ФБК

Аудит | Консалтинг | Право

Обзор новых требований Банка России к организации операционной надежности при осуществлении банковской деятельности

Положение №787-П

Спикер

Положение Банка России от 12.01.2022 №787-П «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»: когда вступает в силу, на кого распространяется, цели и задачи, взаимосвязь с Положением Банка России №716-П.

Савицкая Майя

Менеджер

Департамент аудиторских и консультационных услуг финансовым институтам ФБК

Mayya.Savitskaya@fbk.ru

Спикер

Обзор Положения Банка России от 12.01.2022 №787-П

- Учет и контроль критичной архитектуры, ее защита. Тестирование готовности кредитной организации противостоять реализации информационных угроз в отношении критичной архитектуры с использованием результатов сценарного анализа.
- Обеспечение осведомленности об информационных угрозах и их нейтрализация.
- Мероприятия по обеспечению операционной надежности обязательные к осуществлению кредитными организациями.

Спикер

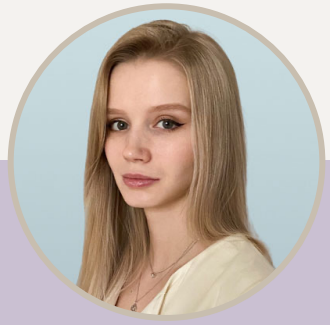
Манцуров Михаил

Консультант по ИТ
Департамент аудиторских и консультационных услуг финансовым институтам
ФБК

Спикер

Обзор Положения Банка России от 12.01.2022 №787-П

- Операционная надежность – как один из элементов системы управления операционным риском.
- Контрольные показатели уровня операционного риска как сигналы о нарушении функционирования технологического процесса.
- Требования к операционной надежности и их отражение в документах кредитной организации.
- Информирование Банка России о выявленных инцидентах операционной надежности и раскрытие информации о них.



Спикер

Русских Виктория

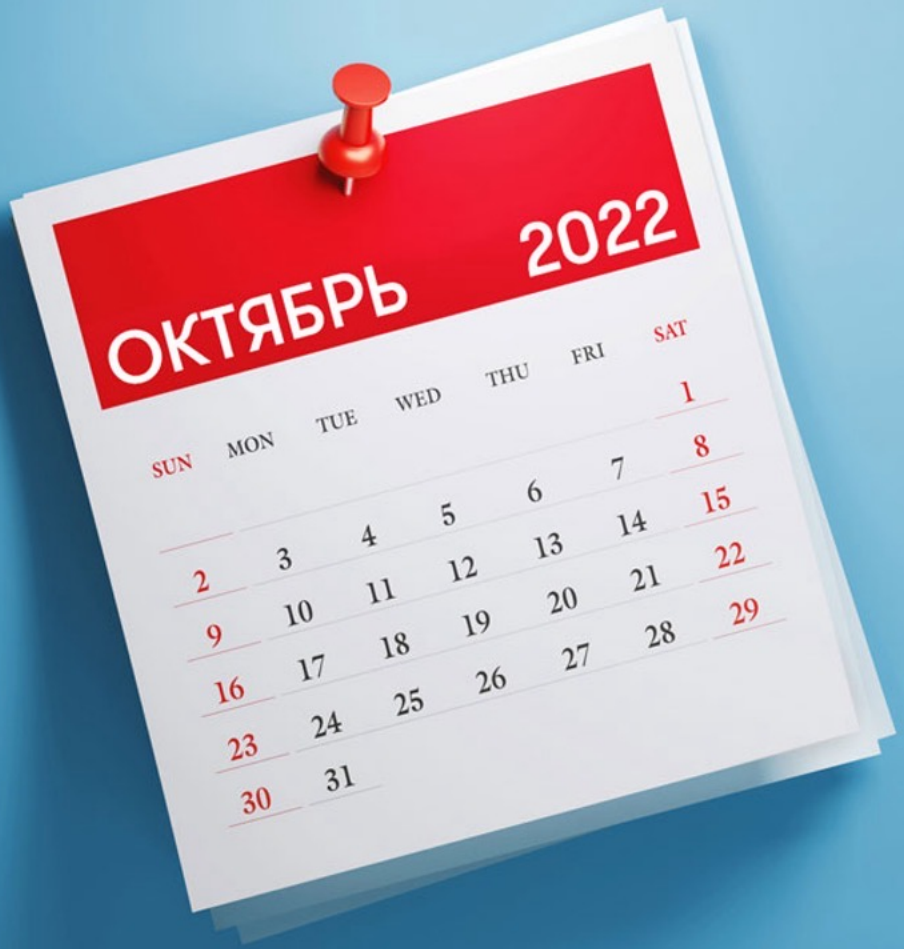
Старший эксперт
Департамент аудиторских и консультационных услуг финансовым институтам
ФБК

Положение БР от 12.02.2022 №787-П

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

ФБК

Вступает в силу



С 01 октября 2022 года

ФБК

На кого распространяется

Кредитные организации

За исключением

- **центрального контрагента** в значении, установленном пунктом 17 статьи 2 Федерального закона от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте»
- **центрального депозитария** в значении, установленном в статье 2 Федерального закона от 7 декабря 2011 года №414-ФЗ «О центральном депозитарии»

ФБК

Что регламентирует

Требования к операционной надежности при осуществлении банковской деятельности (далее — **требования к операционной надежности**)

ФБК

Цель регулирования

Обеспечение непрерывности оказания банковских услуг

ФБК

“

Особенности регулирования

С учетом требований к системе управления операционным риском, установленных Положением Банка России от 08.04.2020 № 716-П

«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

(далее — Положение № 716-П)

”

Процедуры, направленные на реализацию требований к операционной надежности, должны быть установлены во внутренних документах КО

С учетом требований пп 4.1.2, абзаца первого пп 4.1.3 и абзаца второго пп. 4.1.4 п. 4.1 Положения № 716-П

Политика управления операционным риском

Внутренние документы, описывающие процедуры управления операционным риском, а также процедуры оценки эффективности функционирования системы управления операционным риском

Требования к операционной надежности должны соблюдаться кредитными организациями при выполнении критически важных процессов

Критически важные процессы определены в пп 4.1.1 пункта 4.1 Положения № 716-П:

- обеспечивают выполнение операций КО указанных в п.1-4 и 9 части первой ст.5 Федерального закона "О банках и банковской деятельности"
  - привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);
  - размещение указанных в пункте 1 части первой настоящей статьи привлеченных средств от своего имени и за свой счет;
  - открытие и ведение банковских счетов физических и юридических лиц;
  - осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам;
  - осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов).
- ведение бухгалтерского учета,
- представление отчетности в Банк России в соответствии с Указанием БР от 08.10.2018 № 4927-У "О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации",
- поддержание ликвидности,
- выполнение операций на финансовых рынках,
- выполнение кассовых операций,
- работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций,
- соблюдение требований Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных",
- соблюдение Трудового кодекса Российской Федерации,
- другие процессы, которые определены КО и прерывание функционирования которых оказывает влияние на выполнение ее обязательств перед клиентами и контрагентами

ФБК

Необходимо определить для каждого технологического процесса и соблюдать целевые показатели операционной надежности

С учетом требований главы 5 Положения № 716-П:

Глава 5 устанавливает правила организации Системы контрольных показателей уровня операционного риска (КПУОР):

- Целевые значения КПУОР:
  - Сигнальное значение — значение показателя, при нарушении которого проводится ежедневный мониторинг значений показателя и реализация мер, направленных на устранение превышения фактического значения данного показателя над предельно допустимым значением
  - Контрольное значение — предельно допустимое значение показателя, при нарушении которого информация доводится до совета директоров (наблюдательного совета) и применяются меры реагирования

- Совет директоров (наблюдательный совет) КО
  - утверждает сигнальные и контрольные значения КПУОР на плановый годовой период, которые ежегодно подлежат пересмотру и актуализации

- Подразделение, ответственное за организацию управления операционным риском, оформляет расчет и обоснование сигнальных и контрольных значений КПУОР в виде заключения и включает его в состав материалов, направляемых им на рассмотрение коллегиальным исполнительным органом КО при утверждении (пересмотре) политики управления операционным риском.

ФБК

Инциденты операционной надежности должны регистрироваться в Базе событий ОР

С учетом требований главы 6 Положения № 716-П

Глава 6 «Ведение базы событий»

- Порядок ведения базы событий, включая требования к форме и содержанию вводимой информации, должен быть установлен во внутренних документах КО

- База событий ведется на постоянной основе.

- База событий имеет унифицированную структуру и регламентированные классификаторы событий

В ВНД КО предусматриваются дополнительные типы событий ОР при классификации инцидентов операционной надежности

С учетом требований п.3.7 Положения № 716-П

- Дополнительные типы событий операционного риска применяются в разрезе классификации типов событий:
  - преднамеренные действия персонала,
  - преднамеренные действия третьих лиц,
  - нарушение кадровой политики и безопасности труда,
  - нарушение прав клиентов и контрагентов,
  - ущерб материальным активам,
  - нарушение и сбои систем и оборудования,
  - нарушение организации, исполнения и управления процессами.

- Используется перечень типов инцидентов операционной надежности, размещаемого Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет»

По каждому инциденту операционной надежности в базе событий должна регистрироваться дополнительная информация

С учетом требований п.6.6 Положения № 716-П

- База событий имеет унифицированную структуру и регламентированные классификаторы событий

- Дополнительная информация:
  - данные, используемые для фиксации превышения установленных значений целевых показателей операционной надежности;
  - данные, позволяющие выявить причину превышения установленных значений целевых показателей операционной надежности;
  - результат реагирования на инцидент операционной надежности (о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитной организацией или Банком России инцидент операционной надежности).

Моделирование информационных угроз в отношении критичной архитектуры проводится с учетом требований к проведению качественной оценки уровня риска

С учетом требований пп 2.1.5 п.2.1 Положения № 716-П

- Качественная оценка уровня операционного риска, проводимая в отношении выявленных операционных рисков в дополнение к количественной оценке и включающая следующие способы:
  - самооценку операционного риска;
  - профессиональную оценку ;
  - сценарный анализ операционных рисков.
- Подразделение, ответственное за организацию управления операционным риском, разрабатывает на ежегодной основе план мероприятий по проведению качественной оценки уровня операционного риска, который утверждается коллегиальным исполнительным КО и включает определение ответственных и участвующих подразделений

Проведение с использованием результатов сценарного анализа тестирования готовности кредитной организации противостоять реализации информационных угроз

С учетом требований пп 2.15 пункта 2.1 Положения № 716-П:

- Сценарный анализ является одним из способов качественной оценки уровня операционного риска

- Подразделение, ответственное за организацию управления операционным риском, разрабатывает на ежегодной основе план мероприятий по проведению качественной оценки уровня операционного риска, который утверждается коллегиальным исполнительным КО и включает определение ответственных и участвующих подразделений

- Порядок проведения сценарного анализа операционных рисков определяется во внутренних нормативных документах КО

Во внутренних документах должны быть установлены критерии шкалы качественных оценок и методика определения оценок качественных потерь от реализации инцидентов операционной надежности

С учетом требований пп 3.13.2 п.3.13 Положения № 716-П

- Качественные потери включают в себя:
  - возникновение источников других видов риска (например, кредитного риска, рыночного риска, риска ликвидности, риска потери деловой репутации, регуляторного риска, стратегического риска);
  - приостановку деятельности в результате события операционного риска (например, технологического сбоя);
  - отток клиентов;
  - неисполнение обязательств по сделке и (или) неоказание услуги;
  - ограничения, приводящие к выполнению невыгодных для кредитной организации действий, накладываемые со стороны суда, исполнительных органов государственной власти, Банка России;
  - снижение качества предоставления услуг, выполнения операций (например, нарушение регламентированных сроков выполнения процессов и операций, установленных во внутренних документах кредитной организации);
  - утечку, потерю или искажение защищаемой, в том числе коммерческой, информации;
  - судебные акты (решения, определения, постановления), акты исполнительных органов государственной власти, Банка России, не связанные с уплатой штрафов;
  - снижение лимитов на межбанковское кредитование;
  - другие качественные потери.
- Оценка значимости качественных потерь проводится в соответствии с установленной в ВНД КО шкалой качественных оценок (например, по четырехуровневой шкале: "очень высокие", "высокие", "средние", "низкие").
- В ВНД КО устанавливается шкала качественных оценок и методика определения оценок для качественных потерь от реализации события операционного риска, включая критерии соотнесения шкалы качественных оценок с количественными потерями.

Учет результатов идентификации риска информационной безопасности, а также его оценки, проводимой в составе процедур управления операционным риском при планировании применения организационных и технических мер, направленных на реализацию требований к операционной надежности

С учетом требований глав 2 и 7 Положения № 716-П

Глава 2 «Процедуры управления операционным риском»

Глава 7 «Управление риском информационной безопасности»

Необходима корреляция с Политикой ИБ и Процедурами управления ОР, принятыми в КО.

Требования к взаимодействию с поставщиками услуг в сфере информационных технологий

С учетом требований главы 7 и 8 Положения № 716-П:

Глава 7 «Управление риском информационной безопасности»

Глава 8 «Управление риском информационных систем»

Поставщики услуг в сфере информационных технологий — третьи лица (внешние подрядчики, контрагенты, участники банковской группы), оказывающие услуги в сфере информационных технологий, связанные с выполнением технологических процессов.

Необходима корреляция с Политикой ИБ и Политикой ИС, принятыми в КО.

Целевые показатели операционной надежности

Целевые показатели операционной надежности. Часть 1

Допустимая доля деградации технологического процесса

- = количество банковских и иных операций, совершенных во время нарушений технологических процессов, приводящих к неоказанию или ненадлежащему оказанию банковских услуг / ожидаемое кол-во банковских и иных операций в случае непрерывного оказания банковских услуг
- Значение допустимой доли деградации технологических процессов должно рассчитываться на основании статистических данных за период 12+ мес.
- **В случае превышения допустимой доли деградации технологических процессов осуществляется фиксация:**
- фактического времени простоя и (или) деградации технологического процесса по каждому инциденту операционной надежности;
- фактической доли деградации технологического процесса в рамках отдельного инцидента операционной надежности;
- суммарного времени простоя и (или) деградации технологического процесса за последние 12 месяцев.

Целевые показатели операционной надежности. Часть 2

Допустимое время простоя и (или) деградации технологических процессов

- Значение данного показателя устанавливается не выше значений, предусмотренных Приложением к 787-П.

Допустимое суммарное время простоя и (или) деградации технологического процесса

- Рассчитывается за очередной календарный год.

Соблюдение режима работы (функционирования) технологического процесса

- Режим функционирования: время начала, время окончания, продолжительность и последовательность процедур в рамках технологического процесса.

! **Анализ необходимости пересмотра значений целевых показателей операционной надежности не реже одного раза в год.**

Требования к операционной надежности

Требования к операционной надежности. Часть 1

Целевые показатели операционной надежности

- Порядок определения целевых показателей;
- Требования к обеспечению контроля за соблюдением показателей.

Инциденты операционной надежности, восстановление технологических процессов

- Порядок выявления, регистрации и реагирования на инциденты операционной надежности;
- Порядок восстановления функционирования технологических процессов и объектов информационной инфраструктуры после реализации инцидентов операционной надежности;
- Требование к проведению анализа причин и последствий реализации инцидентов операционной надежности;
- Порядок взаимодействий подразделений кредитной организации в рамках настоящего процесса.

Требования к операционной надежности. Часть 2

Взаимодействие с третьими лицами

- Требования к управлению риском ИБ и риском ИС (главы 7 и 8 Положения Банка России № 716-П: п. 7.8, 8.7.2, 8.7.3);
- Нейтрализация информационных угроз, связанных с привлечением поставщиков услуг в сфере ИТ и обусловленных технологической зависимостью функционирования объектов информационной инфраструктуры от поставщиков.

Учет и контроль состава критичной архитектуры

- Технологических процессов;
- Подразделений и работников ответственных за функционирование технологических процессов и имеющих к ним доступ;
- Объектов информационной инфраструктуры;
- Технологических участков технологических процессов;
- Технологических процессов, технологических участков, реализуемых поставщиками услуг в сфере информационных технологий;
- Взаимосвязей и взаимозависимостей с другими организациями;
- Каналов передачи защищаемой информации.

Требования к операционной надежности. Часть 3

Управление изменениями критичной архитектуры

- Управление уязвимостями в критичной архитектуре;
- Планирование и внедрение изменений;
- Управление конфигурациями объектов информационной инфраструктуры;
- Управление уязвимостями и обновлениями объектов информационной инфраструктуры.

Тестирование операционной надежности технологических процессов

- Разработка и внедрение организационных и технических мер направленных на проведение сценарного анализа реализации информационных угроз в отношении критичной архитектуры и возникновения сбоев объектов информационной инфраструктуры с учетом требований подпункта 2.1.5 пункта 2.1 Положения Банка России N 716-П.
- Используя результаты сценарного анализа проводить тестирование готовности кредитной организации противостоять реализации информационных угроз в отношении критичной архитектуры

ФБК

Требования к операционной надежности. Часть 4

Нейтрализация информационных угроз

- Защита от несанкционированного использования предоставленных полномочий;
- Повышение осведомленности об информационных угрозах;
- Создание «дублирующего» персонала на критичных участках технологических процессов;
- Защита «удаленного» доступа сотрудников;
- Исполнение требований ФСТЭК при активах ≥ 500 млрд. руб. и отнесении к субъектам критичной информационной инфраструктуры.

Обязанности кредитных организаций в рамках обеспечения операционной надежности

- Моделировать информационные угрозы;
- Планировать, реализовать и контролировать соблюдение требований к операционной надежности;
- Определить в нормативных документах порядок ведения базы событий;
- Провести классификацию типов инцидентов операционной надежности;
- Регистрировать инциденты операционной надежности дополнительно включая исходные данные, причину и результаты реагирования на инцидент;
- Регламентировать критерии шкалы качественных оценок и методику определения оценок качественных потерь при невозможности определении их в денежном выражении.

Определение требований 787-П в ВНД

Пункт 787-П	Содержание	Определение в ВНД кредитной организации
П. 9	• Процедуры, направленные на выполнение требований к операционной надежности и порядок их пересмотра; • Взаимодействие подразделений кредитной организации, участвующих в соблюдении требований к операционной надежности; • Порядок осуществления контроля за соблюдением требований к операционной надежности в рамках СВК; • Выделение ресурсного обеспечения.	«Политика управления операционным риском» *и/или* «Политика обеспечения операционной надежности в целях обеспечения непрерывности оказания банковских услуг»
П. 6	**Требования к операционной надежности:** • Целевые показатели операционной надежности (определение, контроль); • Критичная архитектура (идентификация элементов); • Управление изменениями критичной архитектуры; • Инциденты операционной надежности и восстановление выполнения технологических процессов и функционирования объектов информационной инфраструктуры; • Взаимодействие с третьими лицами; • Тестирование операционной надежности; • Нейтрализация информационных угроз со стороны НСД к объектам информационной инфраструктуры; • Обеспечение осведомленности кредитной организации об актуальных информационных угрозах.	«Политика обеспечения операционной надежности в целях обеспечения непрерывности оказания банковских услуг» *и/или* «Требования к операционной надежности в целях обеспечения непрерывности оказания банковских услуг» Со ссылками на иные документы Банка: • Документы по управлению рисками; • Документы в области обеспечения ИБ; • Документы в рамках 716-П.
П. 2, 3, 4, 5	Может быть детализирующим документом к Требованиям к операционной надежности. • Перечень показателей, порядок и методика оценки, пороговые значения, порядок актуализации.	«Методика оценки показателей операционной надежности»

Информирование Банка России

Кредитные организации в рамках обеспечения операционной надежности должны информировать Банк России:

- о выявленных инцидентах операционной надежности (в случае превышения допустимой доли деградации технологических процессов), а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитной организацией или Банком России инцидент операционной надежности;
- о планируемых мероприятиях по раскрытию информации, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на своих официальных сайтах в сети "Интернет", в отношении указанных в абзаце втором настоящего пункта инцидентов операционной надежности не позднее одного рабочего дня до дня проведения мероприятия.

ФБК

Аудит | Консалтинг | Право

Спасибо за внимание!

ул. Мясницкая, 44/1,
Москва, Россия 101990

T: (495) 737 5353
Ф: (495) 737 5347
E: fbk@fbk.ru

fbk.ru

fbk-pravo.ru