USSC

Требования Банка России по информационной безопасности для кредитных организаций. 683-П, 672-П, изменения в 382-П

Сергей Борисов
Диана Лейчук

Требования Банка России по ИБ

- Устанавливает требования ИБ для финансовых организаций
- В случае неисполнения требований – предписание Банка России
- В случае не устранения нарушений, указанных в предписании, – предусмотренная законом ответственность

План

- [ ] Обзор 683-П
- [ ] Обзор 672-П
- [ ] Обзор изменений в 382-П
- [ ] Дорожная карта по выполнению требований

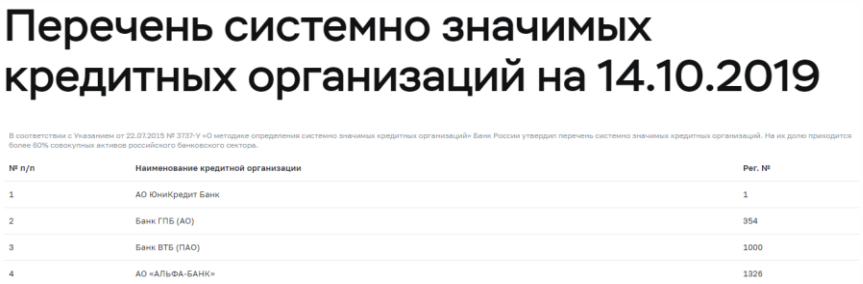
Организации, на которые распространяется 683-П

USSC

Все кредитные организации

с 01.01.2021

Системно значимые кредитные организации
https://www.cbr.ru/banking_sector/credit/



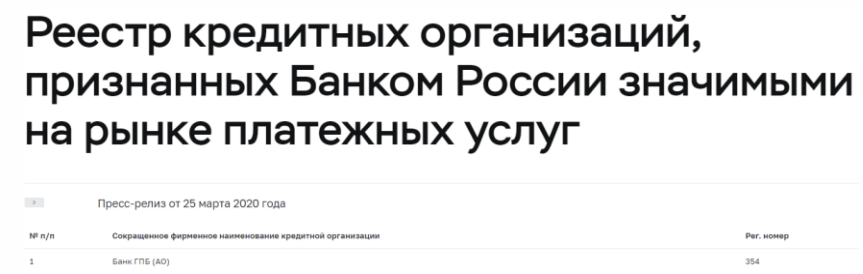
Усиленный уровень

Операторы услуг платежной инфраструктуры системно значимых платежных систем:

- Платежная система Банка России
- Платежная система НРД

https://www.cbr.ru/Content/Document/Page/93088

Кредитные организации, значимые на рынке платежных услуг
https://www.cbr.ru/registries/nps/reestr/



Стандартный уровень

Остальные кредитные организации

Системы, на которые распространяется 683-П

Все системы, используемые для банковских операций, связанных с осуществлением перевода денежных средств, в которых обрабатывается следующая информация:

электронные сообщения

информация, необходимая для авторизации клиентов

информация об осуществленных банковских операциях

криптографические ключи

Требования 683-П

1. **Тестирование на проникновение** (ежегодное)

2. Сертифицированное прикладное ПО или ПО, в отношении которого проведен анализ уязвимостей к ОУД4 (с 01.01.2020):

- ПО, распространяемое клиентам для осуществления банковских операций
- ПО, обрабатывающее защищаемую информации при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием сети Интернет

Сертификация – в системе сертификации ФСТЭК России

Анализ уязвимостей – с привлечением организации-лицензиата ФСТЭК России

Вебинары:

29.04	Анализ уязвимостей по требованиям к ОУД4
15.07	Пентесты для финансовых организаций

Требования 683-П

3. Подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить составление уполномоченным на это лицом

- усиленная квалифицированная электронная подпись
- усиленная неквалифицированная электронная подпись
- простая электронная подпись

} условия использования отражать в договорах с клиентами

4. Реализация технологии безопасной обработки защищаемой информации

5. Требования к средствам криптографической защиты информации (СКЗИ):

- эксплуатация СКЗИ в соответствии с технической документацией
- применение СКЗИ, сертифицированных ФСБ России

Вебинар:

16.09	Требования к средствам криптографической защиты информации в финансовых организациях

Требования 683-П

6. Доведение до клиентов рекомендаций:

- по защите информации от воздействия вредоносного кода
- о возможных рисках несанкционированного доступа (НСД)
- о мерах по предотвращению НСД
- о мерах по контролю конфигурации устройств

Организация самостоятельно принимает решение о способе и периодичности доведения информации.

Варианты:

- приложение к договору
- рассылка на электронные адреса
- размещение на сайте организации
- периодическая sms-рассылка

Рекомендуется фиксировать факт ознакомления клиентов с рекомендациями

Требования 683-П

7. Установление порядка работы с инцидентами защиты информации:

СТО БР БФБО-1.5-2018

- определение перечня типов инцидентов
- порядок регистрации инцидентов
- регистрация инцидентов
- информирование Банка России:

  Основной канал - АСОИ ФинЦЕРТ (https://lk.fincert.cbr.ru)

  Резервные каналы:

  - электронная почта (fincert@cbr.ru);
  - телефонный звонок в Банк России (+7 495 7 727 090)

Требования 683-П

8. Оценка соответствия уровня защиты информации по ГОСТ Р 57580.2-2018 (с 01.01.2021):

- с привлечением лицензиатов ФСТЭК России
- не реже одного раза в два года
- хранение отчета по результатам оценки – не менее 5 лет

9. Обеспечить определенный уровень соответствия:

- не ниже третьего (01.01.2021 – 31.12.2022)
- не ниже четвертого (с 01.01.2023)

Вебинары:

20.05	Обзор требований ГОСТ Р 57580.1-2017
17.06	Как проводится аудит по ГОСТ Р 57580?

Организации, на которые распространяется 672-П

Участники платежной системы Банка России:

- Кредитные организации, имеющие доступ к услугам по переводу денежных средств с использованием распоряжений в электронном виде
- Операционный центр сторонней платежной системы
- Платежный клиринговый центр сторонней платежной системы

Системы, на которые распространяется 672-П

Автоматизированные системы (АС), программное обеспечение, средства вычислительной техники (СВТ), телекоммуникационное оборудование, применяемые для обработки информации:

информация об остатках денежных средств

информация о совершенных переводах денежных средств

информация, содержащаяся в оформленных распоряжениях

информация о платежных клиринговых позициях

информация, необходимая для удостоверения прав клиентов

криптографические ключи

информация о конфигурации АС, ПО, СВТ…

информация ограниченного доступа

Основные требования 672-П

1. Размещать объекты информационной инфраструктуры в выделенных сегментах

- ОПКЦ: уровень защиты сегмента – усиленный (ГОСТ Р 57580.1-2017)
- участники ССНП и СБП: уровень защиты сегмента – стандартный (ГОСТ Р 57580.1-2017)

2. Разработать документацию:

- состав и порядок применения организационных мер защиты информации и использования технических средств защиты информации
- в рамках процессов ГОСТ Р 57580.1-2017

3. Требования к СКЗИ:

- эксплуатация СКЗИ в соответствии с технической документацией
- применение СКЗИ, сертифицированных ФСБ России

4. Оценка соответствия уровню защиты по ГОСТ Р 57580:

- не реже одного раза в два года, а также по требованию Банка России
- уровень защиты – не ниже четвертого по ГОСТ Р 57580.2-2018

«Старая» версия 382-П

Последние изменения – указание Банка России от 07.05.2018 №4793-У

Распространяется на:

- операторов по переводу денежных средств
- банковских платежных агентов (субагентов)
- операторов платежных систем
- операторов услуг платежной инфраструктуры

«Старая» версия 382-П

Автоматизированные системы (АС), программное обеспечение, средства вычислительной техники (СВТ), телекоммуникационное оборудование, применяемые для обработки информации:

информация об остатках денежных средств

информация о совершенных переводах денежных средств

информация, содержащаяся в оформленных распоряжениях

информация о платежных клиринговых позициях

информация, необходимая для удостоверения прав клиентов

криптографические ключи

информация о конфигурации АС, ПО, СВТ…

информация ограниченного доступа

Требования «старой» версии 382-П

1. Сертифицированное прикладное ПО или в отношении которого проведен анализ уязвимостей к ОУД4 (с 01.01.2020)

2. Тестирование на проникновение и анализ уязвимостей (ежегодно)

3. Требования к СКЗИ:

- эксплуатация СКЗИ в соответствии с технической документацией и НПА

4. Реализация технологии безопасной обработки защищаемой информации

5. Информирование Банка России об инцидентах защиты информации

6. Оценка соответствия требованиям 382-П:

- с привлечением лицензиата ФСТЭК России
- через 6 месяцев после получения статуса и раз в 2 года

«Новая» версия 382-П

Вступает в силу с 1 января 2023

Распространяется на:

- операторов по переводу денежных средств,
- банковских платежных агентов (субагентов)
- операторов платежных систем
- операторов услуг платежной инфраструктуры
- операторов услуг информационного обмена
- поставщиков платежных приложений

Требования «новой» версии 382-П

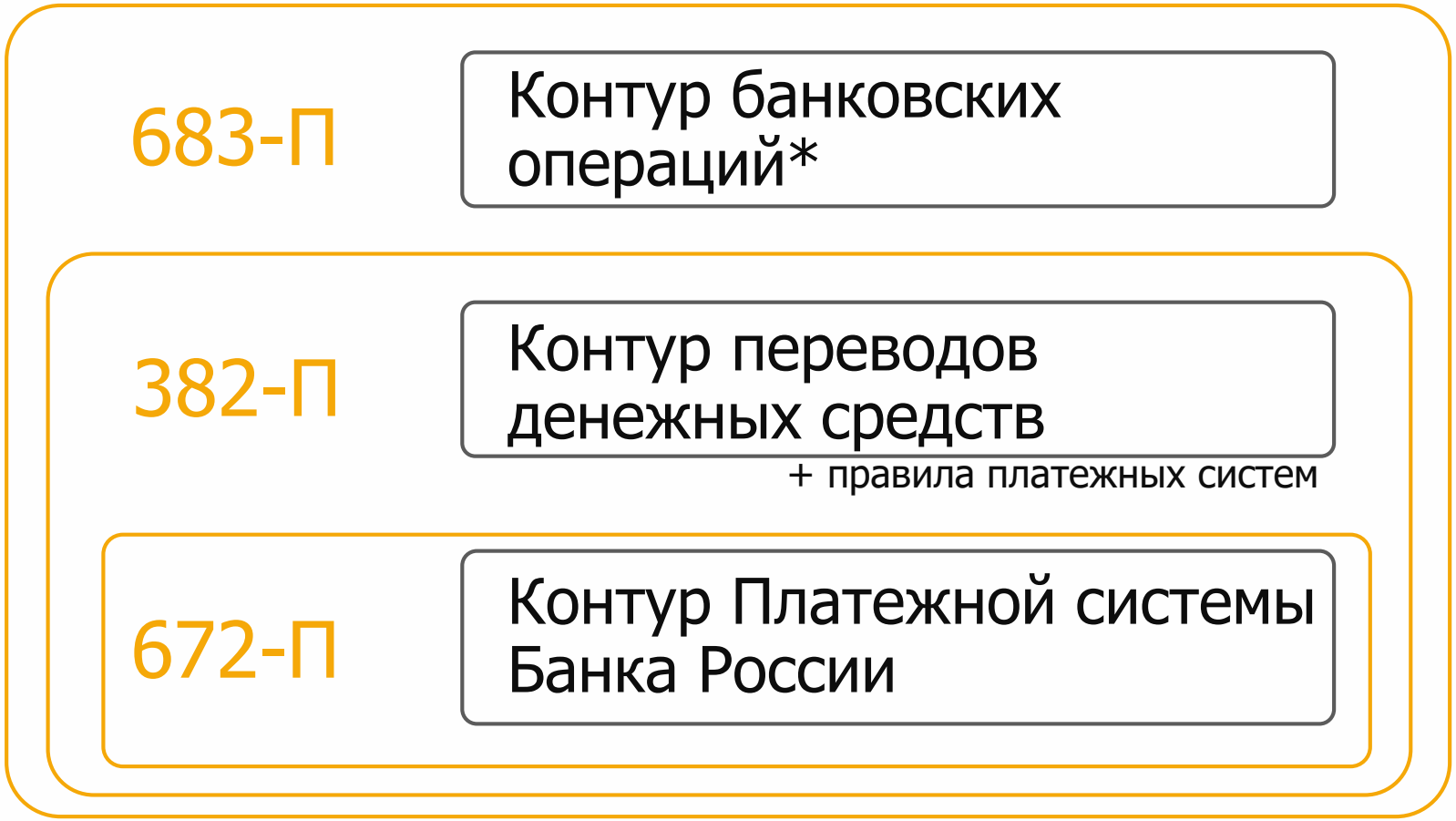
	операторы по переводу денежных средств	банковские платежные агенты (субагенты)		операторы услуг информационного обмена		операторы услуг платежной инфраструктуры	
		являющиеся платежными агрегаторами, привлекаемые системно значимыми кредитными организациями, кредитными организациями, значимыми на рынке платежных услуг	иные	оказывающие системно значимым кредитным организациям, кредитным организациям, значимым на рынке платежных услуг, услуги обмена информацией при осуществлении операций с использованием электронных средств платежа	иные	оказывающие услуги платежной инфраструктуры в рамках системно значимых платежных систем	иные
Реализация уровней защиты по ГОСТ Р 57580.1-2017	+ (см. 683-П)	Стандартный уровень	Минимальный уровень	Усиленный уровень	Стандартный уровень	Усиленный уровень	Стандартный уровень
Сертификация прикладного ПО или анализ уязвимостей к ОУД4	+	+	Самостоятельно определяют необходимость	+	+	+	Самостоятельно определяют необходимость

Требования «новой» версии 382-П

	операторы по переводу денежных средств	банковские платежные агенты (субагенты)		операторы услуг информационного обмена		операторы услуг платежной инфраструктуры	
		являющиеся платежными агрегаторами, привлекаемые системно значимыми кредитными организациями, кредитными организациями, значимыми на рынке платежных услуг	иные	оказывающие системно значимым кредитным организациям, кредитным организациям, значимым на рынке платежных услуг, услуги обмена информацией при осуществлении операций с использованием электронных средств платежа	иные	оказывающие услуги платежной инфраструктуры в рамках системно значимых платежных систем	иные
Тестирование на проникновение	ежегодно	ежегодно	Самостоятельно определяют необходимость	ежегодно		ежегодно	ежегодно
Оценка соответствия уровням защиты по ГОСТ Р 57580.2-2018	1 раз в 2 года	1 раз в 2 года	1 раз в 3 года	1 раза в 2 года		1 раз в 2 года	
	Уровень соответствия не ниже 4	Уровень соответствия не ниже 4	Уровень соответствия не ниже 3	Уровень соответствия не ниже 4		Уровень соответствия не ниже 4	

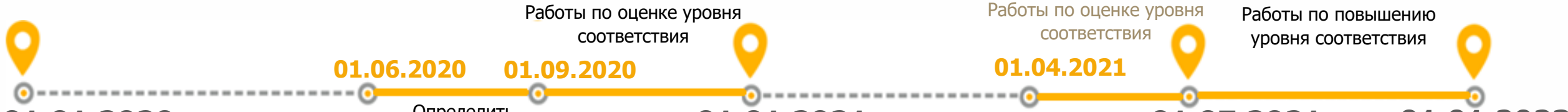
Соотношение между Положениями Банка России

По контурам безопасности



*банковских операций, связанных с переводом денежных средств

Реализация требований по ИБ



01.01.2020
Сертифицированное ПО / анализ уязвимостей к ОУД 4

Иные требования

01.06.2020
Определить предварительный уровень соответствия

Реализовать меры из ГОСТ Р 57580.1

Работы по оценке уровня соответствия
01.09.2020

01.01.2021
Оценка уровня соответствия по ГОСТ Р 57580 Уровень ≥3

Работы по оценке уровня соответствия
01.04.2021

01.07.2021
Оценка уровня соответствия по ГОСТ Р 57580

Работы по повышению уровня соответствия

с 01.01.2023
Оценка уровня соответствия Уровень ≥4 (683-П и 672-П)

683-П: Требования для контура безопасности банковских операций*

672-П: Требования для контура безопасности Платежной системы Банка России

xx.xx.20xx рекомендуемая дата

xx.xx.20xx дата, установленная Положением Банка России

Реализация регулярных требований по ИБ

01.06.2019+(1)

Тестирование на проникновение

Оценка уровня соответствия по ГОСТ Р 57580

с 01.01.2021+(2)

с 01.07.2021+(2)

Оценка уровня соответствия по ГОСТ Р 57580

Оценка уровня соответствия по ГОСТ Р 57580

с 01.01.2023+(2)

683-П: Требования для контура безопасности банковских операций*

382-П: Требования для контура безопасности переводов денежных средств

672-П: Требования для контура безопасности Платежной системы Банка России

xx.xx.20xx дата, установленная Положением Банка России

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

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

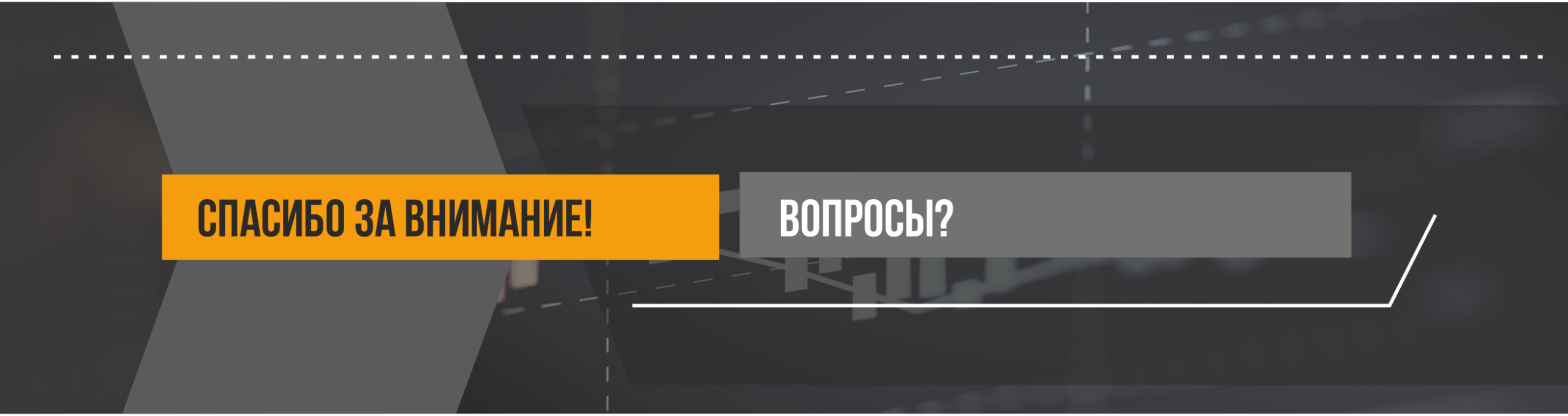
USSC.RU

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



НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Борисов Сергей

Обособленное подразделение в г. Краснодар

sborisov@ussc.ru

Лейчук Диана

Аналитический центр

dleichuk@ussc.ru