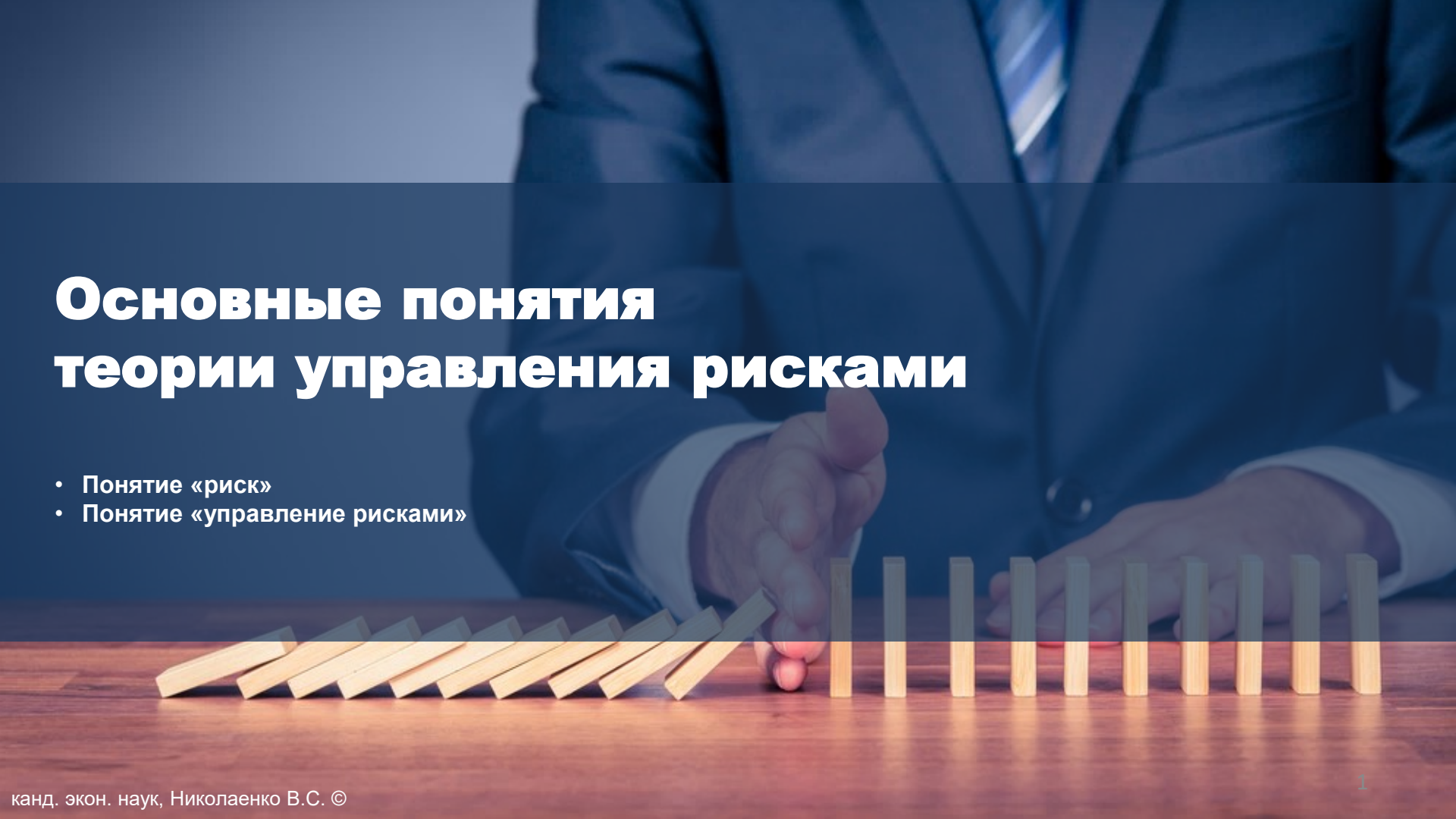


Основные понятия теории управления рисками

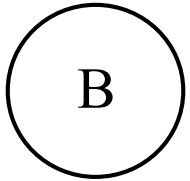
- Понятие «риск»
- Понятие «управление рисками»

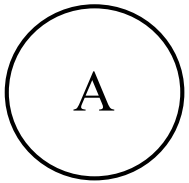
Переход субъекта из состояния А в состояние В

Эффективное и результативное управление рисками возможно, когда ясны и понятны цели, которые требуется достичь. **Для проектов такими целями являются запланированный объем работ (услуг, товаров), качество и срок их выполнения, а также бюджет. Для организаций, в зависимости от численности работников и специфики их деятельности, цели различны.** Они могут быть стратегическими, тактическими, операционным, целями конкретных отделов, подразделений, департаментов и др.

Переход субъекта из состояния А в состояние В

Рассмотрим субъект, который желает совершить переход из **состояния А** в **состояние В**. Достичь желаемого состояния субъект планирует спустя время **Т1**. Желаемое состояние В является для субъекта его целью.

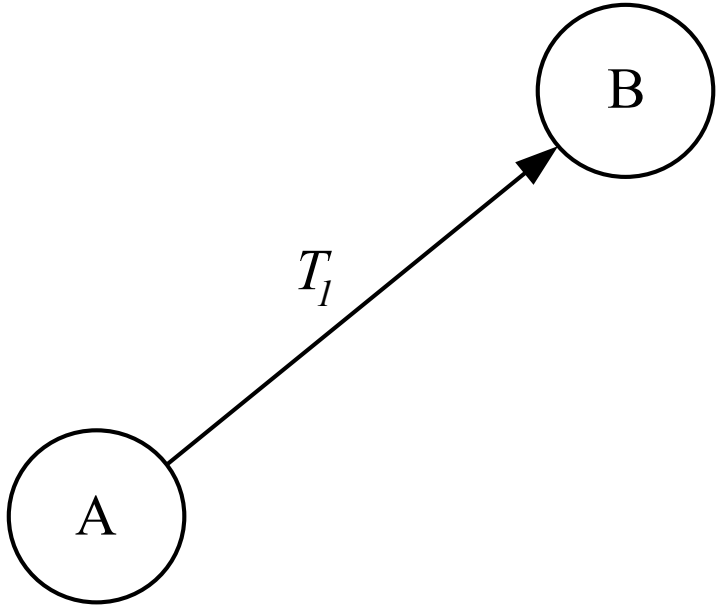




Переход субъекта из состояния А в состояние В

Сценарий 1

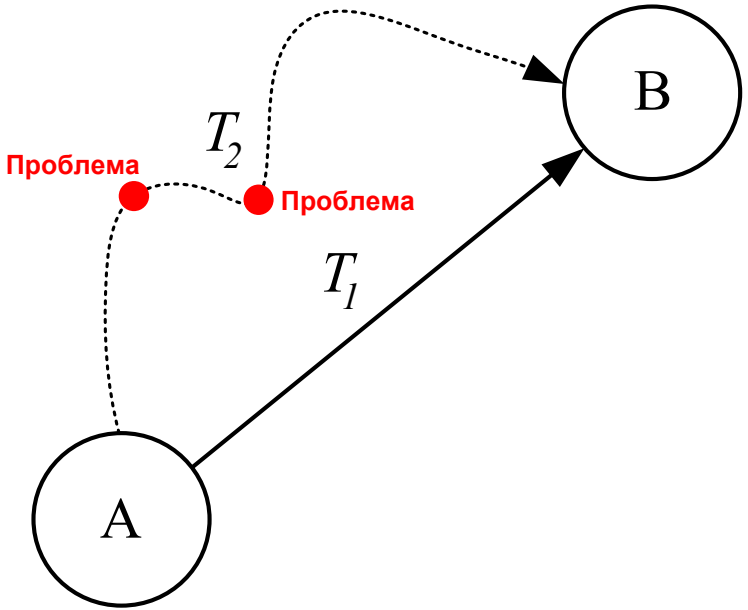
При достижении цели ничего не произойдет и субъект благополучно спустя запланированное **время Т1** достигнет ее. Этот сценарий маловероятен, потому что на процесс достижения цели будут влиять различные **штатные и нештатные ситуации**. Например, изменится цель, будут отсутствовать необходимые компетенции, ключевой сотрудник будет занят на других проектах и др. Если эти ситуации наступят, тогда для субъекта будут актуальны иные сценарии.



Переход субъекта из состояния А в состояние В

Сценарий 2

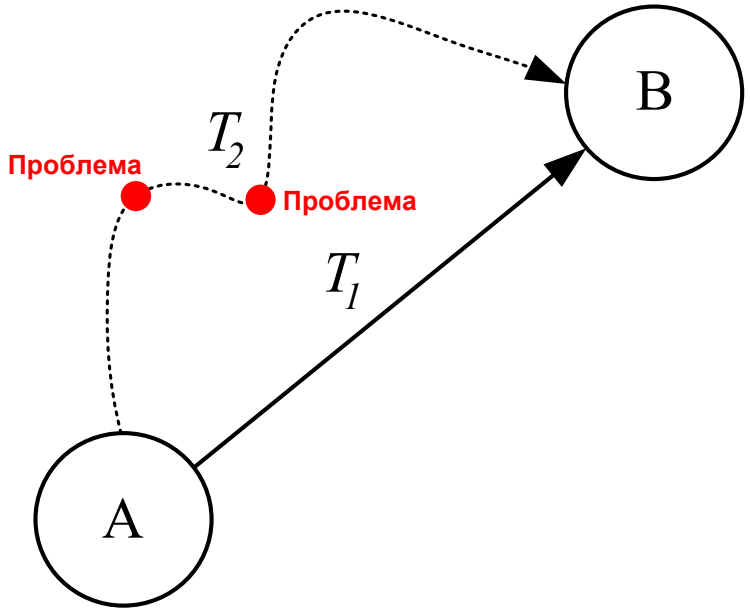
При достижении цели наступили события, которые повлияли на процесс достижения целей и на запланированное время. В результате субъект достигнет цели через **Т2**. Если наступившие события были **негативными**, то **Т2>Т1**, если **позитивными** – **Т2<Т1**. Подобный сценарий может считаться допустимым, если риск-аппетит и толерантность к риску приемлемы для субъекта. Однако если материализовавшиеся события окажут значительный материальный ущерб, то субъект не достигнет запланированной цели.



Переход субъекта из состояния А в состояние В

В качестве примера материализации рисков можно привести ущерб, который был получен от материализации **192 комплаенс рисков**.

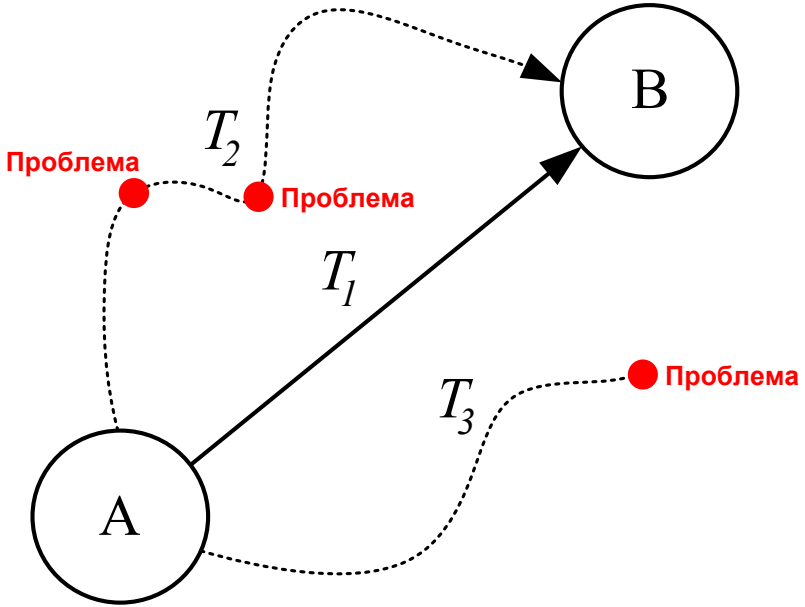
Количество комплаенс рисков обусловлено количеством исследованных решений судов, которые были выявлены во время анализа деятельности **495 ИТ-организаций Томской области (ОКВЭД: 62.0)**. На момент проведения анализа совокупные материальные потери в ИТ-организациях Томской области составили более **53 млн руб.**, а причиненный средний материальный ущерб от наступления одного комплаенс риска – **277 тыс. руб.**



Переход субъекта из состояния А в состояние В

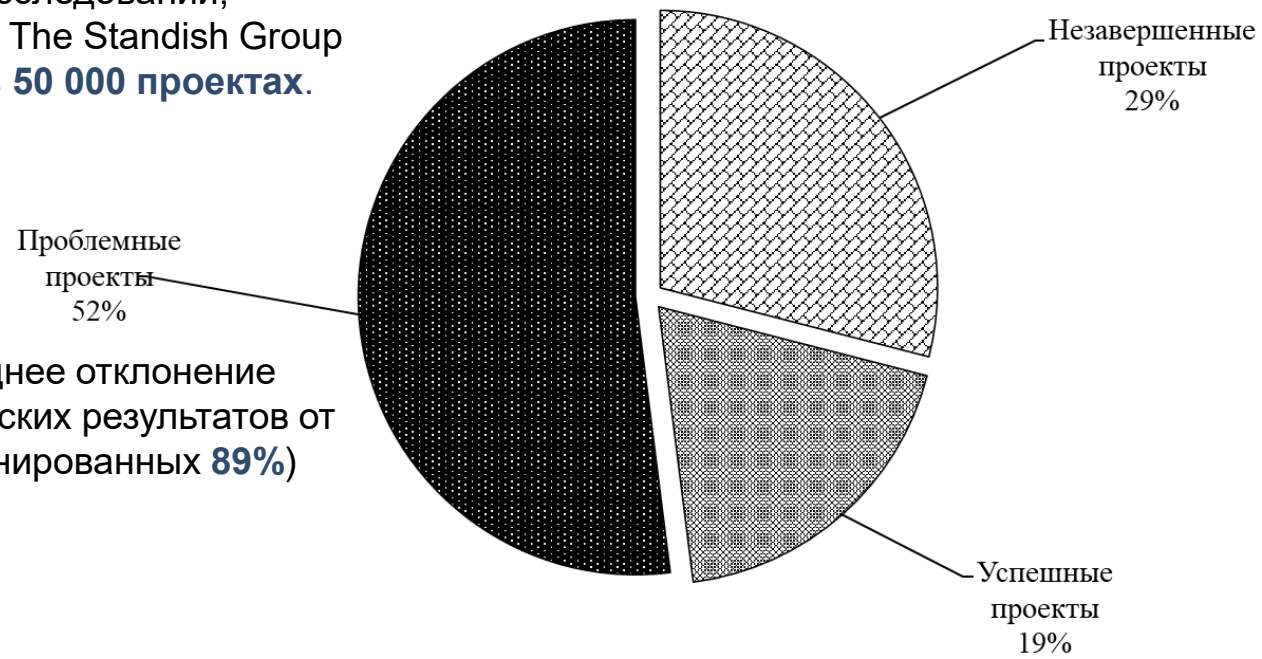
Сценарий 3

Во время достижения цели наступили события, которые не позволили субъекту достичь запланированной цели. Для субъекта подобный сценарий является неприемлемым и недопустимым. В этой связи логично предположить, что прежде чем приступить к достижению цели, субъекту необходимо заблаговременно выявить события, которые могут оказать воздействие на данный процесс.



Переход субъекта из состояния А в состояние В

Результаты исследований, проведенные The Standish Group International в **50 000 проектах**.

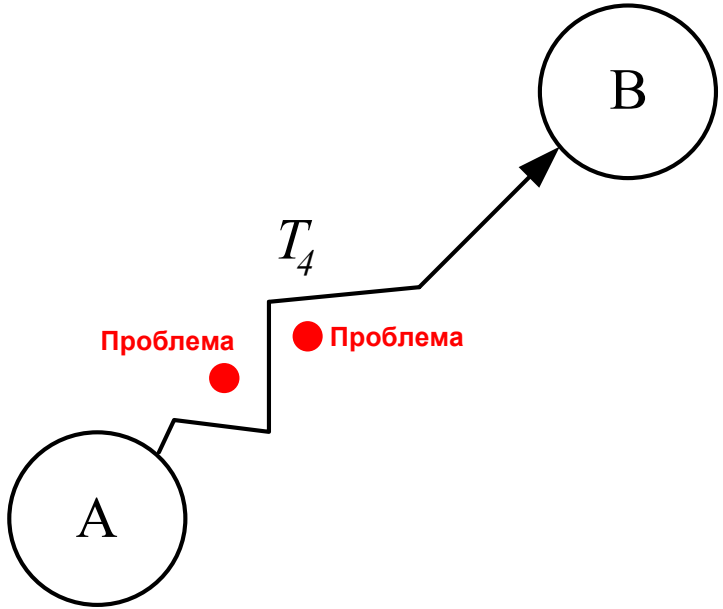


(среднее отклонение фактических результатов от запланированных **89%**)

Переход субъекта из состояния А в состояние В

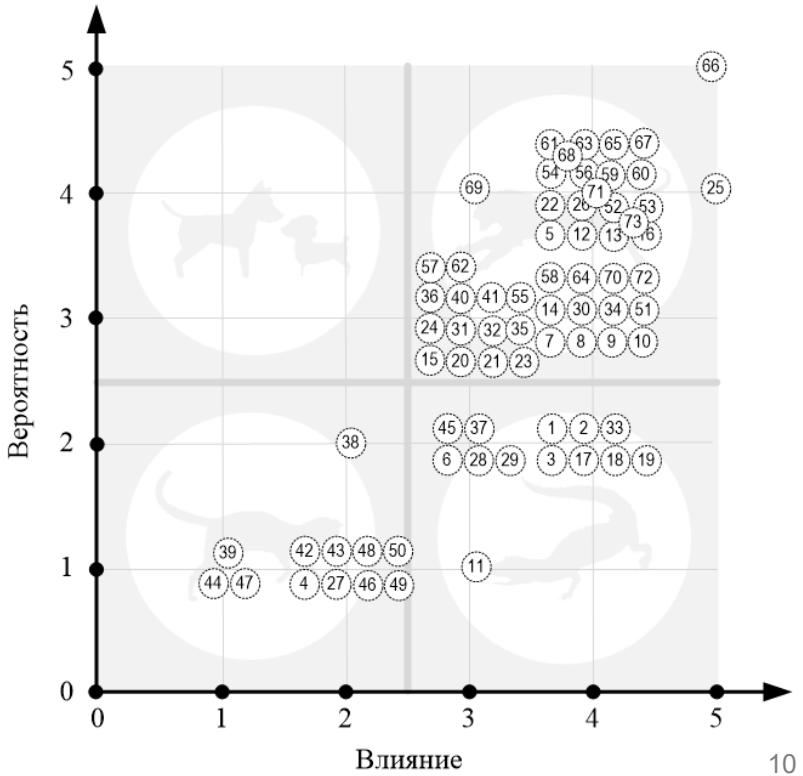
Сценарий 4

Субъект прежде чем приступать к достижению цели продумал наиболее безопасное движение и заблаговременно выявил события, которые могут повлиять на данный процесс. Кроме того, для повышения шансов на успех субъект запасся дополнительными ресурсами на случай, если наступят непредвиденные события. Стоит отметить, что возможно достижение цели в рамках сценария 4 займет больше времени (**Т4**), однако субъект гарантированно достигнет желаемой цели. Подобный процесс достижения целей называют **риск-ориентированным**.



Переход субъекта из состояния А в состояние В

Стартап: «Центр Востока»
Тип проекта: -
Методика управления: -
Количество человек: -
Размер проекта: -
Планируемая длительность: -
Фактическая длительность: -
Отклонение факта от плана: -



ПОНЯТИЕ «РИСК»

Стоит отметить, что среди лингвистов также нет единого мнения относительно этимологии понятия «риск». По мнению одних специалистов, слово **«risk»** имеет французские и итальянские истоки. Например, в итальянском языке **«risiko»** означает «опасность». С французского **«risdoe»** трактуется как «объезжать утес». Другие специалисты предполагают, что слово «риск» имеет греческие корни, беря начало от слова **«ridsikon»**, **«ridsa»**, что означает «утес», «скала» и «лавирование между скалами».

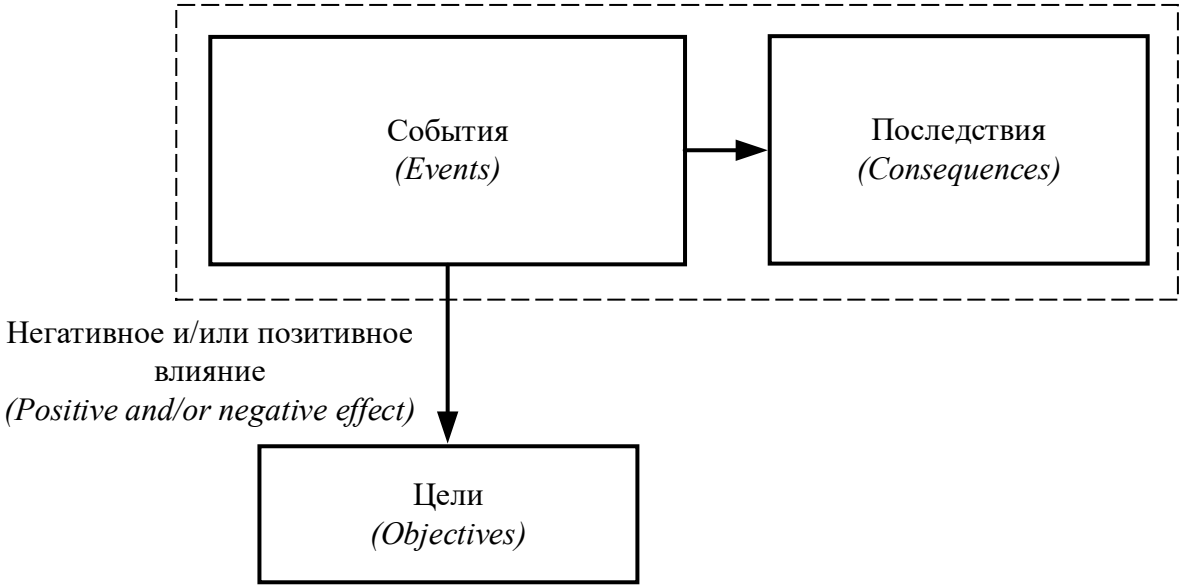
В азиатской культуре «риск» включает в себя два иероглифа 风 险, которые одновременно означают опасность и позитивную возможность.

ПОНЯТИЕ «РИСК»

Подходы к определению понятия «риск»	Источник
Влияние неопределенности на цели, где цели могут иметь различные аспекты и применяться на различных уровнях	ГОСТ Р ИСО 31000
Угроза и/или опасность	Балабанов И. Т., Машков Д. М.
Неопределенность	Филимонов Д. И., В. Н. Бурков и Д. А. Новиков, И. И. Мазур и В. Д. Шапиро
Условие или неопределенное событие, которое в случае наступления оказывает влияние хотя бы на одну цель проекта	Стандарт проектного управления Project Management Body of Knowledge
Угроза и/или возможность	Сангхира П.
Событие, которое одновременно несет угрозу, опасность, неопределенность и возможность	PricewaterhouseCoopers
Вероятность недополучения доходов и/или вероятность возникновения убытков	Грабовый П. Г., Петрова С. Н.
Численная мера опасности	Шохин Е. И.
Совокупность значений возможного ущерба в некоторой стохастической ситуации	Королев В. Ю., Бенинг В. Е., Шоргин С. Я.
Возможность получения убытков от предпринимательской деятельности	Гражданский кодекс Российской Федерации
Действия, сделанные наудачу	Даль В.

ПОНЯТИЕ «РИСК»

Современные позиции толкования термина «риск» закреплены в отечественных и международных стандартах. В частности, в отечественном стандарте **ГОСТ Р ИСО 31000** «риск» характеризуется как влияние неопределенности на запланированные цели.

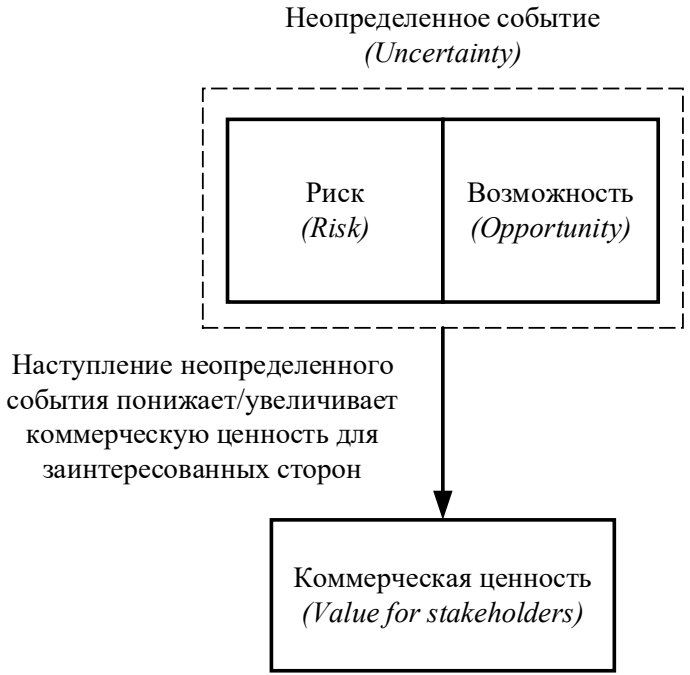


ПОНЯТИЕ «РИСК»

В международном своде знаний проектного управления **Project Management Body of Knowledge (PMBoK® Guide)** под термином «риск» понимается неопределенное событие (ситуация), которое при наступлении оказывает негативное или позитивное влияние на проектные цели, такие как содержание, длительность, стоимость и/или качество проекта.

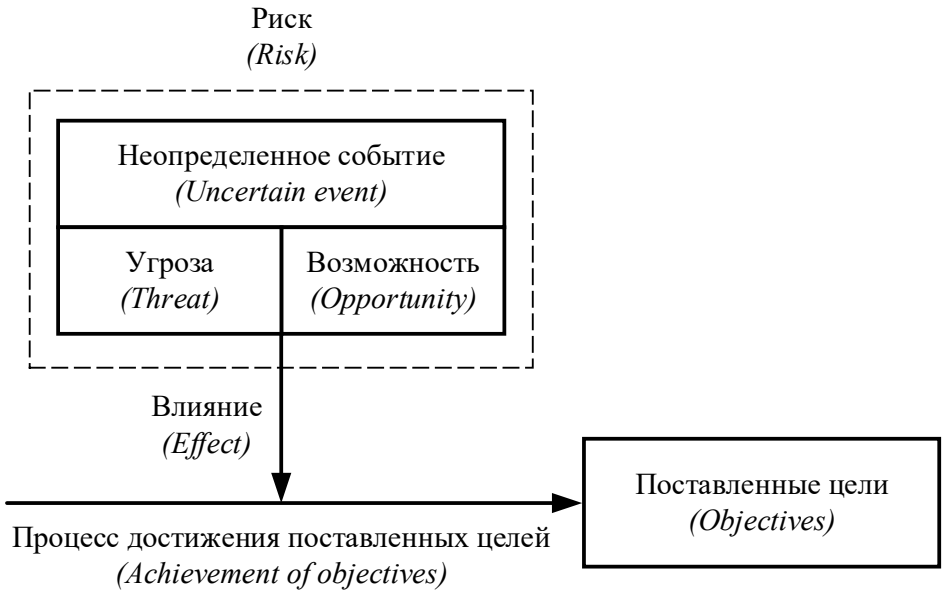
ПОНЯТИЕ «РИСК»

Свод правил **The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO ERM)** опирается на концепцию природы риска, которая была разработана PricewaterhouseCoopers (PwC). Специалисты PwC считают, что риск – это неопределенное событие, которое одновременно несет угрозу и опасность, наступление которого понижает/увеличивает коммерческую ценность для заинтересованных сторон.

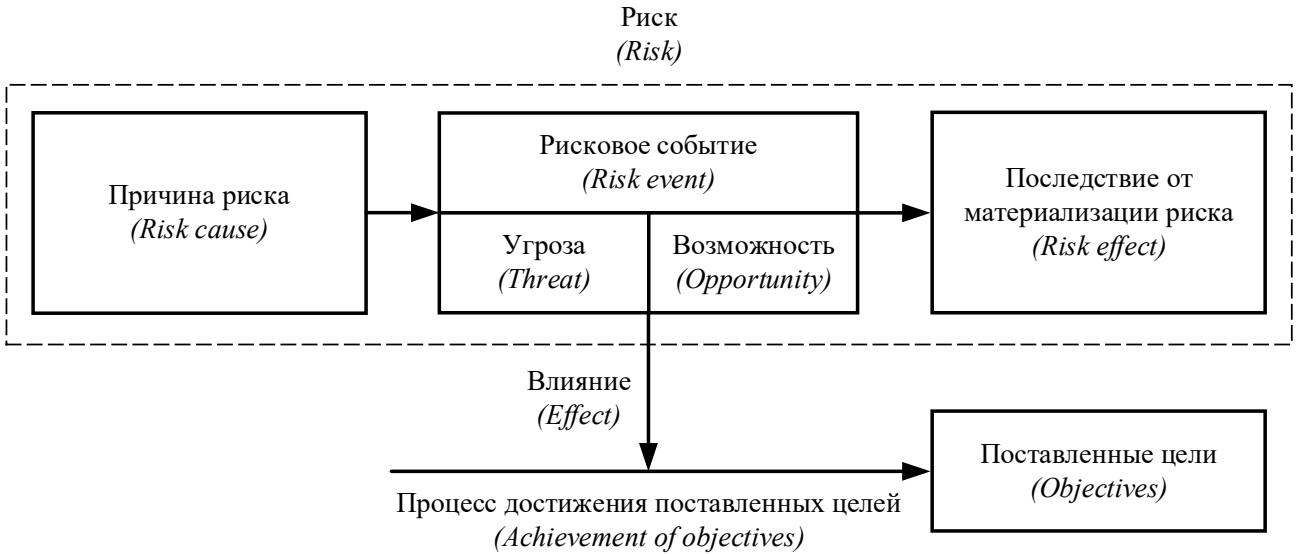


ПОНЯТИЕ «РИСК»

В международном своде управления рисками (**Management of Risk: Guidance for Practitioners, M_o_R®**) под «риском» понимается неопределенное событие, состоящее одновременно из угрозы и позитивной возможности, которое при наступлении оказывает влияние на процесс достижения целей организации.



ПОНЯТИЕ «РИСК»



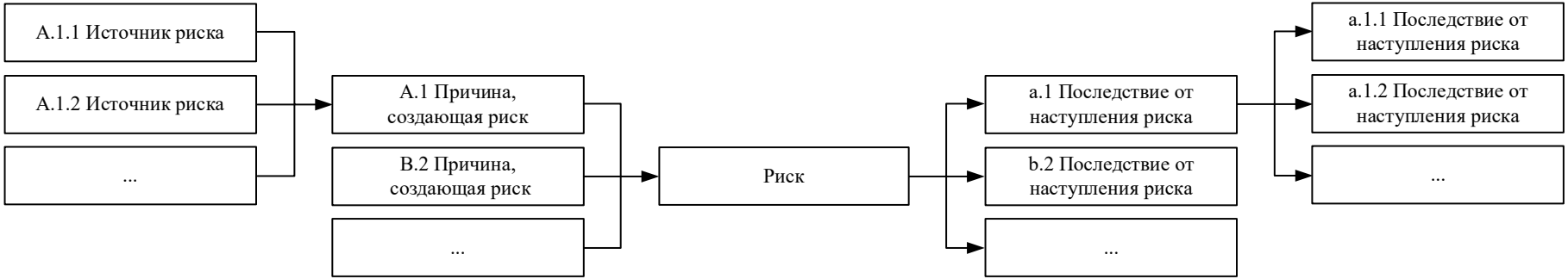
Международный свод знаний проектного управления **PRINCE2®** считает «риск» неопределенным событием, которое имеет сложную структуру. В частности, риск состоит из причины риска, угрозы, позитивной возможности и последствия в случае его материализации.

ПОНЯТИЕ «РИСК»

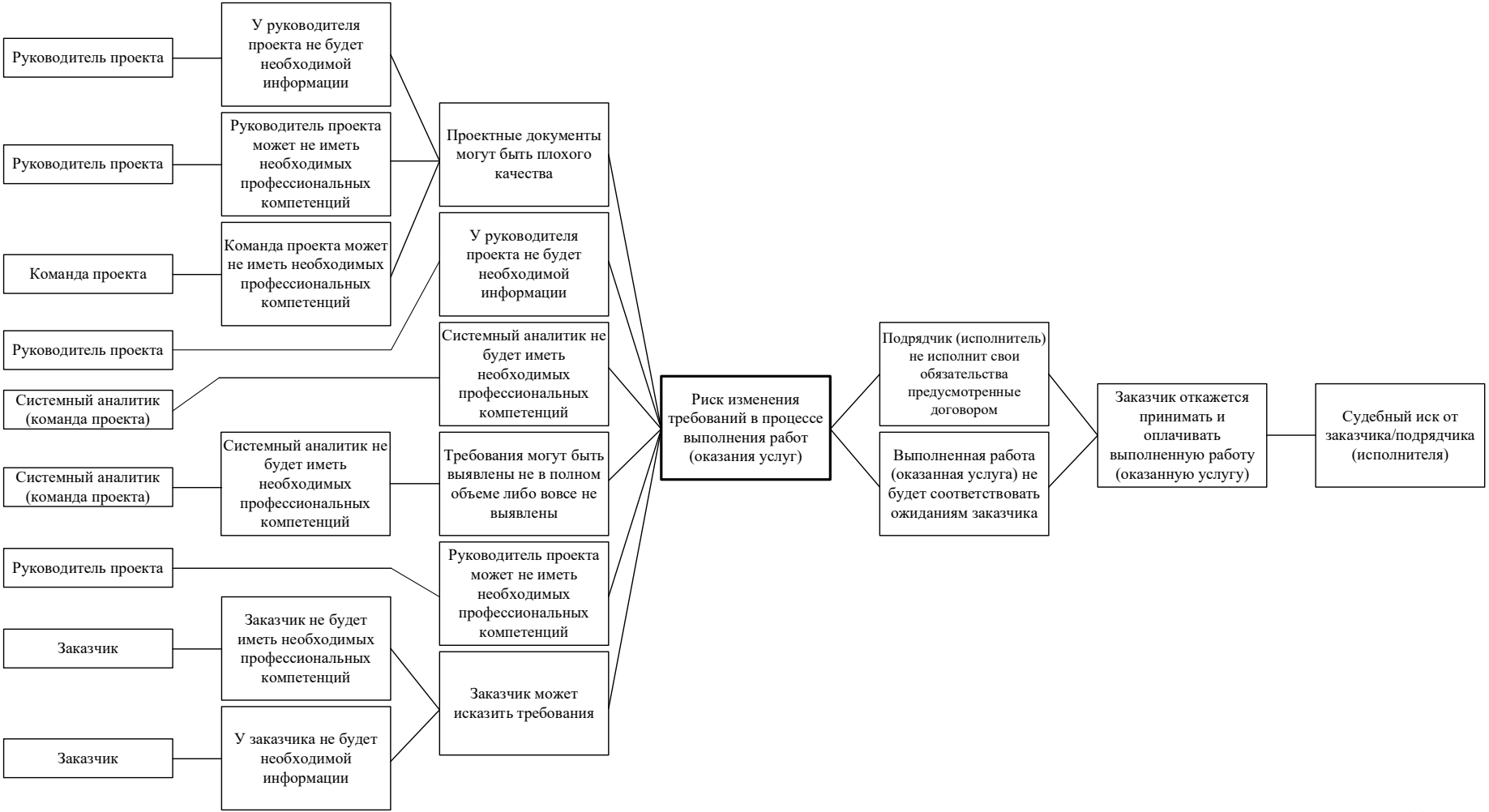
Стоит отметить, что согласно отечественным и международным стандартам понятия **«неопределенность»** и **«риск»** часто воспринимаются как синонимы. Однако между ними есть существенные различия. В частности:

- Неопределенность возникает, когда нет необходимой и достоверной информации. Риск, напротив, базируется на накопленных предшественниками статистических данных, поэтому материализация риска может быть спрогнозирована.
- При недостатке необходимой и достоверной информации неопределенность опирается на субъективные мнения, например на предыдущий опыт работников и экспертов. Риск же оперирует объективными фактами (причина, создающая риск, источник риска, последствия от материализации риска и др.).
- Источники неопределенности, как правило, не известны. Риск же создают конкретные причины и источники, каждый из которых может быть идентифицирован.

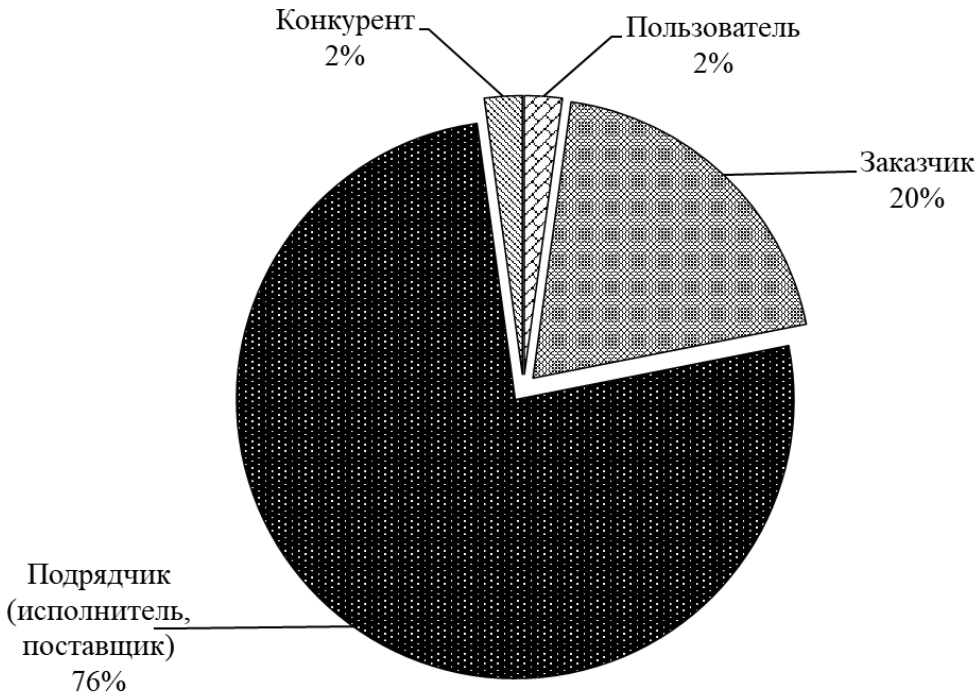
ПОНЯТИЕ «РИСК»



Таким образом, на основе рассмотренных выше точек зрения можно заключить, что **риск** – это вероятное событие, проистекающее из конкретных источников, материализация которого может привести к наступлению благоприятных/проблемных последствий. Под **причинами, создающими риск**, понимаются условия, имеющие потенциал создавать события, которые способны оказывать влияние на процесс достижения целей, под **источниками риска** понимаются объекты, имеющие потенциал создавать события, которые способны оказывать влияние на процесс достижения целей, а под **последствиями от наступления риска** понимаются новые обстоятельства, которые возникают в результате материализации риска.



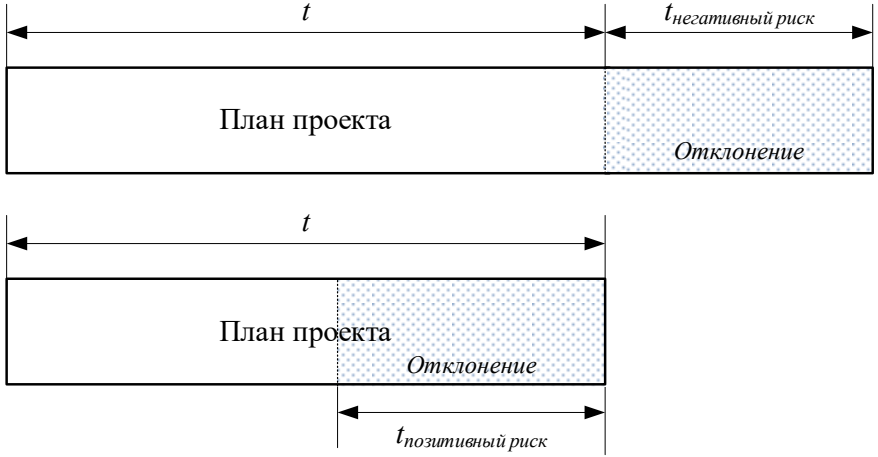
Распределение долей между источниками универсальных рисков



ПОНЯТИЕ «РИСК»

Наличие благоприятных последствий является основанием для дифференциации рисков на негативные, позитивные, нейтральные и смешанные.

- **Негативный риск** – это вероятное событие, которое может привести к наступлению проблемных последствий.
- **Позитивный риск** – это вероятное событие, которое может привести к наступлению благоприятных последствий.
- **Смешанный риск** – это вероятное событие, наступление которого приводит одновременно к проблемным и благоприятным последствиям.
- **Нейтральный риск** – это вероятное событие, которое не приводит к проблемным и/или благоприятным последствиям.



ПОНЯТИЕ «РИСК»

Необходимо отметить, что структура риска позволяет сделать важные практико-ориентированные выводы касательно последствий от наступления риска:

- Если оперативно не локализовать проблемные последствия, то в скором времени они **приведут к новым проблемным последствиям**. Например, установлено, что спецификация требований к программе для ЭВМ является неполной и недостоверной. Если оперативно не устранить данное отклонение, то вскоре последует изменение требований и целей.
- Для нейтральных и смешанных рисков необходимо блокировать наступление проблемных последствий, усиливая при этом возможный благоприятный эффект. Например, при атаке на критическую информационную инфраструктуру (КИИ), необходимо блокировать возможность неправомерного доступа, копирования, предоставления и/или распространения конфиденциальной информации, неправомерного уничтожения и/или модификации конфиденциальной информации, заражения КИИ вредоносным программным обеспечением, идентифицируя при этом возможные уязвимости КИИ.

ПОНЯТИЕ «РИСК»

Влияние материализовавшихся негативного и позитивного рисков можно охарактеризовать формулами, где **Im(negative)** – влияние в результате наступления негативного риска, **C1** – прямой материальный ущерб, **C2** – ресурсы, которые будут направлены на ликвидацию последствий, **C3** – ресурсы, которые будут направлены на восстановление, **C4** – материальный ущерб, вызванный отклонением от запланированных целей, Im(positive) – влияние в результате материализации позитивного риска, **C5** – материальная польза, вызванная отклонением от запланированных целей.

$$\mathrm{Im}_{negative} = C_1 + C_2 + C_3 + C_4 \qquad \mathrm{Im}_{positive} = C_5$$

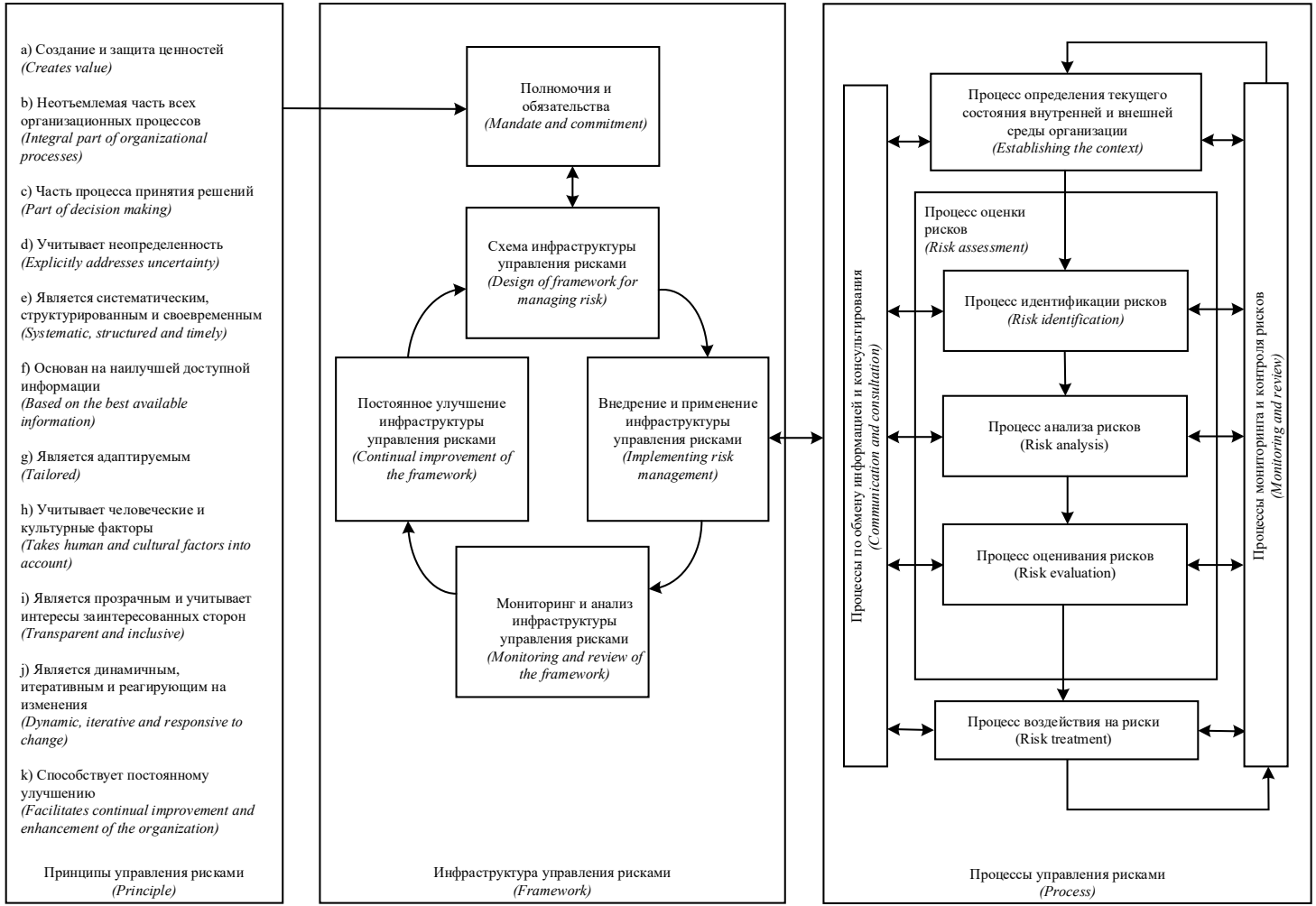
В качестве примера наступившего негативного риска можно рассмотреть ситуацию потери сервера жестких дисков в ИТ-организации в результате пожара (**C1**). Для того, чтобы ликвидировать полученные последствий ИТ-организации необходимо приобрести новый сервер (**C2**), осуществить пуско-наладочные работы (**C3**), а также оплатить простой трудовых ресурсов (**C4**),спровоцированный потерей информационных данных.

ПОНЯТИЕ «РИСК»

Наглядным примером влияния наступившего позитивного риска является привлечение в ИТ-проект программиста более высокого квалификационного уровня либо возможность проведения дополнительного аудита спецификаций требований к программам для ЭВМ. Эмпирические данные показывают, что проведение аудита по обнаружению и исправлению дефектов в спецификации требований обходится ИТ-организациям примерно в **$200**. Если же аудит не проводится, то исправление дефектов и ошибок, которые будут обнаружены конечным пользователем в созданной программе для ЭВМ, обойдутся ИТ-организации в **$4200**.

ПОНЯТИЕ «УПРАВЛЕНИЕ РИСКАМИ»

Далее рассмотрим значение термина «управление рисками» (risk management). Согласно ГОСТ Р ИСО 31000 **управление рисками** – это совокупность принципов, скоординированных действий и процессов по оценке, воздействию, мониторингу и контролю рисков. Необходимо отметить, что отечественный стандарт ГОСТ Р ИСО 31000-2010 является локализованной версией международного стандарта **ISO 31000:2009. «Risk Management – Principles and Guidelines»**.



ПОНЯТИЕ «УПРАВЛЕНИЕ РИСКАМИ»

Принципы управления рисками. Стандарт ГОСТ Р ИСО 31000 содержит 11 принципов, которых должны придерживаться организации для результативного и эффективного управления рисками. Согласно перечисленным в ГОСТе принципам, управление рисками:

1. направлено не только на достижение целей, но и на **создание и защиту общепринятых ценностей**, таких как безопасность жизни и здоровья работников, соответствие законодательным и другим обязательным требованиям, защита окружающей среды, предоставление качественной продукции, сервисов и услуг клиентам и др.;
2. **является неотъемлемой частью всех организационных процессов** (управление рисками – это часть обязанностей руководства и неотъемлемая часть всех организационных процессов, включая стратегическое планирование, управление проектами и управление изменениями);
3. **выступает частью процесса принятия решений** (управление рисками помогает работникам, принимающим решения, делать осознанный выбор и определять приоритетность действий);
4. **учитывает характер неопределенности** и стремится обеспечить переход к объективным фактам и информации;
5. **является систематическим, структурированным и своевременным** (систематический, структурированный и своевременный подход к управлению рисками способствует достижению устойчивых и стабильных результатов);
6. **основывается на наилучшей доступной информации** (входные данные для процесса управления рисками основываются на таких источниках информации, как исторические данные, опыт, обратная связь от заинтересованных сторон, наблюдения, прогнозы и экспертные оценки);
7. **является адаптируемым** (управление рисками должно соответствовать текущей внешней и внутренней ситуации (контексту));
8. **учитывает человеческие и культурные факторы** (возможности, интересы и намерения работников);
9. **является прозрачным и учитывает интересы заинтересованных сторон** (своевременное вовлечение заинтересованных сторон и лиц, принимающих решения, гарантирует, что управление рисками будет отвечать их интересам и требованиям);
10. **предстает динамичным, итеративным и реагирующим на изменения** (управление рисками должно непрерывно распознавать и реагировать на изменения, в частности, как только происходит внешнее и/или внутреннее событие, необходимо актуализировать перечень рисков, т. к. могут появиться новые риски и исчезнуть ранее выявленные);
11. **способствует постоянному улучшению** (накопление знаний о рисках дает возможность организациям создавать более совершенные стратегии управления рисками).

ПОНЯТИЕ «УПРАВЛЕНИЕ РИСКАМИ»

Инфраструктура управления рисками. Согласно стандарту ГОСТ Р ИСО 31000, для обеспечения перечисленных принципов в инфраструктуру управления рисками необходимо включить 5 элементов:

1. **Полномочия и обязательства**. Управление рисками – это итеративный и непрерывный процесс, который требует поддержки внимания со стороны руководства. Полномочия и обязательства в части управления рисками должны быть закреплены на всех уровнях организации, включая высшее руководство, средний менеджмент и остальных работников.
2. **Схема инфраструктуры управления рисками**. Результативное и эффективное внедрение управления рисками организации возможно при наличии зрелой инфраструктуры организации. Под инфраструктурой организации понимаются работники, ответственные за управление рисками, их трудовые договоры и должностные инструкции, рабочие места, специализированное программное обеспечение и др.
3. **Внедрение и применение инфраструктуры управления рисками**. При внедрении инфраструктуры управления рисками руководство должно определить стратегию, сроки и ресурсы, необходимые для внедрения, а также провести обучающие сессии для среднего менеджмента и остальных работников. Применение инфраструктуры управления рисками предусматривает внедрение процессов управления рисками на всех уровнях организации.
4. **Мониторинг и анализ инфраструктуры управления рисками**. Для поддержания инфраструктуры управления рисками в работоспособном состоянии требуется систематически оценивать качество, результативность и эффективность управления рисками, пересматривать политику, внутренние регламенты и должностные инструкции.
5. **Постоянное улучшение инфраструктуры управления рисками**. Основываясь на результатах мониторинга, руководству необходимо принимать решения в отношении улучшения инфраструктуры управления рисками.

ПОНЯТИЕ «УПРАВЛЕНИЕ РИСКАМИ»

Процессы управления рисками. Процессы управления рисками согласно ГОСТ Р ИСО 31000 включают в себя 7 процессов: обмен информацией и консультирование, определение текущего состояния внутренней и внешней среды организации, идентификацию рисков, анализ рисков, оценивание рисков, воздействия на риски, мониторинг и контроль рисков. Отметим, что процессы по идентификации, анализу и оцениванию рисков также принято называть оценкой рисков.

Процессы управления рисками состоят из таких операций, как:

- **обмен информацией и консультирование**. Обмен информацией и консультирование с внешними и внутренними заинтересованным сторонами осуществляется во всех процессах управления рисками. Данный процесс должен способствовать обмену правдивой, существенной, точной и понятной информацией с учетом аспектов конфиденциальности;
- **определение текущего состояния внутренней и внешней среды организации**. Посредством установления ситуации (контекста) организации формулируют свои цели, определяют внешние и внутренние параметры, которые следует принять во внимание в процессе управления рисками;
- **идентификация рисков**. Целью идентификации рисков является составление всеобъемлющего перечня рисков, которые в случае своего наступления могут оказать влияние на процесс достижения целей. Документ, в котором фиксируются выявленные риски, называется реестром рисков;
- **анализ рисков**. Анализ рисков направлен на сбор информации об идентифицированных рисках, а именно на установление причин, источников и возможных последствий от наступления рисков;
- **оценивание рисков**. Цель оценивания рисков – это количественное измерение вероятности наступления идентифицированных рисков и возможного влияния в случае их материализации. Под вероятностью в ГОСТ Р ИСО 31000 понимается шанс того, что что-то может произойти, а под влиянием – какое-либо отклонение от того, что ожидается (отрицательное или положительное). Документ, в котором фиксируются результаты изменения характеристик рисков, называется матрицей рисков;
- **воздействия на риски**. Данный процесс включает в себя разработку мер превентивного воздействия на риски (план А) и мер принятия рисков (план Б). Документ, в котором фиксируются разработанные меры воздействия на риски, называется план управления рисками;
- **мониторинг и контроль рисков**. Мониторинг рисков – это процесс, направленный на выявление рисков, которые не были ранее зафиксированы в реестре рисков (неидентифицированные риски). Контроль рисков – это надзор за рисками, зафиксированными в реестре рисков.