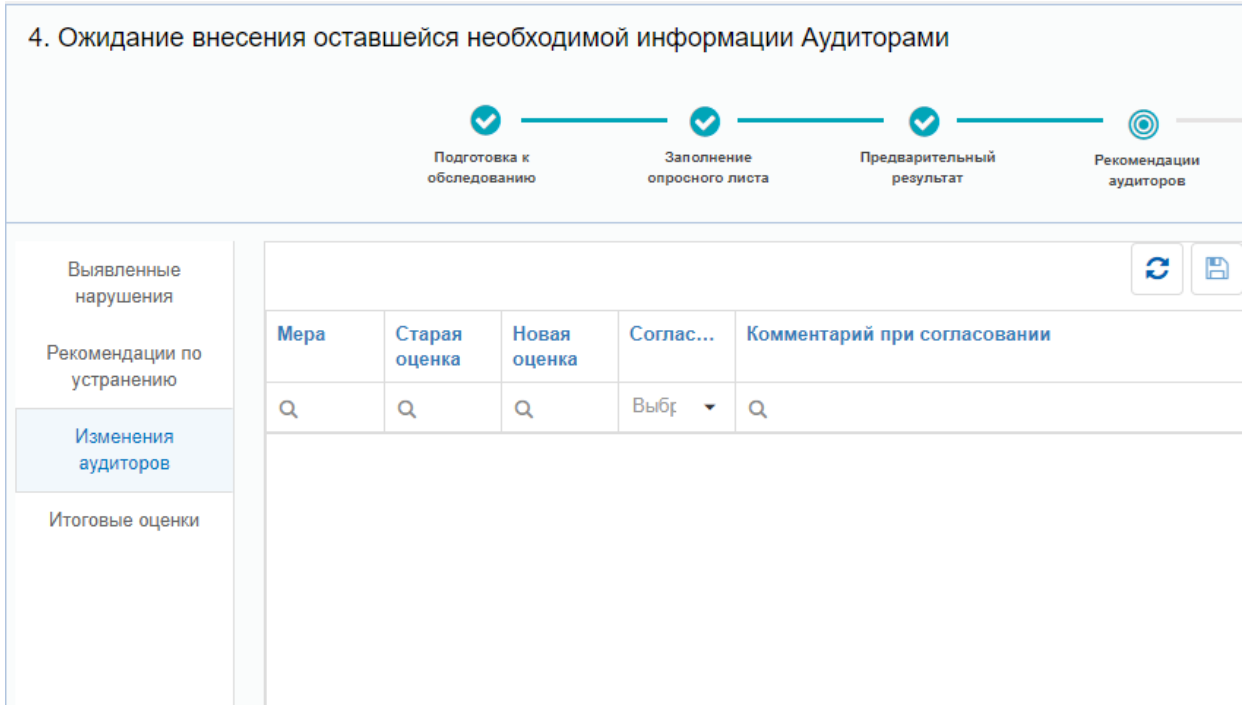


Этапы работы в онлайн-сервисе

1. Работа Заказчика в онлайн-сервисе
2. Работа аудитора в онлайн-сервисе
3. Согласование результатов аудита Заказчиком
4. Распечатка итоговых документов в бумажном виде

Согласование результатов аудита Заказчиком

- Возможность отслеживания изменений
- Итоговые оценки
- Рекомендации по повышению уровня соответствия
- Итоговые листы сбора свидетельств



Листы сбора свидетельств

Наименование	Файл для скачивания
Лист УПД	Листы сбора свидетельств оцен...
Лист ВС	Листы сбора свидетельств оцен...
Лист КЦ	Листы сбора свидетельств оцен...
Лист АВЗ	Листы сбора свидетельств оцен...
Лист ПУИ	Листы сбора свидетельств оцен...
Лист ИНЦ	Листы сбора свидетельств оцен...
Лист ЗСВ	Листы сбора свидетельств оцен...
Лист УД	Листы сбора свидетельств оцен...
Лист Полнота ОТМ по PDCA	Лист сбора свидетельств направ...
Лист ЗИ на этапах ЖЦ АС	Лист сбора свидетельств мер З...

Этапы работы в онлайн-сервисе

1. Работа Заказчика в онлайн-сервисе
2. Работа аудитора в онлайн-сервисе
3. Согласование результатов аудита Заказчиком
4. Распечатка итоговых документов в бумажном виде

Варианты предоставления онлайн-сервиса

Сервис для предварительной самостоятельной оценки

Сервис для проведения дистанционного аудита

Преимущества онлайн-сервиса

- возможность проведения предварительной самооценки
- консультации по вопросам
- дистанционная проверка аудиторами
- упрощение процедуры проведения последующих проверок

Контакты для запроса демо-доступа

Руководитель отдела продаж продуктов разработки

Бочкарев Вадим Викторович


vbochkarev@ussc.ru


+7 (343) 379-98-34 (вн. 1585)


+79120429798

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**

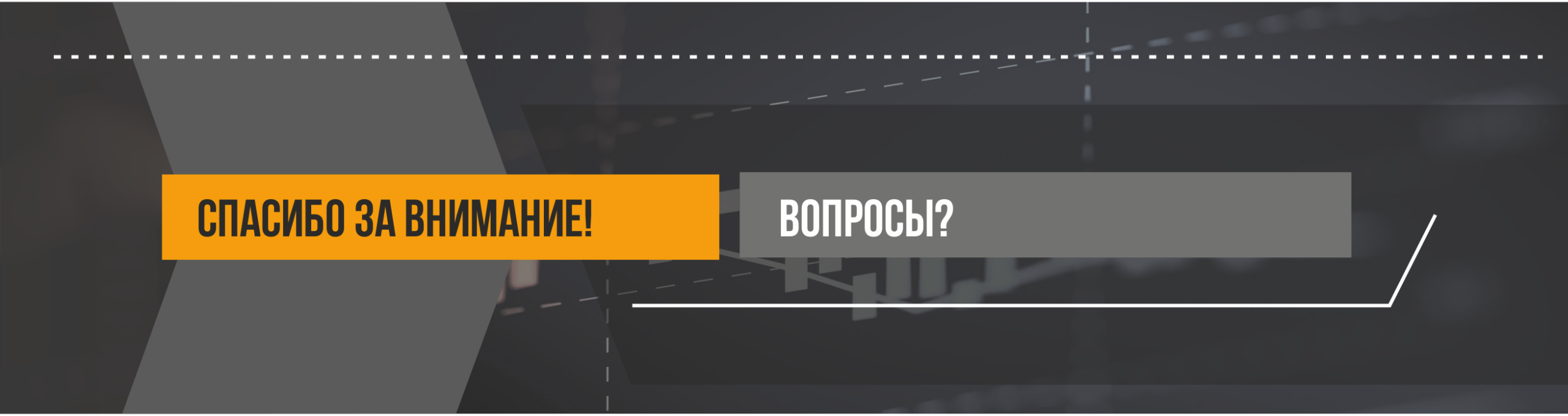
USSC.RU

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

Лейчук Диана

Аналитический центр

dleichuk@ussc.ru

Краснова Анастасия

Отдел разработки специального ПО

akrasnova@ussc.ru