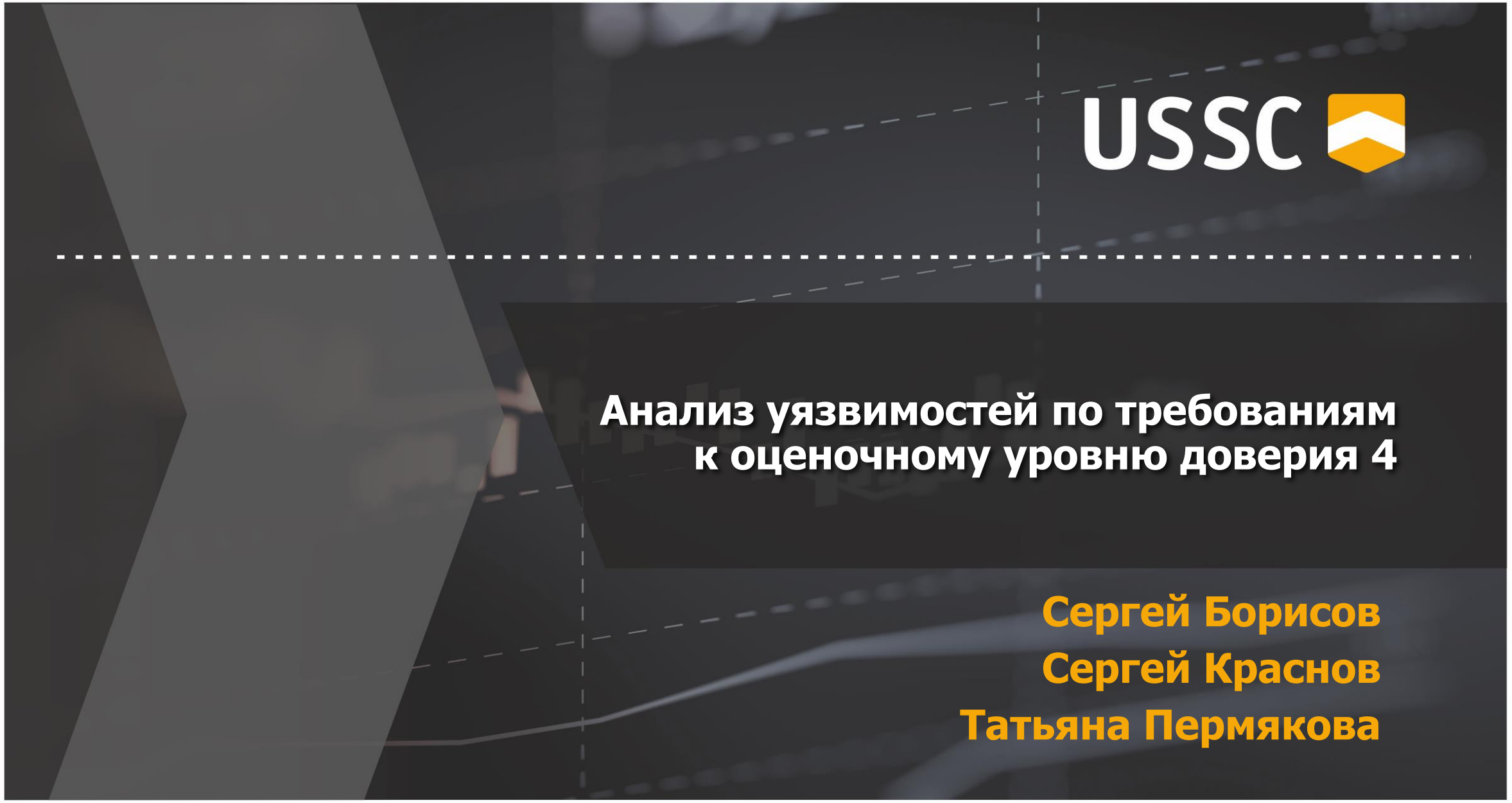


Анализ уязвимостей по требованиям к оценочному уровню доверия 4

Сергей Борисов
Сергей Краснов
Татьяна Пермякова

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?
6	15.07	Пентесты для финансовых организаций
7	19.08	Биометрия в финансовых организациях
8	16.09	Требования к средствам криптографической защиты информации в финансовых организациях
9		Онлайн-сервис оценки соответствия ГОСТ Р 57580.2-2018

Ведущие третьего выпуска

Сергей Борисов

Заместитель руководителя по ИБ

обособленного подразделения УЦСБ

г. Краснодар

Сергей Краснов

Руководитель направления Анализа защищенности

Аналитический центр УЦСБ

г. Екатеринбург

CEH, CHFI

Татьяна Пермякова

Аналитик

Аналитический центр УЦСБ

г. Екатеринбург

Блог: https://sborisov.blogspot.com

План

- [ ] Обзор нормативных требований
- [ ] Исходные данные для проведения оценки
- [ ] Основные этапы и методы оценки
- [ ] Описание результатов проведения оценки

План

- [ ] Обзор нормативных требований
- [ ] Исходные данные для проведения оценки
- [ ] Основные этапы и методы оценки
- [ ] Описание результатов проведения оценки

Требования положений Банка России

382-П	Операторы по переводу денежных средств Операторы услуг платежной инфраструктуры Операторы услуг информационного обмена	Сертифицированное прикладное ПО или ПО, в отношении которого проведен анализ уязвимостей к ОУД4	с 01.01.2020
683-П	Все кредитные финансовые организации	Сертифицированное прикладное ПО или ПО, в отношении которого проведен анализ уязвимостей к ОУД4	с 01.01.2020
684-П	Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации	Сертифицированное прикладное ПО или ПО, в отношении которого проведен анализ уязвимостей к ОУД4	с 01.01.2020
672-П	Участники платежной системы Банка России	Уровень защиты информации по ГОСТ Р 57580.1-2017: • стандартный (уровень 2) для участников СБП • усиленный (уровень 1) для ОПКЦ	с 01.07.2021 с 06.04.2019

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017
Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

	Мера СЗИ	Уровень защиты информации		
		3	2	1
ЖЦ.8	Применение прикладного ПО АС, сертифицированного на соответствие требованиям по безопасности информации, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3	Н	О	О

Необходимость проведения анализа уязвимостей

USSC

Прикладное ПО и приложения, распространяемое клиентам для осуществления банковских операций

Прикладное ПО и приложения, обрабатывающие защищаемую информацию при приеме электронных сообщений к исполнению с использованием сети Интернет

Проведение анализа уязвимостей необходимо:

- **для каждого обновления ПО**
  (или в отношении всего процесса разработки ПО для релизов, затрагивающих существенные изменения в части функционирования ядра, обеспечения ИБ)
- **не менее 1 раза в год**
  в соответствии с ГОСТ Р 57580.1-2017 (п 9.7 ЖЦ.20)

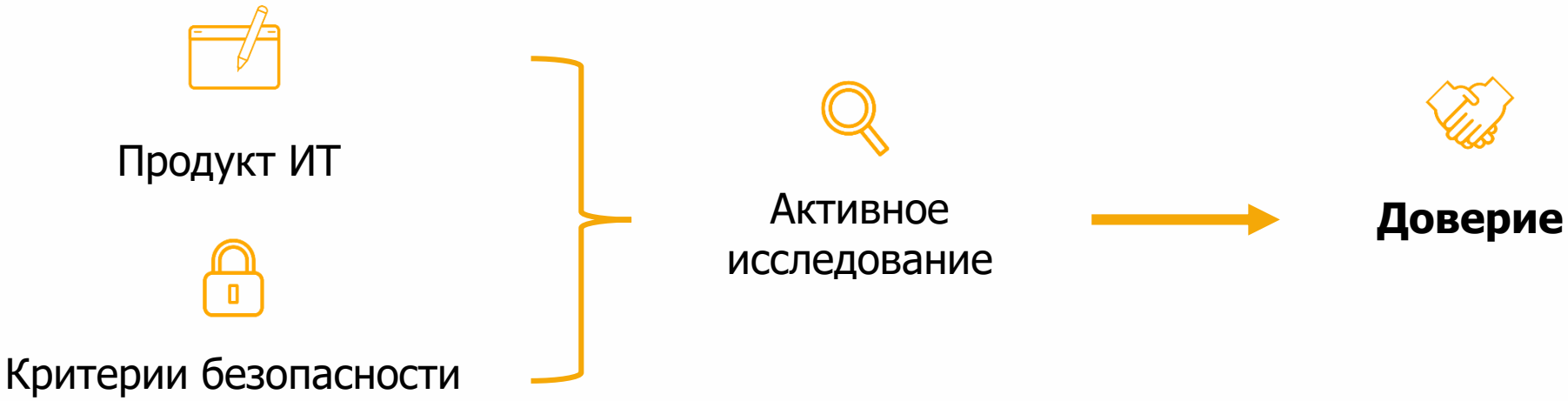
Критерии и методология оценки

ГОСТ Р ИСО/МЭК 15408-3

Информационная технология.
Методы и средства обеспечения безопасности.
Критерии оценки безопасности информационных технологий.
Часть 3. Компоненты доверия к безопасности

ГОСТ Р ИСО/МЭК 18045-2013

Информационная технология.
Методы и средства обеспечения безопасности.
Методология оценки безопасности информационных технологий



Анализ уязвимостей представляет собой оценку с целью сделать заключение, могут ли потенциальные уязвимости позволить нарушителям нарушить функциональные требования безопасности

План

- [x] Обзор нормативных требований
- [ ] Исходные данные для проведения оценки
- [ ] Основные этапы и методы оценки
- [ ] Описание результатов проведения оценки

Исходные данные

Описание архитектуры безопасности

Обоснование безопасности процесса инициализации и невозможности обхода ФБО, обеспечения собственной защиты объекта оценки от вмешательства

Функциональная спецификация

Описание назначения и методов использования интерфейсов ФБО, их параметров, связанных с ними действий для выполнения ФТБ и формируемых сообщений об ошибках

Руководство пользователя по эксплуатации

Описание доступных пользователям функций, интерфейсов прав и обязанностей, описание принципов безопасной работы пользователей с интерфейсами ОО

Представление реализации ФБО

Процессы внутреннего содержания ФБО в виде исходного текста программ, микропрограмм, схем аппаратных средств и/или программного кода модели интегральных схем или размещения данных

Проект ОО

Описание структуры ОО на уровне подсистем и модулей, их назначение и взаимодействие

Задание по безопасности / Профиль защиты

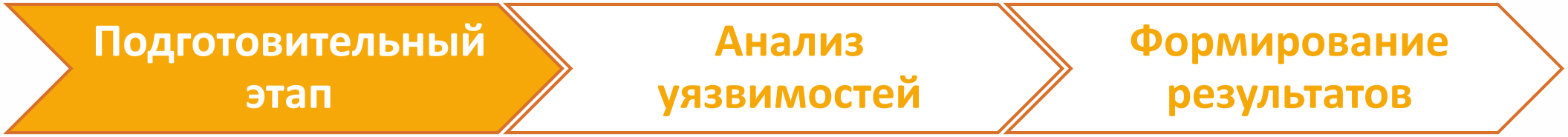
Изложение потребности в безопасности

План

- [x] Обзор нормативных требований
- [x] Исходные данные для проведения оценки
- [ ] Основные этапы и методы оценки
- [ ] Описание результатов проведения оценки

Основные этапы анализа уязвимостей

Основные этапы анализа уязвимостей



1. **Сбор исходных данных**

2. **Исследование объекта оценки:**
   - ✓ Анализ ЗБ: согласуется ли тестируемая конфигурация с оцениваемой (определенной в ЗБ)
   - ✓ Анализ конфигурации: соответствует ли реальное состояние ОО известному (правильно ли установлен)

Основные этапы анализа уязвимостей

USSC

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

1. **Идентификация потенциальных уязвимостей**
   - ✓ Исследование общедоступных источников:
     - специальные публикации (журналы, книги)
     - исследовательские статьи
     - материалы конференций

Основные этапы анализа уязвимостей

USSC

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

1. **Идентификация потенциальных уязвимостей**
   - ✓ Исследование общедоступных источников:
   - ✓ Фокусированный поиск в документации на ОО

Оценщик использует знания проекта ОО и функционирования ОО, чтобы выдвинуть гипотезу и идентифицировать потенциальные недостатки в разработке и специфицированном методе функционирования ОО

Основные этапы анализа уязвимостей

ГОСТ Р 56546-2015 Защита информации. Уязвимости ИС. Классификация уязвимостей ИС

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

Классификация уязвимостей по области происхождения

- уязвимости кода
- уязвимости конфигурации
- уязвимости архитектуры
- организационные уязвимости
- многофакторные уязвимости

Основные этапы анализа уязвимостей

ГОСТ Р 56546-2015 Защита информации. Уязвимости ИС. Классификация уязвимостей ИС

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

Классификация уязвимостей по типу недостатка ОО

- неправильная настройка параметров ПО
- неполнота проверки входных данных
- прослеживание пути доступа к каталогам
- внедрение команд ОС
- межсайтовый скриптинг
- внедрение разметки
- внедрение произвольного кода
- неконтролируемая форматная строка
- недостатки в вычислениях
- утечка/раскрытие информации ограниченного доступа
- управление привилегиями и доступом
- недостатки шифрования
- подмена межсайтовых запросов
- недостатки, связанные с управлением ресурсами

Основные этапы анализа уязвимостей

ГОСТ Р 56546-2015 Защита информации. Уязвимости ИС. Классификация уязвимостей ИС

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

Классификация уязвимостей по месту возникновения

- уязвимости в общесистемном ПО
- уязвимости в прикладном ПО
- уязвимости в специальном ПО
- уязвимости в технических средствах
- уязвимости в портативных технических средствах
- уязвимости в сетевом оборудовании
- уязвимости в средствах защиты информации

Основные этапы анализа уязвимостей

USSC

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

1. **Идентификация потенциальных уязвимостей**
   - ✓ Исследование общедоступных источников:
   - ✓ Фокусированный поиск в документации на ОО
   - ✓ Документирование перечня кандидатов на тестирование в Техническом отчете

Основные этапы анализа уязвимостей

USSC

Подготовительный этап → **Анализ уязвимостей** → Формирование результатов

1. **Идентификация потенциальных уязвимостей**
2. **Тестирование на проникновение :**
   - ✓ Разработка тестов проникновения и тестовой документации

Тестовая документация содержит:

- идентификацию тестируемой потенциальной уязвимости оцениваемого ОО
- инструкции по подключению и настройке тестового оборудования и установке начальных условий
- инструкции по инициированию и наблюдению режима выполнения ФБО
- описание ожидаемых результатов и дальнейшего анализа

Основные этапы анализа уязвимостей

USSC

Подготовительный этап | **Анализ уязвимостей** | Формирование результатов

1. **Идентификация потенциальных уязвимостей**
2. **Тестирование на проникновение :**
   - ✓ Разработка тестов проникновения и тестовой документации
   - ✓ Тестирование на проникновение

Оценщик принимает на себя роль нарушителя с **усиленным базовым** потенциалом

Потенциал нарушителя

Факторы анализа потенциала нарушителя:

Общее затрачиваемое время
время, затрачиваемое на идентификацию уязвимости и её использование

Компетентность специалиста
уровень общих знаний основополагающих принципов, типа продукта или методов нападения

Знание ОО
знание проекта ОО и его функционирования

Возможность доступа к ОО
временной интервал или количество образцов ОО, необходимые для использования уязвимостей

Оборудование
аппаратные средства/программное обеспечение ИТ или другое оборудование

Основные этапы анализа уязвимостей

1. **Идентификация потенциальных уязвимостей**
2. **Тестирование на проникновение :**
   - ✓ Разработка тестов проникновения и тестовой документации
   - ✓ Тестирование на проникновение
   - ✓ Фиксация фактических результатов

Основные этапы анализа уязвимостей

Подготовительный этап → Анализ уязвимостей → **Формирование результатов**

Разработка Технического отчета об оценке

План

- [x] Обзор нормативных требований
- [x] Исходные данные для проведения оценки
- [x] Основные этапы и методы оценки
- [ ] Описание результатов проведения оценки

Содержание Технического отчета

1. Описание идентифицированных и тестируемых уязвимостей:

- ✓ источник уязвимости
- ✓ связанные с ней невыполненные ФТБ
- ✓ описание
- ✓ пригодна ли она для использования в среде функционирования или нет
- ✓ расчет потенциала нападения

2. Информация об усилиях оценщика:

- ✓ тестируемые конфигурации ОО
- ✓ ИФБО, которые подвергались тестированию проникновения

3. Заключение:

- ✓ о соответствии исследуемого ОО предоставленным свидетельствам
- ✓ о выполнении/невыполнении заявленных ФТБ

4. Формирование общих рекомендаций по устранению найденных уязвимостей

План

- Обзор нормативных требований
- Исходные данные для проведения оценки
- Основные этапы и методы оценки
- Описание результатов проведения оценки

Наши предложения для финансовых организаций

Опыт

Специалисты компании УЦСБ свободно владеют различными методиками сетевых атак и имеют богатый опыт реализации мероприятий по анализу защищенности

Сертификации

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

- Certified Information System Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Computer Hacking Forensic Investigator (CHFI)
- 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**

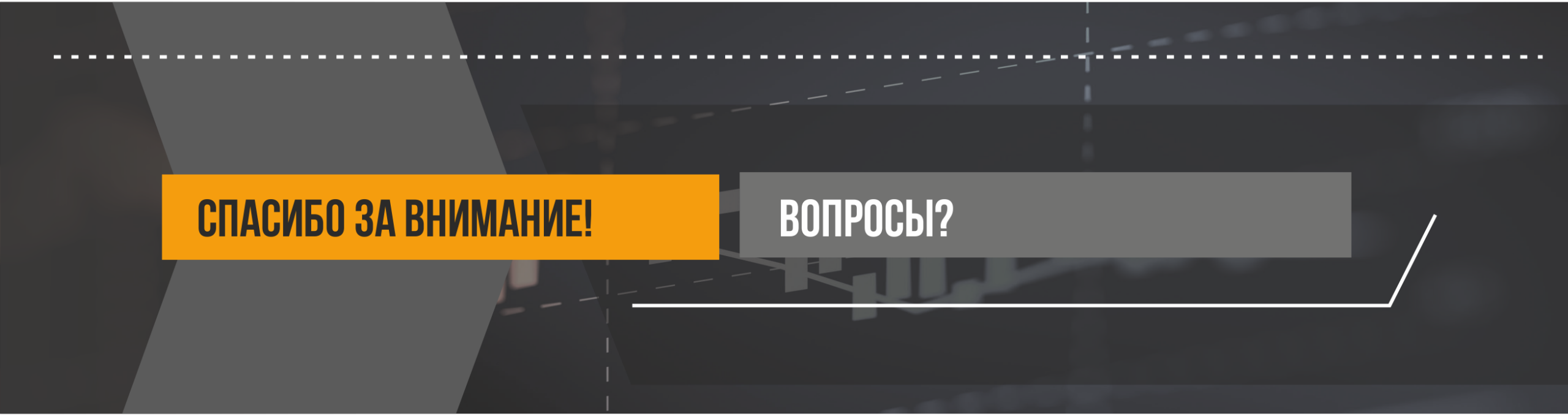
USSC.RU

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

Краснов Сергей

Аналитический центр

skrasnov@ussc.ru

Пермякова Татьяна

Аналитический центр

tpermyakova@ussc.ru