USSC

ИЗМЕНЕНИЯ НОРМАТИВНО-ПРАВОВЫХ АКТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИБ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ЗА 2020 ГОД

Борисов Сергей
Батурин Олег
Кузнецова Ксения

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	Онлайн-сервис оценки соответствия ГОСТ Р 57580.2-2018
7	26.08	Требования к средствам криптографической защиты информации в финансовых организациях
8	16.09	Пентесты для финансовых организаций
9	**10.02**	**Последние изменения НПА в области обеспечения безопасности финансовых организаций**

ВЕДУЩИЕ ДЕВЯТОГО ВЫПУСКА

Сергей Борисов

Заместитель руководителя по ИБ
обособленного подразделения УЦСБ
г. Краснодар

Работа в ИБ – 15 лет

Блог
https://sborisov.
blogspot.com

Батурин Олег

Аналитик
Аналитического центра УЦСБ
г. Екатеринбург

Работа в ИБ – 8 лет

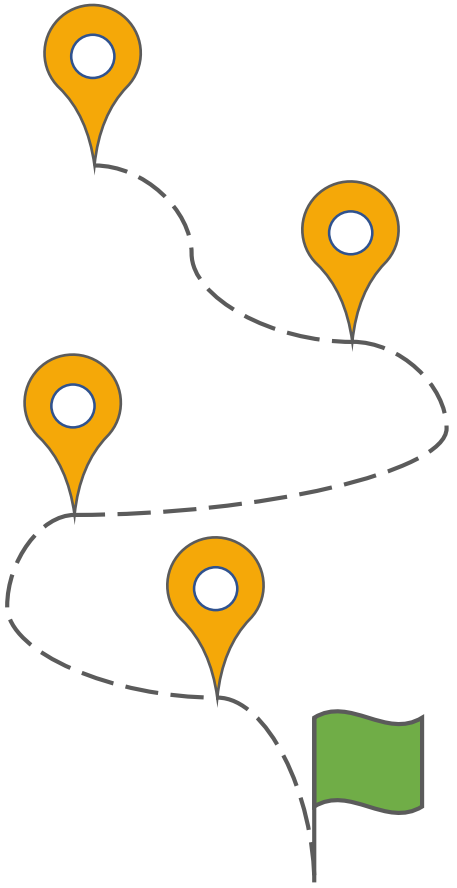
Кузнецова Ксения

Аналитик
Аналитического центра УЦСБ
г. Екатеринбург

Работа в ИБ – 2 года

ПЛАН ВЕБИНАРА

1	Основные изменения, вносимые в рамках Положения 719-П
2	Основные изменения в рамках проекта замены Положения 684-П
3	Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений
4	Обзор требований по защите информации при обмене электронными сообщениями в платежной системе Банка России
5	Обзор требований к управлению новыми категориями операционных рисков



1. ОСНОВНЫЕ ИЗМЕНЕНИЯ, ВНОСИМЫЕ В РАМКАХ ПОЛОЖЕНИЯ 719-П

Положение Банка России от 4 июня 2020 г. № 719-П
«О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Положение Банка России от 9 июня 2012 г. № 382-П
«О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

ОБЛАСТЬ ПРИМЕНЕНИЯ 719-П

Субъекты доступа:

- операторы по переводу денежных средств
- банковские платежные агенты
- операторы платежных систем
- операторы услуг платежной инфраструктуры
- поставщики платежных приложений
- операторы услуг информационного обмена

Объекты доступа:

- автоматизированные системы
- программное обеспечение
- средства вычислительной техники
- телекоммуникационное оборудование

ОТЛИЧИЯ ОТ 382-П

USSC

1	2	3	4	5
Структура документа	Новые субъекты	Требования к защите информации	Требования соответствия оценочному уровню доверия	Санкционные меры
Удобная структура документа	Введено два новых субъекта	Определены требования к защите информации в соответствии с ГОСТ Р 57580.1 и проведению оценки соответствия по ГОСТ Р 57580.2	Введены требования по соответствию оценочному уровню доверия по полному профилю (ОУД4), не только в отношении уязвимостей	Санкционные меры за ненадлежащее исполнение Положения

ТРЕБОВАНИЯ 719-П

Тип организации / Критерий сравнения	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)	минимальный уровень		усиленный уровень	стандартный уровень	усиленный уровень	стандартный уровень
Сертификация прикладного ПО или анализ уязвимостей ОУД4	обязательная сертификация	по требованию операторов по переводу денежных средств		+	+	+	самостоятельно определяют необходимость
Уровень доверия в системе сертификации ФСТЭК России	5 (для системно значимых - 4)	6 или выше, по требованию операторов по переводу денежных средств		**5**	**5**	**4**	**5**
Тестирование на проникновение	ежегодно	ежегодно	по требованиям ОПДС, но не реже 1 раза в год	ежегодно		ежегодно	
Оценка соответствия уровням защиты по ГОСТ Р 57580.2-2018	1 раз в 2 года	1 раз в 2 года	требования не формализованы	1 раза в 2 года		1 раз в 2 года	
	Уровень соответствия не ниже 4	уровень соответствия не ниже 4		уровень соответствия не ниже 4		уровень соответствия не ниже 4	

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

USSC

1. Хранение и восстановление защищаемой информации
2. Сверка результатов осуществления финансовых операций, реализация двойного контроля правильности формирования электронных сообщений
3. Система управления логическим доступом клиентов, сотрудников, участников обмена электронными сообщениями
4. Использование электронной подписи

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

USSC

1 Хранение и восстановление защищаемой информации

Обеспечение хранения защищаемой информации, информации о событиях, подлежащих регистрации, информации об инцидентах защиты информации в течение **пяти лет** с даты формирования информации в неизменном виде

Восстановление защищаемой информации в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

USSC

2 Сверка результатов осуществления финансовых операций, реализация двойного контроля правильности формирования электронных сообщений

Проверка соответствия (сверка) результатов осуществления операций, связанных с переводом денежных средств, с информацией, содержащейся в электронных сообщениях

Реализация мер, направленных на проверку правильности формирования электронных сообщений

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

USSC

3 Система управления логическим доступом клиентов, сотрудников, участников обмена электронными сообщениями

Реализация механизма идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств

Реализация механизма двухфакторной аутентификации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

4 Использование электронной подписи

Взаимная (двухсторонняя) аутентификация участников обмена средствами вычислительной техники операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, клиентов операторов по переводу денежных средств

Использование простой или усиленной электронной подписи в соответствии с Федеральным законом № 63-ФЗ

Использование усиленной электронной подписи для контроля целостности и подтверждения подлинности электронных сообщений в соответствии с Федеральным законом № 63-ФЗ

Получение подтверждения от оператора по переводу денежных средств права клиента оператора по переводу денежных средств распоряжаться денежными средствами

ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ ТРЕБОВАНИЙ 719-П

Вступление в силу Положения 719-П
Утрачивает силу 382-П

с 01.01.2022

с 01.01.2024

Требования к обеспечению операторами значимых платежных систем использования **СКЗИ** при переводе денежных средств

Требование по применению **СКЗИ**, прошедших сертификацию

с 01.01.2031

2. ОСНОВНЫЕ ИЗМЕНЕНИЯ, В РАМКАХ ПРОЕКТА ЗАМЕНЫ ПОЛОЖЕНИЯ 684-П

Проект Положения
«Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

ПРОЕКТ 684-П

На основании определенного уровня защиты информации некредитные финансовые организации должны обеспечивать защиту информации в отношении объектов информационной инфраструктуры в соответствии с требованиями ГОСТ Р 57580.1-2017

СУБЪЕКТЫ, ОПРЕДЕЛЕННЫЕ ПРОЕКТОМ 684-П

Субъекты, которые должны реализовывать требования ГОСТ Р 57580.1-2017, соответствующие **усиленному** уровню защиты информации:

- Центральные контрагенты
- Центральный депозитарий
- Регистраторы финансовых транзакций

СУБЪЕКТЫ, ОПРЕДЕЛЕННЫЕ ПРОЕКТОМ 684-П

Субъекты, которые должны реализовывать требования ГОСТ Р 57580.1-2017, соответствующие **стандартному** уровню защиты информации:

- специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов
- клиринговые организации, репозитарии, организаторы торговли, страховые организации
- негосударственные пенсионные фонды
- брокеры, дилеры, депозитарии и управляющие
- операторы инвестиционной платформы
- операторы финансовой платформы
- регистраторы финансовых транзакций
- операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов
- операторы обмена цифровыми финансовыми активами

СУБЪЕКТЫ, ОПРЕДЕЛЕННЫЕ ПРОЕКТОМ 684-П

Федеральный закон от 20.07.2020 № 211-ФЗ
«О совершении финансовых сделок
с использованием финансовых платформ»

Федеральный закон от 31.07.2020 № 259-ФЗ
«О цифровых финансовых активах,
цифровой валюте и о внесении изменений
в отдельные законодательные акты Российской Федерации»

- операторы финансовой платформы
- регистраторы финансовых транзакций
- операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов
- операторы обмена цифровыми финансовыми активами

СУБЪЕКТЫ, ОПРЕДЕЛЕННЫЕ ПРОЕКТОМ 684-П

USSC

Субъекты, которые должны реализовывать требования ГОСТ Р 57580.1-2017, соответствующие **минимальному** уровню защиты информации:

- брокеры, дилеры, депозитарии и управляющие, не достигающие стандартного уровня защиты
- управляющие компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов
- форекс-дилеры
- операторы финансовой платформы, не достигающие стандартного уровня защиты
- страховые организации, не достигающие стандартного уровня защиты
- общества взаимного страхования
- страховые брокеры и страховые агенты

ТРЕБОВАНИЯ ПРОЕКТА 684-П

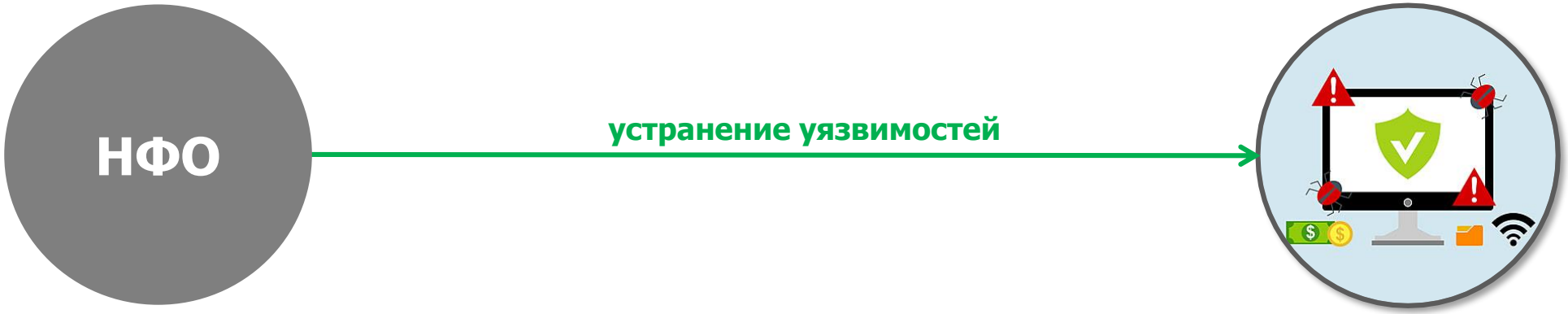
Некредитные финансовые организации, реализующие усиленный и стандартный уровень защиты информации, должны осуществлять тестирование объектов информационной инфраструктуры на предмет проникновений и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры

тестирование на проникновение

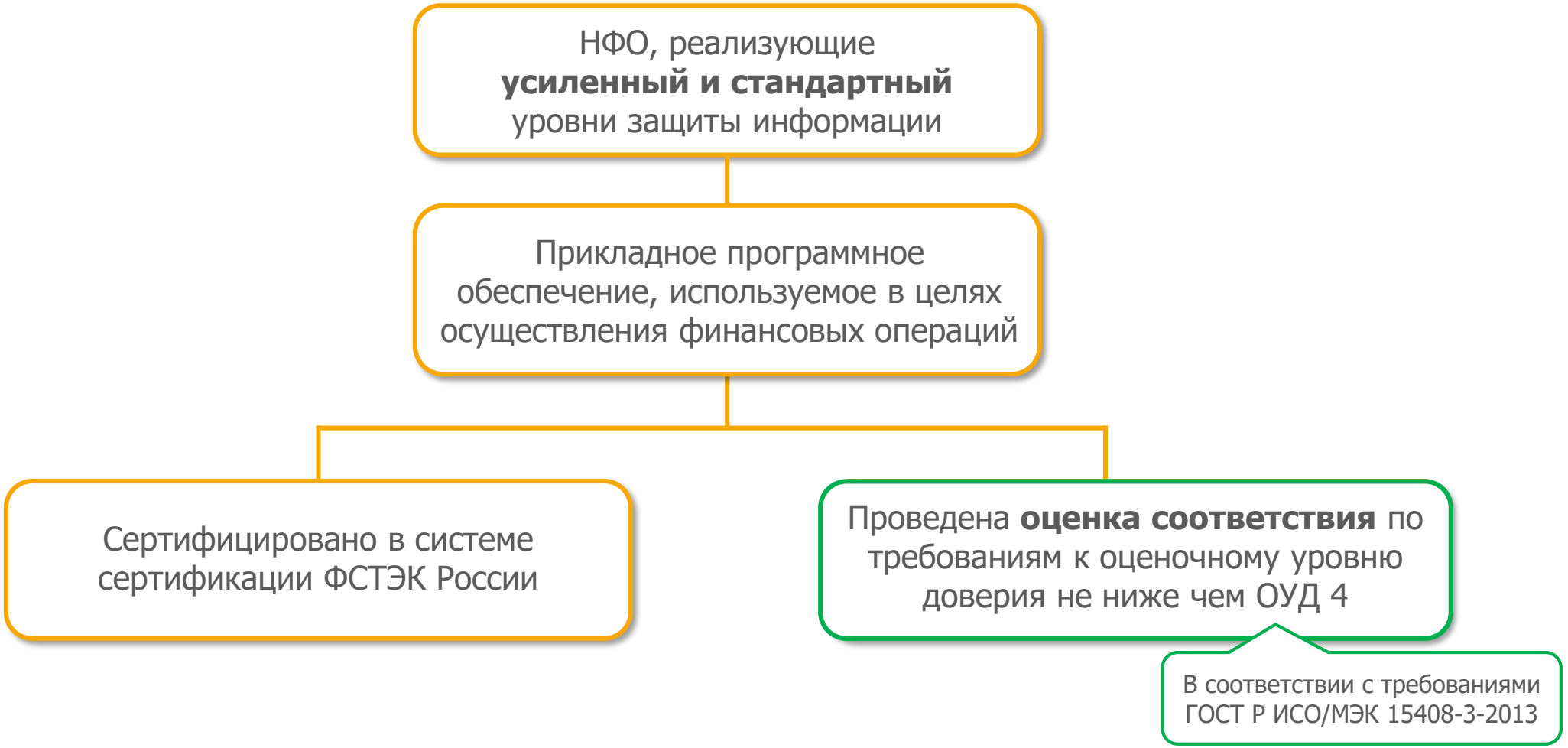
анализ уязвимостей

ТРЕБОВАНИЯ ПРОЕКТА 684-П

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны **устранять выявленные уязвимости** информационной безопасности объектов информационной инфраструктуры



ТРЕБОВАНИЯ ПРОЕКТА 684-П



ТРЕБОВАНИЯ ПРОЕКТА 684-П

ТРЕБОВАНИЯ ПРОЕКТА 684-П

ТРЕБОВАНИЯ ПРОЕКТА 684-П

USSC

В целях обеспечения контроля целостности электронных сообщений некредитных финансовых организаций, реализующих усиленный и стандартный уровни защиты информации, должны обеспечивать **подписание электронных сообщений усиленной электронной подписью** или использовать иные аналоги собственноручной подписи, коды, пароли и другие средства с применением дополнительных организационных и технических мер защиты информации в соответствии с Проектом Положения

В случае использования единой информационной системы персональных данных некредитные финансовые организации должны обеспечивать мероприятия, предусмотренные:

- **Приказом ФСТЭК России №21**
- **Приказом ФСБ России №378**

В случае использования единой системы идентификации и аутентификации некредитные финансовые организации должны обеспечивать мероприятия, предусмотренные **Приказом Минцифры России №210**

ТРЕБОВАНИЯ ПРОЕКТА 684-П

Некредитные финансовые организации должны осуществлять **регистрацию инцидентов**, связанных с обеспечением защиты информации при осуществлении деятельности в сфере финансовых рынков.

Некредитные финансовые организации должны **информировать** Банк России о:

- выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный инцидент защиты информации
- сайтах в сети «Интернет», которые используются некредитной финансовой организацией для осуществления деятельности в сфере финансовых рынков

3. ПРОФИЛЬ ЗАЩИТЫ

Методический документ

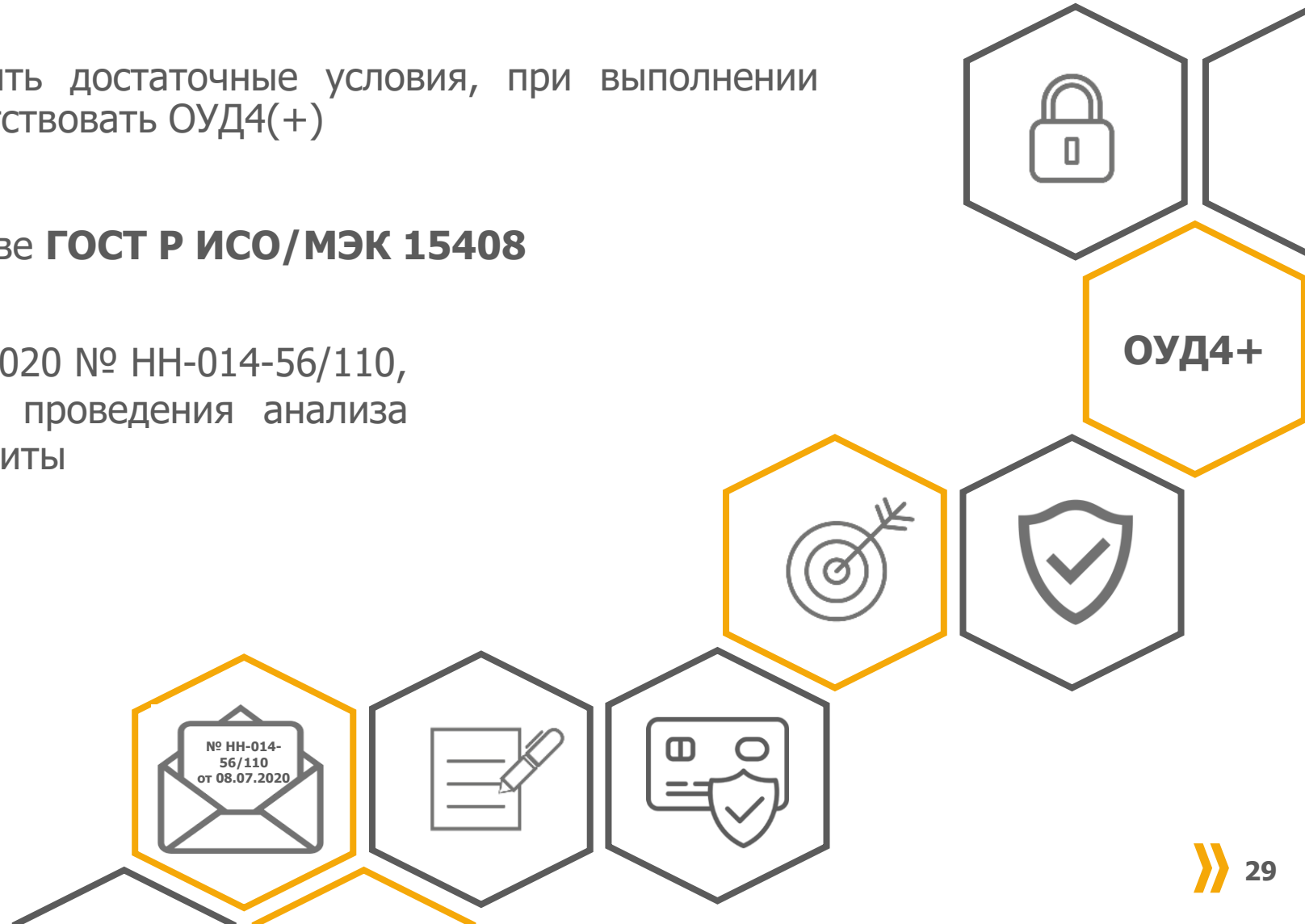
«Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций»

ПРОФИЛЬ ЗАЩИТЫ

Цель профиля защиты – установить достаточные условия, при выполнении которых объект оценки будет соответствовать ОУД4(+)

Профиль защиты разработан на основе **ГОСТ Р ИСО/МЭК 15408**

В информационном письме от 08.07.2020 № НН-014-56/110, Банк России рекомендует в целях проведения анализа уязвимостей применять Профиль защиты



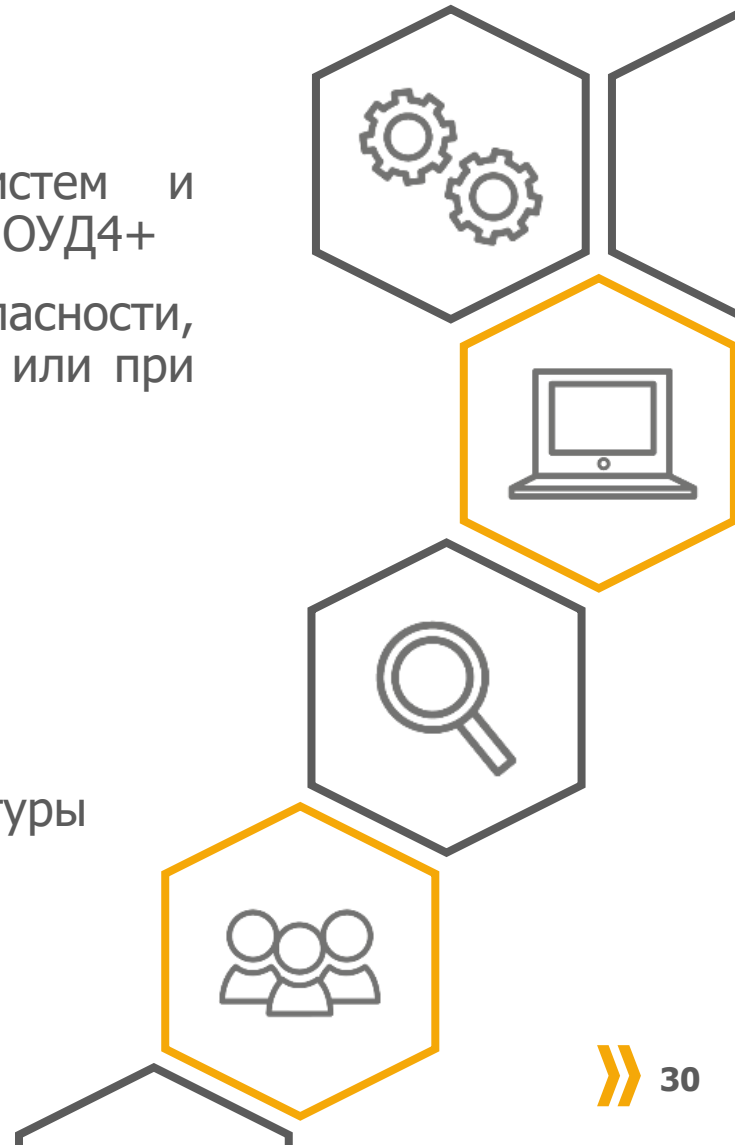
НАЗНАЧЕНИЕ ПРОФИЛЯ ЗАЩИТЫ

Назначение:

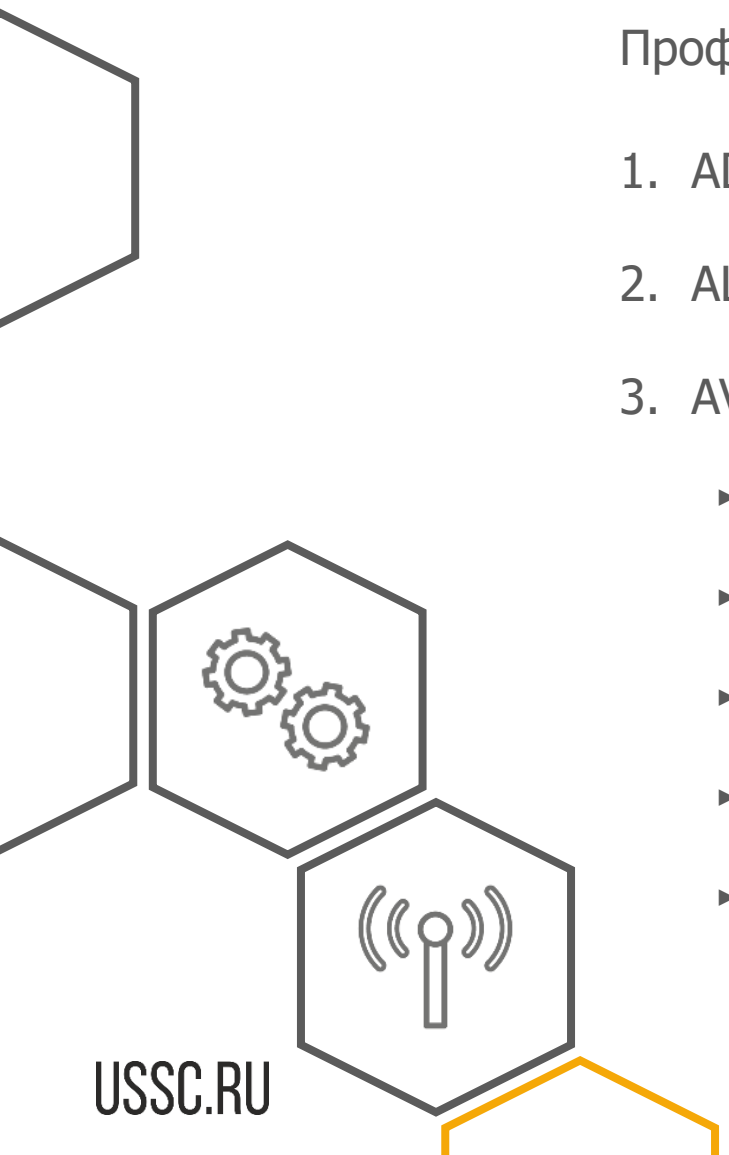
1. **анализ уязвимостей** прикладного ПО автоматизированных систем и приложений по требованиям к оценочному уровню доверия не ниже чем ОУД4+
2. **формирование** достаточных **функциональных требований** безопасности, при дальнейшей сертификации в системе сертификации ФСТЭК России или при проведении оценки соответствия по ОУД4+

Субъекты, использующие профиль защиты:

1. субъекты Положений Банка России 683-П, 684-П, 382-П
2. независимые проверяющие организации
3. разработчики и проектировщики объектов информационной инфраструктуры



ПРОФИЛЬ ЗАЩИТЫ



Профиль защиты соответствует пакету **требований доверия ОУД4+** :

1. ADV_IMP.2 «Полное отображение представления реализации ФБО»
2. ALC_FLR.2 «Процедуры сообщений о недостатках»
3. AVA_VAN.5 «Усиленный методический анализ», расширенный компонентами:
   - ADV_IMP_EXT.3 «Реализация ОО»
   - ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения»
   - ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки»
   - AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность»
   - AVA_CCA_EXT.1 «Анализ скрытых каналов»

4. УСЛОВИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

«Условия по защите информации»

УСЛОВИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Субъекты отношений:

- Банк России
- клиенты Банка России, использующие платёжную систему Банка России, либо систему передачи финансовых сообщений

Объекты регулирования:

- правовые отношения между Банком России и его клиентами
- сотрудники клиентов Банка России
- объекты информационной инфраструктуры, используемые для обмена электронными сообщениями, её компоненты

Банк России
Центральный банк Российской Федерации

ОСНОВНЫЕ ТРЕБОВАНИЯ К КЛИЕНТАМ (ДЛЯ ПЛАТЕЖНЫХ СИСТЕМ)

USSC

1. Размещение информационной инфраструктуры, предназначенной для обмена электронными сообщениями в выделенных сегментах вычислительных сетей, соответствующей минимальному уровню по ГОСТ Р 57580.1
2. Документы Клиента, определяющие порядок обеспечения защиты при обмене электронными сообщениями, должны определять состав и порядок применения организационных и технических мер защиты по всем процессам ГОСТ Р 57580.1

с 01.07.2021

3. При обмене электронными сообщениями с использованием СКЗИ должны выполняться требования к использованию СКЗИ
4. Передача и прием электронных сообщений должны осуществляться с использованием программного комплекса, предоставляемого Банком России
5. Хранение входящих и исходящих электронных сообщений в течение 5 лет
6. При обмене электронными сообщениями при переводе денежных средств должна применяться электронная подпись, сертификат ключа которой выдан Банком России
7. При обмене электронными сообщениями между Клиентом и Банком России должны руководствоваться Условиями управления криптографическими ключами
8. Клиенты должны информировать Банк России об инцидентах

с 05.10.2020

ОСНОВНЫЕ ТРЕБОВАНИЯ К КЛИЕНТАМ (ПРОДОЛЖЕНИЕ) (ДЛЯ ПЛАТЕЖНЫХ СИСТЕМ)

9. Организационные меры и технические средства защиты информации, используемые при обмене электронными сообщениями, применяются с учетом требований:

- формированием электронных сообщений и контролем реквизитов электронных сообщений в информационной инфраструктуре Клиента в соответствии с приложением 6 к Условиям защиты, а также использованием **двух усиленных электронных подписей** для контроля целостности и подтверждения подлинности электронных сообщений
- применением **третьего варианта защиты**, предусмотренного Альбомом унифицированных форматов электронных банковских сообщений, размещенным на официальном сайте Банка России
- **шифрованием** электронных сообщений на прикладном уровне

с 05.10.2020

- применением **средств защиты информации**, реализующих двухстороннюю аутентификацию и шифрование информации на уровне звена данных или сетевом уровне

с 01.07.2021

ОСНОВНЫЕ ТРЕБОВАНИЯ К ПОЛЬЗОВАТЕЛЯМ (СИСТЕМА ПЕРЕДАЧИ ФИНАНСОВЫХ СООБЩЕНИЙ)

1.	Размещение информационной инфраструктуры, предназначенной для обмена финансовые сообщения в выделенных сегментах вычислительных сетей	с 01.07.2021
2.	Документы Клиента, определяющие порядок обеспечения защиты при обмене финансовыми сообщениями должны определять состав и порядок применения организационных и технических мер защиты по всем процессам ГОСТ Р 57580.1	
3.	При обмене финансовыми сообщениями с использованием СКЗИ, должны выполняться требования к использованию СКЗИ	с 05.10.2020
4.	Передача и прием финансовых сообщений должны осуществляться с использованием программного комплекса, предоставляемого Банком России	
5.	Хранение входящих и исходящих финансовых сообщений в течении 5 лет	
6.	При обмене ФС при переводе денежных средств, должна применяться электронная подпись, сертификат ключа которой выдан Банком России	
7.	При обмене ФС между Клиентом и Банком России должны руководствоваться Условиями управления криптографическими ключами, **в части изготовления ключей**	
8.	Клиенты должны информировать Банк России об инцидентах	

СОСТАВ ПРИЛОЖЕНИЙ К УСЛОВИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Приложение 1: Акт о готовности Клиента (Пользователя) к обмену электронными сообщениями, включая сведения об информационной инфраструктуре, предназначенной для формирования, контроля и направления электронными сообщениями в платежной системе Банка России

Приложение 2: Условия управления криптографическими ключами

Приложение 3: Порядок направления обращений о приостановлении (возобновлении) обмена электронными сообщениями или заявлений о приостановлении (возобновлении) обмена финансовых сообщений в случае выявления инцидента, связанного с несоблюдением Клиентом (Пользователем) требований к защите информации

Приложение 4: Урегулирование споров и разногласий при обмене электронными сообщениями

Приложение 5: Требования к использованию СКЗИ

Приложение 6: Требования к формированию электронных сообщений и контролю реквизитов электронных сообщений

5. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ НОВЫМИ КАТЕГОРИЯМИ ОПЕРАЦИОННЫХ РИСКОВ

Положение Банка России от 08.04.2020 **№ 716-П** «О требованиях к системе управления операционным риском в кредитной организации и банковской группу»

ПОЛОЖЕНИЕ БАНКА РОССИИ ОТ 08.04.2020 № 716-П

с 01.10.2020

Вступает в силу Положение № 716-П от 08.04.2020

с 01.01.2022

Система управления операционным риском приведена в соответствие с требованиями Положения №716-П

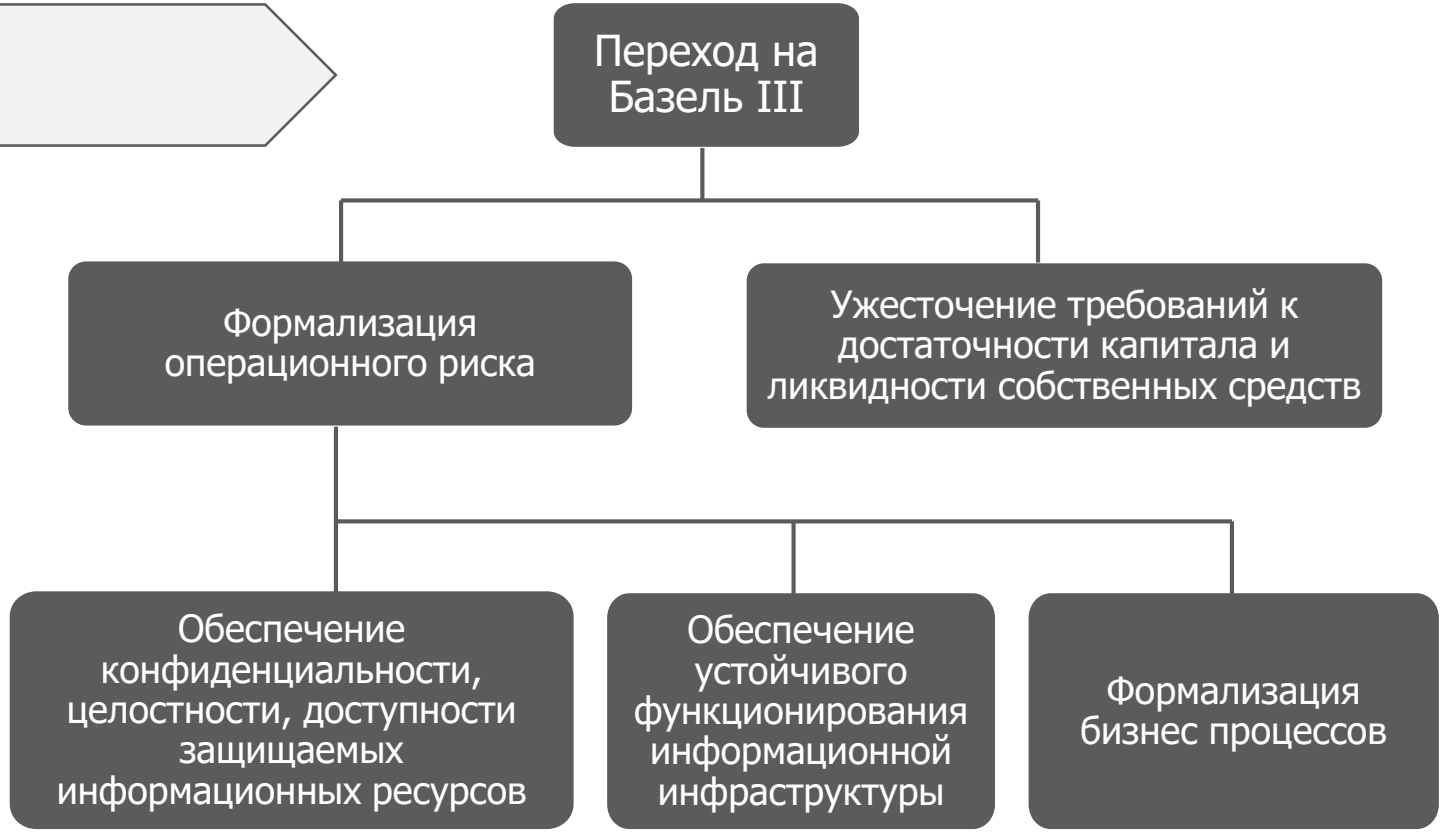
Кредитные организации в случае приведения системы управления операционным риском в соответствие с требованиями Положения №716-П ранее 1 января 2022 года, вправе проинформировать об этом Банк России в целях организации Банком России оценки соответствия системы управления операционным риском требованиям Положения

СОСТАВ МЕРОПРИЯТИЙ

Повышение устойчивости финансовой системы

Формализация риска, введение избыточной ликвидности

Моделирование угроз,
формирование состава мероприятий, направленных на снижение уровня риска,
унификация бизнес-процессов, унификация квалификационных требований к персоналу,
повышение операционной эффективности



ТРЕБОВАНИЯ К КРЕДИТНЫМ ОРГАНИЗАЦИЯ

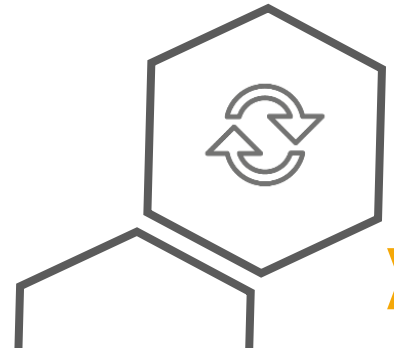
USSC

1	2	3	4
Банк, размер активов которого составляет 500 миллиардов рублей и более на начало текущего отчетного года	Банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей на начало текущего отчетного года	Кредитная организация (головная кредитная организация банковской группы), которая на начало текущего отчетного года является банком с базовой лицензией	Кредитная организация (головная кредитная организация банковской группы), которая на начало текущего отчетного года является небанковской кредитной организацией
Соблюдать п. 9.1.1	Соблюдать п. 9.2.1	Соблюдать п. 9.3.1	Соблюдать п. 9.3.4

ПОНЯТИЕ ОПЕРАЦИОННОГО РИСКА

Риск возникновения убытков в результате ненадежности и недостатков внутренних процедур управления кредитной организации, отказа информационных и иных систем либо вследствие влияния на деятельность кредитной организации внешних событий. Правовой риск является частью операционного риска

Риск **возникновения прямых и непрямых потерь** в результате **несовершенства или ошибочных внутренних процессов** кредитной организации, **действий персонала и иных лиц**, **сбоев и недостатков информационных, технологических и иных систем**, а также в результате реализации **внешних событий**. Правовой риск, риск информационной безопасности и риск информационных систем являются частью операционного риска



ВИДЫ ОПЕРАЦИОННОГО РИСКА

1. Риск информационной безопасности
2. Риск информационных систем
3. Правовой риск
4. Риск ошибок в управлении проектами
5. Риск ошибок в управленческих процессах
6. Риск ошибок в процессах осуществления внутреннего контроля
7. Модельный риск
8. Риск потерь средств клиентов, контрагентов, работников и третьих лиц
9. Риск ошибок процесса управления персоналом
10. Риск платежной системы

ТРЕБОВАНИЯ 716-П
К СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

USSC

1. Создание модели угроз:
   - приведен перечень источников угроз
   - перечень уязвимостей
   - основные сценарии реализации угроз
   - рекомендуемый перечень мер, направленных на снижение риска
   - методика оценки уровня риска
2. Реализация процесса управления инцидентами рисков информационных систем и информационной безопасности:
   - ведение базы данных событий риска,
   - определение процедур реагирования и уведомления об инцидентах информационной безопасности и непрерывности бизнеса
3. Организация процессов обеспечения непрерывности бизнеса
4. Обеспечение непрерывности и качества функционирования информационных систем за счет формализации и привязки бизнес-процессов к информационным технологиям
5. Создание политики и назначение ответственных в области непрерывности и качества информационных систем
   - отражение информационных систем соответствия выполнения функций информационных систем обеспечению конкретных бизнес-процессов
   - описание информационных систем требований к стандартизации и унификации

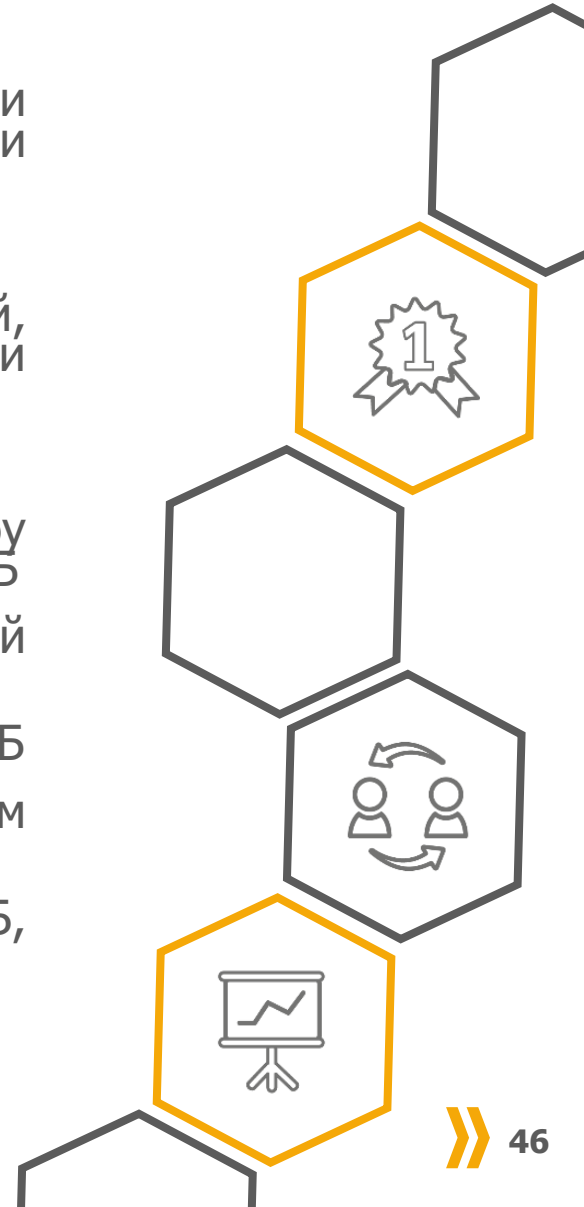
ФУНКЦИИ СЛУЖБЫ ИБ (В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИБ)

USSC

1. Разработка Политики ИБ
2. Контроль осуществления работниками кредитной организации мероприятий в области обеспечения информационной безопасности и защиты информации
3. Осуществление планирования и контроля процессов обеспечения ИБ
4. Разработка предложений по совершенствованию процессов обеспечения ИБ
5. Составление отчетов по обеспечению ИБ и направление их должностному лицу, ответственному за обеспечение ИБ
6. Осуществление других функций, связанных с обеспечением ИБ, предусмотренных внутренними документами кредитной организации
7. Проведение ежегодного тестирования на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры в соответствии с требованиями, изложенными в Положении 683-П
8. Проведение независимой оценки соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации в соответствии с требованиями, изложенными в Положении 683-П

ФУНКЦИИ СЛУЖБЫ ИБ (В ЦЕЛЯХ УПРАВЛЕНИЯ РИСКОМ ИБ)

1. Соблюдение процедур управления операционным риском, в части идентификации, сбора и регистрации информации о событиях риска ИБ и потерях в базе событий, мониторинга риска ИБ
2. Ведение базы событий риска ИБ
3. Участие в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ
4. Оценка эффективности управления риском ИБ
5. Составление отчетов по событиям риска ИБ и направление их в службу управления рисками и должностному лицу, ответственному за обеспечение ИБ
6. Осуществление мониторинга сигнальных и контрольных значений контрольных показателей уровня риска ИБ
7. Участие в разработке внутренних документов в области управления риском ИБ
8. Информирование работников кредитной организации по вопросам, связанным с управлением риском ИБ
9. Осуществление других функций, связанных с управлением риском ИБ, предусмотренных внутренними документами кредитной организации



СНИЖЕНИЕ РАСХОДОВ ЗА СЧЕТ УПРАВЛЕНИЕ ОПЕРАЦИОННЫМ РИСКОМ

USSC

СНИЖЕНИЕ ПРЯМЫХ РАСХОДОВ

Определение достаточности капитала, учёт расходов на операционный риск	Формализация операционных рисков	Формализация процессов и процедур	Унифицированная СОИБ	Улучшение операционной эффективности
Оценка достаточности капитала Оценка уровня риска на основе прогнозируемых значений Формирование избыточной ликвидности	Идентификация рисков Прогнозирование рисков Подбор метрик Классификация событий Моделирование угроз	Формирование состава и описание процессов Формирование состава и описание процедур и мероприятий	Организация СОИБ на основе модели угроз	Оценка уровня риска на основе событий Снижение уровня риска за счет унификации Снижение уровня риска за счет принятых мер Переоценка избыточной ликвидности

НАШИ ПРЕДЛОЖЕНИЯ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

USSC

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 требованиям регуляторов

Автоматизация процессов ИБ в организации

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**

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

О КОМПАНИИ

Опыт

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

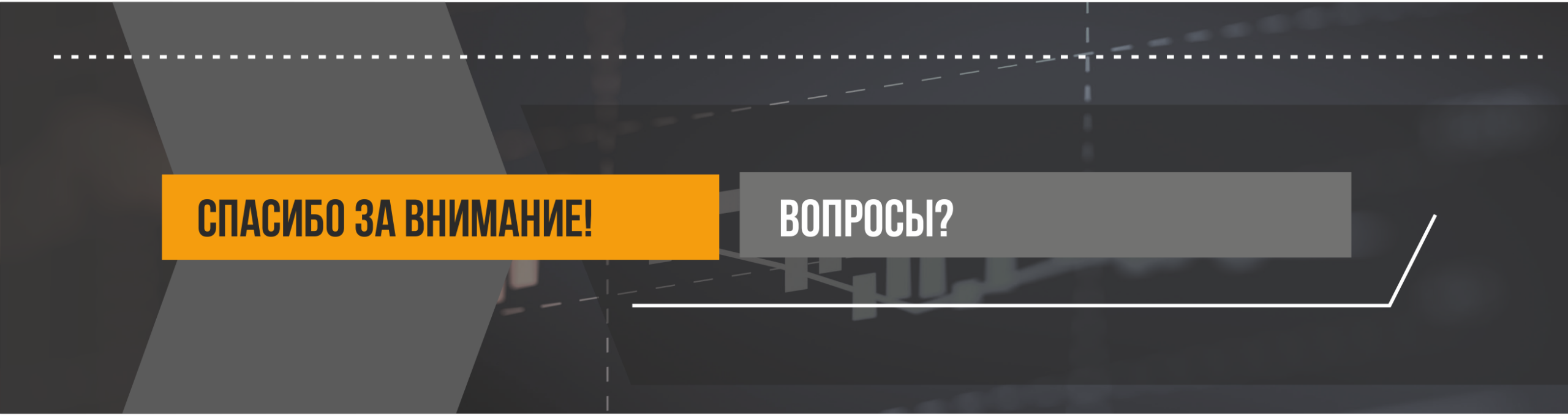
Сертификации

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 Information Security Manager (CISM)
- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Computer Hacking Forensic Investigator (CHFI)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Web Expert (OSWE)

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

USSC



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Сергей Борисов

Заместитель руководителя по ИБ обособленного подразделения УЦСБ

sborisov@ussc.ru

Олег Батурин

Аналитик

Аналитический центр УЦСБ

obaturin@ussc.ru

Ксения Кузнецова

Аналитик

Аналитический центр УЦСБ

kkuznecova@ussc.ru