03/2022

ПОЛОЖЕНИЕ ЦБ РФ №716-П

ЧТО УЖЕ ТРЕБУЮТ И БУДУТ ТРЕБОВАТЬ ОТ БАНКОВ?

ПОЛОЖЕНИЯ БАНКА РОССИИ

- Банки
- Небанковские кредитные организации

№716-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

01 октября 2020 г. — Вступило в силу

01 января 2022 г. — Срок приведения в соответствие требованиям Положения

Положение описывает:
- порядок управления рисками
- **требования к управлению риском ИБ и ИС**
- и другое

Проект положения
«Об обязательных для кредитных организаций требованиях к операционной надёжности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»

01 октября 2022 г. — Вступает в силу

2023 – 2024 г. — Сроки приведения в соответствие требованиям Положения пока не определены

Положение устанавливает требования:
- К допустимому времени простоя процессов
- К обеспечению операционной надёжности
- К информированию Банка России о выявленных инцидентах операционной надёжности

Проект ГОСТ
«Управления риском реализации информационных угроз и обеспечение операционной надежности»

Стандарт определяет **требования** к составу и содержанию мер по управлению **риском реализации информационных угроз и обеспечение операционной надежности**

ПОЛОЖЕНИЕ № 716-П «О ТРЕБОВАНИЯХ К СИСТЕМЕ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМ РИСКОМ»

ОПЕРАЦИОННЫЕ РИСКИ

Операционный риск (ОР) — риск возникновения убытков в результате ненадежности и недостатков внутренних процедур управления **кредитной организации (КО)**, отказа информационных и иных систем, либо вследствие влияния на деятельность КО внешних событий

РИСКИ ИБ

РИСКИ ИС

Риск ИБ — риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения ИБ, в том числе применения технологических и других мероприятий, недостатками прикладного ПО АС и приложений, а также несоответствия указанных процессов деятельности КО

Риск ИС — риск отказов и (или) нарушения функционирования применяемых КО ИС и (или) несоответствия их функциональных возможностей и характеристик потребностям КО

ПОЛОЖЕНИЕ № 716-П
«О ТРЕБОВАНИЯХ К СИСТЕМЕ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМ РИСКОМ»

РИСК ИБ — риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспеч ИБ, в том числе применения технологических и мероприятий, недостатками прикладного ПО АС и приложений, а также несоответствия указанных процессов деятельности КО

ОПЕРАЦИОННЫЙ РИСК (ОР) — риск возникновения убытков в результате ненадежности и недостатков внутренних процедур управления **кредитной организации (КО)**, отказа информационных и иных систем, либо вследствие влияния на деятельность КО внешних событий

РИСК ИС — риск отказов и (или) нарушения функционирования применяемых КО ИС и (или) несоответствия их функциональных возможностей и характеристик потребностям КО

ПРОЕКТ ПОЛОЖЕНИЯ

«ОБ ОБЯЗАТЕЛЬНЫХ ДЛЯ КРЕДИТНЫХ ОРГАНИЗАЦИЙ ТРЕБОВАНИЯХ К ОПЕРАЦИОННОЙ НАДЁЖНОСТИ»

ПРОЕКТОМ УСТАНАВЛИВАЮТСЯ ТРЕБОВАНИЯ

- По операционной надёжности технологических процессов (допустимого времени простоя, доли деградации) Преимущественно 2 часа для Банков и НКО
- К обеспечению операционной надёжности
- К описанию деятельности для обеспечения операционной надёжности
- **К** информированию ЦБ РФ о выявленных инцидентах операционной надёжности

Операционная надёжность — способность Банка обеспечить непрерывность функционирования критически важных процессов в случае возникновения рисков ИС и ИБ

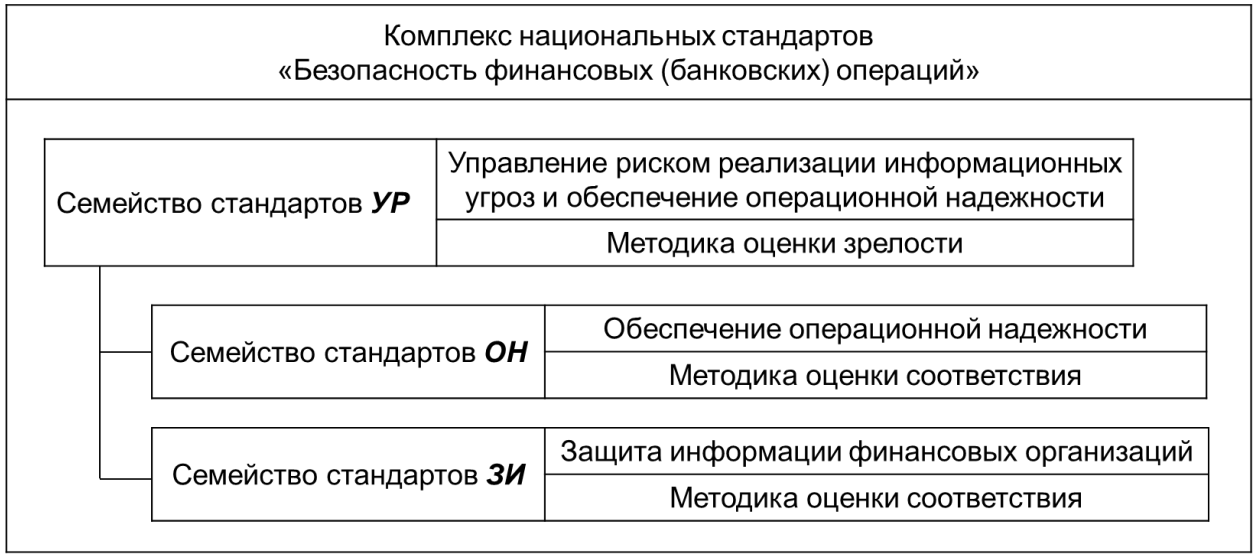
КАКИЕ ТРЕБОВАНИЯ ПО ДОСТУПНОСТИ?

Проект положения «Об операционной надёжности» выдвигает требования по доступности:

Технологический процесс (сокращённо)	Допустимое время простоя
Денежные переводы ФЛ и ЮЛ	2 часа
Открытие и ведение счетов	2 часа
ДБО, онлайн-банкинг	2 часа
Кассовые операции	2 часа
Размещение и обновление биометрических персональных данных	0,5 часа
Выполнение операций на финансовых рынках	24 часа

Наш опыт говорит о том, что данные показатели часто не выдерживаются

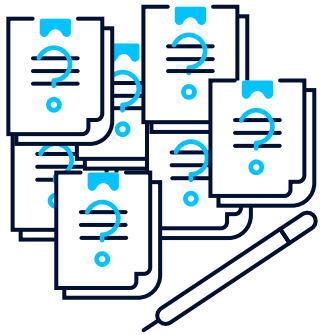
ПРОЕКТ ГОСТ «УПРАВЛЕНИЯ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ»



- Структура документа похожа на хорошо знакомый многим подразделениям ИБ в кредитных и не кредитных организаций на ГОСТ 57580.1-2017\57580.2-2018
- Требования (Организационные «О» и Технические «Т») установлены для трех уровней
- Данный документ дублируют требования из других НПА ЦБ РФ
- Подготовлен проект стандарта ГОСТ по операционной надежности. Базовый состав организационных и технических мер

- Документ содержит требования, которые разделены на 4 направления (цикл PDCA)
- Будут подготовлены методики оценки зрелости и соответствия по данному стандарту

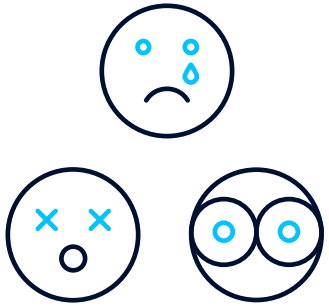
СЛОЖНОСТИ ИСПОЛНЕНИЯ ТРЕБОВАНИЙ



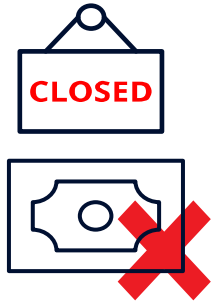
БОЛЬШОЙ ОБЪЁМ ТРЕБОВАНИЙ
Больше 100 требований
в 716-П и проектах положений

НЕОБХОДИМОСТЬ АНАЛИЗА
СООТВЕТСТВИЯ ИТ И ИБ

БОЛЬШОЙ ОБЪЁМ
ДОКУМЕНТАЦИИ
Более **40** документов согласно
716-П и проекту Положения



ОГРАНИЧЕННЫЙ
СРОК ПРИВЕДЕНИЯ В СООТВЕТСТВИЕ



САНКЦИИ: СОГЛАСНО ИНСТРУКЦИИ
БАНКА РОССИИ №188-И

ЧЕМ МОЖЕТ ПОМОЧЬ ДЖЕТ?

«ИНФОСИСТЕМЫ ДЖЕТ» ВЫПОЛНЯЕТ ПОЛНЫЙ СПЕКТР УСЛУГ ПО РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ЦБ РФ

1 ЭТАП — ОБСЛЕДОВАНИЕ ТЕКУЩЕГО СОСТОЯНИЯ

2 ЭТАП — ПОДГОТОВКА ВСЕЙ ДОКУМЕНТАЦИИ

3 ЭТАП — ДОРОЖНАЯ КАРТА ПРОЕКТОВ

4 ЭТАП — ПОДДЕРЖКА ИНФРАСТРУКТУРЫ

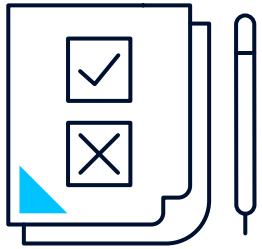
5 ЭТАП — АВТОМАТИЗАЦИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ РИСКАМИ ИБ

6 ЭТАП — ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ИБ

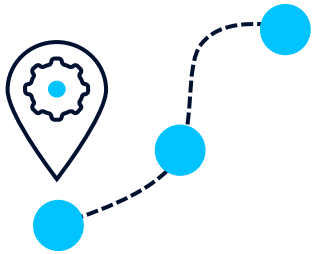
7 ЭТАП — ОКАЗАНИЕ КОНСУЛЬТАЦИОННОЙ ПОДДЕРЖКИ

ЧЕГО МЫ ДОСТИГНЕМ?

Готовый набор документации



Реальная картина соответствия требованиям



Дорожная карта проектов

Выполнение требований ЦБ!

Всё это при минимальных трудозатратах сотрудников Банка

ВОПРОСЫ И ОБСУЖДЕНИЕ

ВОПРОСЫ?

ОПЫТ БАНКОВ В РЕАЛИЗАЦИИ ТРЕБОВАНИЙ?

ТЕСТ

ПРОВЕРЬТЕ СВОЙ БАНК!

ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

ВЫХОДНЫЕ РЕЗУЛЬТАТЫ ГЛАВ 1-6

Документ	Результат
Политика по управлению ОР	Актуализация верхнеуровневой политики по управлению ОР
Классификатор событий ОР	Разработка перечня источников операционного риска, типов событий ОР, направлений деятельности, в том числе в разрезе составляющих их процессов, и видов потерь от реализации ОР
Порядок/методология оценки уровня ОР	Разработка порядка проведения количественной и качественной оценки общего уровня ОР, системы показателей уровня ОР
Методология определения потерь (прямых / непрямых) и возмещения	Разработка порядка, содержащего способы и источники определения прямых и непрямых потерь по событиям ОР и описание источников и определение сумм возмещений по событиям ОР
Методология по КИР	Разработка порядка и критериев определения БП для установления КИР, способов и периодичности их расчета, источников информации для КИР, исполнителей, составления перечня КИР
Порядок/методика проведения самооценки	Разработка порядка проведения самооценки ОР, включая опросные листы
Порядок/методика формирования отчетности	Разработка документа, описывающего формирование и заполнение отчетности, методологические рекомендации по расчету показателей, шаблоны форм отчетности
Порядок ведения базы событий ОР	Разработка порядка сбора информации по событиям ОР (требования к форме и содержанию вводимой информации, включая события ИБ и ИС), идентификации, определения потерь и возмещений по событиям ОР, порядка взаимодействия подразделений

МОДЕРНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 7 Положения 716-П требует наличие:

- Политики ИБ
- Процесса управления риском ИБ (и документа, определяющего порядок управления риском ИБ)
- Документа, определяющего порядок ведения базы событий риска ИБ
- Документа, определяющего выявление, идентификацию риска ИБ и его оценку, порядок реагирования на выявленные события риска ИБ и восстановления деятельности КО
- Документального закрепления участия руководства в решении вопросов управления риском ИБ и распределение функций и ответственности по ИБ
- Организации ресурсного (кадрового и финансового) обеспечения ИБ
- Повышения осведомленности в области противодействия угрозам ИБ
- Управления риском ИБ при передаче третьим лицам/использовании внешних информационных систем (ИС) и управление риском внутреннего нарушителя
- Обеспечения операционной надежности (в том числе при создании, эксплуатации, модернизации, снятии с эксплуатации ИС) в части управления изменениями, конфигурациями и уязвимостями
- Программ контроля, в том числе программ аудита

Требования на основе 683-П:

- Обеспечение осведомленности об актуальных угрозах ИБ, обмен информацией о событиях риска ИБ (в том числе об инцидентах ИБ и предоставление данных в Банк России) **(пункт 8 Положения 683-П)**
- Установление и реализация программ контроля, в том числе программ аудита, включая независимую оценку соответствия уровня защиты КО **(пункт 9 Положения 683-П)**
- Планирование, реализация, контроль и совершенствование комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ, в том числе в соответствии с реализуемыми уровнями защиты КО **(подпункт 3.1 пункта 3 Положения 683-П)**
- Выполнение требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств **(пункт 5 Положения 683-П)**
- Процессы применения прикладного программного обеспечения автоматизированных систем (ПО АС) и приложений **(пункт 4 Положения 683-П)**
- Ежегодное тестирование на проникновение и анализ уязвимостей ИБ **(подпункт 3.2 пункта 3 Положения 683-П)**
- Независимая оценка соответствия уровня защиты информации КО **(пункт 9 Положения 683-П)**

ТРЕБОВАНИЯ К СИСТЕМЕ УПРАВЛЕНИЕ РИСКОМ

ГЛАВА 8. УПРАВЛЕНИЕ РИСКОМ ИНФОРМАЦИОННЫХ СИСТЕМ

Политика ИС

- Функции и полномочия подразделений функционирования ИС
- Требования к ИС
- Порядок взаимодействия в рамках реализации политики информационных систем

Обеспечение качества функционирования ИС

- Структура информационных систем
- Стандартизация и унификация
- Надежность функционирования

Обеспечение качества данных в ИС

- Обеспечение качества данных

Обеспечение непрерывности функционирования ИС

- Условия эксплуатации
- Резервное копирование
- Процесс обеспечения непрерывности
- Оценка состояния ИТ-инфраструктуры
- Управление уязвимостями

и т.д.

ВЫХОДНЫЕ РЕЗУЛЬТАТЫ ГЛАВЫ 8 (1/2)

Область	Раздел положения 716-П	Требования раздела\Результат
Аудит ИТ-инфраструктуры заказчика	-	Внутренний документ о составе инфраструктуры заказчика
Общее требование	8,1	Требование к наличию внутренней документации\Документ не требуется
Политика ИС	8.2 - 8.6	Политика ИС
Общее требование	8.7	Требование к наличию внутренней документации\Документ не требуется
Структура Информационных систем	8.7.1	Архитектурная схема ИС*
Стандартизация ИТ-инфраструктуры	8.7.2	Политика стандартизации ИТ-инфраструктуры Политика классификации ИС Требования к квалификации работников
Надежность функционирования	8.7.3	Требования к надёжности функционирования ИС Требования к режимам функционирования ИС Перечень показателей надёжности функционирования
Обеспечение качества данных	8.7.4 - 8.7.6	Политика обеспечения качества данных Методика обеспечения качества данных Порядок обеспечения качества данных Техническое решение (если необходима автоматизация \ встраивание \ интеграция в общий процесс управления операционным риском)
Дополнительное\опциональное требование	8.7.7	Требование к наличию дополнительной документации (в случае необходимости, с учётом специфики ИС)
Политика ИС	8.7.8	Политика ИС

* Схема составляется для каждой критичной информационной системы

ВЫХОДНЫЕ РЕЗУЛЬТАТЫ ГЛАВЫ 8 (2/2)

Область	Раздел положения 716-П	Требования раздела\Результат
Общее требование	8.8	Требование к наличию внутренней документации\Документ не требуется
Описание связи разделов 8.8.1 и 7.7	8.8.1	Требование к наличию внутренней документации\Документ не требуется
Условия эксплуатации	8.8.2	Требования к обеспечению условий эксплуатации
Резервное копирование	8.8.3	Политика резервного копирования
Требование соответствия ПО разделу 8.7.2	8.8.4	Требование должно быть описано в документе раздела 8.7.2
Процесс обеспечения непрерывности	8.8.5	Политика и стратегия непрерывности
Аудит ИТ-инфраструктуры	8.8.6	Регламент внутренних аудитов ИТ-инфраструктуры и информационных систем
Порядок управления уязвимостями	8.8.7	Порядок управления уязвимостями
Политика ИС	8.8.8-8.8.13	Политика ИС

03/2022

ГОТОВЫ К СОТРУДНИЧЕСТВУ!