

# Описание бизнес-процессов

написано Александр Астахов | 10 июня, 2023

Идентификацию (инвентаризацию) активов следует начинать сверху вниз, т.е. с идентификации и описания бизнес-процессов, а не снизу вверх, как это склонны делать ИТ специалисты, формируя при помощи специализированных программных средств ни к чему не привязанные списки информационных, программных и аппаратных активов.

Бизнес-процессы сами по себе рассматриваются в качестве основных активов организации, которые представляют собой комбинацию разнородных активов, таких как информация, технические и программные средства, кадровые ресурсы, юридические и контрактные обязательства и т.п. Все эти активы представляют ценность для организации только в контексте ее бизнес-процессов, в рамках которых они используются для достижения целей бизнеса. Поэтому, прежде чем начинать заниматься активами, необходимо разобраться с целями организации и процессами, реализуемыми для достижения этих целей.

Организации используют большое количество процессов, одни из которых можно отнести к внутренним, другие к внешним. В маленьких организациях большое количество этих процессов может реализовываться одним подразделением или даже одним человеком. Поскольку оценка информационных рисков входит в обязанности всей организации, все участники бизнеса должны идентифицировать информационные активы, являющиеся критичными для выполнения ими своих функций, и должны убедиться в том, что связанные с ними риски были оценены, а соответствующие механизмы контроля были реализованы и поддерживаются для управления идентифицированными рисками.

Для целей управления рисками мы делим все процессы на внешние и внутренние, а также на основные и вспомогательные. Определенные категории рисков являются специфичными для

определенных групп процессов. Прежде всего необходимо описать основные направления деятельности организации и бизнес-процессы в рамках этих направлений. Это внешние процессы, ориентированные на конечного потребителя и приносящие организации доход. Именно с нарушением этих бизнес-процессов связаны основные риски организации. Любые неурядицы с вспомогательными процессами несут риски для организации лишь в той степени, в которой эти вспомогательные процессы оказывают влияние на основные бизнес-процессы организации. Далее мы рассмотрим специфику основных и вспомогательных процессов и соответствующие категории рисков более подробно.

## **Основные бизнес-процессы организации**

Основными бизнес-процессами мы называем такие процессы, которые позволяют организации непосредственно зарабатывать деньги, осуществлять миссию организации и достигать ее бизнес-целей. Поскольку цели любой организации заключаются в производстве некоторых продуктов или услуг и предоставлении этих продуктов или услуг заинтересованным внешним сторонам, то мы называем такие процессы внешними. Эти процессы либо состоят во взаимодействии с внешними сторонами, либо ориентированы на внешние стороны. К внешним процессам относятся:

- продажи и маркетинг;
- производство и эксплуатацию;
- поддержку клиентов;
- логистику и доставку;
- работу с дилерами и контрагентами;
- внешние инвестиции;
- налоговый учет и уплата налогов;
- работу с акционерами;
- и т.д.

Следующие риски являются специфичными для отдельных внешних процессов организации:

- *Продажи и маркетинг.* Эти виды деятельности представляют собой жизненно важный интерфейс между организацией и обществом. В любой организации существует потенциальный риск нарушения конфиденциальности информации в ходе торговых и маркетинговых операций, а также причинения ущерба репутации организации по причине того, что не были обеспечены точность и доступность информации.
- *Производство и эксплуатация.* Информация, используемая в процессах производства и эксплуатации, должна быть очень точной и согласованной, а также доступной по первому требованию. Для тех ресурсов, которые являются критическими для процессов производства и эксплуатации, соответствующие риски должны быть четко идентифицированы и обработаны.
- *Поддержка клиентов.* Этот процесс требует точной информации, доступной по первому требованию. Последствиями нарушений являются причинение ущерба репутации организации.

## **Вспомогательные процессы организации**

Вспомогательными процессами мы называем такие процессы, которые необходимы для поддержания (обеспечения условий выполнения) основных процессов организации. Эти процессы предоставляют информацию, услуги и другие ресурсы внешним бизнес-процессам. Поэтому мы также называем такие процессы внутренними и обычно даже не используем слово бизнес в их названии, а просто говорим о внутренних либо о вспомогательных процессах организации. К таким процессам относят следующее:

- управление кадрами;
- исследования и разработки;
- администрирование и ИТ;
- финансы и бухгалтерию;
- обеспечение безопасности (физической, экономической, информационной);

- аудит;
- риск-менеджмент;
- и т.п.

Вслед за внешними бизнес-процессами такие внутренние процессы также необходимо идентифицировать и описать, т.к. без них невозможна реализация внешних бизнес-процессов.

Следующие риски являются специфичными для внутренних процессов организации:

- *Управление кадровыми ресурсами.* Риски информационной безопасности неизбежно возникают при взаимодействии сотрудников и информационных систем. Следовательно, все сотрудники играют важную роль в состоянии дел с рисками в организации. Эти риски должны учитываться при найме, обучении, поощрении, наказании, а также при увольнении или переводе на другую работу.
- *Исследования и разработки.* Эти виды деятельности могут представлять собой значительный риск в случае, если существует неконтролируемая связь между средой разработки и средой производства/эксплуатации. Исследования и разработки могут также производить строго конфиденциальную информацию, составляющую коммерческую тайну организации, такую как информация, относящаяся к разрабатываемым продуктам. Поэтому участники этих процессов должны быть осведомлены о рисках и о своей ответственности за управление ими.
- *Администрирование и ИТ.* Эти процессы часто рассматриваются в качестве процессов, несущих основную ответственность за оценку и управление рисками информационной безопасности. Однако важно, чтобы осознавалась взаимосвязь между информационными рисками и рисками организации, и, как следствие, оценка рисков информационной безопасности выполнялась всеми функциональными подразделениями и риски информационной

безопасности не рассматривались бы как исключительно «проблема ИТ».

- **Финансы и бухгалтерия.** Оценка рисков информационной безопасности имеет первостепенное значение для финансовых и бухгалтерских процессов в любой организации. Хорошее корпоративное управление требует согласованной и точной финансовой информации, которая может быть прослежена с момента своего происхождения до момента ее использования при помощи понятного журнала аудита. В соответствии с требованиями бизнеса и нормативной базы должна обеспечиваться конфиденциальность ценовой информации, финансовых результатов и прогнозов.

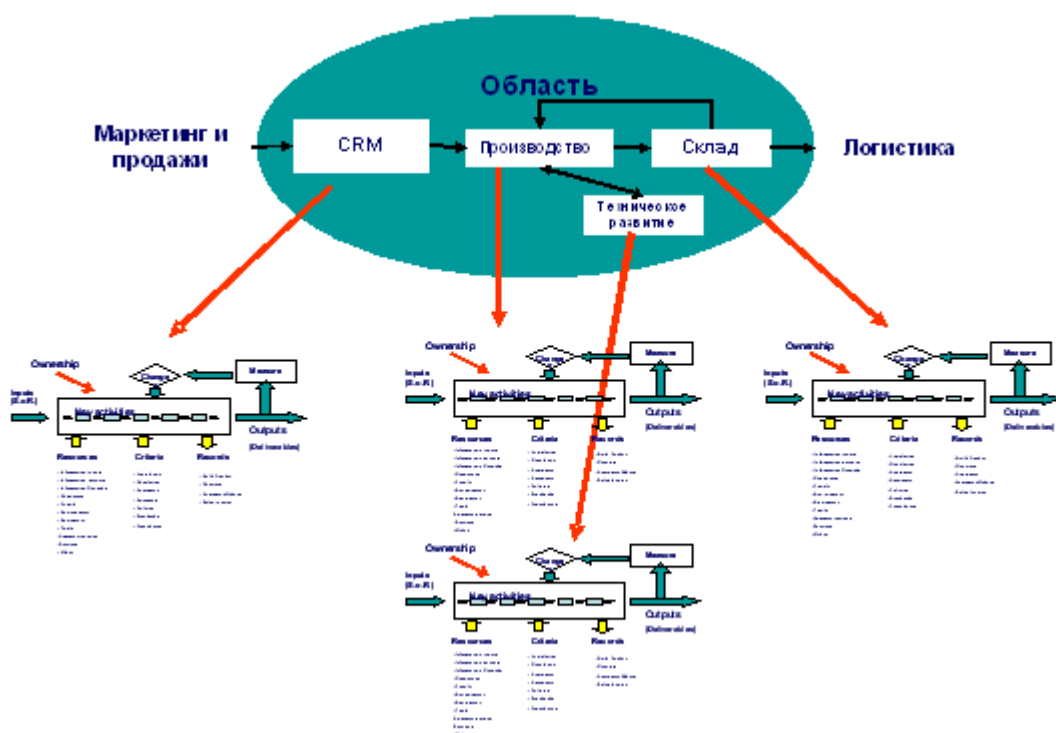
## Как идентифицировать и описывать бизнес-процесс

Информация о бизнес-процессах извлекается в ходе интервьюирования владельцев и участников этих процессов. Каждый процесс характеризуется рядом параметров, показанных на рисунке.



У каждого процесса есть определенные цели и выходные данные, которые он производит. Конечно, помимо данных, на выходе

процесса могут производиться и другие результаты, продукты, услуги или активы, однако для целей оценки рисков нам потребуются именно выходные данные. Точно таким же образом на вход любого процесса должны поступать какие-либо входные данные. Часто входные данные одного процесса являются выходными данными для другого процесса. Это, а также другие факторы определяют взаимосвязи между процессами, которые также должны быть описаны на данном этапе.



У каждого процесса должен быть явным образом назначенный владелец, который отвечает за конечный результат. Размывание ответственности за процессы и их результаты, отсутствие явным образом назначенных владельцев обычно приводит к возникновению различных сбоев, коллизий, дезорганизации процесса, отсутствию либо искажению конечного результата. Владелец процесса должен контролировать его выполнение, выходные данные и результаты. Для осуществления контроля используются такие механизмы, как аудит, мониторинг, оценка эффективности, анализ со стороны руководства и т.п. По результатам анализа результатов, выходных данных и операций в процесс могут вноситься изменения и усовершенствования. Определенные контролирующие функции, например обеспечение безопасности, владелец процесса может делегировать соответствующим специалистам, однако ответственность за процесс в целом при этом должна оставаться за владельцем.

Каждая организация осуществляет свои бизнес-процессы в определенном правовом поле, в соответствии с требованиями контрактных обязательств, требованиями клиентов, а также требованиями собственного бизнеса, т.е. теми требованиями, которые она сама для себя вырабатывает, чтобы обеспечить осуществление своей миссии. Все эти требования также должны быть идентифицированы и описаны для каждого процесса.

Подобным образом описываются все процессы в области действия СУИР и взаимосвязи между ними. Степень детализации описания процессов не должна быть слишком глубокой, однако она должна быть достаточной для идентификации информационных и связанных с ними активов, используемых для осуществления процесса, а также требований безопасности, предъявляемых к процессу и участвующим в нем активам. Бизнес-процессы обычно имеют довольно сложную структуру и если слишком глубоко в эту структуру погружаться, то можно было бы погрязнуть в деталях, зачастую бесполезных для оценки информационных рисков. Поэтому надо помнить о том, что мы начали рассмотрение бизнес-процессов лишь в связи с необходимостью идентифицировать

используемые для их осуществления информационные активы. Углубленный анализ прочих параметров смело можно оставить бизнес-аналитикам. При высокоуровневой оценке рисков описание всех бизнес-процессов организации уместается всего на нескольких страницах.

Примерный перечень вопросов, задаваемых во время интервьюирования владельцев и участников процессов, может выглядеть, например, следующим образом:

- Каковы основные бизнес-цели вашей деятельности?
- В каких бизнес-процессах вы (ваше подразделение) участвуете, какие основные функции выполняете, каким образом регламентируются ваши функциональные обязанности?
- Какие исходные данные (представленные в бумажной или электронной форме) вы используете для решения основных бизнес-задач?
- Из каких источников вы получаете исходные данные и как организован процесс получения данных?
- Где размещаются данные (документы), с которыми вы работаете?
- Каким образом осуществляется обработка (использование) данных?
- Какие приложения (локальные или серверные) вы используете для получения доступа к данным и обработки данных?
- Как осуществляется работа с приложениями (порядок выполнения основных операций)?
- Каковы предоставляемые вам полномочия по доступу к данным и приложениям?
- Кто еще является пользователями этих данных и приложений, какие полномочия имеются у них?
- За подготовку каких документов (отчетов, БД, справок и т.п.) вы отвечаете (принимаете участие)?
- Кто является заказчиком результатов вашей работы? Кому передаются подготавливаемые вами документы и в каких



бизнес-процессах они используются?

- По вашей оценке, насколько критичными для бизнеса компании являются данные, с которыми вы работаете (входные, промежуточные, выходные)?
- Как вы оцениваете возможные последствия (юридические, финансовые, репутационные и т.п.) утечки этой информации (к конкурентам, в прессу, в регулирующие органы, к криминальным элементам и т.п.)?
- Как вы оцениваете возможные последствия нарушения целостности информации (несанкционированная модификация данных, подделка документов, ошибки в отчетах, рассинхронизация БД и т.п.)?
- Как вы оцениваете возможные последствия недоступности информации (в результате сбоя системы, потери данных, случайного стирания или кражи носителей и др.)?
- Каково, по вашему мнению, максимально допустимое время недоступности данных, по истечении которого наступают крайне серьезные последствия для бизнеса компании?
- Какие требования законодательства и нормативной базы регулируют вашу деятельность?
- Каким требованиям клиентов (партнеров) вы должны удовлетворять?
- Какие существуют внутренние требования вашей организации (политики, регламенты, процедуры, инструкции и т.п.), регулирующие вашу деятельность?
- Какие записи создаются в процессе вашей работы?

Интервьюирование сотрудников организации может проводиться в произвольной форме. Результаты интервью фиксируются в таблице, показанной на рисунке.

### **Опросник №1. Описание бизнес процессов и классификация информационных ресурсов**

| <b>Название</b><br>(информационного ресурса или группы ресурсов) | <b>Назначение</b><br>(краткое описание для чего используется) | <b>Размещение</b><br>(помещения, оборудование, носители информации) | <b>Приложения и сервисы</b> | <b>Пользователи и владельцы</b> | <b>Критичность</b><br>(конфиденциальность, целостность, доступность) |
|------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------|---------------------------------|----------------------------------------------------------------------|
|                                                                  |                                                               |                                                                     |                             |                                 |                                                                      |
|                                                                  |                                                               |                                                                     |                             |                                 |                                                                      |
|                                                                  |                                                               |                                                                     |                             |                                 |                                                                      |
|                                                                  |                                                               |                                                                     |                             |                                 |                                                                      |

Можно и вовсе обойтись без каких-либо промежуточных таблиц и сразу заносить данные, полученные в ходе интервью в реестр информационных активов, описываемый далее.

## **Реестр информационных активов**

Конечной целью этапа идентификации активов является формирование реестра информационных активов. Этот ключевой документ является самым первым и одним из наиболее важных результатов на пути осознания информационных рисков и установления контроля над ними. Реестр информационных активов необходим не только для оценки рисков, но также для решения других задач, таких как планирование резервного копирования или аварийного восстановления, распределения ответственности за активы, учет активов и распределение прав доступа к ним, классификация активов по критериям конфиденциальности, целостности и доступности (при необходимости могут быть добавлены также и другие критерии классификации активов, такие как, например, аутентичность и неотказуемость). Пример реестра информационных активов изображен на рисунке.

| Реестр информационных ресурсов Компании                                                       |                             |                                                     |                 |                                                                                  |        |                    |             |             |                                   |                     |                    |
|-----------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------|-----------------|----------------------------------------------------------------------------------|--------|--------------------|-------------|-------------|-----------------------------------|---------------------|--------------------|
| Конфиденциально                                                                               |                             |                                                     |                 |                                                                                  |        |                    |             |             |                                   |                     |                    |
| Дата последнего изменения: 06.07.2008                                                         |                             |                                                     |                 |                                                                                  |        |                    |             |             |                                   |                     |                    |
| Ценность ресурса: VL - очень низкая, L - низкая, M - средняя, H - высокая, VH - очень высокая |                             |                                                     |                 |                                                                                  |        |                    |             |             |                                   |                     |                    |
| Категория                                                                                     | Название                    | Описание                                            | Размещение      | Использование (бизнес процессы)                                                  | Формат | Конфиденциальность | Целостность | Доступность | Максимальный период недоступности | Сервисы, приложения | Владелец           |
| Веб сайты                                                                                     | Корпоративный сайт Компании | <a href="http://компания.ru">http://компания.ru</a> | офисная сеть    | Представительство компании в сети Интернет                                       |        | –                  | L           | L           | 1 день                            |                     | ИТ, маркетинг      |
|                                                                                               | Сайт проекта X              | <a href="http://проект1.ru">http://проект1.ru</a>   | ЦОД             | Представительство проекта в сети Интернет, коммуникация с клиентами и партнерами |        | –                  | M           | M           | 1 час                             |                     | ИТ                 |
|                                                                                               | Сайт проекта У              | <a href="http://проект2.ru">http://проект2.ru</a>   | ЦОД             | Представительство проекта в сети Интернет, коммуникация с клиентами и партнерами |        | –                  | L           | M           | 1 час                             |                     | ИТ                 |
| Данные по клиентам и партнерам                                                                | Коммерческое предложение    |                                                     | файловый сервер | Работа с клиентами, пресейп                                                      | doc    | L                  | –           | –           | 1 неделя                          |                     | Департамент продаж |
|                                                                                               | Электронные сообщения       | Входящая и исходящая электронная почта сотрудников  | файловый сервер | Внутренние и внешние коммуникации                                                |        | H                  | –           | M           | 3 часа                            |                     | все                |
|                                                                                               | Презентации                 | Презентации для клиентов и партнеров                | файловый сервер | Привлечение новых клиентов и партнеров                                           | ppt    | L                  | –           | –           | 2 недели                          |                     | Департамент продаж |

В реестре активов вводится определенная классификация активов по своему назначению, месторасположению, принадлежности к бизнес-процессам. Так отдельную категорию активов составляют веб-сайты организации, бухгалтерская документация, проектная документация и хранилище электронной почты. Такая классификация активов облегчает ведение их учета.

Каждая категория активов может содержать как группы активов, так и отдельные активы. Однотипные активы, схожие по своему назначению, предъявляемым требованиям, способам использования и предоставления доступа и имеющие примерно одинаковую ценность для организации, следует группировать. Группа однотипных активов может рассматриваться при последующей оценке рисков в качестве единого актива. Степень детализации описания активов в реестре должна быть достаточной для оценки рисков этих активов. Для первичной высокоуровневой оценки не требуется высокой степени детализации, поэтому для средней организации может рассматриваться всего лишь несколько десятков основных активов. Для более детальной оценки рисков, необходимость в которой возникает далеко не всегда и не у

всех, может производиться декомбинация имеющихся групп активов на подгруппы и на отдельные активы. В этом случае реестр активов может насчитывать сотни и даже тысячи записей.

Для каждого актива (группы активов) в реестре должно быть приведено его описание, указано месторасположение этого актива в терминах оборудования и площадок, сервисы и приложения, использующие данный актив, форматы, в которых он представлен, а также пользователи и владелец данного актива.

Помимо всего перечисленного, реестр также определяет для каждого актива его классификацию в терминах конфиденциальности, целостности и доступности, включая максимально допустимое время недоступности данного актива. Эти характеристики определяются и проставляются в реестре активов позднее – на этапе оценки ценности активов.

Вместе с формированием реестра активов в организации должен быть реализован непрерывный процесс инвентаризации активов, обеспечивающих актуальность этого документа и его взаимосвязь с другими реестрами: программными, аппаратными, кадровыми, если таковые имеются в организации. Регламентирует этот процесс, как правило, политика инвентаризации активов. Для инвентаризации активов, помимо интервьюирования владельцев и пользователей этих активов, может использоваться специализированное программное обеспечение, обеспечивающее актуализацию, хранение и управление доступом к реестру активов.