Сафина Е.А., Ткачев Е.Д., Яненко Е.Н.
Проблемы и принципы идентификации риска

*Российская академия народного хозяйства и государственной службы при
Президенте Российской Федерации Сибирский Институт Управления –
филиал РАНХиГС
(Россия, Новосибирск)*

doi:10.18411/spc-08-04-2019-14

idsp: sciencepublic-08-04-2019-14

Сегодня основной проблемой в управлении рисками можно назвать то, что отсутствует конкретный, четко прописанный алгоритм выявления рисков для конкретной отрасли экономики. Существует лишь некий набор приемов, согласно которому можно определить перечень возможных рисков.

Цифровая экономика – это уже ближайшее будущее. Выбранный мегатренд трансформации общества не терпит отсрочки, так как весь мир стремительно развивается с помощью цифровых технологий и роботизации и вытесняет с рынков неконкурентоспособные страны. Однозначно, трансформацию будут претерпевать не только экономические интересы, но и механизмы их реализации, и система распределения ответственности за принятые решения [2]. Это, несомненно, должно наложить свой отпечаток на все сферы деятельности в области экономики, привести к упрощению расчетов и увеличению скорости обработки информации.

Идентификация (выявление) рисков - достаточно значимый элемент в управлении рисками. Риск, не идентифицированный на данном этапе, не подлежит рассмотрению в последующем анализе. [4]. Например, риск, который идентифицирован поверхностно, имеет возможность быть принятым несущественным и неактуальным. Это может привести в дальнейшем к погрешностям оценивания рисков и ошибочной обработки. В условиях цифровизации экономики важно понимать проблемы, возникающие в процессе идентификации риска. В данной статье обозначим принципы, с помощью которых можно преодолеть эти проблемы.

Главной задачей идентификации и изучения рисков является формирование у лиц четкой и единой картины рисков, которые угрожают бизнесу компании, для здоровья и жизни ее сотрудников, имущественным интересам хозяев/ владельцев акций, обязанностям, которые возникают во взаимоотношениях с клиентами и иными партнёрами, правам третьих лиц и т.п. В этом случае важен как список рисков, так и осознание менеджерами того, насколько серьезно эти опасности могут воздействовать на деятельность компании. Таким образом, будет, верно организовать систему управления рисками, которая обеспечит эффективный уровень защиты компании от этих рисков.

Согласно международному стандарту ISO/IEC 31000 работа по управлению риском строится из таких фаз [4]:

- установка контекста,
- идентификации риска,
- анализ риска,
- оценивание риск и его обработка.

Перечисленные фазы идентификации, анализа и оценивания риска значительно взаимосвязаны и взаимозависимы между собой, и создают единый постоянный процесс – процесс оценки риска. Это означает, что один метод оценки риска не имеет возможности гарантировать и обеспечить равные условия и эффективность на различных фазах. Для этого рекомендовано применить всевозможные дополнительные методы. Преимущества и недостатки всевозможных методов на различных фазах рассмотрены в международном стандарте ISO/IEC 31010 [7]. Значимость

идентификации риска заключается в определении полноты и адекватности процесса оценки риска.

Одна из главных и первостепенных проблем, которая возникает при идентификации риска, заключается в отсутствии единого понятия риска [1, 9]. Различия в определениях риска находятся в зависимости от контекста потерь, их оценки и измерения [9]. Присутствие некоторых, иногда очень противоречивых трактовок понятия «риск» затрудняет описание и последующую обработку обнаруженного риска.

Так, ISO/IEC 31000 трактует риск как «влияние неопределенности на цели организации» [4]. Данная трактовка подходит, скорее, для оценки значения риска, но не для его идентификации. С точки зрения идентификации и анализа рисков большими возможностями владеет трактовка риска как цепочки влияния угроз на активы [3] (рис.1). Каждый фактор данной цепочки расширяет все новые и новые границы в определении риска, разрешая наиболее четко сформулировать и провести оценку риска. Замечена вероятность того, что порой трудно отследить и изучить цепные (косвенные) влияния, и надлежащие угрозы.

Рисунок 1 - Цепочка влияния угроз на активы [3]

В последующем недостатки будут заключаться в рисках, которые будут забыты и/или проигнорированы до их анализа [1, 6], следуя принципу ALARA: «Факт существования риска имеет место быть, в случае, если его степень выше допустимой для объекта значения» [6]. Это приводит к сокращению адекватности выявленных оценок риска.

Итоги, которые были получены при оценке риска, нередко неудовлетворительны по причине применения неполной, неточной информации [1, 4]. Уровень неполноты с трудом поддается измерению и достаточно часто не будет приниматься во внимание при расчетах. А это, как раз, увеличивает риск того, что мы пропустим важные изменения условий хозяйствования субъекта экономики уже на стадии идентификации риска.

Почти все методы оценки риска сегодня основываются на определении риска как вероятностного ущерба [1]. Впрочем, «...идентификация риска должна подключать испытание цепной реакции конкретных результатов, охватывая каскадный эффект и суммарные действия» [4]. Некорректная оценка или же недостаточный учет побочных результатов понижает предсказательную (предупредительную) силу оценки риска.

Идентификация (выявление рисков) считается первым и наиболее необходимым этапом в процессе управления рисками. В случае, если была допущена оплошность в выявлении конкретного риска, т.е. риск был выявлен неточно, неправильно или же вообще не был предусмотрен, иные этапы в управлении данного риска не будут реализованы вообще. А это означает, что изучить этот риск и минимизировать издержки от него не получится. Также данный риск не будет учтен в последующих периодах до момента его возникновения.

Для управления рисками организация должна знать, с какими рисками в собственной деятельности она имеет возможность столкнуться. В этом случае она должна уметь проводить их оценку. Выявление рисков считается первым этапом в разработке профиля рисков организации. Идентификация риска, может быть разбита на 2 отдельных этапа:

1) первоначальное определение риска – для организаций, которые раньше не видели собственные риски в структурированном формате, а также для новых организаций, нового плана или же деятельности организации;

2) постоянная идентификация рисков, которая важна для выявления новых рисков, не возникавших раньше, и изменений рисков, которые существуют уже сейчас, или же рисков, которые присутствовали раньше, но именно в этот момент стали важны для организации.

В управлении рисками применяют разнообразные формулы и шаблоны. Каждая организация использует определенный метод, в зависимости от направления отрасли и специфики работы самой организации. Но все же есть общие методы выявления рисков. К ним можно отнести: мозговой штурм, метод Дельфи, SWOT-анализ, контрольные листы, метод построения блок-схем.

Кратко опишем специфику каждого метода отдельно.

Мозговой штурм. Данный метод применяют, когда цели четко сформулированы и понятны. Этот метод подразумевает корпоративный мыслительный процесс членов-участников, который направлен на создание перечня рисков. В случае правильного организованной мозгового штурма члены-участники согласованно сотрудничают, трудятся как одно целое, дабы сконструировать список вероятных рисков.

Для проведения процедуры мозгового штурма нужно выбрать фасилитатора – человека, который станет управлять ходом, обозначать временные сроки и наблюдать за соблюдением всех правил. Желательным условием считается присутствие у фасилитатора лидерских свойств. Все члены-участники должны быть в полной мере подготовлены и осведомлены с вопросом до начала сессии, т.е. они должны быть специалистами в ситуации, по которой в будущем должно быть принято определенное решение о проведении мозгового штурма [7].

Роль в мозговом штурме сотрудников организации из различных активных подразделений наращивает эффективность метода и значимость конечного итога, т.к. разрешает расценить, как могут воздействовать риски на всевозможные виды деятельности внутри организации.

Метод Дельфи. При применении способа Дельфи фасилитатор выдает экспертам определенные анкеты. Эксперты выражают свое личное мнение по поводу рисков проекта на критериях анонимности. Затем, как все эксперты определились с ответами, фасилитатор суммирует их и выводит точки соприкосновения мнений. Вслед за этим экспертам предлагается возможность ознакомиться с обработанными ответами коллег и изменить свои ответы. После чего, процесс повторяется до тех пор, пока все эксперты не достигнут консенсуса. С помощью метод Дельфи можно минимизировать воздействие отдельных членов экспертной группы и это позволит экспертам предоставить наиболее объективные ответы.

SWOT-анализ. Данный метод применяется в разработке стратегии организации и базируется на анализе сильных и слабых сторон организации. Сильные и слабые стороны считаются внутренними для организации и включают в себя культуру организации, структуру, денежные и человеческие ресурсы. Ключевые сильные стороны организации соединяются в главные центры ответственности, которые обеспечивают базу с целью конкурентного выдающегося преимущества. Возможности и угрозы относятся к внешним факторам и, как правило, не подконтрольны вышестоящему руководству организации в краткосрочной перспективе. Речь идет о широком диапазоне политических, общественных, экологических и отраслевых рисков.

Для эффективного SWOT-анализа в идентификации рисков, нужно затратить конкретное количество времени и приложить усилия на вычленение слабых сторон организации и вероятных угроз [7].

Контрольные листы. Отдельные организации разрабатывают контрольные листы. В них отражаются вероятные угрозы проекта. Контрольные листы базируются на собранной информации прошлых проектов. Контрольный лист - это быстрый и довольно простой метод идентификации рисков, но его не нужно относить к главному методу выявления рисков, т.к. довольно непросто выстроить исчерпывающий и актуальный список рисков для нового плана при условии быстро меняющейся экономической ситуации.

Метод построения блок-схем. Данный метод применяется для графического отображения алгоритма действий, операций или процессов определения рисков, опасностей и угроз. В рамках предоставленного метода есть большое количество иных методов, которые имеют все шансы быть применены для выявления рисков: анализ продукта (услуги), анализ взаимосвязей, анализ сайта, анализ управленческих решений и т.д. Эти методы имеют все шансы показать связи внутри организации. С их поддержкой возможно обнаружить слабые участки организации. Данные методы нацелены на выявление рисков именно в бизнес-процессах внутри самой организации, в следствие этого они имеют ограниченное использование [8].

С помощью вышеперечисленных методов можно увеличить результативность и полноту этапа идентификации риска. Для преодоления образующихся проблем применяются всевозможные пути решения [1]. Обобщим их в следующих ключевых принципах:

- 1) для оценки риска необходимо применять методы, учитывающие всевозможные методы влияния угроз на активы [4];
- 2) применять перечни рисков из соответственной области [3];
- 3) дополнить перечень рисков ситуациями с неблагоприятным итогом [5];
- 4) идентифицировать и принимать во внимание все виды ущерба, которые возможно причинят вред активам;
- 5) детализировать цепочку факторов риска начиная с последствий [3];
- 6) последствиям сравнить фиктивную уязвимость и источник, которые не идентифицированы;
- 7) детализировать моменты, начиная с более существенных;
- 8) для оценки значимости воздействия фактора, рассчитать значение ущерба от него, в самых неблагоприятных случаях;

Внедрение данных принципов для дополнения существующих методов оценки риска, позволит увеличить результативность, эффективность и полноту этапа идентификации риска. В свою очередь, это позволит ускорить процесс обработки информации, снизить время на разработку мероприятий по сокращению рисков, свойственных организации, сократить издержки.

1. Беххман Готтхард, Горохов Виталий Георгиевич, Социально-философские и методологические проблемы обращения с технологическими рисками в современном обществе [Электронный ресурс] // Журнал "Вопросы философии". – URL: http://vphil.ru/index2.php?option=com_content&task=view&id=570&pop=1&page=0&Itemid=52. (дата обращения: 20.02.2019).
2. Крылов Альберт Александрович, Концептуализация государственной информационной политики Российской Федерации // Известия Юго-Западного государственного университета. Серия: История и право. 2018. Т. 8, №1(26). С. 123–129. Википедия. Риск [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Риск>. (дата обращения: 20.02.2019).
3. Вихорев Сергей Викторович, Классификация угроз информационной безопасности. [Электронный ресурс] // Журнал Cnews. – URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения: 20.10.2018).
4. ГОСТ Р ИСО/МЭК 31000-2010. – М. :Стандартинформ, 2012. – 27 с.

5. Законы Мерфи [Электронный ресурс]. – URL: <http://murphy-law.net.ru/>. (дата обращения: 20.02.2019).
 6. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки рисков. – М.: Стандартинформ, 2012. – 70 с.
 7. Соколова Ирина Александровна, Учебно-методическое пособие по дисциплине «Оценка и анализ рисков» / сост. И.А. Соколова. – Тольятти: Изд-во ПБГУС, 2012. – 72 с.
 8. Википедия. Риск [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Риск>. (дата обращения: 20.02.2019).
-