Сергей Пищиков
независимый эксперт по управлению рисками компаний инфраструктуры рынка ценных бумаг

Александр Баранов
директор департамента риск-менеджмента АО «Ай Кью Джи Управление Активами», председатель Комитета ПАРТАД по внутреннему контролю, внутреннему аудиту и управлению рисками

УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ: ИСТОРИЯ, ПРАКТИКА И РЕГУЛЯТОРНЫЕ ТРЕБОВАНИЯ

Обеспечение непрерывности бизнеса, т. е. способность постоянно и непрерывно поддерживать осуществление внутренних критически важных процессов в любых условиях, в том числе при чрезвычайных обстоятельствах, является приоритетной задачей фактически любой компании, в частности некредитной финансовой организации (НФО). А в 2016 г., когда ЦБ РФ утвердил Методические рекомендации от 18 августа 2016 г. № 28-МР[1], вопрос управления непрерывностью деятельности НФО актуализировался и на регуляторном уровне.

В настоящей публикации описывается эволюция подходов и существующие стандарты организации непрерывности деятельности, практика управления в смежных секторах финансового рынка, особенности определения понятия ЧС[2] в нормативных документах ЦБ РФ и некоторые нюансы отражения инцидента непрерывности бизнеса в разрезе управления рисками, непрерывностью деятельности и информационной безопасности. Рассмотрены возможные перспективы нормативного регулирования непрерывности деятельности НФО.

[1] Методические рекомендации Банка России от 18.08.2016 г. № 28-МР «По обеспечению непрерывности деятельности некредитных финансовых организаций».
[2] Чрезвычайная ситуация.

СКАЗКА О ПОТЕРЯННОМ ВРЕМЕНИ

В 2007 г. Нассим Николас Талеб[3] выдвинул понятие «черный лебедь» (*Black Swan*), чтобы описать непредвиденные события, которые поражают внезапно, например: террористический акт в США 11 сентября 2001 г., вспышки смертельно опасных заболеваний, японское землетрясение 2011 г., цунами и последующая авария на ядерном объекте. И хотя чаще всего в организации «залетают» более мелкие «черные лебеди» (отказ коммунальных сетей, частичное возгорание офиса, падение сервера, обрыв кабеля, отключение электричества и т. д.), но каждый из них также способен осложнить, приостановить или даже прервать нормальную деятельность компании. Учитывая, что предпринимательство по своей экономической сути — процесс непрерывный, риск «потерянного времени» является одним из самых разрушительных рисков, присущих бизнесу. Ведь время — это, как известно, деньги.

Тема управления непрерывностью деятельности настолько актуальна, что подчас встречается в самых неожиданных местах: в народных пословицах и поговорках, художественных произведениях. Например, в «Сказке о потерянном времени» В. Губарева[4] четыре злых волшебника решили вернуть себе молодость, для чего должны были найти людей, **бесцельно растрачивающих свое время**. Удача улыбнулась им в лице безалаберных школьников. Из-за колдовства школьники постарели, а волшебники превратились в детей. Но у превращенных остался шанс: до заката солнца им надо найти избушку волшебников и перевести стрелки волшебных часов назад.

Мораль сказки с точки зрения управления непрерывностью деятельности выглядит следующим образом. С одной стороны, источником риска являются систематические нарушения учениками своих функциональных обязанностей или даже, чего уж говорить, «мошеннические» действия в целях получения личной выгоды, с другой — уже явно мошеннические действия третьих лиц — группы злых волшебников. Объектом риска является процесс учебы (бизнес-процесс), последствия — катастрофическое разрушение (старение) «активов» компании молодых людей — их непутевых жизней. Неявное рисковое событие — очередное опоздание, усиленное кумулятивным эффектом прошлых прогулов. Многочисленные ошибки и злоупотребления при выполнении критического бизнес-процесса позволили третьим лицам нанести ребятам катастрофический ущерб. Однако не без помощи случая был оперативно составлен и реализован План аварийного восстановления (***DRP***[5]), и все закончилось благополучно.

На этот раз ребятам повезло, но «сказка — ложь, да в ней намек, добрым молодцам урок». Исходя из сюжета произведения, молодые люди смогли переосмыслить свои взгляды на жизнь, учебу, управление личными рисками и осознать необходимость перейти на более высокий уровень управления непрерывностью деятельности: от спонтанной ***DRP*** к регулярному ***BCP***[6] (непрерывной учебе). А тут уж совсем недалеко и до ***BCM***[7], что, несомненно, поможет бывшим двоечникам повысить свою личную эффективность и, возможно, стать незаурядными личностями.

Характерно, что из всех жизненных рисков автор выделил в качестве основного именно риск потерянного времени, как воздействующий на единственный ресурс, который нельзя восполнить. Ведь «жизнь невозможно повернуть назад, и время ни на миг не остановишь».

На сегодняшний день существуют несколько точек зрения, являющихся причиной разногласий между специалистами по непрерывности бизнеса и управлению рисками:

- процессы управления непрерывностью бизнеса и рисками тесно взаимосвязаны «на равных»;
- процессы связаны, при этом непрерывность — компонент риска;
- процессы связаны, при этом риски — компонент непрерывности;
- процессы взаимосвязаны, но сосуществуют без какой-либо иерархии между ними;
- процессы не взаимосвязаны.

В сущности, непрерывность это прежде всего свойство бизнес-процесса, а ее нарушение — уже реализовавшийся «риск потерянного времени». Большинство рисков, в том числе кредитный, ликвидности, рыночный, имеют в своей структуре и процессную составляющую: риски организации процесса. В методологии рисков эти процессные риски условно выделены в отдельный риск — операционный. То есть, если кредитный специалист ошибется в выборе банка, в котором компания имеет расчетный счет (депозит), или казначей не оптимально диверсифицирует портфель ценных бумаг, по сути, это — событие операционного риска (ошибка сотрудника), однако потери по этим направлениям деятельности будут отнесены к кредитному и рыночному рискам. Фактически любой финансовый риск — это произведение операционного риска (риска организации процесса, включая квалификацию сотрудников и т. д.) на независимый от компании финансовый риск (риск изменения макроэкономической ситуации, колебания процентных ставок, «истинное» финансовое положение клиента, контрагента и т. д.).

Соответственно, у каждого бизнес-процесса присутствуют свои специфические параметры и свой специфический профиль рисков. Но при этом каждый процесс всегда характеризуется определенным уровнем (параметрами) непрерывности, нарушение которого — реализация риска потери непрерывности. Особенность этого риска в том, что он в разной мере присущ любым бизнес-процессам на всех уровнях управления компанией, в том числе на стратегическом.

Риски потери непрерывности рассматриваются в ГОСТ Р ИСО/МЭК 31010 «Методы оценки риска». Так, метод анализа воздействия на бизнес *(BIA*) позволяет исследовать, как ключевые виды отказов/нарушений/разрушений могут повлиять на ключевые виды деятельности и процессы организации, а также идентифицировать и количественно определить возможности, необходимые для управления организацией в этих условиях. Параметром непрерывности в данном случае является определение максимально допустимого периода простоя при нарушении/разрушении для каждого процесса, основанного на идентифицированных последствиях и критических факторах выполняемых видов деятельности.

Еще в ГОСТ Р 53647.1 указано: *«Менеджмент непрерывности бизнеса (МНБ) является **дополнительной структурой** по отношению к менеджменту риска, которая позволяет осознать существующие опасности для деятельности и бизнеса организации, а также последствия возникновения опасных событий, подчеркивая ее отношение к противодействию нарушениям».* Однако уже в стандарте ГОСТ Р 22301 МНБ выделен как ***«Полный***

---

[3] Нассим Николас Талеб — американский экономист и трейдер. Основная сфера научных интересов — изучение влияния случайных и непредсказуемых событий на мировую экономику и биржевую торговлю, а также механизмы торговли производными финансовыми инструментами.

[4] Виталий Георгиевич Губарев (1912–1981 гг.) — русский советский детский писатель.

[5] DRP (Disaster Recovery Planning) — план восстановления после сбоев.

[6] BCP (Business Continuity Planning) — планирование непрерывности бизнеса.

[7] BCM (Business Continuity Management) — управление непрерывностью бизнеса.

***процесс управления**, предусматривающий идентификацию потенциальных угроз и их воздействия на деятельность организации, который создает основу для повышения устойчивости организации к инцидентам и направлен на реализацию эффективных ответных мер против, что обеспечивает защиту интересов ключевых причастных сторон, репутации организации, ее бренда и деятельности, добавляющей ценность».*

Очевидно, что на данный момент функционал управления непрерывностью деятельности отнюдь не исчерпывается управлением рисками непрерывности. Современный МНБ как эффективное средство управления и контроля любого бизнес-процесса присутствует во всех ключевых процессах управления организацией, таких как:

- улучшение отношений со стейкхолдерами, что включает ориентацию покупателей на продукты, произведенные с учетом принципов ответственности (экологической и социальной), внимание кредиторов и инвесторов к этичности бизнеса (о чем говорит растущая популярность социально-ответственных инвестиций), потребность сотрудников делать вклад в устойчивое развитие и т. д.;
- повышение эффективности деятельности компании (за счет повышения энергоэффективности, уменьшения отходов, снижения процента брака продукции, штрафных выплат и т. д.);
- снижение рисков компании (как репутационных, так и рисков санкций со стороны регуляторов);
- управление цепочками поставок;
- управление ликвидностью и платежеспособностью предприятия;
- управление теми же рисками — непрерывность управления системой управления рисками, и это не тавтология;
- управление любым важным для компании процессом и т. д.

У МНБ есть еще одно уникальное свойство. Она предлагает структуру для понимания того, как создается ценность (доход, прибыль или стоимость компании) и как она поддерживается в компании.

Так все-таки это — риск или не риск? С точки зрения «потерянного времени», конечно же, риск, а с точки зрения времени приобретенного, выигранного — конкурентное преимущество! Средство управления рисками и бизнесом, средство сжимать, экономить и управлять временем. Не зря народная мудрость гласит: «Порядок время бережет», или обратимся к Суворову: «Скорость нужна, а поспешность вредна. Время драгоценнее всего». А как известно Александр Васильевич не проиграл ни одного сражения!

ЭВОЛЮЦИЯ УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Ни один план сражения не переживет первую встречу с врагом.

Управление во многом сводится к умению справляться с неопределенностями. Старая немецкая военная мудрость гласит: «Ни один план сражения не переживет первую встречу с врагом». Немцы первыми начали применять военные игры (тактические учения на карте или макете, которые представляли собой форму анализа сценария) для подготовки, что во многом способствовало их военным успехам в начале Второй мировой войны. Одна из основных целей сценарного планирования — выявить тенденции развития ситуации в состоянии неопределенности и, используя их, изучить результаты потенциальных событий, т. е. осмыслить «неосмысляемое». Большой вклад в сценарное планирование внес американский ученый Герман Кан (*Herman Kahn*), который работал в корпорации *RAND*, крупнейшем аналитическом центре США, а затем основал *Hudson Institute*. В моделировании Герман Кан широко использовал теории игр. Его работы стали существенным вкладом в развитие ядерной стратегии Соединенных Штатов. Им же впервые была сформулирована идея Машины Судного дня — своеобразный апофеоз доктрины взаимного гарантированного уничтожения. В 60-х гг. XX в. Герман Кан впервые начал использовать метод сценариев для решения не только военных, но и бизнес-задач.

В 1970-х гг. сценарный метод вышел на новый уровень развития благодаря идеям Пьера Вака, работавшего в *Shell*[8] — компании, которая первой спланировала сценарий отсутствия доступа к основным компьютерам и инвестировала средства в создание *IT*-бэкапов. На идеях сценарного планирования также базировался первый этап управления непрерывностью бизнеса — планирование восстановления после сбоев (*Disaster Recovery Planning, DRP*) — методика, появившаяся в 1950–1960 гг. Само слово *disaster* (авария, катастрофа) происходит от латинского «несчастливая звезда» (*dis* + *astro*), так как бедствия в античности воспринимались как результат неблагоприятного астрологического влияния (воздействия звезд).

Целью *DRP* является снижение влияния аварии и выполнение действий, необходимых для максимально быстрого восстановления деятельности компании после стихийного или антропогенного бедствия. Планы, однако, не включали мер предотвращения: аварийное восстановление *DR*[9] фокусировалось в основном на ИТ[10] и технологических системах, поддерживающих критические бизнес-функции организации.

На этом этапе компании начали хранить резервные копии критически важных бумажных или электронных данных на альтернативных сайтах — «сайтах горячего доступа». Основным драйвером развития *DRP* на тот момент послужило стремление банков США лучше защитить свои корпоративные центры обработки данных. Сначала хранилище данных вне офиса использовалось отдельными предприятиями от случая к случаю, но к концу 1970-х гг. их необходимость стала очевидной и появились специализированные компании, предлагавшие услуги хранения. Первым крупным коммерческим поставщиком таких услуг стала *Sun Information Systems*[11] в 1978 г., но уже в 1980-х в одних только США «горячие» резервные вычислительные центры предлагали более ста компаний.

За последующие два десятилетия *DRP* развился в *BCP* и затем в *BCM* (см. рисунок). Эта эволюция лучше всего характеризуется серией подходов, предложенных *Elliott, Swartz and Herbane* (2010 г.) [10].

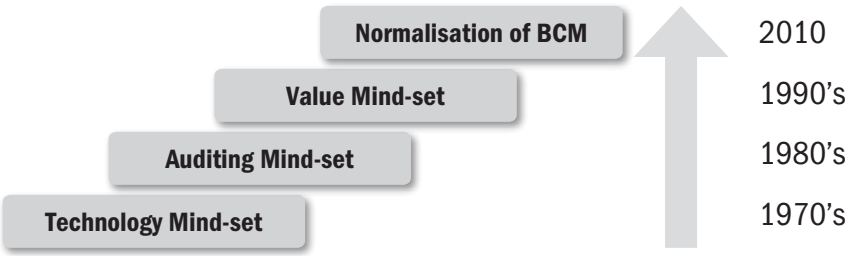
1. *Technology Mind-set* (технологический подход). Этот подход, сфокусированный исключительно на технологическом аспекте, предполагает, что бедствия были вызваны отказом технологий, и игнорирует бизнес-причины. «*Фокусировка на технологиях позволяет только частично исследовать причины бедствий и стремится рассматривать их результаты или симптомы, а не предотвращать их*»[1].

2. *Auditing Mind-set* (аудиторский подход). Шаг на пути от *DRP* к *BCP*. Помимо управления технологическими нарушениями этот метод предполагает защиту деловой активности, в основном ориентируясь на внешнее регулирование.

Этот этап делится на четыре фазы с точки зрения эволюции нормативного законодательства: начальное формирование законодательства (середина

[8] Royal Dutch Shell—нидерландско-британская нефтегазовая компания. Штаб-квартира в Гааге (Нидерланды).
[9] Disaster Recovery.
[10] ИТ — информационные технологии.
[11] Sun Microsystems — американская компания, производитель программного и аппаратного обеспечения, основанная в 1982 г. С апреля 2009 г. по январь 2010 г. была поглощена корпорацией Oracle.

ЭВОЛЮЦИЯ БИЗНЕС-ПРОЦЕССОВ УПРАВЛЕНИЯ



1970-х — середина 1990-х гг.); появление стандартов и расширение их влияния (середина1990-х — 2001-х гг.); состояние после 11 сентября, ускорение и фокусировка (2002—2005 гг.); интернационализация, конкурирующие стандарты и прорыв (2006—2010 гг.). Подход *BCP* уже гораздо шире *DRP* и предусматривает подготовку к инцидентам, которые могут нарушить деятельность организации. *BCP* помог определить и понять комплексные причины нарушения деятельности организации. Было замечено, что наличие *BCP* как центрального бизнес-процесса управления дает организации конкурентные преимущества. Аудиторский подход, тем не менее, не принимал во внимание влияние человеческого фактора в развитии деструктивных событий и воздействие этого фактора на эффективность процесса *BCP*. Основное внимание аудиторского подхода было сконцентрировано на том, как предотвратить, «пережить» деструктивное событие, а также обеспечить соответствие требованиям внешнего регулирования.

На стыке 80-х — 90-х гг. XX в. область *BCP* была расширена за счет элементов кризисного управления (*Crisis Management, CM*).

3. *Value Based Mind-set* (подход, направленный на создание стоимости). Шаг на пути от *BCP* к *BCM.* Все сфокусировано больше на самом бизнесе, чем на соблюдении инструкций и минимизации технологических ошибок. Фактически при этом подходе *BCM* рассматривается как процесс, способный увеличивать стоимость организации.

При этом подходе границы *BCP* были расширены и включали, помимо вопросов ИБ, практически все аспекты деловой активности, в том числе процессы управления человеческими ресурсами, которые являются самой сложной задачей в реализации и управлении. *BCP* превращается в целостную структуру взглядов на методы обеспечения непрерывности бизнеса — устойчивости организации к всевозможным сбоям, разрушениям и потерям, прежде всего финансовым.

4. *Business Continuity Management within Organizational Resilience* (управление непрерывностью бизнеса в рамках корпоративной устойчивости). В целях достижения корпоративной устойчивости (*OR*[12]) *BCM* как элемент *OR* должен учитывать человеческие, организационные и социальные аспекты корпоративной среды. *OR* базируется на понятии «тройного итога» деятельности организации, включающего в себя финансовое и экологическое измерение, соответствующее идее экоэффективности с добавлением оценки социального и широкого экономического воздействия. Главными компонентами корпоративной устойчивости являются 3*P*: *People*, *Planet*, *Profits* (люди, планета, прибыль). В соответствии с моделью 3*P* ее элементы находятся в симбиозе, и развитие одного из компонентов приводит к развитию остальных.

СТАНДАРТЫ И ПОДХОДЫ К ВОПРОСУ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ, ИЛИ «В АНГЛИИ ВСЕ ЕСТЬ»

Как уже было сказано, управление непрерывностью деятельности началось с проработки информационно-технологических аспектов. Уже с 1983 г. финансовые институты США должны были иметь планы восстановления, записанные на бумаге. В 1988 г. в США был основан Международный институт аварийного восстановления, а в 1994 г. в Великобритании — Институт непрерывности бизнеса (*Business Continuity Institute*).

В 1995 г. по заказу правительства Великобритании был разработан прародитель международных стандартов управления информационной безопасностью — британский *BS* 7799 (прообраз *ISO* 27000). Документ описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью организации, определенных исходя из лучших примеров мирового опыта в данной области. Стандарт во многом опередил свое время. Проработка вопросов безопасности на таком уровне еще никого особенно не интересовала.

В 1990-х гг., помимо США и Великобритании, в Канаде, Сингапуре, Японии и других странах вступили в силу ряд нормативных документов по регулированию непрерывности. Однако первыми по-настоящему интернациональными документами в этой области стали «Рекомендации по наблюдению за непрерывностью деятельности для системно значимых платежных систем (СиПС)» Европейского центрального банка и выпущенные Базельским комитетом по банковскому надзору «Руководящие принципы обеспечения непрерывности деятельности», определяющие понятийный аппарат управления непрерывностью бизнеса для финансовых организаций и систематизирующие подходы к нему.

В документе были сформулированы базовые принципы управления непрерывностью:

- Вся полнота ответственности за управление непрерывностью бизнеса, *в отличие от управления другими рисками*, ***ложится на совет директоров*** и высшее руководство организации.
- Необходимо оценивать опасность и составлять планы на случай крупного операционного нарушения.
- Участники финансового сектора должны сформулировать цели восстановления, отразить в них уровень потенциального риска для операций финансовой системы. Участники финансового сектора, которые оказывают критически важные услуги в рамках данной финансовой системы или могут служить причиной значительного риска для операций системы, должны придерживаться более высоких стандартов в управлении непрерывностью бизнеса, чем другие участники этого сектора. ***Принцип пропорциональности оказался непривычным для ряда участников финансового сектора,*** *п*оскольку меры, необходимые для повышения устойчивости финансовой системы, потребовали больших затрат, чем меры, которые предприняли бы такие участники по своей воле.
- План обеспечения непрерывности бизнеса должен отражать все аспекты осуществления внутреннего и внешнего обмена информацией в случае крупного операционного нарушения. Этот принцип еще раз поясняет, что ***четкий и регулярный обмен информацией при наступлении крупного операционного нарушения*** является необходимым условием выхода из кризиса и сохранения доверия населения.

[12] Organizational Resilience — корпоративная устойчивость.

• В случае крупного операционного нарушения, которое может происходить в пределах нескольких различных юрисдикций, необходимо разработать процедуры оповещения и обмена информацией о подобном нарушении.

• Для того чтобы разработанные Планы ОНиВД[13] могли действительно предупредить и минимизировать последствия ЧС и обеспечить восстановление в требуемое бизнесом время, нужно проводить регулярную проверку Планов ОНиВД на актуальность, а также оценивать эффективность и результативность их работы.

• Контроль за управлением непрерывностью бизнеса со стороны финансовых органов. Финансовые органы (в РФ это ЦБ РФ) обязаны проводить внешнюю независимую оценку участников деятельности финансового сектора.

Почти одновременно с Базельскими[14] рекомендациями в ноябре 2006 г. Британский институт стандартов опубликовал первую часть стандарта *BS* 25999–1 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство», а в ноябре — вторую. Обе части стандарта внесли значительный вклад в разработку проблематики непрерывности деятельности и легли в основу многих национальных и международных стандартов.

ЦБ РФ плавно подготавливает некредитные финансовые организации к предоставлению обязательной отчетности по непрерывности деятельности.

На основе *BS* 25999 разработан и ныне действующий главный международный стандарт *ISO* 22301, содержащий описание основных элементов системы управления непрерывностью бизнеса: планирования, разработки, внедрения, сопровождения, мониторинга, анализа и непрерывного улучшения. Стандарт *ISO* 22301 может быть применен любой организацией, вне зависимости от ее размера, вида деятельности и формы собственности. Тем не менее внедрение стандарта особенно актуально для финансовых, телекоммуникационных, энергетических компаний, ритейлеров и многих государственных структур — одним словом, для практически любых организаций, которым критически важна непрерывность деловой активности. Многие стандарты непрерывности деятельности, действующие в РФ, также своей основе содержат принципы и положения *BS* 25999.

Для кредитных организаций в России тема управления непрерывностью деятельности получила актуальность в марте 2009 г., в связи с внесением Банком России дополнений в Положение ЦБ РФ от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах». Речь идет о Приложении № 5 «Рекомендации по структуре и содержанию плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (далее — План ОНиВД КО) в случае возникновения непредвиденных обстоятельств, а также по организации проверки возможности его выполнения». Дополнения устанавливают необходимость наличия Планов ОНиВД и весьма конкретно определяют требования надзорного органа к их структуре и содержанию.

Однако из материалов, представленных на семинарах, проводимых представителями Банка России, становилось понятно, что ЦБ РФ не рекомендовал рассматривать План ОНиВД КО в отрыве от практики управления непрерывностью деятельности в соответствии с лучшими мировыми стандартами. Область действия стандарта ГОСТ Р ИСО 22301 и семейства ГОСТ Р 53647 шире, чем у Положения Банка России. Стандарт более подробно описывает некоторые вопросы, которые возникают как при построении системы управления непрерывностью бизнеса, так и при разработке Плана. Поэтому стандарты удачно дополняют Положение № 242-П и содержат множество «подсказок», которые окажут неоценимую помощь при попытке выполнить на практике требования отечественного регулятора.

8 августа 2016 г. ЦБ РФ опубликовал «Методические рекомендации по обеспечению непрерывности деятельности некредитных финансовых организаций № 28-МР» (далее — План ОНиВД НФО). Данный документ уже явно содержит предложение использовать наравне с вышеуказанными методическими рекомендациями национальные стандарты непрерывности деятельности: ГОСТ Р 53647.1–2009, ГОСТ Р 53647.2–2009, ГОСТ Р 53647.3–2015, ГОСТ Р 53647.4–2011 и в части рисков национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 31010–2011 «Менеджмент риска. Методы оценки риска».

ЧРЕЗВЫЧАЙНЫЕ СОБЫТИЯ И НАСКОЛЬКО ОНИ ЧРЕЗВЫЧАЙНЫЕ. План ОНиВД глазами ЦБ РФ: от кредитных к некредитным финансовым организациям. Как одним инцидентом трех генералов накормить?

В плане ОНиВД КО нестандартной или чрезвычайной ситуацией считается событие, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению кредитной организацией принятых на себя обязательств. Планы восстановления рекомендуется разрабатывать применительно к крупномасштабным нестандартным и чрезвычайным ситуациям, сопоставимым с чрезвычайной ситуацией муниципального характера. Это явный ***DRP***.

При этом рекомендуется предусмотреть возможность реализации отдельных автономных частей Плана ОНиВД в случае нестандартных и чрезвычайных ситуаций ***меньшего масштаба***, связанных с проявлением (по отдельности или в сочетаниях) таких факторов, как выход из строя технических средств, сбои в работе автоматизированных информационных систем кредитной организации, нарушение коммунальной инфраструктуры, перебои в электроснабжении и т. д. В этой части регламентируются уже процессы уровня ***BCP***.

В Плане ОНиВД НФО акценты расставлены несколько иначе: ЧС определяется в контексте повседневного функционирования компании. Финансовой организации рекомендуется обеспечить непрерывность деятельности, под которой понимается поддержание режима повседневного функционирования внутренних критически важных процессов финансовой организации. Под критически важными процессами в целях настоящих методических рекомендаций понимаются процессы финансовой организации, ***приостановление которых влечет нарушение нормального осуществления деятельности финансовой организации***, ее контрагентов и (или) ее клиентов, в том

[13] ОНиВД — обеспечение непрерывности и/или восстановление деятельности.
[14] Рекомендации Базельского Комитета по банковскому надзору, основанного в 1974 г. при Банке международных расчетов.

СТАНДАРТЫ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ

ГОСТ Р	Источник
ГОСТ Р ИСО 22301–2014 «Системы менеджмента непрерывности бизнеса. Общие требования»	ISO 22301:2012 Международный стандарт ISO 22301, разработанный в 2012 г. на основе стандарта BS 25999
ГОСТ Р 53647.1–2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство»	BS 25999–1:2006 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство»
ГОСТ Р 53647.2–2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования»	BS 25999–2:2007 «Менеджмент непрерывности бизнеса. Часть 2. Спецификация»
ГОСТ Р 53647.3–2010 «Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению»	Разработан с учетом основных нормативных положений национального документа Великобритании BIP 2142:2012 «Маршрутная карта менеджмента непрерывности бизнеса
ГОСТ Р 53647.4–2011 «Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности»	ISO/PAS 22399:2007 «Социальная безопасность. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности»
ГОСТ Р 53647.5–2012 «Менеджмент непрерывности бизнеса. Готовность к опасным ситуациям и инцидентам	Разработан с учетом основных нормативных положений международного документа IWA 5:2006* «Готовность к опасным ситуациям» (IWA 5:2006 Emergency preparedness, NEQ)
ГОСТ Р 53647.6–2012 «Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных»	Соответствует основным положениям национального стандарта Великобритании BS 10012:2009 «Защита данных. Требования к системе менеджмента персональной информации»
ГОСТ Р 53647.8–2013 «Менеджмент непрерывности бизнеса. Управление человеческими ресурсами»	Настоящий стандарт разработан с учетом основных нормативных положений документа Великобритании PD 25111:2010 «Менеджмент непрерывности бизнеса. Руководство по человеческим аспектам непрерывности бизнеса»
ГОСТ Р 53647.9–2013 «Менеджмент непрерывности бизнеса. Управление организацией в условиях кризиса»	PAS 200:2011 «Менеджмент в условиях кризиса. Руководство и надлежащая практика»

числе создает угрозу ***полной утраты их*** жизнеспособности.

Таким образом, основной функцией управления непрерывностью является не восстановление деятельности после катастрофических событий, а обеспечение непрерывности и предотвращение ситуации, вызванной событиями, ***нарушающими нормальную деятельность организации***, в том числе создающими угрозы ***полной утраты жизнеспособности***. К примеру, в ГОСТ Р ИСО 22301, на который в той или иной мере ориентируются оба документа, ЧС (инцидент) определен наиболее нейтрально — как ситуация, которая может произойти и привести к нарушению деятельности организации, разрушениям, потерям, чрезвычайной ситуации или кризису в бизнесе.

В Плане ОНиВД НФО конкретно сформулированы рекомендации по обеспечению непрерывности функционирования информационных систем, в том числе: определение перечня информационных систем и обрабатываемой информации, используемых для обслуживания критически важных процессов; внедрение и настройка программно-технических средств, обеспечивающих защиту информационных систем; разработка политики информационной безопасности и осуществление на постоянной основе мероприятий по защите информационных систем от противоправных действий.

В целях практической реализации рекомендуется ориентироваться на положения нормативных актов Банка России и документов, разрабатываемых Банком России, в рамках законодательства Российской Федерации о техническом регулировании (национальные стандарты, стандарты Банка России, рекомендации Банка России в области стандартизации). Скорее всего, имеется в виду широко распространенный (и единственный) Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации — СТО БР ИББС [9] и семейство стандартов по информационной безопасности — ГОСТ Р ИСО/МЭК 27000 (см. таблицу).

В Плане ОНиВД НФО не детализируется типология возможных критических процессов в отличие от плана ОНиВД КО, регламентирующего помимо восстановления инфраструктурных сбоев «*обеспечение непрерывности производства продукции и оказания услуг*», таких как непредвиденный дефицит ликвидности, в том числе по причине потери деловой репутации, отказ кредитных организаций-корреспондентов и (или) организаций-контрагентов, в том числе поставщиков услуг (провайдеров) кредитной организации, от исполнения своих обязательств и т. д.

Скорее всего, это объясняется разнообразием видов деятельности некредитных финансовых организаций, однако создается впечатление, что основной упор в ОНиВД НФО все-таки делается на обеспечение непрерывности технических и технологических систем.

В части рекомендаций по непрерывности деятельности Планы ОНиВД для кредитных и некредитных финансовых организаций фактически идентичны.

Из нового в ОНиВД НФО можно отметить акцент на необходимость утверждения плана обеспечения непрерывности советом директоров компании, что коррелирует с рекомендациями Базельского комитета. И предложения по включению в отчет по непрерывности ряда показателей устойчивости технических средств, интенсивности нарушений и среднего времени восстановления систем. Также рекомендуется не только представлять отчет уполномоченному органу управления организации не реже 1 раза в год, но и направлять его в Департамент рынка ценных бумаг и товарного рынка Банка России в форме электронного документа с усиленной квалифицированной электронной подписью. Таким образом, ЦБ РФ плавно подготавливает некредитные финансовые организации к предоставлению обязательной отчетности по непрерывности деятельности.

По-прежнему актуальным является вопрос управления ЧС или, иными словами, инцидентом. Дело в том, что один

и тот же инцидент часто проходит по трем системам управления: системе управления рисками, в данном случае операционными, Плане ОНиВД и системе информационной безопасности. Эти направления регламентируются в банковской сфере несколькими документами. Для рисков — это Указание ЦБ РФ № 3624-У [5], Письмо ЦБ РФ № 76-Т[4], ОНиВД — Приложение 5 к Положению ЦБ РФ № 242-П [7] и Информационная безопасность — СТО БР ИББС [9]. Похоже, так же будет организована нормативная база и для некредитных финансовых организаций: Указание «О требованиях к организации профессиональным участником рынка ценных бумаг системы управления рисками…», Методические рекомендации ЦБ РФ № 28-М [6] и либо переработанный вариант СТО БР ИББС, либо стандарт ГОСТ Р ИСО/МЭК 27000.

Регулирующих документов много, а инцидент один. Скажем, произошел сбой сервера, но этот случай должен определяться как событие операционного риска, как инцидент непрерывности деятельности и как информационный инцидент. А значит, по-хорошему, надо отработать план управления инцидентом в трех ипостасях, минимизировать его как риск, разработать план управления инцидентом в Плане ОНиВД и выработать порядок обнаружения и реагирования на инцидент информационной безопасности. Понятно, что каждая из этих систем ведущих банков РФ обслуживается отдельной сложной дорогой программой и многочисленными профильными отделами. По какой-то сервисной шине, скорее всего, происходит синхронизация результатов, а может, и не происходит, если сильна конкуренция между отделами. Но для сравнительно небольших кредитных и некредитных финансовых организаций такое «расстроение» — непозволительная роскошь. Поэтому задача — как одним инцидентом «трех генералов накормить» — скоро может стать актуальной и для профессиональных участников финансового рынка.

Логично, что в «Указаниях по хорошей практике Института непрерывности бизнеса [*BCI* 1]» вообще рекомендуется объединять группы управления инцидентами информационной безопасности и инцидентами непрерывности бизнеса.

В ближайшие месяцы ожидается вступление в силу нормативного акта Банка России, в котором будут описаны обязательные требования регулятора по организации системы управления рисками (СУР) отечественных профучастников рынка ценных бумаг. Более чем вероятно, что после принятия этого документа наступит время и обязательного нормативного регулирования управления непрерывностью деятельности. Установившаяся практика доработки нормативных документов большинства национальных центробанков обычно заключается в трансформации ряда рекомендаций на основе выборочного анкетирования регулируемой стороны (в данном случае профучастников рынка ценных бумаг и иных небанковских финансовых учреждений) в новые законодательные требования. После этого будет определен некоторый период приведения системы безопасности непрерывности деятельности в соответствие новым нормативным требованиям. И каким бы он ни был, расслабляться профучастникам не рекомендуется. Сразу после внедрения СУР им придется плотно заняться задачей «непрерывности деятельности» и информационной безопасностью, системами сложными, ресурсозатратными и методологически непростыми. Причем 28-М — это только верхушка айсберга, фактически свод требований к системе. Практическая их реализация является сложной системной задачей, причем имеющей непосредственное отношение к управлению операционным риском, что в свою очередь может привести к необходимости доработки, а то и переработки только что внедренной СУР. ■

СПИСОК ИСТОЧНИКОВ

1. *Herbane B.* (2010) *The evolution of business continuity management*: *A historical review of practices and drivers*. *Business History*.

2. Руководящие принципы обеспечения непрерывности бизнеса (*The Join Forum*, *High-level principles for business continuity*). Базельский комитет по банковскому надзору, Банк международных расчетов. 2006. Август.

3. Рекомендации по наблюдению за непрерывностью деятельности для системно значимых платежных систем (СиПС) Европейский центральный банк. 2006. Июнь.

4. Письмо ЦБ РФ от 24 мая 2005 г. № 76-Т «Об организации управления операционным риском в кредитных организациях».

5. Указание ЦБ РФ от 15 апреля 2015 г. № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы.

6. Методические рекомендации ЦБ РФ от 18 августа 2016 г. № 28-МР «По обеспечению непрерывности деятельности некредитных финансовых организаций»

7. Приложение 5 к Положению Банка России от 16 декабря 2003 года № 242-П «ОБ организации внутреннего контроля в кредитных организациях и банковских группах».

8. *ISO* 22301 *Societal security — Business continuity management systems — Requirements*.

9. СТО БР ИББС СТО БР ИББС-1.0—2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

10. *The Evolution of Business Continuity Management in large Irish enterprises between* 2004 *and* 2009. *David*. *N*. *Garrett BA*.

11. *Баранов А. В.* Международные стандарты управления рисками: не Базелем единым // Рынок ценных бумаг. 2015. Июнь.