

**Комментарии Департамента информационной безопасности¹ к вопросам и предложениям
по Положению № 787-П²**

№ п/п	Структурная единица Положения № 787-П	Содержание вопроса и предложения	Пояснение	Комментарий ДИБ
1	2	3	4	5
1.	Абз. 4 пункта 3., форма 0409072	Как должно рассчитываться фактическое значение 3 ЦПОНа, если отчет по форме 0409072 за 3 квартал 2023, то графа 5 раздела 2 отчётной формы 0409072 заполняется предельно допустимым для КО временем простоя и (или) деградации технологического процесса (в случае превышения ДДД ТП – 1 ЦПОН), установленным на период с 01.01.2023 по 31.12.2023, а в графе 6 раздела 2 необходимо указать фактическое значение за последние 12 месяцев, то есть за период с 01.10.2022 по 30.09.23? Почему фактическое значение в графе 6 раздела 2 считается не в рамках календарного года формируемой отчётной формы 0409072 и не в рамках установленного предельного значения 3 ЦПОНа на календарный год, совпадающий с календарным годом отчётной формы 0409072?	Согласно абз.4 п.3 787-П 3 ЦПОН «допустимое суммарное время простоя и (или) деградации технологического процесса кредитной организации (в случае превышения допустимой доли деградации технологического процесса) в течение очередного календарного года» рассчитывается за очередной календарный год, что согласно Федеральному закону от 03.06.2011 №107-ФЗ «Об исчислении времени» является периодом времени с 1 января по 31 декабря продолжительностью 365/366 календарных дней. В порядке составления и предоставления отчёта по форме 0409072 Указания Банка России от 10.04.2023 №6406-У (находится на регистрации в МинЮсте на текущий момент) отражено, что графа 6 раздела 2 заполняется фактическим значением 3 ЦПОН за последние 12 месяцев от отчётной даты, под которой в рамках формы 0409072 подразумевается квартал.	Целевое значение устанавливается на 12 календарных месяцев, пересматривать его необходимо не реже одного раза в год. Передавать показания необходимо с момента установления целевых значений. Фактическое значение в графе 6 является плавающим и будет иметь разные показатели в разных кварталах.
2.	Абз.5 подпункта 6.1.	Просим разъяснить критерии отнесения отдельных операций к технологическим участкам технологических процессов	Положение требует обеспечивать учёт технологических участков, при этом зафиксирован только перечень участков, а критерии отнесения отдельных шагов процессов и технологических операций к тем или иным участкам не определены. Как	Основанием отнесения тех или иных конкретных операций к тому или иному технологическому участку является факт того, что осуществление этих операций направлено на обеспечение
¹ Далее – ДИБ. ² 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» (далее – Положение № 787-П).				

			следствие, обеспечить контроль корректности отнесения операций не представляется возможным, возникают разночтения и риск несоблюдения требований к автоматизации данных участков. Например, не ясно, к какому участку необходимо относить проверку наличия клиента в стоп-листах, требуется ли учёт технологических участков в процессе обработки расчётных документов, получаемых из Банка России.	функционирования этих технологических процессов.
3.	Абз.6 пункта 6	Требуется ли информировать ФинЦЕРТ об инцидентах, вызванных технологическими сбоями на стороне ИТ-сервисов ФОИВ, платёжной системы или регулятора?	Положение 787-П не предъявляет требований к защите от инцидентов, вызванных сбоями на стороне сервисов ФОИВ и регуляторов. Однако подобные сбои могут приводить к технологическим инцидентам с долей деградации, которая превышает установленные в Банке целевые показатели операционной надёжности. Реализуются косвенные потери. Требуется ли информировать ФинЦЕРТ о таких инцидентах?	Да, в случае превышения допустимой доли деградации технологического процесса, вызванного сбоями на стороне ИТ-сервисов ФОИВов, требуется информировать ФинЦЕРТ.
4.	Абз.7 пункта 10.	Необходимо ли вести учёт ИОН в базе СОР с риском нарушения непрерывности деятельности, когда в рамках 787-П по инциденту операционной надёжности есть превышение ДДД, по сути это СОР с риском нарушения непрерывности деятельности, но нет потерь? Можно ли фиксировать информацию об ИОНе в базе СОР как СОР с риском нарушения непрерывности деятельности при отсутствии потерь (не будут попадать в форму 0409106), или лучше отдельно вести учёт таких случаев?		В случае если событие операционного риска привело только к качественным потерям, оценка значимости которых в соответствии с абзацем двенадцатым подпункта 3.13.2 пункта 3.13 Положения № 716-П³ соотносится с уровнем «средние» или «низкие», кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах требования к регистрации таких событий операционного риска в базе событий. По категории «качественные потери» кредитной организацией (головной кредитной организацией банковской группы) устанавливаются следующие виды потерь: приостановление и (или) прекращение банковских процессов;
³ Положение 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).				

				потеря работоспособности объектов информационной инфраструктуры; нарушение целостности (искажение) или потеря данных; возникновение уязвимостей в объектах информационной инфраструктуры, программном обеспечении и приложениях, банковских процессах; другие потери качества объектов информационной инфраструктуры кредитной организации.
5.	Абз.7 пункта 10.	Если ИОН затрагивает несколько ТП, фиксировать ли 1 инцидент в 1 СОР, или по каждому ТП в нескольких СОР (учитывая индивидуальные параметры инцидента: возможно различное время простоя, вид потерь, ДДД)?		При идентификации и регистрации инцидентов операционной надежности, затрагивающих сразу несколько технологических процессов, ДИБ рекомендует разделять их на отдельные инциденты по каждому технологическому процессу. Такой подход позволяет обеспечивать полноценный и корректный расчет параметров каждого технологического процесса, в том числе элементов критичной архитектуры и целевых показателей по каждому технологическому процессу. Кредитные организации при желании могут группировать разделенные отдельные инциденты.
6.	Абз.7 пункта 10.	Если ИОН признается СОР с риском нарушения непрерывности деятельности в рамках п.1.4. 716-П, то необходимо ли при классификации данный риск указывать в атрибутом составе базы СОР согласно абз.17 п.6.6., или можно в рамках требований абз.17 п.6.6. указать при регистрации СОР, например, риск ИБ или ИС, а про риск нарушения непрерывности деятельности упомянуть в другом поле базы СОР, заполняемом в соответствии с требованиями абз.18		В соответствии с абзацем семнадцатым пункта 6.6 Положения № 716-П кредитная организация указывает в базе событий вид операционного риска, указанный в пункте 1.4 Положения № 716-П, в зависимости от источника операционного риска, которым обусловлено возникновение события (в приведенном примере – риск информационной безопасности или риск информационных систем). Реализация риска нарушения непрерывности деятельности является следствием реализации одного из указанных видов

		п.6.6. (связь с другими видами операционного риска)?		рисков и отражается в базе событий в соответствии с абзацем восемнадцатым пункта 6.6 Положения № 716-П.
7.	Абз.9-12 пункта 10.	Необходимо ли в базу СОР заносить помимо информации из абз.10-12 п.10 787-П иную информацию, предусмотренную 787-П, или достаточно дополнить базу СОР только тем атрибутивным составом, который поименован для занесения в базу в данных абзацах? Например, ПО (программное обеспечение) не выделен как атрибут для ИОН в абз.9-12 п.10 787-П, но в рамках критичной архитектуры должен учитываться?	Согласно п.6.5. 787-П в отношении критичной архитектуры с использованием результатов сценарного анализа проводится тестирование готовности КО противостоять реализации информационных угроз, и косвенно вытекает необходимость все-таки фиксировать в базе СОР атрибутивный состав по критичной архитектуре, который будет затронут тем или иным ИОН.	Согласно пункту 6.5 Положения № 787-П в отношении критичной архитектуры с использованием результатов сценарного анализа проводится тестирование готовности КО противостоять реализации информационных угроз и косвенно вытекает необходимость все-таки фиксировать в базе СОР атрибутивный состав по критичной архитектуре, который будет затронут тем или иным ИОН.
8.	Абз.2 пункта 11.	Просим определить порядок информирования ФинЦЕРТ о ситуации, когда расследование инцидента операционной надёжности показывает, что нарушения допустимой доли деградации технологического процесса в инциденте не было, инцидент операционной надёжности не подтвердился.	В соответствии с требованиями стандарта Банка России от 08.02.2023 № СТО БР БФБО-1.5-2023 участники информационного взаимодействия, реализующие усиленный или стандартный уровни защиты информации в соответствии с ГОСТ Р 57580.1 – 2017, должны в течение 3 часов с момента выявления инцидента операционной надёжности проинформировать Банк России о событии. Нередки случаи, когда по результатам первичного анализа влияние инцидента оценивается как нарушающее допустимую долю деградации технологического процесса, однако расследование показывает, что целевой показатель не был превышен или деградация отсутствовала. Просьба уточнить, в каком/й виде/форме мы должны информировать, что по итоговым расчётам событие не явилось инцидентом операционной надёжности.	В случае если расследование события операционного риска не завершено и неизвестно, является ли событие инцидентом операционной надёжности, необходимо направить первичное уведомление в соответствии с СТО БР БФБО-1.5-2023. После завершения расследования финансовая организация в рамках вторичного уведомления информирует, являлось ли событие инцидентом операционной надёжности.