Общение с работниками банков на вебинаре по обзору требований Положения № 787-П[1] показало, что для них остаются некоторые недостаточно транспарентные зоны, влияющие на оперативность и корректность выполнения новых регуляторных норм. Мы обработали полученные вопросы, проанализировали текущую нормативную базу и нормы Положения № 787-П и разработали рекомендации о том, как нужно действовать.

**Майя САВИЦКАЯ**, *ООО «ФБК», менеджер Департамента аудиторских и консультационных услуг финансовым институтам*
**Михаил МАНЦУРОВ**, *ООО «ФБК», консультант по ИТ Департамента аудиторских и консультационных услуг финансовым институтам*

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

С 1 октября 2022 г. вступает в силу Положение № 787-П. Этот документ, развивая подходы к управлению операционным риском в целом, установленные в Положении № 716-П[2], значительно расширяет и углубляет процедуры управления такими видами операционного риска, как риск информационных систем и риск информационной безопасности.

## Технологические процессы

Согласно требованиям Положения № 787-П, для обеспечения операционной надежности кредитные организации должны обеспечить непревышение порогового уровня допустимого времени простоя и (или) нарушения технологических процессов, обеспечивающих выполнение критически важных процессов, приводящих к неоказанию или ненадлежащему оказанию банковских услуг.

Также кредитные организации должны определить во внутренних документах значения целевых показателей операционной

[1] 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».

[2] Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

надежности для каждого технологического процесса и соблюдать их.

Как видим, все процедуры управления операционной надежностью базируются на технологическом процессе. Соответственно определение перечня таких процессов — ключевая задача при внедрении норм Положения № 787-П.

Однако расшифровка понятия технологического процесса в документе отсутствует. И именно определение и идентификация таких процессов вызывают множество вопросов у банков.

*Что такое технологический процесс? Является ли перечень технологических процессов в Приложении к Положению № 787-П закрытым? Что является операцией в технологическом процессе?*

Согласно Комментариям Банка России в письме Ассоциации банков России от 06.10.2021 (далее — Комментарии БР)[1], определение технологического процесса планируется ввести указанием Банка России «О внесении изменений в Положение Банка России № 716-П “О требованиях к системе управления операционным риском в кредитной организации и банковской группе”».

Все процедуры управления операционной надежностью базируются на технологическом процессе. Соответственно определение перечня таких процессов – ключевая задача при внедрении норм Положения № 787-П.

В п. 2 Положения № 787-П сказано, что перечень технологических процессов, обеспечивающих выполнение критически важных процессов, приводящих к неоказанию или ненадлежащему оказанию банковских услуг, приведен в Приложении, однако в Комментариях БР регулятор обращает внимание, что указанные в приложении технологические процессы установлены императивно 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 № 716-П.

Действительно, в Положении № 787-П все требования к технологическим процессам рассматриваются через призму их роли в обеспечении выполнения критически важных процессов. Полагаем, что список технологических процессов находится в прямой корреляции с пониманием критически важных процессов и его построение базируется на списке таких процессов.

Давайте обратимся к Положению № 716-П.

Согласно п. 8.5 Положения № 716-П, в политике информационных систем (далее — Политика ИС) кредитная организация определяет

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

Майя САВИЦКАЯ
Михаил МАНЦУРОВ

перечень ИС, обеспечивающих функционирование процессов (Перечень ИС).

Структурный классификатор перечней процессов, в том числе по направлениям деятельности, достаточно подробно регламентирован в п. 4.1.1 и 3.9 Положения № 716-П, также в п. 4.1.1 регулятор обозначил список процессов, являющихся для кредитных организаций критическими.

Вспомним алгоритм построения Перечня ИС (табл. 1).

Таблица 1

## Алгоритм построения Перечня ИС

| | |
|---|---|
| 1. Определяем направления деятельности, присущие кредитной организации | |
| А) Направления деятельности первого уровня | Корпоративное финансирование.<br>Операции и сделки на финансовом рынке.<br>Розничное банковское обслуживание.<br>Коммерческое банковское обслуживание корпоративных клиентов.<br>Осуществление переводов денежных средств, платежей и расчетов через платежные системы.<br>Агентские и депозитарные услуги.<br>Управление активами.<br>Розничное брокерское обслуживание.<br>Обеспечение деятельности кредитной организации |
| Б) Классификация направлений деятельности, в том числе в разрезе составляющих их процессов, до второго уровня и далее с учетом осуществляемых операций и (или) действующих процессов (определяется кредитной организацией самостоятельно) | |
| 2. Определяем в каждом из направлений деятельности критически важные процессы, присущие кредитной организации | |
| Список критически важных процессов, определенных регулятором | 1) Обеспечивающие выполнение операций, указанных в п. 1–4 и 9 ч. 1 ст. 5 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»:<br>— привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);<br>— размещение данных привлеченных средств от своего имени и за свой счет;<br>— открытие и ведение банковских счетов физических и юридических лиц;<br>— осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам;<br>— осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов);<br>2) ведение бухгалтерского учета;<br>3) представление отчетности в Банк России в соответствии с Указанием от 08.10.2018 № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации»;<br>4) поддержание ликвидности;<br>5) выполнение операций на финансовых рынках;<br>6) выполнение кассовых операций;<br>7) работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций; |

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

Окончание таблицы 1

| | |
|---|---|
| | 8) соблюдение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;<br>9) соблюдение Трудового кодекса Российской Федерации;<br>10) другие процессы, которые определены кредитной организацией и прерывание функционирования которых оказывает влияние на выполнение ее обязательств перед клиентами и контрагентами |
| 3. Для каждого получившегося процесса определяем перечень информационных систем банка, от которых зависит функционирование этого процесса | |
| 4. Строим классификатор ИС с учетом их критичности и влияния на процессы, а также влияния сбоев* в работе ИС на процессы кредитной организации | |

* Согласно Положению № 787-П, под сбоями объектов информационной инфраструктуры понимаются отказы и (или) нарушения функционирования объектов информационной инфраструктуры, и (или) несоответствие их функциональных возможностей и характеристик потребностям кредитной организации.

Таким образом, при идентификации технологических процессов единственный правильный путь — обратиться к Политике ИС, а именно к Перечню ИС, обеспечивающих функционирование критически важных процессов банка.

Также для формирования понятийного аппарата предлагаем обратиться к следующим определениям[1]:

— 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.

Список технологических процессов находится в прямой корреляции с пониманием критически важных процессов и его построение базируется на списке таких процессов.

*Технологический процесс вмещает в себя несколько бизнес-процессов. Правильно ли декомпозировать пороговый уровень деградации/простоя технологического процесса на каждый из составляющих его процессов?*

Обращаем внимание, что в п. 5.2 Положения № 683-П[2] установлено понятие технологического участка. Пункт 6.1 Положения № 787-П трактует данное понятие как «технологические участки технологического процесса», а именно:

— идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;

[1] https://ru.wikipedia.org/wiki/Технологический процесс.

[2] Положение 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».

Майя САВИЦКАЯ
Михаил МАНЦУРОВ

— 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 об установлении порогового уровня деградации для технологических участков технологического процесса.

В настоящий момент Положение № 787-П не содержит требования об установлении порогового уровня деградации для технологических участков технологического процесса.

*Для каждого технологического процесса должны быть установлены контрольные показатели уровня операционного риска. Однако если для примера взять технологический процесс «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 банку устанавливать значение контрольных показателей в этом случае?*

Если обратиться к классификаторам, используемым Положением № 716-П, то в направлении деятельности «розничное банковское обслуживание» можно выделить три критически важных процесса, применимых к описанным процессам:

— работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций;

— привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);

— открытие и ведение банковских счетов физических и юридических лиц.

Очевидно, что для обеспечения каждого из этих процессов используется своя комбинация объектов информационной инфраструктуры, к которым относятся автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование.

В Комментариях БР также сделан акцент на том, что операционная надежность технологических процессов рассматривается только относительно установленного режима работы для технологического процесса и значение целевого показателя операционной надежности «показатель соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках техно-

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

логического процесса)» кредитная организация устанавливает самостоятельно.

В вопросе речь идет о двух разных процессах, для выполнения каждого из которых функционирует отдельный технологический процесс как взаимосвязь отдельных действий (людей и, что важнее, ИС), выполняющихся с момента возникновения исходных данных (обращения клиента за услугой) до получения нужного результата (получения услуги клиентом). Да, часть этих действий будет похожа, но часть будет уникальна для каждого из этих двух технологических процессов, особенно объекты информационной инфраструктуры. И время (режим) работы каждого из двух технологических процессов для обеспечения его непрерывности требуется разное, соответственно и интервалы «неработы», которые будут трактоваться как деградация и простой технологического процесса, будут различны.

Таким образом, в рамках исполнения требований Положения № 787-П «привлечение денежных средств во вклады в офисе» и «привлечение денежных средств во вклады по системе ДБО» — это два разных технологических процесса с индивидуальными требованиями к режиму и особенностям функционирования.

В рамках исполнения требований Положения № 787-П «привлечение денежных средств во вклады в офисе» и «привлечение денежных средств во вклады по системе ДБО» — это два разных технологических процесса с индивидуальными требованиями к режиму и особенностям функционирования.

*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 Положения № 787-П — в части перечня критически важных процессов и сроков их восстановления?*

Действительно, согласно Приложению 5 к Положению № 242-П[1], в План ОНиВД рекомендуется включать такие атрибуты, как перечень внутренних банковских процессов, критически важных для обеспечения режима повседневного функционирования кредитной организации, а также показатели восстановления внутренних процессов, в том числе срок восстановления, допустимый размер материальных затрат, допустимый размер потерь информации. Эти показатели, а также устанавливаемые на их основе критерии непрерывности внутренних банковских процессов рекомендуется определять с учетом необходимости соблюдения требований в том числе нормативных актов Банка России.

Согласно Комментариям БР, при выполнении требований Положения № 242-П в рамках плана ОНиВД допустимо формировать

[1] Положение Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».

Майя САВИЦКАЯ
Михаил МАНЦУРОВ

перечень критически важных процессов, совпадающий с перечнем технологических процессов, указанных в Приложении к Положению № 787-П.

Полагаем, что для единообразия управленческой модели риск-менеджмента и внутреннего контроля и повышения сопоставимости используемых «рисковиками» и «контролерами» данных целесообразно использовать единую систему координат для понятия «критически важные процессы», употребляемого как в процедурах управления операционным риском, так и в Плане ОНиВД.

## Целевые показатели надежности

Согласно нормам Положения № 787-П, обеспечение операционной надежности достигается установлением и соблюдением целевых показателей операционной надежности (ЦПОН).

Целевые показатели операционной надежности определяются во внутренних документах для каждого технологического процесса и включают в себя четыре показателя:

1. Допустимая доля деградации технологического процесса. Определяется по формуле:

$$\frac{\text{(Общее количество операций в рамках технологического процесса, совершенных во время его деградации в рамках инцидента операционной надежности)}}{\text{(Ожидаемое количество операций в рамках технологического процесса в случае непрерывного оказания банковских услуг)}},$$

где инцидент операционной надежности — события операционного риска или серия связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к неоказанию или ненадлежащему оказанию банковских услуг.

Значение показателя рассчитывается:

— на основании статистических данных за период не менее 12 календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности;

— если технологический процесс существует менее 12 календарных месяцев — на основании статистических данных за период с даты начала его функционирования;

— на основании иных данных (по выбору кредитной организации).

Одним из примеров расчета доли деградации технологического процесса является подсчет среднего количества технологических

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

операций на основании статистических данных за один календарный год. Расчет возможно проводить как путем деления общего количества операций (для круглосуточных технологических процессов) за один год на количество часов в году — 8760, результатом будет среднее значение количества операций в час. Или можно рассчитать среднее количество операций в разрезе дней недели (так как возможен рост количества операций в выходные и предпраздничные дни), календарных дней, месяцев и т.д. Отклонение от полученных средних значений на определенный процент, найденный экспертным методом, и будет считаться допустимой долей деградации технологического процесса.

2. Допустимое время простоя и (или) деградации технологических процессов в рамках инцидента операционной надежности (в случае превышения допустимой доли деградации технологического процесса).

Значение этого показателя устанавливается кредитной организацией не выше значений, предусмотренных Приложением к Положению № 787-П.

3. Допустимое суммарное время простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации) в течение очередного календарного года.

4. Показатель соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса).

Одним из примеров расчета доли деградации технологического процесса является подсчет среднего количества технологических операций на основании статистических данных за один календарный год.

*Верно ли, что целевые показатели операционной надежности — это частный пример КПУР (контрольных показателей уровня риска), требования к которым установлены в гл. 5 Положения № 716-П, а значит, и управляться должны как КПУР?*

Как уже было сказано, нормы Положения № 787-П развивают принципы, подходы и инструментарий риск-менеджмента, заложенные ранее в Положении № 716-П.

Согласно Комментариям 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 гл. 5 Положения № 716-П. Установление целевых показателей операционной надежности вне Приложения 1 к Положению № 716-П обусловлено целесообразностью отражения ключевых требований к операционной надежности в рамках одного нормативного акта.

Майя САВИЦКАЯ
Михаил МАНЦУРОВ

И действительно, п. 3 Положения № 787-П говорит о том, что значения ЦПОН должны быть установлены с учетом требований гл. 5 Положения № 716-П.

О каких же требованиях идет речь?

Глава 5 Положения № 716-П устанавливает основные правила организации системы контрольных показателей уровня операционного риска (КПУОР):

1. Для каждого КПУОР, а значит и для ЦПОН, должны быть установлены целевые значения:

— сигнальное значение, при нарушении которого проводится ежедневный мониторинг значений и реализуются меры, направленные на устранение превышения фактического значения над предельно допустимым;

— контрольное значение — предельно допустимое значение, при нарушении которого информация доводится до совета директоров (наблюдательного совета) и применяются меры реагирования.

Интеграцию требований к установлению и расчету целевых показателей операционной надежности целесообразно базировать на тех нормах, которые банк уже заложил в Политику управления операционным риском.

2. Совет директоров (наблюдательный совет) утверждает сигнальные и контрольные значения КПУОР (ЦПОН) на плановый годовой период.

3. Подразделение, ответственное за организацию управления операционным риском, оформляет расчет и обоснование сигнальных и контрольных значений КПУОР (ЦПОН) в виде заключения и включает его в состав материалов, направляемых им на рассмотрение коллегиальному исполнительному органу при утверждении (пересмотре) политики управления операционным риском.

4. Значения КПУОР (ЦПОН) нужно пересматривать и актуализировать ежегодно.

Следовательно, интеграцию требований к установлению и расчету ЦПОН целесообразно базировать на тех нормах, которые банк уже заложил в политику управления операционным риском.

Целевые значения ЦПОН — контрольное и сигнальное — следует устанавливать в той же парадигме, что и целевые значения КПУОР, чтобы соблюдалось единообразие процентного уровня от допустимого (порогового) значения, уже заложенного в отношении КПУОР в политике управления операционным риском (обычно в рыночной практике это 85 и 90%).

*Существуют ли рекомендации по расчету доли деградации технологического процесса и других ЦПОН?*

Согласно Комментариям БР, фактическую долю деградации технологического процесса нужно рассчитывать, исходя из фактического

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

и ожидаемого количества финансовых операций. Ожидаемое количество финансовых операций должно определяться с учетом статистических данных и (или) иных данных по выбору кредитной организации. То есть регулятор не дает конкретных рекомендаций, предполагая, что кредитные организации самостоятельно разработают методику расчета.

На наш взгляд, помимо статистических наблюдений целесообразно использовать экспертное мнение владельцев/участников технологических процессов о приемлемой доле деградации. Также полезными инструментами будут сценарный анализ и шкала качественных потерь, закрепленная во внутренних методиках по определению оценок качественных потерь от реализации инцидентов операционной надежности.

В Положении № 716-П Банк России предлагает использовать четырехуровневую шкалу оценки значимости качественных потерь: «очень высокие», «высокие», «средние», «низкие»).

Соответственно инциденты с оценкой значимости потерь «очень высокие» и «высокие» можно будет включить в определение доли деградации. Критерии соотнесения шкалы качественных потерь с количественными потерями банки разрабатывают самостоятельно. Например, в рыночной практике распространен подход, представленный в табл. 2.

При расчете доли деградации технологического процесса, помимо статистических наблюдений, целесообразно использовать экспертное мнение владельцев/участников технологических процессов о «приемлемой» доле деградации.

Таблица 2

**Пример перевода качественных потерь в количественные**

| Критерии шкалы качественных потерь | Сумма потерь (% от капитала/собственных средств/лимита капитала на ОР) |
|---|---|
| Низкий | До 0,1 |
| Средний | От 0,1 до 0,5 |
| Высокий | От 0,5 до 1 |
| Очень высокий | Свыше 1 |

## Инциденты операционной надежности

*Понятие «инцидент операционной надежности» включает в себя инциденты, связанные:*

*1) со сбоями, деградацией ИС банка?*

*2) со сбоями у партнеров (например, АО «НСПК», СБП, поставщиков услуг связи)?*

Майя САВИЦКАЯ
Михаил МАНЦУРОВ

Согласно Комментариям 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 примеры — это примеры причин/источников возникновения инцидента, для которых регулятор дает унифицированные классификаторы.

При классификации инцидента операционной надежности используются классификаторы, регламентированные как в гл. 3 и Приложении 5 к Положению № 716-П, так и в п. 3.7 Положения № 787-П.

В классификаторах регулятора содержатся как внутренние, так и внешние источники операционного риска, типы событий риска.

У одного и того же события операционного риска может быть один или несколько источников. В приведенных примерах возможно 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».

При классификации инцидента операционной надежности используются классификаторы, регламентированные как в гл. 3 и Приложении 5 к Положению № 716-П, так и в п. 3.7 Положения № 787-П.

*Учитывать ли в определении инцидентов операционной надежности инциденты, произошедшие в чрезвычайной ситуации (ЧС в терминологии ОНиВД)?*

Понятия «инцидент операционной надежности» и «чрезвычайная ситуация», приведенные соответственно в Положении № 787-П и Законе № 68-ФЗ[1], — про разное и для разных целей. Чрезвычайная ситуация — это фон, источник, база для возникновения сбоя объектов информационной инфраструктуры, который в парадигме системы управления операционным риском (СУОР) будет событием операционного риска (с источником риска по Положению № 716-П — «внешние причины» и «сбой систем и оборудования» и типами события — «ущерб материальным активам» (к которому относятся события, близкие по трактовке к чрезвычайной ситуации по Закону № 68-ФЗ: природные факторы, включая стихийные бедствия, техногенные факторы) и «нарушение и сбои систем и оборудования»), в рамках которого и реализуется инцидент операционной надежности — деградация технологического процесса.

[1] Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

## Организационные вопросы внедрения норм Положения № 787-П

*Возможно ли требования к операционной надежности прописывать не в отдельном документе, а, к примеру, в уже существующем положении по операционному риску, учитывая, что они взаимосвязаны?*

Достаточно включить регламентацию выполнения требований к операционной надежности в уже существующий пул внутренних нормативных документов по управлению операционным риском. Нет необходимости создавать такие документы с нуля.

Согласно п. 9 Положения № 787-П, описание процедур, направленных на реализацию требований к операционной надежности, кредитные организации должны установить во внутренних документах, предусмотренных п. 4.1.2, абз. 1 п. 4.1.3 и абз. 2 п. 4.1.4 Положения № 716-П. Это такие документы, как:

— политика управления операционным риском;

— внутренние документы, описывающие процедуры управления операционным риском, а также процедуры оценки эффективности функционирования СУОР;

— внутренние документы, устанавливающие в кредитной организации (головной кредитной организации банковской группы) структуру и организацию СУОР, 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 внешних экспертов для оценки эффективности функционирования СУОР.

Достаточно включить регламентацию выполнения требований к операционной надежности в уже существующий пул внутренних нормативных документов по управлению операционным риском. Нет необходимости создавать такие документы с нуля.

*Как лучше организовать процесс внедрения: «со стороны ИТ/ИБ» или «со стороны СУОР»? Кто в системе управления операционными рисками должен быть ключевым?*

Корректное и эффективное внедрение норм Положения № 787-П возможно только при симбиозе и плотном сотрудничестве трех подразделений: подразделения, ответственного за организацию управления операционным риском (при его отсутствии — службы управления рисками), подразделений ИТ и ИБ, которые являются специализированными подразделениями по управлению риском информационных систем и риском информационной безопасности.

Обращаем внимание, что подразделение, ответственное за организацию управления операционным риском, является подразделением, ответственным за организацию управления операционным риском

Майя САВИЦКАЯ
Михаил МАНЦУРОВ

в целом в кредитной организации (п. 1.3 Положения № 716-П). То есть организовать процесс управления, регламентировать подходы, принципы, инструментарий и процедуры управления оперриском (в т.ч. риском ИС и риском ИБ) — это зона ответственности рисковиков.

Безусловно, без специфических знаний подразделений ИТ и ИБ рисковики не могут методологически правильно наполнить процедуры. Например, подразделения ИТ и ИБ дают статистическую информацию для расчета допустимых и целевых значений ЦПОН, являются поставщиками информации об инцидентах операционной надежности, методах сбора сведений о них, а подразделение, ответственное за организацию управления операционным риском, методологически встраивает эти знания в политику управления операционным риском и иные процедурные документы и распределяет ролевые модели. Определение технологических процессов тоже целесообразно проводить совместно, базируясь на Перечне ИС по критически важным процессам, заложенным в Политику ИС.

*Необходимо ли добавить информацию об инцидентах операционной надежности в годовую отчетность в рамках ВПОДК (в раздел отчетности об управлении операционным риском)?*

В настоящее время в Указании № 3624-У[1] таких требований нет.

Полагаем, что данная информация должна включаться в отчетность по оперрискам, формируемую для органов управления на основании п. 4.2.2 Положения № 716-П, в том числе:

— результаты качественной оценки уровня операционного риска — включаются результаты сценарного анализа, тестирования готовности кредитной организации противостоять реализации информационных угроз в отношении критичной архитектуры;

— фактические значения контрольных показателей уровня операционного риска — включаются фактические значения целевых показателей операционной надежности.

## Информирование Банка России

*В каком формате и в какие сроки информировать Банк России об инцидентах операционной надежности? Необходимо ли отдельно информировать о восстановлении процесса после инцидента?*

Кредитные организации информируют подразделение ФинЦЕРТ об инцидентах, связанных с нарушением требований к обеспечению

[1] Указание Банка России от 15.04.2015 № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы».

# Новые требования к операционной надежности: анализируем узкие места Положения № 787-П

защиты информации в соответствии со стандартом СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности».

Планируется, что сведения об инцидентах операционной надежности банки также будут предоставлять в соответствии с данным стандартом. Его новую версию, содержащую формы и сроки информирования об инцидентах операционной надежности, Банк России разместит на своем официальном сайте после доработки.

*Какое подразделение рекомендуется назначить ответственным за информирование Банка России об инцидентах операционной надежности?*

Действующая форма отчетности об инцидентах защиты информации предполагает предоставление отчетности как подразделением рисков, так и подразделением ИБ, то есть решение о назначении ответственного подразделения принимается на уровне кредитной организации. На наш взгляд, наиболее оптимально назначить ответственным подразделение по управлению рисками — как консолидирующее и формирующее отчетность по операционным рискам.

Также логичной выглядит позиция, что это то подразделение, которое в настоящее время направляет в ФинЦЕРТ отчетность об инцидентах информационной безопасности согласно СТО БР БФБО-1.5-2018. Полагаем, ситуация будет определеннее, когда Банк России выпустит доработанный стандарт.