# Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 7 (182)/2008

# Этюды об управлении непрерывностью бизнеса

КОРПОРАТИВНЫЙ МЕНЕДЖМЕНТ

# Этюды об управлении непрерывностью бизнеса

СОДЕРЖАНИЕ

**Введение** .....2

**Комментарии ко второй части стандарта «BS 25999: Управление непрерывностью бизнеса. Спецификации»** *(К. Мусатов)*.....3

**Управление непрерывностью бизнеса и управление операционными рисками. Где курица и где яйцо?** *(Б. Альтерман)*.....26

## Введение

Данный номер содержит постатейный комментарий ко второй части британского стандарта «BS 25999: Управление непрерывностью бизнеса. Спецификации». Этот стандарт был выбран не случайно. Документы, регламентирующие управление непрерывностью бизнеса, стали появляться в разных странах с начала 2000-го года. Среди них можно назвать стандарты Сингапура, Австралии, США. Но лишь спустя несколько лет появился документ, вобравший в себя накопленный опыт и описавший процесс управления в терминах, которые приняты в международных стандартах. Высокое качество этого документа было быстро оценено не только в Великобритании, но и в других странах. Большим достоинством BS 25999 является то, что соответствие его требованиям может подтверждаться сертификатом, который выдается независимыми аудиторами.

Комментарий подготовлен на основе опыта ведения компанией «Инфосистемы Джет» проектов по обеспечению непрерывности бизнес- и ИТ-сервисов и их подготовке к сертификации на соответствие требованиям стандарта BS 25999, а также на основе наилучших мировых практик.

Комментарий рассчитан на специалистов, чья деятельность связана с разработкой, внедрением, использованием, тестированием и совершенствованием мер реагирования на чрезвычайные ситуации и восстановления штатного хода деятельности. Кроме того, он будет интересен всем, кто хочет дополнить теоретические знания в области непрерывности практическими рекомендациями.

# Комментарии ко второй части стандарта «BS 25999: Управление непрерывностью бизнеса. Спецификации»

**Константин Мусатов,**
**инженер-проектировщик в группе консалтинга**

## Используемые термины

Используемая во второй части стандарта BS 25999 терминология расширилась по сравнению первой частью и стала больше соответствовать терминологии других стандартов по системам менеджмента (см. табл.1).:

Предшественником стандартов серии 25999 был документ BSI PAS 56:2003. Его терминология претерпела значительные изменения. Большое количество понятий совершенно справедливо не вошло в стандарт, поскольку их смысл был со временем уточнен, а многие были заменены более распространенными терминами.

**Табл. 1**

| Термин | BS 25999-1 | BS 25999-2 | Комментарий |
|---|---|---|---|
| Аудит | отсутствует | Регулярная проверка того, соответствуют ли описанные в документах меры восстановления и реагирования стоящим перед ними целям | Основным способом подтверждения соответствия организации требованиям стандарта является проведение независимого аудита |
| Внутренний аудит | отсутствует | Аудит, проводимый самой организацией или от ее имени, в результате которого могут быть получены основания для заявления организацией о соблюдении ею соответствующих требований | Аудит, проводимый самой организацией или от ее имени, в результате которого могут быть получены основания для заявления организацией о соблюдении ею соответствующих требований |
| Персонал по управлению непрерывностью бизнеса | отсутствует | Сотрудники, чьи обязанности и сфера деятельности связана с системой управления непрерывностью деятельности | Люди являются ключевой частью любого процесса, поэтому полное отсутствие терминов, связанных с участниками процесса управления непрерывностью бизнеса выглядело странно |
| Реагирование в рамках управления непрерывностью бизнеса | отсутствует | Элемент УНБ, связанный с разработкой и реализацией надлежащих планов и мероприятий, направленных на обеспечение непрерывности критически важных видов деятельности, а также управление инцидентами | Расширение понятия «план управления инцидентами», который использовался в первой части стандарта, но не охватывал всех аспектов реагирования. |
| Планирование мероприятий на случай чрезвычайных ситуаций | Разработка и поддержание согласованных процедур по предупреждению, уменьшению масштабов, контролю, смягчению последствий и принятию других мер в случае наступления гражданской чрезвычайной ситуации | отсутствует | Поскольку вторая часть стандарта четко привязана к методологии ПРПД, в ней появились термины соответствующие всем стадиям этой методологии |

**Табл. 1**

| Термин | BS 25999-1 | BS 25999-2 | Комментарий |
|---|---|---|---|
| Несоблюдение требований | отсутствует | Любое отклонение от соответствующих стандартов выполнения работ, методов, процедур, законодательных требований и т.п. | В первой части стандарта не было четкого определения того, в каких случаях происходит активация мер и планов реагирования на ЧС |
| Процесс | отсутствует | Ряд взаимосвязанных или взаимодействующих видов деятельности, с помощью которых ресурсы преобразуются в результаты | Один из неспецифических терминов, необходимый для определения ключевого термина «Управление непрерывностью бизнеса» |
| Ресурсы | отсутствует | Все активы, которыми должна располагать организация для использования по мере необходимости с целью осуществления деятельности и достижения своих целей | В методиках описания процессов ресурсы являются одним из важных компонентов. |
| Готовность к принятию риска | Общая величина риска, который организация готова принять, перенести или действию которого готова подвергнуться в любой момент времени | отсутствует | Этот термин оказалось возможным заменить на более распространенные термины риск менеджмента: риск, оценка риска и управление рисками |
| Система | отсутствует | Набор взаимосвязанных или взаимодействующих элементов | Один из неспецифических терминов, который используется для определения других терминов |
| Система управления | отсутствует | Система, направленная на определение политики и целей, а также на достижение этих целей | Один из неспецифических терминов, который используется для определения других терминов |
| Система управления непрерывностью бизнеса | отсутствует | Часть общей системы управления организации, охватывающая все аспекты управления непрерывностью | Термин введен взамен менее четкого термина «Программа управления непрерывности бизнеса» |

## Применяемые сокращения

| Аббревиатура | Расшифровка | Пояснение |
|---|---|---|
| Цикл ПРПД | Цикл Планирование-Реализация-Проверка-Действие | Широко распространенный метод непрерывного улучшения качества. Другие названия - цикл Деминга, колесо Деминга или спираль непрерывного улучшения. Он был разработан в 1920-х гг. выдающимся экспертом по статистике Shewhart Mr. Walter, который ввел концепцию Plan, Do and See (Планируй, Делай и Смотри). Деминг модифицировал цикл Shewart на: PLAN, DO, STUDY (CHECK) and ACT (ПЛАНИРУЙ, ДЕЛАЙ, ИЗУЧАЙ и ДЕЙСТВУЙ). |
| УНБ | Управление Непрерывностью Бизнеса | Целостный процесс управления, в рамках которого выявляются угрозы, оцениваются возможные последствия их реализации и внедряются превентивные и восстановительные меры |
| СУНБ | Система Управления Непрерывностью Бизнеса | Часть общей системы управления организацией, связанная с разработкой, внедрением, использованием и совершенствованием непрерывности бизнеса |

## Содержание стандарта BS 25999-2

Содержательная часть стандарта разбита на четыре раздела, которые соответствуют циклу Деминга: Планирование-Реализация-Проверка-Действие (Plan-Do-Check-Act). Он служит основой для многих других стандартов по системам управления, таких как BS EN ISO 9001:2000 (Системы управления качеством), BS EN ISO 14001:2004 (Системы управления окружающей средой), BS ISO/IEC 27001:2005 (Системы управления информационной безопасностью) и BS ISO/IEC 20000:2005 (Управление ИТ сервисами). Благодаря использованию единой методической базы внедрение становится последовательным и комплексным, а применение управления непрерывностью бизнеса хорошо сочетается с родственными системами управления. В данном конкретном случае этапы цикла ПРПД соответствуют следующим разделам стандарта:

- этап Plan соответствует разделу Планирование СУНБ;
- этап Do – разделу Внедрение и эксплуатация СУНБ;
- этап Check – разделу Мониторинг и анализ СУНБ;
- этап Act – разделу Сопровождение и совершенствование СУНБ.


**Рис. 1. Интепретация цикла ПРПД в стандарте BS 25999**

В данном номере приведены комментарии к первым двум из четырех частей стандарта.

## Планирование системы управления непрерывностью бизнеса

Раздел 3 содержит описание требований, предъявляемых к различным аспектам процедуры планирования системы управления непрерывностью бизнеса (первого этапа цикла ПРПД).

Раздел 3.1. Общие положения
Раздел 3.2. Создание и управление СУНБ
Раздел 3.2.1. Рамки и цели СУНБ
Раздел 3.2.2. Политика УНБ
Раздел 3.2.3. Обеспечение ресурсами
Раздел 3.2.4. Компетентность персонала, участвующего в УНБ
Раздел 3.3. Внедрение УНБ в культуру организации
Раздел 3.4. Документация и записи по СУНБ
Раздел 3.4.1. Общие положения
Раздел 3.4.2. Управление записями по СУНБ
Раздел 3.4.3. Управление документацией по СУНБ

### Комментарии к разделу 3.1 стандарта BS 25999-2

1. Вводный раздел 3.1 посвящен четырем этапам жизненного цикла системы управления непрерывностью бизнеса. В соответствии с циклом ПРПД этими этапами являются разработка, внедрение, поддержание и совершенствование. Отдельно упоминается требование фиксировать на бумаге положения системы управления непрерывностью бизнеса. Остальные требования, предъявляемые к процессу планирования СУНБ, подробно описаны в разделах 3.2-3.4.

### Комментарии к разделу 3.2 стандарта BS 25999-2

1. Раздел 3.2 содержит описание требований, предъявляемых при создании СУНБ и в процессе последующего управления ею. В преамбуле раздела выделены три цели, которые должны быть достигнуты на первом этапе.
2. При создании СУНБ в качестве первой цели важно четко определить задачи, стоящие перед СУНБ, которые должны быть указаны высшим руководством организации и доведены до всех предполагаемых участников УНБ и других сотрудников, деятельность которых будет влиять или зависеть от процесса УНБ.
3. Второй целью на стадии учреждения и управления СУНБ является вовлечение руководителей организации в процесс обеспечения непрерывности бизнеса. Их участие может выражаться в регулярном отслеживании

процесса внедрения, обеспечении СУНБ необходимыми ресурсами, ознакомлении с регламентами и другими документами, создаваемыми в рамках СУНБ, и выполнении прописанных в них требований. Они также принимают участие в обучении и тренингах, посвященных непрерывности бизнеса.

4. Наконец, в качестве третьей цели указана необходимость удостовериться в том, что ответственные за УНБ сотрудники имеют достаточную квалификацию. Стоит заметить, что не во всякой организации есть достаточное количество специалистов, имеющих богатый опыт в области непрерывности бизнеса уже в самом начале проекта по внедрению СУНБ, что не должно служить причиной для отказа от подобного проекта. Нужный уровень квалификации достигается достаточно быстро благодаря обучению на специализированных курсах, чтению соответствующей литературы и, самое главное, получению практического опыта.

### Комментарии к разделу 3.2.1 стандарта BS 25999-2

1. В разделе рассматриваются требования к тому, какими характеристиками должны обладать границы и цели создания СУНБ, а также вопросы, которым надо уделить особое внимание при их формулировании.
2 В подразделе 3.2.1.1 перечислены пять вопросов, которые должны учитываться при описании границ СУНБ и целей УНБ.
3. Задавая границы СУНБ и цели УНБ, должны быть сформулированы требования, предъявляемые к обеспечению непрерывности. Под ними подразумеваются оценки допустимого времени простоя, размер ущерба, объем потерянных данных, допустимая степень деградации бизнес-процессов и другие количественные параметры.
4. При описании границ СУНБ и целей УНБ должны быть учтены обязательства организации перед клиентами и партнерами, а также ее цели, стремление к достижению которых было объявлено публично и отказ от достижения которых нанесет ущерб репутации организации.
5. Описывая границы СУНБ и цели УНБ, необходимо принимать во внимание риск-аппетит руководства организации. Низкий риск-аппетит означает более низкий уровень приемлемого риска, что подразумевает более жесткие меры по обеспечению непрерывности деятельности. Более подробно риски рассматриваются в разделе стандарта 4.2.1.
6. Если в организации уже существует процесс управления рисками, в рамках которого разработаны регламентирующие документы, например, политика управления рисками, то границы и цели СУНБ необходимо разрабатывать на основе этих документов.
7. При формулировании целей СУНБ обязательно нужно учесть требования существующего законодательства, российских, международных и отраслевых стандартов, а также требования, вытекающие из обязательств перед клиентами и партнерами. Пока в Российской Федерации нет законодательных актов в области непрерывности деятельности, относящихся ко всем хозяйствующим субъектам. Наиболее подробно разработаны нормативные документы, регулирующие деятельность финансовых организаций, относящиеся к непрерывности бизнеса, в числе которых можно упомянуть положение ЦБР от 16 декабря 2003 г. N 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» и отраслевой стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». В других отраслях УНБ упоминается вскользь в документах, посвященных другим темам, например, Приказ Министерства информационных технологий и связи Российской Федерации от 2 июля 2007 г. №73 «Об утверждении правил применения автоматизированных систем расчетов». Помимо нормативных актов в России был принят стандарт СТО БР ИББС-1.0-2006 ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности», часть которого также касается вопросов обеспечения непрерывности деятельности.
8. При описании границ СУНБ и целей УНБ следует учитывать возможные финансовые потери различных заинтересованных сторон (собственники, акционеры, клиенты, партнеры, аварийные службы, страховые компании, кредитные организации, регулирующие органы и т.д.), вызванные перерывом в деятельности организации. Защита их интересов также может входить в число целей СУНБ.
9. В подразделе 3.2.1.2 содержится требование четко обозначить, какие из предоставляемых организацией продуктов и/или услуг являются ключевыми. и, соответственно, обязатель-

но должны быть включены в рамки СУНБ. В их число могут входить продукты или услуги, как предоставляемые клиентам организации, т.е. внешние, так и одним подразделением другому, т.е. внутренние. При выборе ключевых продуктов и услуг важно хорошо понимать их роль для осуществления деятельности компании. В качестве примера можно привести обеспечение бесперебойной работы ИТ-сервиса автоматизированной обработки персональных данных работников. Хотя этот сервис относится к поддерживающим, но юридические, политические и имиджевые риски, в случае его длительной недоступности, могут оказаться неприемлемо высокими.

### Комментарии к разделу 3.2.2 стандарта BS 25999-2

1. В разделе 3.2.2 подробно рассматривается содержание такого важного документа как политика УНБ — условия, которые обязательно должны быть соблюдены при ее создании и дальнейшей с ней работе.
2. Отдельный подраздел 3.2.2.1 посвящен высшему руководству. В контексте политики УНБ его роль заключается в том, чтобы, в первую очередь, оно само знало, соблюдало и способствовало совершенствованию политики УНБ.
3. В подразделе 3.2.2.2 указано, что политика УНБ должна быть связана с целями и границами обеспечения непрерывности деятельности организации. Приводимые в политике характеристики границ могут содержать как описание того, что обязательно должно в них войти, так и явные исключения, т.е. те продукты и услуги, которые не считаются критичными и не входят в СУНБ.
4. В подразделе 3.2.2.3 указаны три условия, которые необходимо соблюдать в рамках жизненного цикла документа «Политика УНБ».
5. Во-первых, в любой момент времени политика должна оставаться согласованной с высшим руководством организации. Политика — это документ высокого уровня, который используется руководителями при принятии решений, поэтому он должен пользоваться их одобрением.
6. Во-вторых, политику УНБ должны учитывать в своей работе все сотрудники организации, а также лица, работающие от ее имени. По этой причине в стандарте четко прописано требование ознакомить с политикой всех постоянных и временных сотрудников.
7. В-третьих, по мере развития организации ее цели в области УНБ также будут меняться. В связи с этим в стандарт включено требование обязательного обновления политики. Оно может происходить как регулярно (зачастую, один раз в год), так и внепланово, в случае значительных изменений в деятельности организации, например, слияния или поглощения другой организации.

### Комментарии к разделу 3.2.3 стандарта BS 25999-2

1. В разделе 3.2.3 рассматриваются вопросы, которые относятся к обеспечению процесса внедрения и поддержания СУНБ различными ресурсами.
2. Подраздел 3.2.3.1 содержит единственное требование о предоставлении руководством ресурсов, необходимых на всех этапах разработки СУНБ — проектирования, внедрения, использования и совершенствования.
3. В подразделе 3.2.3.2 речь идет об организации распределения ресурсов. С этой целью необходимо зафиксировать на бумаге роли, соответствующие им зоны ответственности, требуемые уровень квалификации и полномочия всех участников процесса УНБ. Распределение ресурсов, предоставляемых сотруднику, будет логично поставить в зависимость от степени его вовлеченности/ответственности в рамках СУНБ.
4. Отдельный подраздел 3.2.3.3 посвящен использованию такого важного ресурса как участие высшего руководства. Он должен использоваться для решения двух задач.
5. Для назначения сотрудника, который будет нести ответственность за выполнение политики и внедрение СУНБ в организации. Он должен обладать соответствующим статусом и полномочиями. В российских компаниях его положение в организационной структуре часто бывает не слишком высоким, что ставит под угрозу успешность всего начинания. Стоит взглянуть на пример западных компаний, где Директор по непрерывности бизнеса подчиняется напрямую исполнительному директору. Такой высокий статус легко объясним. Данный сотрудник должен иметь возможность изменять устоявшуюся структуру бизнес-процессов и влиять на деятельность самых различных бизнес-подразделений.
6. Для назначения одного или нескольких сотрудников, в обязанности которых войдет внедрение и поддержание СУНБ. В органи-

зациях, чей штат насчитывает несколько сот человек, для внедрения и поддержания в актуальном состоянии СУНБ потребуются усилия нескольких человек. Причем решение этой задачи по мере внедрения СУНБ будет отнимать все большую часть рабочего времени, что приведет к необходимости создания отдельного структурного подразделения, занимающегося только СУНБ.

### Комментарии к разделу 3.2.4 стандарта BS 25999-2

1. Раздел 3.2.4 посвящен вопросам обеспечения компетентности сотрудников, участвующих в процессе УНБ, как одного из важнейших ресурсов для успешного внедрения СУНБ. Прежде всего, в стандарте провозглашено, что ответственность за уровень компетентности сотрудников лежит на руководстве. Для решения этой задачи предлагается выполнять следующие пять шагов.
2. Шаг первый — определить сферу ответственности каждого из участвующих в процессе УНБ сотрудников и его уровень компетентности, который требуется для выполнения возложенных обязанностей.
3. Шаг второй — в случае несоответствия уровня компетентности сотрудника возложенным на него обязанностям констатировать необходимость его обучения и описать области, в которых требуется получение дополнительных знаний. Обучение может носить как теоретический, так и практический характер.
4. Шаг третий — обучить сотрудника. Эта задача может быть решена как силами самой организации, так и третьей стороной, например, учебным центром или внешним консультантом.
5. Шаг четвертый — удостовериться в том, что сотрудник приобрел необходимый уровень компетентности. Если сотрудник проходил обучение в независимом учебном центре, то, как правило, его минимальный уровень квалификации уже подтвержден сертификатом о сдаче выпускного экзамена или хотя бы о прохождении курса. Но более эффективным способом проверки, несомненно, служит проведение тренингов с участием обученного сотрудника и последующей оценкой действий стажера.
6. Шаг пятый — зафиксировать факт получения необходимой квалификации, а также результаты проведенных учений. Эти записи играют важную роль особенно в том случае, если организация будет проходить внешний аудит на соответствие требованиям стандарта BS 25999.

### Комментарии к разделу 3.3 стандарта BS 25999-2

1. Раздел 3.3 посвящен условию успешности СУНБ в организации — вовлечению всех сотрудников организации в процесс УНБ. Оно является очень важным для организаций любого размера, с любой структурой и в любой сфере деятельности. Для обеспечения непрерывности деятельности соответствующие процедуры должны быть включены в штатные должностные инструкции и регламенты.
2. В стандарте предлагается пять путей, способствующих внедрению задачи обеспечения непрерывности деятельности в корпоративную культуру.
3. Во-первых, вовлеченность сотрудников предлагается достигать за счет обучения. Для новых сотрудников вопросы обеспечения непрерывности их деятельности должны входить в стандартную процедуру адаптации. В дополнение к процессу обучения должна быть организована регулярная процедура, оценивающая навыки обеспечения непрерывности деятельности. Если в организации уже существует регулярная аттестация сотрудников, она должна быть соответствующим образом дополнена.
4. Во-вторых, все сотрудники должны быть осведомлены о целях организации в области УНБ. Им следует регулярно напоминать о важности их достижения. Очень важным будет личный пример руководства компании.
5. В-третьих, все сотрудники должны ознакомиться с политикой непрерывности бизнеса организации и осознавать важность ее соблюдения. Здесь также хочется подчеркнуть большое значение личного примера руководства. Любые требования соблюдения политики будут малоэффективными, если поступки и решения руководства им противоречат.
6. В-четвертых, до всех сотрудников необходимо донести мысль о том, что процесс УНБ не является окончательным и неизменным, что он должен и будет непрерывно улучшаться и совершенствоваться в соответствии с новыми условиями как внутри организации, так и за ее пределами. Тем самым руководство даст понять, что данное начинание — это не мимолетная прихоть и не дань

моде, а стратегическое решение, призванное обеспечить долгосрочный устойчивый рост компании, что, в конечном итоге, выгодно самим сотрудникам.

7. В-пятых, все сотрудники должны совершенствовать процесс УНБ. Важность этого требования трудно переоценить, поскольку непрерывность бизнеса в целом зависит от своевременных и эффективных действий каждого сотрудника на своем рабочем месте. Заставить кого-либо проявить инициативу невозможно, поэтому для выполнения данного требования следует использовать скорее разного рода поощрения, чем принуждение.

### Комментарии к разделу 3.4 стандарта BS 25999-2

1. В менеджменте часто встречается фраза «вы не можете управлять тем, что не можете измерить», а единственным способом управлять процессом является наличие документов и ведение записей. Описанию документов, которые должны входить в СУНБ, а также требованиям к средствам контроля и посвящен раздел 3.4.

### Комментарии к разделу 3.4.1 стандарта BS 25999-2

1. Раздел 3.4.1 содержит три подраздела, каждый из которых посвящен одному из элементов контроля эффективности и актуальности СУНБ. К ним относятся документы, записи и процедуры контроля.
2. Стандарт не содержит списка документов, наличие которых обязательно для процесса управления непрерывностью бизнеса. Однако в подразделе 3.4.1.1 приведен перечень из 15 пунктов, которые в той или иной степени должны быть отражены в документации. Многие из них подробно описываются в других разделах стандарта.
3. В документах СУНБ должны быть четко описаны ее границы и цели. Описанию требований, которым они должны удовлетворять, посвящен раздел стандарта 3.2.1. Обычно этот пункт бывает представлен не в виде отдельного документа, а как подраздел другого, более общего, например, политики УНБ.
4. Должна быть сформулирована и зафиксирована на бумаге политика управления непрерывностью бизнеса. Предъявляемые к ней требования подробно изложены в разделе стандарта 3.2.2.
5. В документах СУНБ должен быть рассмотрен вопрос выделения необходимых ресурсов. Этой теме посвящен раздел стандарта 3.2.3. Обычно этот вопрос описывается не в виде отдельного документа, а как подраздел другого, более общего, например, политики УНБ.
6. В документах должны быть отражены результаты оценки компетентности участвующих в УНБ сотрудников, записи о мерах, предпринимаемых для ее повышения, и результаты учений. Данные записи могут вестись департаментами, ответственными за повышение квалификации, отделом кадров или специалистом, отвечающим за СУНБ. Подробнее эта тема разбирается в разделе стандарта 3.2.4.
7. Желание обеспечить непрерывность деятельности организации должно иметь серьезное финансовое обоснование. Таким обоснованием служат результаты анализа влияния на бизнес, естественно, изложенные на бумаге. Исходная информация и сделанные выводы можно представить как в виде отдельного документа, так и в виде подраздела другого документа, например, стратегии непрерывности бизнеса. Требования, предъявляемые к содержанию анализа влияния на бизнес, подробно изложены в разделе стандарта 4.1.1.
8. Помимо оценки возможного ущерба необходимо определить, что угрожает организации и каковы ее наиболее уязвимые места. Анализ угроз и уязвимостей также можно представить как в виде отдельного документа, так и в виде подраздела другого документа, например, стратегии непрерывности бизнеса. Требования, предъявляемые к содержанию анализа влияния на бизнес, подробно изложены в разделе стандарта 4.1.2.
9. На основе анализа влияния на бизнес и анализа рисков должна быть разработана и зафиксирована на бумаге стратегия непрерывности бизнеса. Предъявляемые к ней требования изложены в разделе стандарта 4.2. Обычно стратегия излагается в виде отдельного документа.
10. В организации должен быть сформулирован порядок действий в случае наступления инцидента. Он может иметь вид самостоятельного документа или быть включен в планы управления инцидентами. Предъявляемые к нему требования изложены в разделе стандарта 4.3.2.
11. В организации должны быть написаны инструкции для сотрудников, описывающие действия в чрезвычайных ситуациях. К таким инструкциям относятся планы непре-

рывности бизнеса и планы управления инцидентами, требования к которым изложены в разделе стандарта 4.3.3. Обычно разрабатывается большое количество подобных планов, предназначенных для разных подразделений, руководителей разного ранга и различных типов ЧС.

12. Процесс управления непрерывностью бизнеса должен регулярно тестироваться. Для обеспечения этого в организации должен существовать документ, описывающий стратегию или программу тестирования. Кроме того, необходимо протоколировать ход и результаты учений, которые также следует проводить на регулярной основе. Требования, предъявляемые к процессу тестирования существующих мер УНБ, описаны в разделе стандарта 4.4.2.
13. Помимо тестирования реализованных мер обеспечения непрерывности деятельности в организации должны быть предусмотрены и описаны процедуры, которые позволяют отслеживать актуальность существующих мер УНБ, а также извлекать уроки из произошедших инцидентов. Описание этих процедур может быть представлено как в виде отдельного документа, так и быть включено в виде подраздела другого документа, например, стратегии актуализации СУНБ. Требования, предъявляемые к подобным процедурам, описаны в разделе стандарта 4.4.3.
14. В организации должна быть описана процедура проведения внутреннего аудита. Проводить ее могут как представители подразделения внутреннего аудита, так и других подразделений. По результатам проведения аудита должны быть составлены отчеты. Более подробно требования к процедуре проведения внутренних аудитов СУНБ рассмотрены в разделе стандарта 5.1.
15. Помимо внутреннего аудита система управления непрерывностью бизнеса должна регулярно пересматриваться высшим руководством организации. В ходе этой проверки руководство вносит изменения в границы и цели СУНБ, корректирует политику и другие высокоуровневые документы. Результаты этой проверки-пересмотра фиксируются для последующего внесения корректив в документы. Требования, предъявляемые к процедуре проведения управленческого пересмотра[1], подробнее описываются в разделе стандарта 5.2.
16. В организации должны быть описаны процедуры выполнения превентивных действий, предотвращающих прерывание бизнеса и корректирующих действий, которые служат для того, чтобы не допустить аналогичной чрезвычайной ситуации в будущем. Данные описания обычно хранятся в виде отдельных документов. Требования, предъявляемые к процедурам превентивных и корректирующих действий, подробнее описаны в разделе стандарта 6.1.
17. Непрерывное совершенствование СУНБ, очевидно, является жизненно необходимым условием для того, чтобы система работала успешно и решала поставленные перед ней задачи. Поэтому в организации должен существовать документ или раздел документа, подтверждающий приверженность руководства идее непрерывного повышения эффективности СУНБ вместе с описанием способов, которые могут быть для этого использованы. Подробнее требования к процедуре непрерывного совершенствования изложены в разделе стандарта 6.2.
18. Подраздел 3.4.1.2 содержит требование к тому, чтобы в организации велись записи[2]. И все этапы своего жизненного цикла — с момента создания и до переноса в архив записи — должны свидетельствовать об эффективности функционирования СУНБ.
19. Подраздел 3.4.1.3 содержит требование к наличию в организации процедур контроля документации и записей, причем сами эти процедуры должны быть описаны на бумаге. Они предназначены для того, чтобы определить показатели или инструменты контроля. Например, такой процедурой может служить регулярный мониторинг эффективности существующей документации. Документ можно считать эффективным, если описанная в нем последовательность действий в ходе проверки позволила восстановить прерванный процесс. Контролируемым показате-

1 Управленческий пересмотр (management review) — регулярно проводимый руководителями компании анализ системы управления непрерывностью бизнеса.

2 Запись (record) — специальный вид документа, содержащий достигнутые результаты или свидетельства осуществленной деятельности. Записи могут использоваться, например, для документирования прослеживаемости, т.е. возможности проследить историю, применение или местонахождение того, что рассматривается, свидетельства проведения верификации, предупреждающих и корректирующих действий. Примерами записей могут быть записи в трудовой книжке о пройденном обучении, записи в журнале инцидентов или журнале регистрации инструктажа по технике безопасности. В отличие от документов зарегистрированные записи не могут быть изменены.

лем в таком случае может служить количество или процент документов, соответствующих зафиксированным требованиям, скажем, в этот раз 80% документов оказались эффективными, т.е. позволили восстановить процессы в установленное время, что на 10% больше, чем в прошлый раз.

### Комментарии к разделу 3.4.2 стандарта BS 25999-2

1. Помимо ведения записей в рамках СУНБ в стандарте подчеркивается роль контроля этих действий. Раздел 3.4.2 содержит два обоснования необходимости контроля записей СУНБ.
2. В процессе контроля можно удостовериться, удастся ли найти нужные записи, прочитать и восстановить в случае утраты.
3. Осуществление контроля способствует использованию идентификации записей, формализует процедуру их хранения, создания резервных копий и восстановления.

### Комментарии к разделу 3.4.3 стандарта BS 25999-2

1. Аналогично контролю записей в стандарте подчеркивается высокая роль контроля документации СУНБ. Хотя ее создание и занимает длительное время, его можно считать однократным действием, результатом которого будут статичные документы. Они быстро утрачивают свою актуальность и, следовательно, полезность с течением времени. Только благодаря процедуре контроля и обновления организация сможет поддерживать актуальность документов на должном уровне. В разделе 3.4.3 приведены шесть причин, по которым в организации должна существовать процедура контроля документации СУНБ.
2. Процедура контроля позволит удостовериться в актуальности документа до того, как он будет распространен среди сотрудников, которые самостоятельно не могут удостовериться в корректности содержащейся в нем информации.
3. Благодаря процедуре контроля документы будут пересматриваться, в них будут вноситься необходимые изменения, после чего они будут проходить процесс утверждения.
4. В рамках формальной процедуры контроля легче отслеживать внесенные в документы изменения и следить за тем, на каком этапе пересмотра находится каждый. Учитывая, что количество документов в рамках СУНБ быстро превысит несколько десятков, дополнительно к формальной процедуре контроля полезно воспользоваться специализированным программным обеспечением, облегчающим контроль версий и внесение изменений.
5. Процедура контроля дает возможность отслеживать, чтобы не только старые версии документов своевременно заменялись новыми, но и новые версии находились именно в тех местах и у тех сотрудников, которым предстоит эти документы использовать.
6. Процедура контроля помогает идентифицировать документы, которые создаются вне пределов организации и отслеживать их распространение. К ним можно отнести инструкции компетентных органов, ведомственную информацию для служебного пользования и т.п.
7. Формальная процедура контроля исключает возможность использования старых версий документов. Поддержание корректной нумерации версий является важной, но часто игнорируемой задачей в рамках СУНБ. Следование устаревшему документу в условиях чрезвычайной ситуации может иметь весьма тяжелые последствия, вплоть до невозможности возобновления деятельности за заданный промежуток времени.

## Внедрение и эксплуатация СУНБ

Раздел 4 содержит описание требований, предъявляемых к различным аспектам процедуры реализации и использования системы управления непрерывностью бизнеса (второго этапа DO цикла ПРПД). Однако сам этап реализации можно в свою очередь представить как цикл ПРПД, где:

- этап Plan соответствует разделу Понимание организации;
- этап Do — разделу Определение стратегии непрерывности бизнеса;
- этап Check — разделу Разработка и реализация реагирования в рамках УНБ;
- этап Act — разделу Тренировка, поддержка и пересмотр мер УНБ.

Раздел 4.1. Анализ организации
Раздел 4.1.1. Анализ воздействия на бизнес
Раздел 4.1.2. Оценка рисков
Раздел 4.1.3. Определение возможных вариантов

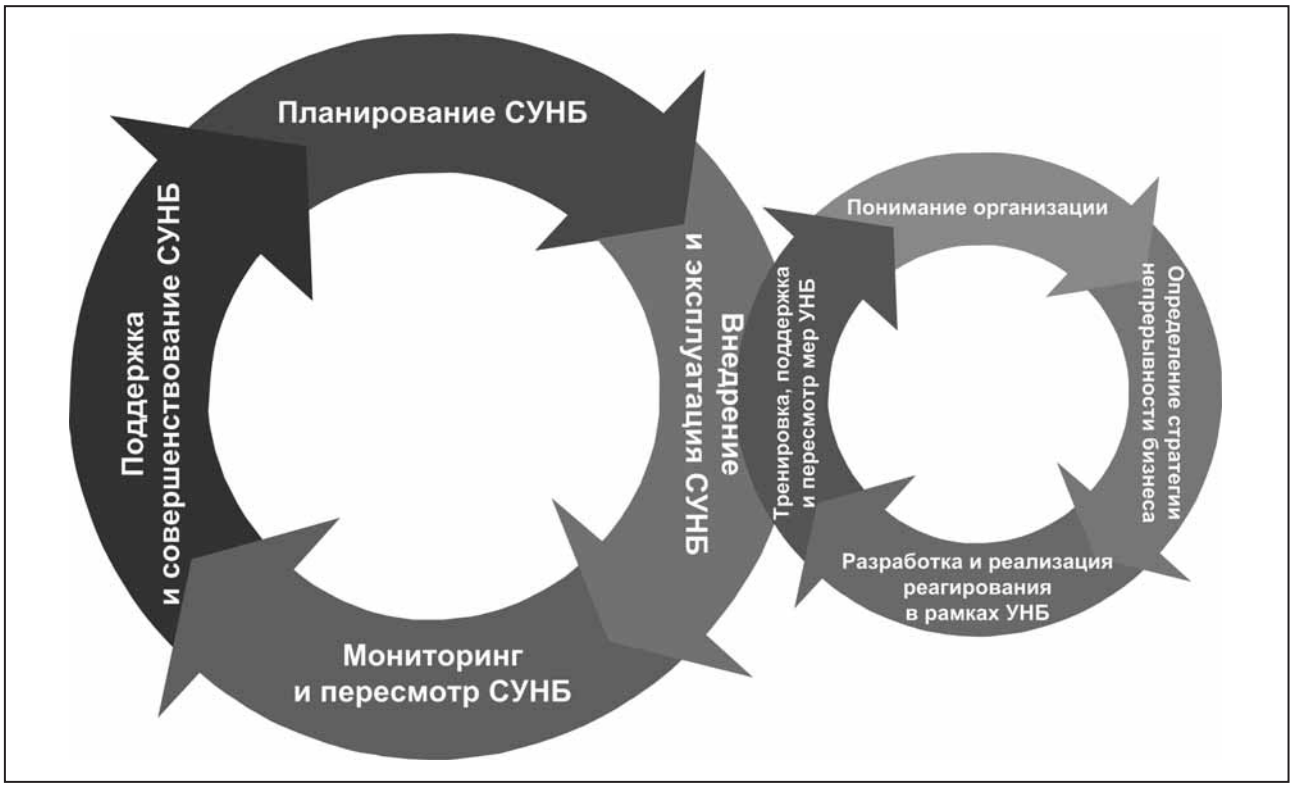


**Рис. 2. Цикл ПРПД для этапа «Внедрение и эксплуатация СУНБ»**

Раздел 4.2. Определение стратегии обеспечения непрерывности бизнеса
Раздел 4.3. Разработка и осуществление мер реагирования в рамках УНБ
Раздел 4.3.1. Общие положения
Раздел 4.3.2. Структура реагирования на инциденты
Раздел 4.3.3. Планы обеспечения непрерывности бизнеса и планы управления инцидентами
Раздел 4.4. Отработка, сопровождение и анализ мер по УНБ
Раздел 4.4.1. Общие положения
Раздел 4.4.2. Учения по УНБ
Раздел 4.4.3. Сопровождение и анализ мер по УНБ

## Комментарии к разделу 4.1 стандарта BS 25999-2

1. Целью этапа «Понимание организации» является сбор и обработка необходимой информации, что позволит принимать обоснованные решения на последующих этапах внедрения СУНБ. Соответственно, в разделе 4.1 собраны требования, которые должны быть выполнены при проведении анализа влияния на бизнес ЧС, анализа рисков и выборе адекватных мер снижения рисков.

## Комментарии к разделу 4.1.1 стандарта BS 25999-2

1. В разделе 4.1.1 собраны требования, которые предъявляются к применяемому методу и содержанию работ по анализу влияния на деятельность организации.
2. Среди перечисленных в подразделе 4.1.1.1 требований к методу определения влияния на бизнес главным можно считать его документированность. Только наличие зафиксированного метода обеспечит его объективность и исключит зависимость от исполнителей. Кроме того, он должен быть конкретным и адекватным масштабу задач. Наконец, в данном подразделе подчеркивается, что данный метод следует применять к оценке влияния прерывания лишь тех активностей, входящих в рамки СУНБ, которые описаны в разделе 3.2.1.
3. В подразделе 4.1.1.2 перечислены десять требований, предъявляемых к последовательности и содержанию работ по анализу влияния на бизнес.
4. Для того, чтобы полученные результаты были полезны на дальнейших этапах, от организации требуется, прежде всего, идентифицировать процессы и активности, которые поддерживают выпуск ключевых продуктов и

предоставление ключевых услуг. В стандарте нет требований к количеству процессов, которые должны быть охвачены СУНБ. Здравый смысл и лучшие мировые практики рекомендуют начинать внедрение процесса обеспечения непрерывности деятельности в организации с одного ключевого процесса, охватывая другие процессы по мере накопления практического опыта.

5. Организация должна определить, какое влияние может оказать на деятельность компании прерывание критичных процессов и активностей. Влияние должно быть оценено количественно. Если подсчитать абсолютную величину ущерба невозможно, можно использовать приблизительные величины относительно единой шкалы, принятой в компании для оценки приемлемого ущерба. Также необходимо описать изменение величины и характера ущерба со временем.
6. Для каждого критичного процесса необходимо указать максимальную продолжительность времени с момента его прерывания и до момента возобновления в чрезвычайной ситуации, возможно, не в полном объеме. Грубую оценку этого промежутка можно получить, например, разделив сумму максимально допустимого ущерба с точки зрения руководства на величину ущерба в час в результате прерывания данного процесса.
7. Для каждого критичного процесса необходимо указать минимальный уровень, на котором он должен функционировать до восстановления штатного режима работы. Определение минимального уровня производительности позволяет оценить минимальный уровень материальных и людских ресурсов, необходимых для работы в чрезвычайной ситуации.
8. Для каждого критичного процесса должна быть указана продолжительность времени восстановления штатного режима работы. На основе этого параметра можно будет оценить загрузку ресурсов, используемых для функционирования на минимальном уровне. В случае, если процесс восстановления займет достаточно длительное время, предусмотреть их своевременную замену.
9. В случае большого количества активностей, подлежащих восстановлению, необходимо разбить их на категории. Подобное разбиение на категории может осуществляться относительно разных критериев. Наиболее очевидными являются категории, соответствующие важности активностей в штатном режиме. Например, к первой категории относятся активности, критичные для самого существования организации, ко второй — критичные для производства одного из ключевых продуктов, к третьей — все остальные. Другой способ разбиения соответствует очередности, в которой активности должны восстанавливаться, причем эта очередность не всегда совпадает с критичностью в штатном режиме. Третий способ — может соответствовать минимальным уровням функционирования, которые были определены в четвертом пункте. Здесь имеется в виду, что сначала все активности восстанавливаются до минимального уровня, затем активности из второй категории восстанавливаются до более высокого уровня, наконец, активности из третьей категории восстанавливаются в полном объеме.
10. Должны быть выявлены все зависимости активностей и производственных процессов от третьих фирм, таких как: поставщики оборудования, сырья, услуг аутсорсинга (например, колл-центр, поддержка ИТ-систем, курьерская доставка), сервисов Интернета, телефонной связи, электричества и др.
11. Необходимо собрать информацию о том, какие шаги по обеспечению непрерывности предоставления услуг предприняты самими поставщиками и аутсорсинговыми партнерами. На основе собранной информации организации необходимо принять дополнительные меры обеспечения непрерывности. Осуществлять шаги можно в двух направлениях. Первый путь состоит в том, чтобы вынудить партнеров предпринимать меры по обеспечению непрерывности собственной деятельности, например, путем включения соответствующих пунктов в контракты. Второй путь — это устранение единых точек отказа путем заключения договоров с альтернативными поставщиками, например, вторым интернет-провайдером, вторым оператором связи и т.п.
12. Для каждого критичного процесса и активности требуется определить целевые времена восстановления. Эта величина задает промежуток времени, за который функционирование процесса или активности должно быть полностью восстановлено. Продолжительность этого промежутка меньше или равна параметру, определенному на четвертом шаге. Взаимосвязь различных терминов, описывающих сроки восстановления и

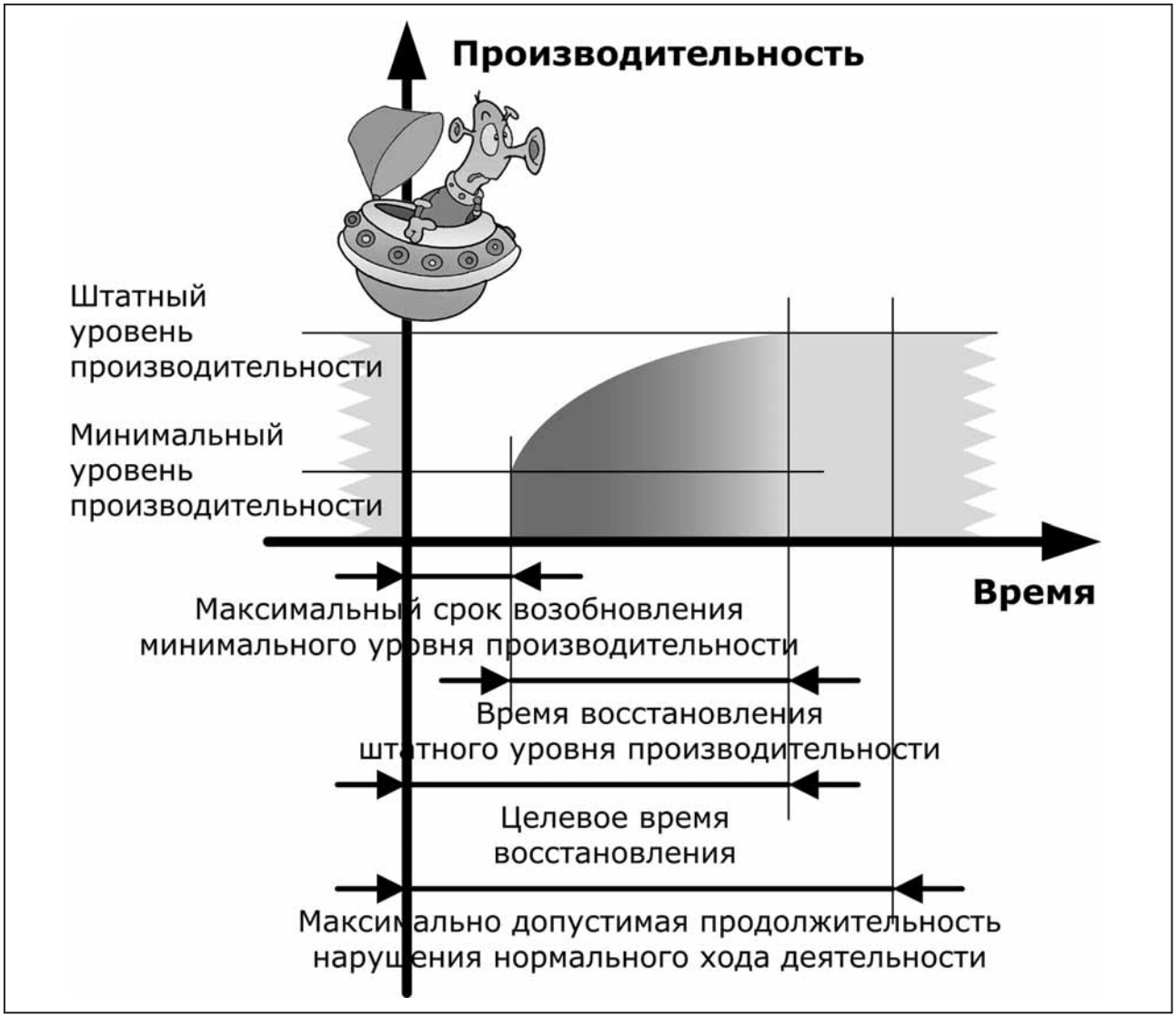


**Рис. 3. Взаимосвязь терминов, описывающих восстановление деятельности.**

уровни производительности, показана на рисунке 3.

13. Необходимо дать оценку ресурсов, которые потребуются для восстановления критичных процессов и активностей. Следует иметь в виду, что в чрезвычайной ситуации повышается вероятность возникновения ресурсных конфликтов. При оценке необходимо обращать внимание на то, чтобы один и тот же ресурс не использовался одновременно на двух участках работ. Например, один и тот же сотрудник не может одновременно заниматься восстановлением и участвовать в функционировании процесса на минимальном уровне.

### Комментарии к разделу 4.1.2 стандарта BS 25999-2

1. В разделе 4.1.2 собраны требования, которые предъявляются к применяемым методу и результату работ по оценке рисков деятельности организации.
2. В подразделе 4.1.2.1 содержатся требования к методу проведения оценки рисков. Как и в случае с методом анализа воздействия на бизнес, одним из важнейших является требование наличия документированной процедуры оценки рисков. Эта процедура также должна быть конкретной и однозначной. В стандарте обращается внимание на то, что при оценке рисков следует учитывать угрозы и уязвимости не только процессов и ресурсов, создаваемых и поставляемых внутри организации, но и тех, которые поступают в организацию извне от поставщиков и аутсорсинговых партнеров. Если в организации уже ведется работа по управлению рисками, следует воспользоваться имеющимися результатами. На практике управление риска-

ми и управление непрерывностью бизнеса могут оказаться в зонах ответственности различных подразделений, что грозит привести к дублированию работ и конфликтам. Проблема разделения зон ответственности между этими управленческими процессами решается в каждой организации по-своему. Одна из точек зрения на то, как соотносятся друг с другом управление рисками и управление непрерывностью бизнеса изложена в статье «Управление непрерывностью бизнеса и управление операционными рисками. Где курица и где яйцо?» в этом же номере «Jet Info».

3. В подразделе 4.1.2.2 сказано, что должна получить организация в качестве результата оценки рисков — понимание последствий реализации угроз. Хочется отметить, что в стандарте говорится о качественном понимании последствий наступления инцидента, а не о численных оценках вероятности угроз. Поскольку в УНБ рассматриваются, в том числе, такие редкие события как землетрясение, пожар или террористический акт, невозможно дать правдоподобные оценки вероятности их реализации, которые могут быть использованы на практике.

## Комментарии к разделу 4.1.3 стандарта BS 25999-2

1. Раздел 4.1.3 посвящен требованиям к мерам управления рисками, применяемым в организации, и к параметрам, на основании которых происходит их выбор.
2. В подразделе 4.1.3.1 речь идет о трех направлениях, в которых применяемые в организации защитные меры могут управлять рисками.
3. Средства управления рисками могут уменьшать вероятность того, что ход критичного процесса или активности может быть прерван. Примером такого средства может быть замена старого оборудования на более новое, которое реже выходит из строя.
4. Средства управления рисками могут уменьшить продолжительность прерывания нормального хода деятельности. Например, наличие на складе организации запасного оборудования и комплектующих, в случае выхода этого оборудования из строя, позволит сократить срок восстановления нормального хода деятельности.
5. Средства управления рисками могут способствовать уменьшению влияния, которое оказывает прерывание процесса или активности на предоставление критичных продуктов или сервисов. В качестве такого средства можно предусмотреть альтернативные способы производства продуктов или предоставления сервисов, например, доставка информации на бумажных, а не на электронных носителях или ручной ввод информации вместо автоматизированного.
6. Выбор того, какой именно способ или их комбинация будет использован для управления рисками каждого критичного процесса или активности, организация делает самостоятельно на основе параметров, которые

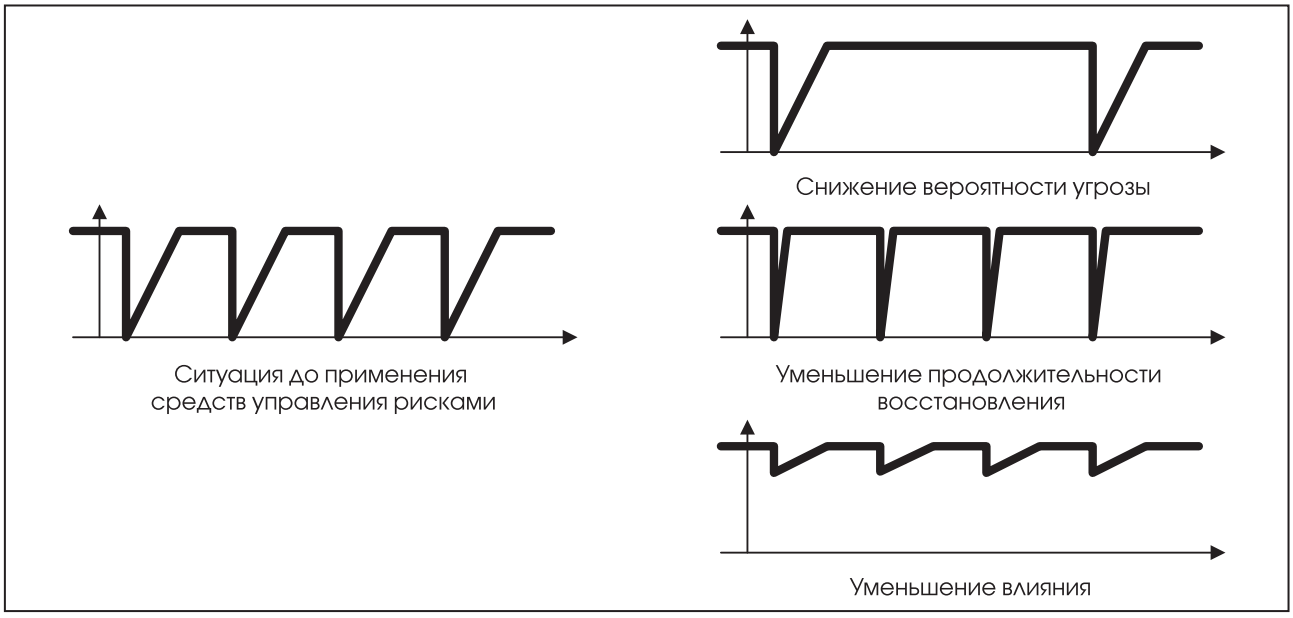


**Рис. 4. Три направления управления рисками**

были определены в разделе 4.1.1, посвященному анализу воздействия на бизнес.

7. В подразделе 4.1.3.2 подчеркивается, что главным критерием для выбора соответствующих средств управления рисками служит уровень приемлемого риска каждого процесса или активности, который был определен при описании границ и целей СУНБ в соответствии с требованиями раздела 3.2.1. Уровень приемлемого риска является субъективным понятием, поэтому не может быть вычислен. Кроме того, в тексте подраздела подчеркивается, что для реализации СУНБ соответствующие средства управления рисками надо не только выбрать, но и внедрить.

### Комментарии к разделу 4.2 стандарта BS 25999-2

1. Раздел 4.2 посвящен этапу выбора того, как организация будет реагировать на чрезвычайную ситуацию. Эта реакция может быть самой различной: от самой распространенной реакции — «ничего не делать», до переноса всех процессов в дублирующие подразделения организации без остановки деятельности и деградации производительности. Какой бы она ни была, она должна соответствовать трем требованиям.
2. Для того, чтобы действия по управлению непрерывностью деятельности были максимально эффективными, в организации должна быть заблаговременно зафиксирована структура реагирования на инциденты, т.е. любые ситуации, приводящие или способные вызвать нарушение нормального хода деятельности. Такая структура должна предоставлять данные о том, в чью зону ответственности попадает каждый инцидент, контактную информацию и порядок эскалации. Детальная информация о самих шагах по восстановлению содержится в документах более низкого уровня, таких как: планы непрерывности бизнеса и реагирования на инциденты.
3. Должны быть описаны меры УНБ для восстановления каждого критичного производственного процесса. При выборе этих мер необходимо помнить о том, чтобы восстановление заняло не больше целевого времени восстановления процесса, определенного в разделе 4.1.1. Кроме того, необходимо предусмотреть доступность необходимых ресурсов, в том числе тех, которые предоставляются внешними поставщиками. На практике стратегия не содержит исчерпывающей информации о восстановлении, в противном случае из-за своего объема она может превратиться в документ, которым невозможно пользоваться. Такая информация есть в документах более низкого уровня, таких как: планы непрерывности бизнеса и реагирования на инциденты. Описание мер УНБ, приводимое в стратегии, обычно лишь задает рамки, например, класс технологических решений или минимальный уровень функционирования.
4. Организации необходимо продумать вопрос взаимодействия с внешним миром. Этот вопрос в чрезвычайной ситуации может оказаться более сложным, чем кажется на первый взгляд. С одной стороны, все контакты должно вести одно лицо, что позволяет контролировать содержание всей исходящей информации. С другой стороны, в случае угрозы жизни или здоровью большого количества сотрудников, невозможность оперативно связаться с близкими может парализовать и без того нарушенную деятельность организации. Это в свою очередь поднимает вопрос о наличии надежных каналов связи с высокой пропускной способностью. В некоторых ситуациях информацию о перерыве деятельности целесообразно стараться сохранить в тайне. Однако возможны и противоположные ситуации, в которых доведение информации о чрезвычайной ситуации до клиентов лишь улучшит репутацию пострадавшей организации. Многообразие вариантов взаимодействия так велико, что дать какие-либо универсальные рекомендации не представляется возможным. Можно также отметить, что в стандарте даже не содержатся требования о том, чтобы процедура взаимодействия с заинтересованными сторонами была описана в виде документа.
5. Стоит отметить, что стратегия реагирования и восстановления не должна превращаться в формальную бюрократическую процедуру. Суть стратегии состоит в том, чтобы направить действия руководителей и рядовых сотрудников в нужное русло, но при этом не мешать им проявлять инициативу и эффективно реагировать на изменения в окружающей обстановке.

### Комментарии к разделу 4.3 стандарта BS 25999-2

1. Раздел 4.3 содержит требования к тому, какую информацию следует использовать при разработке регламентов и мер реагиро-

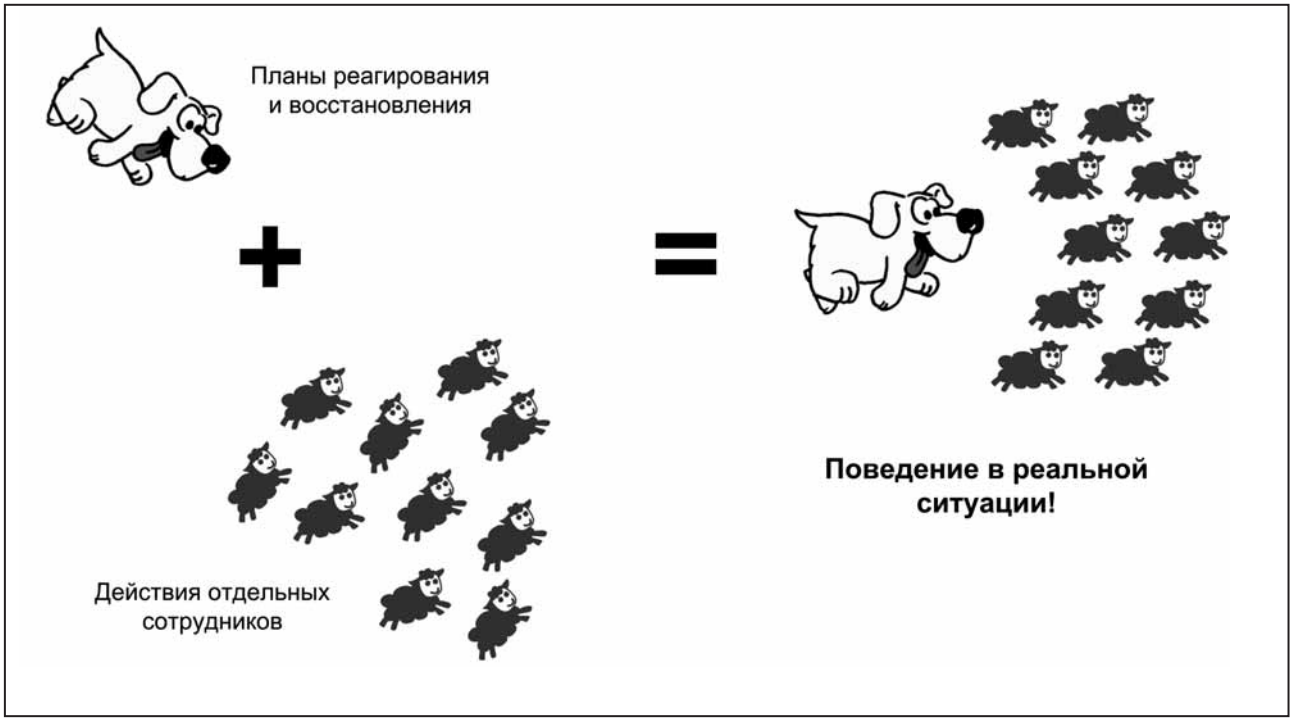


**Рис. 5. Планы реагирования и восстановления должны задавать общее направление действиям сотрудников в кризисной ситуации, не мешая им проявлять инициативу и предпринимать действия, требующиеся в конкретной ситуации.**

вания в рамках УНБ, причины, по которым организации следует заблаговременно разработать структуру реагирования на инцидент, а также перечень основных вопросов, которые должны быть отражены в планах непрерывности бизнеса и реагирования на инциденты.

## Комментарии к разделу 4.3.1 стандарта BS 25999-2

1. Во вводном разделе 4.3.1 содержится требование использовать при разработке планов обеспечения непрерывности и управления инцидентами тех результатов, которые были получены на предыдущих этапах. Прежде всего, планы должны соответствовать выбранной стратегии. Это означает, что если в стратегии указано, что критичные процессы восстанавливаются силами сотрудников определенных подразделений, то и в планах должны быть описаны действия именно этих сотрудников. Или если в стратегии указано целевое время восстановления, то и планы должны описывать восстановление штатного уровня производительности именно за это время. Кроме того, в этом разделе специально указывается необходимость не только разработать и изложить на бумаге, но и реализовать описанные защитные меры, как, например, оборудовать запасные рабочие места, скомплектовать аварийные чемоданчики, установить дополнительные средства связи и т.п.

## Комментарии к разделу 4.3.2 стандарта BS 25999-2

1. Раздел 4.3.2 содержит требования, предъявляемые к ответственным за реагирование на инцидент сотрудникам, и обоснование необходимости доведения информации о структуре реагирования до всего коллектива организации.
2. В подразделе 4.3.2.1 подчеркивается, что сотрудники, ответственные за реагирование на инцидент, должны быть также наделены соответствующими полномочиями. Характер инцидента может быть таков, что не оставит времени для большого количества согласований, поэтому инцидент-менеджер должен обладать правом проявлять инициативу и принимать ответственные решения. Кроме того, за реагирование на инциденты в организации могут отвечать несколько специалистов. Чтобы избежать конфликтов и неразберихи в нештатной ситуации, необходимо заблаговременно четко распределить зоны ответственности каждого из этих сотрудников. Наконец, последним требованием к ответственным за реагирование на инци-

дент является уровень их компетентности, который должен соответствовать выполняемым обязанностям инцидент-менеджера. В стандарте не приводится никаких формальных критериев для определения уровня компетентности. С одной стороны, это не дает внешним аудиторам или регулирующим органам поводов выдвигать какие-либо претензии. С другой стороны, это накладывает дополнительную ответственность на руководство организации, поскольку не дает критериев для отбора достойных кандидатур.

3. В подразделе 4.3.2.2 приведено пять причин, по которым структура реагирования на инцидент должна быть доведена до всех сотрудников организации.
4. Знание структуры реагирования позволяет быстрее собрать информацию о том, какова природа и масштаб инцидента. Информация о нем будет быстрее собрана и картина происходящего окажется более подробной, если все сотрудники будут оперативно сообщать по заранее установленным каналам заранее указанным людям.
5. Без знания структуры реагирования невозможно не только собрать данные об инциденте, но и запустить процедуры реагирования, предусмотренные в данной ситуации, или же их запуск займет гораздо больше времени. Никогда не стоит надеяться на то, что в условиях инцидента сотрудники будут действовать оптимальным образом. Всегда лучше заранее в спокойной обстановке проинструктировать коллектив о том, какие действия будут ожидаться от них в случае наступления инцидента.
6. Знание структуры реагирования и своей зоны ответственности побуждает сотрудников организации отслеживать наличие у них планов и регламентов, регулирующих их деятельность при наступлении инцидента, а также проверять самим или интересоваться работоспособностью средств связи и актуальностью контактной информации.
7. Знание структуры реагирования побуждает сотрудников организации проверять наличие у них штатных аварийных средств, таких как, например, тревожные чемоданчики.
8. Знание структуры реагирования позволяет более оперативно как собирать, так и распространять информацию, причем не только внутри организации, но и за ее пределами, оповещая все заинтересованные стороны, такие как: аварийные службы, важных клиентов или поставщиков.
9. Можно еще добавить, что доступность информации о структуре реагирования облегчает ее совершенствование, поскольку рядовые сотрудники могут высказать соображения, которые были упущены из вида при ее разработке или обновлении.

## Комментарии к разделу 4.3.3 стандарта BS 25999-2

1. Раздел 4.3.3 содержит требования к содержанию и условиям хранения отдельных планов непрерывности бизнеса и реагирования на инцидент, а также и список тех вопросов, которые должны быть отражены в планах в целом.
2. Главное требование подраздела 4.3.3.1 заключается в том, что планы действий по обеспечению непрерывности критичных процессов и активностей и реагированию на инциденты должны быть сформулированы и зафиксированы на бумаге. Очевидно, что в любой организации есть неписанные правила, которые помогают сотрудникам решать поставленные задачи, а, возможно, даже опыт восстановления после чрезвычайных ситуаций. Но для того, чтобы действия были максимально эффективны, воспроизводимы и не зависели от конкретных персоналий, они должны быть изложены в письменном виде. Кроме того, планы должны опираться на ранее собранную информацию, а именно описывать порядок восстановления и поддержания критичных процессов и активностей на минимальном или штатном уровне производительности, описанных в разделе 4.1.1.
3. В подразделе 4.3.3.1 содержится список из четырех требований, которым должен удовлетворять каждый план.
4. Рамки и цели должны быть определены не только для СУНБ в целом, но и для каждого плана. Это поможет убедиться в том, что все описанные цели СУНБ детализированы хотя бы в одном из документов и что ни одна из включенных в рамки СУНБ областей не осталась неохваченной.
5. Планы необходимо писать доступным языком с использованием принятой в организации терминологии. На практике первый вариант планов пишут те, кто выполняет описываемые функции. В дальнейшем, в ходе тестирования к доработке документов привлекаются другие сотрудники схожей квалификации, которым, может быть, придется выполнять описываемые действия в условиях ЧС. Эти сотрудники корректируют фор-

мулировки планов таким образом, чтобы они сами могли воспользоваться этими инструкциями.

6. У каждого плана должен быть владелец или владельцы. Именно эти сотрудники несут ответственность за регулярное их обновление. В процессе согласования им может оказывать помощь сотрудник, ответственный за выполнение политики и внедрение СУНБ в организации, или его помощники (см. раздел 3.2.3). Но наполнение плана информацией и поддержание ее в актуальном состоянии полностью лежит на владельце(ах) планов.
7. Помимо мер восстановления деятельности, предпринимаемых силами организации, может существовать целый ряд действий аварийных служб, компетентных органов и других третьих сторон. В стандарте напоминается о необходимости учитывать подобные внешние меры и добиваться, чтобы планы организации им не противоречили. Например, в случае угрозы террористического акта доступ в здание, в котором располагается организация, будет ограничен, а в случае пожара могут оказаться недоступными линии коммуникации на значительном расстоянии от самого здания.
8. Как уже было сказано выше, планы непрерывности и реагирования на инцидент, обычно, бывают многочисленны и каждый из них имеет небольшой объем, поскольку содержит детальное описание только одной задачи. Разбиение процесса восстановления на отдельные задачи очень индивидуально. Поэтому в подразделе 4.3.3.3 стандарта приведен перечень вопросов, которые должны быть освещены. Никаких требований к тому, в каком именно документе или документах и насколько подробно должны быть освещены эти вопросы, стандарт не содержит.
9. В планах должны быть указаны способы коммуникации. Удобно указывать эти способы в каждом из документов.
10. В каждом документе следует указывать решаемые задачи и соответствующую справочную информацию. Ей может быть местоположение строений, складов с резервным вычислительным и офисным оборудованием, необходимые меры информационной и физической безопасности, регламент общения со СМИ, ссылки на другие справочные документы, существующие в организации и т.п.
11. В планах должна быть расписана организационная структура восстановления с указанием руководителей групп восстановления, их состава и зон ответственности. Подобную организационную структуру удобно включать в виде приложения в каждый план. Наличие такой диаграммы облегчает понимание ролей отдельных участников процесса восстановления и оценку текущей ситуации.
12. Помимо детального описания предпринимаемых действий, которые составляют суть каждого плана, он должен содержать информацию о том, в каких ситуациях и в соответствии с какими критериями сотрудники могут принять решение об активации плана. Распространенной практикой в России является ситуация, при которой сотрудник не имеет права принять такое решение самостоятельно, поскольку оно может потребовать значительных финансовых и человеческих ресурсов. Например, такое как активация резервного вычислительного центра и перенос туда оказавшихся под угрозой критичных производственных процессов. В таком случае в плане должно быть описано, кто может принять такое решение и как с ним связаться.
13. Планы должны содержать информацию о том, каким образом они активируются. Стоит заметить, что каждый план должен содержать информацию об активации не только себя, но и других планов, с ним связанных. Например, если план восстановления рабочих мест должен активироваться только после завершения восстановления серверных комнат, то план восстановления серверных должен содержать инструкцию по активации плана восстановления рабочих мест. Планы руководителей должны содержать информацию о методах активации всех планов более низкого уровня, которые находятся в их зоне ответственности.
14. В ряде планов, которые описывают перемещения сотрудников в процессе восстановления, должны быть указаны места сбора. Поскольку в чрезвычайной ситуации выбранное место сбора может оказаться недоступным, следует предусмотреть альтернативы. На практике часто выбирают одно основное и два запасных варианта, расположенных на разном удалении от месторасположения организации. Помимо мест сбора в планах должна присутствовать контактная информация и технология вызова аварийных служб, компаний, предоставляющих сервисы транспортировки, уборки и других внешних организаций, участие которых может потребоваться в процессе восстановления или реагирования.

15. Процесс восстановления можно разделить на три фазы: первичное реагирование, управление непрерывностью бизнеса и возвращение в штатный режим работы. Каждой фазе может соответствовать свой набор планов: первичное реагирование описывается в рамках ответа на возникший инцидент; управление непрерывностью — в планах восстановления деятельности. Для описания третьей фазы — возвращения в штатный режим работы в стандарте не предусмотрено отдельного направления деятельности и специальной категории документов. Тем не менее, в нем содержится требование о том, чтобы процесс, в рамках которого организация сможет вернуться в штатный режим функционирования, был описан в виде приложений к планам восстановления. На практике описание возвращения в штатный режим работы обычно не содержит детальной информации, поскольку такое описание может потребовать дополнительных работ по планированию уже после преодоления инцидента.
16. В планах должна содержаться контактная информация всех заинтересованных сторон, например, владельцев, представителей акционеров, поставщиков и аутсорсинговых партнеров, страховых компаний, охранных агентств, ключевых заказчиках и др. Часть этой информации может быть конфиденциальной, поэтому ее включение во все планы нецелесообразно.
17. Стандарт содержит отдельный подпункт, в котором подчеркивается первостепенная важность сохранения жизни и здоровья людей в процессе управления восстановлением деятельности организации. Для выполнения этого требования рекомендуется во всех планах выделить те шаги и меры, которые будут предназначены для обеспечения безопасности людей.
18. При описании процесса управления необходимо описать возможные варианты ответных действий в тех планах, где это имеет смысл. Для наглядности их можно представить на блок-схеме управленческих действий, на которой в каждом узле сформулирован однозначный вопрос. Ответ на такой вопрос поможет выбрать правильное направление действий.
19. В планах должно быть уделено внимание мерам по предотвращению и минимизации материальных потерь, а также сокращению простоя производственных процессов.
20. В планах, описывающих реагирование на инцидент, должен быть детально и ясно изложен порядок решения управленческих вопросов во время инцидента. Если в организации уже внедрен процесс кризис-менеджмента, то для выполнения этого требования следует воспользоваться существующими регламентами действий в кризисной ситуации.
21. Из совокупности планов должна быть ясна связь между процессами реагирования на инцидент и восстановления критичных процессов и активностей, т.е. должны быть описаны вехи или критические точки, в которых будут приниматься управленческие решения по запуску процессов восстановления. В качестве примеров можно назвать завершение эвакуации персонала, прибытие групп восстановления в места сбора, фиксированный срок недоступности сервиса, т.е. процедура восстановления активируется, если перерыв в предоставлении критичного сервиса составил 60 минут и т.п.
22. В совокупности планов должно быть уделено особое внимание процедурам и средствам связи с сотрудниками, членами их семей, ключевыми заинтересованными сторонами и аварийными службами. На практике целиком структура эскалации среди персонала организации часто описывается в отдельном документе, а в планах приводятся ее части, связанные с действиями лица, для которого предназначен данный план. Оповещение сотрудников в условиях инцидента может быть автоматизировано. Подобные решения уже существуют, в том числе и на российском рынке.
23. Очень важным является вопрос связи сотрудников со своей семьей, которому не всегда уделяют должное внимание. Как уже отмечалось в комментариях к разделу 4.2, невозможность связаться с родными может оказать сильное негативное влияние на работоспособность сотрудников.
24. Приложение с контактной информацией аварийных служб обычно включается во все планы, чтобы любой сотрудник, независимо от его роли в процессе восстановления, мог их вызвать.
25. Наконец, связь с различными заинтересованными сторонами должна поддерживаться в зависимости от конкретной ситуации, поэтому контакты с ними должны осуществляться только после распоряжения руководства и сотрудников, отвечающих за уп-

равление реагированием на инцидент или восстановлением критичных процессов или активностей.

26. Для многих организаций отношение со СМИ имеет очень большое значение. Например, стоимость акций компании может резко упасть, если в СМИ появится сообщение о каком-либо инциденте. Следует учесть, что это сообщение будет тем негативнее, чем менее достоверной информацией располагают журналисты. Поэтому лучше контролировать предоставление сведений, т.е. должна быть описана общая стратегия взаимодействия со средствами массовой информации в условиях инцидента. В стратегии должны быть отражены цели (например, донести информацию, оказать влияние, создать впечатление), целевая аудитория (кому следует сообщать в первую очередь), информация, которую следует доводить в первую очередь и которую — не сообщать совсем.
27. При описании деталей взаимодействия организации со СМИ следует предусмотреть предпочтительный способ общения с их представителями. Это может быть рассылка пресс-релизов, электронных писем, проведение пресс-конференций, выступление по радио или телевидению, публикация статей на корпоративном сайте и т.д. Необходимо предусмотреть влияние, которое может оказать чрезвычайная ситуация на возможность предоставлять информацию конкретным способом. Например, недоступность центрального офиса может затруднить публикацию информации на корпоративном сайте.
28. Подготавливая взаимодействие со СМИ, следует составить документ, регламентирующий это взаимодействие и содержащий рекомендации, на что надо обращать внимание и каких ошибок следует избегать. Для ускорения процесса подготовки пресс-релизов в кризисной ситуации следует заранее подготовить шаблон заявления для прессы.
29. Необходимо заранее определить сотрудников, в обязанности которых входит предоставление информации СМИ. Задача донесения информации в условиях кризиса является гораздо более сложной задачей, чем в штатной ситуации. Может потребоваться более внимательно учитывать эмоции аудитории, например, при сообщении о пострадавших или погибших. Накал эмоций в условиях кризиса гораздо выше, поскольку прерывание деятельности обычно затрагивает благосостояние множества людей, и ответственные за взаимоотношения с общественностью сотрудники должны уметь работать в такой обстановке.
30. В планах реагирования и восстановления должна быть предусмотрена возможность фиксирования ключевой информации об инциденте, времени выполнения предпринятых действий, принятых управленческих решениях, причинах задержек и т.п. Подобные комментарии обычно вносятся в сам план во время выполнения описываемых в нем действий. По этой причине на практике описание действий в планах представляется в табличном виде, где каждая таблица содержит несколько дополнительных столбцов для записи времени начала и окончания операции и комментариев. Можно использовать и другие методы фиксации информации об инциденте, например, видеозаписи и записи камер наблюдения, а также аудиозаписи, например, персональные диктофонные записи. Ведение записей является важной задачей кризисного управления, поскольку в дальнейшем они могут потребоваться для предоставления их страховым компаниям, аудиторам, регулирующим органам. Они могут быть использованы в суде для ответов на официальные запросы, а также для проведения послеаварийного анализа.
31. В планах должны быть подробно описаны те действия, которые будут выполняться в случае наступления инцидента. По важности этот пункт должен был бы стоять на первом месте. Ведь именно ради детализации шагов восстановления или реагирования и создаются все планы. Стоит еще раз подчеркнуть, что стандарт не содержит требований к количеству документов и степени детализации описываемых шагов. Может возникнуть искушение создать один документ, описывающий все аспекты восстановления, но стоит иметь в виду, что результатом этого, скорее всего, будет толстый том, который удобно поддерживать в актуальном состоянии (поскольку все в одном месте), но совершенно невозможно использовать в аварийной ситуации. Также стандарт не содержит требований к степени детализации описываемых шагов. Историки утверждают, что Наполеон перед тем как отдать приказ генералам проверял доходчивость и однозначность формулировки, показывая его простолюдину, который специально для этой цели находился при императоре. Если тот правильно пересказывал содержание приказа, можно было

быть уверенным, что и генералы ничего не перепутают. Похожий подход следует использовать и для тестирования планов, когда в них речь идет о достаточно простых действиях, а не о восстановлении сложных информационных систем.

32. В планах должно быть учтено, какие материальные, финансовые, людские ресурсы потребуются для поддержания минимального уровня производительности и для восстановления штатного уровня производительности. Следует иметь в виду, что процесс восстановления может занимать достаточно продолжительное время и на каждом этапе могут потребоваться различные ресурсы. Как правило, они описываются в планах реагирования и восстановления. Для удобства ресурсы можно упомянуть дважды. Один раз в тексте, описывающем предпринимаемые действия, а второй раз — в отдельном приложении. В таком виде проще контролировать наличие и степень их готовности.
33. На практике не всегда удается описать все действия в виде однозначных цепочек шагов, относящихся к восстановлению одного процесса. Часто один план описывает возобновление нескольких процессов, что делает необходимым установление их очередности. Исполнители могут не располагать информацией о том, как ход восстановительных работ других критичных процессов зависит от нормального функционирования данного процесса. Не всегда представляется целесообразным указывать эти зависимости в самих планах. Вместо этого следует задать четкие временные рамки. Тогда в планах восстановления других процессов можно будет оперировать абстрактными временными интервалами. Наконец, при описании планов всех процессов должны указываться уровни производительности, до которых процессы должны быть восстановлены. Например, для ИТ-процессов это может быть количество работающих серверов или пропускная способность каналов, а для офисных процессов — количество занятых сотрудников или стандартных операций, выполняемых в час.

### Комментарии к разделу 4.4 стандарта BS 25999-2

1. Все меры реагирования и восстановления, будь то организационные или технические, начинают устаревать сразу же после внедрения. Это связано с тем, что в любой организации постоянно происходят изменения: замена оборудования, смена сотрудников, появление новых сфер деятельности, изменение законодательства и т.д. Чтобы гарантировать непрерывность деятельности организации даже в условиях постоянных изменений, необходимо тренировать сотрудников, обновлять планы и проверять оборудование. Назначение раздела 4.4 стандарта состоит в том, чтобы перечислить требования, которые позволят эффективно поддерживать меры реагирования и восстановления в актуальном состоянии, тренировать и обучать сотрудников тому, как эти меры должны применяться в кризисной ситуации, и проводить пересмотр этих мер организованным образом.

### Комментарии к разделу 4.4.1 стандарта BS 25999-2

1. В разделе 4.4.1 содержится единственное требование, выражающее смысл всего раздела, — актуальность мер УНБ, реализованных в организации, должна поддерживаться путем проведения реальных тестов и проверочных мероприятий. Дополнительный акцент в данном разделе сделан на том, что руководство организации должно удостовериться в актуальности, т.е. для соблюдения требований стандарта одних утверждений о необходимости тестирования недостаточно. Практика показывает, что наличие даже двух альтернативных способов осуществления деятельности в случае ЧС может оказаться бесполезным просто потому, что без проведения тестирования в реальных условиях оба способа оказались нереализуемыми.

### Комментарии к разделу 4.4.2 стандарта BS 25999-2

1. Для поддержания мер реагирования и восстановления стандарт предлагает использовать несколько способов. Это могут быть различные тренировочные мероприятия, в которых участвуют сотрудники, ответственные или связанные с мерами реагирования и восстановления, или это могут быть проверочные мероприятия, когда оценку существующим мерам дают сотрудники организации. В разделе 4.4.2 речь идет о требованиях к тренировочным мероприятиям.
2. В подразделе 4.4.2.1 говорится о том, что меры реагирования и восстановления должны удовлетворять требованиям бизнеса. Таким

образом, еще раз подчеркивается необходимость привлекать к участию в УНБ бизнес-подразделения. Исходные требования этих подразделений к параметрам непрерывности были получены в рамках анализа воздействия на бизнес (см. комментарии к разделу 4.1.1). Но требования меняются со временем. Изменяются приоритеты, ужесточаются параметры восстановления, поскольку скорость ведения бизнеса постоянно возрастает. Поэтому стандарт требует, чтобы организация проверяла адекватность существующих мер, и лучшим способом сделать это является проведение тренировок.

3. Подраздел 4.4.2.2 содержит описание требований, предъявляемых к подготовке, проведению и составу тренировочных мероприятий.
4. Тренировки, которые разрабатываются в организации, должны соответствовать границам системы управления непрерывности бизнеса. Конечно, существует искушение сузить область и тренироваться в том, что лучше получается, но подобный подход не принесет пользы, а лишь создаст иллюзии готовности к чрезвычайной ситуации.
5. Тренировки должны носить регулярный характер. На практике периодичность и характер тренировочных мероприятий описываются в отдельном документе, который носит название «Стратегия тестирования». Он утверждается высшим руководством и содержит описание того, какие виды тренировочных мероприятий и в каких случаях используются в организации, с какой регулярностью они проводятся, а также описываются ситуации, в которых тестирование проводится внепланово.
6. В организации должны использоваться различные типы тренировочных мероприятий. Например, документы можно обсуждать в спокойной обстановке, сидя за столом;тестировать оборудование — в нерабочее время, а сотрудников — тренировать с помощью учебных тревог. На начальном этапе рамки каждого такого мероприятия довольно узкие и охватывают только часть процесса. По мере накопления опыта тренировки все более усложняются, их рамки расширяются, а условия проведения все более приближаются к реальным. В конечном счете, должны быть проверены все меры реагирования и восстановления. Причем, со временем граница между тренировками и штатной деятельностью может исчезнуть. Например, некоторые банковские организации в России закрывают банковский день, пользуясь только резервным серверным оборудованием и системами хранения данных. А одна из крупнейших телекоммуникационных компаний «British Telecom» каждые две недели в режиме реального времени переносит деятельность из одного вычислительного центра в другой.
7. Организация должна таким образом планировать каждое тренировочное мероприятие, чтобы свети риск наступления инцидента к минимуму. Известны случаи, когда руководство отключало основное электропитание помещения с оборудованием, поддерживающим критичные процессы, чтобы проверить справедливость утверждений подчиненных о том, что организация готова к наступлению ЧП такого рода. Подобный импульсивный подход, конечно, позволяет проверить наличие мер реагирования и восстановления, но и последствия его могут оказаться поистине катастрофическими. Т.е. вместо того, чтобы способствовать предотвращению или минимизации ущерба, неподготовленная тренировка может его увеличить.
8. Для каждого тренировочного мероприятия должны быть в явном виде определены цели его проведения и задачи, решаемые в его рамках. Одно и то же мероприятие может быть использовано для более активного вовлечения участников в процесс УНБ, для более глубокого ознакомления с планами, для нахождения пробелов и неточностей в документации, для проверки достаточности выделенных ресурсов и т.д. Четкая формулировка решаемых задач и преследуемых целей позволит качественнее подготовиться к проведению тренировки (например, написать сценарий, определить круг участников, подготовить ресурсы) и получить результаты, которые можно будет в дальнейшем использовать для совершенствования СУНБ.
9. Необходимо проводить разбор результатов каждого тренировочного мероприятия. Этот разбор может проходить как сразу по окончании тренировки (по горячим следам), так и спустя некоторое время, когда все участники смогут сформулировать свое мнение о произошедшем. В ходе разбора должно быть четко определено, в какой мере были достигнуты поставленные цели, какие действия были уместны, а какие — нет, и как надо было бы действовать на самом деле, какие изменения следует внести в планы, каких ресурсов оказалось недостаточно и т.д.

10. Результаты тренировки должны быть зафиксированы. Причем для повышения эффективности фиксацией результатов должен заниматься независимый наблюдатель, например, внутренний аудитор организации. Подобные отчеты способствуют совершенствованию СУНБ, поскольку помимо результатов содержат рекомендации по улучшению и позволяют, например, внешним сертифицирующим организациям получить представление о качестве процесса УНБ.

### Комментарии к разделу 4.4.3 стандарта BS 25999-2

1. В разделе 4.4.3 речь идет о требованиях к проверочным мероприятиям. Проверки могут осуществляться самими сотрудниками, вовлеченными в процесс УНБ. Подобное мероприятие в стандарте называется самооценкой. Либо для проведения проверок могут привлекаться независимые сотрудники компании. Такая организация проверочного мероприятия носит название аудита.
2. В подразделе 4.4.3.1 содержится требование проводить проверочные мероприятия на регулярной основе, чтобы подтвердить их работоспособность и эффективность. В отличие от тренировочных мероприятий, о которых шла речь в разделе 4.4.2, стандарт в данном случае не содержит требования проводить пересмотр мер УНБ в случае значительных изменений, однако это упущение будет исправлено в следующем подразделе. В рамках проверочных мероприятий решаются такие задачи, как: соответствие СУНБ стратегическим целям организации, полнота перечня угроз и сценариев угроз, проверка требований к ресурсному обеспечению, пересмотр контрактных обязательств и их влияния на меры УНБ и т.п.
3. В подразделе 4.4.3.2 говорится, что организация должна не просто проверять работоспособность и эффективность мер УНБ, но и гарантировать регулярность таких проверок. Кроме того, в данном подразделе выдвигается требование проводить проверочные мероприятия в случае значительных изменений. На практике к таким изменениям относятся появление новых угроз или снижение риск-аппетита руководителей организации, смена целей организации, уменьшение доступных или увеличение требуемых для восстановления ресурсов, изменения во взаимоотношениях с заинтересованными сторонами, например, поставщиками уникальных услуг и др.
4. В подразделе 4.4.3.3 описывается, в какой форме должно проходить проверочное мероприятие. Стандарт предусматривает две такие формы: самооценка и аудит. При проведении самооценки участвуют те же сотрудники, которые отвечают за разработку и внедрение СУНБ организации. Преимуществом такой проверки является то, что для ее проведения не требуется привлекать дополнительные ресурсы. Недостаток — при оценке результатов собственной работы трудно сохранить объективность. Более предпочтительной формой проверочного мероприятия является аудит. Его проводит сотрудник организации, который не вовлечен в процесс УНБ. Эта процедура отличается от проведения внутреннего аудита, который описан в разделе 5.1. Независимость специалиста, выполняющего аудит, обычно гарантируется тем, что он не отвечает за результаты проверяемого им процесса или активности. Таким образом, при проведении аудита можно получить более объективную оценку мер УНБ, но он может занять больше времени и потребует привлечения дополнительных людских ресурсов.
5. В подразделе 4.4.3.4 перечислены пять требований, совершенных при возникновении инцидента и для устранения его последствий, которым должен удовлетворять анализ действий. В данном подразделе, в отличие от подраздела 4.4.2.2, не указано, что данный анализ должен быть документально зафиксирован. Однако отсутствие такого документа, прежде всего, затруднит организации совершенствование СУНБ и произведет негативное впечатление на сертифицирующую организацию.
6. Анализ действий по устранению инцидента должен выявить природу инцидента и вызвавшие его причины. Какие риски были упущены из виду? Что не было предпринято для предотвращения инцидента?
7. В рамках анализа действий по устранению инцидента должна быть дана оценка действиям и принятым решениям руководителей. Какую помощь могли бы оказать руководители непострадавших подразделений? Что бы произошло в случае отсутствия ключевых лиц? Какие проблемы возникали с координацией и контролем действий?
8. В рамках анализа действий по устранению инцидента должна быть оценена адекватность параметров восстановления. Был ли

минимальный уровень производительности достигнут за установленный промежуток времени? Является ли установленный уровень действительно минимально допустимым? Был ли восстановлен штатный уровень производительности за целевое время восстановления? Смогли ли сотрудники эффективно работать сразу после завершения процесса восстановления?

9. В рамках анализа действий по устранению инцидента необходимо оценить адекватность и достаточность мер, которые предпринимались для подготовки сотрудников к возможному инциденту. Демонстрировало ли руководство пример? Проводилось ли обучение сотрудников на регулярной основе? Присутствует ли упоминание обязанностей сотрудников в случае инцидента в должностных инструкциях?
10. В рамках анализа действий по устранению инцидента необходимо сформулировать те изменения, которые будут внесены в СУНБ. Эти изменения могут касаться планов реагирования и восстановления, технических мер, сотрудников, ответственных за УНБ, организационной структуры организации, ее территориального распределения и даже организации бизнес-процессов. После того, как все изменения будут сформулированы и согласованы, следует составить календарный план их внедрения. С некоторым преувеличением можно сказать, что тренировочное или проверочное мероприятие не завершено, пока не завершена реализация этого плана.

### Заключение

Выше были рассмотрены два из четырех этапов ПРПД-цикла — Планирование системы управления непрерывностью бизнеса и Внедрение и эксплуатация СУНБ. После завершения этих этапов, можно считать сделанным первый шаг — удалось ввязаться в драку, как говорил Наполеон. Но теперь предстоит совершить второй шаг, к которому так беспечно отнесся французский император. Во второй части комментарии будут относиться к тому, каким образом СУНБ надо поддерживать в работоспособном состоянии и совершенствовать. Иными словами, как из состояния аврала, кризиса, ломки устоявшегося образа действий происходит переход в спокойное, стабильное, будничное состояние. Опасно преуменьшать значение этого шага, ведь именно здесь кроются главные причины неудач разнообразных проектов, продолжительных по срокам внедрения и связанных с достижением нематериальных или трудноизмеримых целей, таких как внедрение систем корпоративного управления (ERP) или реинжиниринг бизнес-процессов.

Закончить этот номер хочется старым, но как нельзя более уместным анекдотом.

*Нашли как-то Петька с Василием Ивановичем популярный журнал по летному делу и решили полетать на трофейном самолете. Сели в кабину, Петька — читает, Василий Иванович — делает.*

- *Завести мотор — ключ по часовой стрелке направо.*
- *Сделано!*
- *Газ до упора.*
- *Сделано!*
- *Руль на себя.*
- *Сделано, взлетаем!*
- *Мертвая петля — руль до конца на себя, должны лететь вверх.*
- *Сделано!*
- *Теперь руль от себя — должны лететь вертикально вниз.*
- *Сделано, Петька, быстро-то как летим!*
- *Все, Василий Иванович, прилетели, тут пишут, что продолжение в следующем номере!!!*

## Список литературы


1. British Standard BS 25999-2:2007 Business continuity management — Part 2: Specification. (http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030169700)
2. Названия разделов и перевод терминов соответствует русскому переводу британского стандарта «Управление непрерывностью бизнеса — часть 2: Спецификация», выполненному компанией ООО «ГлобалТраст Солюшинс» (http://gtrust.ru/show_good.php?idtov=1135) совместно с ООО «Алмитек».
3. Business Continuity Management. A crisis approach. Dominic Elliott, Ethne Swartz и Brahim Herbane
4. Business Continuity: best practices. World-Class Business Continuity Management, Andrew Hiles, 2 издание

# Управление непрерывностью бизнеса и управление операционными рисками. Где курица и где яйцо?

**Борис Альтерман,**
**исполняющий обязанности руководителя группы консалтинга**

*Здравый смысл –*
*это интуитивное чувство истины*
*(Макс Жакоб)*

В настоящем обзоре представлен анализ взаимосвязи процессов управления непрерывностью бизнеса и управления рисками, выполненный известными специалистами в данной предметной области.

Сэр Уинстон Черчилль однажды охарактеризовал Британию и Америку, как: «две нации, разделенные общим языком». Эта старая шутка довольно хорошо работает для дисциплин управления непрерывностью бизнеса и управления рисками. Обе эти дисциплины адресованы к одним и тем же проблемам, имеют одни цели и используют единую терминологию, при этом временами демонстрируя недопонимание друг друга. Риск-менеджеры пытаются учесть все типы рисков, стремятся оценить как величину ущерба, так и вероятность наступления ЧС, и затем определяют риск, как линейную функцию этих двух величин.

Специалисты по непрерывности бизнеса всегда обращают значительно большее внимание на последствия, т.е. на ущерб, который является результатом реализации ЧС. В случаях, когда возможен очень большой ущерб, бессмысленно для определения бюджета защитных мероприятий перемножать очень большую стоимость ущерба на очень малую вероятность наступления события. Получится «средняя температура по больнице», не отражающая реальное положение вещей.

Опубликованный «BSI Business Continuity Code of practice, 25999», рассматривает систему управления непрерывностью бизнеса (BCM) как дисциплину, дополняющую систему взглядов управления рисками (RM). BCM определяет риски и управляет их последствиями для бизнеса или для отдельных процессов организации. При этом, организация определяет меры, необходимые для защиты людей, помещений, производственных технологий, ИТ-инфраструктуры, цепочек поставок, интересов акционеров и репутации. На основе этой информации формируются планы действий в соответствующих обстоятельствах.

На сегодняшний день сосуществуют три точки зрения, являющиеся причиной разногласий между специалистами по непрерывности бизнеса и управлению рисками:

1. процессы управления непрерывностью бизнеса и рисками тесно взаимоувязаны «на равных»;
2. жестко связаны, при этом непрерывность — компонента риска;
3. взаимосвязаны, но сосуществуют без какой — либо иерархии между ними.

Управление рисками — хорошо укоренившаяся и понимаемая составная часть бизнес-процесса организации. В эту функциональность с трудом интегрируются современные технологии управления непрерывностью бизнеса по причине не столько реальной сложности, сколько проблемами восприятия и противодействия нововведениям. Специалисты, имеющие опыт работы с управлением рисками, имели дело с предшественниками современных методологий управления непрерывностью бизнеса, аварийного восстановления, кризисного управления и т.д., интерпретируя их, как реакцию на конкретные риски. При такой точке зрения BCM рассматривается как подмножество RM, точнее как одну из компонент RM. По сути это означает восприятие BCM как вновь изобретенного преемника аварийного восстановления (Disaster recovery), что неверно.

На самом деле управление непрерывностью бизнеса интегрирует в себе: планирование действий в чрезвычайных ситуациях (emergency planning), кризисное управление (crisis

management), планирование аварийного восстановление (disaster recovery planning), мероприятия по защите здоровья и безопасности персонала.... Такой набор процессов вполне можно интерпретировать как отдельный процесс управления рисками!

Если не привязываться к опыту специалистов по управлению рисками, анализируя функциональность процессов, можно придти к выводу, что речь идет о двух самостоятельных процессах: управление непрерывностью бизнеса и управление рисками. Ключевой вопрос: почему мы должны управлять рисками? Риторический ответ — для того, чтобы обеспечить непрерывность бизнеса! Этот довод является ключевым аргументом для позиционирования RM как компоненту BCM и в этом есть здравый смысл. Как бы то ни было, одним из первых шагов программы BCM является оценка рисков. Однако в этой аргументации существует серьезный изъян.

Управление рисками в большинстве организаций можно разделить на две части, связанные с двумя категориями рисков. Например, обеспечение возврата долгов по кредитам — предмет управления рисками банков. Защита непрерывности этого бизнес-процесса, также содержащая компоненты управления рисками, является частью общего управления непрерывностью бизнеса организации. Таким образом, управление рисками может быть как составной частью всеобъемлющих (end-to-end) бизнес-процессов, так и ключевой функцией обработки угроз выполнения самого BCM процесса, и тогда эти две функциональности RM взаимосвязаны, но существуют отдельно, без какой-либо иерархии между ними. Рассмотрим в качестве примера хеджирование обменного курса. Эта функция — часть бизнеса организации и имеет мало общего с управлением непрерывностью бизнеса. Эта функция сама по себе — управление рисками бизнеса.

Непрерывность бизнеса в данном случае заключается в способности без сбоев выполнять процесс хеджирования обменного курса. Этот процесс в условиях угроз подвержен различным рискам, т.е. необходимо управление рисками.

Из сказанного следует, что риски имуществу, людям и вообще любым ресурсам, на которых базируется бизнес, четко ассоциируется с управлением непрерывностью бизнеса и, соответственно, управлением этими рисками — подмножество BCM. Это управление не включает риски капитализации бизнеса, хеджирование и другие аналогичные функции.

Существует ошибочное мнение, что раз уж в организации поддерживаются оба эти процесса, не имеет значения, как позиционировать между собой RM и BCM. Такой подход может очень негативно отразиться на деятельности организации. Речь идет о корректном позиционировании сущности и важности этих функций в организации. Например, невозможно представить программу управления непрерывностью сложного бизнеса, ответственность за выполнение которой возложена на административно-хозяйственный отдел.

Резюмируя, приходим к следующим выводам:

1. Процесс управления непрерывностью бизнеса не должен подчиняться управлению рисками.
2. Функциональность RM является компонентой BCM.
3. Существует отдельный процесс управления рисками (операционными и стратегическими), влияющий на бизнес организации.

Любое другое распределение зон ответственности между BCM и RM каждая организация выбирает для себя сама, исходя из здравого смысла и опыта.

## Литература:

1. Andrew McCrackan — Is Business Continuity a Subset of Risk Management
2. Julia Graham — Business Continuity and Risk Management are Interwinded
3. Lyndon Bird — Business Continuity & Risk Management — two sides of the same coin

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Слободчикова Т.А. *(slobodchikova@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
*email: JetInfo@jet.msk.su  http://www.jetinfo.ru*

Подписной индекс по каталогу Роспечати 32555