Ответы специалистов ФБК на вопросы участников вебинара от 16.06.2022

«Обзор новых требований Банка России к организации операционной надежности, вводимых Положением 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».

№	Вопрос участника	Ответ специалистов ФБК
1.	Подскажите, пожалуйста, на ваш взгляд, распространяются ли требования Положения 787-П на центрального контрагента при осуществлении банковской деятельности?"	В п.1. Положения БР №787-П установлено что выполнять установленные настоящим Положением требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг обязаны все 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». Подходы Регулятора к показателям операционной надежности центрального контрагента установлены в Главе 3 Положение Банка России от 30.12.2016 №575-П"О требованиях к управлению рисками, правилам организации системы управления рисками, клиринговому обеспечению, размещению имущества, формированию активов центрального контрагента, а также к кругу лиц, в которых центральный контрагент имеет право открывать торговые и клиринговые счета, и методике определения выделенного капитала центрального контрагента". Также требования операционной надежности центрального контрагента Положение Банка России от 15.11.2021 №779-П "Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)", в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)", которое вступает в силу с 01.10.2022.

2	Коллеги, если можно, дайте пожалуйста ссылку на комментарии ЦБ по 787-П."	Даем сноской к настоящим Ответам на вопросы [i] (далее – «Разъяснения»)
	ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ	
3	Относятся ли процессы оформления банковских продуктов к технологическим процессам открытия ведения банковских счетов. Имелись ввиду процессы взаимодействия с клиентами при оформлении кредитных продуктов. Там также открываются счета. Вопрос - относятся ли эти процессы к обозначенным технологическим в списке"	В своих Разъяснения Регулятор делает акцент на то, что *«Указанные в приложении технологические процессы императивно установлены и не могут носить характер рекомендательных. Вместе с тем кредитная организация может самостоятельно дополнить указанный перечень с учетом своей системы управления операционными рисками. …Требования к определению перечня критически важных процессов установлены в Положении Банка России от 08.04.2020 N 716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе"»* (далее - Положение БР N 716-П).» Согласно п.2 Положения БР 787-П кредитные организации в рамках обеспечения операционной надежности должны обеспечить непревышение значения порогового уровня допустимого времени простоя и (или) нарушения технологических процессов, обеспечивающих выполнение критически важных процессов. Таким образом, полагаем что список технологических процессов находится в прямой корреляции с пониманием критически важных процессов в КО и его построение базируется на списке таких процессов. На наш взгляд определение Технологических процессов целесообразно проводить используя утвержденный в КО Перечне ИС по критически важным процессам заложенный в Политику ИС.
4	"Под ""ведением счетов"" в списке технологических процессов подразумевается только РКО или любое открытие счета?"	
5	В Приложении 1 787-П одним из технологических процессов значится (п.6) технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц. Вопрос: относятся ли процессы открытия счетов в рамках оформления банковских продуктов (карты, кредиты наличными, ипотека и т.д.) к этой категории?	
6	Как по Вашему мнению технологический процесс = бизнес-процессу?	Согласно Разъяснениям БР *«Определение технологического процесса планируется ввести указанием Банка России "О внесении изменений в Положение Банка России N 716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе"».* Следуя Википедии [ii] Технологический процесс — это система взаимосвязанных действий, выполняющихся с момента возникновения исходных данных до получения нужного результата. Технологическая операция – это наименьшая часть технологического процесса, обладающая всеми его свойствами. Согласно п.2 Положения 787-П перечень технологических процессов, обеспечивающих выполнение критически важных процессов
7	"Коллеги, где найти определение технологического процесса?"	
8	Подскажите пожалуйста, что является операцией в технологическом процессе на ваш взгляд?"	
9	Технологический процесс вмещает в себя несколько бизнес-процессов. Правильно ли декомпозировать пороговый уровень деградации / простоя технологического процесса на каждый из составляющих его бизнес-процессов?	

		приводящих к неоказанию или ненадлежащему оказанию банковских услуг указан в Приложении к Положению. Вместе с тем в своих Разъяснения Регулятор делает акцент на то, что *«Указанные в приложении технологические процессы императивно установлены и не могут носить характер рекомендательных. Вместе с тем кредитная организация может самостоятельно дополнить указанный перечень с учетом своей системы управления операционными рисками. …Требования к определению перечня критически важных процессов установлены в Положении Банка России от 08.04.2020 N 716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе" (далее - Положение Банка России N 716-П).»* Обращаем внимание, что в пп.5.2. Положения Банка России от 17.04.2019 №683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента" установлено понятие технологического участка, которые п.6.1. Положения №787-П трактует как технологические участки технологического процесса, а именно • идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций; • формирование (подготовка), передача и прием электронных сообщений; • удостоверение права клиентов распоряжаться денежными средствами; • осуществление банковской операции, учет результатов ее осуществления; • хранение электронных сообщений и информации об осуществленных банковских операциях. В настоящий момент Положение №787-П не содержит требования о необходимости установления порогового уровня деградации для технологических участков технологического процесса.
10	Как по Вашему мнению технологический процесс = бизнес-процессу? В соответствии с Приложением 787-П установлены пороговые уровни допустимого времени простоя для технологического процесса. Для	В приведенном Вами примере 2 разных бизнес-процесса, для выполнения которого функционирует отдельный технологический процессом, как взаимосвязь отдельных действий (людей и, что важнее

	каждого технологического процесса должны быть установлены контрольные показатели уровня операционного риска. Однако, если для примера взять ТП Привлечение денежных средств во вклады, то в банке реализованы бизнес-процессы привлечения в офисе, которые выполняются 5 дней в неделю с 9 до 17, и привлечение через ДБО - 24/7. Как устанавливать значение контрольных показателей в этом случае???"	ИС (за надежностью которых мы и следим)), выполняющихся с момента возникновения исходных данных (обращения клиента за услугой) до получения нужного результата (получения услуги клиентом). Да, часть этих действия будет похожа, но часть будет уникальна для каждого технологического процесса (ТП). И необходимое время (режим) работы каждого их двух ТП в Вашем примере для обеспечения его непрерывности требуется разное, соответственно и интервалы «неработы», которые будут трактоваться как деградация и простой ТП будут различны. По Разъяснениям Регулятора КО необходимо установить самостоятельно *значения целевого показателя операционной надежности: "показателя соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса)". Таким образом, операционная надежность технологических процессов рассматривается только относительно установленного режима работы.* Таким образом, в Вашем примере, целесообразно для каждого из ТП (привлечение в офисе и привлечение через ДБО) установить свои целевые показатели операционной надежности.
	ЦЕЛЕВЫЕ ПОКАЗАТЕЛИ НАДЕЖНОСТИ	
11	Правильно мы понимаем, что целевые показатели операционной надёжности - это частный пример КПУР, требования к которым установлены в главе 5 716-П, а значит и должны управляться как КПУР?"	Да, мы понимаем также. Согласно Разъяснениям БР «*Контрольные показатели уровня операционного риска для целей обеспечения операционной надежности (целевые показатели операционной надежности) входят в систему контрольных показателей уровня операционного риска, требования к которой установлены главой 5 Положения Банка России N 716-П. Установление целевых показателей операционной надежности вне приложения 1 к Положению Банка России N 716-П обусловлено целесообразностью отражения ключевых требований к операционной надежности в рамках одного нормативного акта».*
12	Приведите пример расчета целевых показателей операционной надежности в рамках ТП"	БР в своих Разъяснениях указывает что *«расчет сигнальных и контрольных значений контрольных показателей уровня*

		операционного риска в части операционной надежности кредитные организации осуществляют самостоятельно (для показателя "допустимое время простоя и (или) деградации технологического процесса" должен быть учтен пороговый уровень, установленный в приложении к Положению №787-П). Проведение анализа необходимости пересмотра осуществляется в целях фиксации решения относительно необходимости или отсутствия необходимости изменения значений целевых показателей операционной надежности.» Согласно Положению №787-П значения допустимой доли деградации технологических процессов должно рассчитываться кредитной организацией на основании статистических данных за период не менее двенадцати календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности, а в случае если технологический процесс функционирует менее двенадцати календарных месяцев, - на основании статистических данных за период с даты начала его функционирования и (или) иных данных, обосновывающих их определение (по выбору кредитной организации). Также Регулятор не исключает применение экспертного мнения специалиста Банка при установлении таких значений. Целевые значения показателей- контрольное и сигнальное- устанавливаются в той же парадигме что и контрольные показатели уровня операционного риска (КПУОР), описанной в Главе 5 Положения БР № 716-П и целесообразно чтобы процентовки по ним соответствовали тем процентовкам которые заложены к отношении КРУОР в Политике управления операционным риском КО (обычно в рыночной практике это 85 и 90% от допустимого (порогового) значения. Исходя из нашей практики возможно применение методики расчета доступности – длительность прерывания технологического процесса не более 30 минут в год. Процент не осуществленных операций – не более 0,5% от среднегодового показателя и т.д. Но более «правильные» значения банк получит только проведя статистическое исследвание как предлагает Банка России.
13	Существуют ли рекомендации по расчету доли деградации технологического процесса и других целевых показателей операционной надежности?	Согласно Разъяснениям БР *«В Расчет фактической доли деградации технологического процесса должен проводиться исходя из*

		фактического и ожидаемого количества финансовых операций. Определение ожидаемого количества финансовых операций должно осуществляться организацией с учетом статистических данных и (или) иных данных по выбору кредитной организации». Т.е. регулятор не дает конкретных рекомендаций, предполагая, что кредитные организации самостоятельно разработают методику расчета. На наш взгляд помимо статистических наблюдений как было описано в предыдущем пункте, целесообразно использовать экспертное мнение владельцев/участников технологических процессов о «приемлемой» доле деградации. Также, полагаем, полезным инструментарием будут результат сценарного анализа и шкала перевода качественной оценки от реализации инцидентов операционной надежности в количественную, тогда инциденты с оценкой значимости потерь «очень высокие» и «высокие» можно будет включить в определении доли деградации.
	ИНЦИДЕНТЫ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ	
14	"Понятие инцидент операционной надёжности включает в себя инциденты, связанные 1) со сбоями, деградацией информационных систем банка? 2) со сбоями у партнёров (например, нспк, сбп, интернет-провайдеры)?"	Согласно п.3 Положения №787-П инцидент операционной надежности это нарушений технологических процессов, приводящих к неоказанию или ненадлежащему оказанию банковских услуг (деградация технологического процесса (технологических процессов), в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к неоказанию или ненадлежащему оказанию банковских услуг. Согласно Разъяснениям БР «*к инцидентам операционной надежности относятся случаи простоя и (или) деградации технологических процессов как в результате реализации операционного риска, обусловленного источниками риска, относящимися к категории "сбои систем и оборудования", так и в результате реализации киберриска.»* Приведенные Вами примеры – это примеры причин/источников возникновения инцидента, для которых Регулятор дает унифицированные классификаторы. При классификации инцидента операционной надежности используется как классификаторы регламентированные в Главе 3 и

		Приложении 5 Положения БР № 716-П, так и п.3.7 Положения БР №787-П. В классификаторах Регулятора содержатся как внутренние так и внешние источники оперриска, типы событий оперриска. У одного и того же события операционного риска может быть один источник или несколько источников операционного риска. Так в Ваших примерах, источниками возникновения инцидента операционного риска может быть сочетание таких источников как «сбои систем и оборудования» и «внешние причины» и/или «сбои систем и оборудования» и «действия персонала и других связанных с кредитной организацией лиц»
15	Как Вы считаете, будет ли Банк России требовать от кредитных организаций ведение учета операционных рисков в промышленном ПО, а не в табличном редакторе Exel"	Ни Указание БР 3624-У, ни Положение БР №716-П не содержат требования об ограничении ведения учета операционных рисков в промышленном ПО. Согласно п.6.2. Положения БР №716П кредитные организации самостоятельно устанавливают и отражают в ВНД порядок ведения базы событий, включая требования к форме и содержанию вводимой информации. П.6.19 Положения №716-П говорит о том, что *«в случае корректировки значения потерь и возмещений в базе событий предыдущее значение потерь кредитной организацией (головной кредитной организацией банковской группы) не исправляется, а добавляется новая информация с новым значением (должна быть обеспечена сохранность предыдущих значений)»* Также в п.6.20 повторяется что «*Кредитная организация (головная кредитная организация банковской группы) обеспечивает сохранность всех записей в базе событий».* По нашему мнению, обеспечить эти условия возможно и в продвинутых версиях инструментария Excel
16	П. 6.19 в 716-п требует обеспечение сохранности данных предыдущих значений, поэтому косвенно в 716-п отражено требование к ведению БД событий ОР в специализированных программах."	
	ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ	
17	Как лучше ,на ваш взгляд, организовать процесс внедрения: со стороны ИТ/ИБ или со стороны СУОР?"	Уверены что только в полном симбиозе и плотном сотрудничестве всех трех подразделений! Обращаем внимание, что согласно п.1.3. Положения БР №716-П подразделение, ответственное за организацию управления
18	Кто в системе управления операционными рисками должен быть ключевым?	

		операционным риском является подразделением, ответственным за организацию управления операционным риском в целом в кредитной организации. Риск ИС и риск ИБ, лишь элементы системы рисе-менеджмента оперриска, соответственно ИТ/ИБ – как специализированные подразделения специализированные подразделения в рамках функциональных обязанностей выполняют процедуры управления операционным риском. ИТ/ИБ дают фактуру по целевым показателям операционной надежности, а СУОР методологически встраивает их Политику ОР и иные процедурные документы по ОР. Определение Технологических процессов целесообразно проводить совместно, базируясь на утвержденном в КО Перечне ИС по критически важным процессам заложенным в Политику ИС.
19	А возможно ли требования к операционной надежности прописывать не в отдельном документе, а к примеру, в уже существующем положении по операционном риску? Учитывая что они взаимосвязаны."	Согласно п.9 Положения №787-П кредитные организации должны установить во внутренних документах, предусмотренных подпунктом 4.1.2, абзацем первым подпункта 4.1.3 и абзацем вторым подпункта 4.1.4 пункта 4.1 Положения Банка России № 716-П, описание процедур, направленных на реализацию требований к операционной надежности. Это такие документы как: • Политика управления операционным риском • Внутренние документы, описывающие процедуры управления операционным риском, а также процедуры оценки эффективности функционирования системы управления операционным риском. • Внутренние документы, устанавливающие в кредитной организации (головной кредитной организации банковской группы) структуру и организацию системы управления операционным риском, в том числе полномочия и функции руководителей подразделения, ответственного за организацию управления операционным риском, специализированных подразделений, центров компетенций с учетом исключения конфликта интересов. • Внутренние документы устанавливающие уполномоченное подразделение, а также правила привлечения для оценки эффективности функционирования системы управления операционным риском внешних экспертов. Соответственно, полагаем, что включение регламентации выполнения КО требований к операционной надежности в уже существующий в КО

		пул ВНД по управлению оперриском достаточно, и нет целесообразности создавать новый класс ВНД.
20	Необходимо ли добавить информацию об инцидентах операционной надежности в годовую отчетность Банка ВПОДК (в раздел отчетность об управлении операционным риском)?	В настоящее время в указании 3624-У, содержащем требования к наполнению отчетности по ВПОДК таких требований нет. Полагаем что данная информация должна включаться в отчетность по оперрискам формируемую для органов управления кредитной организации на основании п.4.2.2. Положения Банка России №716-П, в том числе, например, для атрибута • о результатах процедуры качественной оценки уровня операционного риска – включаются результаты сценарного анализа тестирование готовности кредитной организации противостоять реализации информационных угроз в отношении критичной архитектуры; • о фактических значениях контрольных показателей уровня операционного риска – фактические значения целевых показателей операционной надежности
	ПЕРЕСЕЧЕНИЕ 787-П и ОНиВД	
21	В Плане ОНиВД Банк ранее определил перечень критически важных процессов, ответственных за процесс, а также сроки восстановления процесса. Необходимо ли пересматривать План ОНиВД в связи с внедрением 787-П - в части Перечня критически важных процессов и сроков их восстановления?	Согласно Разъяснениям БР при выполнении требований Положения Банка России N 242-П в рамках плана ОНиВД допустимо формировать перечень критически важных процессов, совпадающий с перечнем технологических процессов, указанных в приложении к Положению 787-П. Вместе с тем Регулятор делает акцент что указанные в приложении технологические процессы императивно установлены и не могут носить характер рекомендательных. Вместе с тем кредитная организация может самостоятельно дополнить указанный перечень с учетом своей системы управления операционными рисками.
22	Учитывать ли в определении инцидентов операционной надежности инциденты, произошедшие в чрезвычайной ситуации (ЧС в терминологии ОНиВД)?	Такие инциденты напрямую влияют на операционную надежность и на наш взгляд должны учитываться в определении инцидентов операционной надежности.
	ИНФОРМИРОВАНИЕ БР ОБ ИНЦИДЕНТАХ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ	
23	Если информировать будем через АСОИ ФинЦЕРТ, то сейчас там недостаточно полей и справочников. Сообщать должны риски или ОИБ?"	Согласно Разъяснениям БР по аналогии с инцидентами защиты информации сведения об инцидентах операционной надежности необходимо будет представлять в соответствии со стандартом Банка России СТО БР БФБО-1.5-2018 "Безопасность финансовых (банковских) операций. Управление инцидентами информационной

		безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации", который будет доработан в части инцидентов операционной надежности и размещен на сайте Банка России в разделах "Информационная безопасность", "Стандарты Банка России". В настоящее время форма отчетности предполагает назначение ответственным подразделением как подразделение рисков, так и подразделение информационной безопасности, т.е. решение о назначении ответственного подразделения принимается на уровне кредитной организации.
24	В каком формате и в какие сроки должно происходить информирование ЦБ (ФинЦЕРТ) об инцидентах операционной надежности? Необходимо ли отдельно информировать ЦБ о восстановлении процесса после инцидента?	Как указано в ответе на вопрос №23 Разъяснений БР будет доработан стандарт СТО БР БФБО-1.5-2018, этот стандарт в настоящее время содержит требования и к срокам предоставления отчетности об инцидентах информационной безопасности. Соответственно в новой версии стандарта также будет указаны сроки информирования Банка России об инцидентах операционной надежности. Текущая форма отчетности содержит поля о промежуточном и конечном информировании об инцидентах, предполагается аналогичное информирование об инцидентах операционной надежности.
25	Какое подразделение Банка Вы порекомендовали бы назначить ответственным за информирование ЦБ об инцидентах операционной надежности?	Решение о назначении ответственного подразделения принимается кредитной организацией самостоятельно. На наш взгляд наиболее оптимальным является подразделение по управлению рисками, как подразделение консолидирующее и формирующее отчетность по операционным рискам. Также логичной выглядит позиция что это то подразделение которое в настоящее время направляет в ФинЦЕРТ отчетности об инцидентах информационной безопасности согласно СТО БР БФБО-1.5-2018. Полагаем ситуация будет определенноее когда Банк России выпустит доработанный стандарт СТО БР БФБО-1.5-2018, как обещает в своих комментариях.

[i] https://asros.ru/dialog/information-security/bank-rossii-razyasnil-trebovaniya-k-operatsionnoy-nadezhnosti-bankov/

[ii] https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81