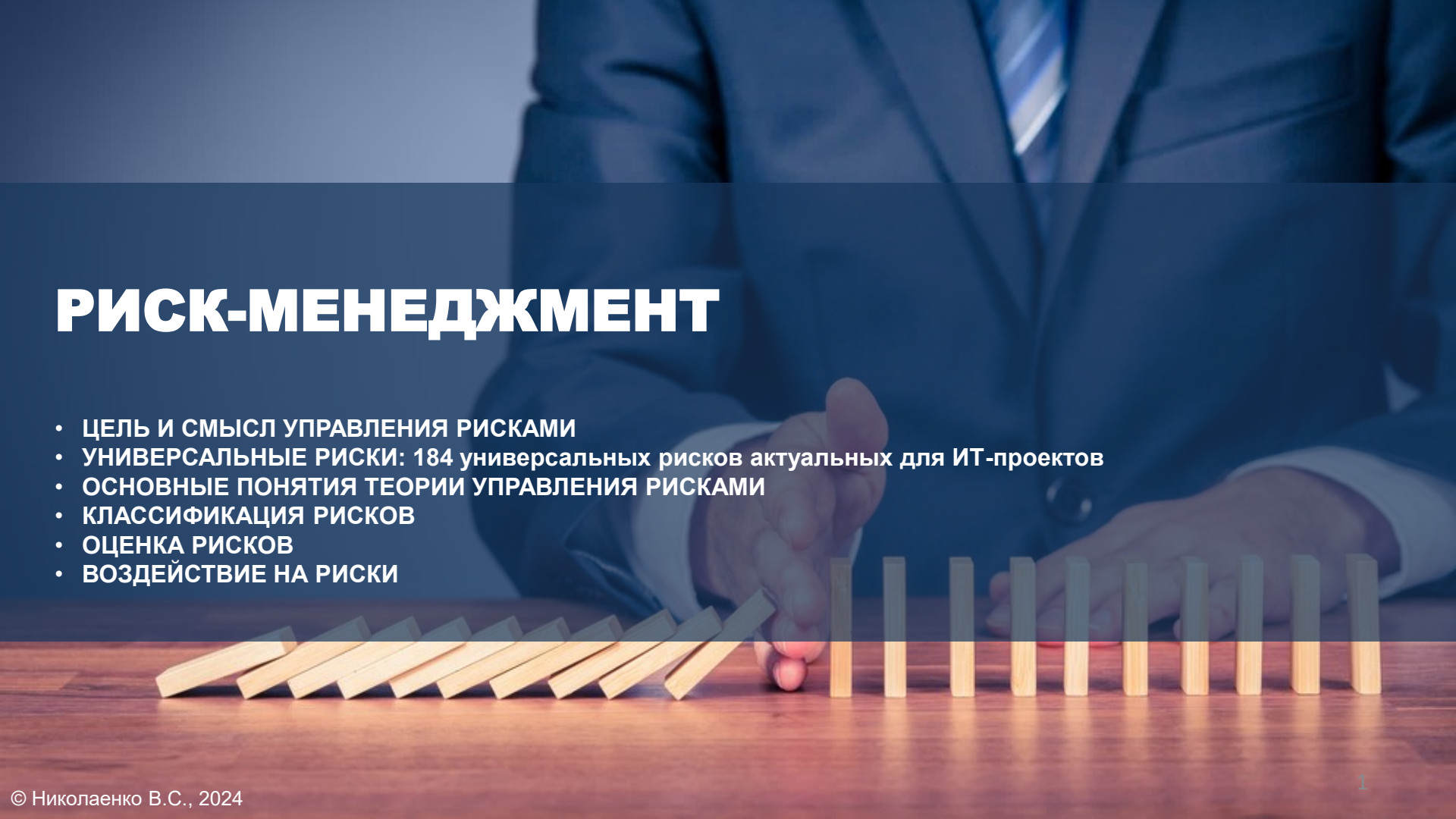
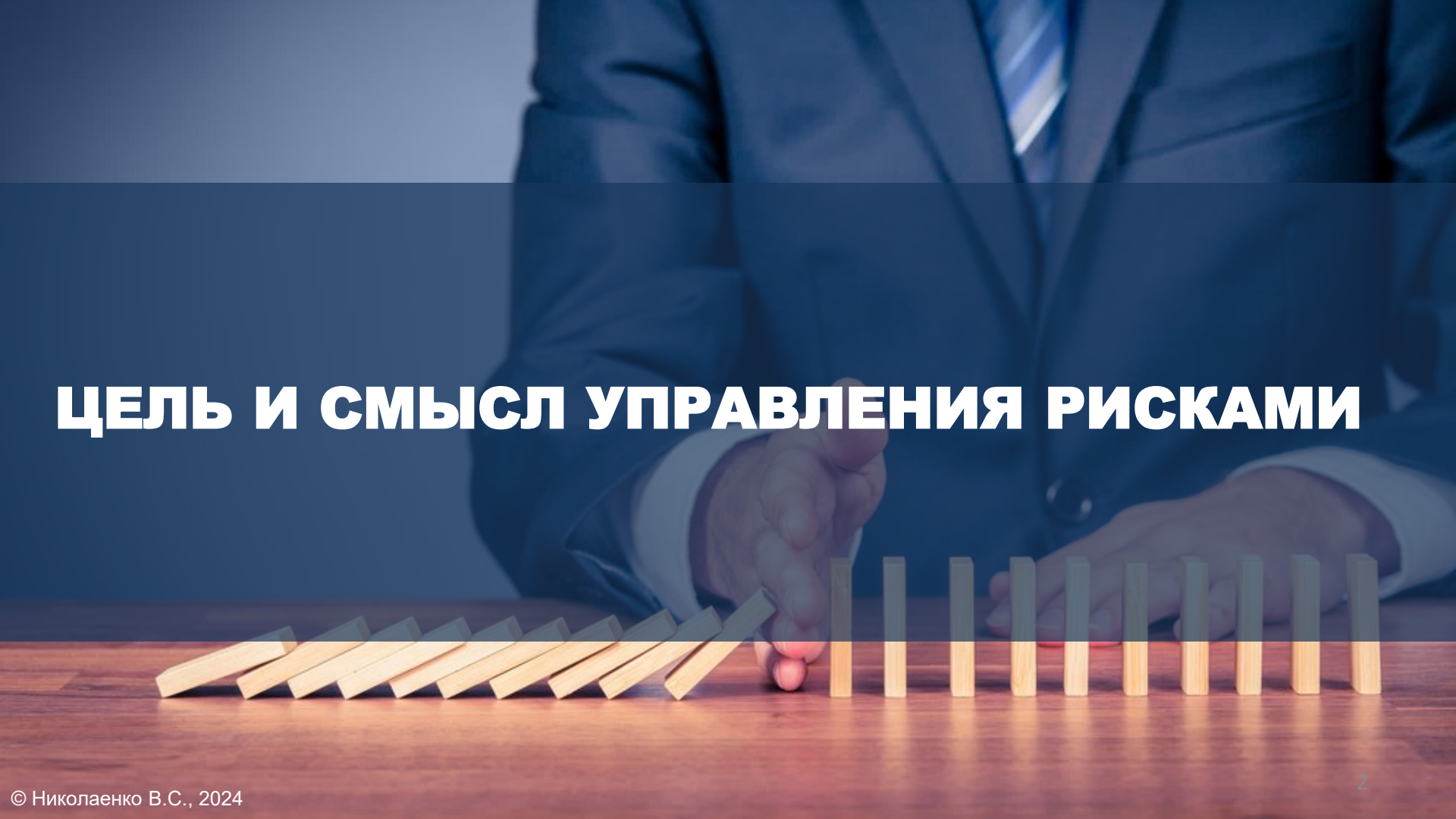


РИСК-МЕНЕДЖМЕНТ

- ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ
- УНИВЕРСАЛЬНЫЕ РИСКИ: 184 универсальных рисков актуальных для ИТ-проектов
- ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ УПРАВЛЕНИЯ РИСКАМИ
- КЛАССИФИКАЦИЯ РИСКОВ
- ОЦЕНКА РИСКОВ
- ВОЗДЕЙСТВИЕ НА РИСКИ

ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ

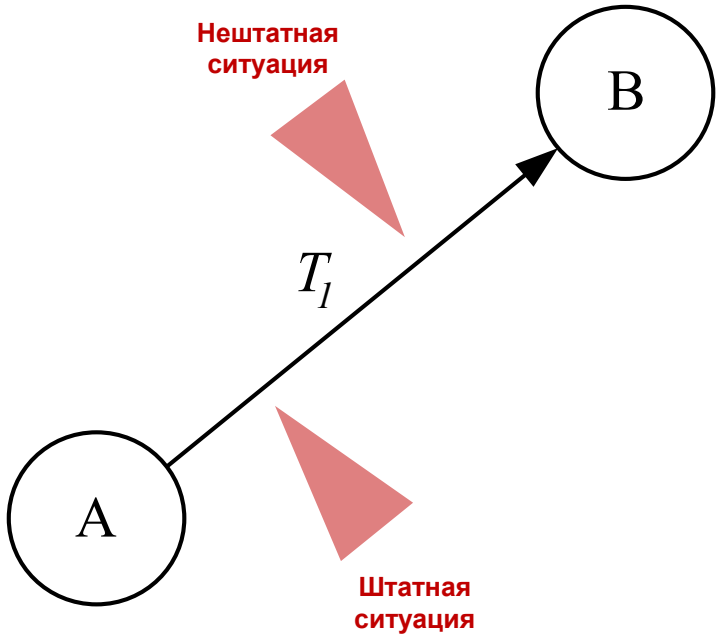


ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

Сценарий 1

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.

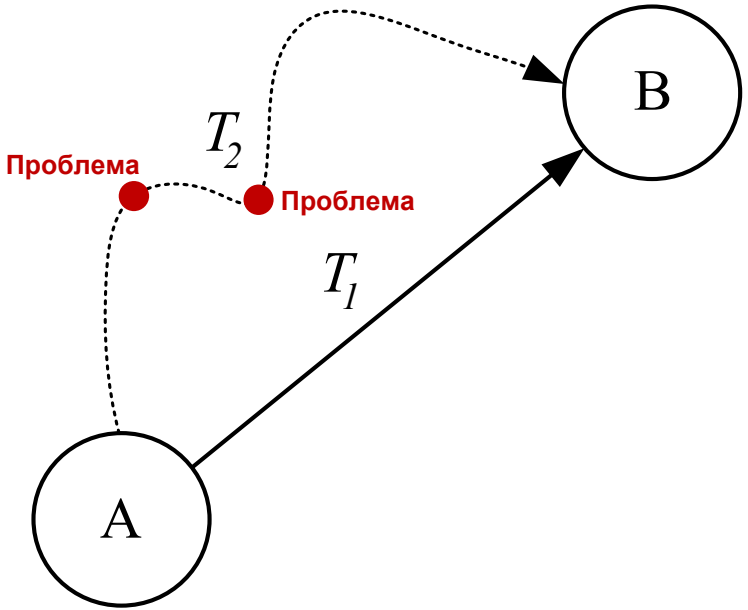
При достижении цели ничего не произойдет и субъект благополучно спустя запланированное **время Т1** достигнет ее. Этот сценарий маловероятен, потому что на процесс достижения цели будут влиять различные **штатные** и **нештатные ситуации**. Например, изменится цель, будут отсутствовать необходимые компетенции,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



ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

Сценарий 2

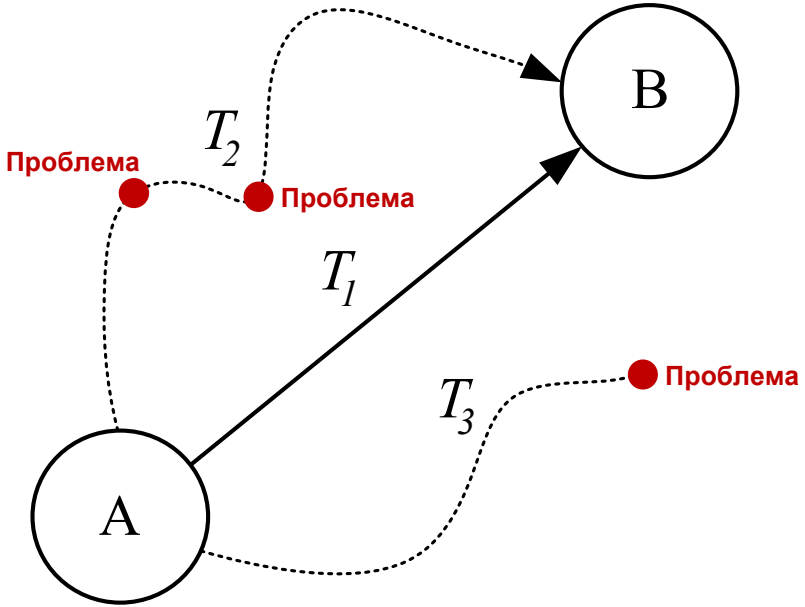
При достижении цели наступили события, которые повлияли на процесс достижения целей и на запланированное время. В результате субъект достигнет цели через **Т2**. Если наступившие события были **негативными**, то **Т2>Т1**, если **позитивными** – **Т2<Т1**. Подобный сценарий может считаться допустимым,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



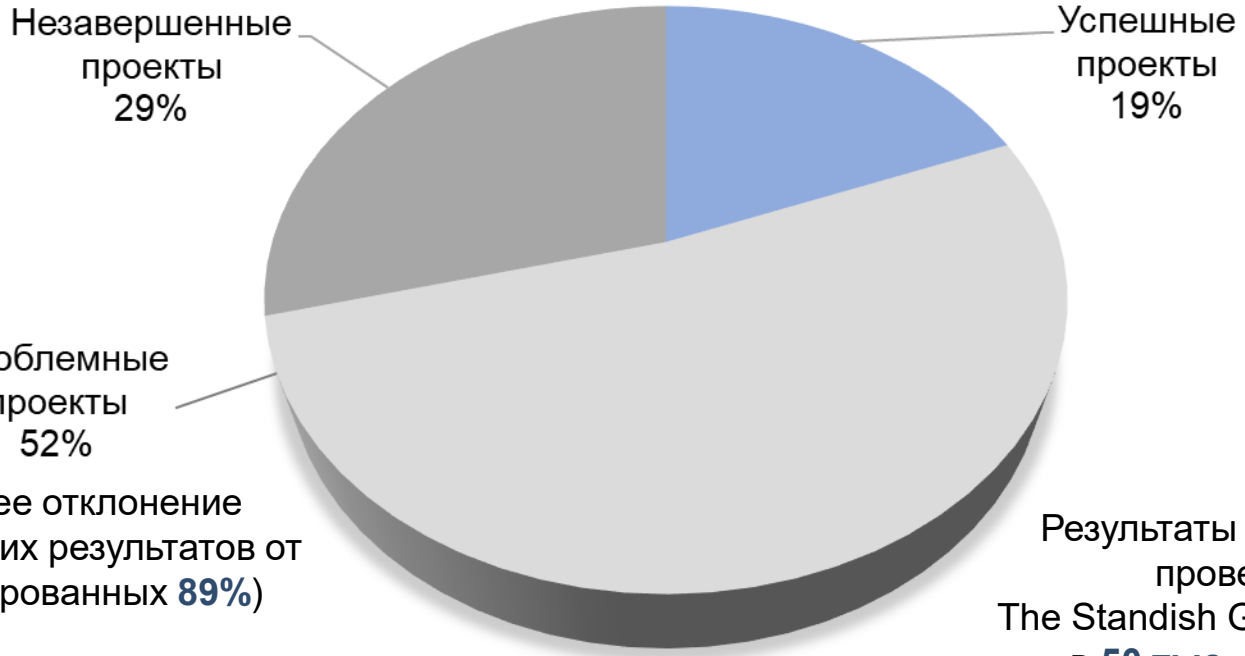
ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

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.



ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ:
Переход субъекта из состояния А в состояние В



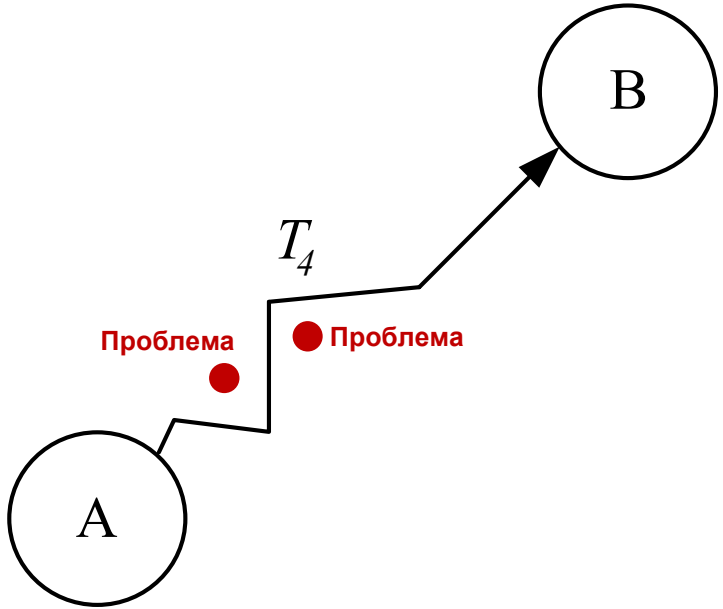
(среднее отклонение фактических результатов от запланированных **89%**)

Результаты исследований, проведенные The Standish Group International в **50 тыс. ИТ-проектах**

ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

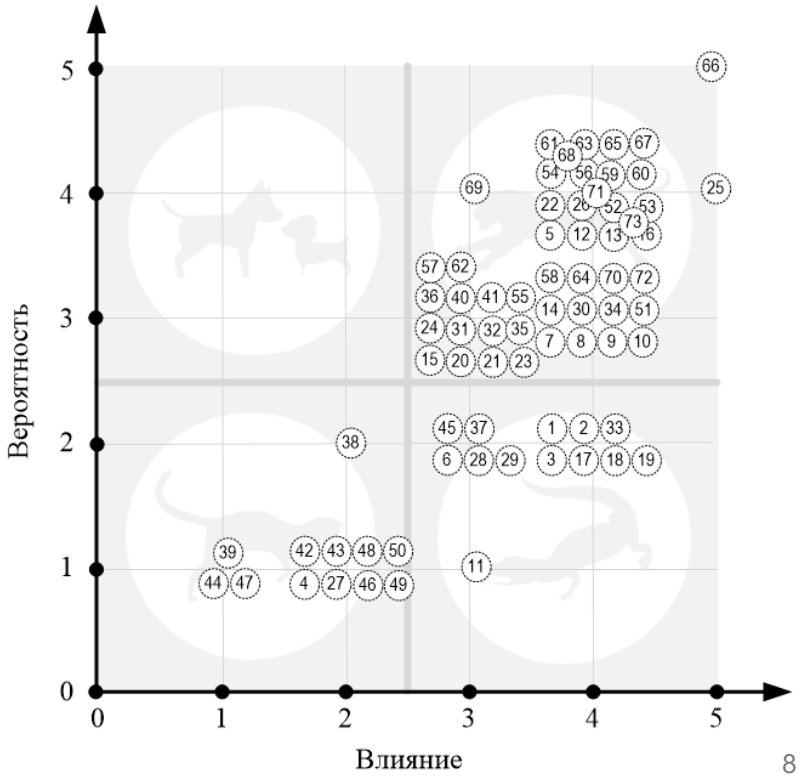
Сценарий 4

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**.



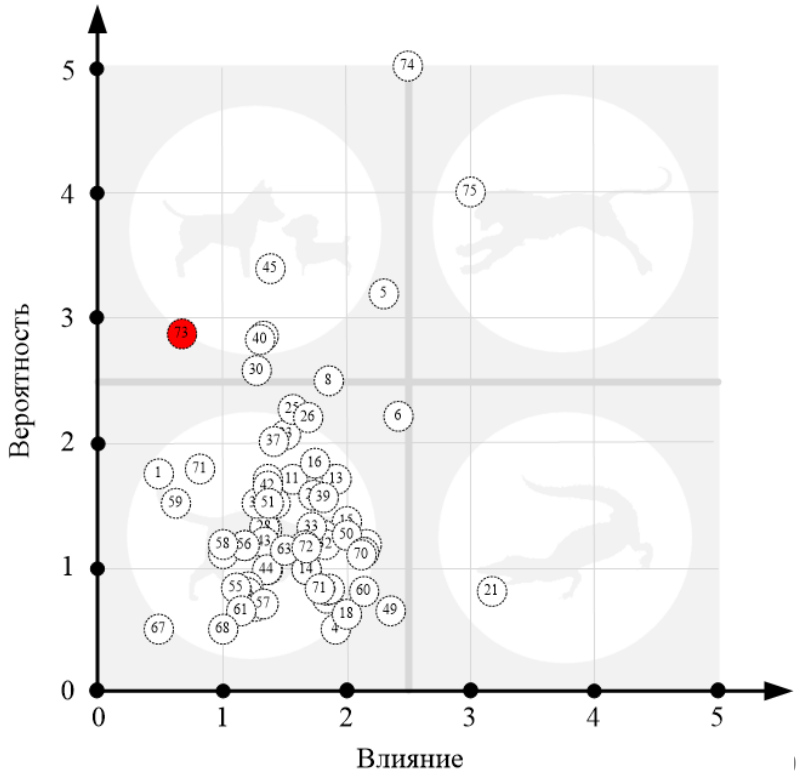
ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ:
Переход субъекта из состояния А в состояние В

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



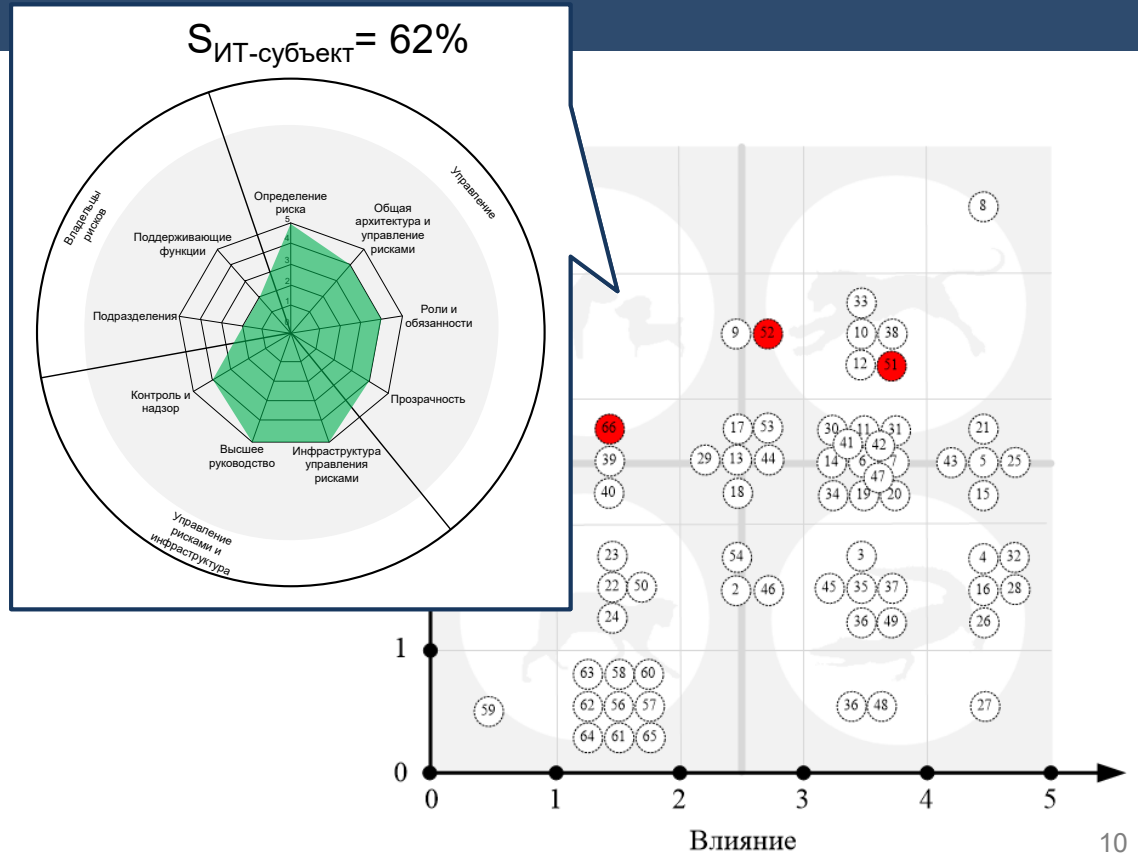
ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ:
Переход субъекта из состояния А в состояние В

ИТ-Проект: «ERM-система»
Тип проекта: ERM-система
Методика управления: Waterfall
Количество человек: 8
Размер проекта: Долгосрочный
Планируемая длительность: 416 дней
Фактическая длительность: 452 дня
Отклонение факта от плана: 8%



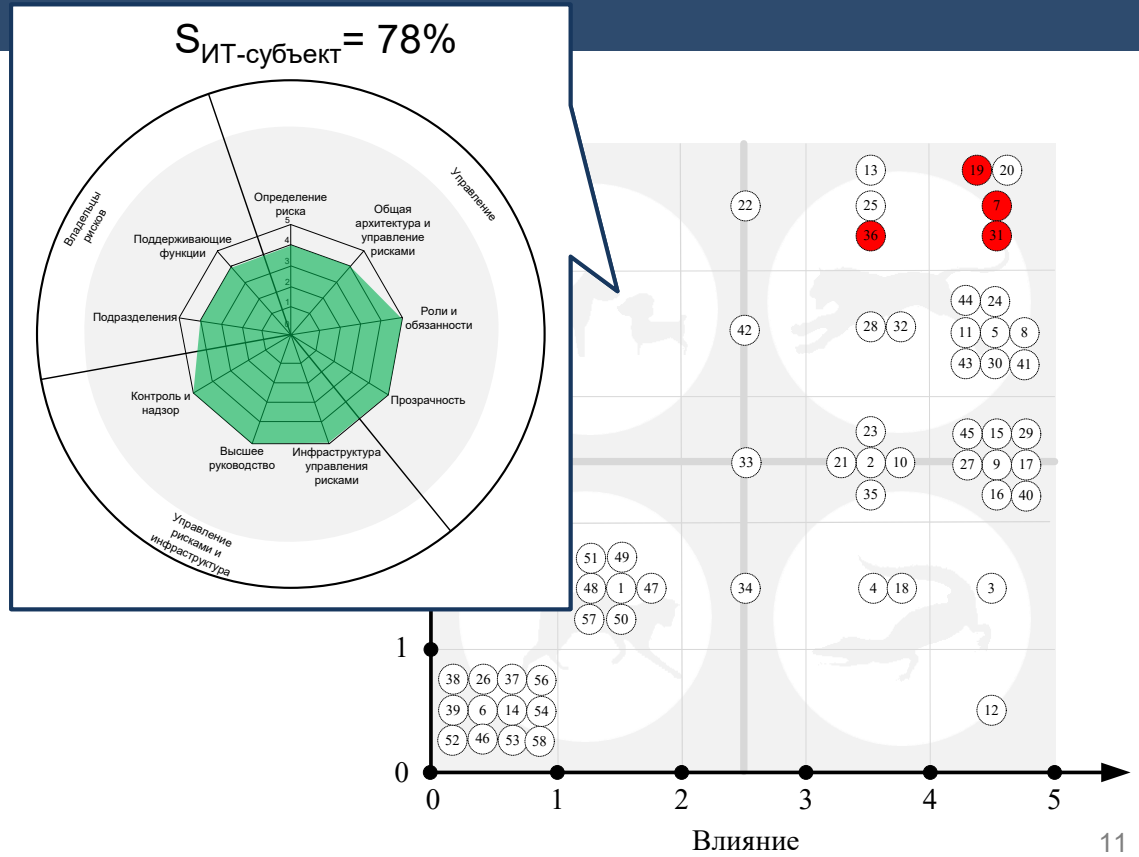
ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

ИТ-Проект: «Cinemood»
Тип проекта: Мобильное приложение
Методика управления: Waterfall
Количество человек: 7
Размер проекта: Малый
Планируемая длительность: 63 дней
Фактическая длительность: 63 дней
Отклонение факта от плана: 0%



ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

ИТ-Проект: «Hyper Vibe»
Тип проекта: ПО
Методика управления: Waterfall
Количество человек: 6
Размер проекта: Малый
Планируемая длительность: 51 день
Фактическая длительность: 53 дня
Отклонение факта от плана: 3,8%

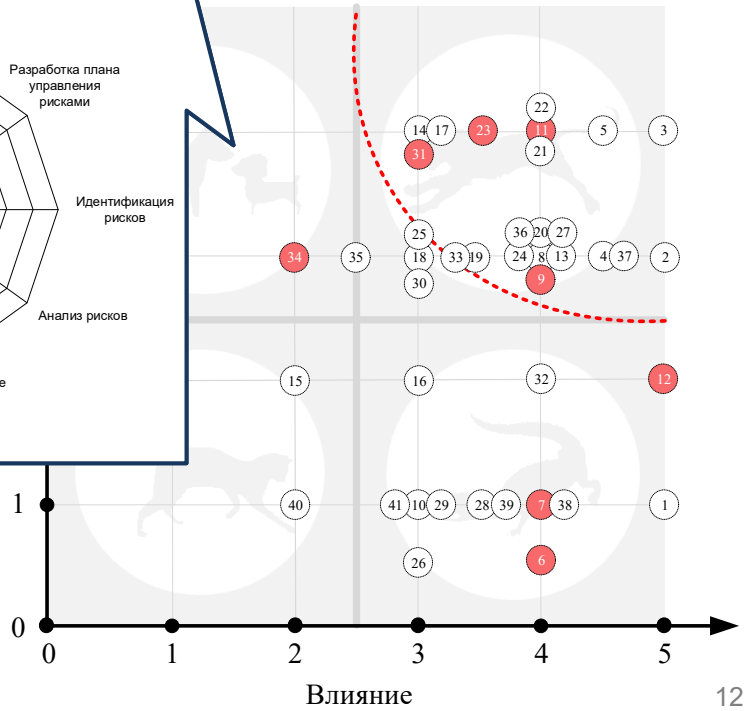


ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

ИТ-проект: Внедрение системы лояльности в 294 магазина

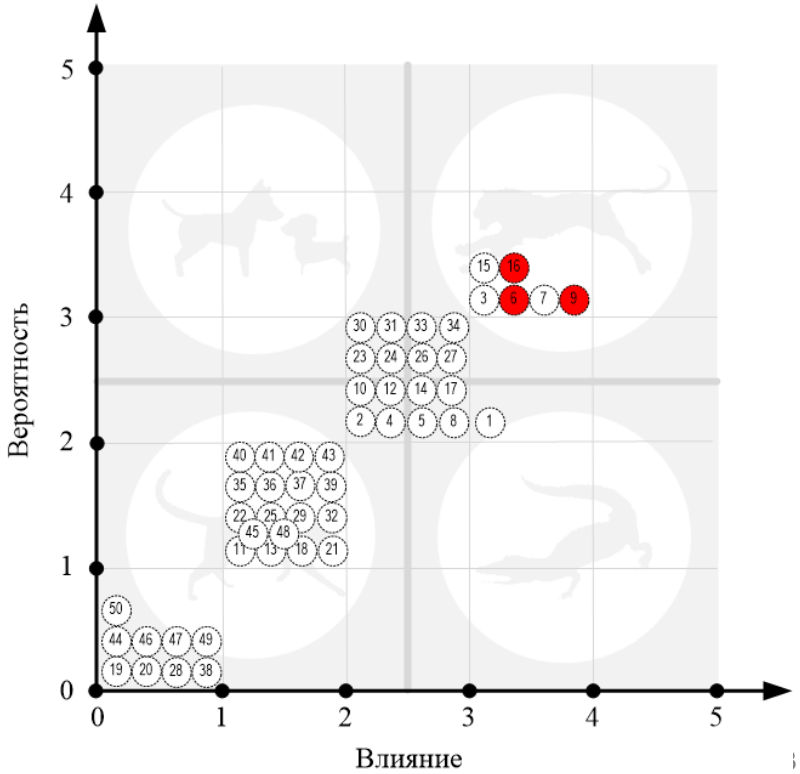
Тип проекта: ИТ-продукт
Методика управления: Waterfall
Количество человек: 3
Размер проекта: Среднесрочный
Планируемая длительность: 165 дней
Фактическая длительность: 250 дней
Отклонение факта от плана: 34%

$S_{ИТ\text{-}субъект}$=7%



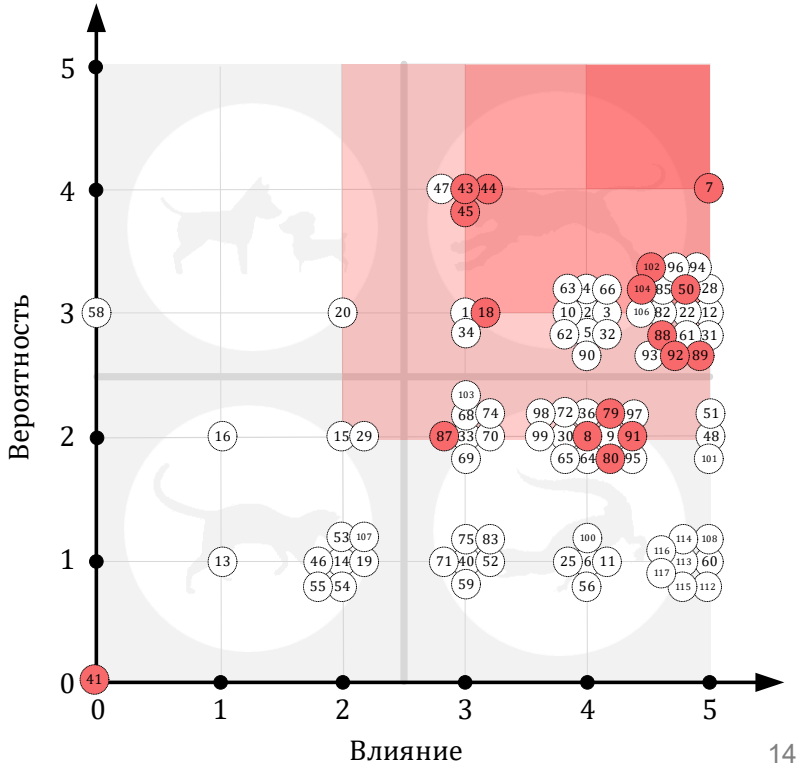
ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ:
Переход субъекта из состояния А в состояние В

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



ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

Разработать систему для эффективного распределения ресурсов внутри компании
Тип проекта: Сайт
Методика управления: Agile (Scrum)
Количество человек: 6
Размер проекта: Малый проект
Планируемая длительность: 41 рабочий день
Фактическая длительность: -
Отклонение факта от плана: -

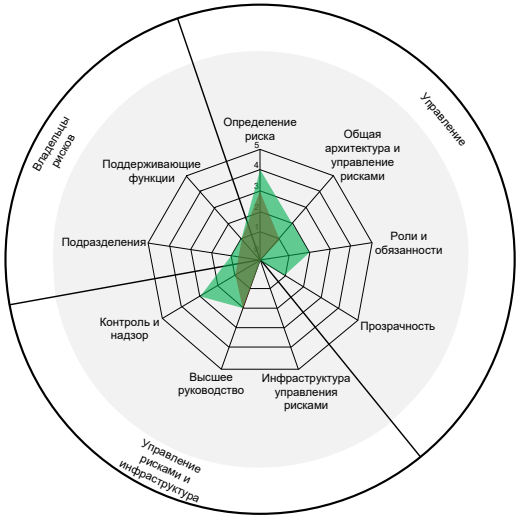


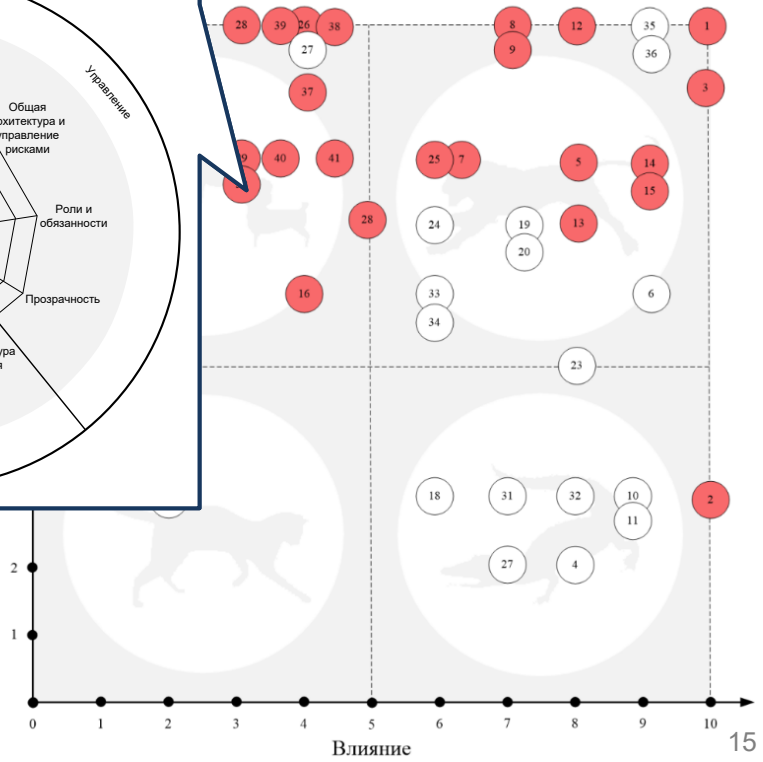
ЦЕЛЬ И СМЫСЛ УПРАВЛЕНИЯ РИСКАМИ: Переход субъекта из состояния А в состояние В

Образовательное учреждение высшего образования

Тип проекта: -
Методика управления: -
Количество человек: 234 ППС
Размер проекта: -
Планируемая длительность: -
Фактическая длительность: -
Отклонение факта от плана: -

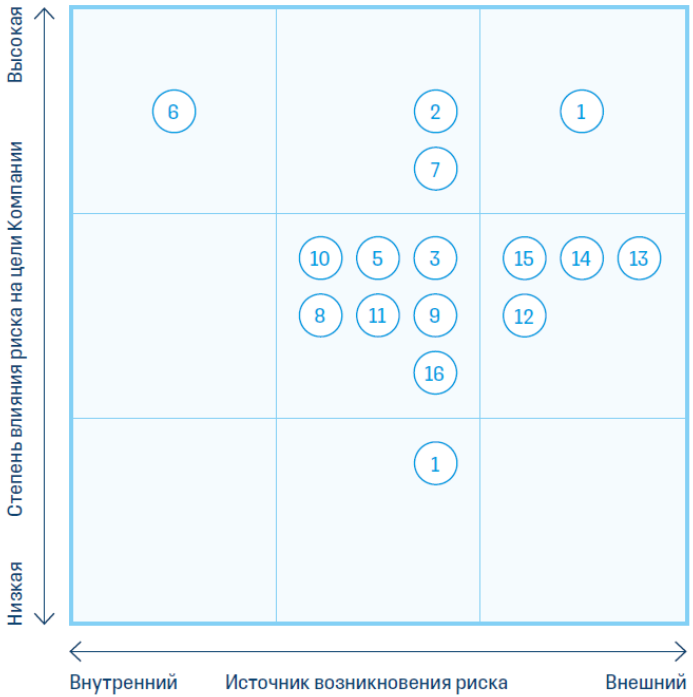
$S_{вуз}$= с 7% до 17%





Карта значимых рисков «Норникель» (2021)

КАРТА РИСКОВ



НАИМЕНОВАНИЕ РИСКОВ

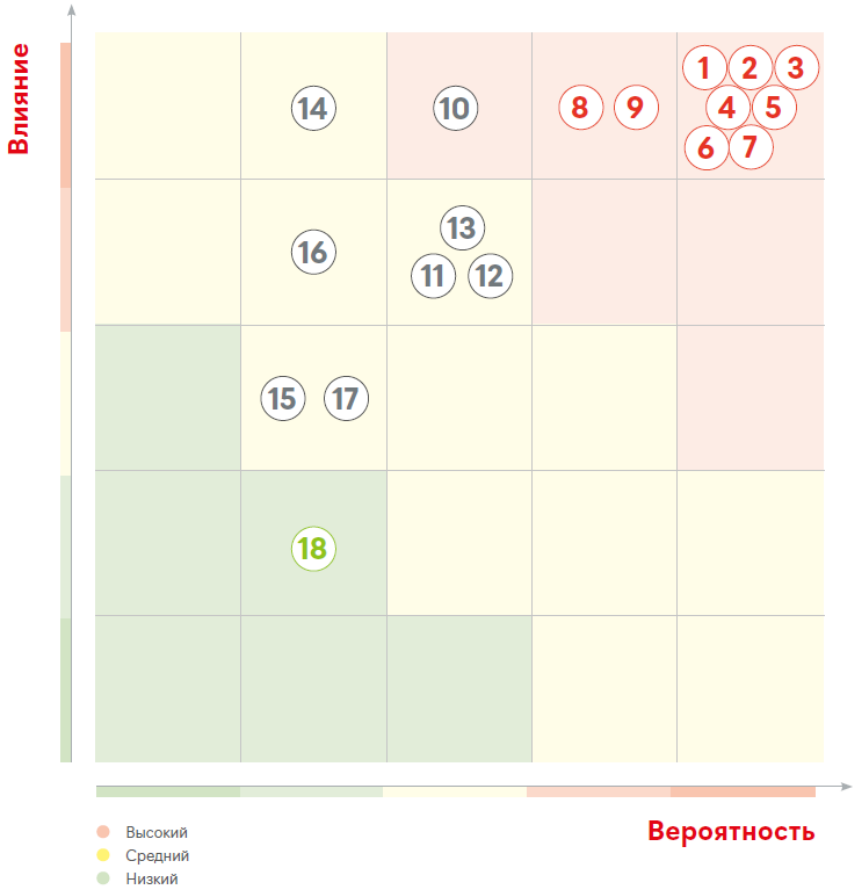
1. Ценовой риск (падение рыночных цен на производимые металлы)
2. Рыночный риск (снижение привлекательности продукции Компании на рынке)
3. Ужесточение экологических требований
4. Валютный риск
5. Инвестиционный риск
6. Производственный травматизм
7. Риски информационной безопасности
8. Технико-производственный риск
9. Перерыв в энергоснабжении производственных подразделений и социальных объектов в Норильском промышленном регионе
10. Комплаенс-риск
11. Социальный риск
12. Изменение законодательства и правоприменительной практики
13. Нехватка водных ресурсов
14. Растепление грунтов
15. Эпидемический риск
16. Риск прерывания цепочки поставок

Риск: влияние неопределенности на достижение целей (ISO / ГОСТ Р 31000).

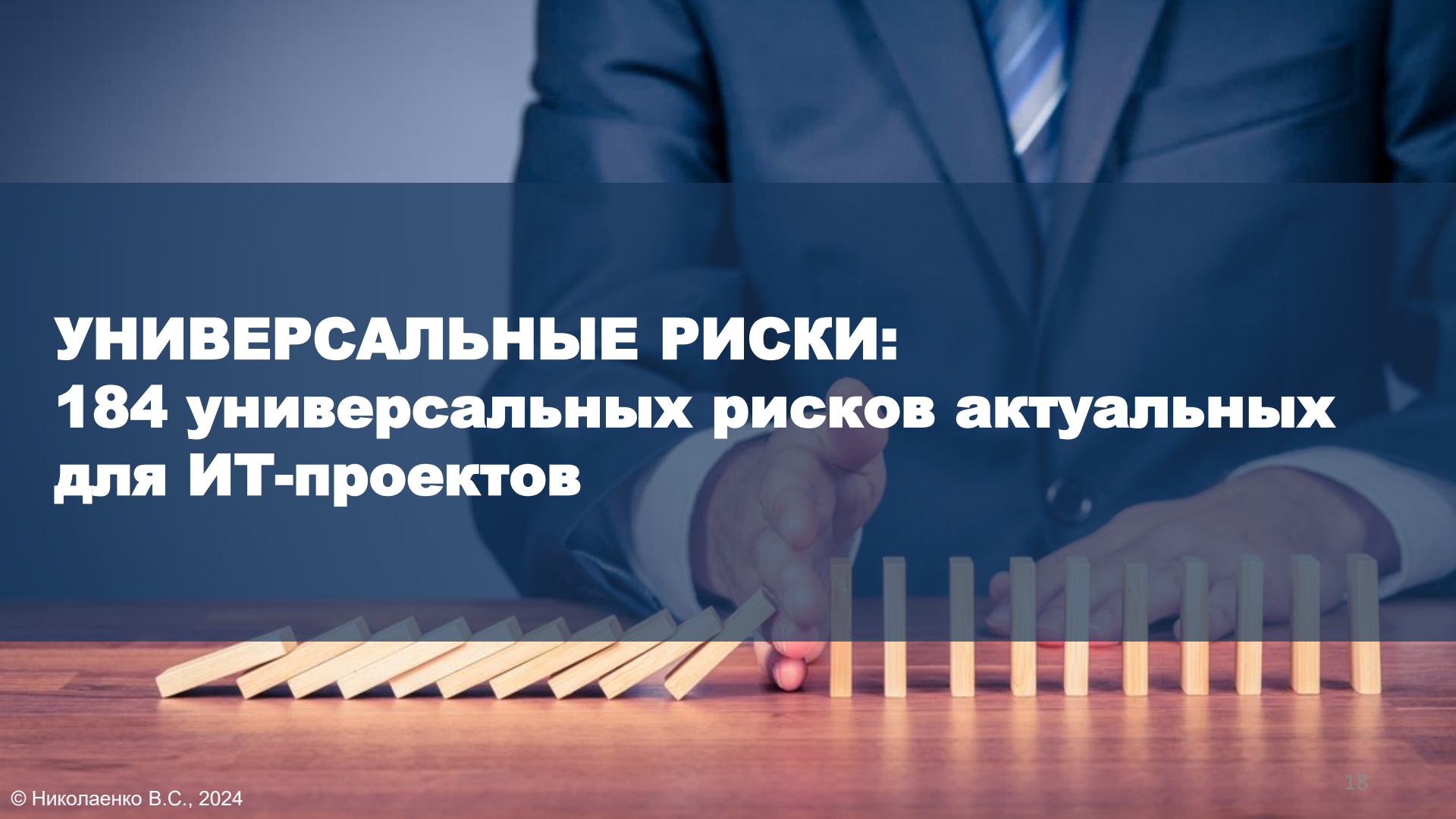
Источник риска: элемент, который отдельно или в сочетании с другими элементами может повлечь за собой риск (ISO / ГОСТ Р 31000).

- Оценка риска выросла по сравнению с прошлым годом
- Оценка риска снизилась по сравнению с прошлым годом
- Оценка риска не изменилась по сравнению с прошлым годом
- Новый риск

Карта значимых рисков «Магнит» (2021)



1. Риски ухудшения социально-экономических и политических параметров в Российской Федерации
2. Риски, связанные с дефицитом / полным отсутствием импортного товара – продуктов питания, специфического оборудования, запасных частей
3. Риск трансформации
4. Риски неблагоприятных регуляторных изменений
5. Ограничение/приостановка работы зарубежного софта/сервисов
6. Риски, связанные с ИТ-безопасностью
7. Риски, связанные с поддержкой инфраструктуры ИТ
8. Риски усиления конкуренции
9. Риски сверхнормативных потерь ТМЦ
10. Риск отсутствия и привлечения кадров
11. Риски коррупции и мошенничества сотрудников
12. Риски в области промышленной безопасности, охраны труда и окружающей среды
13. Риски принятия неэффективных инвестиционных решений
14. Риски, связанные с качеством продаваемых и производимых товаров
15. Риски влияния негативной эпидемиологической обстановки на деятельность Компании
16. Риск потери деловой репутации
17. Риски, связанные с изменением налогового законодательства
18. Климатические риски



УНИВЕРСАЛЬНЫЕ РИСКИ:
184 универсальных рисков актуальных для ИТ-проектов

УНИВЕРСАЛЬНЫЕ РИСКИ

Универсальные риски

– вероятные события, которые актуальны для **любой сделки** и **проекта** независимо от его масштаба, сложности, длительности, типа, способов управления и численности участников команды.

Анализ **192 судебных решений** и бизнес-деятельности **495 ИТ-субъектов Томской области** (ОКВЭД код 62), проведенный в рамках научно-исследовательского гранта РФФИ №16-36-00031 «мол_а».

Специальные риски

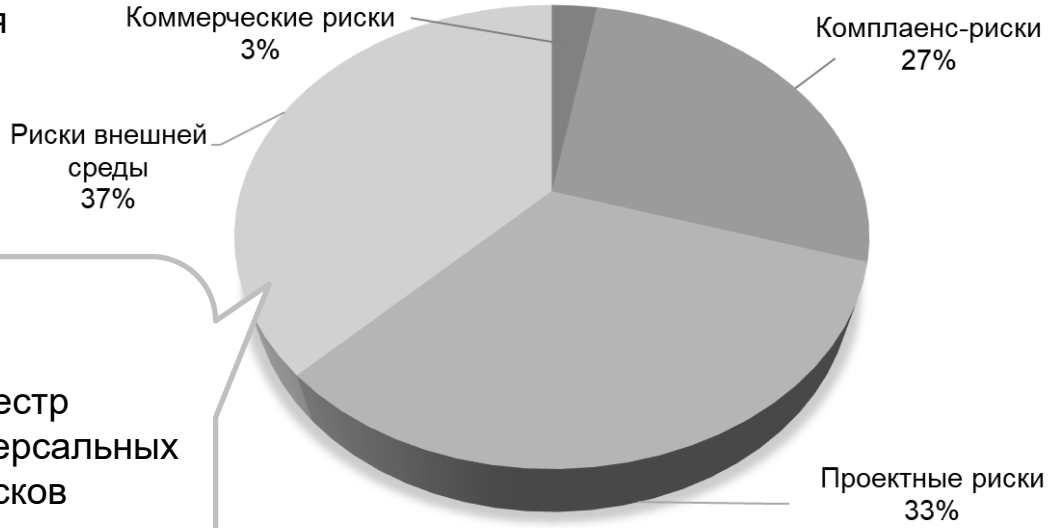
– вероятные **индивидуальные события**, которые актуальны для частной сделки или проекта.

УНИВЕРСАЛЬНЫЕ РИСКИ:
184 универсальных рисков актуальных для ИТ-проектов

Основные результаты анализа:

1. (2021): **105** универсальных рисков.
2. ИТ-проект – это гражданско-правовая сделка.

(2022) **170** универсальных рисков
(2023) **184** универсальных рисков



Реестр
184 универсальных рисков

УНИВЕРСАЛЬНЫЕ РИСКИ:
Коммерческие риски

Под **коммерческими рисками** понимаются любые потенциальные угрозы, которые могут помешать заинтересованным сторонам получить прибыль от эксплуатации созданного ИТ-продукта. Например, **присутствие на рынке нежелательных производных произведений**, **«пиратство»** и др. Несмотря на свою малочисленность от общего объема рисков (3%), материализация одного коммерческого риска способна нивелировать все затраченные ресурсы и усилия заинтересованных сторон, нанеся им катастрофический материальный ущерб.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Коммерческие риски

В качестве примера наступления коммерческого риска можно привести дело **№ А56-38522/2020**, где истец просил суд солидарно взыскать с владельцев сайта **panpartner.ru** компенсацию в размере **2 млн. руб**. В обосновании своих требований истец заявил, что программная часть сайта «поисковый модуль» является его ИТ-продуктом. Назначенные судом эксперты пришли к выводу, что общий объем кода «поискового модуля» составляет 2 669 строк, из которых 589 строк (22%) используются сайтом без изменений, а 1 522 строк (57%) изменены частично. На основании заключения экспертов суд пришел к выводу, что владельцы сайта незаконно модифицировали «поисковой модуль» создав тем самым нежелательное производное произведение.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Коммерческие риски

Другим примером материализации коммерческого риска является уголовное дело **№ 1-190/2016**, где подсудимый в целях сбыта и получения прибыли осуществлял установку «пиратских» копий программ **Компас-3D V16**, **CorelDRAW X6**, **Microsoft Windows 7** и **Microsoft Office**. Своими преступными действиями подсудимый причинил правообладателям ущерб на сумму **1,6 млн. руб**.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Коммерческие риски

Ярким примером материализации коммерческого риска является уголовной дело **№ 1-209/2022**, где виновный без соответствующего разрешения правообладателя ООО «1С-Софт» скопировал на USB-носитель файл ИТ-продукта **«1С Предприятие»** и осуществил множественное копирование. Своими преступными действиями подсудимый нарушил права правообладателя ООО «1С-Софт» и причинил ущерб на общую сумму **4,2 млн. руб.** Суд признал подсудимого виновным и назначил ему наказание в виде 2 лет условного лишения свободы с испытательным сроком на 1 год.

В качестве иных примеров, где субъекты извлекали прибыль от неправомерно использования ИТ-продуктов принадлежащих ООО «1С», можно привести дела **№ А83-6393/2023**, **№ А81-11865/2022**, **№ А50-4247/2023**, **№ А36-7440/2022**, **№ А35-7078/2022**, **№ А29-10372/2022**, **№ А50-17729/2022**, **№ А14-13243/2022** и **№ А08-16/2022**.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Комплаенс-риски

Под **комплаенс-рисками** понимаются вероятные события, связанные с нарушением норм действующего законодательства, требований национальных стандартов и кодексов поведения. Характерной особенностью комплаенс-рисков являются юридические последствия, выражающиеся в санкциях со стороны регулирующих и надзорных органов, отраслевых ассоциаций, а также лиц, чьи права и интересы были нарушены.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Комплаенс-риски

В качестве примера привлечения субъекта к административной ответственности следует привести дело **№ 5-1637/2021**, где правонарушитель незаконно использовал игровые приставки SONY «PlayStation 4 Pro» и ИТ-продукты для них в компьютерном клубе «Colizeum». Суд признал правонарушителя виновным и назначил ему наказание в виде административного штрафа в размере **15 тыс. руб. без конфискации имущества**.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Комплаенс-риски

Примером претензий со стороны лиц, чьи права и интересы были нарушены, следует привести дело **№ А40-81328/11**, где ИТ-субъект просил суд запретить использование его ИТ-продукта «HIST DoCoMo» иным лицам и возместить причиненный ущерб в размере **124,2 млн. руб**.

УНИВЕРСАЛЬНЫЕ РИСКИ: Комплаенс-риски

Одним из **наиболее часто встречаемых комплаенс-рисков является возможность отказа заказчика принимать и (или) оплачивать выполненную ИТ-субъектом работу**. Например, в деле **№ А22-1042/2020** ИТ-субъект просил суд взыскать задолженность в размере **33,6 тыс. руб**. В деле **№ А40-162480/13** истец просил взыскать убытки в размере **567 млн. руб**. В деле **№ А67-8506/2018** ИТ-субъект просил суд взыскать задолженность в размере **3,5 млн. руб**.

УНИВЕРСАЛЬНЫЕ РИСКИ: Комплаенс-риски

Анализ комплаенс-рисков позволил установить следующее:

- Причиненный ущерб от наступления **одного комплаенс-риска** в среднем составляет **277 тыс. руб.** Если во время выполнения ИТ-проекта материализуются **два комплаенс-риска**, то ущерб удваивается и составляет **544 тыс. руб.**, если наступает три комплаенс-риска – **утраивается** (**831 тыс. руб.**) и др.
- Если ИТ-субъект не имеет **механизма превентивного элиминирования универсальных рисков**, то успех выполнения ИТ-проекта зависит не от добросовестности, надежности, квалифицированности и зрелости данного лица, а от размера его **риск-аппетита**.
- Наиболее опасными комплаенс-рисками являются **риски, связанные с правами на результаты интеллектуальной деятельности**.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Проектные риски

Проектными рисками называют риски, наступление которых оказывает влияние на одну цель проекта либо на их совокупность. Данные риски, как правило, материализуются во время **фазы жизненного цикла ИТ-проекта «создание ИТ-продукта»** из-за действий (бездействий) руководителя проекта, системного аналитика, юриста, субподрядчика и других участников проекта.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Связь между проектными и комплаенс-рисками

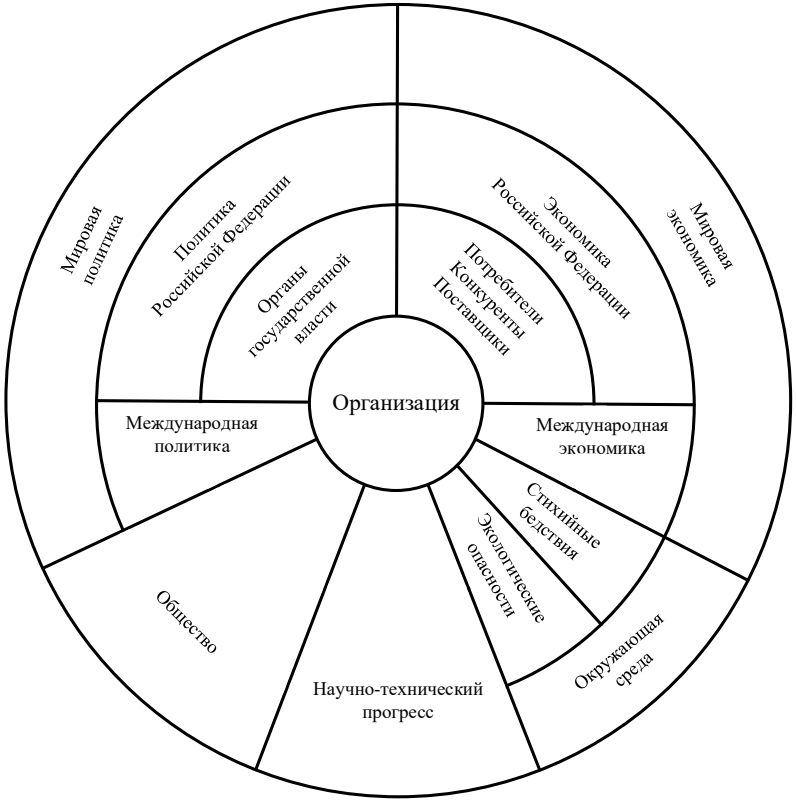
Наступление проектных рисков оказывает влияние на цели ИТ-проекта (содержание, длительность, стоимость, качество), где **наиболее опасными рисками** являются:

- риск отсутствия знаний, навыков и опыта у руководителя проекта;
- риск того, что руководитель проекта допустит ошибку при оценивании длительности проектных работ;
- риск нерационального расходования ограниченных ресурсов проекта;
- риск занятости руководителя проекта в других проектах;
- риск изменения качества проекта;
- **риск изменения длительности проекта**; и
- **риск изменения стоимости проекта**.

Наступление данных проектных рисков значительно повышает **вероятность изменения существенных условий контракта** и **провоцирует наступление комплаенс-рисков**.

УНИВЕРСАЛЬНЫЕ РИСКИ:
Риски внешней среды

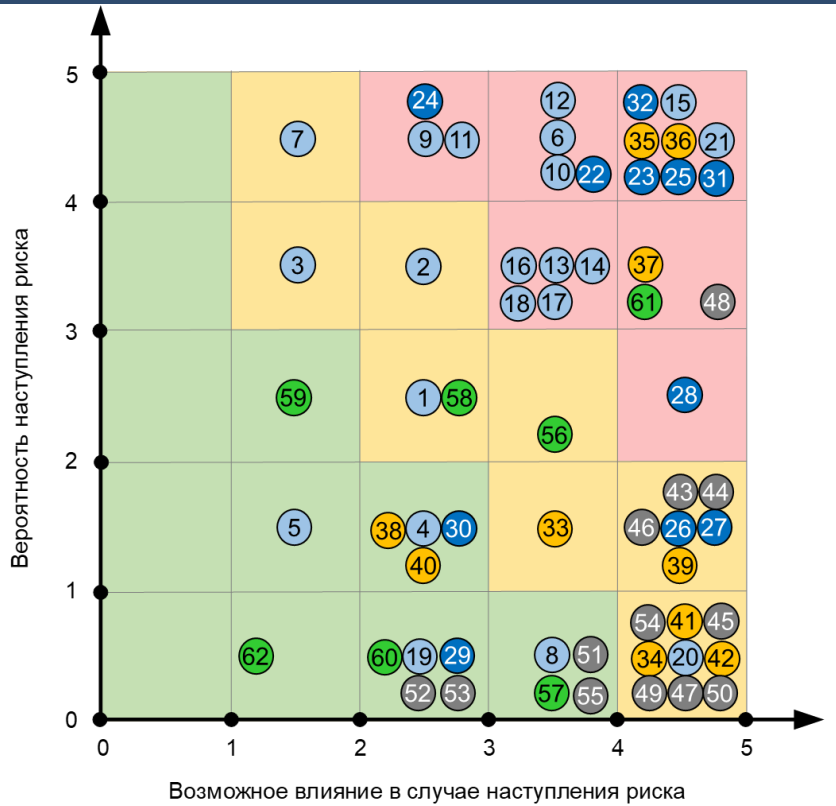
Если источники рисков находятся внутри организации, то эти риски называют **внутренними рисками**, если источники рисков находятся за пределами организации – **внешними рисками**.



УНИВЕРСАЛЬНЫЕ РИСКИ:
Риски внешней среды (2024 г.)

ЭКОНОМИКА

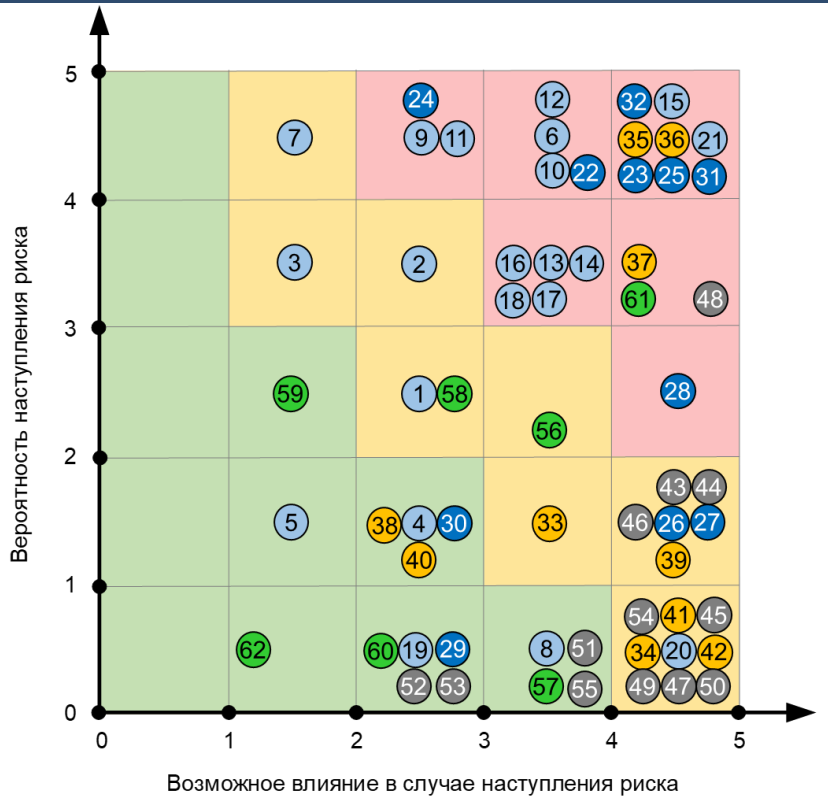
1. Риск изменения цен на нефть
2. Риск изменения цен на газ
3. Риск изменения цен на металл
4. Риск изменения цен на уголь
5. Риск изменения цен на зерно
6. Риск дефицита (профицита) федерального бюджета
7. Риск изменения курса валют
8. Риск внесения изменений в Федеральный закон «О федеральном бюджете»
9. Риск изменения налоговой политики
10. Риск изменения размера государственного долга
11. Риск изменения денежно-кредитной политики
12. Риск эмиссии денежной массы
13. Риск изменения ключевой ставки
14. Риск изменения процентов кредитных и депозитных ставок
15. Риск изменения темпов инфляции
16. Риск изменения темпов роста экономики
17. Риск изменения уровня жизни населения
18. Риск изменения фондовых индексов
19. Риск запрета торговли ценными бумагами определенных организаций
20. Риск дефолта
21. Риск экономического кризиса



УНИВЕРСАЛЬНЫЕ РИСКИ:
Риски внешней среды (2024 г.)

ОБЩЕСТВО

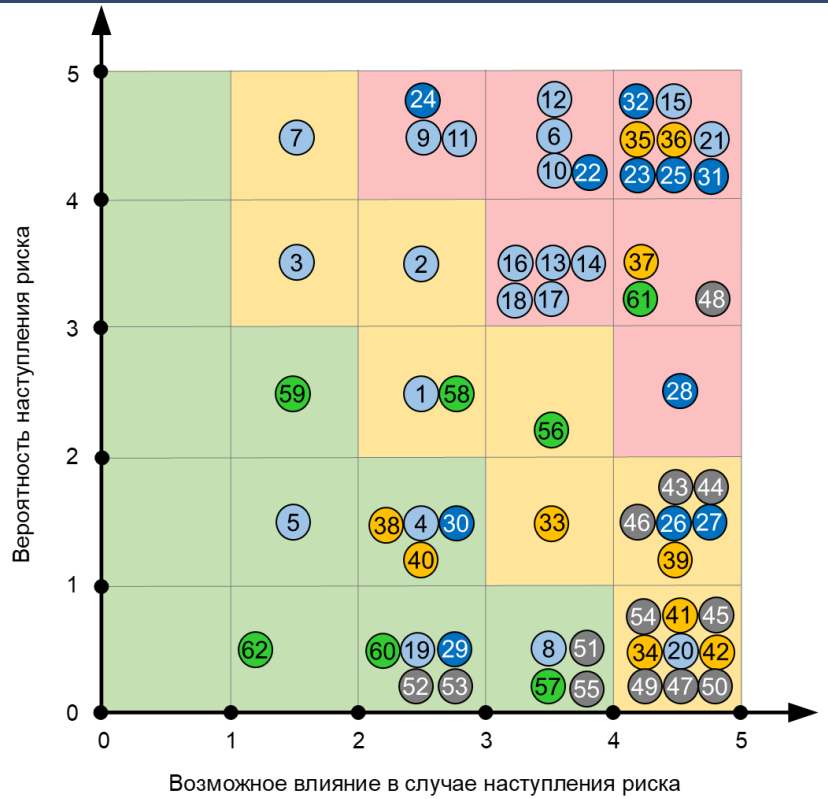
- 22. Риск изменения уровня смертности
- 23. Риск изменения уровня рождаемости
- 24. Риск того, что на рынке труда будут отсутствовать квалифицированные кадры
- 25. Риск социальной напряженности
- 26. Риск изменения уровня образования
- 27. Риск изменения уровня медицины
- 28. Риск изменения уровня преступности
- 29. Риск изменения уровня миграции
- 30. Риск голода
- 31. Риск изменения численности
- 32. Риск изменения духовно-нравственной (культурной) сферы



УНИВЕРСАЛЬНЫЕ РИСКИ:
Риски внешней среды (2024 г.)

ПОЛИТИКА

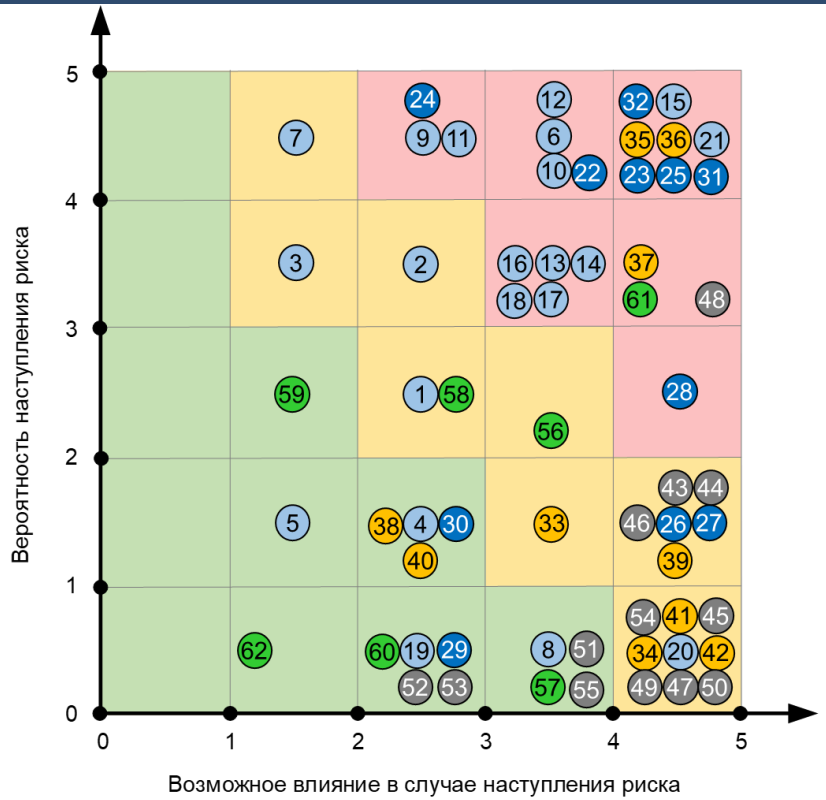
33. Риск изменения геополитического давления
34. Риск расширения альянса НАТО
35. Риск военного конфликта
36. Риск террористического акта
37. Риск изменения норм действующего законодательства
38. Риск интеграции РФ с внешними субъектами
39. Риск государственного переворота
40. Риск национализации и экспроприации имущества
41. Риск массовых беспорядков
42. Риск импичмента президента



УНИВЕРСАЛЬНЫЕ РИСКИ:
Риски внешней среды (2024 г.)

ОКРУЖАЮЩАЯ СРЕДА

43. Риск нехватки природных ресурсов
44. Риск изменения климата
45. Риск загрязнения окружающей среды
46. Риск пандемии
47. Риск наводнения
48. Риск радиоактивного заражения
49. Риск тайфуна
50. Риск землетрясения
51. Риск падения космического тела
52. Риск извержения вулкана
53. Риск пожара
54. Риск уничтожения Земли
55. Риск таяния ледников

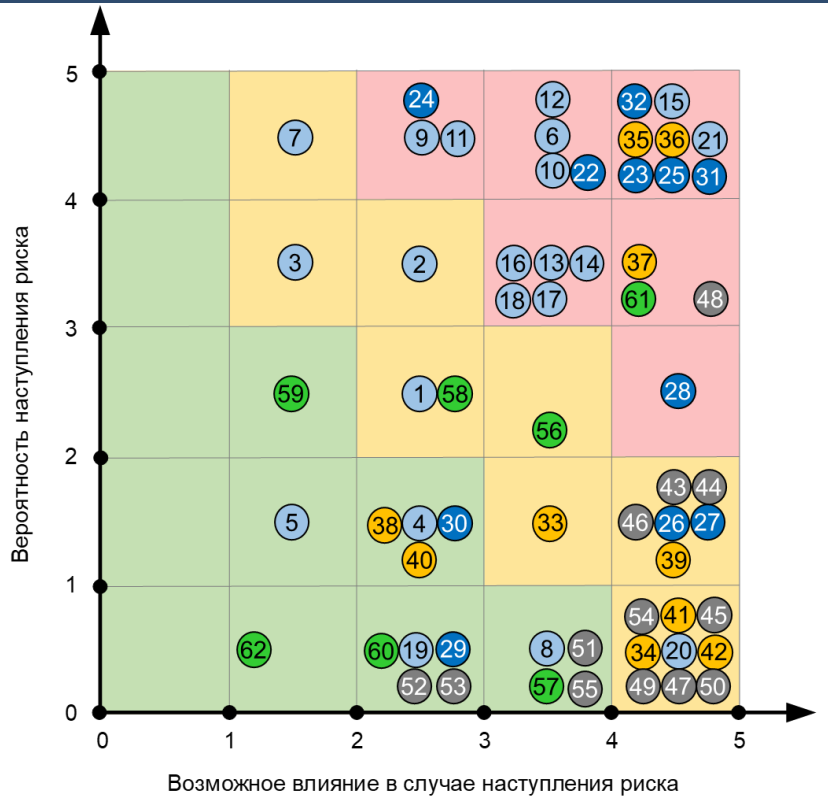


УНИВЕРСАЛЬНЫЕ РИСКИ:
Риски внешней среды (2024 г.)

ТЕХНИКА И ТЕХНОЛОГИИ

- 56. Риск атаки искусственного интеллекта (ИИ)
- 57. Риск отключения Интернета
- 58. Риск кибератак на критическую информационную инфраструктуру (КИИ)
- 59. Риск атаки на критическую инфраструктуру
- 60. Риск использования новых технологий
- 61. Риск поломки оборудования
- 62. Риск нехватки электроэнергии

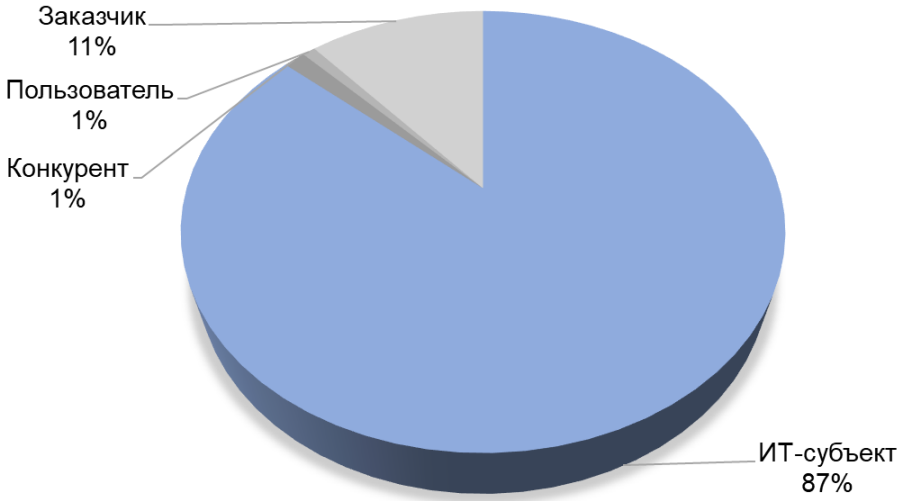
- Наступивший риск
- Оценка риска не изменилась по сравнению с прошлым годом
- Новый риск
- Оценка риска выросла по сравнению с прошлым годом
- Оценка риска снизилась по сравнению с прошлым годом



УНИВЕРСАЛЬНЫЕ РИСКИ:
Источники универсальных рисков

Согласно действующему законодательству (см. гл. гл. 37, 39 ГК РФ) **после подписания контракта ответственность за наступление всех последующих рисков несет ИТ-субъект**. Однако, как показали результаты анализа ИТ-субъект является источником универсальных рисков только на 87%. Порядка 11% рисков наступают по вине заказчика, 1% конкурента(-ов) и 1% пользователя(-ей), эксплуатирующих созданные ИТ-продукты.

Это означает, что **ИТ-субъект должен заблаговременно, до заключения контракта, поводить экспресс-оценку универсальных рисков и превентивно воздействовать на них, в том числе за счет формализации в тексте контракта действий и (или) бездействий (ковенантов), которые должны выполнить заинтересованные стороны для элиминирования наиболее опасных рисков либо их «достойного» принятия**. Если сформулированное выше условие не будет выполняться, то **при материализации рисков весь материальный и репутационный урон будет компенсировать сторона ИТ-субъекта**.



УНИВЕРСАЛЬНЫЕ РИСКИ: Профстандарт: 06.016 «Руководитель проектов в области ИТ»

Уровень квалификации – 6 (бакалавриат). **Трудовые функции:**

- **A/29.6.** Идентификация рисков проектов в области ИТ в соответствии с трудовым заданием
- **A/30.6.** Разработка плана управления рисками и мониторинг рисков в проектах в области ИТ в соответствии с трудовым заданием
- **A/06.6**. Организация заключения договоров в проектах в области ИТ в соответствии с трудовым заданием
- **A/07.6**. Мониторинг выполнения договоров в проектах в области ИТ в соответствии с полученным планом проекта

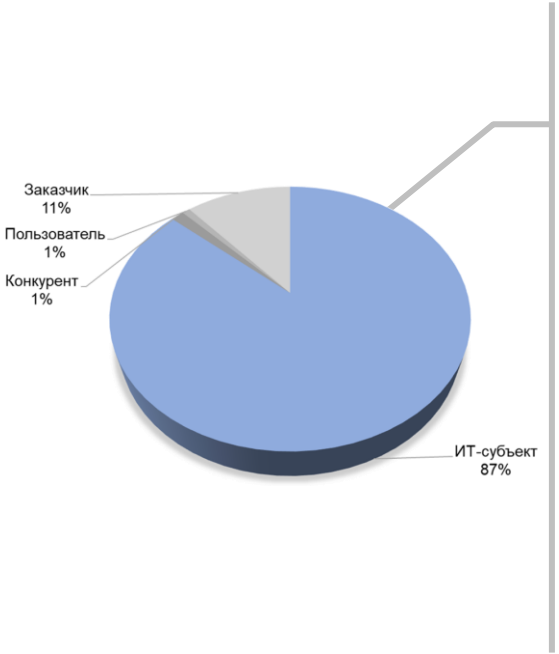
Уровень квалификации – 7 (магистратура или специалитет). **Трудовые функции:**

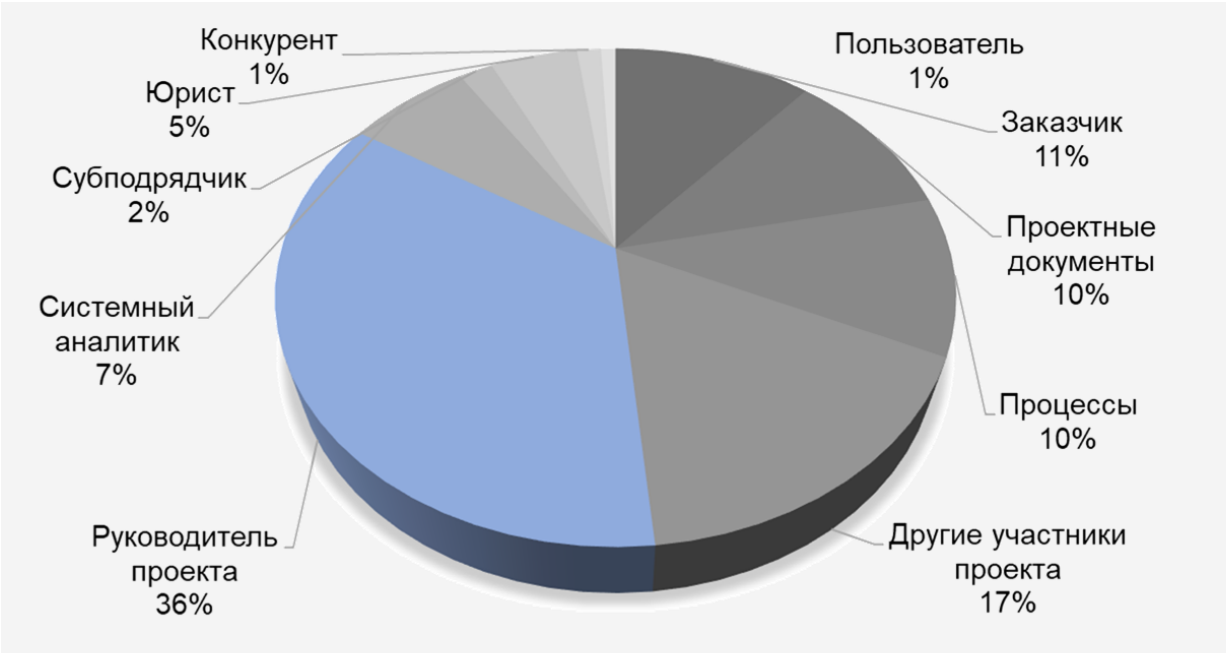
- **B/59.7.** Планирование управления рисками в проектах малого и среднего уровня сложности в области ИТ
- **B/60.7.** Идентификация рисков в проектах малого и среднего уровня сложности в области ИТ
- **B/61.7.** Планирование работы с рисками в проектах малого и среднего уровня сложности в области ИТ
- **B/62.7.** Мониторинг рисков и управление рисками в проектах малого и среднего уровня сложности в области ИТ
- **B/12.7.** Организация заключения договоров в проектах малого и среднего уровня сложности в области ИТ
- **B/13.7.** Мониторинг договоров и управление договорами в проектах малого и среднего уровня сложности в области ИТ
- **B/14.7.** Организация заключения дополнительных соглашений к договорам в проектах малого и среднего уровня сложности в области ИТ
- **B/15.7.** Закрытие договоров в проектах малого и среднего уровня сложности в области ИТ

Уровень квалификации – 8 (аспирантура). **Трудовые функции:**

- **C/59.8**. Планирование управления рисками в проектах любого уровня сложности в области ИТ
- **C/60.8**. Идентификация рисков в проектах любого уровня сложности в области ИТ
- **C/61.8**. Планирование работы с рисками в проектах любого уровня сложности в области ИТ
- **C/62.8**. Мониторинг рисков и управление рисками в проектах любого уровня сложности в области ИТ
- **C/11.8**. Планирование управления договорами в проектах любого уровня сложности в области ИТ
- **C/12.8**. Организация заключения договоров в проектах любого уровня сложности в области ИТ
- **C/13.8**. Мониторинг договоров и управление договорами в проектах любого уровня сложности в области ИТ
- **C/14.8**. Организация заключения дополнительных соглашений к договорам в проектах любого уровня сложности в области ИТ
- **C/15.8**. Закрытие договоров в проектах любого уровня сложности в области ИТ

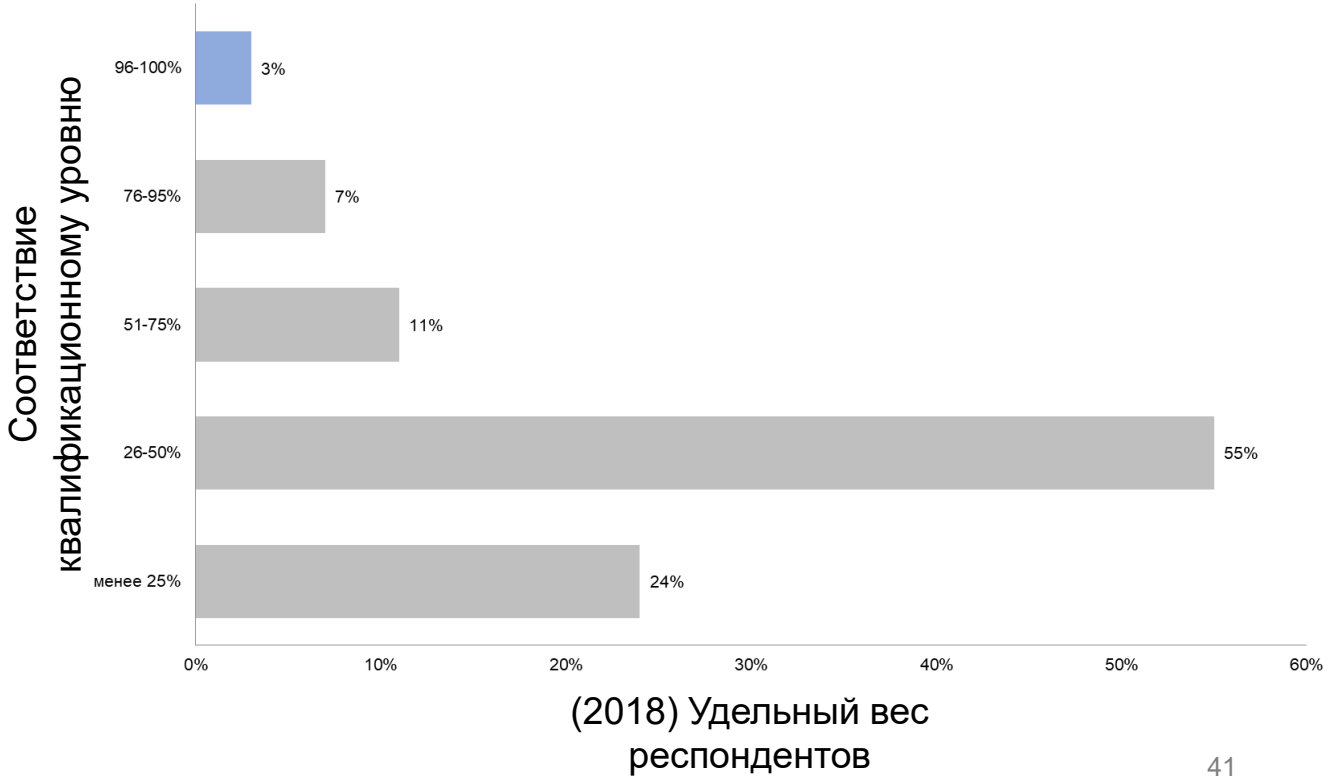
УНИВЕРСАЛЬНЫЕ РИСКИ:
Источники универсальных рисков



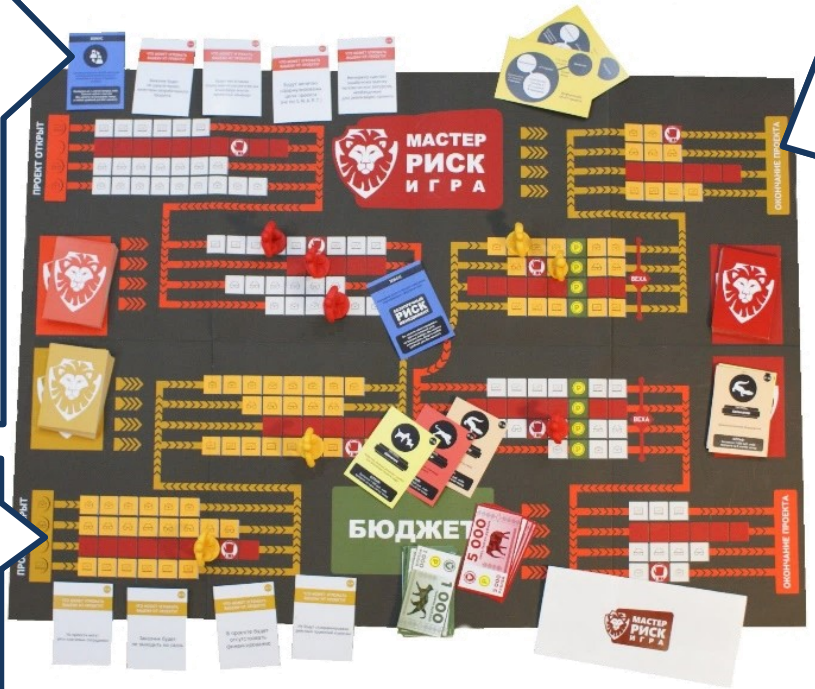


УНИВЕРСАЛЬНЫЕ РИСКИ

Былков В. Г. Методические и организационные проблемы внедрения профессиональных стандартов // Азимут научных исследований: экономика и управление, 2019. – Т. 8. – № 2 (27). – С. 83-87.



НАСТОЛЬНЫЙ ТРЕНАЖЕР МАСТЕР РИСК©



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПРОМЫШЛЕННЫЙ ОБРАЗЕЦ

№ 121649

ИГРОВОЕ ПОЛЕ НАСТОЛЬНОГО ТРЕНАЖЕРА ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ

Патентообладатель(ли): *Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский Томский политехнический университет" (RU)*

Автор(ы): *Николаенко Валентин Сергеевич (RU)*

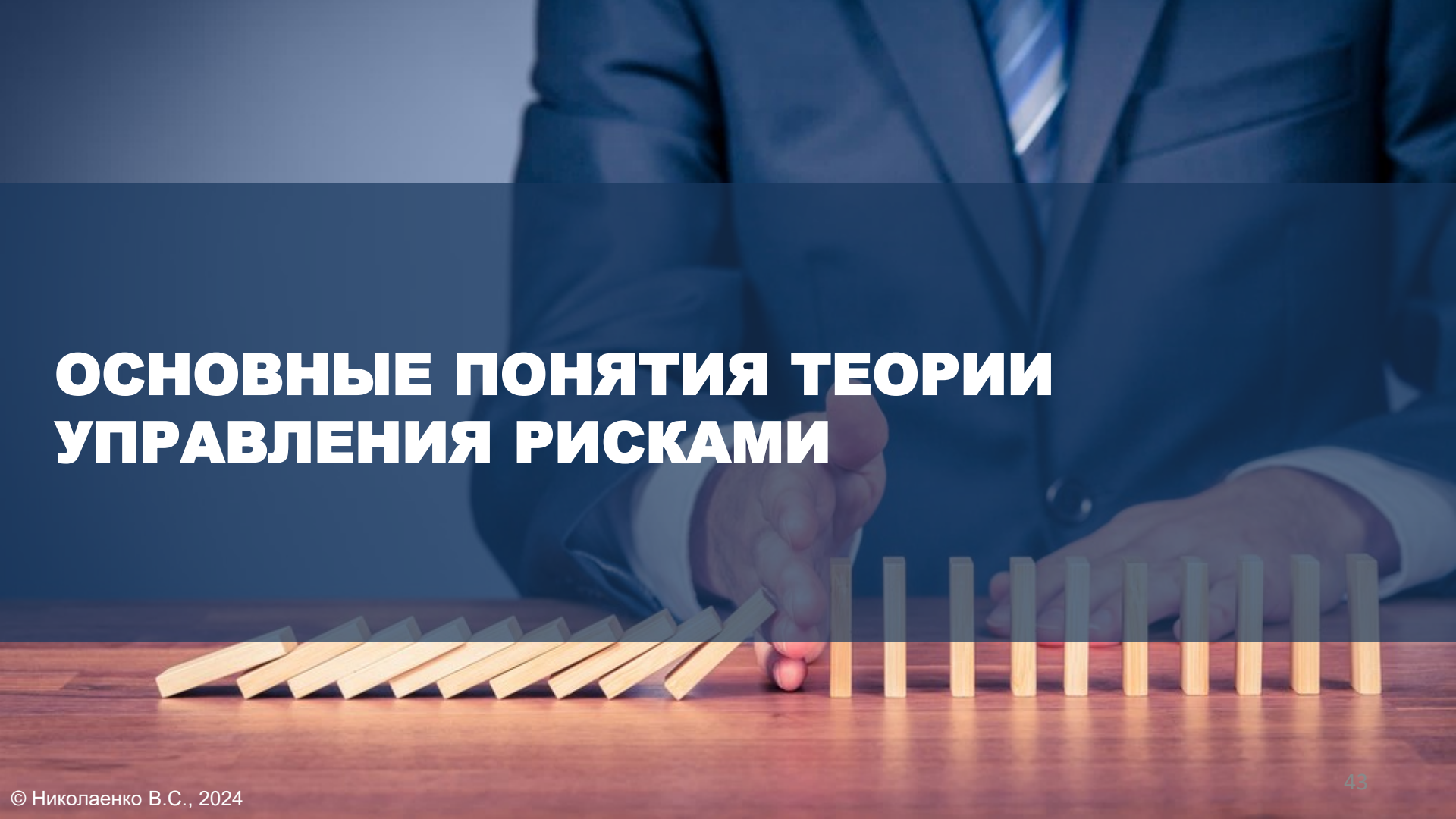
Заявка № 2020500922
Приоритет(ы) промышленного образца 02 марта 2020 г.
Дата государственной регистрации в Государственном реестре промышленных образцов Российской Федерации 18 сентября 2020 г.
Срок действия исключительного права на промышленный образец истекает 02 марта 2025 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Лучшая практика преподавания по итогам II Всероссийского конкурса молодых преподавателей вузов

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ УПРАВЛЕНИЯ РИСКАМИ

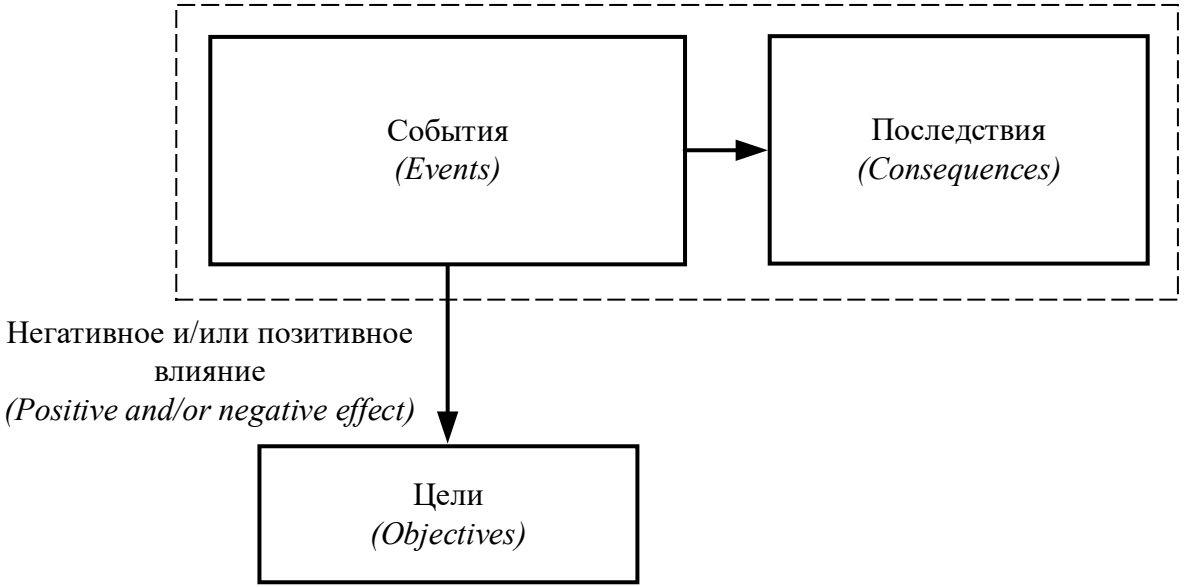


ПОНЯТИЕ «РИСК»

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.

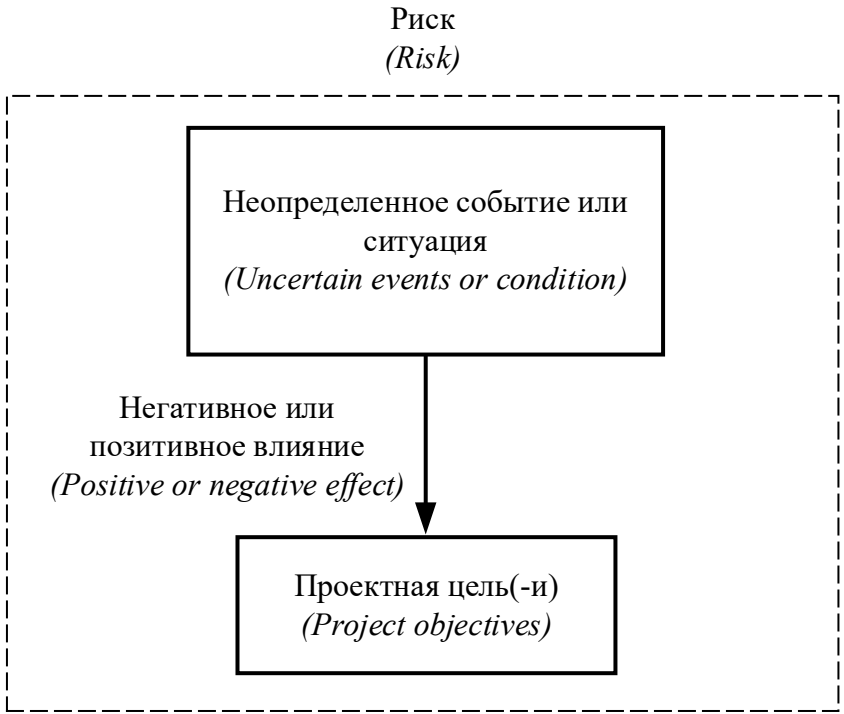
ПОНЯТИЕ «РИСК»

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.



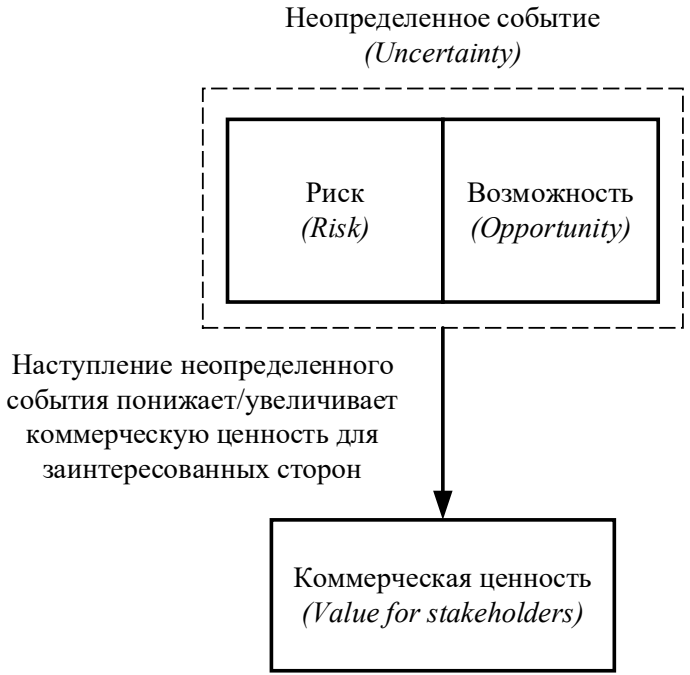
ПОНЯТИЕ «РИСК»

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.



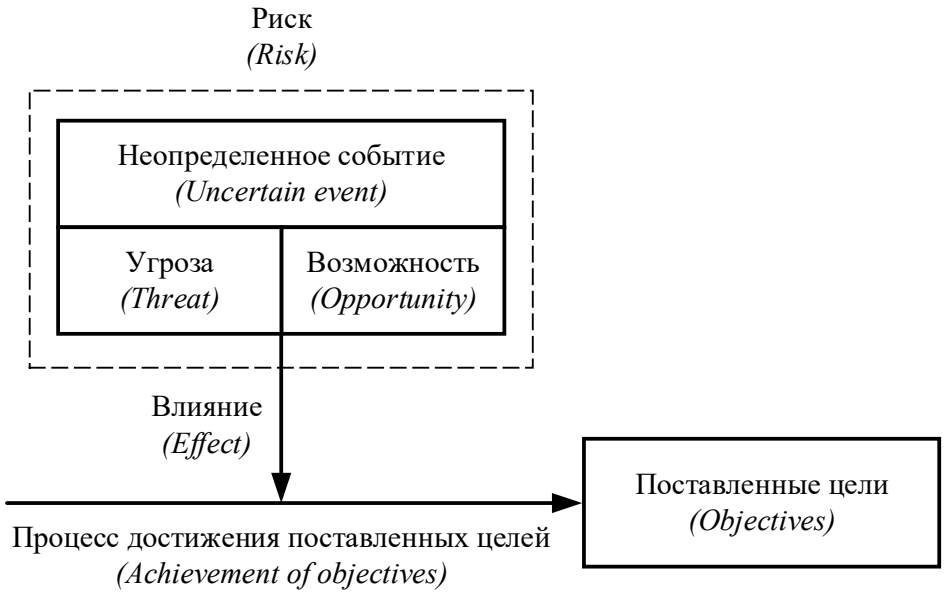
ПОНЯТИЕ «РИСК»

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.

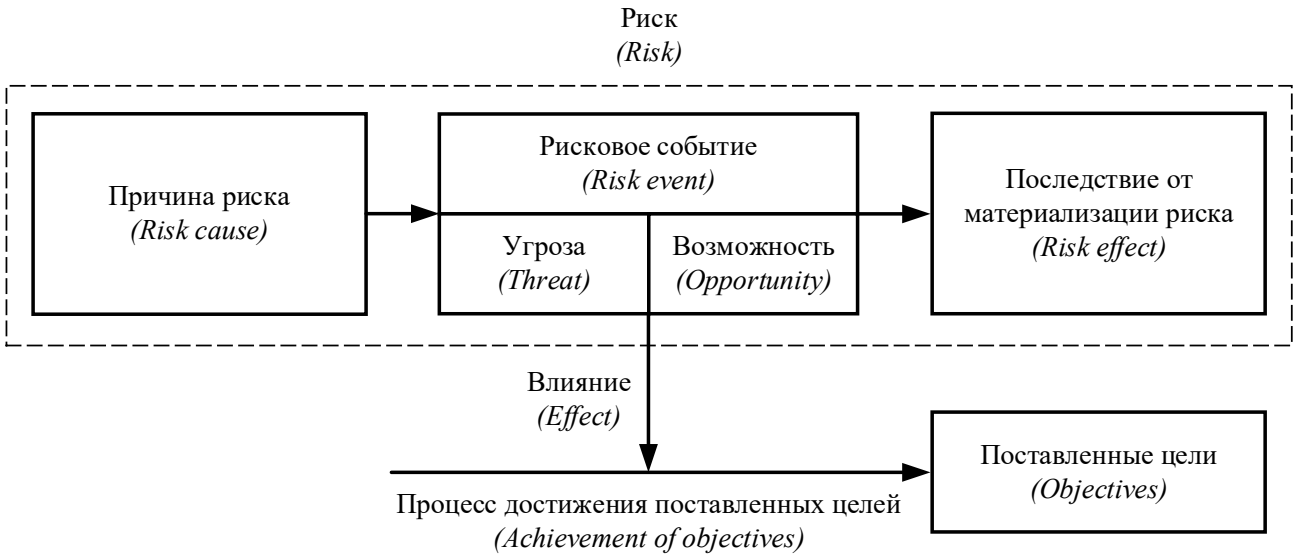


ПОНЯТИЕ «РИСК»

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»



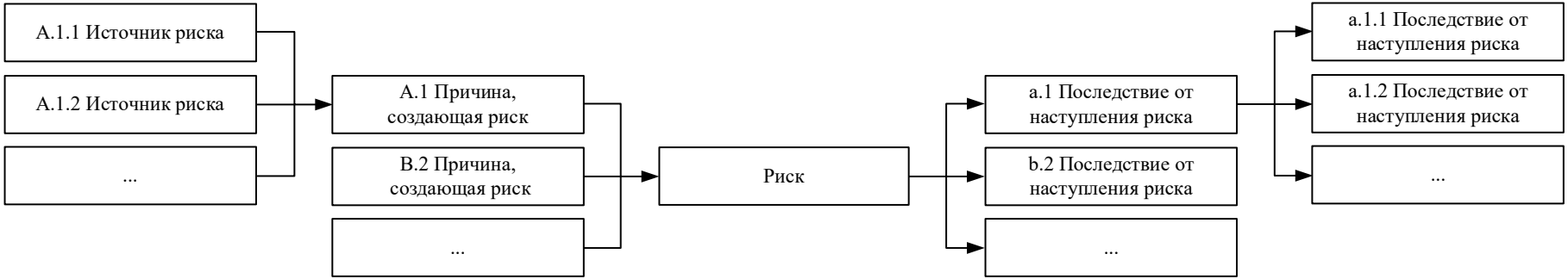
Международный свод знаний проектного управления **PRINCE2®** считает «риск» неопределенным событием, которое имеет сложную структуру. В частности, риск состоит из причины риска, угрозы, позитивной возможности и последствия в случае его материализации.

ПОНЯТИЕ «РИСК»

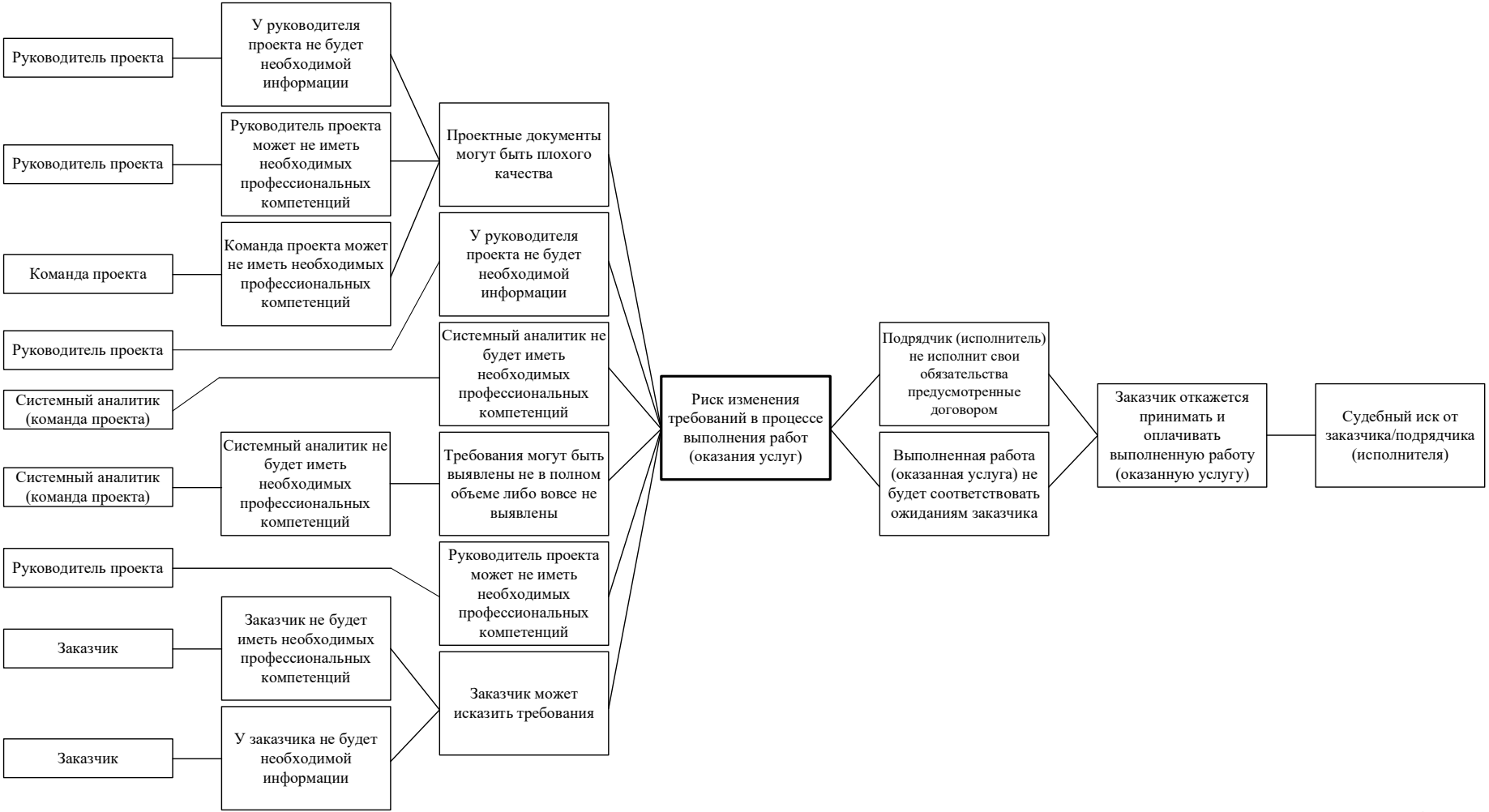
Стоит отметить, что согласно отечественным и международным стандартам понятия **«неопределенность»** и **«риск»** часто воспринимаются как синонимы. Однако между ними есть существенные различия. В частности:

- 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»



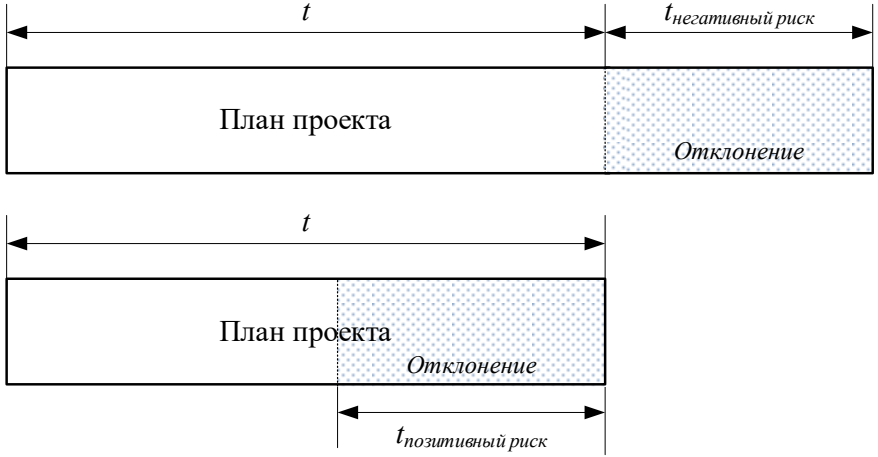
Таким образом, на основе рассмотренных выше точек зрения можно заключить, что **риск** – это вероятное событие, проистекающее из конкретных источников, материализация которого может привести к наступлению благоприятных/проблемных последствий. Под **причинами, создающими риск**, понимаются условия, имеющие 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.



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.

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

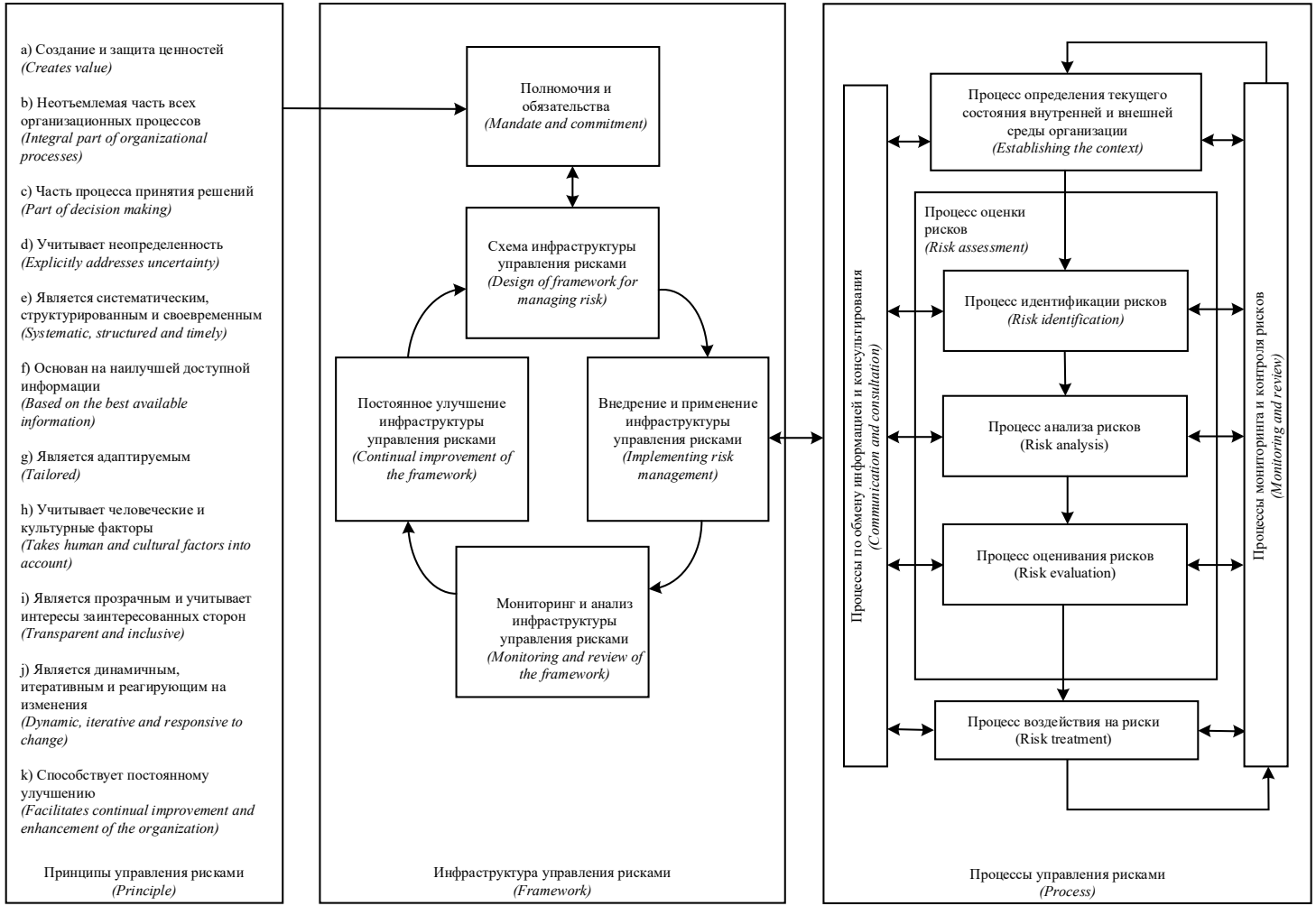
В качестве примера наступившего негативного риска можно рассмотреть ситуацию потери сервера жестких дисков в ИТ-организации в результате пожара (**C1**). Для того, чтобы ликвидировать полученные последствий ИТ-организации необходимо приобрести новый сервер (**C2**), осуществить пуско-наладочные работы (**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.

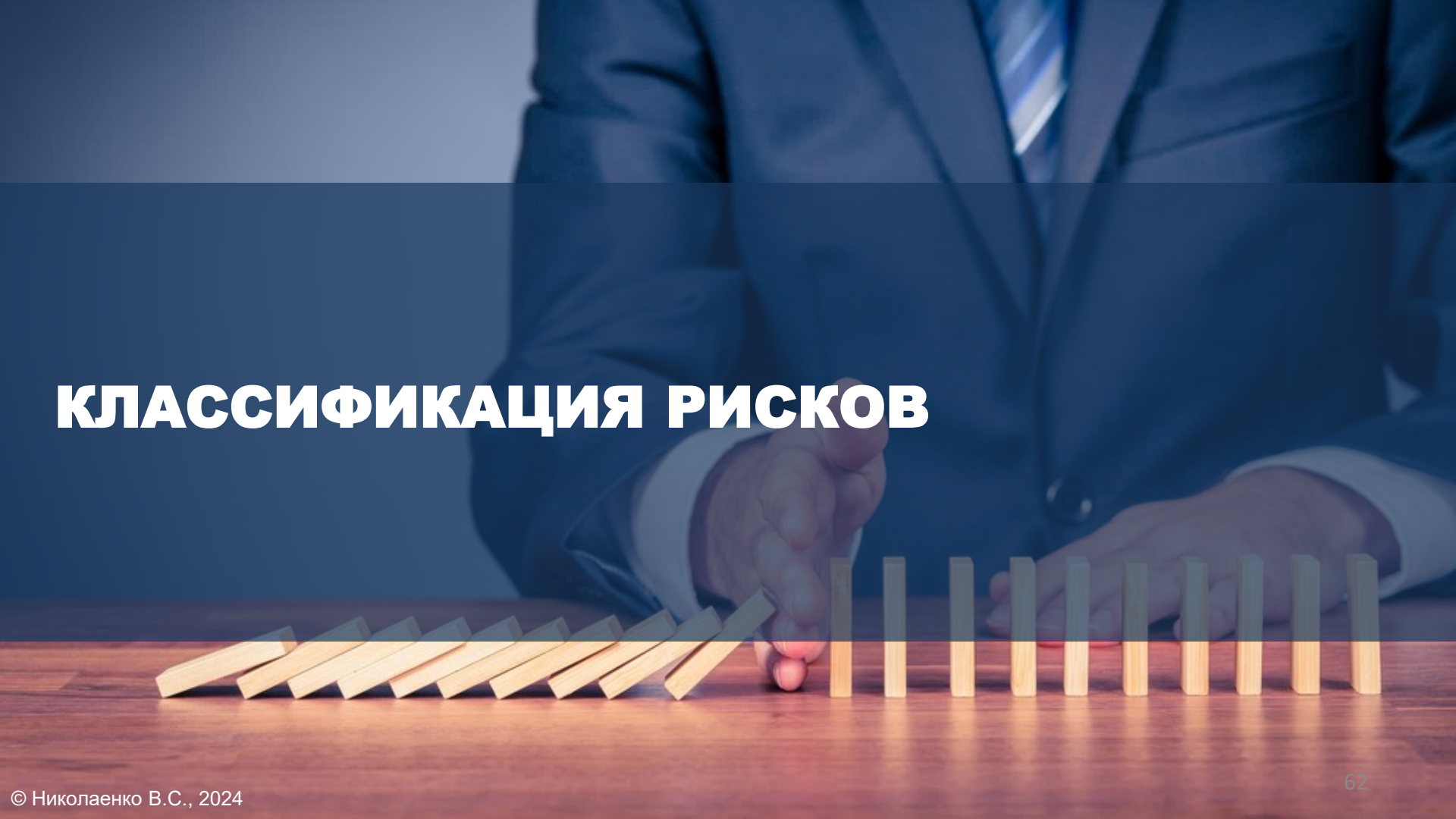
ПОНЯТИЕ «УПРАВЛЕНИЕ РИСКАМИ»

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.

КЛАССИФИКАЦИЯ РИСКОВ



КЛАССИФИКАЦИЯ
в зависимости от масштабов воздействия

По масштабу воздействия риски разделяются на:

- **Макориски** – глобальные риски, последствия от материализации которых отражаются на всех экономических агентах. Например, экономический кризис 2007-2009 годов, который начался с ипотечного кризиса в США отразился в итоге на экономике Российской Федерации вызвав одно их самых глубоких падений ВВП (–7,8% в 2009 году).
- **Мезориски** – риски, последствия от наступления которых влияют на определенный регион или отрасль экономики.
- **Микориски (предпринимательские риски)** – вероятные события, наступление которых оказывает влияние на экономическую деятельность конкретных экономических агентов. Например, алмазодобывающий холдинг **«Алроса»** в 26 июня 2022 года не смог выплатить купонный доход по еврооблигациям на сумму **$7,75 млн.** из-за рестрикций США, ЕС и Великобритании.

КЛАССИФИКАЦИЯ
по функциональной области организации

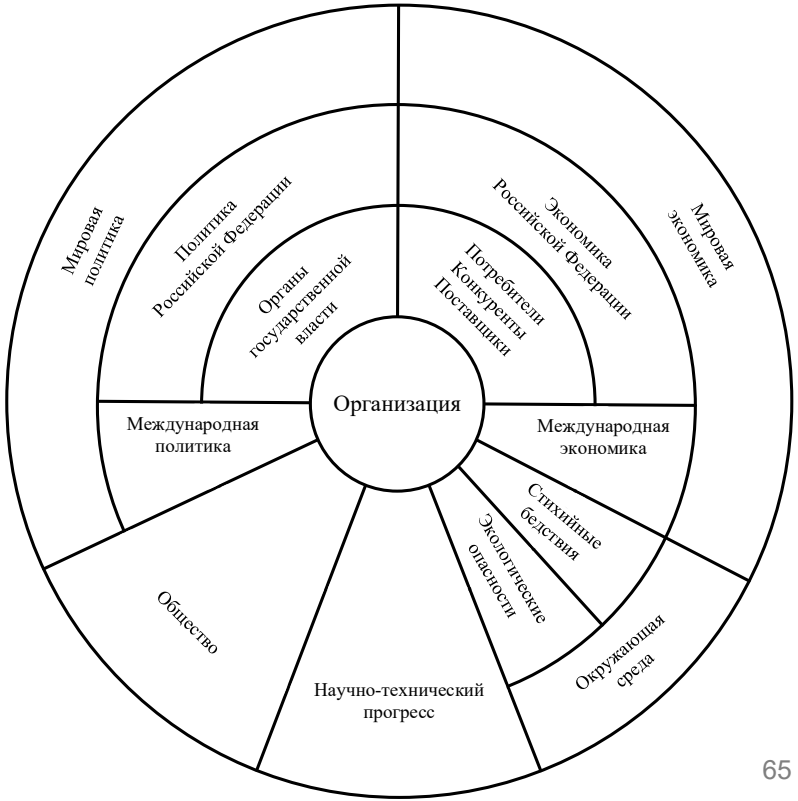
По функциональной области организации риски подразделяются на:

- Внутренние и внешние риски.
- Коммерческие риски.
- Имущественные риски.
- Производственные риски.
- Торговые риски.
- Транспортные риски.
- Финансовые риски.
- Инвестиционные риски.
- Комплаенс риски.
- Проектные риски.

КЛАССИФИКАЦИЯ
по функциональной области организации

Внутренние и внешние риски

Если источники рисков находятся внутри организации, то эти риски называют **внутренними рисками**, если источники рисков находятся за пределами организации – **внешними рисками**.



КЛАССИФИКАЦИЯ
по функциональной области организации

Коммерческие риски – непредвиденные расходы (доходы), которые могут быть получены во время ведения финансово-хозяйственной деятельности организаций.

КЛАССИФИКАЦИЯ
по функциональной области организации

Имущественные риски – вероятность потери имущества по причине пожара, кражи, диверсии, халатности и др.

КЛАССИФИКАЦИЯ
по функциональной области организации

Производственные риски – возможный ущерб от остановки производства, гибели или повреждения оборудования, полученного брака продукции и др.

КЛАССИФИКАЦИЯ
по функциональной области организации

Транспортные риски – вероятность повреждения или потери товара во время перевозки автомобильным, морским, речным, железнодорожным и/или воздушным транспортом.

КЛАССИФИКАЦИЯ
по функциональной области организации

Финансовые риски – вероятность получения убытков (прибыли).

КЛАССИФИКАЦИЯ
по функциональной области организации

Инвестиционные риски – вероятность неполучения (получения) ожидаемого коммерческого эффекта. При рассмотрении инвестиционных рисков в негативном ключе выявляются следующие их подвиды:

- **Риски упущенной выгоды** – возможность получения финансового ущерба в результате неосуществления какой-либо превентивной меры, например страхования, хеджирования др.
- **Риски снижения доходности** возникают в результате снижения размера дивидендов по портфельным инвестициям и/или вкладам.
- **Риски прямых финансовых потерь**.
- **Кредитный риск** – вероятность неуплаты заемщиком основного долга и процентов, причитающихся кредитору. К данному риску относится ситуация, при которой эмитент, выпускающий долговые ценные бумаги, окажется не в состоянии выплачивать процент по ним или основную сумму долга.

КЛАССИФИКАЦИЯ
по функциональной области организации

Комплаенс риски

Термин **«комплаенс»** (от англ. to comply – соответствовать) означает соответствие внутренним требованиям организации и внешним нормам действующего законодательства. Возможное несоответствие нормативным актам, правилам, стандартам и кодексам поведения называется комплаенс рисками. Последствия от наступления этих рисков проявляется в форме юридических санкций со стороны регулирующих и надзорных органов, отраслевых ассоциаций, а также лиц, чьи права и интересы были нарушены.

КЛАССИФИКАЦИЯ
по функциональной области организации

Проектные риски – вероятные события, наступление которых оказывает влияние на одну цель проекта либо на их совокупность (содержание, длительность, стоимость и качество проекта). Проектные риски, как правило, возникают из-за действий/бездействий руководителей проектов, участников проектных команд, а также применяемых технологий и оборудования.

КЛАССИФИКАЦИЯ
по покупательной способности денег

К рискам, связанным с покупательной способностью денег, относятся:

- **Рыночные риски** – это риски того, что изменение цен и ставок на рынке снизят денежную стоимость капитала, ценных бумаг или портфеля.
- **Инфляционные риски** – вероятность обесценивания реальной покупательной способности денег.
- **Дефляционные риски** – вероятность усиления реальной покупательной способности денег.
- **Валютные риски** – вероятность денежных потерь при конвертации одной валюты на другую валюту.
- **Риски ликвидности** – вероятность неисполнения денежных обязательств в установленном объеме и в согласованный срок.

КЛАССИФИКАЦИЯ
по степени контролируемости

По степени контролируемости риски классифицируются на **неконтролируемые**, **частично контролируемые** и **контролируемые**.

КЛАССИФИКАЦИЯ
относительно наступивших последствий

В зависимости от наступивших последствий риски могут быть **негативными**, **позитивными**, **смешанными** и **нейтральными**.

В литературе также можно встретить иную классификацию рисков относительно характера последствий наступления рисковых событий. В частности, риски принято разделять на чистые и спекулятивные.

- **Чистые риски** – вероятные события, которые могут привести к наступлению проблемных последствий.
- **Спекулятивные риски** – вероятные события, которые могут привести к наступлению как проблемных, так и благоприятных последствий.

КЛАССИФИКАЦИЯ
относительно частоты наступлений в ранее заключенных сделках (завершенных проектах)

В зависимости от частоты наступлений в ранее заключенных сделках и завершенных проектах различают:

- **универсальные риски** — вероятные события, которые актуальны для любой сделки и проекта независимо от его масштаба, сложности, длительности, типа, способов управления и численности участников команды;
- **специальные риски** — вероятные индивидуальные события, которые актуальны для частной сделки или проекта

КЛАССИФИКАЦИЯ
в зависимости от времени актуализации (наступления) рисков относительно фаз жизненного цикла проекта

В зависимости от времени актуализации (наступления) рисков относительно фаз жизненного цикла проекта выделяют:

- **постоянные риски** — вероятные события, которые имеют потенциал материализоваться в любой временной период выполнения проекта;
- **риски, связанные с фазой жизненного цикла** — вероятные события, которые могут материализоваться только во время определенной фазы жизненного цикла проекта.

ОЦЕНКА РИСКОВ

МЕТОДЫ ИДЕНТИФИКАЦИЯ РИСКОВ

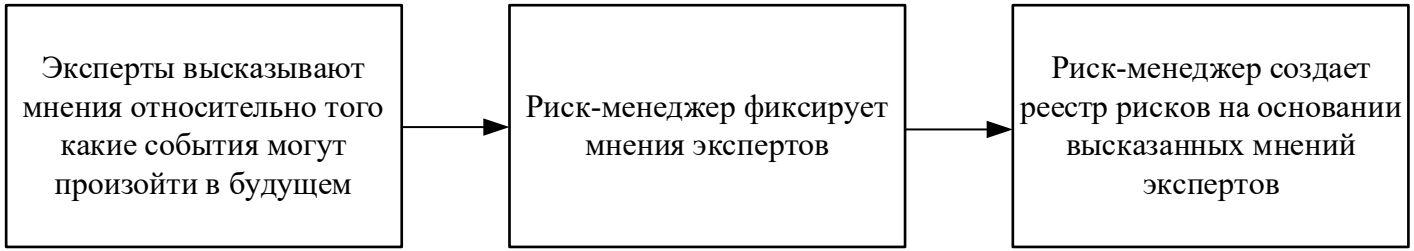
Название (на английском)	Название (перевод на русский)	Разработчики
Retrospective	Ретроспективный анализ документации	Никонов В., Россия Поляков А. А. и Ключников В.О., Россия
Brainstorming	Мозговой штурм, мозговая атака	Осборн А., США
Delhi	Метод Дельфи, дельфийский метод	Хелмер О., Далки Н. и Ресчер Н., США
SWOT matrix (Strengths, Weaknesses, Opportunities, Threats)	SWOT-анализ	Эндрюс К., США
STEEP matrix (Social, Technological, Economic, Ecological, Political)	STEEP-анализ / PEST-анализ	Мишель Портер, Генри Минтзберг, Брюс Хендерсон, Гари Хамел, США
Hazard and Operability Study, HAZOP	Исследование опасности и работоспособности	Клетз Т., Великобритания
Structured What-If Technique, SWIFT	Структурированный анализ сценариев методом «что, если?»	Лравли Ф., Великобритания
Preliminary Hazard Analysis, PHA	Предварительный анализ опасностей	Хенкли Э. Дж., Кумамото Х., США

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ ДОКУМЕНТОВ (RETROSPECTIVE)

Анализ документов, например договоров и реестров рисков ранее заключенных сделок и завершенных проектов, позволяет оперативно выявить уже наступившие риски, которые материализовались и оказали влияние на достижение запланированных целей.

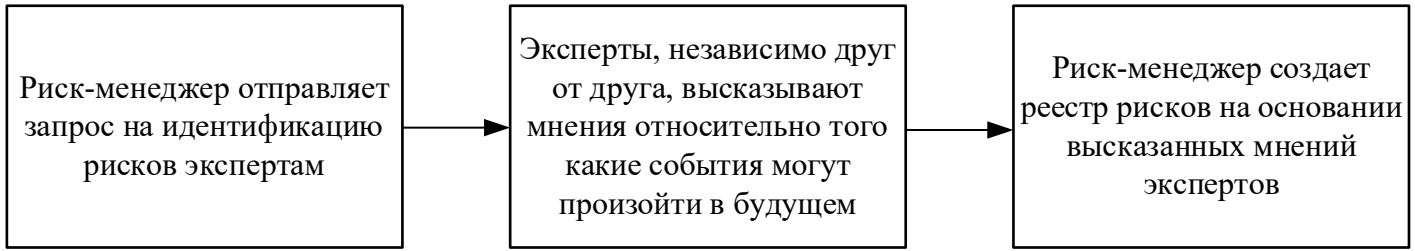
Пример 170 рисков ранее наступивших рисков, представлен в реестре универсальных рисков. Данные риски являются **универсальными**, т. е. они актуальны для любого проекта (сделки), независимо от его масштаба, сложности, длительности, типа, способов управления и численности участников команды. Вероятные события, которые актуальны исключительно для частного проекта, называются **специальными рисками**. Для выявления специальных рисков ретроспективный анализ документов не подходит, т. к. требуется использовать творческий подход.

МЕТОД «МОЗГОВОЙ ШТУРМ» (BRAINSTORMING)



Метод является коллективным и творческим. Основными преимуществами метода являются выявление специальных рисков, легкость применения, а также коллаборация участников. Среди недостатков можно отметить низкое качество процесса идентификации рисков.

МЕТОД «ДЕЛЬФИ» (DELHI)



Созданный в 60-е годы XX века сотрудниками RAND Corporation, метод «Дельфи» изначально разрабатывался как метод прогнозирования трендов развития технологий. Однако спустя время метод показ свою результативность во время выявления рисков. Особенность метода заключается в том, что эксперты могут индивидуально и анонимно выражать свое мнение, имея при этом возможность узнавать мнения и идеи друг друга, что позволяет выявлять специальные риски, которые обычно не произносятся вслух.

SWOT-АНАЛИЗ И STEEP-АНАЛИЗ

Данный метод позволяет выявлять не только сильные и слабые стороны, но и возможности (позитивные риски) и угрозы (негативные риски). На практике SWOT-анализ усиливают STEEP-анализом, который предоставляет возможность исследовать в том числе социальные, технологические, экономические, экологические и политические риски.

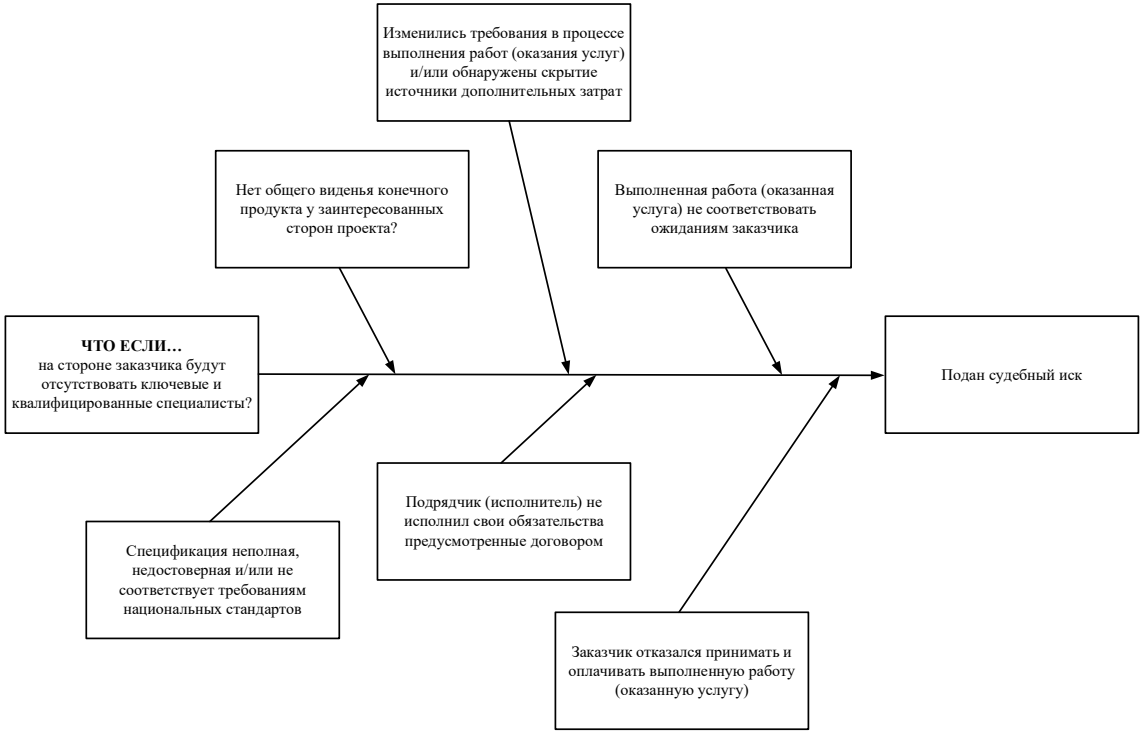
HAZARD AND OPERABILITY STUDY (HAZOP) И COMPUTER HAZARD AND OPERABILITY ANALYSIS (CHAZOP)

№	Тип отклонения	Управляющее слово	Примеры отклонений для ИТ-проекта
1	Отрицательный	НЕТ	НЕТ информации, которая необходима для реализации ИТ-продукта
2	Количественные изменения	БОЛЬШЕ	Источников, где хранится актуальная информация о проекте, БОЛЬШЕ, чем необходимо
		МЕНЬШЕ	Сотрудников в проекте МЕНЬШЕ, чем необходимо
3	Качественные изменения	ТАК ЖЕ, КАК	Ожидается отклонение от запланированных сроков ТАК ЖЕ, КАК и в проекте, который был завершен ранее
		ЧАСТЬ	Доступна только ЧАСТЬ актуальной информации, которая необходима для создания ИТ-продукта
4	Замена	ПЕРЕМЕНА	В процессе реализации ожидается ПЕРЕМЕНА запланированных требований
		ДРУГОЙ	Проектом будет управлять ДРУГОЙ руководитель
5	Время	РАНО	Реализация проекта будет начата слишком РАНО
		ПОЗДНО	Реализация проекта будет начата слишком ПОЗДНО
6	Порядок или последовательность	ПРЕЖДЕ, ЧЕМ	Заказчик будет знакомиться с разработанным инкрементом программного кода ПРЕЖДЕ, ЧЕМ завершится тестирование
		ПОСЛЕ	Актуальная информация поступит ПОСЛЕ разработанных функций

Т. Клетз, разрабатывая HAZOP, в первую очередь стремился избежать промышленных инцидентов, таких как пожары, выбросы вредных веществ и утечки химикатов. Со временем его метод доказал свою работоспособность и в 1974 году HAZOP вошел в состав обязательных методов, применяемых для идентификации рисков. Позднее метод был адаптирован и для разработки программ для ЭВМ. Метод получил название Computer Hazard and Operability Analysis (CHAZOP).

STRUCTURED WHAT-IF TECHNIQUE (SWIFT)

Анализ сценариев развития последствий в результате наступления рисков с помощью метода SWIFT является упрощенной версией CHAZOP. В частности, такие фразы, как «что, если… ?» «к чему это приведет… ?», «что случится, если… ?», «может ли кто-либо… ?», «может ли что-либо… ?», помогают выявить возможные последствия в случае наступления риска. Главными достоинствами метода является простота его использования, т. к. метод не требует предварительной подготовки, а также его графическое исполнение, что стимулирует творческий процесс.



PRELIMINARY HAZARD ANALYSIS (PHA)

Метод PHA направлен на выявление угроз, которые могут причинить вред используемому оборудованию или разрабатываемой программе для ЭВМ. Благодаря определению критических контрольных точек с помощью метода определяются стадии, которые требует создания дополнительных профилактических мер, нивелирующих угрозу наступления катастрофических рисков. PHA распределяет риски на 3 класса:

- **первый класс** – безопасные вероятные события, которые не могут оказать негативного влияние;
- **второй класс** – пограничные вероятные события, которые, например, не вызывают поломки оборудования, но сказываются на качестве выполненной работы;
- **третий класс** – критические вероятные события. К данным рисками относятся поломка оборудования, уход ключевого сотрудника, отсутствие финансирования и др.

МЕТОДЫ АНАЛИЗА РИСКОВ

№	Название (оригинал)	Название (перевод на русский)	Разработчики
1	Bow-tie	Метод «Галстук-бабочка» (первый этап)	Б. Лангминд
2	5Why	Метод «Почему-почему»	С. Тоеда

МЕТОД «ГАЛСТУК-БАБОЧКА» (BOW-TIE)

Метод состоит из двух этапов. На первом этапе проводится анализ рисков, где устанавливаются причины, создающие риски, источники рисков и прогнозируются возможные последствия в случае их наступления. На втором этапе разрабатываются «барьеры», которые направлены на локализацию источников рисков, и «меры восстановления (усиления)», призванные оперативно локализовать причиненный ущерб (усилить благоприятный эффект). Второй этап метода применяется в процессе воздействия на риски во время разработки мер плана А и плана Б.

МЕТОД «ПОЧЕМУ-ПОЧЕМУ» (5WHY)

Название риска	Почему есть вероятность наступления этого риска?	Почему есть вероятность наступления этого риска?	Источник риска
Риск того, что по факту проектные работы окажутся значительно сложнее, чем предполагалось изначально	Руководитель проекта может не иметь необходимых профессиональных компетенций	Нет ответа	Руководитель проекта
	У руководителя проекта не будет необходимой информации	Нет ответа	Руководитель проекта
	Требования могут быть выявлены не в полном объеме либо вовсе не выявлены	Системный аналитик не будет иметь необходимых профессиональных компетенций	Системный аналитик (команда проекта)
	Проектные документы могут быть плохого качества	У руководителя проекта не будет необходимой информации	Руководитель проекта
		Руководитель проекта может не иметь необходимых профессиональных компетенций	Руководитель проекта
		Команда проекта может не иметь необходимых профессиональных компетенций	Команда проекта

Данный метод был предложен С. Тоёда с целью повышения качества продукции фирмы «Тойота». Впоследствии метод стал применяться и в других сферах. Суть метода заключается в последовательном задавании вопроса «Почему есть вероятность наступления этого риска?», для того чтобы определить источник риска. Если источник риска во время первой итерации не устанавливается, тогда процедура повторяется.

МЕТОДЫ ОЦЕНИВАНИЯ РИСКОВ

Представим, что в процессе идентификации рисков было выявлено большое количество рисков и что после проведения анализа стало очевидно, что не все они одинаково важны. Например, риск возможного ухода ключевого сотрудника будет представлять для нас больший интерес, нежели отключение электричества или интернета. В связи с этим логично предположить, что выявленные риски следует определенным образом сгруппировать, так чтобы выделить среди них группу наиболее опасных, группу рисков, которые будут требовать постоянного управленческого внимания, группу незначительных рисков, которые можно не учитывать и др.

Для решения данной проблемы применяют **оценивание рисков**.

МЕТОДЫ ОЦЕНИВАНИЯ РИСКОВ

Согласно **ГОСТ Р 31010-2011** оцениваются две основные характеристики риска – **вероятность материализации риска** и **возможное влияние в случае его наступления**. Измерение степени вероятности и влияния риска осуществляется с помощью специальных количественных и качественных методов.

Количественные методы – это методы, использующие математический аппарат для прогнозирования вероятности материализации рисков и возможного влияния в случае их наступления.

Примерами количественных методов являются:

- математическое ожидание;
- дисперсия и среднеквадратическое отклонение;
- полудисперсия;
- Value-at-Risk (VaR).

Качественные методы – это методы, которые используют экспертные мнения для оценивания характеристик вероятностей и влияний рисков. Как правило, качественные методы применяются, когда наблюдается большая неопределенность, отсутствует необходимая информация и/или нет накопленных статистических данных о ранее наступивших рисках.

КОЭФФИЦИЕНТЫ ОЦЕНИВАНИЯ ВЕРОЯТНОСТИ МАТЕРИАЛИЗАЦИИ РИСКА И ВОЗМОЖНОГО ВЛИЯНИЯ В СЛУЧАЕ НАСТУПЛЕНИЯ РИСКА

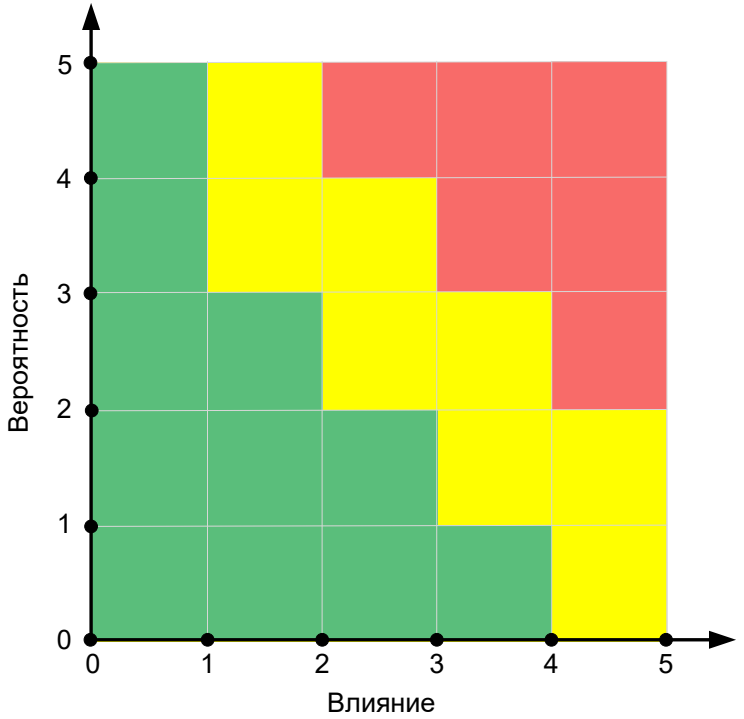
Степень влияния риска на проект	Коэффициент Харрингтона (согласно PMBoK)	Коэффициент Харрингтона
Очень высокая	0,8-1,0	5
Высокая	0,64-0,8	4
Средняя	0,37-0,64	3
Низкая	0,2-0,37	2
Очень низкая	0,1-0,2	1
Нет влияния	0,0-0,1	0

Степень вероятности наступления риска в проекте	Коэффициент Харрингтона (согласно PMBoK)	Коэффициент Харрингтона
Очень высокая	0,8-1,0	5
Высокая	0,64-0,8	4
Средняя	0,37-0,64	3
Низкая	0,2-0,37	2
Очень низкая	0,1-0,2	1
Нет вероятности	0,0-0,1	0

МЕТОДЫ ОЦЕНИВАНИЯ РИСКОВ

Визуализация полученных оценок осуществляется с помощью специального инструмента – **матрица рисков**. Пример матрицы рисков, который применяется Министерством обороны США (**The Department of Defense United States of America, DoD**) представлен на рисунке. Следует отметить, что DoD рассматривает риск только в негативном ключе, поэтому матрица рисков имеет три группы:

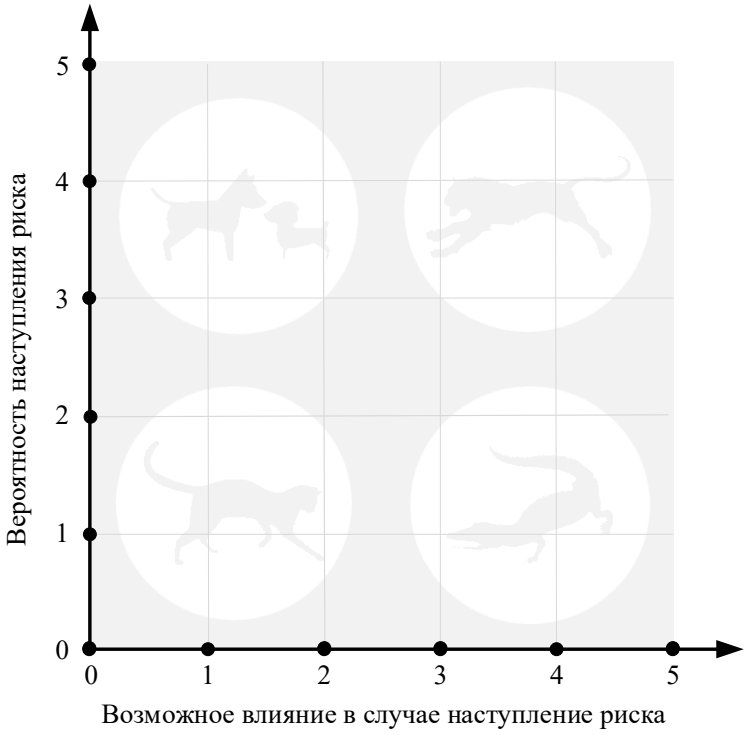
- **Красная**. Риски «красной» группы самые опасные, способные нанести катастрофический ущерб.
- **Желтая**. Риски «желтой» группы умеренные, способные нанести приемлемый ущерб.
- **Зеленая**. Риски «зеленой» группы безопасны.



МЕТОДЫ ОЦЕНИВАНИЯ РИСКОВ

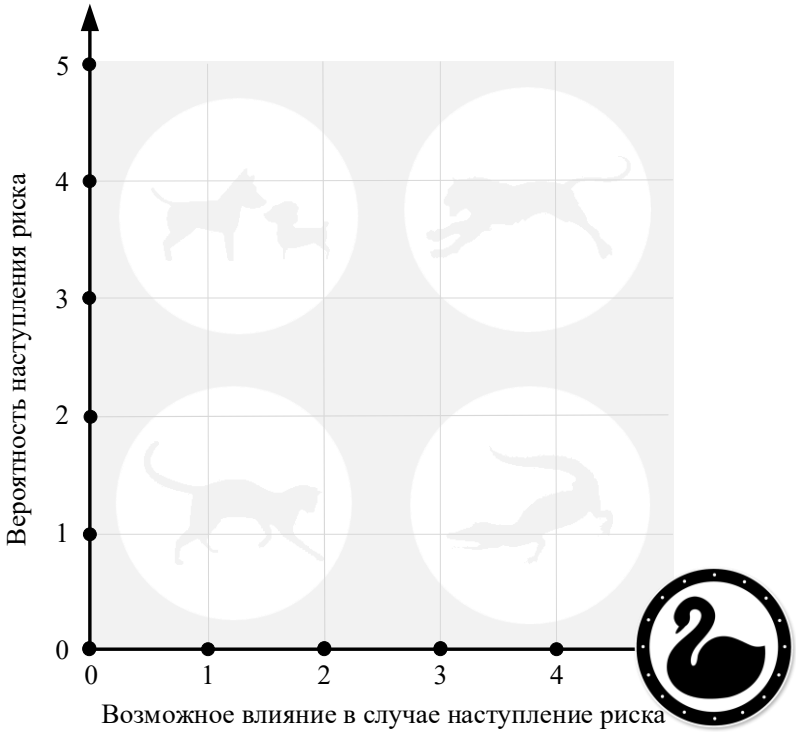
Т. Мерна и Ф. Ал-Хани предлагают распределять риски негативные риски на 4 группы:

- **Катастрофические риски или «тигры» (tiger)** – это негативные риски, которые имеет высокую вероятность материализации и способны оказать значительное негативное влияние в случае их наступления. По мнению Т. Мерна и Ф. Ал-Хани, материализация одного «тигра», например «проект покинул руководитель проекта», способно привести к полной остановке работ (оказания услуг).
- **Непредсказуемые риски или «аллигаторы» (alligator)** – это негативные риски, которые имеет низкую вероятность материализации, но обладают способностью оказывать значительное негативное влияние. Как правило, к «аллигаторам» относятся комплаенс риски. Например, организация, реализующая проект, может получить штраф в связи с нарушением императивных норм **ч. 1 ст. 9.5 КоАП РФ, ч. 3 ст. 14.1 КоАП РФ, ст 15.33.2 КоАП РФ** и др.
- **Часто встречаемые риски, или «щеночки» (puppy)** – это негативные риски, которые имеет высокую вероятность материализации, но при этом не способны оказывать какого-либо значительного влияния. Примерами часто встречаемых рисков могут быть риски, связанные с социально-психологической атмосферой в команде проекта, внутренней мотивацией, конфликтами и др.
- **Несущественные риски, или «котята» (kitten)** – это негативные риски, которые имеет низкую вероятность материализации и при этом не обладает способностью оказывать какого-либо значительного влияния. По мнению Т. Мерна и Ф. Ал-Хани, «котята» не способны хоть как-то навредить проекту, поэтому данными негативными рисками можно пренебречь.



МЕТОДЫ ОЦЕНИВАНИЯ РИСКОВ

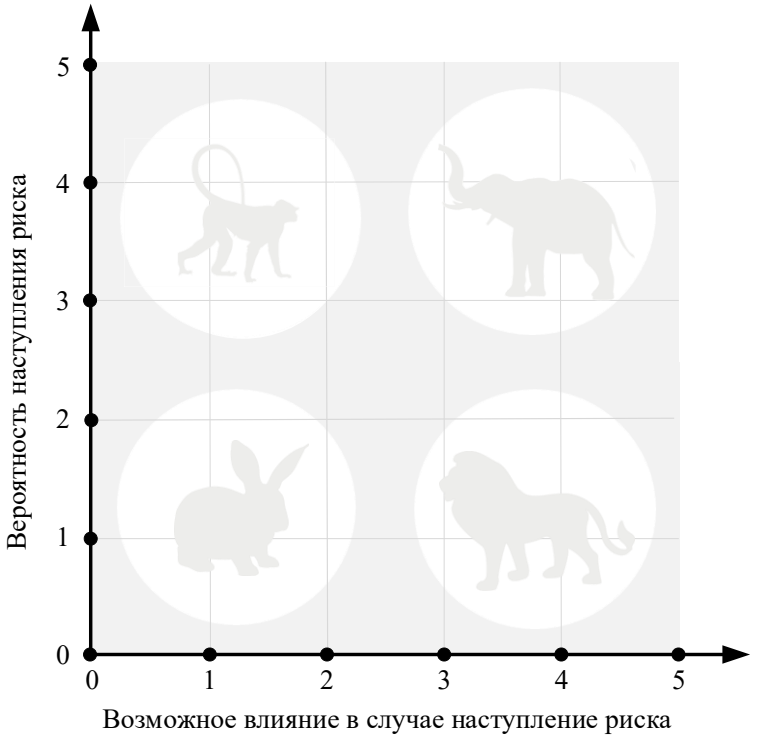
Отдельно необходимо выделить группу маловероятных, но очень опасных рисков, таких как промышленные катастрофы, потрясения, природные катаклизмы, пандемии и эпидемии. Н. Н. Талеб называет подобные риски **«черные лебеди»**.



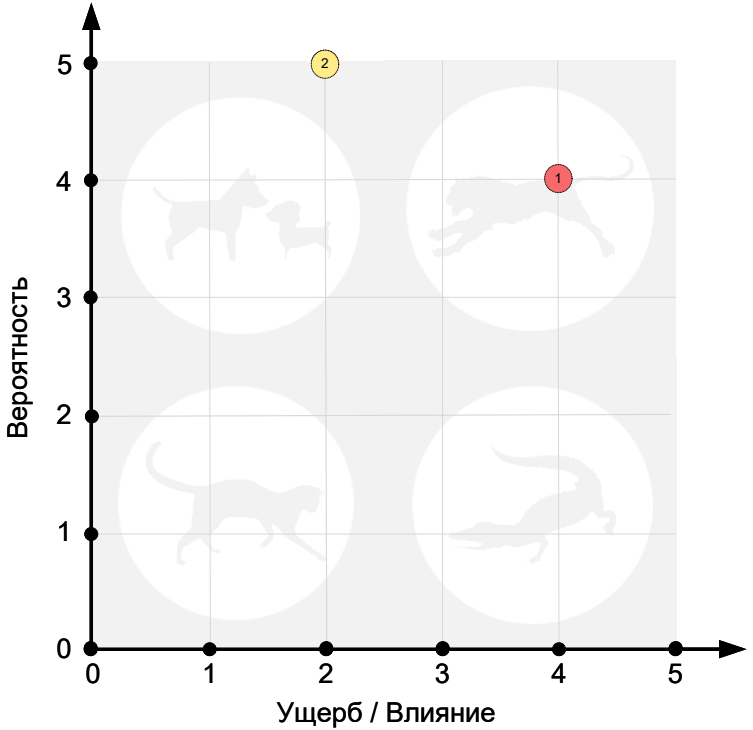
МЕТОДЫ ОЦЕНИВАНИЯ РИСКОВ

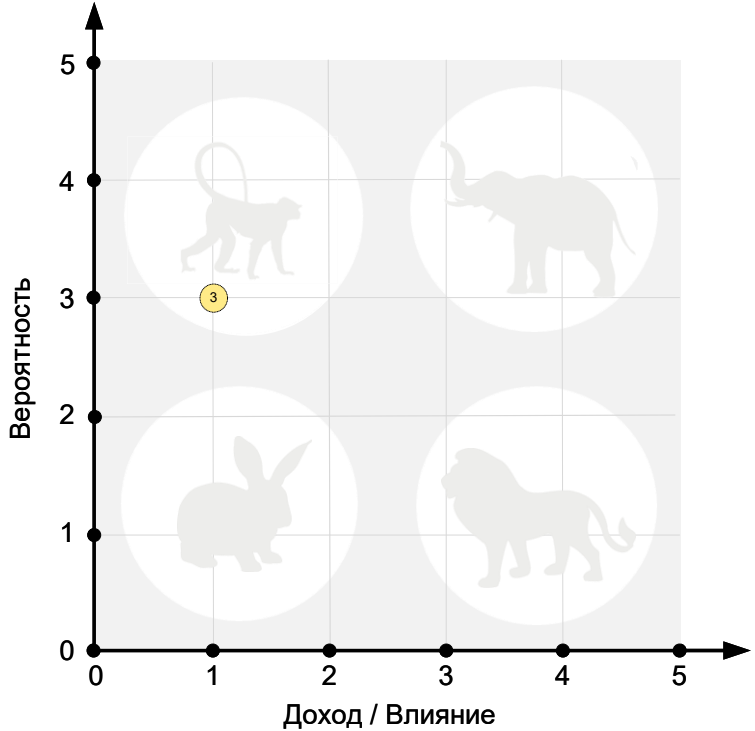
Позитивные риски автор настоящего пособия рекомендует распределять на следующие 4 группы:

- **Созидательные риски, или «слоны»** – это позитивные риски, которые имеют высокую вероятность материализации и способны оказывать значительное влияние. За частую «слоны» наступают независимо от превентивных мер воздействия на риски, поэтому для них не рекомендуется проводить какие-либо дополнительные меры воздействия.
- **Непредсказуемые риски, или «львы»** – это позитивные риски, которые имеют низкую вероятность материализации, но обладают способностью оказывать значительное влияние. Исходя из вышесказанного можно заключить, что «львы» имеют большой практический интерес. Например, если заблаговременного будут проведены стимулирующие меры, то в проект могут быть привлечены ведущие программисты, что позитивно повлияет на процесс достижения целей.
- **Часто встречаемые риски, или «обезьяны»** – это позитивные риски, которые имеют высокую вероятность материализации, но не способны оказывать значительного влияния. Отделение данных позитивных рисков от остальных имеет большую практическую ценность, т. к., «дразня» заинтересованные стороны, «обезьяна» вынуждает расходовать ограниченные ресурсы, не оказывая при этом какого-либо значительного влияния на процесс достижения целей.
- **Незначительные риски, или «кролики»** – это позитивные риски, которые имеют низкую вероятность материализации и не обладает способностью оказывать значительного позитивного влияния. Рисками данной группы можно пренебречь.



ПРИМЕР ГРУППИРОВКИ НЕГАТИВНЫХ И ПОЗИТИВНЫХ РИСКОВ





ПРИМЕРЫ ПОЗИТИВНЫХ РИСКОВ

№	Статус проекта	Распределение, %
1	Успешные проекты	67
2	Незавершенные проекты	5
3	Проекты, в которых проблемы повлекли изменение целей	28

Риск того, что численность участников проекта не будет превышать 6 человек

В аналитических докладах CHAOS Manifesto приводятся статистические данные, которые показывают, что проекты, в состав которых входили менее 6 участников, были гораздо успешнее, чем проекты, в которых принимало участие более 6 человек.

ПРИМЕРЫ ПОЗИТИВНЫХ РИСКОВ

Риск привлечения в проект высококвалифицированного работника

Результаты исследований показывают, что материализация данного позитивного риска повышает вероятность успешного достижения запланированных целей до 70%.

ПРИМЕРЫ ПОЗИТИВНЫХ РИСКОВ

Риск привлечения в проект руководителя проекта, который имеет профессиональное образование в области управления проектами (опыт управления проектами более 2-х лет)

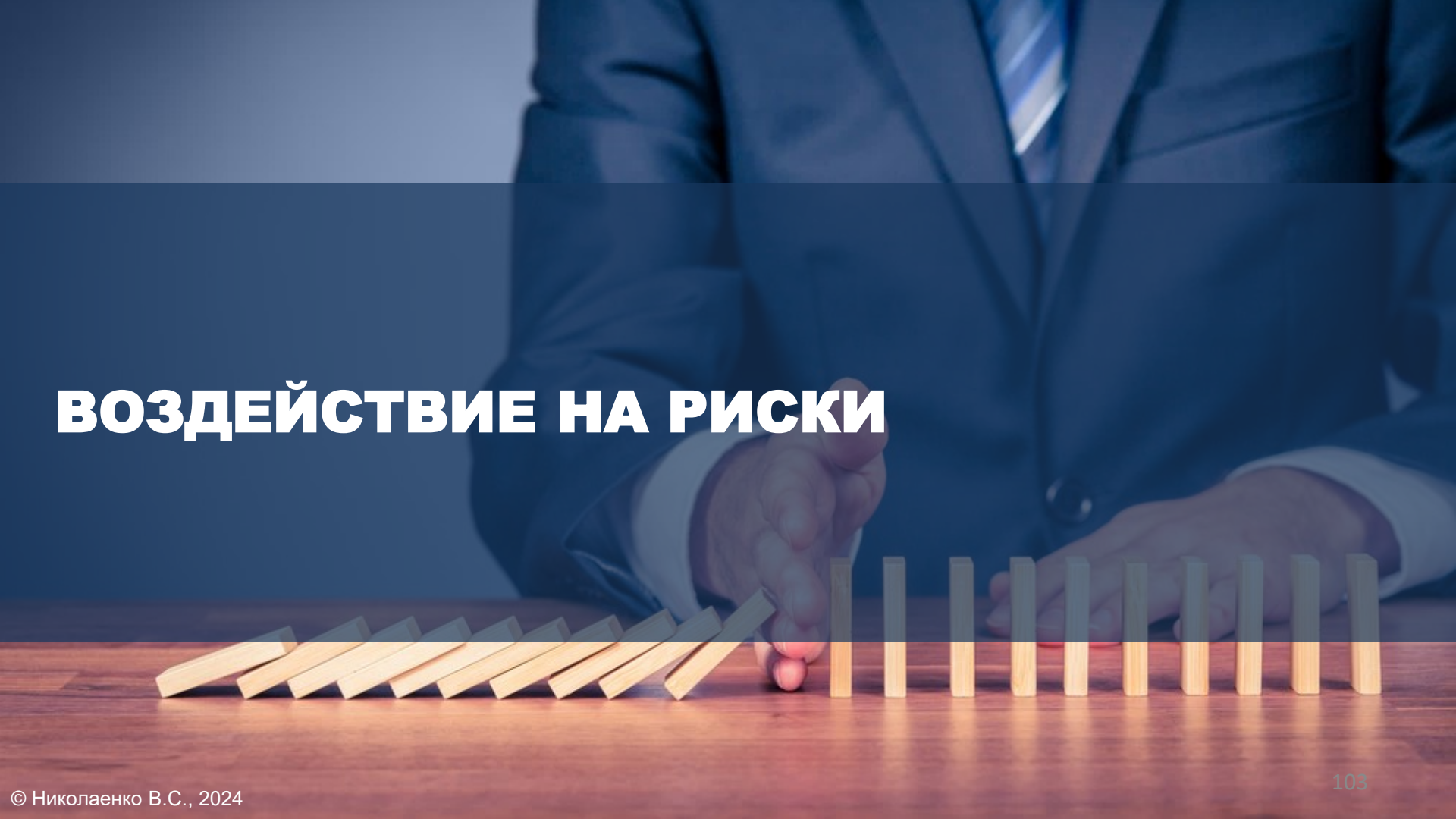
В аналитических отчетах CHAOS Manifesto утверждается, что на успешное завершение проекта значительно влияют профессиональные и личные качества руководителя проекта. В частности, если руководитель проекта имеет профессиональное образование в области управления проектами, то проекты под его руководством ведутся согласно общепринятым нормам, что нивелирует значительную часть негативных рисков. Кроме того, стоит упомянуть результаты исследования В.А.Гаги, С.А.Козловой, А.П.Тютюшева и Е.Н.Ярославцевой, которые доказали, что на эффективность и результативность рабочих групп значительно влияет эмоциональный интеллект руководителя. Например, эксперименты показали, что негативные эмоции руководителя проекта быстро передаются участникам проекта, что отражается на их координации, мотивации и энтузиазме.

ПРИМЕРЫ ПОЗИТИВНЫХ РИСКОВ

Риск декомпозиции большого проекта на малые проекты (длительностью не более 4-х месяцев)

Согласно статистическим данным CHAOS Manifesto доля краткосрочных проектов, трудоемкость которых составляет не более 700 человеко-часов равна 76%, в то время как доля среднесрочных (700–2500 человеко-часов) – 14%, долгосрочных ИТ-проектов (более 2 500 человеко-часов) – 10%.

ВОЗДЕЙСТВИЕ НА РИСКИ



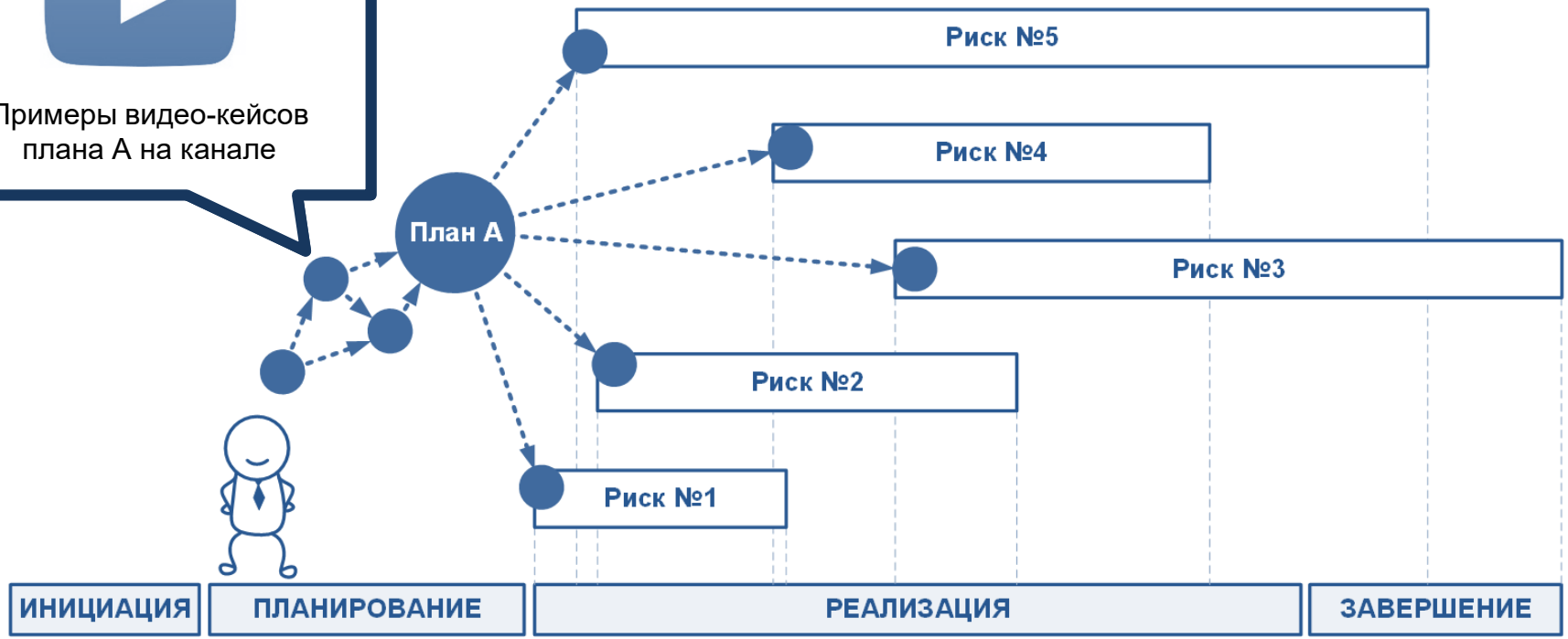
ВОЗДЕЙСТВИЕ НА РИСКИ

После того как среди выявленных рисков установлены наиболее важные и самые опасные риски, которые требуют постоянного управленческого внимания, и риски, которым можно пренебречь, необходимо разработать точечные меры воздействия на данные риски. Процесс разработки мер воздействия на риски включает в себя имплементацию мер превентивного воздействия и мер принятия рисков.

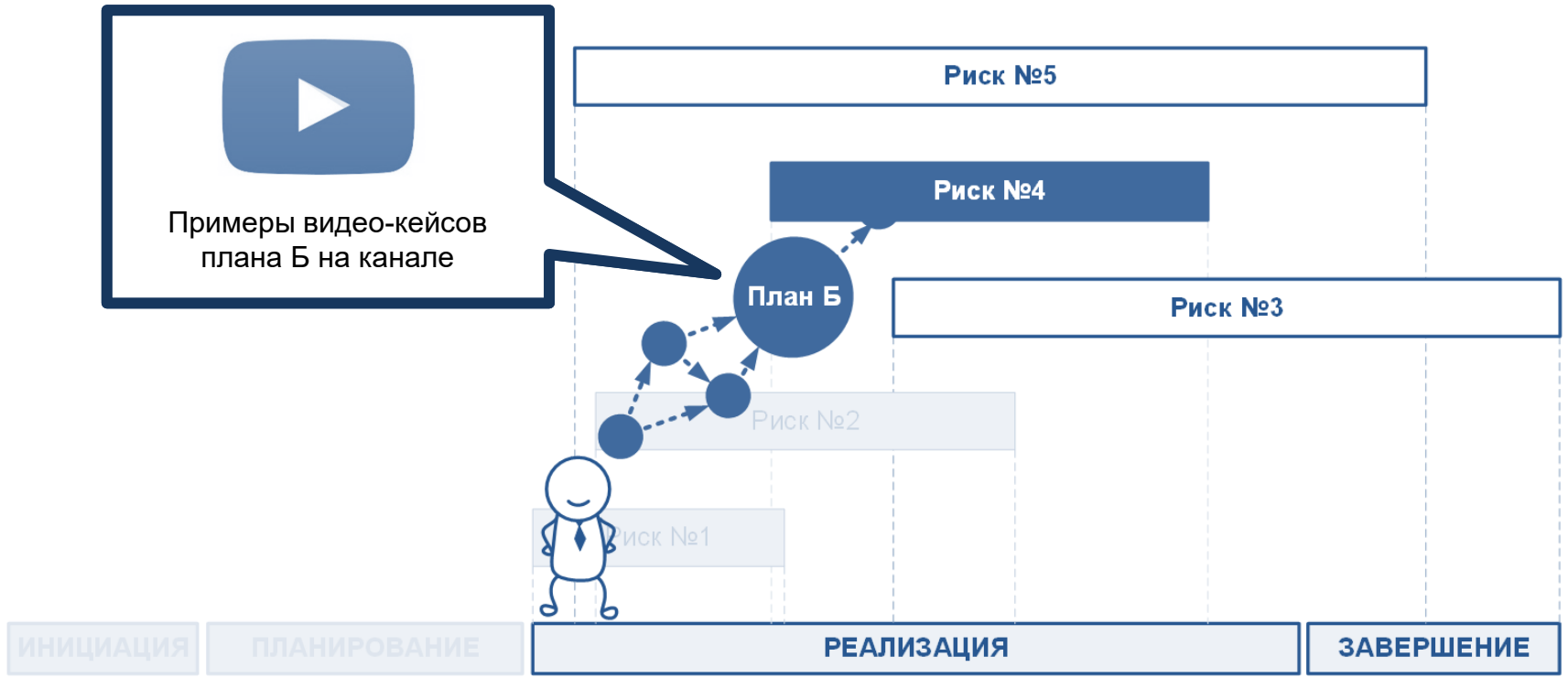
- **Меры превентивного воздействия на риски (план А)** – это перечень профилактических мер упреждающего управления. Например, если будет идентифицирован риск, связанный с отсутствием знаний, навыков и опыта у участников проекта, то превентивной мерой будет организация курсов повышения квалификации и привлечение в проект сторонних экспертов.
- **Меры принятия рисков (план Б)** – это резервы и инструкции по локализации последствий в случае наступления риска. План Б необходим, если произойдет наступление вторичных рисков и рисков-невидимок. **Вторичные риски** – это вероятные события, которые могут наступить несмотря на проведение профилактических мер плана А. **Риски-невидимки** – это скрытые риски, которые не были обнаружены во время идентификации. Опасность данных рисков заключается в их неожиданном наступлении.

ВОЗДЕЙСТВИЕ НА РИСКИ

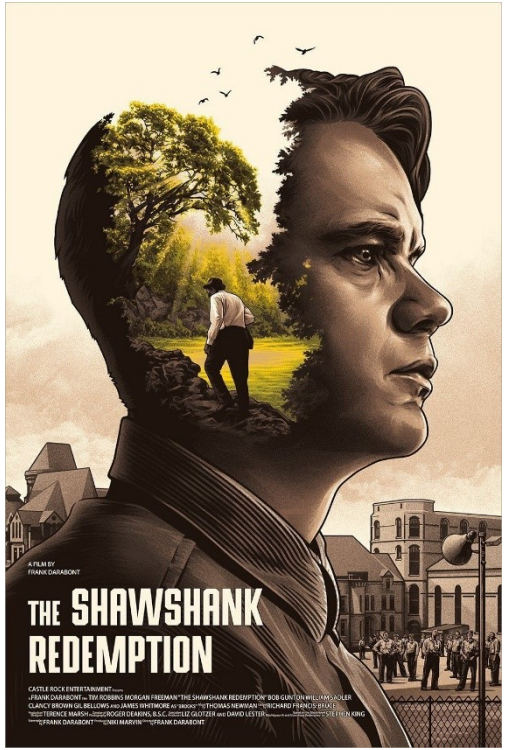
Примеры видео-кейсов плана А на канале



ВОЗДЕЙСТВИЕ НА РИСКИ



ВОЗДЕЙСТВИЕ НА РИСКИ



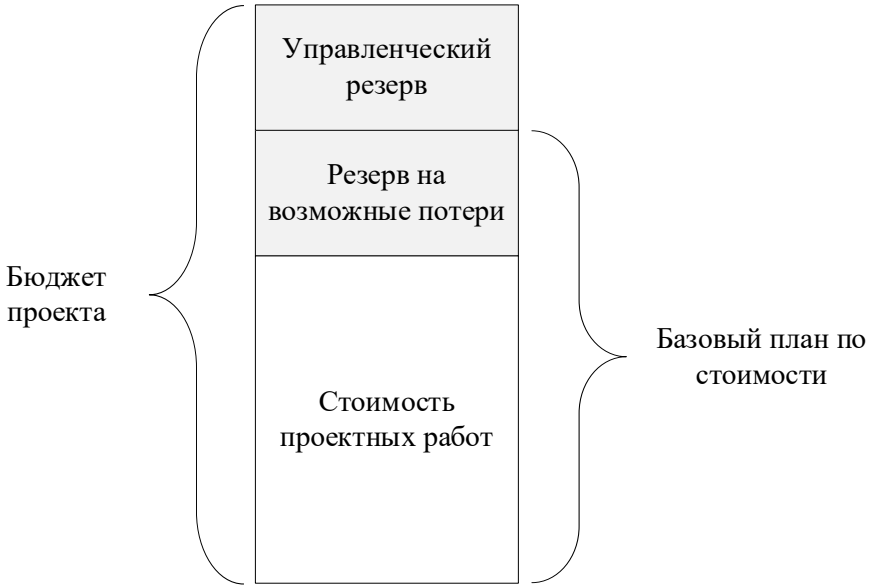
В качестве примера мер плана Б можно рассмотреть возможный уход ключевого сотрудника. Наступление этого риска, как правило, оказывает значительное негативное влияние на процесс достижения целей, поэтому для уменьшения возможного ущерба рекомендуется заблаговременно формировать денежные, временные, кадровые и управленческие резервы.

В фильмах также часто можно встретить яркие примеры применения мер плана Б. Например, в картине 1994 года **«Побег из Шоушенка»** главный герой Энди Дюфрейн смог уйти в побег только потому что он заблаговременно подготовил «тайный ход» и спрятал на счетах $370 тыс.

ВОЗДЕЙСТВИЕ НА РИСКИ

В проектах резервы мер плана Б входят в общий бюджет проекта. Более того, специалисты **PMBOK® Guide** утверждают, что успех проекта во многом зависит от правильно запланированных резервов. Например, трудовых резервов, материальных резервов, резервов на покрытие инфляции, средств на возможные потери и др. На рисунке представлена структура бюджета проекта с учетом управленческих резервов и резервов на возможные потери.

Отдельно стоит отметить управленческий резерв, который, как правило, не входит в базовый план по стоимости. **Управленческий резерв** – это сумма в бюджете проекта или временной промежуток в расписании проекта, которые зарезервированы для управленческого контроля, выполнения какой-либо непредвиденной работы либо принятия ранее неидентифицированных рисков (**рисков-невидимок**).



СТРАТЕГИИ ВОЗДЕЙСТВИЯ НА РИСКИ

Для увеличения качества разрабатываемых мер плана А и мер плана Б рекомендуется вести их имплементацию, придерживаясь определенной стратегии воздействия на риски. Под **стратегией воздействия** на риски понимается совокупность разрабатываемых мер, направленных на изменение вероятности наступления риска и возможного влияния в случае их материализации, а также иных мер, которые смогут обеспечить наиболее результативную и эффективную работу с данными рисками.

СТРАТЕГИИ ВОЗДЕЙСТВИЯ НА РИСКИ

Тип риска	Стратегия воздействия	Описание стратегии воздействия
Негативный риск	Нивелирование	Выявляются источники риска с их последующей ликвидацией
	Ослабление	Изменяются вероятность материализации риска и/или возможное влияние в случае его наступления
	Передача (страхование и хеджирование)	Риск передается третьему лицу
	Эскалация	Риск передается компетентному лицу
	Наблюдение	Активных действий в отношении риска не ведется, но осуществляется процесс мониторинга
	Принятие	Активных действий в отношении риска не ведется
Позитивный риск	Масштабирование	Увеличивается масштаб возможного благоприятного эффекта
	Усиление	Изменяются вероятность материализации риска и/или возможное влияние в случае его наступления
	Передача	Риск передается третьему лицу
	Эскалация	Риск передается компетентному лицу
	Наблюдение	Активных действий в отношении риска не ведется, но осуществляется процесс мониторинга
	Принятие	Активных действий в отношении риска не ведется

ВОЗДЕЙСТВИЕ НА РИСКИ

Ярким примером **страхования рисков** является стратегия теннисного клуба Уимблдон, который с 2003 года ежегодно платил по $2 млн. на случай наступления пандемии. В 2020 году клуб получил $141 млн.

Отметим, что по мнению И. Селиховкина, самой результативной стратегией воздействия на негативные риски является стратегия **нивелирования**. Суть данной стратегии заключается в ликвидации источников рисков. Если не будет источника риска, то не будет и самого риска. Для позитивных рисков И. Селиховкин рекомендует использовать стратегии **масштабирования** и **усиления**.

В банковской и страховой сферах встречаются специальные виды стратегий, такие как диверсификация и хеджирование. Под стратегией **диверсификации рисков** понимается перераспределение капитала между несколькими, не связанными между собой инвестиционными инструментами: акциями, облигациями, валютой, недвижимостью, криптовалютой и др. Под стратегией **хеджирования рисков** понимается перенос рисковых событий на тех, кто готов их принять. Перенос рисков осуществляется посредством заключения фьючерсных контрактов, форвардных контрактов, свопов и опционов.

МЕТОДЫ, ПРИМЕНЯЕМЫЕ ДЛЯ РАЗРАБОТКИ МЕР ВОЗДЕЙСТВИЯ НА РИСКИ

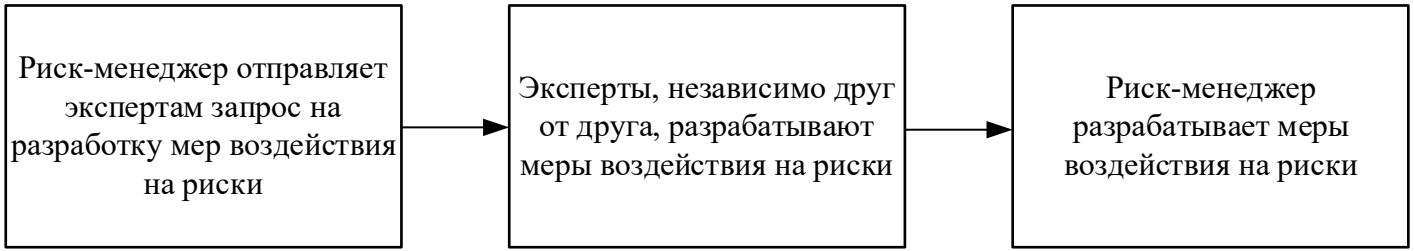
№	Название	Название (перевод на русский)	Разработчики
1	Retrospective	Ретроспективный анализ документов	В. А. Никонов, А. А. Поляков и В. О. Ключников
2	Delhi	Метод «Дельфи»	О. Хелмер, Н. Далки и Н. Ресчер
3	Brainstorming	Метод «Мозговой штурм»	А. Осборн
4	Bow-tie	Метод «Галстук-бабочка» (2-й этап)	Б. Лангминд
5	Method of Walt Disney	Метод Уолта Диснея	У. Дисней

Когда для каждого идентифицированного риска определена стратегия воздействия, далее с помощью специальных методов непосредственно разрабатываются меры плана А и плана Б.

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ ДОКУМЕНТОВ

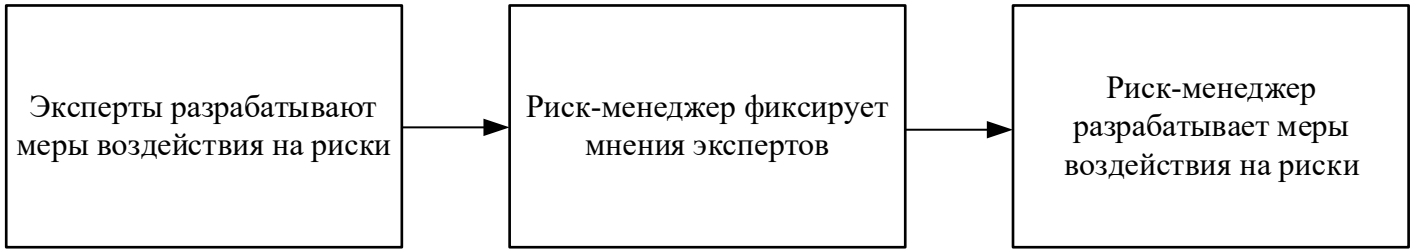
Договоры, реестры рисков, планы управления рисками ранее завершенных проектов и заключенных сделок позволяют оперативно установить наиболее результативные и эффективные меры воздействия на риски.

МЕТОД «ДЕЛЬФИ»



Как было отмечено ранее, риски условно могут быть универсальными и специальными. Для универсальных рисков применимы стандартные меры воздействия, которые могут быть установлены, например, во время проведения ретроспективного анализа документов. Так как эти меры показали свою надежность в ранее заключенных сделках и завершенных проектах, то нет необходимости создавать для них какой-либо иной механизм воздействия. Для специальных рисков ввиду их индивидуальности, напротив, требуется использование творческого подхода в процессе создания мер плана А и плана Б. Одним из методов, который использует творческое мышление экспертов, является метод «Дельфи».

МЕТОД «МОЗГОВОЙ ШТУРМ»



Результативно себя проявляет метод «Мозгового штурма» в при работе в малых группах до 6 человек. Творческая свобода и отсутствие критики дает возможность экспертам создать большое количество разнообразных мер воздействия не только для специальных рисков, но и пересмотреть механизм воздействия для универсальных рисков.

МЕТОД «ГАЛСТУК-БАБОЧКА»

Как уже было отмечено ранее, на втором этапе метода «Галстук-бабочка» разрабатываются «барьеры», которые направлены на локализацию источников рисков, и «меры восстановления (усиления)», которые призваны оперативно локализовать причиненный ущерб (усилить благоприятный эффект).

МЕТОД УОЛТА ДИСНЕЯ

Суть метода заключается в условном выделении ролей «фантазера», «критика» и «реалиста», где «фантазер» отвечает за поиск творческих идей, включая фантастические и волшебные, «критик» ищет слабые места в предложенных мерах, а «реалист» оценивает достижимость и целесообразность разработанных мер воздействия на риски.

ПЛАН УПРАВЛЕНИЯ РИСКАМИ

Помимо разработки мер плана А и плана Б в процессе воздействия на риски также рекомендуется выявлять триггерные условия. **Триггерными условиями (триггеры)** в управлении рисками называют условия, события или ситуации, которые указывают на скорую материализацию рисков. Например, если в процессе общения заказчик произнес такую фразу, как «мне это не нравится» или «чего-то тут не хватает», то эта фраза будет являться триггерным условием, которое предупреждает о том, что скоро наступит риск изменения требований.

Результаты разработки мер превентивного воздействия на риски и мер принятия рисков необходимо фиксировать в **плане управления рисками**.

ПЛАН УПРАВЛЕНИЯ РИСКАМИ

ID	Тип риска	Название риска	Стратегия воздействия	Меры превентивного воздействия	Владелец риска	Триггерные условия	Меры принятия рисков
1	Негативный	Риск изменения условий контрактов сотрудников	Ослабление	Провести переговоры с представителями Профсоюза для того, чтобы выявить их цели и интересы	ФИО	Требования от Профсоюза пересмотреть контракты сотрудников кафетерия	Привлечь юриста
2	Негативный	Риск того, что выполненная работа (оказанная услуга) не принесет ожидаемый коммерческий эффект	Ослабление	Провести обучение сотрудников	ФИО	Обратная связь от работников	Подготовить руководство пользователя программы для ЭВМ
3	Негативный	Риск того, что партнеры откажутся от сотрудничества	Ослабление	Заключение контрактов с партнерами	ФИО	Непредоставление скидки	Привлечь юриста
4	Негативный	Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям конечного пользователя	Ослабление	Подготовить спецификацию требований к программе для ЭВМ	ФИО	Обратная связь от работников	Доработка программы для ЭВМ

МОНИТОРИНГ И КОНТРОЛЬ РИСКОВ

Мониторинг рисков – это процесс, направленный на выявление ранее неидентифицированных рисков, т. е. рисков, которые не были ранее зафиксированы в реестре рисков.

Контроль рисков – это процесс наблюдения за уже идентифицированными рисками, т. е. рисками, которые были ранее зафиксированы в реестре рисков и плане управления рисками.

Стоит отметить, что оптимальным механизмом, обеспечивающим контроль рисков, являются **триггерные условия**. Именно благодаря триггерам владельцы рисков могут понять, что меры плана А не принесли ожидаемого результата и поэтому необходимо готовиться к наступлению рисков.

Процесс контроля триггерных условий индивидуален, потому что риски закрепляются за конкретным ответственным лицом. Во многом это связано с тем, что некоторые риски и их триггеры могут быть замечены только определенными работниками. Например, триггерное условие «во время тестирования была обнаружена ошибка в программном коде» риска, связанного с изменением длительности проекта, может выявить только работник, ответственный за тестирование программного кода.

МОНИТОРИНГ И КОНТРОЛЬ РИСКОВ

Сопровождение процессов мониторинга и контроля рисков посредством модели жизненного цикла риска заключается в получении ответов на следующие вопросы:

- Были ли выявлены новые ранее не идентифицированные риски?
- Были ли замечены триггерные условия для ранее идентифицированных рисков?
- Все ли запланированные цели достигнуты? Если нет, то в чем причины?
- Верно ли были выбраны стратегии воздействия на риски?
- Оказались ли меры превентивного воздействия на риски достаточно эффективными и результативными?
- Оказались ли меры принятия рисков достаточно эффективными и результативными?
- Есть ли замечания от владельцев рисков в части управления рисками?
- Если ли замечания у заинтересованных сторон в части управления рисками?