Пока регуляторных требований по проведению единой политики непрерывности для банков нет. Однако это вопрос недалекого будущего. Соединив установленные Банком России перечни технологических процессов и процессов банка, определенных как критически важные, автор вводит практическую классификацию, позволяющую построить достаточно аргументированный и понятийно прозрачный перечень критически важных процессов, на базе которого можно разрабатывать процедуры обеспечения непрерывности и интегрировать эти процедуры в План ОНиВД.

Подходы к построению системы обеспечения непрерывности деятельности: кооперация регуляторных норм

Майя САВИЦКАЯ,
ООО «ФБК», руководитель направления, менеджер Департамента аудиторских и консультационных услуг финансовым институтам

Сохранение непрерывности своей деятельности — одна из важнейших задач любой организации. И кредитные организации не являются исключением.

Организация защиты кредитной организации (далее — КО, банк) от внутренних и внешних событий, могущих оказать негативное влияние на непрерывность ее функционирования, всегда была и будет актуальной. От способности банка принимать как превентивные меры защиты, так и меры оперативного реагирования на инциденты прерывания его бизнес-процессов и восстановления их осуществления в нормальном режиме зависят как операционная надежность банка, так и его операционная устойчивость.

Каждая КО имеет свой План обеспечения непрерывности и восстановления деятельности (План ОНиВД), требования к разработке которого установлены достаточно давно Положением № 242-П[1], и необходимые регуляторные требования, безусловно, внедрены во всех банках.

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

Подходы к построению системы обеспечения непрерывности деятельности

С выпуском новых нормативных актов Банка России — Положения № 716-П[1], а затем и Положения № 787-П[2] — появились новые аспекты обеспечения непрерывности деятельности, дополнились процессы и задачи, расширились объекты контроля, прерывание функционирования которых неприемлемо. Чтобы эффективно внедрить их в уже существующие процессы и процедуры, необходимо грамотно объединить «старые» и «новые» нормы, оптимизировать и улучшать процедуры обеспечения непрерывности деятельности.

И Положение № 242-П, и Положение № 716-П, и Положение № 787-П устанавливают отдельные требования к обеспечению непрерывности. Давайте посмотрим, чем они концептуально различаются (табл. 1).

Таблица 1

Требования к обеспечению непрерывности

№	Область обеспечения непрерывности	Когда нужно обеспечить непрерывность	Цели	Причины нарушения непрерывности	Введены Положением Банка России
1	Обеспечение непрерывности деятельности КО	При возникновении нестандартных и чрезвычайных ситуаций, нарушающих режим повседневного функционирования КО	1. Предотвращение или своевременная ликвидация последствий нарушения режима повседневного функционирования КО 2. Минимизация существенных материальных потерь или иных последствий, препятствующих выполнению КО принятых на себя обязательств	1. Нестандартные и чрезвычайные ситуации 2. Иные события, наступление которых возможно, но труднопредсказуемо, связанные с угрозой невыполнения КО принятых на себя обязательств	№ 242-П
2	Обеспечение непрерывности осуществления критически важных процессов и критически важных операций	При выполнении критически важных процессов и критически важных операций	Поддержание операционной устойчивости	1. Источники операционного риска[3]. 2. Изменение процессов КО. 3. Действия третьих лиц. 4. Нарушение операционной надежности	№ 716-П

[1] Положение Банка России от 08.04.202 №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

[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».

[3] Недостатки процессов, действия персонала и других связанных с КО лиц, сбои систем и оборудования, внешние причины (п. 3.3 Положения № 716-П).

Майя САВИЦКАЯ

Окончание табл. 1

№	Область обеспечения непрерывности	Когда нужно обеспечить непрерывность	Цели	Причины нарушения непрерывности	Введены Положением Банка России
3	Обеспечение непрерывности оказания банковских услуг при выполнении критически важных процессов, связанных с предоставлением банковских услуг	При оказании банковских услуг	Обеспечение операционной надежности при осуществлении банковской деятельности с использованием объектов информационной инфраструктуры	1. Сбои объектов информационной инфраструктуры[1]. 2. Реализация киберриска	№ 787-П
4	Обеспечение непрерывности оказания финансовых услуг	При оказании финансовых услуг, в рамках деятельности КО как профессионального участника рынка ценных бумаг	Обеспечение операционной надежности при осуществлении деятельности профессионального участника рынка ценных бумаг с использованием объектов информационной инфраструктуры	Реализация информационных угроз	№ 779-П[2]
5	Обеспечение непрерывности функционирования информационных систем	При осуществлении процессов КО с использованием информационных систем	Минимизация вероятности реализации риска информационных систем[3] и снижение его негативного влияния на деятельность КО	Источники операционного риска	№ 716-П

Пока регуляторных требований по проведению единой политики непрерывности для банков нет. Однако это вопрос недалекого будущего, и такие регуляторные планы уже обсуждаются Банком России.

На мой взгляд, организацию системы обеспечения непрерывности необходимо базировать на системе управления операционным риском (СУОР), и без функционирующей СУОР невозможно построить эффективную защиту от прерывания функционирования ни одной из этих областей.

[1] Отказы и (или) нарушения функционирования объектов информационной инфраструктуры, несоответствие их функциональных возможностей и характеристик потребностям КО (абз. 1 п. 1 Положения № 787-П).

[2] 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 № 86-ФЗ "О Центральном банке Российской Федерации (Банке России)", в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)».

[3] Риск отказов и (или) нарушения функционирования применяемых КО информационных систем и (или) несоответствия их функциональных возможностей и характеристик потребностям КО (абз. 3 п. 1.4 Положения № 716-П).

Подходы к построению системы обеспечения непрерывности деятельности

Уже сейчас Банк России в качестве одного из важных мероприятий, направленных на ограничение размера потерь от реализации событий операционного риска, выделяет такое мероприятие, как разработка планов по обеспечению непрерывности и (или) восстановления критически важных процессов и функционирования информационных систем, эксплуатация и использование которых обеспечивается кредитной организацией для осуществления процессов и операций, с учетом внешних факторов, влияющих на критически важный процесс и (или) информационную систему[1].

Очевидно, что работоспособность и эффективность системы обеспечения непрерывности зависят от того, насколько раньше банк начнет ее строить, не ожидая выпуска соответствующего нормативного акта.

Как соединить План ОНиВД и систему управления операционным риском

Одной из главных целей системы управления операционным риском является снижение уровня потерь от реализации событий операционного риска. Для достижения этой цели разрабатываются и внедряются как превентивные меры, способствующие митигации риска, так и мероприятия, направленные на уменьшение негативного влияния операционного риска.

Чрезвычайные и непредвиденные события, влияющие на способность банка непрерывно осуществлять свою деятельность, — это события внешние, в системе СУОР классифицируемые как источники операционного риска. Потери, полученные банком от реализации таких событий и затрат на восстановление его деятельности в повседневном режиме, — это всегда потери от реализации событий операционного риска.

Согласно требованиям п. 3 Приложения 5 к Положению № 242-П, разрабатывать План ОНиВД необходимо с учетом в том числе результатов анализа следующих факторов:

— виды и характер возможных нестандартных и чрезвычайных ситуаций, связанные с ними виды и степени воздействия на деятельность банка, способные нарушить режим его повседневного функционирования и способность выполнять принятые на себя обязательства;

— перечень критически важных для обеспечения режима повседневного функционирования КО внутренних банковских процессов;

— перечень автоматизированных информационных систем (ИС), обеспечивающих осуществление критически важных процессов;

[1] Абзац 12 п. 4.1.5 Положения № 716-П.

Майя САВИЦКАЯ

— показатели восстановления внутренних банковских процессов, в том числе срок восстановления, допустимый размер материальных затрат, допустимый размер потерь информации.

Разберем, какие источники информации нужно и целесообразно использовать при проведении такого анализа из реализованных КО «новых» регуляторных требований.

Критически важные процессы

Что же такое критически важные процессы? Под такими процессами Банк России подразумевает процессы, приостановление которых влечет за собой нарушение нормального осуществления деятельности финансовой организации, ее контрагентов и (или) ее клиентов, в том числе создает угрозу полной утраты их жизнеспособности[1].

Банк России установил, что в Плане ОНиВД КО в обязательном порядке должен быть определен перечень критически важных для обеспечения режима повседневного функционирования внутренних банковских процессов, которые являются *совокупностью последовательных и законченных действий по осуществлению банковских операций и сделок, а также автоматизированных информационных систем, обеспечивающих их осуществление*[2]. Однако перечень конкретных критически важных процессов в Положении № 242-П Банком России не установлен.

Вместе с тем Положениями № 716-П и № 787-П регулятор не просто ввел базовый принцип организации систем управления операционным риском и обеспечения операционной надежности — сосредоточить усилия риск-менеджмента именно на критически важных процессах, — но и установил достаточно полный перечень таких процессов[3].

Также после появления новых регуляторных норм в словаре риск-менеджера банка появился термин «технологический процесс», под которым понимается *набор взаимосвязанных операций с информацией и (или) объектами информатизации, используемых при функционировании финансовой организации и (или) необходимых для предоставления финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств*[4].

[1] Методические рекомендации Банка России по обеспечению непрерывности деятельности некредитных финансовых организаций от 18.08.2016 № 28-МР.

[2] Пункт 3.2 Приложения 5 к Положению № 242-П.

[3] Пункт 4.1.1 Положения № 716-П.

[4] ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций».

Подходы к построению системы обеспечения непрерывности деятельности

Не правда ли, это определение до степени смешения сходно с определением внутреннего банковского процесса в Положении № 242-П?

Таким образом, соединив установленные Банком России перечни технологических процессов и процессов банка, определенных им как критически важные, мы можем ввести для разработки КО внутренней методологии следующую практическую классификацию процессов банка, позволяющую построить достаточно аргументированный и понятийно прозрачный перечень критически важных процессов, на базе которого можно разрабатывать процедуры обеспечения непрерывности и интегрировать эти процедуры в План ОНиВД (табл. 2), а именно:

— процессы, связанные с предоставлением КО банковских услуг, — процессы, прерывание функционирования которых оказывает влияние на выполнение банком обязательств перед клиентами и контрагентами;

— процессы, связанные с внутренней деятельностью КО, — процессы, прерывание функционирования которых оказывает влияние на выполнение принятых банком на себя обязательств.

Таблица 2

Классификация процессов банка

Технологические процессы (Положение № 787-П)	**Критически важные процессы (Положение № 716-П)**	**Классификация процессов**	
		процессы, связанные с предоставлением КО банковских услуг	**процессы, связанные с внутренней деятельностью КО**
Технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады	Привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок)	X	
Технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады		X	
Технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет	Размещение указанных в предыдущем пункте привлеченных средств от своего имени и за свой счет	X	
Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам	Осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам	X	

Майя САВИЦКАЯ

Продолжение табл. 2

Технологические процессы (Положение № 787-П)	Критически важные процессы (Положение № 716-П)	Классификация процессов	
		процессы, связанные с предоставлением КО банковских услуг	процессы, связанные с внутренней деятельностью КО
Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам, за исключением переводов по распоряжениям участников платежной системы (для переводов денежных средств по распоряжениям участников платежной системы — в соответствии с Положением № 607-П[1])		X	
Технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц	Открытие и ведение банковских счетов физических и юридических лиц	X	
Технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц		X	
Технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)	Осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)	X	
Технологический процесс, обеспечивающий выполнение операций на финансовых рынках	Выполнение операций на финансовых рынках	X	
Технологический процесс, обеспечивающий выполнение кассовых операций	Выполнение кассовых операций	X	
Технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	Работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	X	
Технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе		X	
Технологический процесс, обеспечивающий идентификацию и (или) аутентификацию с использованием биометрических персо-		X	

[1] Положение Банка России от 03.10.2017 № 607-П «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков».

Окончание табл. 2

Технологические процессы (Положение № 787-П)	Критически важные процессы (Положение № 716-П)	Классификация процессов	
		процессы, связанные с предоставлением КО банковских услуг	процессы, связанные с внутренней деятельностью КО
нальных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия			
	Ведение бухгалтерского учета		X
	Представление отчетности в Банк России		X
	Поддержание ликвидности		X
	Соблюдение Закона № 152-ФЗ[1]		X
	Соблюдение Трудового кодекса РФ		X
	Соблюдение Закона № 395-1[2]		X
	Другие (внутренние) процессы, которые определены КО и прерывание функционирования которых оказывает влияние на выполнение обязательств перед клиентами и контрагентами		X

Информационные системы

Следующий фактор, знание о котором необходимо учесть при разработке Плана ОНиВД, — это автоматизированные информационные системы, обеспечивающие осуществление критически важных процессов.

Стоит обратить внимание, что одним из важных элементов СУОР является не только непосредственно составление перечня процессов, но и ведение учета взаимосвязей между критически важными процессами, работниками подразделений, информационными системами, задействованными при выполнении критически важных процессов, с учетом зависимости процессов от третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы). Постоянный мониторинг изменений в выявленных взаимосвязях и актуализация

[1] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

[2] Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».

Майя САВИЦКАЯ

перечня процессов — одна из задач риск-менеджмента операционного риска. Очевидно, что без оценки степени влияния информационной системы на бесперебойность функционирования процесса и без понимания уровня покрытия автоматическими процедурами отдельных звеньев жизненного цикла процесса невозможно разработать адекватные меры реагирования на приостановку процесса и предусмотреть необходимые ресурсы и шаги для восстановления его функционирования в обычном режиме и обеспечения непрерывности деятельности КО.

При разработке отдельных модулей Плана ОНиВД важно предусмотреть меры реагирования на такие факторы, способные оказать негативное влияние на непрерывность функционирования процессов, как выход из строя технических средств, сбои в работе автоматизированных ИС, отказ поставщиков услуг (провайдеров) от исполнения своих обязательств.

А так как в настоящее время ни один банковский процесс не осуществляется вручную, только полное и точное знание об участии конкретной ИС в осуществлении процесса и о критичности ее нефункционирования для непрерывности как отдельных процессов, так и деятельности КО в целом позволит ей оперативно отреагировать на различного рода негативные события и восстановить свою работоспособность в полном объеме.

Если подход банка к внедрению норм Положений № 716-П и № 787-П будет не формальным и все регуляторные требования будут проработаны и внедрены в полном объеме, то спектр аналитических ресурсов, которые можно и нужно использовать для учета требуемого фактора при разработке Плана ОНиВД, значительно расширяется.

Итак, какие же дополнительные ресурсы для решения этой задачи предлагают новые регуляторные требования:

1. Архитектура информационных систем.

Для выстраивания системы управления риском информационных систем, являющимся одним из видов операционного риска КО описывает во внутренних документах архитектуру информационных систем[1].

Базовым элементом архитектуры ИС является перечень ИС банка с соотнесением их с процессами, выполнение которых они обеспечивают (по уровню критичности процессов). И такая структурированная информация — именно то, что непременно необходимо включать в аналитические процедуры при разработке Плана ОНиВД.

[1] Пункт 8.5 Положения № 716-П.

Подходы к построению системы обеспечения непрерывности деятельности

Иные имеющиеся данные об архитектуре ИС также будут крайне информативны при разработке Плана ОНиВД. Например, в архитектуре также содержится информация об ИТ-поставщиках, обеспечивающих функционирование ИС, о поставленных ИТ-поставщиками ИС, обеспечивающих процессы банка, и структуре информационного обмена между такими системами и информационными системами банка.

2. Реестр ИТ-поставщиков.

Реализуя требования Банка России к обеспечению операционной надежности, банк на постоянной основе должен вести такой учетный регистр, как реестр ИТ-поставщиков[1]. В реестре фиксируются роли и степень участия ИТ-поставщика в реализации технологического процесса, что также является полезнейшим источником информации при разработке мер реагирования на прерывание процессов КО, включаемых в План ОНиВД.

3. Критичная архитектура.

Критичная архитектура (понятие, введенное регулятором в нормативную область требований к обеспечению операционной надежности КО)[2] — своего рода глобальная база данных, подлежащая формированию КО, о реализации жизненного цикла технологического процесса с сегментированием его на отдельные технологические участки, содержащая информацию:

— какие объекты информационной инфраструктуры обеспечивают функционирование процесса (в разрезе участков) и на каких его этапах и как эти объекты взаимодействуют между собой;

— какие существуют взаимосвязи и взаимозависимости банка с иными кредитными организациями, некредитными финансовыми организациями, ИТ-поставщиками в рамках технологического процесса/технологического участка.

Таким образом, существование Плана ОНиВД изолированно от СУОР — подход «вчерашнего» дня, не соответствующий сегодняшним и будущим вызовам системы риск-менеджмента и задачам системы внутреннего контроля банка.

Построение системы обеспечения непрерывности как единого процесса

Менеджмент непрерывности бизнеса определяет непрерывность бизнеса как стратегическую и тактическую способность организации планировать свою работу в случае инцидентов и нарушения

[1] Абзац 10 п. 6.1 Положения № 787-П.

[2] Пункт 6.1 Положения № 787-П.

Майя САВИЦКАЯ

ее деятельности, направленную на обеспечение непрерывности деловых операций на установленном приемлемом уровне[1]. И, ставя перед собой цель обеспечить непрерывность функционирования банка вообще, необходимо говорить о такой задаче, как создание единой системы обеспечения непрерывности. Системы как совокупности связанных между собой элементов, находящихся и во взаимном влиянии друг на друга, которая строится как единая область управления.

Вернемся к табл. 1 и вспомним перечень областей, непрерывность функционирования которых необходимо обеспечить банку:

1. Деятельность банка.
2. Осуществление критически важных процессов и критически важных операций.
3. Оказание банковских услуг при выполнении критически важных процессов, связанных с предоставлением банковских услуг.
4. Оказание финансовых услуг.
5. Функционирование информационных систем.

В каждой из этих областей непрерывность не может быть обеспечена обособленно. Только при их объединении в единую область управления (рис. 1), использовании единых методологических подходов и аналитических инструментов, разработке единых

Рисунок 1

Единая область управления непрерывностью

[1] ГОСТ Р 53647.1-2009 «Национальный стандарт Российской Федерации. Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство».

Подходы к построению системы обеспечения непрерывности деятельности

многофункциональных мероприятий по обеспечению непрерывности можно построить систему обеспечения непрерывности.

При построении единой системы обеспечения непрерывности отдельное внимание необходимо уделить процедурам управления риском информационных систем (риск ИС) и риском информационной безопасности (риск ИБ) и их корреляции/интеграции с процедурами Плана ОНиВД в части методологических подходов к обеспечению непрерывности функционирования информационных систем.

Процедуры управления рисками ИС и ИБ в первую очередь строятся с учетом влияния ИС на бесперебойную работу процессов и операционную устойчивость банка, а достижение операционной устойчивости является также и одной из основных целей Плана ОНиВД.

В рамках управления риском ИС[1] коллегиальный исполнительный орган банка определяет должностное лицо (лицо, его замещающее), ответственное за обеспечение непрерывности функционирования ИС, и соответствующее структурное подразделение. Безусловно, разрабатываемые и проводимые таким должностным лицом/подразделением мероприятия по управлению риском ИС (например, тестирование информационных систем (при проведении сценарного анализа операционного риска) на их влияние на непрерывность осуществления критически важных процессов и (или) функционирования иных информационных систем) должны быть согласованы с Планом ОНиВД. Важно, чтобы взаимодействие должностного лица, ответственного за обеспечение непрерывности функционирования ИС, с менеджером Плана ОНиВД было постоянным.

Обеспечение непрерывности через единый центр управления

В настоящее время лучшие практики предлагают банкам пересмотреть «узкую» специализацию Плана ОНиВД, интегрировав с ним все области деятельности КО, в которых также важна задача обеспечения непрерывности.

Какие же выгоды можно получить при реализации такого подхода:

1. В распоряжении всех служб банка появится единый классификатор процессов по уровню критичности, что упростит диалог между владельцами процессов, службой информационной безопасности и ИТ-подразделениями. Нахождение в одном информационном поле

[1] Пункт 8.8.10 Положения № 716-П.

значительно упрощает коммуникацию и позволяет оперативно определить и приоритизировать процессы по степени их влияния на те или иные аспекты бизнеса, по необходимости их повседневного функционирования.

2. Такие ресурсы данных, как архитектура ИС, реестр ИТ-поставщиков, критичная архитектура, — колоссальная база данных, дающая широкий спектр информации о взаимосвязи критически важных для банка процессов с персоналом банка, третьими лицами, информационными системами банка и третьих лиц и об их взаимном влиянии.

3. Положение № 242-П рекомендует привлекать к проверке (тестированию) Плана ОНиВД контрагентов, в том числе поставщиков услуг (провайдеров), от деятельности которых зависят непрерывность осуществления критически важных банковских процессов и (или) сроки их восстановления. Реестр ИТ-поставщиков — готовый перечень кандидатов для включения в процедуры тестирования Плана. И их выбор будет построен на риск-ориентированном подходе с учетом всей информации о степени участия ИТ-поставщика в функционировании процесса, степени его технологической зависимости от поставщика ИС. Также такая информация будет релевантна для принятия решений об использовании альтернативных поставщиков при невозможности получить услуги, необходимые для осуществления процесса, в случае отказа поставщика от исполнения договорных обязательств или невозможности оказания им услуг в полном объеме.

4. База событий операционного риска — источник данных о фактах воздействия на банк внешних непредвиденных ситуаций, об их источниках, финансовых последствиях и эффективности ответных мер по снижению вероятности получения такого же объема негативных последствий в будущем. Анализ таких данных поможет более продуктивно подойти к оценке потенциального влияния чрезвычайных и непредвиденных ситуаций на конкретные бизнес-процессы. Также и меры по оперативному реагированию на последствия прерывания деятельности и возвращению ее в повседневный режим смогут быть более предметными, учитывающими накопленный опыт реализации процедур управления операционным риском.

5. Собираемую банком информацию о деградации технологических процессов и реализованных инцидентах операционной надежности, об их причинах и влиянии деградации и (или) простоя технологического процесса на непрерывность оказания банковских и финансовых

услуг можно использовать при разработке Плана ОНиВД по аналогии с информацией, получаемой из базы событий операционного риска.

Вместо заключения: новый вид операционного риска

Нормативные требования к обеспечению непрерывности и восстановлению деятельности кредитной организации поступательно развиваются и расширяются.

Сравнительно недавно Банком России был выделен новый вид операционного риска — риск нарушения непрерывности деятельности (РННД), представляющий собой риск нарушения способности кредитной организации (головной кредитной организации банковской группы) поддерживать свою операционную устойчивость[1].

При этом регулятор подчеркнул важность этого вида риска в системе риск-менеджмента. Так, в комплекс мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, КО необходимо включать мероприятия, направленные на предотвращение и (или) снижение вероятности событий РННД, и мероприятия, направленные на ограничение размера потерь от реализации таких событий.

Устанавливая для финансовых организаций требования к операционной надежности, Банк России также обращает внимание, что процессы обеспечения операционной надежности существенным образом связаны с поддержанием КО непрерывности деятельности и ее восстановлением после возможных прерываний.

Таким образом, политика обеспечения непрерывности должна встать в один ряд с иными документами риск-менеджмента, дополняя и расширяя их нормы и выстраивая между ними методологические связи (рис. 2).

Систематизация и объединение методологических подходов и правил организации обеспечения непрерывности в отдельных областях деятельности — текущая потребность для создания эффективной системы обеспечения непрерывности.

И только наличие такой системы сможет качественно повысить способность КО оперативно и своевременно реагировать на события прерывания бизнеса, возвращая его в режим повседневного

[1] Абзац 12 п. 1.4 Положения № 716-П.

Майя САВИЦКАЯ

Рисунок 2

Место политики непрерывности в комплексе документов риск-менеджмента

функционирования, а также позволит банку снизить уровень потерь от воздействия на его деятельность внешних источников риска и приостановления его отдельных процессов и операций.