Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский Томский политехнический университет»

На правах рукописи

Николаенко Валентин Сергеевич

УПРАВЛЕНИЕ РИСКАМИ ИТ-ПРОЕКТОВ В ОРГАНИЗАЦИЯХ

08.00.05 – Экономика и управление народным хозяйством (менеджмент)

Диссертация на соискание ученой степени
кандидата экономических наук

Научный руководитель
доктор эконмических наук, профессор
И. Е. Никулина

Томск - 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Мировые и отечественные тренды перехода к постиндустриальному развитию обусловливают необходимость формирования цифровой экономики, основанной на знаниях и информационных технологиях (ИТ). Деятельность, связанная с использованием вычислительной техники и ИТ (ОКВЭД 62.0, 62.09, 63.11), цифровая валюта, нейронные сети, искусственный интеллект, интернет-банкинг, интернет-вещей, машинное обучение, цифровой документооборот, коммуникации посредствам программных продуктов являются важными элементами цифровой экономики, развитие которых требует мобилизации колоссальных финансовых, управленческих, временных, энергетических, материальных и кадровых ресурсов от всех субъектов экономической деятельности, в том числе и от государства.

Активное развитие цифровая экономика в Российской Федерации получила благородя принятым Указам Президента РФ от 09.05.2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»[1] и от 21.07.2020 года № 474 «О национальных целях развития Российской Федерации на период до 2030 года»[2], Распоряжению Правительства РФ от 28.06.2017 года № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”»[3] и Постановлению Правительства РФ от 02.03.2019 года № 234 «О системе управления реализацией национальной программы "Цифровая экономика

[1] Официальный сайт Президента Российской Федерации. Указ Президента Российской Федерации №203 от 9 мая 2017 года «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» [Электронный источник]. – URL: https://clck.ru/EXaJo (дата обращения 30.03.2021 г.).

[2] Официальный сайт Российской Газеты. Указ Президента Российской Федерации от 21 июля 2020 г. N 474 «О национальных целях развития Российской Федерации на период до 2030 года» [Электронный источник]. – URL: https://clck.ru/UE769 дата обращения 30.03.2021 г.).

[3] Официальный сайт Правительства Российской Федерации. Распоряжение Правительства Российской Федерации №1632-р от 27 июля 2017 года «Об утверждении программы Цифровая экономика Российской Федерации» [Электронный источник]. – URL: https://clck.ru/EhDkh (дата обращения 30.03.2021 г.).

Российской Федерации"»[4], в рамках которых планируется создать комплекс цифровых продуктов и сервисов, которые в будущем станут основой электронного государства и электронного правительства. Кроме того, необходимо отметить, что 01.01.2021 года вступил в силу Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[5], главными задачами которого являются регулирование отношений, которые возникают при выпуске и обращении цифровых финансовых активов, а также отношения при обороте цифровой валюты на территории РФ.

В октябре 2020 года Банк России выступил с предложением о выпуске новой цифровой валюты – цифрового рубля, который по плану должен стать следующим шагом в развитии цифровизации отечественной экономики. За основу взят передовой опыт Центрального банка Китайской Народной Республики, который намерен полностью отказаться от наличных денег и в ближайшие годы выпустить цифровую версию юаня.

Министерством экономического развития Российской Федерации предполагается, что цифровые продукты и сервисы будут все больше проникать в стратегически важные сектора отечественной экономики, в частности, металлургический и горнодобывающий сектор, финансовый сектор, нефтегазовый сектор, энергетический сектор, потребительский сектор, телекоммуникационный сектор, интегрироваться в системы производств пищевых продуктов, оборудования, машин др. Например, в 2022 году прогнозируется, что около 70% отечественных организаций,

---

[4] Официальный сайт Правительства Российской Федерации. Постановление Правительства Российской Федерации от 2 марта 2019 года № 234 «О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации"» [Электронный источник]. – URL: https://clck.ru/UE7CM (дата обращения 30.03.2021 г.).

[5] Официальный интернет-портал правовой информации. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный источник]. – URL: https://clck.ru/UE7F8 (дата обращения 30.03.2021 г.).

предприятий и государственных учреждений перейдут на облачные технологии, в 2023 году будут разработаны более 500 млн. новых цифровых приложений для всех сфер экономической деятельности, в 2024 году 50% имеющегося оборудования должно будет оснаститься компьютерным зрением, средствами виртуальной и дополненной реальности, в 2025 году около 90% цифровых приложений должны будут использовать алгоритмы нейронных сетей и искусственного интеллекта.

Однако несмотря на стремительно ускоряющуюся интеграцию ИТ-продуктов и ИТ-сервисов во многие сектора отечественной экономики, сегодня успешное проектирование, реализация и внедрение подобных продуктов и сервисов являются трудновыполнимыми задачами. Например, согласно данным международной консалтинговой компании The Standish Group (The SG), доля успешных ИТ-проектов, как правило, не превышает 30%. По мнению экспертов The SG низкие показатели обусловлены отсутствием результативного и эффективного инструментария управления ИТ-проектами и рисками в них.

Исходя из вышесказанного можно сделать вывод, что отечественным государственным учреждениям, коммерческим и некоммерческим организациям для успешного завершения национальных ИТ-проектов, например, «Государственная информационная система ”Моя школа”», «Автоматизированная система управления транспортным комплексом», «Информационная система обмена знаниями и технологиями в сфере сельского хозяйства», «Информационная система социального обеспечения» и др., необходим результативный и эффективный инструментарий управления рисками в ИТ-проектах, который бы мог гарантировать их успешное завершение.

Необходимо отметить, что несмотря на актуальность и востребованность подобного инструментария, методологические подходы управления рисками для области ИТ в Российской Федерации остаются недостаточно проработанными. С одной стороны, это может быть объяснено

отсутствием накопленных лучших отечественных практик управления рисками, с другой стороны – недостаточно высоким развитием риск-ориентированного управления в государственных учреждениях, коммерческих и некоммерческих организациях.

Таким образом, можно сделать вывод – в отечественной сфере информационных технологий существует острая проблема, связанная с недостаточной проработкой применяемого инструментария управления рисками ИТ-проектов в организациях, что и обусловило актуальность и научно-практическую значимость темы настоящего диссертационного исследования.

Степень научной проработанности проблемы. Существенный вклад в развитие теории риска среди отечественных ученых внесли А. Н. Павлов, Н. В. Фадейкина, В. Ю. Королев, В. Е. Бенинг, С. Я. Шоргин, А. Г. Мадера, Р. М. Качалов. Среди зарубежных исследователей природы риска можно упомянуть А. Маршалла, который одним из первых рассмотрел проблемы, связанные с экономическими рисками, Дж. М. Кейнса, первого исследователя предложившего систему классификации инвестиционных рисков. Кроме того, значительный вклад в развитие риск-менеджмента внесли такие ученые, как Ф. Х. Найт, О. Моргенштерн и Дж. Нейман, установившие связь между понятиями «риск» и «неопределенность» благодаря применению теории вероятностей, Д. Кардано, Б. Паскаль и Ф. Ферма, разработавшие математический аппарат сложения вероятностей, Х. Гюйгенс, сформулировавший принципы математического ожидания, Э. Галлей, заложивший основы статистики, Э. Ллойд, разработавший меры ослабления влияния от материализации морских рисков, Д. С. Милль, обосновавший экономические принципы платы за риск, И.Г. фон Тюнен, рассмотревший сущность инновационных рисков.

К теме настоящего диссертационного исследования близки труды отечественных и зарубежных ученых, таких как О. В. Трофимов, О. В. Макушева, Л. А. Горшкова, И. В. Гуськова, А. В. Золотов,

Д. А. Корнилов, М. Д. Лапаев, С. Н. Яшин, И. Т. Балабанов, Ю. П. Ехлаков, В. О. Ключников, Н. Б. Ермасова, В. А. Никонов, Е. Ю. Песоцкая, С. Элтер, М. Гинзберг, Р. В. Змуд, Б. В. Боем, Х. Барки, С. Ривард, Д. Тэлбот, К. Лютинен, Л. Мавиасен, Д. Ропонен, К. Де Бэкер, Т. Демарко, Т. Листер, М. Кейл. Например, С. Элтер и М. Гинзберг в работе, опубликованной в 1970-х гг., высказали мысль о том, что вероятность успеха проекта может быть увеличена, если провести идентификацию ключевых факторов отвечающих за неопределенность. Б. В. Боем рассматривает основные риски, которые присутствуют в долгосрочных ИТ-проектах. Х. Барки, С. Ривард, Д. Тэлбот и К. Лютинен, Л. Мавиасен, Д. Ропонен исследуют влияние риск-менеджмента на процесс достижения запланированных целей в ИТ-проектах. К. Де Бэкер эмпирически устанавливает, что успешное завершение ИТ-проектов зависит от эффективного риск-менеджмента. Т. Демарко и Т. Листер приходят к выводу, что основным источником негативных рисков является человеческий фактор. Ю. А. Макушева обозначает проблематику киберугроз и информационной безопасности для организаций. О. В. Трофимов, И. В. Гуськова, А. В. Золотов, Д. А. Корнилов, Д. Н. Лапаев, С. Н. Яшин оценивают возможные угрозы и опасности в условиях развития цифровой экономики в Российской Федерации для отечественных организаций.

Рассмотренные работы упомянутых выше авторов внесли существенный вклад в развитие теории и практики управления рисками, однако анализ научных трудов показал, что особенности и специфика управления рисками в сфере информационных технологий была недостаточно проработана.

Таким образом, актуальность и недостаточная проработанность теоретических, методических и практических аспектов оценки рисков в сфере ИТ определили постановку цели и задач настоящего диссертационного исследования.

В качестве исходной научной гипотезы исследования выдвинуто предположение о том, что разработка и функционирование ИТ-проектов

происходит под воздействием как негативных, так и позитивных рисков, существенно влияющих на запланированные проектные цели, которые могут быть оценены посредством специфического инструментария управления ими.

Цель диссертационного исследования – создание инструментария управления рисками ИТ-проектов в организациях, включающего в себя идентификацию, анализ, оценивание вероятностей материализации рисков и их возможного влияния в случаях наступления, мониторинг и контроль рисков, а также разработку мер превентивного воздействия (мер «плана А») и мер принятия рисков (мер «плана Б»).

Для достижения поставленной цели автором настоящего диссертационного исследования были поставлены и решены следующие **задачи**:

1) проанализированы наиболее популярные способы управления ИТ-проектами и рисками в них;

2) идентифицированы характерные особенности управления рисками в ИТ-проектах;

3) исследованы основные методы и способы оценки, воздействия, мониторинга неидентифицированных рисков и контроля идентифицированных рисков в ИТ-проектах;

4) создан инструментарий оценки, воздействия, мониторинга неидентифицированных и контроля идентифицированных негативных и позитивных рисков ИТ-проектов в организациях;

5) апробирован созданный инструментарий управления рисками в ИТ-проектах в семи ИТ-организациях.

Объектом исследования выступают организации, занимающиеся проектированием, реализацией и управлением ИТ-проектов, в контексте воздействия на их проектную деятельность различных рисков.

Предметом исследования являются экономические отношения, возникающие в организациях при управлении ИТ-проектами и рисками в них.

Теоретической и методологической основой диссертационного исследования являются теория риска, финансовый менеджмент, проектный менеджмент, риск-менеджмент, стратегический менеджмент, а также антикризисный менеджмент.

Для решения поставленных задач и обоснования научных результатов диссертационного исследования использовались следующие методы познания: наблюдение; анализ; синтез; сравнение; индукция; дедукция; классификация; опрос; эксперимент; статистические методы; экспертное интервью; фокус-групповые дискуссии и др.

Информационную базу исследования составили: ФЗ № 254 от 21 июля 2011 года «О внесении изменений в Федеральный закон «О науке и государственной научно-технической политике»[6]; Приказ Минкомсвязи России № 96 от 1 апреля 2015 года «Об утверждении плана импортозамещения программного обеспечения»[7]; Постановление Правительства Российской Федерации № 1236 от 16 ноября 2015 года «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»[8]; Постановление

---

[6] Официальный сайт Президента Российской Федерации. Федеральный закон от 21.07.2011 г. № 254-ФЗ «О внесении изменений в Федеральный закон “О науке и государственной научно-технической политике”» [Электронный источник]. – URL: https://clck.ru/UE7LD (дата обращения 30.03.2021 г.).

[7] Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Приказ № 96 от 1 апреля 2015 года Минкомсвязи России «Об утверждении плана импортозамещения программного обеспечения» [Электронный источник]. – URL: https://clck.ru/UE7PE (дата обращения 30.03.2021 г.).

[8] Официальный сайт Правительства Российской Федерации. Постановление Правительства Российской Федерации № 1236 от 16 ноября 2015 года «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения

Правительства РФ №57 от 27 января 2017 года «О создании Российского фонда развития информационных технологий»[9]; Указ Президента РФ №203 от 9 мая 2017 года «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»; стандарты ГОСТ 34.201-89 «Информационная технология»; ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения»; ГОСТ 9126 «Информационная технология. Оценка программного продукта»; ГОСТ Р ИСО/МЭК 15271-02 «Процессы жизненного цикла программных средств»; ГОСТ 19.102-77 «Стадии разработки»; IRM; стандарт ГОСТ Р ИСО 31000-2010 «Менеджмент риска. Принципы и руководство» (ISO 31000); ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска»; ГОСТ Р 14.09-2005 «Экологический менеджмент. Руководство по оценке риска в области экологического менеджмента»; ГОСТ Р 51901.3-2007 «Менеджмент риска. Руководство по менеджменту надежности»; ГОСТ Р 51901.12-2007 «Менеджмент риска. Метод анализа видов последствий отказов»; ГОСТ Р ИСО/МЭК 16085-2007 «Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения»; ГОСТ Р 51901.10-2009 «Менеджмент риска. Процедуры управления пожарным риском на предприятии»; ГОСТ Р 51901.21-2012 «Менеджмент риска. Реестр риска. Общие положения»; PMBOK® Guide; PRINCE2®; M_o_R®; ISO 31000:2018 Risk management – Guidelines; аналитические обзоры и материалы отечественных и зарубежных исследовательских центров в областях управления проектами и управления рисками; научные статьи, материалы научных семинаров, симпозиумов, конференций и монографии.

Достоверность и обоснованность научных положений, выводов, результатов и рекомендаций исследования подтверждается и

государственных и муниципальных нужд» [Электронный источник]. – URL: https://clck.ru/UE7Re (дата обращения 30.03.2021 г.).

[9] Официальный сайт Правительства Российской Федерации. Постановление Правительства Российской Федерации №57 от 27 января 2017 года «О создании Российского фонда развития информационных технологий» [Электронный источник]. – URL: https://clck.ru/UE7Uh (дата обращения 30.03.2021 г.).

обеспечивается полнотой анализа теоретических и практических разработок по теме исследования, опубликованными научными работами в научных журналах, входящих в перечень рецензируемых научных изданий ВАК и базы данных Web of Science и Scopus, положительными оценками докладов автора диссертационного исследования на научных международных научно-практических конференциях, справками о внедрении результатов исследования, а также патентом №121649 на промышленный образец.

Соответствие настоящего диссертационного исследования паспорту научной специальности Высшей аттестационной комиссии. Исследование выполнено в рамках специальности 08.00.05 – Экономика управления народным хозяйством (менеджмент): п.10.11. «Управление проектом. Риск-менеджмент».

Научная новизна результатов исследования заключается в выявлении, с учетом особенностей функционирования ИТ-проектов, негативных и позитивных рисков, разработке теоретических положений и практических рекомендаций по управлению рисками ИТ-проектов, которые дополняют знания проектного управления и риск-менеджмента.

Наиболее существенные положения и научные результаты, полученные лично автором и выносимые на защиту:

1) Уточнена сущность и дополнено содержание понятия «управление рисками в ИТ-проектах», трактуемое, как совокупность процессов по оценке негативных (позитивных) рисков, принятия управленческих решений по разработке мер воздействия, мониторинга неидентифицированных рисков и контроля идентифицированных рисков, где под термином «риск» понимается возможное событие, которое порождается конкретными источниками (источниками риска), наступление которого под воздействием определенных факторов (факторов риска) способно оказать негативное (позитивное) влияние на запланированные проектные цели, стимулируя материализацию проблемных (благоприятных) ситуаций. Предложенная дефиниция понятия «управление рисками в ИТ-проектах»

существенно отличается от ныне существующих, так как включает в себя понятие «позитивный риск», управление которым может положительно влиять на план проекта и на проектные цели (содержание, длительность, стоимость и качество проекта) предвосхищая ранее запланированные результаты.

2) Разработана классификация рисков, базирующаяся на классификационных признаках актуальных для ИТ-проектов, таких как среда, внешний и внутренний источники проектного риска, проектная цель, фаза жизненного цикла ИТ-проекта, срочность риска, негативный и позитивный аспекты проектного риска, а также уровень управления риском. Предложенная классификация рисков ИТ-проектов в организациях способствует обнаружению специфических и скрытых рисковых событий в ИТ-проектах, стимулирует развитие стандартизации мер управленческого воздействия на риски, улучшает мониторинг и контроль рисков, а также рационализует функцию планирования управления ИТ-проектами.

3) Сформирована методика определения времени актуализации (материализации) рисков относительно фаз жизненного цикла ИТ-проекта с выявлением постоянных рисков, способных материализоваться на любом этапе реализации ИТ-проекта. Предлагаемый методический инструментарий дает возможность получать исчерпывающую информацию о возможных событиях способных оказать значительное воздействие на проектные цели, а также идентифицировать временные периоды ИТ-проектов, которые представляют наибольшую угрозу.

4) Обоснован способ группировки позитивных рисков с представлением в нем: «слонов», как созидательных рисков; «львов», как непредсказуемых рисков; «обезьян», как часто встречаемых рисков; «кроликов», как незначительных рисков. Данный способ группировки позитивных рисков совершенствует и дополняет классическую группировку рисков, позволяет определять позитивные риски требующие дополнительных стимулирующих мер воздействия, получать информацию о

позиционировании позитивных рисков друг относительного друга и идентифицировать наиболее значимые позитивные рисковые события, что существенно сокращает материальные и временные затраты на управление рисками ИТ-проектов в организациях.

5) Разработан инструментарий управления рисками ИТ-проектов, который применим для проектов различной длительности, типов, численности проектных коллективов, а также способов управления ИТ-проектами, учитывающий негативные и позитивные аспекты природы риска, оперативно реализующий базовые процессы риск-менеджмента, снижающий отклонение фактических трудозатрат от запланированных, что является основанием для приращения научных знаний в области риск-менеджмента и дополнения ГОСТа Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство».

Теоретическая значимость настоящего диссертационного исследования заключается в развитии теоретических положений риск-менеджмента ИТ-проектов в организациях в части уточнения понятий «риск», «неопределенность» и «риск-менеджмент», в разработке классификации рисков в ИТ-проектах, в создании способа ранжирования и группировки позитивных рисковых событий улучшающего процесс оценивания риск-менеджмента, в разработке способа определения времени актуализации (материализации) рисков относительно фаз жизненного цикла, который позволяет определять наиболее опасные временные периоды.

Практическая значимость настоящего диссертационного исследования заключается в создании инструментария оценки негативных и позитивных рисков, разработки мер воздействия, мониторинга неидентифицированных рисков и контроля идентифицированных рисков в ИТ-проектах; классификации рисков ИТ-проектов в организациях, создании иерархических структур негативных и позитивных рисков для ИТ-проектов, применении способа актуализации рисков относительно фаз жизненного цикла в ИТ-проектах, разработке рекомендаций по использованию риск-

менеджмента в ИТ-проектах, дополнение новыми знаниями ГОСТа Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство». Основные результаты диссертационного исследования могут использоваться руководителями ИТ-проектов и руководителями ИТ-организаций, в научных исследованиях цифрового менеджмента, в учебных курсах «Управление проектами», «Риск-менеджмент», «Стратегический менеджмент» и «Цифровой менеджмент».

Апробация результатов настоящего диссертационного исследования. Полученные результаты обсуждались на: Международной научно-практической конференции «Синергия науки и практики в контексте инновационных прорывов в развитии экономики и общества: национальный и международные аспекты», г. Санкт-Петербург, 2019 г.; Конференции лауреатов и стипендиатов 2019 года. Международного научного фонда экономических исследований академика Н.П. Федоренко (МНФЭИ), г. Москва, 2019 г.; Международной молодежной конференции по управлению знаниями «Управление знаниями в цифровой экономике», г. Москва, 2018 г.; I Междисциплинарной Всероссийской научно-практической конференции «Развитие методологии современной экономической науки и менеджмента», г. Севастополь, 2017 г.; Ежегодной международной научно-практической конференции «Современные проблемы и тенденции развития экономики, управления и информатики в XXI веке», г. Санкт-Петербург, 2015 г.; V Юбилейной Всероссийской научно-практической конференции студентов, аспирантов, молодых ученых с международным участием «Актуальные вопросы экономики и менеджмента: свежий взгляд и новые решения», г. Томск, 2014 г.; Международной конференции «Информационные технологии в науке, управлении, социальной сфере и медицине-2014», г. Томск, 2014 г.

Диссертационное исследование поддержано: Российским фондом фундаментальных исследований (РФФИ) – «Мой первый грант» по теме «Управление рисками в ИТ-проектах» (16-36-00031 мол_а); Международным

научным фондом экономических исследований академика Н.П. Федоренко по теме «Разработка отечественного стандарта управления рисками на базе ГОСТ Р ИСО 31000:2010-Менеджмент риска».

Основные научные положения и результаты диссертационной работы рассмотрены, одобрены и внедрены хозяйствующими субъектами сферы информационных технологий, такими как ООО «Синтез Интеллектуальных Систем», ООО «ЛидерГрупп», ООО «Спейс-О технологии», ООО «Аксимедиа Софт», ООО «Телебриз», ООО «Контек Софт», ООО «Сибэйдж». Результаты апробации подтверждены справками об использовании результатов диссертационного исследования.

Кроме того, результаты диссертационного исследования защищены патентом на промышленный образец №121649 «Игровое поле настольного тренажера проектной деятельности» Федеральной службы по интеллектуальной собственности (Роспатент).

Публикации результатов исследования. Основные результаты настоящего диссертационного исследования опубликованы в 20 научных работах общим объемом 34,1 печатных листов, из них 12 научных работ опубликованы в журналах рекомендованных ВАК, 2 научных работы опубликованы в изданиях входящих в базы данных Web of Science и Scopus.

Структура и объем работы. Во **введении** обоснована актуальность, новизна и значимость темы диссертационного исследования, сформулированы гипотеза, цель и задачи, представлены основные результаты научного исследования.

В **первой главе** показано современное состояние и развитие сферы информационных технологий в мире и России. Представлены результаты анализа отечественных и зарубежных сводов лучших практик и стандартов управления проектами и рисками. Уточнены понятия «риск», «неопределенность» и «управление рисками». Описан способ классификации рисков, актуальных для проектов создаваемых в сфере информационных технологий.

Вторая глава посвящена рассмотрению адаптированных методов и способов идентификации, анализа, оценивания, воздействия, мониторинга и контроля рисков для сферы ИТ. Кроме того, во второй главе продемонстрированы иерархические структуры негативных и позитивных рисков, актуальных для ИТ-проектов, представлен способ группировки позитивных рисков, а также описан инструментарий по определению времени актуализации негативных и позитивных рисков относительно фаз жизненного цикла ИТ-проекта.

В **третьей главе** представлены результаты анализа бизнес-деятельности и финансовое состояние 7 субъектов, где проходила апробация разработанного инструментария управления рисками.

В **заключении** сформулированы основные результаты проделанной работы и описаны направления дальнейших исследований.

Текст диссертационной работы изложен на 192 страницах и включает в себя 44 таблицы, 22 рисунка и 11 приложений. Список литературы состоит из 227 источников.

Глава 1. АНАЛИЗ ТЕОРЕТИЧЕСКИХ И ПРАКТИЧЕСКИХ СПОСОБОВ УПРАВЛЕНИЯ РИСКАМИ В ИТ-ПРОЕКТАХ

1.1. Направление развития рынка цифровых технологий в мировой и отечественной экономике

Первая радиосистема, разработанная Александром Степановичем Поповым и продемонстрированная 7 мая 1895 г. на заседании Русского физико-химического общества в Петербурге, дала мощный старт развитию нового направления «связь». Радио решало одну из важнейших и актуальных задач того времени, оперативно обеспечивая беспроводную передачу большего объема данных. Применение подобной технологии давало неоспоримое преимущество, как в экономических, так и в военных сферах, что стимулировало активный рост радиотехники и радиотехнических дисциплин. Обеспечение новой коммуникационной функций потребовало создания государственных органов и институтов. Например, 15 марта 1946 года было инициировано создание Наркомата связи СССР [1].

С 12 мая 2008 года за развитие данной отрасли было ответственно Министерство связи и массовых коммуникаций Российской Федерации, которое в мае 2018 года переименовано в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [2].

Современная цифровая связь, помимо распространения информации, также включает в себя хранение, управление, обработку и защиту информационных данных. Выполнение данных функций происходит с помощью электронных вычислительных машин (ЭВМ) и информационных систем (ИС). Отметим, что технологии работающие с информационными данными, развивающие и эксплуатирующие ИС в литературе именуют информационными технологиями (ИТ) [3].

Информационные и коммуникационные технологии, глобальные информационные сети, персональные компьютеры и Интернет стали

неотъемлемой частью многих отечественных организаций. ЭВМ, локальные вычислительные сети, электронная почта, веб-сайты в современных коммерческих и некоммерческих организациях являются ключевыми инструментами, которые позволяют получать, анализировать и хранить информацию, организовывать и контролировать бизнес-деятельность, осуществлять электронные платежи, вести удаленную работу, а также проводить переговоры не ограничиваясь территориальными границами. Например, по данным Федеральной службы государственной статистики Российской Федерации число персональных компьютеров в обследованных организациях в 2017 году по сравнению с 2013 годом увеличилось на 1 327,9 тыс. шт. (таблица 1.1) [4].

Таблица 1.1 – Число персональных компьютеров в организациях Российской Федерации [4]

Число персональных компьютеров	**2013**	**2014**	**2015**	**2016**	**2017**
в организациях (тыс. шт.)	11438,0	11740,8	11992,3	12422,1	12765,9
подключенные к Интернет	7220,8	8157,5	8362,0	8782,2	9246,2

Масштабная интеграция с цифровыми продуктами и сервисами сегодня наблюдается во всех секторах отечественной экономики. Например, современные коммерческие и некоммерческие организации, государственные учреждения уже активно используют такие программные продукты, как 1С «Заплата и управление персоналом» [5], 1С «Предприятие», 1С «Бухгалтерия», БОСС-Кадровик [6], ИНЭК-Персонал [7], Отдел кадров плюс [8], Assessment Tools [9], Oracle [10], АиТ [11], Платон [12], ЕГАИС [13] и др., формируя основу для создания и развития цифрового государства, цифрового правительства и цифровой экономики.

Эксплуатация подобных цифровых систем оказывает значительное позитивное влияние на бизнес-деятельность коммерческих и некоммерческих организаций, в частности [14]:

- экономит рабочее временя сотрудников, автоматизируя процессы и операции [15];
- повышает качество принимаемых управленческих решений;
- увеличивает производительность труда;
- предоставляет возможность удаленного управления;
- обеспечивает круглосуточный контроль и мониторинг.

CNews Analitics и Gartner в своих аналитических отчетах приходят к выводу, что тренд автоматизации бизнес-процессов и дальнейшее развитие цифровизации в ближайшие 10 лет приведет к тому, что каждый крупный, средний и малый бизнес будет нуждаться в своих собственных уникальных информационных системах, что потребует от ИТ-рынка надежных способов управления проектами и развитого сектора ИТ-услуг [16, 17].

Согласно отчетам Министерства экономического развития Российской Федерации структура отечественного ИТ-рынка разделена на три группы: ИТ-оборудование – 57% ; ИТ-услуги – 24%, разработка и продажа ПО – 19% [18]. Содержание ИТ-рынка России отличается от мировой структуры [19]. Например, в США доля ИТ-оборудования составляет около 28%, ИТ-услуг – 43%, разработка и продажа ПО – 29% [20]. Развитый сектор ИТ-услуг в США свидетельствует о высоком уровне зрелости в областях проектного управления и заказной разработки, что подтверждается стабильным ростом доходности и капитализации ИТ-гигантов, таких как Alphabet, Abobe, Apple, Electronic Arts, Facebook, Microsoft, Twitter, Baidu, Cisco Systems, Activision Blizzard, Amazon, Oracle и др.

Для стимулирования развития отечественного ИТ-рынка и сектора ИТ-услуг, а также биомедицинских, космических, телекоммуникационных, энергоэффективных и ядерных технологий в 2010 году Президентом РФ

было инициировано создание нового инновационного центра «Сколково» [21]. Кроме того, 21 июля 2011 года вступил в силу Федеральный закон РФ № 254-ФЗ «О внесении изменений в закон “О науке и государственной научно-технической политике”», в котором говорится о государственной поддержке по стимулированию развития инноваций [22]. Так с 2011 года благодаря участию государства в России была создана благоприятная среда и условия для активного развития сферы информационных технологий.

Однако в 2014 году ситуация изменилась. Обострение международных отношений привело к санкционированию, блокированию и ограничению отечественных ИТ-компаний и их ИТ-продуктов. Например, в 2014 году платежные системы Visa и Mastercard перестали принимать карты отечественных банков, которые попали под санкции, вызванных присоединением Крыма. Данный аспект негативно сказался на отечественном ИТ-рынке. Например, в отчетах аналитического агентства IDC сказано, что в 2016 году ИТ-отрасль в России сократилась на 40% [19].

1 апреля 2015 года в целях ослабления негативного влияния политических факторов Минкомсвязь РФ был разработан план импортозамещения ПО [23]. План включает в себя [23]:

- предоставление льгот отечественной ИТ-продукции;
- обеспечение правовой поддержкой отечественных ИТ-компаний;
- налоговое, кредитное и грантовое стимулирование ИТ-компаний,

которые заняты созданием ПО для металлургического и горнодобывающего сектора, финансового сектора, нефтегазового сектора, энергетического сектора, потребительского сектора, телекоммуникационного сектора и транспортного сектора. Например, благодаря государственному участию в 2014 году была запущена национальная система платежных карт «МИР», которая сегодня активно используется не только на территории РФ, но и в станах СНГ, Турции и Вьетнаме.

16 ноября 2015 года основные положения Приказа № 96 были усилены Постановлением Правительства Российской Федерации № 1236 «Об

установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [24].

1 января 2016 года вступил в силу Федеральный закон № 188-ФЗ О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»[10] и статья 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [25]. Главной задачей принятого закона и поправок к нему является регулирование деятельности государственного заказчика при выборе ПО, представленного в едином реестре российских программ для электронных вычислительных машин и баз данных [26].

27 января 2017 года Постановлением Правительства РФ №57 было инициировано создание Российского фонда развития информационных технологий [27].

9 мая 2017 года Президентом РФ был издан Указ № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», где закрепляются основные положения Стратегии и стратегические национальные приоритеты РФ в развитии информационного общества [28].

27 июля 2017 года Правительство РФ издает Распоряжение № 1632-р от «Об утверждении программы “Цифровая экономика Российской Федерации”» [29, 30, 31], где формализуются основные вехи и этапы дорожной карты формирования и развития цифровой экономики РФ [32, 33, 34].

[10] Официальный сайт Президента Российской Федерации. Федеральный закон от 29.06.2015 г. № 188-ФЗ О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [Электронный источник]. – URL: https://clck.ru/UE7mE (дата обращения 30.03.2021 г.).

Анализируя современные тренды сферы информационных технологий можно идентифицировать 4 основных сценария развития ИТ-отрасли в Российской Федерации:

1. *открытый рынок.* Если и далее государство будет стимулировать развитие информационных технологий, то высока вероятность того, что отечественные ИТ-продукты смогут провести экспансию на глобальном рынке [35];

2. *особый путь.* Если в отношениях с другими странами произойдет обострение, тогда Россия будет вынуждена ограничить импорт цифровых технологий и понизить зависимость от иностранного ПО до 50% [35];

3. *потерянное десятилетие.* Ухудшение международных отношений, экономические санкции, отсутствие государственной поддержки и отток ИТ-специалистов может лишить Россию собственной ИТ-продукции и остановить развитие сферы информационных технологий на десятки лет;

4. *неприемлемый путь.* Полная интеграция России в мировую экономику только в качестве потребителя ИТ-продуктов.

Из представленных выше сценариев можно заключить, что успешное развитие отечественной ИТ-отрасли не представляется возможным без активной государственной поддержки, лоббирования, протекции и защиты.

Автор диссертационного исследования считает, что реализация программы по импортозамещению зарубежного ПО отечественным не решит всех проблем, т. к. появление на рынке новых ИТ-решений зависит не только от государственного участия. Разработка цифровых продуктов и сервисов – это сложный процесс, требующий применения наукоемкой техники и привлечения большого количества специализированных кадров. Например, в 2019 году штат американской ИТ-компании «Alphabet», бенефициар «Google», «YouTube» и «Android», насчитывал 114 096 сотрудников, а количество сотрудников отечественной ИТ-компании ООО «Яндекс» достигло всего 10 092 сотрудников.

Кроме того, необходимо отметить, что отсутствие материальной базы и инфраструктуры создания микрочипов, низкий уровень зрелости отечественных высокотехнологичных компаний, разрабатывающих сложные интеллектуальные продуты, порождает множество факторов рисков, значительно уменьшающих вероятность успешных исходов для отечественных ИТ-проектов [36].

Поиском решения проблемы низкой доли успешно завершенных ИТ-проектов в США заняты последнее 10 лет. Например, The Standish Group с 2011 года ежегодно проводит исследование в США, Европе и других странах и определяет долю успешно завершенных ИТ-проектов, их факторы успеха, а также идентифицирует основные проблемы, которые не позволили достичь запланированных проектных целей. (таблица 1.2) [37]

Таблица 1.2 – Успешные ИТ-проекты, незавершенные ИТ-проекты и ИТ-проекты, в которых были проблемы с 2011 по 2015 г. [37]

Статус ИТ-проекта	**2011**	**2012**	**2013**	**2014**	**2015**
Успешные ИТ-проекты	29%	27%	31%	28%	29%
Незавершенные ИТ-проекты	22%	17%	19%	17%	19%
ИТ-проекты, в которых были проблемы	49%	56%	50%	55%	52%

О. Ли и Д. Бэби в своих трудах приходят к выводу, что ИТ-проекты подвержены значительному влиянию внешних (политика, экономика, бизнес-окружение и др.) и внутренних факторов (персонал, технологии и др.). В связи с чем вероятность успешного завершения ИТ-проектов очень мала [38].

Эксперты Ernst & Young (EY) считают, что на успех в ИТ-проектах зависит от таких факторов, как макроэкономика (курс рубля, цена на энергоресурсы, процентная ставка рефинансирования), рынок, государство (налоговые, таможенные и тарифные ставки), научное сообщество, люди, экспорт и импорт [35].

Осмысление результатов, полученных в ходе анализа трендов развития мирового и отечественного рынков информационных технологий, позволило сформулировать следующие выводы:

- *во-первых*, в мире и в России наблюдается ориентация организаций и государственных учреждений на цифровизацию [39];
- *во-вторых*, отечественный ИТ-рынок значительно подвержен влиянию извне, что подтверждается закрытием доступа к важной информации, прекращением обслуживания ключевых банковских, управленческих, образовательных и социальных ИТ-сервисов, а также утечкой секретных данных в результате ИТ-шпионажа;
- *в-третьих*, выбранная РФ стратегия по импортозамещению программного обеспечения, защите информации, развитию информационного общества, созданию цифровой экономики включает в себя реализацию множества крупных национальных ИТ-проектов;
- *в-четвертых*, базируясь на опыте США и стран Европы в ИТ-сфере, можно предположить, что в лучшем случае только 30% запланированных крупных отечественных ИТ-проектов будут успешными по причине наступления непредвиденных внешних и внутренних негативных рисков, что в современных экономических условиях является неприемлемым и недопустимым.

Исходя из этого можно заключить, что для обеспечения условий успешного завершения национальных ИТ-проектов и реализации Стратегии развития информационного общества в РФ, программы развития цифровой экономики РФ, плана по импортозамещению ПО требуется углубленное изучение вопроса сопряженного с современными подходами к управлению ИТ-проектами в организациях и управлению рисками в них.

1.2. Эволюция теории и практики управления проектами

Свод лучших практик проектного управления PMBOK® Guide определяет **«проект»**, *как уникальный процесс, создающий уникальные продукты и (или) услуги, имеющий ограниченные ресурсы, а также фиксированные даты начала и окончания* [40, 41, 42, 43]. Таким образом, **«ИТ-проект»** может быть определен, как *уникальный процесс, создающий уникальные ИТ-продукты и (или) ИТ-услуги, имеющий ограниченные ресурсы, а также фиксированные даты начала и окончания*.

Исследования показывают, что инструментарий управления проектами существует несколько тысяч лет, но активное развитие и свою конечную форму проектная деятельность приобрела в начале 20-го века, когда возникла потребность в оперативной реализации сложных проектов (запуск военно-космических аппаратов, строительство высотных зданий и сооружений, эксплуатация атомных станций, прокладка магистралей железных дорог и др.).

Накопленный практический опыт реализации подобных проектов со временем инициировал создание международных объединений по всему миру, которые стали заниматься вопросами повышения результативности и эффективности проектного управления. Примерами подобных объединений являются IPMA (Швейцария) [44], PMI (США) [45], СОВНЕТ (СССР), APM (Великобритания) и др. (таблица 1.3).

На сегодняшний день применение проектного управления не потеряло своей актуальности. Например, 15 октября 2016 года Правительством РФ было принято Постановление № 1050 «Об организации проектной деятельности в Правительстве Российской Федерации» [46], которое утвердило нормативно-правовую базу, правила и особенности управления государственными портфелями, программами и проектами, делегировало полномочия постоянным органам управления проектной деятельности в лице Президиума Совета при Президенте Российской Федерации по

стратегическому развитию и приоритетным проектам, Федерального проектного офиса, Ведомственного координационного органа и Ведомственного проектного офиса, а также формализовало деятельность и ответственность временных государственных органов управления проектной деятельностью и вспомогательных государственных органов управления проектной деятельностью.

Таблица 1.3 – Развитие проектного управления

Год	**Комментарии**
30-е годы 20-го века	Разработка специальных методов координации мегапроектов
1937 год	Матричная структура, направленная на реализацию сложных проектов
1941 год	Манхэттенский проект
1953-1954 гг.	Применение матричной организации в подразделениях специальных проектов воздушных сил США
1955 год	Применение матричной организации в подразделениях специальных проектов морского флота США
1956 год	Создание специальной группы для разработки методов и средств управления проектами Du Pont de Nemours Co
1957 год	Создание специальной группы для разработки методов и средств управления проектами
1957 год	Разработка метода критического пути
1958-1959 гг.	Система сетевого планирования PERT для создания ракеты «Поларис»
1959 год	Управление проектом согласно стадиям жизненного цикла
70-е годы	Создание сетевых моделей в СССР
70-е годы	Ввод методов сетевого управления в образовательные программы вузов в США и СССР
80-е годы	Решение проблем ресурсного и финансового обеспечения
1987 год	Первое издание свода лучших практик управления проектами Project Management Institute
с 1987 года	Создание национальных и международных проектных объединений и ассоциаций

Таблица 1.4 – Концепции и способы управления проектами

№	Название (оригинал)		Название (перевод на русский)	Разработчик
1	Project Management Body of Knowledge (PMBOK® Guide) [40, 41, 42]		Свод правил управления проектами	Project Management Institute (PMI) [43], США
2	International Competence Baseline International Project Management Association (ICB IPMA [47], OCB IPMA [48], PEB IPMA [49])		Международные требования к компетентности специалистов по управлению проектами	Международная Ассоциация Управления Проектами (IPMA), Швейцария
3	Rational Unified Process (RUP) [50]		Рациональный унифицированный процесс	Компания Rational Software
4	Project in Controlled Environments (PRINCE2®) [51, 52]		Свод правил по руководству проектами в сфере информационных технологий	Central Computer and Telecommunications Agency (CCTA), Великобритания
5	Microsoft Solution framework (MSF) [53]		База решений Microsoft	Корпорация Microsoft, США
6	International Standards Organization (ISO 10006:2003) [54]		Руководство по управлению качеством в проектах	Международная организация по стандартизации, США
7	Agile	Extreme Programming (XP) [55]	Экстремальное программирование	К. Бек, У. Каннингем, М. Фаулер и др., США
		Rapid Application Development (RAD)	Быстрая разработка приложений	Дж. Мартин (IBM), США
		Scrum [56]	Скрам	Х. Такэути и И. Нонака, США
		Adaptive Software Development (ADS)	Адаптивная разработка программного обеспечения	Дж. Хигстив, С. Баер, США
		Crystal Clear	Кристально-чистая разработка	А. Коуберн
		Feature-Drive Development (FDD)	ФДД	Дж. Де Люк
		Dynamic System Development Method (DSDM)	Метод разработки динамических систем	Консорциум DSDM
8	Отсутствует		ГОСТ Р 54869-2011 [57] ГОСТ Р 21500-2014 [58]	Федеральное агентство по техническому регулированию и метрологии, Россия

Анализ мировой практики проектной деятельности показал, что в мире насчитывается более десятка различных концепций и способов управления

проектами (таблица 1.4) [59]. Рассмотрим данные концепции и способы подробнее.

Важную роль среди идентифицированных способов управления проектами играет **PMBOK® Guide** [40, 41, 42], разработанный PMI и профессиональным международным сообществом действующих руководителей проектов [43].

PMBOK® Guide базируется на каскадном способе реализации проекта (*waterfall*), где исполнение работ и операций ведется последовательно и непрерывно.

Стоит отметить, что несмотря на накопленную базу знаний и проработанность, концепция декларируемая PMBOK® Guide не всегда может быть применима в ИТ-проектах. Современные ИТ-проекты включают в себя сбор требований, программирование, кастомизацию, тестирование, внедрение, интеграцию и другие уникальные процессы, которые не раскрывает классическая концепция управления проектами PMBOK® Guide. Кроме того, каскадный способ реализации проектов имеет ряд существенных недостатков:

- *во-первых*, управляемость проекта снижается, если отсутствуют детальные и проработанные проектные документы;
- *во-вторых*, фиксированные даты начала и окончания проектных работ, а также ограниченные ресурсы порождают многочисленные риски, связанные с отклонениями от запланированных проектных целей (содержания, длительности, стоимости и качества проекта);
- *в-третьих*, велика вероятность материализации риска, связанного с изменением требований в процессе осуществления проекта.

International Competence Baseline International Project Management Association базируется на сводах лучших управленческих практик, таких как ICB IPMA [47], OCB IPMA [48] и PEB IPMA [49]. Данный способ реализации проектов фокусируется на оценке компетентности руководителей проектов, проектных команд, функционирования организации, результатов реализации

проектов, действующих схем процессов управлении проектами, распределения полномочий и ответственности в проектно-ориентированной структуре управления. Существенным недостатком International Competence Baseline International Project Management Association является ориентированность на классический каскадный способ реализации проектов.

Методология разработки программного обеспечения (Rational Unified Process, RUP) [50]. В основе RUP лежат такие принципы, как ранняя идентификация основных рисков, ожидание изменений требований и проектных решений в процессе разработки, постоянное обеспечение качества на всех этапах разработки ИТ-проекта. Применение данных правил в ИТ-проектах инициировало создание «спиральной модели жизненного цикла» Б. В. Боема [60].

Свод правил по руководству проектами **Project in Controlled Environments** (PRINCE2®) включает в себя описание процедур, процессов и циклов, которые возникают в командах во время создания ИТ-продуктов [52]. Особенностью PRINCE2® является то, что каждый процесс характеризуется формализацией конкретных целей, что дает возможность руководителям ИТ-проектов оперативно предпринимать корректирующие действия. Главным недостатком PRINCE2® является отсутствие какого-либо регламентирования процессов по управлению юридическими сделками, договорами и заказами. По мнению ССТА руководителям ИТ-проектов не следует самостоятельно вырабатывать инструментарий для решения подобных проблем, лучше для данной работы привлекать профессиональных юристов.

Данный подход противоречит нормам отечественного профессионального стандарта 06.016 «Руководитель проектов в области информационных технологий», где к трудовым функциям руководителя ИТ-проектов относятся организация работ по заключению договоров, мониторинг выполнения договоров, заключение дополнительных соглашений к договорам и др.

Методология разработки программного обеспечения Microsoft Solution framework (MSF) была предложена ИТ-гигантом Microsoft [53]. MSF включает в себя две модели (модель проектной группы и модель процессов) и три дисциплины (управление предпроектной подготовкой, управление проектами и управление рисками). Модель проектной группы описывает способ организации работ проектной команды, а модель процессов сочетает в себе свойства каскадного и гибкого способа управления ИТ-проектами.

Управление качеством в проектах согласно International Standards Organization (ISO). International Standards Organization формализует отдельные аспекты проектной деятельности в стандартах различных направлений ISO 9001, ISO 10006, ISO 21500 и др. [54]. Несмотря на проработанность отдельных направлений, необходимо отметить, что International Standards Organization, как правило, руководствуется только каскадным способом реализации проектов, не учитывая особенности и специфику сферы ИТ.

Среди способов управления проектами, которые представлены в таблице 1.4, особое место занимает гибкая методика разработки программного обеспечения (**Agile Software Development**). *Agile* – это комплекс инструментов, который позволяет вести итеративную разработку ИТ-продукта [61].

Применение *agile* стало возможным благодаря цифровым свойствам ИТ-продукта, а именно – возможности эксплуатации части инкремента программного кода еще до того, как сам ИТ-продукт будет полностью готов, т. е. пользователь ИТ-продукта может активно эксплуатировать часть функционала ИС, которая еще находится в процессе создания.

Среди гибких методологий разработки программного обеспечения стоит отметить:

- ***«Экстремальное программирование»*** (Extreme Programming, XP) включает в себя 12 основных инструментов: разработку через

тестирование; «игру в планирование»; правило «заказчик рядом»; способ парного программирования; непрерывную интеграцию.; рефакторинг; частые релизы создаваемого ИТ-продукта; правило «делай проще»; метафоры системы; коллективное владение кодом; внедрение стандарта кодирования; 40-часовая рабочая неделя [55].

- ***«Быстрая разработка приложения»*** (Rapid Application Development, RAD) разработана International Business Machines (IBM). RAD позволят команде разработки привлекать пользователя на всех этапах разработки ИТ-продукта. Подобная коммуникация команды разработки с пользователем позволяет минимизировать риски, связанные с дальнейшей доработкой и эксплуатацией ИТ-продукта. Вместе с тем стоит отметить, что несмотря на уменьшение риска, связанного с отсутствием лояльности пользователя, одновременно увеличивается вероятность материализации риска «затягивания» сроков, что может привести к наступлению казуса «бессрочного проекта».

- ***«Скрам»*** (Scrum) – это способ управления ИТ-проектом, который характеризуется тем, что разработка программного кода происходит в жестко фиксированные итерации – спринты (sprints) [56]. Преимуществом данного способа разработки ПО является нивелирование риска, связанного с частыми изменениями требований проекта. Главным же недостатком скрама считается отсутствие точных дат окончания проектных работ, что часто становится препятствием, если ИТ-проект предполагается реализовать по нормам договора подряда (Глава 37 ГК РФ), где фиксированные сроки начала и окончания проектных работ являются существенными условиями, без которых договор может быть признан ничтожным (статья 708 ГК РФ).

- ***«Адаптивная разработка программного обеспечения»*** (Adaptive Software Development, ADS) использует динамический жизненный цикл «обдумывание-взаимодействие-обучение» (speculate-collaborate-learn) вместо классического – «планирование-проектирование-конструирование» (plan-design-build).

- ***«Кристально-чистая разработка»*** (Crystal Clear). Главной особенностью Crystal Clear является фокусировка на людях, а не на процессах и проектных документах, поэтому в основу заложен принцип создания полезного для пользователей программного кода.
- ***«ФДД»*** (Feature-Drive Development, FDD) предпринимает попытку объединить наиболее популярные способы управления ИТ-проектами. FDD включает 5 базовых видов деятельности: разработка общей модели; составление списка необходимых функций системы; планирование работы для каждой функции; проектирование функции; реализация функции.
- ***«Разработка динамических систем»*** (Dynamic System Development Method, DSDM) дифференцирует проект на 4 фазы: исследование экономической целесообразности ИТ-продукта; создание функциональной модели; проектирование и разработка; реализация информационной системы и обучение пользователей.

Отдельно необходимо отметить отечественный стандарт управления проектами ***ГОСТ Р 54869-2011 «Проектный менеджмент. Требования к управлению проектом»***, где упоминается о риск-менеджменте и излагаются основные правила управления рисками в проектах [57]. В более поздней версии ***ГОСТ Р 21500-2014 «Руководство по проектному менеджменту»*** уже отдельно выделены такие процессы, как «Идентификация рисков», «Оценка рисков», «Реагирование на риски» и «Управление рисками», что может говорить об увеличении значимости процессов риск-менеджмента для успешного завершения проектных работ [58].

Подобное разнообразие концепций и способов управления проектами часто приводит к проблемам. Например, неопытные руководители ИТ-проектов не могут оперативно выбрать какой инструментарий им необходимо применять в конкретном проекте. Для решения данной проблемы С. Брандас, О. Дидрад и Н. Бибу попытались определить лучшую концепцию и способ управления проектами, проведя их сравнительный анализ [62]. Результаты сравнительного анализа представлены в таблице 1.5.

Таблица 1.5 – Сравнительный анализ концепций и способов управления ИТ-проектами [62]. Исследования проходили в 124 ИТ-проектах

Концепция управления проектами	**Фокус на риски**	**Контроль рисков**	**Наличие показателей рисков**	**Сложность реализации ИТ-проекта**	**Необходимость в дополнительных ресурсах**	**Размер ИТ-проекта**
PMBOK® Guide	+	+	+	Простой	Средняя	Долгосрочный (более 6 месяцев)
RUP	+	+	+	Трудный	Немного	Долгосрочный (более 6 месяцев)
PRINCE2®	+	+	-	Простой	Средняя	Долгосрочный (более 6 месяцев)
Agile	-	-	-	Простой	Немного	Краткосрочный (менее 2 месяцев)

На основании проведенного исследования С. Брандас, О. Дидрад и Н. Бибу делают следующие выводы: концепции управления проектами, такие как PMBOK® Guide и PRINCE2®, должны применяться в долгосрочных ИТ-проектах, где срок реализации составляет более шести месяцев; методология гибкой разработки ПО *agile* должна применяться в краткосрочных ИТ-проектах. Причем С. Брандас, О. Дидрад и Н. Бибу заключают, что в *agile* отсутствует формализованный процесс управления рисками, поэтому данный способ управления ИТ-проектами не подходит для молодых команд и начинающих руководителей ИТ-проектов, так как является очень опасным.

Стоит отметить, что несмотря на полученные результаты ученые допускают ошибку, делая вывод, что в *agile* отсутствуют процессы управления рисками. В частности, если ИТ-проект реализуется по *agile*, то после завершения итерации участники ИТ-проекта проводят ретроспективный анализ, где они идентифицируют проблемы, которые

материализовались во время спринта. Кроме того, во время ретроспективного анализа участники ИТ-проекта прогнозируют возможные проблемы (рисков), которые могут материализоваться на следующих спринтах. Данные обстоятельства позволяют утверждать, что в ИТ-проектах, которые разрабатываются по *agile* имеются признаки идентификации, мониторинга и контроля рисков [63, 64].

В результате рассмотрения эволюции теории и практики управления проектами могут быть сделаны следующие выводы: современная проектная деятельность наиболее ярко и значимо представлена в области ИТ, т. к. создание ИТ-проектов и ИТ-услуг требует специфического управления, учитывающего особенности сферы ИТ; уникальность процессов, сложность и многозадачность ИТ-проектов привели к созданию различных способов управления проектами (PMBOK® Guide, ICB IPMA, OCB IPMA, PEB IPMA, RUP, PRINCE2®, ISO 10006:2003, Agile и др.); способы управления проектами, как правило, ориентированы на определенные отрасли, виды, сложность и размеры ИТ-проектов. Анализ показал, что значительная часть, рассмотренных способов, не учитывает специфику сферы информационных технологий.

Также необходимо отметить, что некоторые способы управления проектами (PMBOK® Guide, RUP, PRINCE2®, Agile) делают акцент на управлении рисками. Однако при более детальном рассмотрении установлено, что понимание природы риска в данных сводах знаний является поверхностным. Например, в PMBOK® Guide версии 2013 года процесс «Мониторинг и управление рисками: входы, инструменты, методы и выходы» был изменен на «Контроль рисков» [41]. С позиции автора диссертационного исследования данное обстоятельство является серьезной ошибкой, т. к. контроль осуществляется над рисками, которые были выявлены в процессе идентификации (идентифицированные риски), а мониторинг осуществляется над рисками, которые не были определены во

время идентификации (неидентифицированные риски). Следовательно, процесс необходимо было определить, как «Контроль и мониторинг рисков».

Таким образом, прежде чем приступать к проработке вопроса о том, как в современных условиях применяется управление рисками в ИТ-проектах, требуется определить базовый понятийный аппарат.

1.3. Хронологическое формирование понятийного аппарата управления рисками

Результаты исследования показали, что в литературе нет общепринятого и устоявшегося термина «риск», что создает проблему интерпретации, трактовки и использования данного термина в дальнейшем. Ниже представлены основные позиции к определению понятия «риск» (таблица 1.6).

Таблица 1.6 – Понятия термина «риск»

№	Понятие термина «риск»	Источник
1	Влияние неопределенности на цели	ГОСТ Р ИСО 31000-2010 [65]
2	Угроза и (или) опасность	И. Т. Балабанов [66], Д. М. Машков [67]
3	Неопределенность	Филимонов Д. И. [68], В. Н. Бурков и Д. А. Новиков [69], И. И. Мазур и В. Д. Шапиро [70]
4	Условие или неопределенное событие, которое в случае наступления оказывает влияние хотя бы на одну цель проекта (содержание, длительность, стоимость и качество проекта)	Свод правил проектного управления Project Management Body of Knowledge (PMBOK® Guide) [40, 41, 42]
5	Угроза или возможность	П. Сангхира [71]
6	Событие, которое одновременно несет угрозу, опасность, неопределенность и возможность	PricewaterhouseCoopers [72]
7	Вероятность недополучения доходов и (или) вероятность возникновения убытков	П. Г. Грабовый, С. Н. Петрова [73]
8	Мера опасности	Е. И. Шохин [74]
9	Совокупность значений возможного ущерба в некоторой стохастической ситуации	В. Ю. Королев, В. Е. Бенинг, С. Я. Шоргин [75]
10	Возможность получения убытков от предпринимательской деятельности	Гражданский кодекс Российской Федерации (ст. 926 ГК РФ, ст. 933 ГК РФ) [76]
11	Действия, сделанные наудачу	В. Даль [77]
12	Неопределенное событие или набор неопределенных событий	Management of Risk: Guidance for Practitioners (M_o_R®) [78]

Продолжение таблицы 1.6.

№	Понятие термина «риск»	Источник
13	Неопределенное событие или набор событий, которые в случае наступления, способно оказать влияние на процесс достижения целей	PRojects IN Controlled Environments (PRINCE2®) [52]
14	Искусственная экономическая категория, совокупно отражающая меру реальности нежелательного отклонения от цели хозяйственной деятельности предприятия и размер обусловленного этим отклонением ущерба	Р. М. Качалов [79]
15	Негативная часть неопределенного события, наступление которого может принести организации ущерб и (или) выгоду	The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management» (COSO ERM) [80]
16	Вероятный неблагоприятный исход для субъекта	А. Г. Мадера [81, 82]

Необходимо отметить, что среди лингвистов нет единого мнения, где именно берет свое начало «риск». По мнению специалистов, слово *«risk»* имеет французские и итальянские истоки. Например, в итальянском языке *«risiko»* означает «опасность» [83]. С французского же *«risdoe»* трактуется, как «объезжать утес». Некоторые эксперты предполагают, что «риск» имеет греческие корни и происходит от слова *«ridsikon»*, *«ridsa»* что означает «утес», «скала» [83]. В этом случае, можно заключить, что глагол «рисковать» можно толковать как «лавирование между скалами».

Согласно Национальному государственному стандарту Российской Федерации ГОСТ Р ИСО 31000-2010 риск характеризуется вероятными событиями и последствиями от их материализации [65, 84, 85]. Стоит отметить, что под влиянием понимается отклонение от того, что ожидается (отрицательное или положительное). Определение понятия «риск» в подобном ключе дает больше управленческих возможностей в сравнении с другими трактовками, т. к. выбирая стратегию управления риском можно уменьшить вероятность материализации негативного рискового события и (или) увеличить вероятность материализации положительного рискового события. Данная трактовка риска раскрывает его сущность, однако далее

природа риска подробно не рассматривается. Например, рисковое событие в разные промежутки времени может менять свои свойства. Объясняется это тем, что на источники риска в разные моменты времени воздействуют разные факторы. Следовательно, если принять во внимание данный аспект, то может быть получен дополнительный механизм управления рисками, который можно использовать для прогнозирования времени актуализации (материализации) рисков, выявляя наиболее опасные временные участки. Взаимосвязь риска, вероятных событий, последствий и целей согласно ГОСТ Р ИСО 31000-2010, представлена на рисунке 1.1.

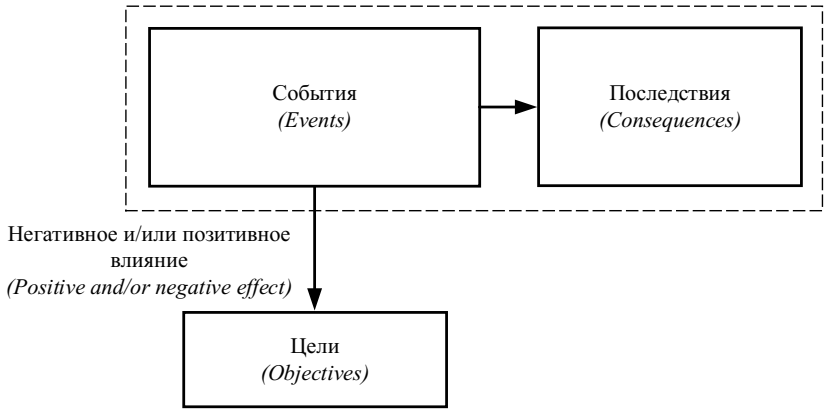


Рисунок 1.1 – Графическое представление содержания термина «риск», согласно позиции обозначенной в ГОСТ Р ИСО 31000-2010

И. Т. Балабанов и Д. М. Машков утверждают, что «риск» есть синоним понятия «угроза» [66, 67]. Под угрозой исследователями понимается возможность потери организацией своих ресурсов, получение доходов в неполном объеме, опасность появления дополнительных расходов в результате осуществления бизнес-деятельности или получение нулевого результата. Данный подход к определению «риска» формализует его, как возможность наступления негативных и нежелательных событий.

Д. И. Филимонов определяет риск, как неопределенность, которая возникает из-за отсутствия или недостатка информации [68]. Необходимо отметить, что согласно выводам Д. И. Филимонова неопределенный исход

несет для выполняемой работы неблагоприятные последствия, из чего следует, что понятие «риск» толкуется в негативном аспекте. В трудах В. Н. Буркова и Д. А. Новикова [69], И. И. Мазура и В. Д. Шапиро [70] риск также отождествляется с неопределенностью, но необходимо подчеркнуть, что «неопределенность» и «риск» – это два совершенно разных понятия, в частности:

- *первое*, неопределенность возникает тогда, когда отсутствует необходимая информация, а риск может быть прогнозируемым, т. к. его сущность базируется на статистической информации и профессиональном опыте сотрудников;
- *второе,* неопределенность связана с вероятностью наступления непрогнозируемых, стохастических событий, а риск порождают конкретные источники под влиянием определенных факторов, каждый из которых может быть идентифицирован;
- *третье,* неопределенность основывается на субъективном экспертном мнении, риск же базируется на объективных фактах.

Следовательно, под **«неопределенностью»** следует понимать, *совокупность непрогнозируемых ситуаций, наступление которых невозможно прогнозировать*. Среди причин, которые порождают неопределенность, следует отметить недостаток информации, присутствие скрытых факторов рисков, действия конкурентов сознательно стремящиеся повлиять на запланированные проектные цели.

В PMBoK® Guide под термином «риск» понимается неопределенное событие, которое если материализуется, то оказывает негативное или позитивное влияние на одну или несколько проектных целей, таких как содержание проекта, длительность проекта, стоимость проекта и качество проекта (рисунок 1.2).

Рисунок 1.2 – Графическое представление содержания термина «риск», согласно позиции обозначенной в PMBOK® Guide

П. Сангхира, сертифицированный специалист Project Management Professional (PMP), в своих трудах отмечает, что риск имеет двоякую природу, поэтому рисковое событие стоит воспринимать не только как грозу, но и как позитивную возможность [71].

Специалисты PricewaterhouseCoopers (PwC) считают, что риск – это событие, которое одновременно несет угрозу, опасность, неопределенность и возможность [72]. Эксперты PwC делают вывод, что если риск рассматривать как угрозу и опасность, то это событие несет для организаций финансовые потери. Если риск рассматривать, как неопределенность, то это вероятность наступления любых событий, негативных или позитивных. Если риск интерпретировать с точки зрения позитивной возможности, то событие способно оказать положительный эффект.

П. Г. Грабовой и С. Н. Петрова под риском понимают некую величину вероятности недополучения доходов по сравнению с прогнозируемым результатом [73].

Е. И. Шохин предлагает математическую трактовку понятия «риск» [74]. По мнению ученого, риск можно определить, как численную меру опасности, которая сочетает 2 элемента: во-первых, частота или

вероятность неблагоприятного события; во-вторых, тяжесть его последствий за определенный промежуток времени.

В. Ю. Королев, В. Е. Бенинг и С. Я. Шоргин в своих трудах определяют понятие «риск», как «возможный ущерб» [75]. Между тем стоит отметить, что подобный взгляд на определение термина «риск» значительно сужает возможности управления рисковым событием. При данной концепции единственное, что можно предпринять – это действовать согласно критерию Сэвиджа (критерий наименьшего вреда), согласно которому выбирается наилучшая альтернатива из самых плохих значений.

В статьях 929 и 933 ГК РФ риск определяется, как возможность получения убытков от предпринимательской деятельности [76, 115].

В словаре В. Даля можно найти трактовку понятия «риск»: «…действия, сделанные наудачу, которые требуют смелости, решительности, предприимчивости» [77].

В международном своде лучших практик управления рисками (Management of Risk: Guidance for Practitioners, M_o_R®) риск определяется, как «неопределенное событие» или «набор неопределенных событий», которое(-ые) в случае материализации могут оказать влияние на процесс достижения целей организации (рисунок 1.3) [78].

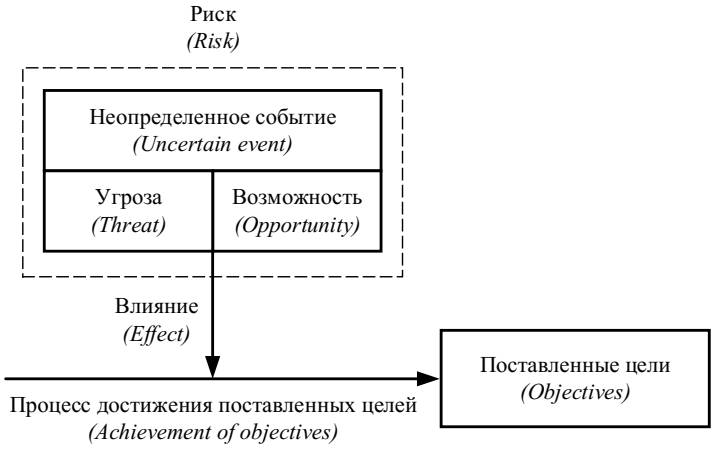


Рисунок 1.3 – Графическое представление содержания термина «риск», согласно позиции обозначенной в M_o_R®

Под «риском» в PRINCE2® понимается неопределенное событие, которое в случае материализации может оказать влияние на процесс достижения целей проекта [86] (рисунок 1.4).

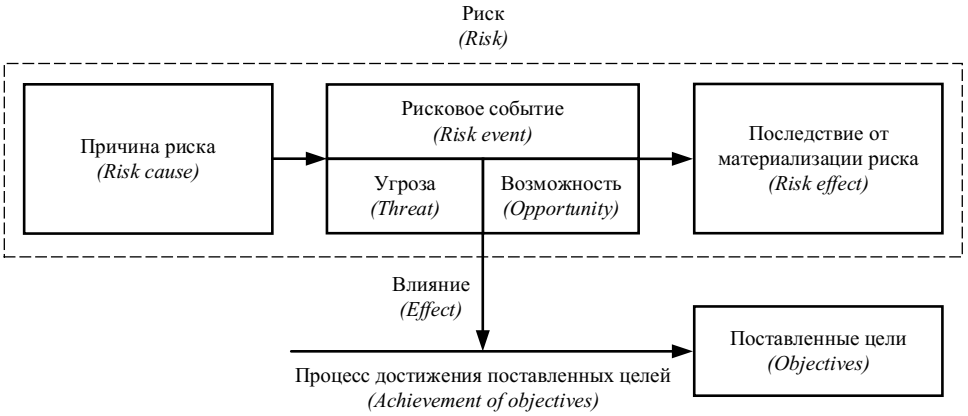


Рисунок 1.4 – Графическое представление содержания термина «риск», согласно позиции обозначенной в PRINCE2®

По мнению авторов PRINCE2® риск состоит из трех элементов [52]:

- *причина риска* – это источник риска;
- *рисковое событие* – это событие, которое может быть угрозой и (или) возможностью;
- *последствие от материализации риска* – это возможный ущерб или возможный позитивный эффект, который может быть получен в случае материализации риска.

Р. М. Качалов определяет риск, как обобщенную искусственную категорию, которая отражает меру реальности нежелательного отклонения от цели хозяйственной деятельности предприятия и размер обусловленного этим отклонением ущерба [79, 87].

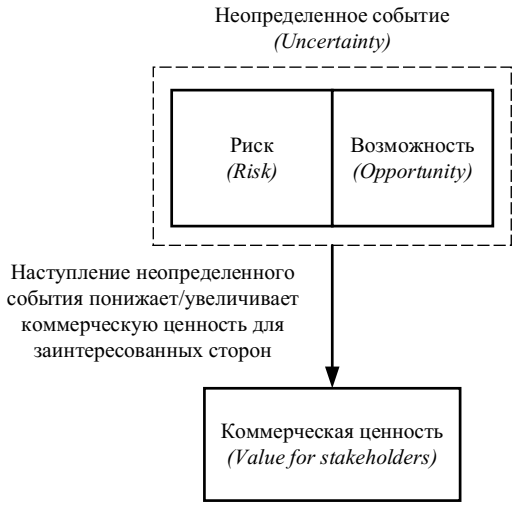


Рисунок 1.5 – Графическое представление содержания термина «риск», согласно позиции обозначенной в COSO ERM

The Committee of Sponsoring Organizations of the Treadway Commission или COSO – это частная некоммерческая организация, созданная в 1985 г. для унификации правил внутреннего контроля корпоративного сектора США с целью борьбы с мошенничеством [80]. На базе лучших практик в области управления рисками COSO разработало свой собственный свод правил Enterprise Risk Management (COSO ERM), первая версия которого была опубликована в 2004 году, вторая (Enterprise Risk Management. Integrating with Strategy and Performance) – в 2017 году [88].

Необходимо отметить, что COSO не дает собственного определения термина «риск» (рисунок 1.5). Вместо этого COSO опирается на концепцию разработанную PricewaterhouseCoopers (PwC) [72].

По мнению Мадера А. Г. «риск» – это вероятный неблагоприятный исход для субъекта, а «шанс» – это вероятный благоприятный исход для субъекта [81, 82].

Критическое осмысление позиций по определению понятия «риск» позволило заключить, что говоря о риске, многие специалисты имеют в виду некую неопределенность, которая может оказать влияние на запланированные цели. Необходимо отметить, что данная точка зрения не

отражает в полной мере природу «риска» и значительно ограничивает его практическое применение в сфере информационных технологий. Таким образом, автором диссертационного исследования была уточнена сущность и дополнено содержание понятия **«риск в ИТ-проектах»**, как *возможное событие, которое порождается конкретными источниками (источниками риска), материализация которого под воздействием определенных факторов (факторов риска) способно оказать негативное/позитивное влияние на запланированные проектные цели, побуждая наступление проблемных/благоприятных ситуаций*.

Благодаря предложенному автором диссертационного исследования уточнению и дополнению стало возможным выделение конкретных источников рисков актуальных для ИТ-проектов: исполнитель/подрядчик и (или) поставщик; заказчик; право (комплаенс риски); рынок; стихийные бедствия; пользователь; технология; проектный коллектив; руководитель ИТ-проекта; информация и коммуникационные каналы. С определением конкретных источников рисков была установлена их связь с факторами рисков, т. е. совокупностью обстоятельств, которые воздействуя на источники рисков, могут уменьшать либо увеличивать вероятность материализации рисков. Стоит отметить, что факторы рисков зависят от времени. Подобный взгляд на природу риска дает возможность заключить, что риск материализуется в конкретный момент времени, трансформируясь в проблемную или в благоприятную ситуацию (рисунок 1.6).

Рисунок 1.6 – Графическое представление риска

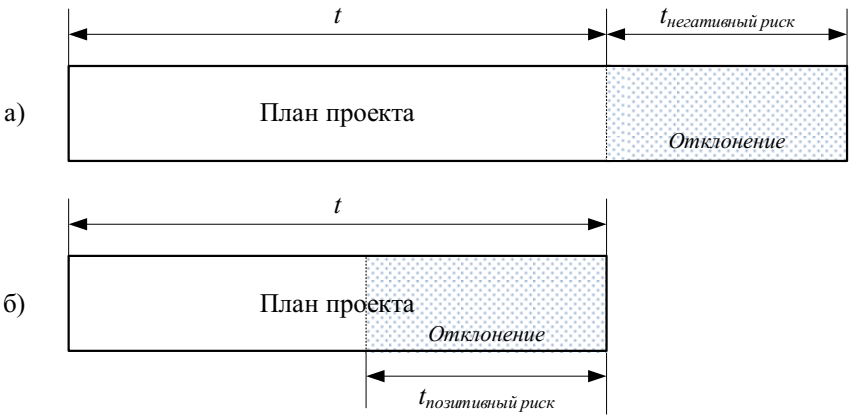


Рисунок 1.7 – Схема, демонстрирующая влияние негативного риска (а) и позитивного риска (б) на план проекта, где *t* – это длительность проекта

Наличие благоприятных последствий по причине материализации риска, послужило основанием для дифференциации рисков на «негативные риски» и «позитивные риски». **«Негативный риск»** – *это событие, которое может отрицательно повлиять на план и на проектные цели, приводя к увеличению длительности проекта, увеличению стоимости проектных работ, уменьшению качества итогового продукта*. **«Позитивный риск»** – *это событие, которое может положительно повлиять на план и на проектные цели, предвосхищая запланированные результаты*. Схема того, как наступление негативного *($t_{негативный\ риск}$)* и позитивного *($t_{позитивный\ риск}$)* риска влияет на длительность проекта *(t)*, представлена на рисунке 1.7.

Стоит отметить, что термин «позитивный риск» *(positive risk)* упоминается во многих источниках. Например, У. Сторидж из Калифорнийского университета в Беркли утверждает, что концепция «позитивного риска» сформировалась во многом благодаря правилам риск-менеджмента COSO ERM:2004 [216]. В PMBOK® Guide 2017 года сказано, что целью управления проектными рисками является снижение вероятности материализации или влияния негативных рисков либо повышение вероятности материализации или влияния позитивных рисков [42]. Финансовый консультант Д. Дункельбергер определяет «позитивный риск», как вероятное событие, которое может оказать положительное влияние на

проект [217]. М. Карпентер в своей работе утверждает, что о наступлении «положительного риска» можно говорить только тогда, когда полученный результат значительно предвосхитил ожидания [218]. Риск-консультант Т. Дэвидсон понимает под «позитивными рисками» шансы и возможности [219, 220]. Дж. А. Лакман в своих трудах не только активно использует термин «позитивный риск», но также предлагает алгоритм его использования при добыче полезных ископаемых [221, 222]. В книге «Effective Opportunity Management for Projects. Exploiting Positive Risk» Д. Хиллсон, исследуя природу риска, пришел к выводу, что для успешного завершения проекта, необходимо не только управлять вероятными угрозами, но и осуществлять менеджмент «позитивных рисков» [223].

Влияние материализовавшихся негативного и позитивного рисков в ИТ-проекте можно охарактеризовать формулами 1.1 и 1.2, где $\mathrm{Im}_{negative}$ – влияние в результате материализации негативного риска, C_1 – прямой материальный ущерб в результате материализации негативного риска, C_2 – материальные потери направленные на ликвидацию последствий, полученных в результате материализации негативного риска, C_3 – материальные потери, полученные по факту вывода ИТ-проекта на уровень, который был до материализации негативного риска, C_4 – материальный ущерб, вызванный отклонением от запланированных проектных целей, $\mathrm{Im}_{positive}$ – влияние в результате материализации позитивного риска, C_5 – материальная польза, вызванная отклонением от запланированных проектных целей.

$$\mathrm{Im}_{negative} = C_1 + C_2 + C_3 + C_4\,, \tag{1.1}$$

$$\mathrm{Im}_{positive} = C_5 \tag{1.2}$$

В качестве примера материализовавшегося негативного риска можно рассмотреть уничтожение сервера HP ProLiant MicroServer Gen8 стоимостью 90 000 руб. в результате пожара (C_1). Для ликвидации полученных последствий необходимо приобрести новый сервер (C_2) и осуществить пуско-наладочные работы стоимостью 30 000 руб. (C_3). По факту простоя работ в ИТ-проекте отклонение от запланированной длительности может составить около 30 человеко-часов или 25 500 руб., при стоимости часа разработки 850 руб./ч. (C_4). Таким образом, влияние от материализации данного негативного риска составит 235 500 руб. ($\mathrm{Im}_{negative}$).

Наглядным примером влияния материализовавшегося позитивного риска на проектные цели ($\mathrm{Im}_{positive}$) является замена в процессе реализации в ИТ-проекте программиста уровня квалификации *Junior Developer* на программиста уровня квалификации *Senior Developer*. Программист высшего квалификационного уровня в ИТ-проекте будет выполнять поставленные задачи быстрее, качественнее и с меньшим количеством ошибок *(bugs)*. Подобная замена приводит к значительному предвосхищению запланированных результатов. Если предвосхищение будет равно 50 человеко-часов, тогда влияние от материализации позитивного риска составит 42 500 руб. (C_5).

Таким образом, дополнение содержания понятия «риск в ИТ-проектах» дает ряд преимуществ:

- *во-первых*, лучше раскрывается сущность и природа риска, устанавливаются причины материализации риска и его источники, что дает возможность значительно повысить результативность мер воздействия, нивелируя не только источники рисков, но и факторы рисков;
- *во-вторых*, понимание того, что материализация «риска в ИТ-проектах» может приводить к проблемным и благоприятным ситуациям, создает основу для разработки инструментария по управлению угрозами и позитивными возможностями;

- *в-третьих*, понимание риска в ИТ-проектах как динамической величины, зависящей от времени, представляет большой теоретико-практический интерес, т. к. кроме вероятности наступления риска и его возможного влияния в случае материализации, риск обладает свойствами актуализации, что дает больше управленческой свободы ИТ-организациям, руководителям ИТ-проектов и проектным коллективам в выборе средств воздействия на данные риски;
- *в-четвертых*, предложенная дефиниция уточняет сущность термина «неопределенность». Под «неопределенностью» следует понимать совокупность непрогнозируемых, стохастических событий, наступление которых невозможно прогнозировать. Сущность риска существенно отличается от природы неопределенности. Риск порождается конкретными источниками под влиянием определенных факторов. Следовательно, риск может быть прогнозируемым.

Далее рассмотрим значение термина «управление рисками» или «риск-менеджмент» *(risk management)*. При классическом рассмотрении риск-менеджмент включает в себя такие процессы, как идентификация рисков, оценивание вероятности материализации рисков и оценивание возможного ущерба/дохода в случаях их наступления, принятие управленческих решений по разработке мер воздействия на риски, а также мониторинг и контроль рисков [89].

Несмотря на потребность в однозначном толковании термина «управление рисками», в литературе нет его единого определения [90, 91, 92, 93]. Например, можно встретить следующие формулировки:

- *риск-менеджмент* – это искусство управления риском инвестиционной деятельности, которое основано на стратегическом планировании [94];

- *риск-менеджмент* – это комплекс навыков, инструментов, знаний и методов, необходимых для успешного завершения проекта [40, 41, 42];
- *управление рисками* – это система управления рисками и финансовыми отношениями, которые возникают в процессе управления [95].

Автор диссертационного исследования считает, что рассмотренные выше определения риск-менеджмента не раскрывают истинную природу «риска». В этой связи под термином **«риск-менеджмент» / «управление рисками»** *понимаются процессы по оценке негативных и позитивных рисков, разработке мер воздействия на риски, а также процессы мониторинга неидентифицированных рисков и контроля идентифицированных рисков*.

Таблица 1.7 – Хронологическое развитие сферы риск-менеджмента [99, 100]

Год	Название свода правил
1988 год	Соглашение Базель I
1999 год	Разработка стандарта управления рисками AS/NZS 4360:1999
2002 год	Разработка стандартов управления рисками FERMA, IRM, AIRMIC и ALARM
2004 год	Соглашение Базель II
2004 год	Создание модели COSO ERM
2005 год	Пособие PRMIA
2008 год	Создание модели организованной зрелости в плате управления рисками RIMS
2008 год	Руководство по передовым стандартам в области управления рисками. Австралийское правительство
2008 год	BS 311000:2008 Свод практик для риск-менеджмента. Великобритания
2010 год	ГОСТ Р ИСО 31000-2010
2011 год	06.12.2011 г. в России принят Федеральный закон №402-ФЗ «О бухгалтерском учете»
2017 год	Усовершенствование модели COSO ERM
2020 год	Информационное письмо Банка России от 01.10.2020 N ИН-06-28/143 «О рекомендациях по организации управления рисками …»

Считается, что скоординированные действия по идентификации рисков, оценке вероятности их материализации и возможного ущерба,

разработке мер воздействия, мониторингу и контролю рисков впервые были закреплены в 1992 году в своде правил управления рисками COSO «International Control – Integrated Framework» [96] (таблица 1.7). Однако с уверенностью можно утверждать, что истоки риск-менеджмента берут свое начало в религиозных учениях, философии, математике, а позднее и теории вероятностей.

Поскольку риск-менеджмент долгое время не являлся самостоятельной дисциплиной и зависел от развития других наук, то имеет смысл рассматривать эволюцию управления рисками в контексте исторических событий. Например, первое осмысление «риска» произошло благодаря азартным играм, где активно применялась теория вероятностей. Ведущую роль в развитии данного направления в 1526 году сыграл Дж. Кардано, который написал «Книгу об игре в кости» [97]. Кроме того, необходимо упомянуть Б. Паскаля и П. Ферма, которые в 1654 году пришли к пониманию математического ожидания и смогли формулировать теоремы сложения и умножения вероятностей. К данному историческому периоду также можно отнести работу Х. Гюйгенса «О расчетах в азартной игре или рассмотренная математически стоимость всех шансов при азартных играх в карты, кости, при заключении пари, при участии в лотерее и т. д.», которая увидела свет в 1657 году [98].

Конец XVII века характеризуется новым витком развития риск-менеджмента, т. к. появляются первые труды по статистике. В частности, в 1693 году публикуются научные работы Э. Галля, которые стали основой для страховых рисков. Также стоит отметить предпринимателя, первого страхового агента Эдварда Ллойда, который благодаря систематизации информации о крупных сделках, судах и другой торговой информации стал заключать первые контракты по страхованию морских рисков.

В XVIII веке активно разрабатываются экономические теории, которые также повлияли на развитие риск-менеджмента. Например, Адам Смит в своем труде «Исследование о природе и причинах богатства народов»

пришел к выводу, что представители более рисковых профессий, такие как врачи или юристы получают более высокие вознаграждения, чем представители профессий с низким уровнем риска [101]. Английский экономист Д. С. Милль в своем труде «Основы политической экономии с некоторыми приложениями их к социальной философии» в 1848 году вводит термин «плата за риск» [102]. В 1850 году исследования, проведенные И. Г. фон Тюненом и закрепленные в работе «Изолированное государство в его отношении к сельскому хозяйству и национальной экономии. Исследование о влиянии хлебных цен, богатства почвы и налогов на земледелие» рассматривают сущность инновационных рисков. Главной идеей данной работы стала классификация рисков на страхуемые (риски, под которые могут быть выделены резервы) и нестрахуемые (предприниматель полностью принимает ущерб на себя в случае их наступления).

В 1921 году развивая идеи И.Г. фон Тюнена о прибыли и риске, Ф. Найт в своей книге «Риск, неопределенность и прибыль» впервые разделил понятия «риск» и «неопределенность». По его мнению, риск является «измеримой неопределенностью, которой можно управлять» [103].

Новый взгляд на риск предложил ученый Дж. М. Кейнс. Введя в деловой оборот такие понятия, как риск кредитора, риск заемщика, риск обесценивания денег и др. В своем труде «Трактат о вероятности» Кейнс использует такое понятие, как «издержка риска».

Одним из важнейших моментов в понимании природа риска стало осознание того, что неопределенность наступает из-за неизвестных желаний и предпочтений людей. Данная концепция легла в основу теории игр и нашла свое отражение в книге «Теория игр и экономическое поведение», опубликованной в 1953 году Дж. Нейманом и О. Моргенштерном [104].

В 1988 году приходит еще одно осознание, что рисковую деятельность финансовых институтов необходимо регулировать. В связи с этим Базельский комитет по банковскому надзору издает документ «Базель I», в

котором рассматриваются вопросы о достаточности капитала банков для покрытия расходов по кредитным рискам.

Сегодня семейство национальных стандартов по управлению рисками насчитывает более 20 документов, которые постоянно обновляются и дополняются (таблица 1.8).

Таблица 1.8 – Семейство национальных стандартов по управлению рисками

Код стандарта	**Название стандарта**
ГОСТ Р 14.09-2005	Экологический менеджмент. Руководство по оценке риска в области экологического менеджмента
ГОСТ Р 51901.11-2005 [105]	Hazard and operability studies (HAZOP studies) – Application guide
ГОСТ Р 51901.3-2007 [106]	Руководство по менеджменту надежности
ГОСТ Р 51901.12-2007 [107]	Метод анализа видов последствий отказов
ГОСТ Р 51901.14-2007 [108]	Структурная схема надежности и булевы методы
ГОСТ Р ИСО/МЭК 16085-2007 [109]	Применение в процессах жизненного цикла систем и программного обеспечения
ГОСТ Р 51901.10-2009	Процедуры управления пожарным риском на предприятии
ГОСТ Р ИСО 31000-2010	Принципы и руководство
ГОСТ Р ИСО/МЭК 31010-2011 [110]	Методы оценки риска
ГОСТ Р 51897-2011	Термины и определения
ГОСТ Р 54617.1-2011	Менеджмент риска в наноиндустрии. Общие положения
ГОСТ Р 54617.2-2011	Менеджмент риска в наноиндустрии. Идентификация опасностей
ГОСТ Р 51901.21-2012 [111]	Реестр риска. Общие положения
ГОСТ Р 51901.22-2012 [112]	Реестр риска. Правила построения
ГОСТ Р 51901.23-2012 [113]	Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска
ГОСТ Р 55059-2012	Безопасность в чрезвычайных ситуациях. Менеджмент риска в чрезвычайной ситуации. Термины и определения
ГОСТ Р 55234.2-2013	Менеджмент биориска
ГОСТ Р 55914-2013	Руководство по менеджменту психосоциального риска на рабочем месте
ГОСТ Р ИСО 11231-2013	Вероятностная оценка риска на примере космических систем
ГОСТ Р ИСО 15743-2012	Менеджмент и оценка риска для холодных систем
ГОСТ Р МЭК 62502-2014	Анализ дерева событий
ГОСТ Р МЭК 62508-2014	Анализ влияния на надежность человеческого фактора
ГОСТ Р ИСО 31000-2019 [227]	Принципы и руководство

Рассмотрим более подробнее модель управления рисками, которая формализована в ГОСТе Р ИСО 31000-2010 «Менеджмент риска. Принципы и руководство» [65].

Риск-менеджмент, согласно ГОСТ Р ИСО 31000-2010, включает в себя следующие процессы: определение текущей ситуации; идентификация риска; анализ риска; оценивание риска; воздействие на риск; мониторинг и контроль риска; обмен информацией и проведение консультаций (рисунок 1.8). Отметим, что объединенный вид деятельности таких процессов, как идентификация риска, анализ риска, оценивание риска принято называть «оценка риска».

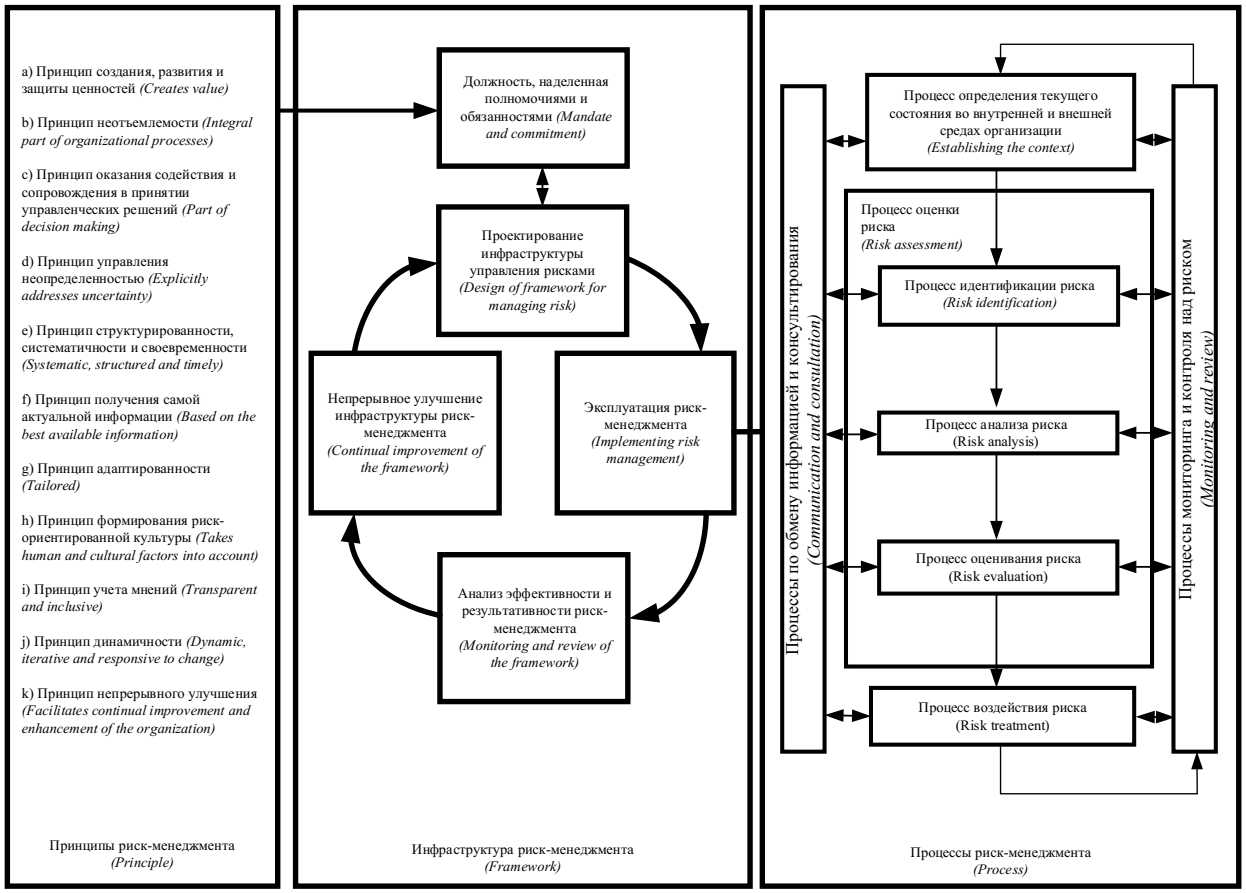


Рисунок 1.8 – Принципы, инфраструктура и процессы риск-менеджмента согласно ГОСТ Р ИСО 31000-2010

Главной задачей процесса *идентификации рисков* является определение и формализация негативных и позитивных рисков в реестре рисков, которые способны оказать влияние на процесс достижения проектных целей.

Задача *анализа рисков* заключается в сборе и анализе информации о рисках. Кроме того, анализ рисков устанавливает источники рисков, факторы рисков и прогнозирует возможные последствия в случае материализации рисков.

Оценивание рисков направлено на установление так называемого уровня риска с помощью матриц вероятностей/влияния. Уровень риска дает возможность определить какие риски являются опасными, умеренными и безопасными [114]. Стоит отметить, что процесс оценивания рисков требует точности измерений, поэтому на практике, как правило, применяют два вида методов – количественные (математическое) методы и качественные (экспертные) методы.

Воздействие на риски включает в себя разработку мер превентивного воздействия на риски (меры «плана А») и мер принятия рисков (меры «плана Б»).

Мониторинг неидентифицированных рисков и контроль идентифицированных рисков – это регулярный надзор за рисками.

На основании проведенного хронологического анализа развития понятийного аппарата управления рисками можно сделать следующие выводы:

- *Во-первых*, среди специалистов и ученых, занятых изучением природы риска, нет единого мнения о том, как необходимо определять понятия «риск», «неопределенность» и «риск-менеджмент». В связи с чем в диссертационном исследовании было уточнено содержание понятия «риск» в ИТ-проектах. «Риск» – это возможное событие, которое порождается конкретными источниками (источники риска), материализация которого под воздействием определенных факторов (факторы риска) способно оказать

негативное (позитивное) влияние на запланированные проектные цели, побуждая наступление проблемных (благоприятных ситуаций), что дополняет классическое толкование, которое определяет риск как влияние неопределенности на запланированные цели. Под термином «неопределенность» в настоящем диссертационном исследовании понимается совокупность непрогнозируемых событий, которые могут материализоваться из-за отсутствия или недостатка актуальной информации. «Риск-менеджмент» – это процессы, связанные с оценкой негативных и позитивных рисков, разработкой мер воздействия на риски, а также процессы мониторинга неидентифицированных рисков и контроля идентифицированных рисков.

- *Во-вторых*, разнообразие способов управления проектами создает определенные проблемы. В частности, проблему выбора оптимального способа управления ИТ-проектами и управления рисками в них.

- *В-третьих*, отсутствие унифицированного механизма управления проектами порождает проблемную ситуацию, связанную с отсутствием единого подхода к классификации рисков в ИТ-проектах. Следует подчеркнуть, что поиск решения данной проблемы представляет как научный, так и практический интерес, т. к. эффективность использования риск-менеджмента напрямую зависит от качественной классификации рисковых событий. Во многом это связано с тем, что классификация рисков в ИТ-проектах позволяет повысить качество идентификации негативных и позитивных рисков, сформулировать стандарты мер воздействия на риски, а также улучшить мониторинг неидентифицированных рисков и контроль идентифицированных рисков.

Выводы по главе 1.

Критическое осмысление имеющихся в научной литературе позиций, позволяют сделать следующие выводы:

1. Анализ современных тенденций в мировой и отечественной экономике продемонстрировал, что сфера информационных технологий является одной из быстрорастущих и перспективных отраслей. Показана сильная зависимость отечественной экономики от иностранного программного обеспечения и ИТ-оборудования, которая побудила Президента РФ, Правительство РФ и другие органы исполнительной власти разработать Стратегию по информационному развитию общества в РФ, план по импортозамещению ПО, программу развития цифровой экономики РФ и нормативно-правовые акты.

2. В результате исследования было подтверждено, что успешное завершение ИТ-проектов во многом зависит от выбранного способа управления проектам (*agile*, *waterfall* и др.) и применения риск-менеджмента.

3. Установлено, что термин «риск» отечественными и зарубежными учеными толкуется по-разному. В ходе исследования было выявлено, что риск представляет собой сложную структуру, которая характеризуется вероятностью наступления, возможным негативным (позитивным) влиянием, источниками риска, а также факторами риска. Исследование природы риска позволило найти отличия от понятия «неопределенности», хотя концептуально эти «риск» и «неопределенность» имеют общие черты. Таким образом, в дальнейшем термин «риск» автор рекомендует определять как вероятное событие, порождаемое определенными условиями или объектами, наступление которого под воздействием факторов рисков в определенный отрезок времени способно оказать негативное (позитивное) влияние на запланированные проектные цели и привести к проблемным (благоприятным) ситуациям.

Необходимо отметить, что результаты проведенного исследования подтверждают актуальность использования риск-менеджмента в ИТ-проектах, но не раскрывают методический инструментарий управления рисками в них. В связи с этим далее необходимо рассмотреть методы идентификации и оценки рисков в ИТ-проектах, учитывая зарубежный и

отечественный опыт, проанализировать негативные и позитивные риски, актуальные для сферы ИТ, а также детально рассмотреть процессы воздействия, мониторинга и контроля над рисками.

Глава 2. МЕТОДИЧЕСКИЕ СПОСОБЫ ОЦЕНКИ, ВОЗДЕЙСТВИЯ, МОНИТОРИНГА НЕИДЕНТИФИЦИРОВАННЫХ И КОНТРОЛЯ ИДЕНТИФИЦИРОВАННЫХ НЕГАТИВНЫХ И ПОЗИТИВНЫХ РИСКОВ В ИТ-ПРОЕКТАХ

2.1. Анализ существующих методов оценки рисков в ИТ-проектах

Уменьшение (увеличение) вероятности материализации рисков и (или) ослабление (усиление) их влияния на запланированные проектные цели за счет применения процессов риск-менеджмента, невозможно без использования специализированных методов оценки рисков, представленных в ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» [110]. Например, для идентификации рисков применяются методы основанные на ретроспективном анализе и экспертных мнениях. Для определения вероятности материализации рисков и возможного влияния в случаях их наступления, используются теория вероятностей, математическая статистика и теория случайных процессов [117]. Автор диссертационного исследования считает необходимым отметить, что несмотря на универсальность, не все методы представленные в стандарте ГОСТ Р ИСО/МЭК 31010-2011 подходят для применения в ИТ-проектах, в связи с чем требуется их адаптация [116].

Одним из наиболее трудоемких процессов риск-менеджмента считается *процесс идентификации рисков*. По мнению В. О. Ключникова сложность выявления рисков вызвана свойством уникальности процессов в проектах, что порождает уникальные и скрытие риски [118, 119, 120]. Ученый в своих трудах отмечает, что в процессе выявления рисков необходимо обеспечивать высокий уровень качества, иначе неучтенные риски, реализовавшись в проектах приведут к незапланированным расходам.

Для выявления рисков отечественными (В. А. Никоновым, А. А. Поляковым, В. О. Ключниковым) и зарубежными (О. Хелмером, Н. Далкиным, Н. Ресчером, К. Эндрюсом, Т. Клетзом и др.) специалистами в областях управления проектами и управления рисками применяются различные методы, а также их комбинации в зависимости от типов проектов, их размеров и способов управления. Методы применяемые для выявления негативных и позитивных рисков представлены в таблице 2.1.

Таблица 2.1 – Методы применяемые для выявления рисков

№	Название метода	Название метода (перевод на русский)	Разработчики
1	Retrospective	Ретроспективный анализ проектных документов ранее завершенных проектов	В.А. Никонов [121], Россия А. А. Поляков и В.О. Ключников [122, 123], Россия
2	Brainstorming	«Мозговой штурм»	А. Осборн, США
3	Delhi	Метод Дельфи, дельфийский метод	О. Хелмер, Н.Далки и Н. Ресчер, США
4	SWOT matrix [124]	SWOT-анализ	К. Эндрюс, США
5	STEEP matrix (PEST matrix)	STEEP-анализ / PEST-анализ	М. Портер, Г. Минтзберг, Б. Хендерсон, Г. Хамел, США
6	HAZOP CHAZOP [125]	Исследование компьютерной опасности и работоспособности систем	Т. Клетз, Великобритания
7	SWIFT [126]	Структурированный анализ сценариев методом «что, если?»	Ф. Лавли, Великобритания
8	PHA	Метод «предварительный анализ опасностей для систем»	Э. Дж. Хенкли, Х. Кумамото, США
9	FTA	Метод «анализ дерева неисправностей»	Компания «Bell Telephone», Х.А. Уинстон, США
10	ETA	Метод «анализ дерева событий»	Комиссия по ядерному регулированию, США

Рассмотрим методы представленные в таблице 2.1 подробнее.

Ретроспективный анализ документации завершенных проектов. В своих трудах В. А. Никонов, А. А. Поляков, В. О. Ключников делают предположение о том, что качественно составленные проектные документы

могут значительно ослабить влияние негативных рисков [121, 122, 123]. Однако ученые в своих трудах не конкретизируют название проектных документов, в связи с чем автором диссертационного исследования был проведен анализ 51 проектного документа PMBOK® Guide, результатом которого стал пакет проектной документации, который включает в себя 10 документов. Согласно проведенным исследованиям данный пакет проектной документации может нивелировать вероятность материализации 26 негативных рисков, актуальных для сферы информационных технологий (таблица 2.2) [42, 225, 226].

Таблица 2.2 – Проектные документы нивелирующие влияние рисков

№	Название проектного документа	Название риска
1	Устав проекта	1. Риск допущения ошибок при формулировании конечных бизнес-целей ИТ-проекта
2	Технико-экономическое обоснование (ТЭО) [127]	2. Риск отсутствия прогнозируемого экономического эффекта
3	Реестр рисков [128, 129]	3. Риск материализации событий, которые повлекут катастрофические последствия
4	Спецификация продукта	4. Риск несоответствия ожиданиям заказчика 5. Риск несоответствия ожиданиям конечного пользователя 6. Риск того, что по факту ИТ-проект будет значительно сложнее, чем предполагалось изначально 7. Риск длительного анализа бизнес-процессов заказчика 8. Риск выявления скрытых, не обнаруженных ранее источников дополнительных затрат 9. Риск того, что заявленные технические требования будет невозможно реализовать 10. Риск применения ранее не используемых технологий 11. Риск использования устаревших технологий
5	Иерархическая структура работ (ИСР)	12. Риск того, что содержание конечного продукта будет не соответствовать ожиданиям заказчика 13. Риск неправильного ранжирования задач руководителем ИТ-проекта
6	Сетевой график и диаграмма Ганта	14. Риск ошибочной оценки сроков, необходимых для реализации проекта 15. Риск отставания от запланированных сроков
7	Бюджет проекта	16. Риск того, что бюджет проекта будет не соответствовать ожиданиям заказчика 17. Риск ошибочной оценки бюджетов, необходимых для реализации ИТ-проекта

Окончание таблицы 2.2

№	Название проектного документа	Название негативного риска
8	План управления коммуникациями	18. Риск отсутствия связи с субподрядом 19. Риск отсутствия актуальной информации, которая необходима для создания ИТ-продукта 20. Риск значительной временной задержки в получении ответов на задаваемые вопросы между участниками ИТ-проекта
9	План управления качеством	21. Риск низкого качества разработанного ИТ-продукта 22. Риск того, что качество конечного ИТ-продукта будет не соответствовать ожиданиям заказчика 23. Риск завышения качества руководителем ИТ-проекта 24. Риск допущения ошибок при реализации ИТ-проекта *(bugs)*
10	План управления рисками	25. Риск материализации событий, которые окажут катастрофическое влияние на процесс реализации ИТ-проекта 26. Риск отсутствия резервов, необходимых для принятия рисков

Метод «мозгового штурма», разработанный А. Осборном в 30-х годах XX века, является коллективным методом и может быть использован для идентификации рисков в ИТ-проектах. Основными преимуществами данного метода являются легкость его применения, а также позитивная коллаборация участников. Среди недостатков можно отметить низкий показатель выявления уникальных рисков, в связи с чем автором диссертационной работы рекомендуется для усиления творческой активности проектной команды использовать программное обеспечение «Speed Boat» [130].

Дельфийский метод, созданный в 60-е годы XX века сотрудниками RAND Corporation, изначально разрабатывался, как метод прогнозирования трендов развития технологий, а также возможных сценариев ведения войны. Однако универсальность алгоритма метода позволила использовать его для выявления вероятных проблем. Неоспоримым достоинством дельфийского метода является возможность идентификации уникальных рисков.

SWOT-анализ с 1963 года использовался, как метод стратегического планирования деятельности организации. Позднее, с развитием проектной деятельности, сильные стороны стали представляться, как свойства проекта и

коллектива, дающие преимущества, слабые стороны – свойства, которые ослабляют проект, возможности – внешние и внутренние факторы, дающие дополнительные преимущества по достижению целей проекта, угрозы – внешние и внутренние факторы, которые способны осложнить процесс достижения проектных целей. На практике метод SWOT-анализ усиливают и дополняют **STEEP-анализом**, который дает возможность исследовать социальные, технологические, экономические, экологические и политические риски.

Таблица 2.3 – Примеры отклонений и управляющих слов метода 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

Ученый-исследователь Т. Клетз, разрабатывая **Hazard and Operability Study** (HAZOP), в первую очередь стремился избежать таких

катастрофических проблем как пожары, выбросы вредных веществ и утечки на химических предприятиях [125]. Со временем его метод доказал свою работоспособность и в 1974 году способ идентификации рисков с помощью слов, таких как «НЕТ», «БОЛЬШЕ», «МЕНЬШЕ», «ЧАСТЬ» и др., вошел в состав обязательных методов рекомендуемых к использованию Институтом инженеров-химиков (IChemE). Позднее HAZOP был адаптирован к разработке программного обеспечения получившего название **C**ontrol **Haz**ards and **Op**erability Analysis или **C**omputer **Haz**ard and **Op**erability Analysis, сокращенно CHAZOP. Преимуществом метода CHAZOP является то, что благодаря управляющим словам (НЕТ, БОЛЬШЕ, МЕНЬШЕ и др.) коллективам предоставляется возможность взглянуть на проекты с разных точек зрения.

Примеры отклонений в результате применения метода CHAZOP для ИТ-проекта представлены в таблице 2.3. Стоит отметить, что управляющие слова необходимо использовать в различных областях (персонал, коммуникации, технологии и др.) увеличивая зону идентификации рисков.

Анализ сценариев развития ИТ-проекта методом **Structured What-If Technique** (SWIFT) является упрощенной версией метода CHAZOP [126]. Набор фраз, например, таких как «что, если… ?» «к чему это приведет… ?», «что случится, если… ?», «может ли кто-либо… ?», «может ли что-либо… ?» помогает коллективу идентифицировать возможные рисковые события и прогнозировать сценарии того, как будет вести себя проект в случаях их наступления. Главными достоинствами метода являются простота его использования (метод не требует предварительной подготовки) и графическое исполнение. Частный случай использования метода SWIFT для проблемы «пользователи недовольны разработанным ИТ-продуктом» представлен на рисунке 2.1.

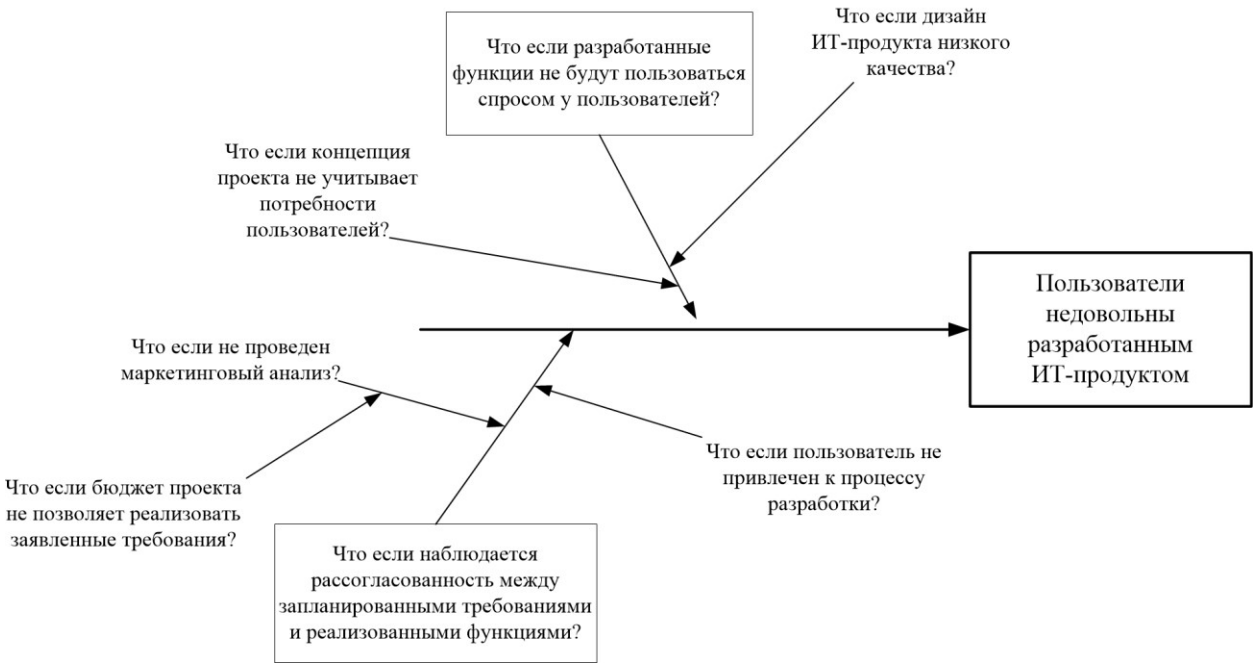


Рисунок 2.1 – Частный случай использования метода SWIFT для выявления негативных рисков в ИТ-проекте

Адаптированный для сферы ИТ **метод «предварительного анализа опасностей для систем»** или **Preliminary Hazard Analysis** (PHA) направлен на выявление возможных угроз, которые могут причинить вред используемому оборудованию или разрабатываемой системе. Благодаря определению критических контрольных точек методом «PHA» могут быть определены стадии процесса разработки, где требуется создание дополнительных профилактических мер, нивелирующих угрозу наступления катастрофических рисков. Отметим, что в методе «PHA» события вызывающие опасное состояние группируются на 3 класса. Первый класс – безопасный, т. е. событие не может оказать негативное влияние на проектные цели. Второй класс – пограничный (не вызывает поломки оборудования, отставание от запланированных сроков и др.). Третий класс – критический, например, уход ключевого сотрудника из проекта, отсутствие финансирования и др. Пример использования адаптированного метода «PHA» в ИТ-проекте представлен в таблице 2.4.

Таблица 2.4 – Пример использования адаптированного для сферы информационных технологий, метода «PHA»

№	Опасный элемент	Событие вызывающее опасное состояние	Последствия	Класс опасности
1	Персонал	Уход ключевого сотрудника в процессе реализации ИТ-проекта	1. Остановка проекта	Третий
2	Оборудование	Поломка оборудования	1. Остановка проекта	Второй
3	Оборудование	Отключение интернета	1. Потеря связи с сервером 2. Потеря связи с заказчиком, субподрядчиками и др.	Первый
4	Заказчик	Отказ от финансирования	1. Остановка проекта 2. Финансовые издержки 3. Судебные прения	Третий
5	Руководитель	Руководитель будет занят на других проектах	1. Будет отставание от запланированных сроков 2. Будет низкая производительность труда проектного коллектива	Второй

Метод «анализ дерева неисправностей» или **Fault Tree Analysis** (FTA) – это графический метод, который дает возможность выявлять риски и оценивать их. Метод «FTA» устанавливает взаимосвязь и взаимозависимость между многочисленными рисками с помощью логических схем. **Event Tree Analysis** (ETA), также является методом графического представления последовательности рисковых событий. Однако метод «ETA» направлен на исследование факторов и источников рисков.

Как видно из результатов проведенного исследования не один из рассмотренных методов идентификации рисков не является универсальным, т. к. каждый метод направлен на исследование только определенной области. В этой связи можно заключить, что для выявления уникальных и специфических событий необходимо использовать комбинации методов идентификации рисков. Данное утверждение также подтверждают в своих трудах В. Никонов, Е. Ю. Песоцкая, С. М. Авдошин [131, 132, 133]. Ученые рекомендуют улучшать процесс идентификации рисков:

- привлекать руководителей и менеджеров из смежных ИТ-проектов, заказчиков и других заинтересованных сторон проекта;
- использовать для определения рисков различные способы и методы;
- анализировать проектную документацию ИТ-проектов, которые были завершены ранее.

Далее рассмотрим методы применяемые для *анализа рисков*. Главной задачей анализа рисков является сбор исчерпывающей информации о вероятных негативных и позитивных событиях. В процессе анализа исследуются факторы рисков, источники рисков, а также прогнозируются последствия в случаях материализаций рисковых событий. На основании проведенного исследования автор диссертационной работы считает, что оптимальными методами для анализа рисков в ИТ-проектах являются «галстук-бабочка» (Bow-tie) (первый этап) [134], «почему-почему» и «диаграмма Исикавы» [135]. Методы, применяемые для анализа рисков в ИТ-проектах, представлены в таблице 2.5.

Рассмотрим данные методы более подробно.

Таблица 2.5 – Методы применяемые для анализа рисков

№	Название (оригинал)	Название (перевод на русский)	Разработчики
1	Bow-tie [134]	Методы «галстук-бабочка» (первый этап)	Лангминд Б., США
2	5Why	Метод «почему-почему»	Тоеда С., Япония
3	Fishbone Diagram, Cause and Effect Diagram [135]	«Диаграмма Исикавы»	Исикава К., Япония

Разработчик **метода «галстук-бабочка»** (первый этап) (Bow-tie) [134] Б. Лангминд (США) объединил воедино концепции двух методов, «дерево событий» и «дерево неисправностей», что дало коллективам возможность комплексно анализировать риски, получая исчерпывающую информацию об источниках рисков, а также возможных последствиях в случаях

материализации рисков [134]. В методе выделяют два основных этапа. На первом этапе проводится анализ рисков, где устанавливаются первопричины, порождающие риски и прогнозируются возможные последствия в случаях их материализации. На втором этапе создаются «барьеры», которые могут препятствовать появлению данных рисков и формируются «меры восстановления», т. е. меры, призванные нивелировать возможный ущерб. Пример графического представления метода «галстук-бабочка» (первый этап) показан на рисунке 2.2.

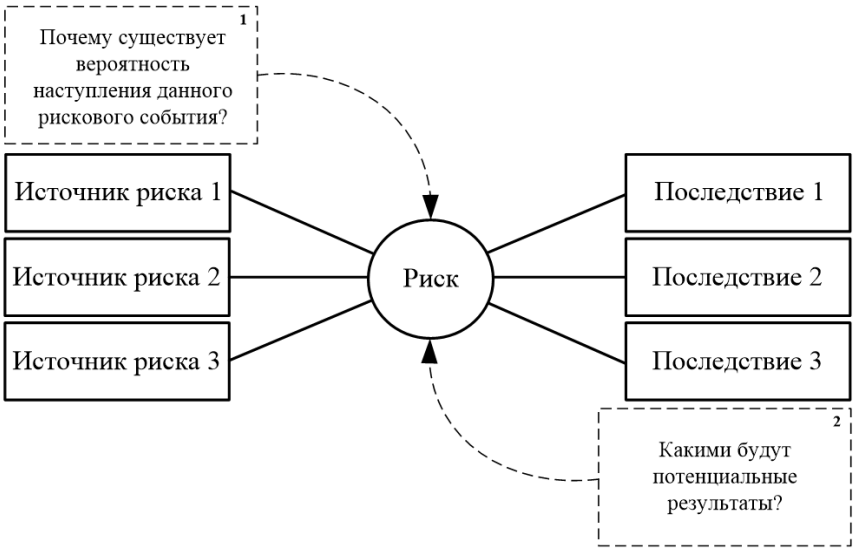


Рисунок 2.2 – Метод «галстук-бабочка» (первый этап) [134]

Следующим методом, который может быть использован для анализа рисков, является метод **«почему-почему»**. Формально способ поиска первопричины был предложен С. Тоеда с целью увеличения качества продукции фирмы «Тойота». Впоследствии метод стал применяться и в других сферах. Например, «почему-почему» часто практикуют в бережливом производстве [136], Кайдзен, шести сигмах [137] и в сфере информационных технологий. Суть метода заключается в последовательном задавании вопроса: «Почему наступает риск?» Если первопричина не установлена, тогда для полученных ответов повторно задается данный вопрос. Процесс повторяется до тех пор, пока первопричина(-ы) появления риска не будет

установлена. Отметим, что при использовании «почему-почему» могут быть определены риски, которые не были ранее идентифицированы, что является неоспоримым достоинством метода. Пример анализа негативного риска «по факту ИТ-проект значительно сложнее, чем предполагалось изначально» представлен в таблице 2.6.

Таблица 2.6 – Пример анализа негативного риска с помощью метода «почему-почему»

Название риска	**Вопрос «Почему?»**	**Вопрос «Почему?»**	**Корневая причина риска**
ИТ-проект будет значительно сложнее, чем предполагалось изначально	Заказчик не владеет всей информацией о существующих бизнес-процессах	Нет информации	Некомпетентный заказчик
	Функционал ИТ-продукта слишком велик	Привлечен не компетентный аналитик	Некомпетентный аналитик
	Руководитель ИТ-проекта не владеет всей информацией о существующих бизнес-процессах	Нет информации	Нет информации
	Руководитель ИТ-проекта не правильно провел оценку трудозатрат	Аналитик подготовил спецификацию ИТ-продукта низкого качества	Некомпетентный аналитик
		Руководитель ИТ-проекта не владеет, инструментарием оценки трудозатрат	Некомпетентный руководитель ИТ-проекта

Предложенный в 1952 году профессором Каору Исикавой графический способ анализа существующих причинно-следственных связей между факторами и последствиями (метод **«диаграмма Исикавы»**) позволил значительно улучить качество продукции фирмы «Тойота» [115]. Несмотря на значительный позитивный опыт применения данного метода необходимо отметить, что классическое представление «диаграммы Исикавы» не

соответствует современным требованиям сферы информационных технологий. Например, в ИТ-проектах вместо «производственного сырья» используются «большие данные *(big data)* и информация». Большие данные и информация являются главными ресурсами, которые необходимы для создания ИТ-продуктов и ИТ-сервисов. В этой связи адаптированная «диаграмма Исикавы» для сферы информационных технологий должна включать персонал, оборудование, информацию, внешнюю среду, контроль и технологии. Пример частного случая исследования риска «будет отсутствовать план-график в ИТ-проекте» с помощью «диаграммы Исикавы» представлен на рисунке 2.3.

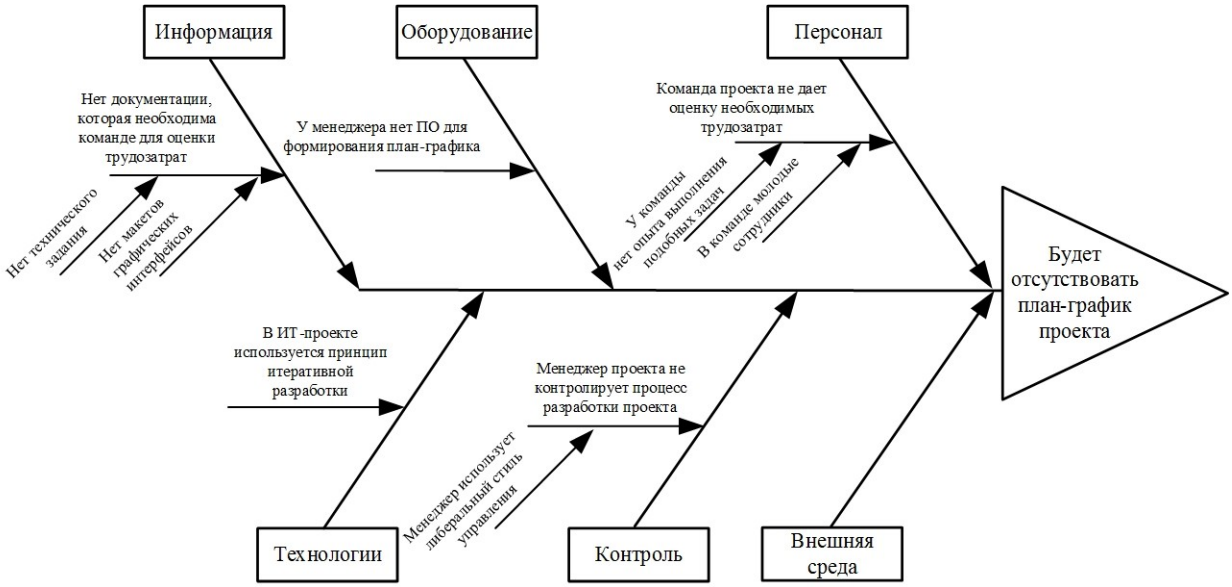


Рисунок 2.3 – Частный случай исследования риска с помощью «диаграммы Исикавы»

Далее рассмотрим методы, которые применяются для *оценивания вероятности материализации рисков и возможного влияния в случаях их наступления*. Методы оценивания рисков могут быть представлены двумя основными группами: количественные методы и качественные методы. Количественные методы – это методы, где используется математический

аппарат для прогнозирования и моделирования рисков [138]. К количественным методам относятся:

- аналитические методы оценивания рисков, предусматривающие построение математических моделей, которые решаются системой уравнений, описывающих проект в контексте его рисков;
- методы имитационного моделирования, где оценивание рисков проводится за счет проведения большого количества повторений;
- структурные методы – это методы, которые при моделировании стремятся учесть явные причинно-следственные связи;
- статистические методы, которые предусматривают моделирование риска на основе наблюдений случайных величин без принятия во внимание причинно-следственных взаимосвязей;
- методы смешанного типа используют различные сочетания количественных методов в целях получения наиболее точного результата в условиях существующих ограничений. Наибольшее распространение на практике получили комбинации статико-аналитических методов (сценарный анализ и стресс-тестирование) и структурно-имитационных методов (value at risk и back testing) [138]. Например, в статико-аналитических методах из статистических методов был заимствован прием отражения взаимосвязей между переменными, а из аналитических – метод реализации математических вычислений.

Качественные (экспертные) методы – это методы, где используются экспертные мнения для оценивания вероятностей материализации рисков и возможного влияния в случаях их наступления [139]. Данные методы базируются на профессиональном опыте экспертов, который агрегируется, обрабатывается и анализируется с помощью провалидированных вопросов.

Как правило, качественные методы применяются для оценивания рисков в случаях, когда в ИТ-проектах наблюдается большая неопределенность, имеется вакуум информации либо в ИТ-организации нет

накопленных статистических данных о материализовавшихся ранее рисках. Кроме того, в сфере информационных технологий выделяют и другие причины отказа от применения количественных методов, в частности:

- В работах Ю. М. Мадорской говорится о том, что время отводимое для планирования на подготовительных этапах проектов по разработке программного обеспечения ограничено, поэтому оценивание рисков необходимо проводить силами экспертов [140].
- Э. Рэймонд утверждает, что при проектировании ПО необходимо руководствоваться правилом KISS (Keep it Short and Simple) – «Простота кода – превыше всего», которое запрещает использование сложного инструментария [141]. Подобное правило декларирует простоту и прозрачность не только программного кода, но и простоту управления ИТ-проектом. По мнению Э. Рэймонда использование сложного управленческого инструментария, такого как количественные методы оценивания рисков, не объединяет заинтересованные стороны проекта, а скорее наоборот, разъединяет их.
- В работе Р. Джеффриса, Э. Андерсона и Ч. Хендриксона также акцентируется внимание на экспертных методах оценивания риска [142]. По мнению специалистов по реализации ИТ-проектов, в процессах проектирования ПО и управления должны подчиняться правилу YAGNI (You aren’t gonna need it) – «Вам это не понадобится», который декларирует отказ от избыточной функциональности и деятельности. Согласно аналитическим выводам Р. Джеффриса, Э. Андерсона и Ч. Хендриксона время, которое тратится на получение информации с помощью количественных методов целесообразнее расходовать на ретроспективу, тестирование и улучшение продукта.
- Использование количественных методов оценивания рисков противоречит концепции гибкой разработки ПО *agile* [123]. Согласно Agile Manifesto люди и их взаимодействие важнее инструментов, продукт важнее

проектных документов, сотрудничество важнее договора, готовность к изменениям важнее плана. Как видно из базовых принципов гибкой разработки программного обеспечения предпочтение отдается общению и работе с экспертами, а не формальным инструментам и проектной документации.

- Использование количественных методов не всегда возможно из-за свойств проекта. В силу определения PMBOK® Guide, «проект» – это уникальный процесс, направленный на создание уникальных продуктов, результатов и (или) услуг [40, 41, 42, 43]. В связи с этим использование статико-аналитических и структурно-имитационных методов не всегда возможно, так как часто недостаточно информации и накопленных статистических данных.
- Для краткосрочных ИТ-проектов, трудозатраты которых составляют менее 700 человеко-часов, использование количественных методов оценивания рисков являются нецелесообразным в связи с тем, что вероятность успешного завершения краткосрочных ИТ-проектов гораздо выше – 76%, чем у среднесрочных проектов – 14% и долгосрочных проектов – 10% [63, 64].

Как правило, количественные и качественные методы оценивания рисков применяются для определения вероятности материализации рисков, возможного влияния в случаях их наступления, а также времени актуализации рисков.

При работе с качественными методами оценивая рисков часто используют весовые коэффициенты, базирующиеся на вербально-числовой шкале Харрингтона [144, 145]. Примеры коэффициентов Харрингтона для оценок степени влияния и степени вероятности представлены в таблицах 2.7 и 2.8. На практике также можно встретить и другие весовые коэффициенты, например, коэффициенты 1, 2, 3, 5, 13, 20, 40, 100 Майкла Кона.

Таблица 2.7 – Коэффициенты Харрингтона, которые используются для оценивания возможного влияния риска в случае его материализации

Степень влияния риска	**Коэффициент Харрингтона (согласно PMBOK® Guide)**	**Коэффициент Харрингтона**	**Комментарии**
Очень высокая	0,8-1,0	5	Работы в проекте полностью остановлены
Высокая	0,64-0,8	4	Работы в проекте выполнены, но с большим опозданием
Средняя	0,37-0,64	3	Есть задержка в выполнении работ, но проект принят заказчиком
Низкая	0,2-0,37	2	Работы в проекте выполнены с небольшим опозданием
Очень низкая	0,1-0,2	1	Есть незначительные отставания от намеченного расписания
Нет влияния	0,0-0,1	0	Материальный ущерб отсутствуют

Таблица 2.8 – Коэффициенты Харрингтона, которые используются для оценивания вероятности материализации риска

Степень вероятности материализации риска	**Коэффициент Харрингтона (согласно PMBOK® Guide)**	**Коэффициент Харрингтона**	**Комментарии**
Очень высокая	0,8-1,0	5	Гарантированная материализация риска
Высокая	0,64-0,8	4	Риск материализуется
Средняя	0,37-0,64	3	Нет гарантий, что риск материализуется, но все же такая возможность остается
Низкая	0,2-0,37	2	Остается возможность материализации риска
Очень низкая	0,1-0,2	1	Остается хоть и малая, но все же возможность материализации риска
Нет вероятности	0,0-0,1	0	Вероятность материализации отсутствует

Ключевым преимуществом применения коэффициентов Харрингтона является возможность расчета величины «подверженность риску». «Подверженность риску» – это характеристика риска, которая показывает

предрасположенность проекта к наступлению рискового события. Расчет «подверженности риску» проводится по формуле:

$$RE = \Pr \times \mathrm{Im} \quad (2.1),$$

где RE – «подверженность риску»; $\Pr$ − вероятность наступления рискового события; Im − влияние рискового события.

Полученные расчетные значения «подверженности риску», ранжированные с помощью матриц вероятности и влияния негативных (позитивных) рисков показаны в таблицах 2.9 и 2.10. Одним из преимуществ использования данных матриц является оперативное получение информации о наиболее важных рисках, представляющих потенциальную угрозу (пользу), а также о рисковых событиях, которыми руководители проектов и коллективы могут пренебречь.

Таблица 2.9 – Матрица вероятности и влияния негативных рисков согласно PMBOK® Guide

Влияние / **Вероятность**		**Коэффициенты Харрингтона для негативных рисков**					
		0	**1**	**2**	**3**	**4**	**5**
Коэффициенты Харрингтона	**5**	0	5	10	15	20	25
	4	0	4	8	12	16	20
	3	0	3	6	9	12	15
	2	0	2	4	6	8	10
	1	0	1	2	3	4	5
	0	0	0	0	0	0	0

Таблица 2.10 – Матрица вероятности и влияния позитивных рисков согласно PMBOK® Guide

Влияние / Вероятность		Коэффициенты Харрингтона для позитивных рисков					
		0	**1**	**2**	**3**	**4**	**5**
Коэффициенты Харрингтона	**5**	0	5	10	15	20	25
	4	0	4	8	12	16	20
	3	0	3	6	9	12	15
	2	0	2	4	6	8	10
	1	0	1	2	3	4	5
	0	0	0	0	0	0	0

Несмотря на простоту определения опасных (полезных) рисков с помощью матриц вероятностей и влияния, подобный способ имеет существенный недостаток. Например, если эксперты присвоили для определенного риска степень вероятности 0, а степень влияния – 5, то расчет «подверженности риску» покажет 0, что в дальнейшем приведет к игнорированию данного риска. О подобной проблеме в своих трудах упоминает Н. Н. Талеб [146, 147, 148]. Ученый утверждает, что существуют риски, которые экспертам изначально кажутся невозможными (вероятность наступления риска стремится к 0). Однако подобные трудно прогнозируемые риски все же случаются и последствия от их материализации чаще всего являются катастрофическими, например, пандемия коронавирусной инфекцией в 2019-2020 гг. (COVID-19). Подобные негативные события Н. Н. Талеб называет в своих трудах «черными лебедями» [148].

В седьмом издании стандарта управления рисками, разработанным Министерством обороны США, эксперты отказываются от расчета «подверженности риску» и используют коэффициенты Харрингтона (от 0 до 5), ранжируя рисковые события на 3 группы опасная, умеренная и безопасная группа [149]. Отметим, что Министерство обороны США рассматривает термин «риск» только в негативном ключе, где риск опасной группы способен нанести катастрофический ущерб в случае материализации, риск

умеренной группы – умеренный ущерб, риск безопасной группы – незначительный ущерб.

Т. Мерна и Ф. Ал-Хани в своих трудах предлагают способ в ранжировании негативных рисковых событий, также используя вербально-числовую шкалу Харрингтона с коэффициентами от 0 до 5 [150]. Авторы отказываются от поиска значений подверженности риску и предлагают распределять негативные риски на 4 группы:

- ***Катастрофический риск или «тигр»*** (tiger) – это негативный риск, который имеет высокую степень вероятности материализации и способен оказать значительное негативное влияние на достижение проектных целей. Необходимо отметить, что по мнению Т. Мерна и Ф. Ал-Хани, материализация хотя бы одного «тигра», например, проект покинул руководитель проекта, становится катастрофической проблемой и чаще всего приводит к полной остановке проектных работ.
- ***Непредсказуемый риск или «аллигатор»*** (alligator) – это негативный риск, который имеет низкую степень вероятности материализации, но обладает способностью оказывать значительное негативное влияние на проектные цели. Как правило, к «аллигаторам» относятся правовые риски (комплаенс риски). Например, ИТ-компания реализующая ИТ-проект, может получить штраф в связи с нарушением императивных норм части 1 статьи 9.5 КоАП РФ, части 3 статьи 14.1 КоАП РФ, статьи 15.33.2 КоАП РФ, либо получить исковое заявление от заказчика, субподрядчика (статья 706 ГК РФ), поставщика и др. Необходимо отметить, что ущерб от материализации «аллигатора» сопоставим с ущербом, который может быть получен от материализации «тигра».
- ***Часто встречаемый риск или «щеночек»*** (puppy) – это негативный риск, который имеет высокую степень вероятности материализации, но при этом не способен оказывать какого-либо значительного влияния на проект. Примерами часто встречаемых рисков

могут быть риски, связанные с социально-психологической атмосферой в команде проекта, внутренней мотивацией, конфликтами и др.

- ***Несущественный риск или «котенок»*** (kitten) – это негативное рисковое событие, которое имеет низкую степень вероятности 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 ученые утверждают, что данными негативными рисками можно пренебречь [150].

Матрица вероятности и влияния, ранжирующая негативные риски согласно принципам Т. Мерна и Ф. Ал-Хани представлена на рисунке 2.4 [150].

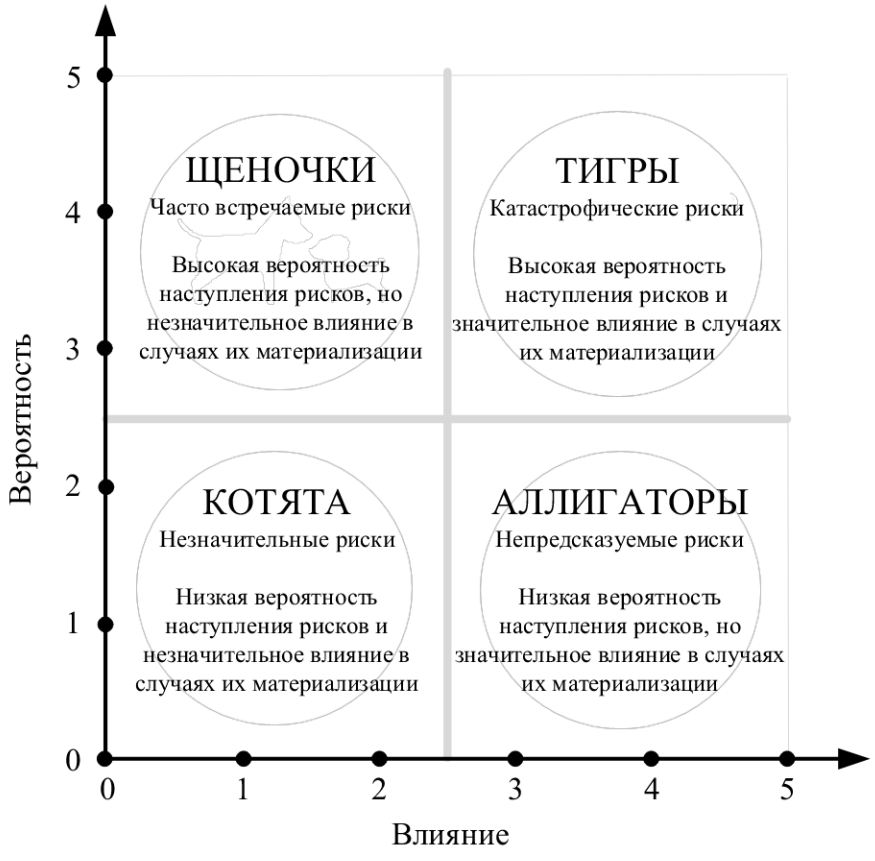


Рисунок 2.4 – Матрица вероятности и влияния Т. Мерна и Ф. Ал-Хани для негативных рисков

Необходимо отметить, что ранжирование негативных рисков, предложенное Т. Мерна и Ф. Ал-Хани, лучше подходит для ИТ-проектов, чем способы, предложенные в PMBOK® Guide или в директиве Министерства обороны США по следующим причинам:

- учитываются все негативные риски;
- ранжирование негативных рисков на «тигров», «аллигаторов», «щеночков» и «котят» дает возможность оперативно определять наиболее опасные риски;
- матрица вероятности и влияния (рисунок 2.4) наглядно показывает местоположение риска относительно других рисков.

Несмотря на удобство использования, предложенный Т. Мерна и Ф. Ал-Хани способ ранжирования рисков имеет существенный недостаток, а именно в нем отсутствует возможность группировки позитивных рисков. В связи с чем, автором диссертационного исследования был предложен способ группировки позитивных рисков:

- ***Созидательный риск или «слон»*** – это позитивный риск, который имеет высокую степень вероятности материализации и способен оказывать значительное влияние на цели проекта в случае своего наступления. Как правило, «слон» материализуется независимо от превентивных мер воздействия на риски, поэтому для позитивных рисков данной группы автор настоящего диссертационного исследования не рекомендует проводить какие-либо дополнительные стимулирующие меры.
- ***Непредсказуемый риск или «лев»*** – это позитивный риск, который имеет низкую степень вероятности материализации, но обладает способностью оказывать значительное влияние на проектные цели. Исходя из вышесказанного можно заключить, что «лев» имеет большой практический интерес для руководителей ИТ-проектов. Например, если заблаговременного будут проведены стимулирующие меры, то в ИТ-проект могут быть привлечены *Seniors* (ведущие программисты). Если подобных

мер не предпринять, то в ИТ-проекте программистов высокого квалификационного уровня не будет. Результаты исследований показывают, что материализация вышерассмотренного позитивного риска повышает вероятность успешного достижения запланированных проектных целей до 70% [224].

- ***Часто встречаемый риск или «обезьяна»***. Сепарация данного позитивного риска от остальных имеет большую практическую ценность, так как «дразня» руководителя ИТ-проекта «обезьяна» вынуждает расходовать ограниченные проектные ресурсы не оказывая при этом значительного влияния на процесс достижения запланированных целей, поэтому важно отделять «обезьян» от остальных позитивных рисков.
- ***Незначительный риск или «кролик»*** – это позитивный риск, который имеет низкую степень вероятности материализации и не обладает способностью оказывать значительное позитивное влияние на процесс достижения запланированных целей. Автор настоящего диссертационного исследования рекомендует «кролика» не учитывать и пренебрегать им при разработке мер превентивного воздействия на риски (меры «плана А») и мер принятия рисков (меры «плана Б»).

Матрица вероятности и влияния позитивных рисков представлена на рисунке 2.5.

При работе с качественными методами есть ряд ограничений, связанных с возможными ошибками, которые могут допускать эксперты в процессе оценивания и измерения рисков. Для увеличения точности экспертных оценок при использовании качественных методов необходимо рассчитать коэффициент конкордации (согласия) Кендалла:

$$W = \frac{12S}{m^2(n^3 - n)}, \qquad (2.2)$$

где m – это число экспертов; n – число факторов. Отметим, что для оценки рисковых событий используются два фактора – вероятность наступления и

возможное влияние, S – сумма квадратов разностей оценок (отклонений от среднего).

Рисунок 2.5 – Матрица вероятности и влияния позитивных рисков

Сумма разностей рангов может быть найдена по формуле:

$$S = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} R_{ij}\right)^2 - \frac{\left(\sum_{i=1}^{n}\sum_{j=1}^{m} R_{ij}\right)^2}{n}, \qquad (2.3)$$

где R –оценка присваиваемая i-му объекту j-м экспертом.

В диссертационной работе для коэффициента конкордации Кендалла автором предлагается использовать следующие условия:

- $W = 0$ – согласованности между экспертами нет. Если отсутствует согласованность оценок, то руководитель проекта самостоятельно определяет величины степеней вероятности наступления риска и возможного влияния;
- $W < 0{,}7$ – слабая согласованность;
- $W \geq 0{,}7$ – полная согласованность.

Подобная градация обусловлена тем, что при значении 0,7 обеспечивается высокая экспертная согласованность относительно оценивания вероятности реализации риска в ИТ-проекте и его возможного влияния в случае наступления. При низкой согласованности полученным значениям нельзя доверять в полной мере, следовательно, необходим повторный анализ с целью уточнения информации об истоках риска и возможных последствиях.

В связи с этим можно заключить, что для оценивания рисков в ИТ-проектах применяются как количественные, так и качественные методы. Однако количественную оценку рисков проводят только тогда, когда есть достаточный объем необходимых данных и статистической информации. При отсутствии достоверной информации применяются качественные методы.

Таким образом, в результате проведенного анализа существующих отечественных и зарубежных методов оценки рисков могут быть сделаны следующие выводы:

- *во-первых*, качественно подготовленные базовые проектные документы в ИТ-проектах нивелируют и (или) ослабляют влияние негативных рисков;
- *во-вторых*, для выявления уникальных рисков необходимо использовать комбинацию методов, т. к. методы, как правило, направлены на исследование определенной области;

- *в-третьих*, несмотря на удобство использования способа группировки рисков, предложенного Т. Мерна и Ф. Ал-Хани, данный способ ранжирования рисков имеет существенный недостаток, а именно, отсутствует возможность группировки позитивных рисков. В связи с чем автор диссертационного исследования предложил способ, где позитивные риски распределяются на такие группы, как созидательные риски (слоны), непредсказуемые риски (львы), часто встречаемые риски (обезьяны), незначительные риски (кролики). Подобный способ ранжирования позитивных рисков позволяет оперативно получать информацию о позиционировании позитивных рисков относительно друг друга, определять группу наиболее значимых позитивных рисковых событий, а также выявлять риски, которые не требуют разработки мер воздействия.

Необходимо отметить, что в процессе проведения анализа существующих методов идентификации рисков было установлено, что при получении информации об источниках рисков предоставляется возможность проводить их классификацию, т. к. становятся ясны связи между рисками и проектными целям, фазами жизненного цикла и др. Однако, как было отмечено ранее в параграфе 1.3 отсутствие единого инструментария управления проектами порождает проблему, связанную с отсутствием единого подхода к классификации рисков, что негативно сказывается на качестве идентификации рисков, на уровне управляемости, а также на мониторинге и контроле рисков.

2.2. Негативные и позитивные риски в ИТ-проектах

Проведенные исследования показали, что многие международные ассоциации, институты, отечественные и зарубежные ученые глубоко и существенно изучили проблематику классификации рисков. Однако, несмотря на теоретическую проработанность вопроса, они не нашли решение проблемы, связанной с тем, как необходимо классифицировать риски в ИТ-проектах. Предлагаемые способы часто противоречат друг другу и имеют существенные недостатки (таблица 2.11). Нерешенность указанной проблемы оказывает отрицательное влияние на процессы управления рисками в ИТ-проектах, что приводит к низкому качеству идентификации негативных, позитивных, скрытых и уникальных рисков, частой потери управляемости по причине отсутствия стандартизированных мер превентивного воздействия на риски (мер «плана А»), что в свою очередь ухудшает мониторинг и контроль рисков.

Таблица 2.11 – Недостатки основных способов классификации рисков

№	Авторы	Недостатки
1	Ю. П. Волкова, Е. А. Олейникова, М. В. Пирогов, В. С. А. Филин [151]	Не полностью охватывает сферу ИТ, ограничиваясь только уровнем предпринимательских рисков
2	И. Т. Балабанов и М. М. Максимцов [152]	Не учитывает источники рисковых событий, актуальных для сферы информационных технологий.
3	Т. Мерна и Ф. Ал-Хани [150]	Не учитывает специфику и особенности рисков, актуальных для сферы информационных технологий
4	Б. Мильнер и Ф. Лиис [152]	Распределение на внешние и внутренние риски не в полной мере соответствует представлениям об организациях работающих в сфере ИТ
5	Д. Н. Колесник [153]	Не удовлетворяет ни одному из требований
6	В. О. Ключников [118]	Не удовлетворяет ни одному из требований
7	А. В. Полковников, М. Ф. Дубовик, Е.Ю. Песоцкая [154]	Требование по улучшению контроля и мониторинга возможных угроз и опасностей удовлетворено не в полной мере
8	Ю. П. Ехлаков [155]	Не удовлетворяет требованиям, таким как обеспечение управляемости посредством стандартизации мероприятий реагирования и ликвидации последствий от наступления риска и улучшение контроля и мониторинга возможных угроз и опасностей

Рассмотрим подробнее наиболее популярные способы классификации рисков, которые предлагают отечественные и зарубежные ученые.

Ю. П. Волкова, Е. А. Олейникова, М. В. Пирогов и С. А. Филин классифицируют риски по масштабу проявления [151]:

- *макориски* – это глобальные риски, последствия от материализации которых отражаются на всех экономических агентах. Например, введение экономических санкций, военные конфликты, пандемия и др.;
- *мезориски* – это риски, которые актуальны только для определенного сектора экономики. Например, риски для металлургического и горнодобывающего сектора, финансового сектора, нефтегазового сектора, потребительского сектора и др.;
- *микориски* или предпринимательские риски – это риски, которые актуальны для индивидуализированного хозяйственного общества (ООО, ПАО и др.).

И. Т. Балабанов и М. М. Максимцов классифицируют риски используя финансовый признак [66].

Классификация рисков, разработанная Ф. Ал-Хани и Т. Мерна базируется на таких источниках рисков как рынок, политика, экономика, технологии, люди, криминал, загрязнение окружающей среды и др. Необходимо отметить, что данный способ не является универсальным, т. к. не учитывает специфику сферы информационных технологий [150].

Классификация рисков Б. Мильнера и Ф. Лииса дифференцирует риски на внешние и внутренние [152].

Д. Н. Колесник предлагает риски распределять по трем группам. К первой группе ученый предлагает отнести организационные риски. Ко второй группе Д. Н. Колесник предлагает отнести проектные риски. К третьей группе по мнению ученого следует отнести технические риски**.**

В. О. Ключников распределяет риски на внутренние, конкурентные и рыночные. Существенным недостатком данного способа классификации

является отсутствие многих областей, которые актуальны для сферы информационных технологий. Например, отсутствуют группы, связанные с фазами жизненного цикла, финансами, стихийными бедствиями, заказчиками, пользователями и др.

Для увеличения охвата областей рисковых событий А. В. Полковниковым, М. Ф. Дубовиком, Е. Ю. Песоцкой предлагается классифицировать проектные риски по [154]:

- *источникам риска*;
- *типами последствий от материализации риска*, например, А – самое значительное влияние, В – значительное влияние, С – незначительное влияние;
- *типами мер воздействия на риск*.

Способ предложенный А. В. Полковниковым, М. Ф. Дубовиком, Е. Ю. Песоцкой удовлетворяет определенным требованиям, которые предъявляются к классификации рисков в сфере информационных технологий. Данный способ классификации рисков позволяет выявлять специфические риски и обеспечивать управляемость проекта путем стандартизации мер воздействия на риски. Однако требование по улучшению контроля и мониторинга возможных угроз и опасностей удовлетворяется не в полной мере.

Классификация рисков предложенная Ю. П. Ехлаковым базируется на рискообразующих факторах [155]. Например, к внутренним рискообразующим факторам Ю. П. Ехлаков относит продукт, персонал, технологии реализации проекта и технологии управления процессом реализации проекта. К внешним рискообразующим факторам ученый относит государство, финансовый рынок и рынок труда. Данный способ классификации рисков имеет существенный недостаток. В частности, он не обеспечивает управляемость посредством стандартизации мер воздействия на риски, а также не улучшает контроль и мониторинг возможных угроз и опасностей.

Таблица 2.12 – Классификация рисков в ИТ-проектах

№	Классификационный признак группы риска в ИТ-проектах	Значение классификационного признака группы риска в ИТ-проектах
1	Среда	Внешний риск
		Внутренний риск
2	Внешний проектный источник	Риск, связанный с субподрядчиком(-ами) и поставщиком(-ами)
		Правовой риск
		Рыночный риск
		Риск, связанный с заказчиком(-ами)
		Риск, связанный со стихийными бедствиями
3	Внутренний проектный источник	Риск, связанный с требованиями
		Риск, связанный с технологиями
		Риск, связанный со сложностью ИТ-проектов и взаимодействием с другими системами
		Риск, связанный с качеством
		Риск, связанный с ресурсами
		Риск, связанный с коллективами ИТ-проектов
		Информационный риск
		Риск, связанный с руководителями ИТ-проектов
		Риск, связанный с финансированием
		Риск, связанный с расстановкой приоритетов
		Риск, связанный с планированием
		Риск, связанный с производительностью труда
		Риск, связанный с контролем
		Коммуникационный риск
4	Цель ИТ-проекта	Риск, связанный с длительностью ИТ-проектов
		Риск, связанный со стоимостью ИТ-проектов
		Риск, связанный с качеством ИТ-продуктов
		Риск, связанный с содержанием ИТ-продуктов
5	Фаза жизненного цикла ИТ-проекта	Риск, связанный с началом проекта
		Риск, связанный с организацией и подготовкой
		Риск, связанный с выполнением работ
		Риск, связанный с окончанием проекта
6	Срочность	Экстренный риск
		Срочный риск
		Несрочный риск
7	Негативный аспект	«Тигр» – Катастрофический негативный риск
		«Аллигатор» – Непредсказуемый негативный риск
		«Щеночек» – Часто встречаемый негативный риск
		«Котенок» – Незначительный негативный риск
8	Позитивный аспект	«Слон» – Созидательный позитивный риск
		«Лев» – Непредсказуемый позитивный риск
		«Обезьяна» – Часто встречаемый позитивный риск
		«Кролик» – Незначительный позитивный риск
9	Уровень управления	Управляемый риск
		Частично управляемый риск
		Неуправляемый риск

Стоит отметить, что отечественные и зарубежные ученые трактуют термин «риск» в негативном ключе. Данное обстоятельство не могло не

повлиять на предлагаемые ими способы классификации рисковых событий, которые акцентируют внимание в основном на отрицательных классификационных признаках. Однако, как было показано ранее «риск» обладает не только негативными свойствами, но и позитивными. На основании чего автором диссертационного исследования была предложена классификация рисков, базирующаяся на классификационных признаках, которые актуальны для сферы информационных технологий – среда, внутренние и внешние проектные источники, цель ИТ-проекта, фаза жизненного цикла ИТ-проекта, срочность, негативный и позитивный аспекты риска, уровень управления риском (таблица 2.12).

Отметим, что для проверки того, удовлетворяет ли предлагаемый автором диссертационного исследования способ классификации рисков в ИТ-проектах заявленным требованиям, таким как идентификация уникальных рисков, стандартизация мер воздействия на рисковые события и улучшение мониторинга и контроля рисков, требуется провести апробацию в действующих ИТ-организациях.

Как правило, по завершению идентификации рисков необходимо обработать полученный перечень рисковых событий для того, чтобы провести их классификацию и ранжирование. Согласно PMBOK® Guide обработку информации о рисках рекомендуется осуществлять с помощью:

1) иерархической структуры рисков (ИСР), в отечественной литературе также встречается другой понятие – «дерево рисков» [156];

2) ранжирования рисков [157];

3) матриц вероятностей материализации рисков и возможного негативного (позитивного) влияния для случаев их материализации [158].

Создание иерархической структуры рисков в ИТ-проектах весьма длительный и кропотливый процесс. Тем не менее, полученные результаты дают целостное представление о негативных и позитивных рисках, их структуре, категориях, подкатегориях и уровнях. Основываясь на

представленном в параграфе 2.2 авторском способе классификации рисков в ИТ-проектах могут быть выделены следующие категории [161]:

- *управленческие риски* – это риски, которые связаны с планированием, производительностью труда, контролем, коммуникациями, оцениванием сроков, бюджетов и ресурсов проекта;
- *организационные риски* – это риски, сопряженные с ресурсами, проектной командой, информацией, финансированием, руководителем проекта, а также процессом приоритезации задач;
- *технологические риски* включают себя риски, относящиеся к функциональным и нефункциональным требованиям ИТ-проекта, а также риски, связанные с качеством ИТ-продукта[159];
- *внешние риски* – это комплаенс риски, рыночные риски, стихийные бедствия, а также рисковые события возникающие по вине субподрядчика (ст. 706 ГК РФ), поставщика, заказчика и других заинтересованных сторон проекта [160].

Иерархические структуры негативных и позитивных рисков ИТ-проектов представлены на рисунках 2.6. и 2.7. Из иерархических структур рисков видно, что для ИТ-проектов негативных рисков значительно больше, чем позитивных. По мнению специалистов The Standish Group это связано с тем, что понятие «риск» чаще всего интерпретируется в негативном ключе. В это связи ИСР негативных рисков ИТ-проектов (рисунок 2.6) представляет собой более развитую структуру, чем ИСР позитивных рисков (рисунок 2.7).

Рассмотрим позитивные рисковые события, представленные на рисунке 2.7 подробнее.

Риск отсутствия субподрядчика. Согласно исследованиям британской аудиторско-консалтинговой компании «Ernst & Young», проекты, реализуемые собственными силами и ресурсами, являются более успешными, т. к. они мало зависят от внешних обстоятельств и уровня управленческой зрелости субподрядчиков.

Риск привлечения высококвалифицированного специалиста в проектный коллектив. Специалисты The Standish Group установили, что если в состав проектной команды входит *Senior*, то качество программного кода повышается. Кроме того, как было отмечено ранее в параграфе 2.2, результаты исследований показывают, что материализация вышерассмотренного позитивного риска повышает вероятность успешного достижения запланированных проектных целей до 70% [224].

Риск уменьшения численности коллектива ИТ-проекта до 6 человек. В докладах CHAOS Manifesto приводятся статистические данные, которые показывают, что ИТ-проекты, в состав которых входили менее 6 участников, были гораздо успешнее, чем проекты, где принимало участие более 6 участников [63, 64].

Риск привлечения руководителя, который имеет профессиональное образование в области управления проектами и опыт управления проектами более 2-х лет. В аналитических отчетах CHAOS Manifesto утверждается, что на успешное завершение проекта могут влиять профессиональные и личные качества руководителя. Например, если руководитель имеет профессиональное образование в области управления, то его проекты, как правило, разрабатываются согласно базовым, общепринятым концепциям и способам управления проектами, что нивелирует значительную часть управленческих и организационных рисков. Также стоит упомянуть результаты исследования В. А. Гаги, С. А. Козловой, А. П. Тютюшева, Е. Н. Ярославцевой, которые показывают, что на эффективность и работоспособность рабочих групп значительно влияет руководитель, а именно эмоциональный интеллект *(emotional intelligence, EI)* [162]. Например, эксперименты показали, что негативные эмоции, демонстрируемые руководителями быстро передаются окружающим, влияя на их результативность, координацию, мотивацию и энтузиазм.

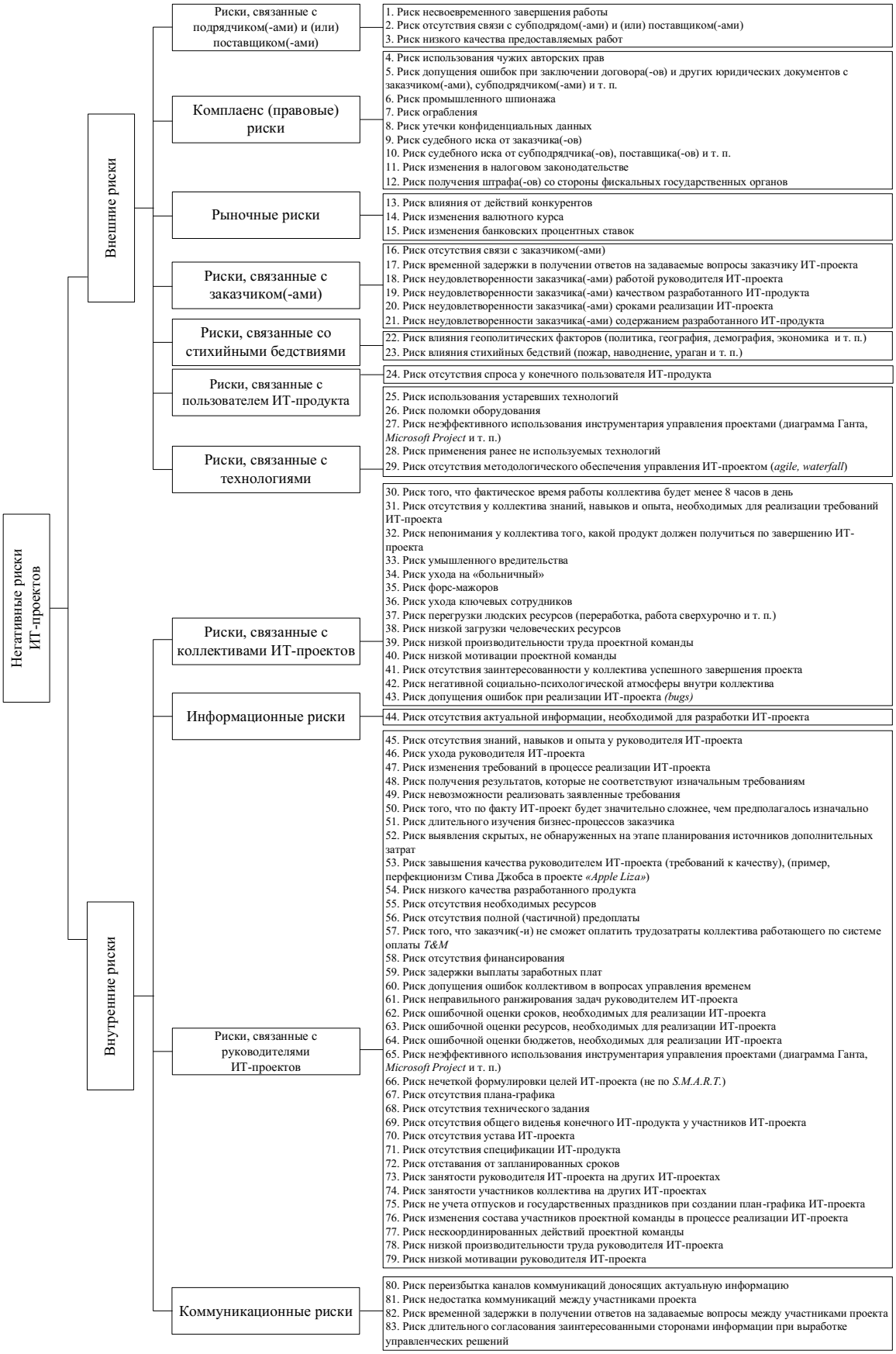


Рисунок 2.6 – Иерархическая структура негативных рисков ИТ-проектов

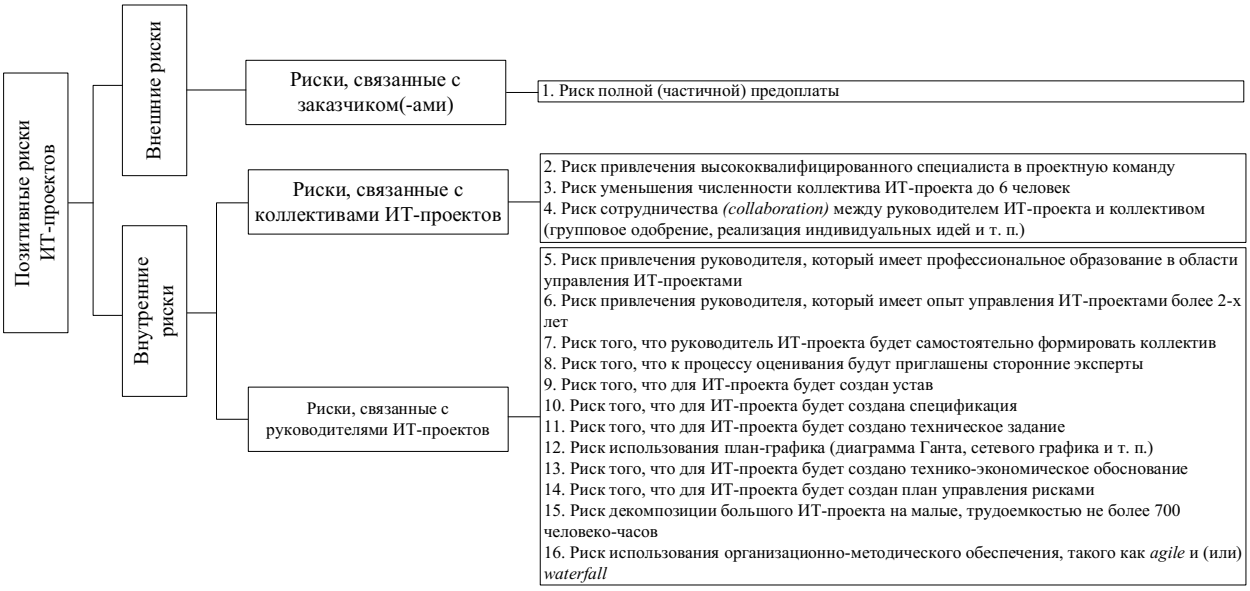


Рисунок 2.7 – Иерархическая структура позитивных рисков ИТ-проектов

Риск декомпозиции долгосрочного ИТ-проекта на краткосрочные ИТ-проекты. Согласно статистическим данным доля краткосрочных ИТ-проектов, трудоемкость которых составляет не более 700 человеко-часов равна 76%, в то время как доля среднесрочных – 14%, долгосрочных ИТ-проектов – 10% [63, 64]. Результаты данной статистики находят свое подтверждение в трудах К. Де Беккера, А. Бунстра и Х. Вортмна [163, 164, 165, 166]. По мнению ученых ежегодное увеличение бюджетов долгосрочных ИТ-проектов федерального значения во многом связано с тем, что при их большом размере возникают многочисленные проблемы, связанные с актуальностью и изменением требований.

Таким образом, подводя итог анализа иерархических структур рисков можно заключить, что несмотря на длительный и трудоемкий процесс обработки рисков, ИСР дает возможность систематизировать негативные и позитивные рисковые события, повышая качество идентификации рисков, обеспечивая их группирование и увеличивая управляемость ИТ-проектов.

Следующим шагом обработки полученного перечня негативных и позитивных рисков является процесс их ранжирования. Цель ранжирования –

определение приоритетных рисков, для которых необходимо разработать меры воздействия.

Для ранжирования негативных и позитивных рисков, представленных на рисунках 2.6 и 2.7 было проведено экспертное оценивание, состоящее из следующих этапов:

- подбор экспертов и формирование экспертных групп;
- составление анкет и формулирование вопросов;
- работа с экспертами;
- формирование правил обработки экспертных оценок;
- анализ и обработка экспертных оценок.

На первом этапе экспертного оценивания негативных и позитивных рисков были отобраны 10 специалистов в области управления ИТ-проектами из различных ИТ-компаний [167, 168, 169, 170, 171, 172, 173]. Все респонденты имели профессиональное образование и опыт работы в сфере информационных технологий не менее 4 лет. Следует отметить, что данная численность обусловлена двумя факторами: во-первых, верификацией экспертных оценок; во-вторых, возможностью получения более достоверных оценок при большем количестве экспертных мнений.

Второй этап включал в себя разработку опросных листов для проведения индивидуального анкетирования. Пример вопросов задаваемых экспертам представлен в Приложении А.

Работа с экспертами включала в себя оценивание двух параметров: вероятности материализации рисков и возможного влияния. Оценивание проходило с использованием коэффициентов Харрингтона от 0 до 5, где 0 – нет вероятности (влияния), 5 – риск неизбежен (значительное влияние).

Для получения интегральных оценок использовался коэффициент Кендалла (формула 2.3). При полной согласованности, когда $W \geq 0{,}7$, значения вероятностей и влияний заносились в итоговые реестры (см. Приложение К).

На заключительном этапе интегральные оценки вероятностей материализации рисков и тяжестей последствий были формализованы в реестры. Отметим, что для негативных рисков рейтинг построен по принципу группировки Т. Мерна и Ф. Ал-Хани [150]. Ранжирование же позитивных рисков проходило согласно авторскому способу, который был описан в параграфе 2.1.

Важно отметить, что для рисков, которые попадали в пограничное состояние между группами, окончательное решение о присвоении «группы риска» принималось респондентами на общем обсуждении. На основании анализа и обработки экспертных данных было установлено, что из общего количества выявленных рисков, актуальных для ИТ-проектов, насчитывается 25 «тигров», 30 «аллигаторов», 21 «щеночек», 7 «котят», 3 «слона», 12 «львов» и 1 «кролик» (см. Приложение К).

На основе систематизированной информации о негативных и позитивных рисках были построены матрицы вероятности материализации рисков и возможного негативного (позитивного) влияния (рисунки 2.8 и 2.9).

Подобное графическое позиционирование рисковых событий друг относительно друга дает возможность оперативно определить наиболее важные риски, для которых необходима разработка мер воздействия. Например, при работе с матрицей вероятности и влияния негативных рисков особое внимание следует уделять рискам групп «тигры» и «аллигаторы». Исследуя матрицу вероятности и влияния позитивных рисков акцент необходимо сместить на вероятные события, относящиеся к группе «львы», т. к. данные риски имеют потенциал на значительное увеличение шансов успешно завершать проекты.

Необходимо отметить, что картографирование и обработка информации с помощью инструментов, рекомендованных PMBOK® Guide, являются недостаточными для сферы информационных технологий, т. к. на практике руководителям ИТ-проектов необходимо знать на какой фазе жизненного цикла стоит ожидать материализации рисков.

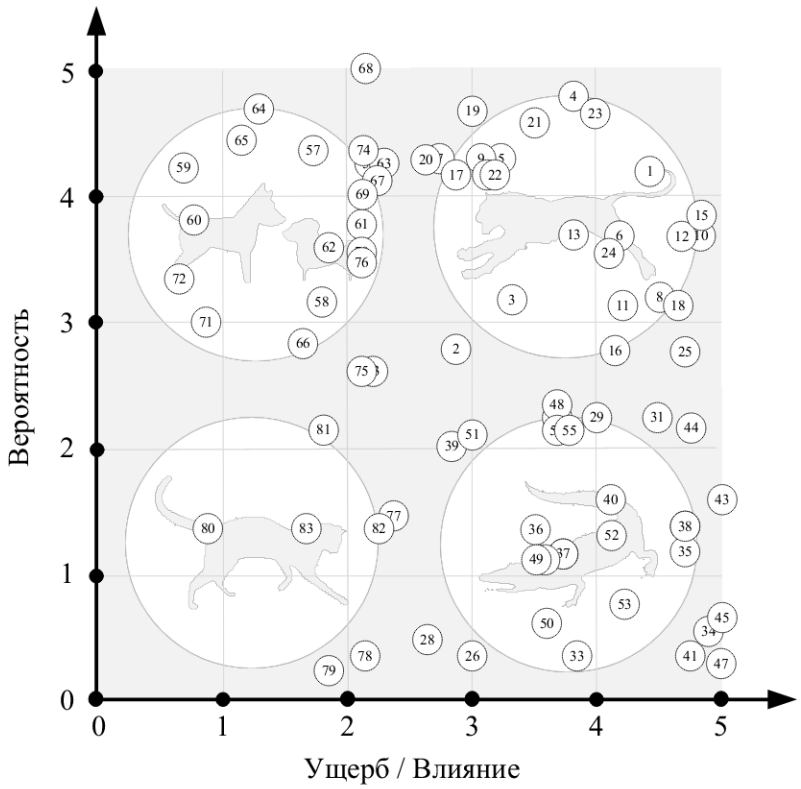


Рисунок 2.8 – Матрица вероятности и влияния негативных рисков ИТ-проектов. Номера соответствуют рискам из таблицы Приложения К

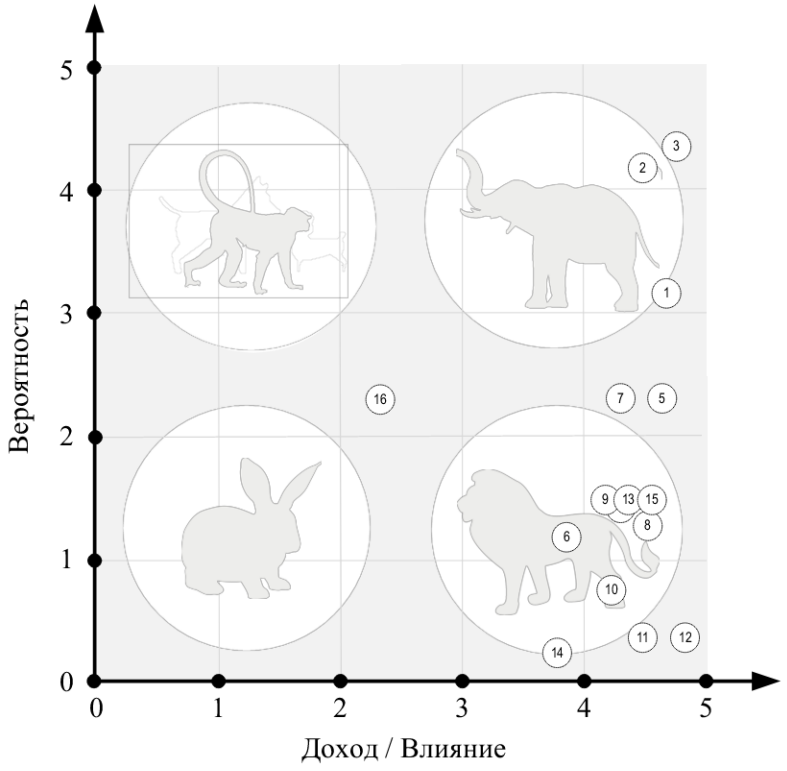


Рисунок 2.9 – Матрица вероятности и влияния позитивных рисков ИТ-проектов. Номера соответствуют рискам из Приложения К

Под *жизненным циклом проекта (project life cycle)* понимается набор фаз, через которые проходит проект с момента его начала до момента завершения. *Фаза проекта* – это совокупность операций, задач, действий и событий, которые завершаются достижением одного или нескольких запланированных результатов. В зависимости от типа, размера и сложности ИТ-проекта фазы проекта могут быть последовательными, итеративными или накладываться друг на друга. Многообразие возможностей построения логических связей между фазами проекта привело к созданию различных *моделей жизненных циклов* ИТ-проектов [174]. Среди основных моделей жизненных циклов выделяют:

- ***V-образную модель жизненного цикла*** (V-model, Validation & Verification Model). Фазы проекта следуют друг за другом последовательно в строго определенном порядке: концепция; проектирование архитектуры; детальное проектирование; реализация; модульное тестирование и интеграция; тестирование и проверка системы; внедрение в эксплуатацию и поддержка; проверка и утверждение [175]. *V-model* не предусматривает работу с параллельными задачами и событиями. Тестирование требований в жизненном цикле проекта происходит слишком поздно, вследствие чего невозможно внести изменения не повлияв на план проектных работ. Также существенным недостатком модели является отсутствие действий, направленных на оценку рисков.
- ***Модель быстрой разработки приложений*** (Rapid Application Development, RAD). *RAD* накладывает последовательные и итеративные фазы проекта друг на друга, привлекая все заинтересованные стороны ИТ-проекта для уточнения требований и оценки текущих результатов. Коммуникации с заинтересованными сторонами минимизируют негативные риски, связанные с качеством и содержанием конечного ИТ-продукта. Однако постоянное присутствие заинтересованных сторон «затягивает» процесс разработки, что часто оказывает катастрофическое влияние на успех проекта.

- ***Инкрементную модель жизненного цикла***. В инкрементной модели жизненного цикла фазы проекта линейно последовательны. ИТ-продукт обновляется от версии к версии, где новая версия включает в себя доработки и улучшения [175]. Использование подобной модели жизненного цикла значительно упрощает проектирование, поскольку в начале разрабатывается базовая архитектура информационной системы. Основным недостатком инкрементной модели жизненного цикла является возможность допущения ошибок при сборе требований на первых фазах проекта, что в последствии может привести к значительными изменениям содержания ИТ-продукта.

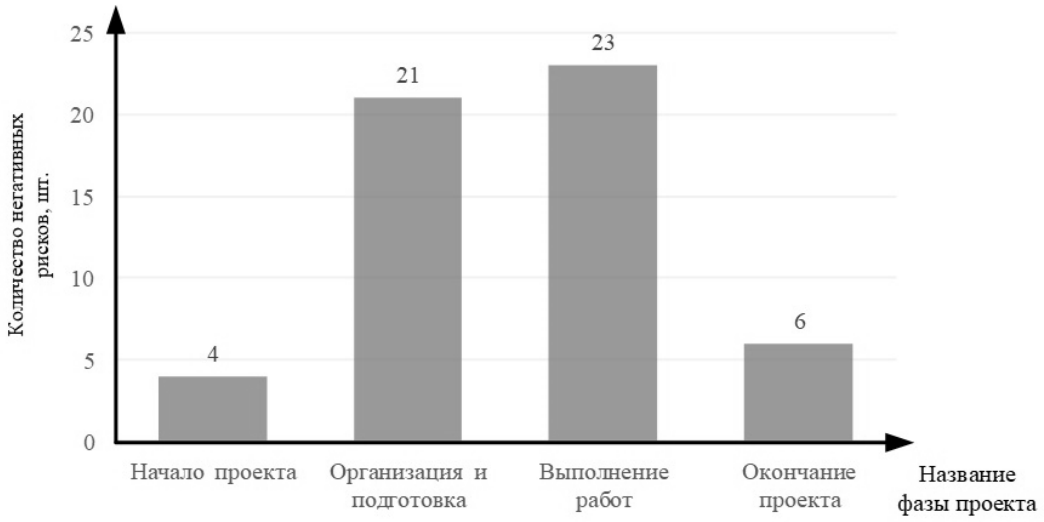
- ***Спиральную модель жизненного цикла Б. В. Боема***. Фазы проекта в модели Б. В. Боема являются итеративными, т. е. выполнение проектных работ идет параллельно с непрерывным анализом полученных результатов. Преимуществами модели является процесс оценки рисков, возможность выбора оптимального варианта разработки программного обеспечения, а также проведение корреляции между полученными прототипами и целями ИТ-проекта [60].

- ***Каскадную модель жизненного цикла*** *(waterfall model)* [175]. Фазы жизненного цикла идут друг за другом последовательно. Однако несмотря на ряд недостатков, которые были описаны ранее в параграфе 1.2, каскадная модель жизненного цикла может быть применима для любого типа (портал, сайт, ПО, мобильное приложение, корпоративная система, ERM-система), размера (краткосрочный, среднесрочный, долгосрочный) и сложности ИТ-проекта. По этой причине для дальнейшего определения времени актуализации рисков относительно фаз жизненного цикла в диссертационной работе будет использована каскадная модель включающая в себя такие фазы, как начало проекта, организация и подготовка, выполнение работ и окончание проекта.

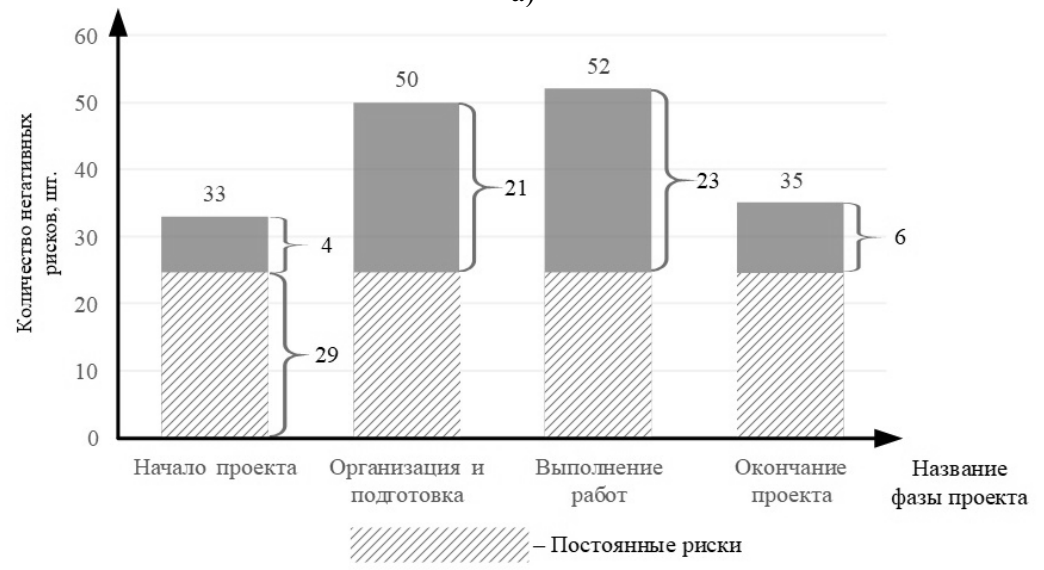
Результаты актуализации рисков относительно фаз жизненного цикла представлены в Приложении Л.

Количество негативных и позитивных рисков, распределенных относительно фаз жизненного цикла проекта показано на рисунке 2.10.

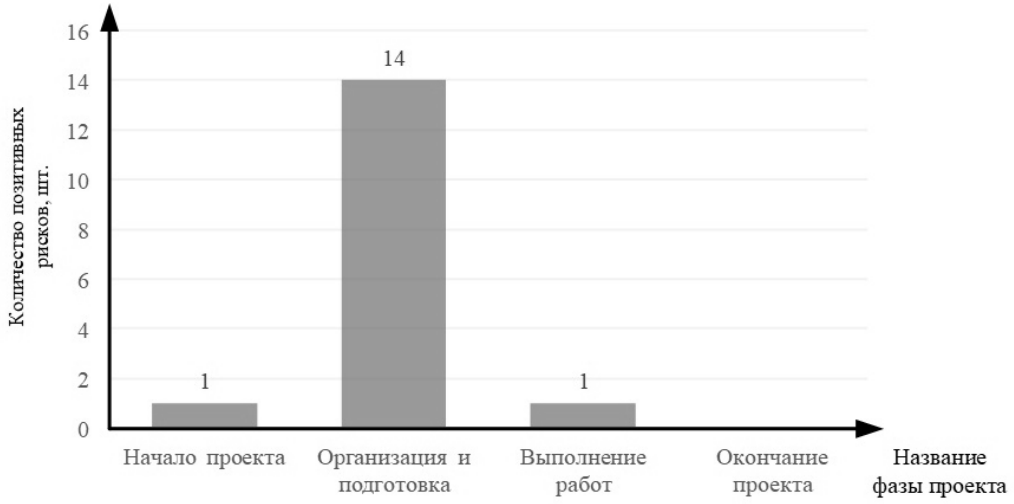
По результатам анализа иерархических структур негативных и позитивных рисков, актуальных для ИТ-проектов (рисунки 2.6 и 2.7) и фаз жизненного цикла было установлено, что наибольшая концентрация негативных рисков сосредоточена в фазе «выполнение работ» (рисунок 2.10 а), наибольшая концентрация позитивных рисков – в фазе «организация и подготовка» (рисунок 2.10 в). Также было установлено, что в ИТ-проектах существуют «постоянные риски», которые имеют потенциал материализоваться в любой временной период существования проекта.



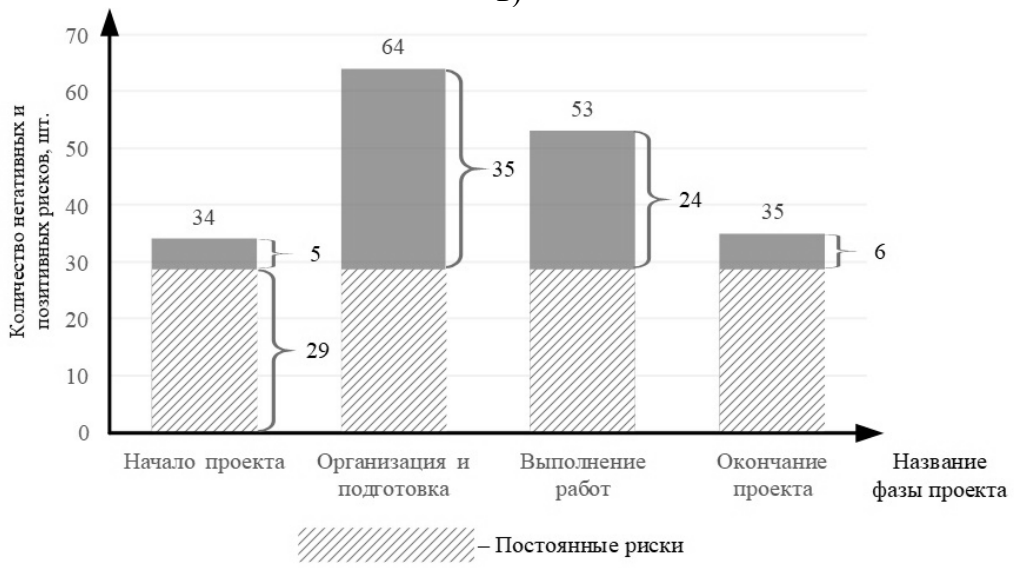
а)



б)



в)



г)

Рисунок 2.10 – Количество негативных и позитивных рисков, распределенных относительно фаз жизненного цикла проекта, где а) количество негативных рисков, распределенных относительно фаз жизненного цикла ИТ-проекта, без учета постоянных рисков; б) количество негативных рисков, распределенных относительно фаз жизненного цикла ИТ-проекта, с учетом постоянных рисков; в) количество позитивных рисков, распределенных относительно фаз жизненного цикла ИТ-проекта; г) общее количество негативных и позитивных рисков, распределенных относительно фаз жизненного цикла ИТ-проекта, с учетом постоянных рисков

Полученные результаты имеют большую практическую ценность, т. к. указывают ИТ-организациям, руководителям ИТ-проектов и проектным коллективам наиболее благоприятные временные периоды и фазы наибольшей опасности. Помимо прочего обнаружение «постоянных рисков» позволяет формализовать методическую рекомендацию, сутью которой является обязательное формирование материальных и временных резервов на случай материализации данных рисков.

Таким образом, в результате проведенного исследования установлено, что помимо стандартного инструментария обработки, классификации и картографирования рисков, в ИТ-проектах необходимо определять время актуализации рисков относительно фаз жизненного цикла. Было установлено, что информация о времени материализации рисков, способствует своевременному предупреждению их деструктивного воздействия на проектные цели в ИТ-проектах.

Также было обнаружено, что для процесса реализации ИТ-проектов актуальны 83 негативных риска, которые способны значительно навредить запланированным проектным целям, увеличивая итоговую стоимость работ и длительность разработки. На основании выше сказанного следует, что далее в диссертационном исследовании необходимо осветить вопросы поиска наиболее результативных и эффективных способов по разработке мер воздействия на риски.

2.3. Разработка инструментария воздействия, мониторинга неидентифицированных и контроля идентифицированных негативных и позитивных рисков в ИТ-проектах

Критическое осмысление многочисленных имеющихся негативных и позитивных рисков [185], представленных в Приложениях К и Л выявляет острую потребность в разработке действенных и результативных мер воздействия, мониторинга и контроля [176, 177]. По мнению Ю. Н. Болкунова [178], О. А. Казарцева и В. В. Бойко [179] квалитативные, превентивные, профилактические и резервные меры воздействия на риски способствуют уменьшению (увеличению) вероятностей материализации рисков, а также понижению (повышению) их влияния.

Стоит заметить, что *процесс разработки мер воздействия на риски* в ИТ-проектах является креативным и творческим. Во многом это связано с уникальностью проектных целей, нестандартностью поставленных задач, множеством противоречий между функциональными и нефункциональными требованиями, размерами и типами проектов. В связи с этим автор диссертационного исследования рекомендует применять различные методы отечественных (Г. С. Альтшуллером [180, 181, 182], Г. Я. Бушом, В. Гильде, К. Д. Штарке) и зарубежных (А. Осборном, У. Диснеем [183], Р. Б. Дилтсом, Эд. Де Боно [184] и др.) специалистов.

Методы, применяемые для разработки мер превентивного воздействия (мер «плана А») и мер принятия рисков (мер «плана Б»), представлены в таблице 2.13.

Важно подчеркнуть, что процессы воздействия, мониторинга и контроля являются индикатором результативности применения риск-менеджмента. Например, если на этапе планирования были проведены все необходимые меры, то по завершении проекта его фактические результаты должны совпадать с запланированными без каких-либо отклонений.

Таблица 2.13 – Методы, используемые для разработки мер воздействия на риски

№	Название	Название (перевод на русский)	Разработчики
1	Brainstorming	Метод «мозговой штурм»	Осборн А., США
2	Delhi	Метод Дельфи, дельфийский метод	Хелмер О., Далки Н. и Ресчер Н., США
3	Bow-tie	Метод «галстук-бабочка» (2-й этап)	Лангминд Б., США
4	Method of Walt Disney	Метод Уолта Диснея	Дисней У., Дилтс Р. Б., США
5	Six Hats Method	Метод разделения мышления де Боно, методы шести шляп, метод де Боно	Де Боно Эд., Великобритания
6	TRIZ	Теория решения изобретательских задач, ТРИЗ	Альтшуллер Г. С., СССР
7	Size Time Cost	Оператор РВС (размер, время, стоимость)	Альтшуллер Г. С., СССР
8	Method of little men	Метод маленьких человечков	Альтшуллер Г. С., СССР
9	Synectics	Метод «синектика»	Гордон У. Дж., США
10	The Meeting of the Pirates	Метод «корабельный совет»	Гильде В., Штарке К. Д., ГДР
11	Mind Map [186, 187]	Метод «интеллект карты»	Бьюзен Т., Великобритания
12	6-3-5 Brainwriting, 635 Method, Method 635	Метод «6-3-5»	Рорбах Б., Германия

Рассмотрим представленные в таблице 2.13 методы подробнее.

Дельфийский метод помимо возможности идентифицировать специфические, скрытые, негативные и позитивные риски может быть использован для разработки мер воздействия. Стоит отметить, что несмотря на такие преимущества, как легкость использования и возможность получения высоко результативных решений, метод имеет существенные недостатки:

- *во-первых*, эксперты могут критически оценивать мнение друг друга не приходя к консенсусу;
- *во-вторых*, длительный процесс коммуникаций может увеличить срок реализации проекта, что в условиях ограниченных ресурсов является неприемлемым;

- *в-третьих*, по мнению специалистов в области риска Ю. Н. Болкунова и О. А. Казарцева при использовании дельфийского метода может быть упущена возможность использования творческого потенциала коллектива [178, 179].

Метод «галстук-бабочка» (второй этап) благодаря анализу источников рисков, дает возможность оперативно создавать «барьеры», препятствуя появлению негативных рисков, а также вести разработку «мер восстановления», если негативные риски все же материализуются.

Схема создания мер воздействия на негативный риск с помощью метода «галстук-бабочка» (второй этап) представлена на рисунке рисунок 2.11.

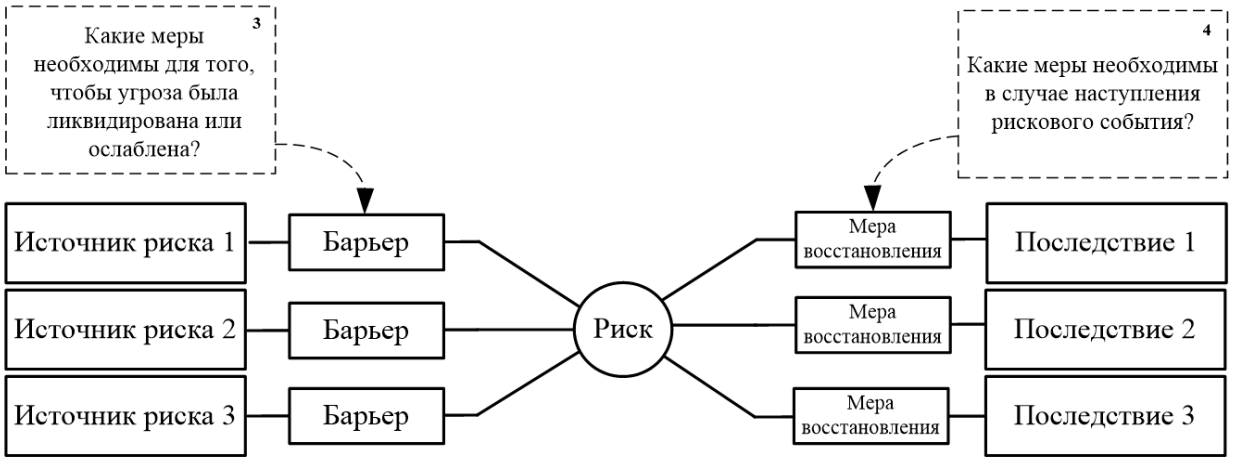


Рисунок 2.11 – Схема разработки мер воздействия на негативный риск с помощью метода «галстук-бабочка» (второй этап)

Метод «галстук-бабочка» акцентирует внимание на анализе и разработке мер воздействия только для негативных рисков, не рассматривая позитивный аспект природы риска. В связи с чем автор диссертационного исследования предлагает усовершенствовать метод «галстук-бабочка», включив в алгоритм «стимулирующие меры» и «меры усиления», которые будут акцентироваться на разработке мер воздействия для позитивных рисков. В качестве примера можно рассмотреть «риск привлечения в проект

опытного руководителя», где «стимулирующими мерами» будут поиск, проведение собеседований и отбор опытного руководителя, а «мерой усиления» будет заключение трудового договора.

Схема разработки мер воздействия для позитивного риска посредством метода «галстук-бабочка» (второй этап) представлена на рисунке 2.12.

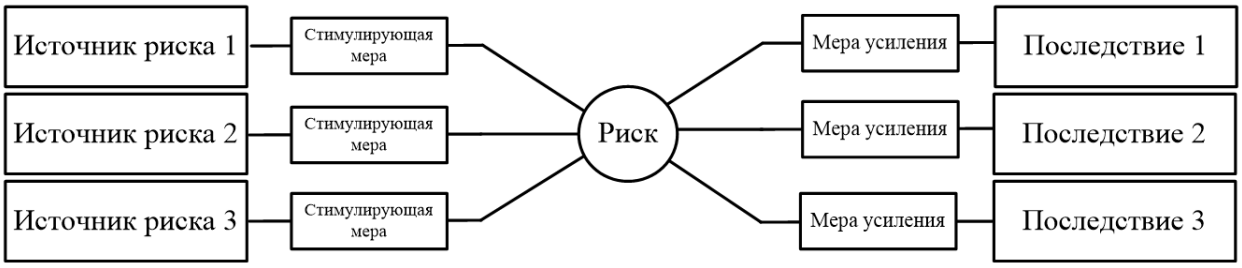


Рисунок 2.12 – Схема разработки мер воздействия на позитивный риск с помощью метода «галстук-бабочка» (второй этап)

Метод Уолта Диснея – это коллективный метод поиска мер воздействия на риски, который использует творческий потенциал проектной команды. Суть метода заключается в условном разделении мышления на «фантазера», «критика» и «реалиста». Направление мышления «фантазер» отвечает за поиск креативных идей, в том числе и фантастических, которые могут нивелировать и ослаблять (усиливать) негативные и позитивные риски. Мышление «критик» оценивает целесообразность предложенных мер, а направление мышления «реалист» анализирует эти меры и выбирает те, которые необходимо обязательно применить.

Классический алгоритм **метода де Боно** является универсальным и нацелен на поиск идей из различных сфер, таких как строительство, автомобилестроение, образование, информационные технологии и др. Однако, несмотря на простоту, метод может быть использован в ИТ-проектах только при определенных условиях. Во-первых, состав группы не должен превышать десяти человек, т. к. при увеличении численности респондентов уменьшается их коллаборация. Во-вторых, в состав группы должны входить

сотрудники, которые будут непосредственно разрабатывать ИТ-продукт. В-третьих, для разработки мер воздействия на риски должны быть привлечены эксперты.

Ядром **теории решения изобретательских задач (ТРИЗ)** стали 5 уровней изобретательности и сорок стандартных приемов, используемых изобретателями для решения сложных инженерных задач [180, 181]. Подобная классификация была получена благодаря проведенному Г. С. Альшуллером массовому исследованию более 40 тысяч патентов и авторских свидетельств в период с 1946 по 1971 гг. Стоит упомянуть о таких популярных инструментах ТРИЗ, как «устранение технических противоречий», оператор РВС (размер, время, стоимость), метод маленьких человечков, понятия «идеальной системы» и «идеальной программы». Современные модификации ТРИЗ успешно применяются и в сфере информационных технологий. К.П. Федоров в своих трудах отмечает, что благодаря использованию теории изобретательских задач могут быть разработаны меры, которые будут увеличивать функциональность разрабатываемой ИТ-системы при одновременном сокращении ее программного кода [188].

Среди организаций, занятых созданием ИТ-продуктов и ИТ-сервисов, большое распространение получил **метод «синектика»**, разработанный в 1960 году У. Гордоном. Основываясь на прямых, субъективных, символьных, фантастических аналогиях метод дает возможность находить креативные и нестандартные решения для специфических и уникальных рисков в ИТ-проектах. Однако для использования метода необходимо выполнять ряд условий, связанных с физической и ментальной подготовкой участников группы, длительным погружением, что часто требует изоляции коллектива, а также присутствием опытного модератора в составе рабочей группы. Подобные ограничения делают метод нерентабельным для краткосрочных и среднесрочных ИТ-проектов.

Метод «корабельный совет» является коллективным методом, где используется опыт, знания и фантазия участников группы, стремящихся найти наиболее результативные меры воздействия на негативные и позитивные риски, совместно критикуя и совместно защищая предложенные идеи. Суть метода заключается в порядке высказывания вариантов решения проблемы «от младшего» участника «к старшему». Метод прост в использовании, однако при его эксплуатации существует риск, что окончательное решение принимаемое «капитаном» может быть ошибочным.

Метод «интеллект-карты» является графическим методом исследования риска путем установления взаимозависимостей и взаимосвязей [186, 187]. Разработчик метода Т. Бьюзен утверждает, что процесс рисования в большей мере стимулирует творческий потенциал коллектива, нежели вербальная и аналитическая работа. По мнению эксперта, радиантный способ представления риска (расхождение многочисленных образов от центрального объекта) дает коллективу возможность оперативно исследовать структуру рискового события, провести его декомпозицию и найти наиболее результативное решение.

Суть **метода «6-3-5»** заключается в формализации 6 респондентами 3 вариантов того, как можно нивелировать (усилить) риск. Разработка вариантов длится в течение 5 минут.

Как видно из проведенного исследования, ни один из методов воздействия на риски не является универсальным. Каждый из методов использует различные способы получения наиболее результативных решений путем использования субъективного мнения, творческого потенциала коллектива, разнообразных алгоритмов и последовательности действий.

На основании проведенного анализа можно заключить, что для разработки мер воздействия на риски в ИТ-проектах необходимо использовать различные вариации методов (см. таблицу 2.14) и их комбинации с целью получения наибольшего количества альтернативных вариантов превентивных, профилактических и резервных мероприятий.

Далее рассмотрим виды стратегий применяемых в риск-менеджменте.

Таблица 2.14 – Стратегии воздействия на негативные и позитивные риски в ИТ-проектах

Тип риска	**Стратегия воздействия**	**Описание стратегии воздействия**
Негативный риск	Нивелирование	Выявляются источники риска с их последующей локализацией и ликвидацией
	Ослабление	Изменяется вероятность материализации риска и степень влияния
	Передача	Риск передается третьему лицу
	Эскалация	Риск передается лицу, который выходит за рамки проекта
	Наблюдение	Активных действий в отношении риска не ведется с целью определить, как он поведет себя в будущем
	Принятие	Нет активных действий в отношении риска. Высвободившиеся ресурсы направляются на резервы
Позитивный риск	Масштабирование	Увеличивается масштаб благоприятных эффектов, а именно, порождаются новые позитивные риски, которые ранее в проекте не были идентифицированы
	Усиление	Изменяется вероятность материализации риска и степень влияния
	Разделение	Передача владения благоприятной возможностью третьей стороне таким образом, чтобы она получила право на часть выгоды в случае ее реализации
	Эскалация	Риск передается лицу, который выходит за рамки проекта
	Наблюдение	Активных действий в отношении риска не ведется с целью определить, как он поведет себя в будущем
	Принятие	Нет активных действий в отношении риска

Согласно исследованиям, проведенным И. Селиховкиным, для обеспечения большей результативности разработанных мер необходимо использовать различные стратегии воздействия на риски [189]. По мнению И. Селиховкина, самой действенной стратегией является «нивелирование». Суть нивелирования заключается в прямом воздействии на источники рисков с целью их локализации и последующей ликвидации. Для позитивных же

рисков эксперт рекомендует использовать две стратегии – это «усиление» (меры воздействия увеличивают вероятность материализации рисков и масштаб влияния) и «использование» (меры воздействия, направленные на гарантированное сохранение благоприятных эффектов).

В PMBOK® Guide рекомендуется применять 10 стратегий для управления рисками [40, 41, 42].

В банковской и ипотечной сфере природу риска в основном рассматривают в негативном ключе, что сказывается на стратегиях риск-менеджмента. По мнению В. К. Селюкова и С. Г. Гончарова, для рисков могут быть использованы стратегии хеджирования и диверсификации [162].

Критически проанализировав предлагаемые отечественными и зарубежными учеными стратегии управления рисками, автор диссертационного исследования рекомендует использовать в ИТ-проектах только те стратегии, которые представлены в таблице 2.14, по следующим причинам:

- *во-первых*, представленные стратегии не противоречат универсальным стратегиям проектного управления PMBOK® Guide;
- *во-вторых*, стратегии оперируют как негативными, так и позитивными свойствами риска;
- *в-третьих*, данные стратегии имеют практическую ценность, заключающуюся в приоритезации мер воздействия [191].

Например, наиболее результативной стратегией управления негативными рисками является стратегия «нивелирования», т. к. осуществляется ликвидация источников риска. Следовательно, «нивелированные» риски не смогут себя проявить в будущем.

Далее идет стратегия «ослабления» направленная на перевод негативных рисков из опасных зон в безопасные (перевод рисков из группы «тигры» в группу «аллигаторы», перевод рисков из группы «аллигаторы» в группу «котята» и др.).

Следующей по результативности является стратегия «передачи», заключающаяся в передаче рисковых событий третьей стороне, которая берет на себя ответственность за управление рисками.

Стратегия «эскалация» является целесообразной в случаях, когда риски выходят за рамки проекта, либо когда предлагаемые меры реагирования выходят за рамки полномочий руководителя проекта. При «эскалации» руководитель проекта определяет, кого следует уведомить об угрозе и доводит информацию о ней до сведения этого лица.

«Наблюдение» используется, когда сущность рисков после анализа остается неясной. В этих случаях принимается решение о взятии паузы с целью понаблюдать, как будут вести себя данные риски в будущем.

В эпизодах, когда угрозы незначительны, либо когда меры воздействия экономически не оправданы, применяется стратегия пассивного «принятия». При данной стратегии превентивные действия не исполняются. Однако высвободившие ресурсы направляются на резервы – время, деньги и другие ресурсы, которые необходимы, чтобы встретить наступающие угрозы.

Рассмотренные выше стратегии воздействия на негативные и позитивные риски необходимы для создания плана мер превентивного воздействия на риски, или «плана А» *(contingency plan)*, а также для создания плана мер принятия рисков, или «плана Б» *(fallback plan)* [189].

План мер по превентивному воздействию на риски – это документ содержащий детальное описание мер упреждающего управления, который включает в себя следующие данные:

- перечень негативных и позитивных рисков;
- информацию о владельцах рисков *(risk owner)* – лицах, ответственных за мониторинг и контроль над риском, а также за выбор и выполнение соответствующей стратегии реагирования на риск;
- результаты анализа и оценивания рисков;
- стратегии воздействия на риски;

- информацию о необходимых ресурсах;
- триггерное условие *(trigger condition)* – событие или ситуация, указывающая на то, что риск вот-вот материализуется, т. е. признаки по которым можно понять, что меры «плана А» оказались нерезультативным и в ближайшем будущем стоит ждать материализации риска [192, 193].

«План Б» включает в себя резервы, которые используются в тех случаях, когда превентивные меры не принесли ожидаемого эффекта. Например, если на этапе реализации проекта триггерное условие негативного риска заблаговременного сообщило, что меры «плана А» не принесли ожидаемого эффекта, то тогда задействуются резервы «плана Б» [194]. Кроме того, меры «плана Б» необходимы для принятия вторичных рисков (рисков, возникающих в результате предпринятых мер реагирования) и рисков-невидимок (скрытых рисков, трансформирующихся сразу в проблемы).

Говоря о резервах «плана Б» необходимо упомянуть систему формирования резервов при разработке бюджета проекта [40, 41, 42]. Согласно PMBOK® Guide успех проекта завит от правильно выверенных резервов, в связи с чем бюджет ИТ-проекта необходимо дифференцировать по таким компонентам, как (рисунок 2.13):

- оценки стоимости работ;
- резерв на возможные потери *(contingency reserve)* – это время или деньги выделенные в базовом расписании или базовом плане по стоимости на случай наступления идентифицированных рисков;
- базовый план по стоимости *(cost baseline)* – это бюджет проекта, который не включает в себя никаких управленческих резервов;
- управленческий резерв *(management reserve)* – это сумма в бюджете проекта и запасное время в расписании проекта, которые зарезервированы для выполнения непредвиденной работы в рамках содержания проекта;

- бюджет проекта *(budget)* – это денежные средства, авторизованные для исполнения проекта.

Рисунок 2.13 – Компоненты бюджета ИТ-проекта

Подводя итог анализа методов, применяемых для разработки мер воздействия на риски, можно сделать вывод, что данный процесс является в большей степени творческим, требующим исчерпывающей информации о разрабатываемом проекте, сплоченного, готового к коллаборации и длительной креативной работе коллектива, а также профессиональных компетенций, необходимых для использования подобных методов, например, навыков лидерства и фасилитации. Также было установлено, что процесс разработки мер воздействия использует интеллектуальные ресурсы не только руководителей и проектных команд, но и всех заинтересованных сторон проекта, с целью выработки стратегии воздействия и последующей разработки плана мероприятий по превентивному воздействию на риски и плана мероприятий по принятию рисков, что делает данный процесс одним из самых трудоемких процессов риск-менеджмента.

Далее рассмотрим такие функциональные процессы риск-менеджмента, как *мониторинг и контроль рисков*. Отметим, что оптимальным механизмом обеспечивающим контроль рисков, являются триггерные условия, по

которым владельцы рисков могут понять, что превентивные меры не принесли ожидаемого результата. Процесс контроля триггерных условий индивидуален, т. к. риски закрепляются за конкретным участником коллектива. Во многом это связано с тем, что некоторые риски и их триггерные условия могут быть замечены только определенной группой узких специалистов [195]. Например, триггерное условие «во время тестирования была обнаружена ошибка в программном коде» для риска «запланированная на итерацию функциональность не завершится в срок» может заметить только разработчик программного кода.

Рынок предлагает обширный выбор программного обеспечения по автоматизации процесса контроля над рисками, а именно:

- *@RISK for Project Management* – программный продукт, выполняющий количественную оценку вероятности завершения проектов и оценку возможного перерасхода бюджетов. @RISK не является самостоятельным приложением, интегрируясь с программным продуктом Exel разработанным Microsoft. Несмотря на простоту использования, @RISK является локальной платформой и имеет существенный недостаток, т. к. одновременно с базой данных может работать только один участник проекта.
- *RiskTrack* – программный продукт, разработанный компанией RiskTrack International [196]. Программное обеспечение RiskTrack поддерживает процесс управления рисками путем контролирования расходов проекта и поддержки при идентификации и оценке рисковых событий. RiskTrack представляет собой хранилище рисков, которое также включает в себя информацию о вероятностях наступления рисковых событий, величине возможного ущерба и урона (дохода), мерах реагирования на риски.
- *OpenPlanProfessional* – это самостоятельный программный продукт, который позволяет оценивать вероятность завершения проекта с помощью использования расчета, базирующегося на методе Монте-Карло [197]. Одной из особенностей OpenPlanProfessional является возможность графического представления плана-графика проекта в виде

диаграммы Ганта и сетевого графика. К недостаткам OpenPlanProfessional можно отнести план-график, где не содержится информации о возможных негативных и позитивных рисках и отсутствие учета особенностей сферы информационных технологий.

- *RiskRadar* (платное ПО) обеспечивает управление рисками, связанными с коммуникациями, бюджетом, стоимостью, технологиями [198].
- *Risk Register* (платное ПО) представляет собой централизованное хранилище рисков с возможностями добавления дополнительной управленческой информации по каждому рисковому событию [199].
- *RiskGap* – это отечественный on-line сервис, который консолидирует информацию о рисках [200]. Главным преимуществом данного сервиса является возможность привлечения к одновременному управлению рисками всю проектную команду, также RiskGap предоставляет шаблоны рисков актуальных для ИТ-проектов, что облегчает процесс идентификации рисковых событий.

Стоит отметить, что рассмотренные программные продукты в основном концентрируют внимание на негативной природе риска и не учитывают благоприятные возможности. Однако несмотря на это, автор диссертационного исследования рекомендует к использованию RiskGap по следующим причинами:

- *во-первых*, функциональность RiskGap не противоречит разработанному инструментарию управления рисками в ИТ-проектах, хотя и не имеет программной функциональности для контроля над позитивными рисками;
- *во-вторых*, оценивание вероятности наступления рисков и возможный урон в случаях их наступления базируются на качественной оценке и осуществляются посредством вербально-числовой шкалы Харрингтона, что соответствует ограничениям предъявляемым к проектам в области ИТ;

- *в-третьих*, RiskGap имеет шаблоны рисков актуальных для сферы информационных технологий, что значительно упрощает процесс идентификации рисков.

Отметим, что процесс мониторинга и контроля рисков в ИТ-проектах может быть усилен операцией «систематический мониторинг и контроль над рисками», которая проводится во время ретроспективного анализа [201]. Автором диссертационного исследования рекомендуется во время ретроспективного анализа обсуждать следующие вопросы:

- Все ли функциональности и задачи, запланированные на спринт были завершены? Если нет, то почему?
- Материализовались ли в проекте проблемы, о которых ранее не было известно? Если да, то какие?
- Были ли во время спринта идентифицированы новые риски? Если да, то тогда нам необходимо провести оценку данных рисков и задействовать меры «плана Б», если выявленные рисковые события являются вторичными рисками или риск-невидимками;
- Были ли замечены триггерные условия? Если да, то необходимо задействовать меры «плана Б».

По мнению отечественных ученых И. Е. Никулиной и А. А. Тарабановского помимо «мониторинг-анализа», необходимо проводить «мониторинг-критерий», позволяющий руководителям в зависимости от установленных критериев получать набор управленческих воздействий и выбирать из них наиболее оптимальные [202]. Однако стоит отметить, что такой подход более целесообразно использовать при контроллинге общего состояния проекта.

На основании проведенного критического анализа основных процессов риск-менеджмента, таких как идентификация рисков, анализ рисков, оценивание рисков, воздействие на риски, мониторинг и контроль рисков, предоставляется возможность проследить изменение статуса риска в ИТ-

проектах. Схема жизненного цикла риска, представленная на рисунке 2.14 показывает, как при исполнении процессов риск-менеджмента изменяется статус рискового события от «неизвестного риска» до «управляемого риска».

Рисунок 2.14 – Жизненный цикл риска в ИТ-проектах

Стоит отметить, что на схеме жизненного цикла риска также учтен «наступивший риск», который может исходить, как от ранее выявленного «известного риска», так и от риска «неизвестного». В связи с этим для рисков, которые не были выявлены на подготовительных этапах предусмотрена следующая последовательность действий:

- анализ источников и воздействия, которые получил проект из-за наступления риска;

- ликвидация (усиление) эффекта от наступления риска;
- осуществление контроля и мониторинга.

Таким образом, в результате анализа методов, применяемых для разработки стратегий управления рисками, мер «плана А» и мер «плана Б», а также программного обеспечения, используемого для мониторинга неидентифицированных рисков и контроля индентифицированных рисков, можно заключить, что несмотря на многообразие и альтернативность способов, только малая их часть отвечает требованиям сферы информационных технологий и особенностям проектной деятельности, изложенной в PMBOK® Guide, RUP, PRINCE2, Agile и др. При этом основное управленческое внимание концентрируется на негативном аспекте природы риска с игнорированием положительных свойств. Учитывая вышеизложенные критические замечания, автором диссертационного исследования был разработан инструментарий по воздействию, мониторингу и контролю рисков в ИТ-проектах, способствующий ослаблению/усилению влияния рисковых событий на запланированные проектные цели.

Выводы по главе 2:

1. В рамках исследования был проведен анализ методов, применяемых для идентификации рисков в ИТ-проектах. Отечественный и зарубежный опыт выявления рисков показал, что для идентификации рисков необходимо применять различные методы и способы выявления рисковых событий. Причем для повышения качества идентификации рисков рекомендуется привлекать руководителей из смежных ИТ-проектов, заказчиков и других заинтересованных лиц проекта.

2. Установлена связь между проектными документами ИТ-проектов и рисками. Обнаружено, что наличие 10 проектных документов, таких как устав проекта, ТЭО, реестр рисков, спецификация продукта, ИСР, сетевой график и диаграмма Ганта, бюджет проекта, план управления коммуникациями, план управления качеством и план управления рисками

нивелирует и (или) ослабляет вероятность наступления и возможное влияние от материализации 26 негативных рисков.

3. Обосновано, почему предпочтение в ИТ-проектах при процессе оценивания рисков отдается качественным методам, а не количественным. Среди рассмотренных причин выявлены такие как:

- ограниченные ресурсы;
- принципы Agile Manifesto, KISS и YAGNI;
- отсутствие накопленных отечественных статистических данных о рисках ИТ-проектов в организациях.

4. На основе анализа способов ранжирования негативных рисков был предложен авторский способ группировки позитивных рисков на: созидательные риски («слоны»); непредсказуемые риски («львы»); часто встречаемые риски («обезьяны»); незначительные риски («кролики»). Подобный способ группировки позволяет определить наиболее благоприятные позитивные риски, которые требуют дополнительных стимулирующих мер, оперативно идентифицирует наиболее значимые риски, существенно сокращает материальные и временные затраты на управление рисковыми событиями в ИТ-проектах, а также дает возможность ИТ-организациям, руководителям ИТ-проектов и проектным коллективам позиционировать риски друг относительно друга и судить об общем состоянии ИТ-проектов.

5. Обнаружено, что международные стандарты управления рисками не имеют универсальной классификации рисков в сфере информационных технологий. Для решения данной проблемы был проведен анализ классификации и предложен авторский способ распределения рисков по областям (среда, уровень негативного (позитивного) риска, фаза жизненного цикла, проектные цели и др.), которые актуальны для сферы ИТ. Предложенная автором диссертационного исследования классификация рисков в ИТ-проектах способствует повышению качества процесса идентификации рисков, формализации единых мер воздействия на риски, а

также улучшению мониторинга неидентифицированных рисков и контролю идентифицированных рисков негативных и позитивных рисков.

6. Идентифицированы негативные и позитивные риски, актуальные для ИТ-проектов с последующим включением их в иерархическую структуру рисков, что позволяет заблаговременно предупреждать деструктивные воздействия на проектные цели. Также обоснованы причины появления и формы проявления данных рисковых событий в ИТ-проектах, представлены оценки определяющие их приоритезацию относительно возможного негативного (позитивного) влияния на проектные цели.

7. Показано, что помимо создания иерархических структур негативных и позитивных рисков, их ранжирования и построения матриц вероятностей материализации рисков и возможного негативного (позитивного) их влияния в ИТ-проектах, также необходимо определять время актуализации рисков относительно фаз жизненного цикла. Сигнализируя о приближении к наиболее значимым проектным периодам, время актуализации дает возможность заблаговременно подготовить руководителей ИТ-проектов и проектные команды к событиям, которые могут материализоваться в эти периоды.

8. Анализ методов, применяющихся для разработки мер воздействия на риски, позволил усовершенствовать метод «галстук-бабочка» (второй этап), который в классическом исполнении акцентирован на работу с негативными событиями. В рамках исследования были проведены авторские усовершенствования, которые включают «стимулирующие меры» и «меры усиления», позволяющие создавать меры воздействия на позитивные риски.

9. Выбраны определенные виды стратегий управления рисками, рекомендуемые автором диссертационного исследования для использования в ИТ-проектах, учитывающие как негативный (нивелирование, ослабление, передача, эскалация, наблюдение и принятие), так и позитивный (масштабирование, усиление, разделение, эскалация, наблюдение и принятие) аспекты природы риска.

10. Проведен сравнительный анализ программного обеспечения, применяемого для контроля над рисками, в ходе которого было установлено, что предлагаемые решения в основном акцентируют внимание на негативной стороне риска. К практическому использованию был рекомендован веб-сервис RiskGap, который учитывает особенности проектной деятельности, а также не противоречит разработанному автором диссертационного исследования инструментарию управления рисками в ИТ-проектах.

11. Предложен процесс «систематического мониторинга и контроля рисков», учитывающий особенности сферы ИТ независимо от используемого способа управления проектами (PMBOK® Guide, RUP, PRINCE2, Agile и др.). Данный процесс базируется на принципах реализации ИТ-проектов, что упрощает внедрение и использование процессов мониторинга и контроля над рисками.

Таким образом, на основе полученных результатов интегральных оценок негативных и позитивных рисков, а также анализа методов в сфере управления рисками, возникает острая необходимость в практической апробации с целью подтверждения или опровержения научной гипотезы о том, что разработка и функционирование ИТ-проектов происходит под воздействием как негативных, так и позитивных рисковых событий, существенно влияющих на запланированные проектные цели.

Глава 3. ПРИМЕНЕНИЕ ИНСТРУМЕНТАРИЯ УПРАВЛЕНИЯ РИСКАМИ В ИТ-ПРОЕКТАХ

3.1. Характеристика деятельности и финансовое состояние объектов исследования

Апробация разработанного инструментария риск-менеджмента в ИТ-проектах проходила в семи организациях: ООО «Аксимедиа Софт», ООО «Лидер Групп», ООО «Синтез Интеллектуальных Систем», ООО «Спейс-О Технологии», ООО «Телебриз», ООО «Контек Софт» и ООО «Сибэйдж» [167, 168, 169, 170, 171, 172, 173]. Несмотря на общий вид деятельности, связанной с разработкой программного обеспечения и оказанием услуг по цифровой автоматизации, вышеуказанные ИТ-организации имеют свою узкую специализацию, фокусируясь на создании корпоративных информационных систем, сайтов, мобильных приложений и продаже программных продуктов в высшие учебные заведения, организации нефтегазовой отрасли и металлургии.

В ходе проведенного исследования было установлено, что в данных организациях часто сознательно отказываются от риск-менеджмента либо частично используют процессы оценки рисков. Среди причин низкой популярности управления рисками в ИТ-проектах были выявлены следующие:

- ***Отсутствие экономической выгоды.*** По мнению менеджмента организаций, риск-менеджмент расходует ограниченные ресурсы не принося ощутимой пользы. Например, разработанный план управления рисками, как правило, быстро теряет свою актуальность, в связи с чем его необходимо постоянно обновлять. А. Сидоренко и Е. Демиденко объясняют данную проблему низким уровнем зрелости механизма управления рисками в организациях [203].

- ***Опасения нарушить отлаженный бизнес-процесс.*** Менеджмент ИТ-организаций сознательно отказывается от применения риск-менеджмента опасаясь, что новые бизнес-процессы окажут негативное влияние на уже отлаженную организационную систему [204].
- ***Не соответствует современным вызовам***. Считается, что риск-менеджмент не учитывает динамику изменений отечественного законодательства [205].
- ***Проблемы необходимо решать, тогда когда они есть***. Менеджмент ИТ-организации придерживается точки зрения, что с проблемами необходимо справляться только тогда, когда они материализовались [206, 207].

На основании проведенного исследования причин низкой популярности риск-менеджмента в ИТ-организациях могут быть сформулированы требования, которым должен отвечать риск-менеджмент в ИТ-проектах, в частности:

- инструментарий риск-менеджмента не должен противоречить способам реализации проектов, таким как *agile* и *waterfall*;
- риск-менеджмент должен учитывать особенности сферы ИТ и интегрироваться в любой проект независимо от его типа, размера и сложности;
- риск-менеджмент должен выявлять негативные, позитивные и уникальные риски;
- процессы идентификации, анализа, оценивания и воздействия на риски должны выполняться оперативно;
- применение риск-менеджмента в ИТ-проектах должно быть экономически оправдано. Стоит отметить, далее в диссертационной работе будет использоваться единица измерения – «человеко-час» [208, 209].

Перед апробацией разработанного инструментария риск-менеджмента было проведено исследование деятельности ИТ-организаций,

проанализировано их финансовое состояние, а также идентифицированы проблемы (на момент внедрения) с целью определения необходимости использования риск-менеджмента.

Анализ финансового состояния проводился на базе информации, которая была представлена в открытых источниках Главного межрегионального центра обработки и распространения статистической информации Федеральной службы государственной статистики (Росстат). Полученные результаты продемонстрированы в таблице 3.1. На основании анализа была определена динамика объемов выручек в исследуемых организациях на конец 2013-2017 гг. Отметим, что для ООО «Лидер Групп» и ООО «Телебриз» информация о доходах в базах данных ГМЦ Росстата отсутствовала [210].

Таблица 3.1 – Финансовые результаты ИТ-организаций за 2013-2017 гг.

№	Название организации	Выручка, тыс. руб.				
		конец 2013 г.	конец 2014 г.	конец 2015 г.	конец 2016 г.	конец 2017 г.
1	ООО «Синтез Интеллектуальных Систем»	0	0	2 804	7 535	5 510
2	ООО «Спейс-О технологии»	3 919	13 146	27 491	75 122	40 008
3	ООО «Аксимедиа Софт»	2 312	5 978	5 140	11 992	16 146
4	ООО «Контек Софт»	22 154	13 063	26 655	27 055	15 014
5	ООО «Сибэйдж»	18 847	17 200	25 931	58 441	67 987

Из таблицы 3.1 видно, что для исследуемых организаций в период 2013-2017 гг. наблюдается существенный рост выручки, кроме ООО «Аксимедиа Софт», где изменение прибыли на конец 2015 г. относительно 2014 г. составило -16,3%. Однако в 2014 году в ООО «Аксимедиа Софт» наблюдался значительный рост заработка на +61,3%. Стабильный рост выручки показала только одна из проанализированных организаций – ООО «Спейс-О технологии», где ее изменение доходов относительно прошлых лет увеличилось на +70,2% в

конце 2014 г. и на +52,2% в конце 2015 г. Подобные скачки связаны с тем, что с 2014 года организация вышла на международный рынок, реализуя ИТ-проекты для заказчиков из США, Индии и некоторых стран Европы. В остальных же организациях наблюдалось уменьшение доходов, например, в ООО «Контек Софт» падение в конце 2014 г. составило -69,6%, в ООО «Сибэйдж» -9,6%.

Анализируя показатели объемов выручек, можно получить представление о бюджетах и размерах реализуемых проектов. Например, показатель выручки в ООО «Синтез Интеллектуальных Систем», специализирующейся на разработке сайтов, не превысил 7 535 тыс. руб. ООО «Аксимедиа Софт», занятая на разработке мобильных приложений для платформ Android и iSO, достигла своего максимального уровня в 2017 г., заработав 16 146 тыс. руб. Организации ООО «Сибэйдж» и ООО «Спейс-О технологии» показывают примерно равную выручку 67 987 тыс. руб. и 40 008 тыс. руб. Это может быть объяснено тем, что данные организации специализируются в основном на реализации среднесрочных и дорогостоящих ИТ-проектов создавая корпоративные информационные системы, программное обеспечение, ERM-системы *(Enterprise Resource Planning)* для крупных заказчиков из нефтегазовой отрасли, металлургии, высших учебных заведений и т. п.

На основании анализа финансового состояния ООО «Синтез Интеллектуальных Систем», ООО «Спейс-О Технологии», ООО «Аксимедиа Софт», ООО «Контек Софт» и ООО «Сибэйдж» можно заключить:

- *во-первых*, с 2013 г. наблюдается рост объемов выручки от +16,2% до +85,7%;
- *во-вторых*, отсутствует финансовая стабильность (несмотря на положительную динамику, практически все организаций сталкивались с падением доходов);
- *в-третьих*, специализация бизнес-деятельности ИТ-организации влияет на объем их выручки.

Результаты идентифицированных проблем в рассматриваемых организациях на момент внедрения разработанного инструментария управления рисками представлены в таблице 3.2.

Было установлено, что в исследуемых организациях, кроме ООО «Телебриз», присутствует общая проблема, связанная со значительным превышением запланированных бюджетов. Исследование показало, что подобная трудность осложняет деятельность организаций, ухудшая бизнес-отношения с заказчиками и приводит к потере деловой репутации. Также наблюдается присутствие негативных рисков, таких как подача исков за неисполнение обязательств по договорам возмездного оказания услуг и «замораживание» ИТ-проектов с отказом заказчика от дальнейшего сотрудничества. Сотрудники управленческого аппарата данных организаций указывают следующие причины появления этой проблемы: в процессе реализации ИТ-проектов часто меняются требования; по факту реализуемые ИТ-проекты оказываются гораздо сложнее, чем планировалось изначально; субподрядчики несвоевременно завершают работы; проекты покидают ключевые сотрудники; проектами управляют неопытные руководители; состав участников проектов меняется в процессе реализации. Вышеперечисленные причины коррелируют с рисками, описанными ранее в параграфе 2.2.

Обнаружено, что с целью снижения стоимости проектов во многих исследуемых организациях были объединены функции руководителя проекта и аналитика (сотрудника, занятого оформлением бизнес- и технических требований ИТ-продукта). Подобная интеграция спровоцировала появление проблем, сопряженных с низким качеством проектной документации, неудовлетворительным управлением, переработкой руководителей. О подобных трудностях упоминается и в трудах В. А. Никонова, А. А. Полякова, В. О. Ключникова. Ученые отмечают, что низкое качество проектной документации впоследствии может создать проблемы, которые вполне можно было бы превентивно нивелировать [121, 122, 123].

Таблица 3.2 – Выявленные проблемы в исследуемых организациях на момент внедрения разработанного инструментария управления рисками в ИТ-проектах

№	Название организации	Название проблемы	Последствия
1	ООО «Синтез Интеллектуальных Систем»	Слияние функций руководителя ИТ-проекта и системного аналитика	• Низкое качество проектной документации (ошибки, неточности в формулировке требований, отсутствие важной информации) • Низкое качество управления • Переработка руководителя приводит к эмоциональному выгоранию
		Отсутствие в организации системного аналитика	• Снижение качества составления проектной документации • Требования, предъявляемые к ИТ-продукту, часто искажены и (или) не выявлены • ООО «Синтез Интеллектуальных Систем» не может реализовывать долгосрочные проекты
		Отсутствие сотрудников отвечающих за проверку и тестирование программного кода (тестировщики)	• Низкое качество программного кода в связи с допущением большого количества ошибок *(bugs)* • Увеличение сроков и стоимости бюджетов ИТ-проектов, т. к. сотрудники привлекаются для исправления программных ошибок
		Руководитель проекта курирует несколько ИТ-проектов	• Увеличение нормы управляемости приводит к ухудшению ведения проектной документации и к снижению качества управления
		Высокая доля проектов, где фактическая их стоимость превышает запланированные бюджеты	• Потеря деловой репутации • Риск получения иска со стороны заказчика • Риск того, что заказчик может отказаться от услуг ООО «Синтез Интеллектуальных Систем»
		Частый срыв запланированных сроков и перенос релизов	• Потеря деловой репутации • Риск получения иска со стороны заказчика
		Заказчики отказываются от дальнейшего сотрудничества после завершения проектов	• Увеличиваются расходы на рекламу, маркетинг, продвижение, на этапы заключения сделок и ведения переговоров • Потеря деловой репутации

Продолжение таблицы 3.2

№	Название организации	Название проблемы	Последствия
2	ООО «Лидер Групп»	Слияние функций руководителя ИТ-проекта и системного аналитика	• Низкое качество проектной документации (ошибки, неточности в формулировке требований, отсутствие важной информации) • Низкое качество управления • Переработка руководителя приводит к эмоциональному выгоранию
		Отсутствие сотрудников отвечающих за дизайн	• Сотрудник не выходит на связь, выполняет поставленные задачи с большим опозданием, предоставляет работу низкого качества
		Высокая доля проектов, где фактическая их стоимость превышает запланированные бюджеты	• Потеря деловой репутации • Риск получения иска со стороны заказчика • Риск того, что заказчик может отказаться от услуг ООО «Лидер Групп»
3	ООО «Спейс-О технологии»	Низкий уровень владения английским языком	• Из-за ухода ключевых сотрудников владеющих английским языком разрабатываемые проекты останавливаются
		Высокая доля проектов, где фактическая их стоимость превышает запланированные бюджеты	• Потеря деловой репутации • Риск получения иска со стороны заказчика • Риск того, что заказчик может отказаться от услуг ООО «Спейс-О технологии»
		Руководитель проекта курирует несколько ИТ-проектов	• Увеличение нормы управляемости приводит к ухудшению ведения проектной документации и к снижению качества управления
		Объемы работ в ИТ-проектах оказались больше, чем могли выполнить сотрудники ООО «Спейс-О технологии»	• Для работы были привлечены субподрядчики, которые некачественно выполнили работу • В 2015 г. ООО «Спейс-О технологии» был подан иск за неисполнение обязательств по договорам возмездного оказания услуг
4	ООО «Аксимедиа Софт»	Низкий уровень владения английским языком	• Из-за ухода ключевых сотрудников владеющих английским языком разрабатываемые проекты останавливаются
		Слияние функций руководителя ИТ-проекта и системного аналитика	• Низкое качество проектной документации (ошибки, неточности в формулировке требований, отсутствие важной информации) • Низкое качество управления

Продолжение таблицы 3.2

№	Название организации	Название проблемы	Последствия
4	ООО «Аксимедиа Софт»	Высокая доля проектов, где фактическая их стоимость превышает запланированные бюджеты	• Потеря деловой репутации • Риск получения иска со стороны заказчика • Риск того, что заказчик(-и) может отказываться от услуг ООО «Аксимедиа Софт»
5	ООО «Контек Софт»	Руководитель проекта курирует несколько ИТ-проектов	• Увеличение нормы управляемости приводит к ухудшению ведения проектной документации и к снижению качества управления
		Заказчик отказался платить за выполненную работу	• В 2013 г. ООО «Контек Софт» был подан иск за неисполнение обязательств по договорам возмездного оказания услуг
		Высокая доля проектов, где фактическая их стоимость превышает запланированные бюджеты	• Потеря деловой репутации • Риск получения иска со стороны заказчика • Риск того, что заказчик может отказаться от услуг ООО «Контек Софт»
6	ООО «Телебриз»	Низкий уровень владения английским языком	• Из-за ухода ключевых сотрудников владеющих английским языком могут быть потеряны клиенты (клиенты ООО «Телебриз» граждане США)
		Уменьшение количества клиентов из-за действий конкурентов	• Снижение объемов выручки
7	ООО «Сибэйдж»	Заказчик отказался платить за выполненную работу	• В 2015 г. и 2017 г. ООО «Сибэйдж» были поданы иски за неисполнение обязательств по договорам возмездного оказания услуг
		Слияние функций руководителя ИТ-проекта и системного аналитика	• Низкое качество проектной документации (ошибки, неточности в формулировке требований, отсутствие важной информации) • Низкое качество управления
		Высокая доля проектов, где фактическая их стоимость превышает запланированные бюджеты	• Потеря деловой репутации • Риск получения иска со стороны заказчика • Риск того, что заказчик(-и) может отказаться от услуг ООО «Сибэйдж»

Стоить также отметить, что среди рассматриваемых организаций была идентифицирована проблема, связанная с комплаенс рисками, а именно неисполнение обязательств по договорам возмездного оказания услуг субподрядчиками и заказчикам. Например, в 2015 г. и 2017 г. ООО «Сибэйдж» выступала истцом в арбитражном суде, где общая сумма исков составила более 2 млн. руб. ООО «Контек Софт» в 2013 г. был подан иск в суд за неисполнение условий договора заказчиком. В 2015 г. состоялся суд, где иск, поданный ООО «Спейс-О Технологии» на субподрядчиков, был полностью удовлетворен.

Таким образом, критически осмыслив идентифицированные проблемы в ООО «Синтез Интеллектуальных Систем», ООО «Лидер Групп», ООО «Спейс-О Технологии», ООО «Аксимедиа Софт», ООО «Контек Софт», ООО «Телебриз» и ООО «Сибэйдж» на момент внедрения разработанного инструментария управления рисками, можно сделать следующие выводы:

- в организациях отсутствует инструментарий, идентифицирующий и стимулирующий наступление позитивных рисков;
- в данных организациях присутствуют актуальные проблемы, сопряженные с изменением запланированных проектных целей, а именно перерасход бюджетов и перенос релизов (показов ИТ-продуктов заказчику) на более поздние сроки;
- руководители, курируя несколько ИТ-проектов и беря на себя функцию по формализации требований, снижают качество проектной документации и не обеспечивают необходимого уровня управления;
- из-за перерасходов бюджетов, переносов релизов и низкого качества ИТ-продуктов заказчики отказываются от дальнейшего сотрудничества, оказывая негативное влияние на деловую репутацию организаций, увеличивая тем самым расходы на рекламу, маркетинг, продвижение и т. п.;

- несмотря на различия в специализации, исследуемые ИТ-организации имеют схожие трудности. Подобная взаимосвязь может быть объяснена тем, что независимо от типа, размера, способа реализации проектов, идентифицированные проблемы имеют общие источники (руководители проектов, коллективы, субподрядчики, заказчики и т. п.). Отметим, что эти источники коррелируют с внутрипроектными источниками рисков, которые были описаны ранее в параграфах 1.3 и 2.2. Иными словами, проблем, описанных в таблице 3.2 можно было избежать, если бы в анализируемых организациях и разрабатываемых ими проектах превентивно применялся инструментарий риск-менеджмента. Следовательно, можно заключить, что актуальность использования управления рисками в ИТ-проектах и ИТ-организациях подтверждена.

Для того, чтобы экспериментально подтвердить, что разработанный инструментарий управления рисками в ИТ-проектах отвечает выдвигаемым требованиям и дает возможность решить идентифицированные проблемы (таблица 3.2), в исследуемых организациях были выбраны 11 ИТ-проектов разного типа, размера, с разной численностью проектных коллективов (от 4 до 10 сотрудников). Например, чтобы соответствовать требованию сопряженному с размером проекта, были отобраны 5 краткосрочных ИТ-проектов сроком реализации менее 700 человеко-часов, 5 среднесрочных – от 700 человеко-часов до 2 500 человеко-часов и 1 долгосрочный – более 2 500 человеко-часов. Более подробная аналитическая информация об ИТ-проектах представлена в таблице 3.3.

Таким образом, была соблюдена корреляция двух первых требований, предъявляемых к разработанному инструментарию риск-менеджмента в ИТ-проектах, т. к. предлагаемый автором диссертационного исследования инструментарий управления рисками ИТ-проектов в организациях был применен в проектах, где использовались различные способы реализации. Кроме того, созданный инструментарий управления рисками был апробирован в 11 ИТ-проектах различных типов.

Таблица 3.3 –ИТ-проекты, где была проведена апробация разработанного инструментария риск-менеджмента

№	Название организации	Название ИТ-проекта	Тип проекта	Способ реализации проекта	Количество человек в проекте	Планируемая длит-ть проекта, день	Размер проекта*
1	ООО «Синтез Интеллектуальных Систем»	«Сайт ТГУ»	Сайт	*Waterfall*	6	126	Среднесрочный
2	ООО «Лидер Групп»	«МирКар»	Сайт	*Waterfall*	4	13	Краткосрочный
3	ООО «Спейс-О Технологии»	«HyperVibe»	ПО	*Waterfall*	6	51	Краткосрочный
		«Reading Log»	ПО	*Waterfall*	4	56	Краткосрочный
4	ООО «Аксимедиа Софт»	«CINEMOOD»	Мобильное приложение	*Waterfall*	7	63	Краткосрочный
5	ООО «Контек Софт»	«Расчет и учет заработной платы в научно-технических учреждениях»	ERM-система	*Agile*	9	294	Среднесрочный
		«Портал логистики»	Портал	*Agile*	6	126	Среднесрочный
		«Торговая площадка»	ERM-система	*Agile*	8	231	Среднесрочный
		«Регламентация ведения номенклатуры ТМЦ»	ERM-система	*Agile*	5	63	Краткосрочный
6	ООО «Телебриз»	«DigitalTV»	ПО	*Agile*	10	120	Среднесрочный
7	ООО «Сибэйдж»	«ERM-система»	ERM-система	*Waterfall*	8	416	Долгосрочный

*к краткосрочным ИТ-проектам относятся проекты, трудозатраты которых составляют менее 700 человеко-часов, к среднесрочным – 700-2500 человеко-часов, долгосрочным – более 2 500 человеко-часов.

Особенности, характеристики и более детальное описание содержания ИТ-проектов представлены в Приложении Б.

Из результатов проведенного исследования видно, что для ИТ-организаций не характерно использование риск-менеджмента. В то же время анализ финансового состояния и выявленных проблем показал, что многие трудности имеют общие корни с внутрипроектными источниками рисков, что дает возможность превентивно нивелировать их негативное влияние. Также установлено, что в ИТ-организациях отсутствует инструментарий, идентифицирующий и стимулирующий наступление позитивных рисков, в связи с чем необходима экспериментальная проверка разработанного инструментария риск-менеджмента в ИТ-проектах.

3.2. Внедрение разработанного инструментария управления рисками в ИТ-проекты

Разработанный инструментарий управления рисками в ИТ-проектах включает в себя адаптированные для сферы информационных технологий способы оценки рисков и разработки мер воздействия на риски, которые не зависят от типов проектов, их размеров, численности коллективов, используемых подходов реализации проектов. Процессы контроля и мониторинга рисков, как было показано ранее в параграфе 2.3, могут обслуживаться с помощью специализированных программных продуктов – RiskGap, OpenPlanProfessional, RiskTrack и других. В связи с этим контроль и мониторинг не требуют детального рассмотрения, т. к. эксплуатация и использование данных программных комплексов строго регламентированы, а операции автоматизированы. Однако результаты апробации остальных этапов разработанного инструментария требуют более подробного рассмотрения и анализа.

Процесс идентификации рисков. Для выявления рисков и составления их перечня к работе были привлечены, помимо проектных команд исследуемых проектов, сторонние эксперты. В качестве экспертов выступили представители сторон заказчиков, субподрядчиков, поставщиков, потенциальные пользовали, а также руководители проектов из других ИТ-организаций (рисунок 3.1). Экспертам было предложено изучить созданную проектную документацию (уставы проектов, спецификации продуктов, сетевые графики и др.) и ознакомиться с отчетами смежных, ранее завершенных проектов. Организация процесса выявления рисков и получение релевантной информации осуществлялась с помощью адаптированных для сферы информационных технологий методов (см. параграф 2.1). Использование разнообразного инструментария выявления рисков дало возможность рассмотреть различные области проектов, идентифицируя уникальные и специфические риски. Например, при

использовании STEEP-анализа был обнаружен риск отказа от привычных форм налоговой отчетности с переходом на новые формы НДФЛ. Благодаря методу «что, если?» были разработаны прогнозы для оптимистических, реальных и пессимистических сценариев развития ИТ-проектов, что дало возможность выявить как негативные факторы, влияющие на успешные исходы, так и позитивные.

Рисунок 3.1 – Процесс идентификации рисков в ИТ-проектах

Результаты, полученные по завершении процесса идентификации рисков в исследуемых ИТ-проектах, представлены в таблице 3.3. Как видно из полученных данных, количество выявленных негативных и позитивных рисков прямо пропорционально размерам проектов. В краткосрочных ИТ-проектах количество негативных рисков варьируется от 51 до 69, среднесрочных – от 53 до 78, в долгосрочном ИТ-проекте было идентифицировано 80 рисков.

Таблица 3.3 – Количество выявленных негативных и позитивных рисков в исследуемых ИТ-проектах

№	Название ИТ-проекта	Негативные риски, шт.	Позитивные риски, шт.
1	«Сайт ТГУ»	55	14
2	«МирКар»	51	0
3	«HyperVibe»	57	0
4	«Reading Log»	58	0
5	«CINEMOOD»	66	0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	69	8
7	«Портал логистики»	78	3
8	«Торговая площадка»	69	5
9	«Регламентация ведения номенклатуры ТМЦ»	69	4
10	«DigitalTV»	53	0
11	«ERM-система»	80	8

В ходе анализа таблицы 3.3 было установлено, что в краткосрочных ИТ-проектах наблюдается дефицит ресурсов способных позитивно влиять на проектные цели, что привело к невозможности управления позитивными рисками. Однако для среднесрочных ИТ-проектов наблюдался рост количества позитивных рисков. Например, в ИТ-проекте «Сайт ТГУ» было идентифицировано 14 позитивных рисков. Это может говорить о появлении факторов, связанных с повышенной ответственностью и сложностью исполнения проектных заданий.

Процесс анализа рисков. В рамках апробации каждый выявленный риск был проанализирован командами проектов с целью построения иерархических структур негативных и позитивных рисков, получения релевантной информации об источниках рисковых событий, о возможных последствиях в случаях их наступления, а также о времени актуализации рисков относительно фаз жизненных циклов (рисунок 3.2). В качестве основного инструментария в процессе анализа были использованы «галстук-бабочка» (первый этап), метод «почему-почему», «диаграмма Исикавы», классификация рисков, а также способ определения времени актуализации рисков, представленный ранее в параграфе 2.2.

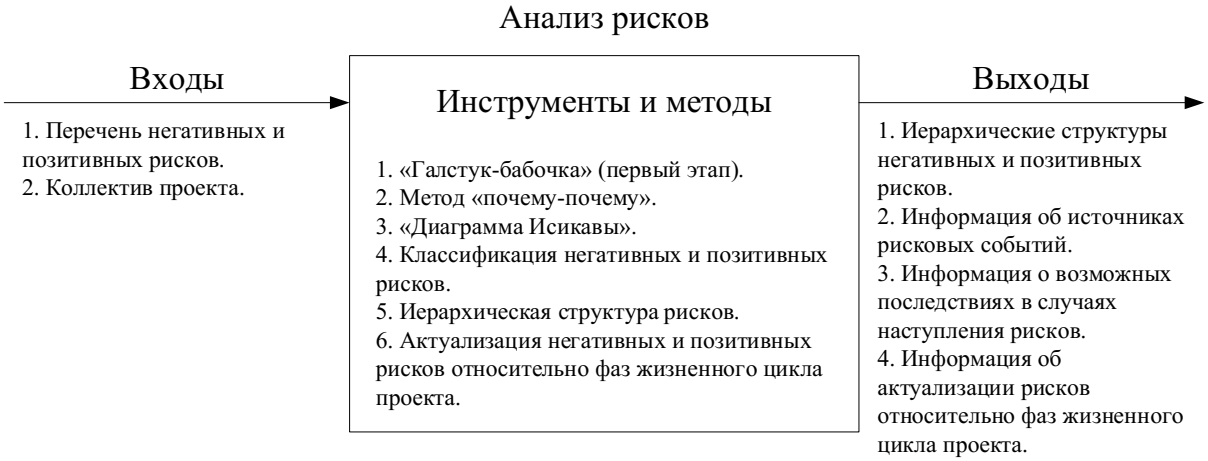


Рисунок 3.2 – Процесс анализа рисков в ИТ-проектах

Процесс оценивания рисков. Получение информации о вероятностях материализации рисков и возможных влияниях обеспечивалось качественными (экспертными) методами, где экспертные оценки были сопряжены с коэффициентами Харрингтона (от 0 до 5). Качественное оценивание было выбрано по причине ограничений, накладываемых принципами KISS, YAGNI, Agile и других, а также чтобы обеспечить удовлетворение требования, связанного с оперативным выполнением процессов риск-менеджмента в ИТ-проектах (рисунок 3.3). Точность экспертных оценок увеличивалась за счет расчета коэффициентов Кендалла, где при слабой согласованности $W < 0{,}7$ или при ее отсутствии $W = 0$ повторно уточнялись данные об источниках рисковых событий и о возможных последствиях в случаях их наступления. Если экспертные мнения вновь показывали низкую согласованность, то окончательные решения о вероятностях и влияниях принимали руководители проектов.

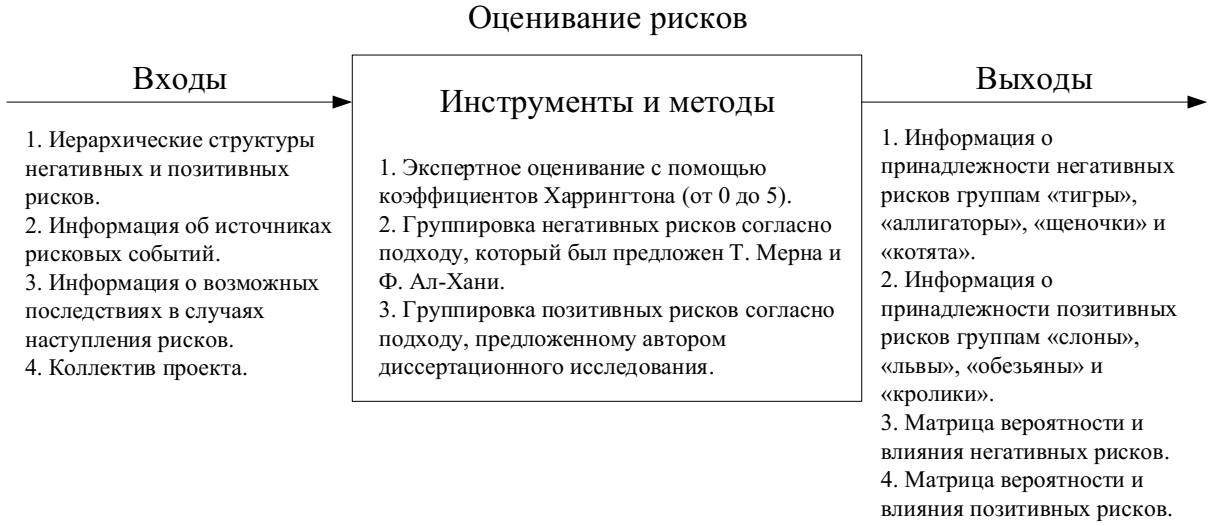


Рисунок 3.3 – Процесс оценивания рисков в ИТ-проектах

На основании интегрированных и согласованных оценок далее проводилась группировка негативных рисков согласно способу, который был предложен Т Мерна и Ф. Ал-Хани [150]. Группировка же позитивных рисков проходила согласно способу, предложенному автором диссертационного исследования. Результаты группировки негативных и позитивных рисков представлены в таблицах 3.4 и 3.5. Диссипация негативных рисков показала, что рисковые события неоднородны и зависят от размеров, типов, численности коллективов или от используемых способов управления проектами. Например, доля «тигров» от общего количества рисков составила для долгосрочного ИТ-проекта «ERM-система» 2,5%, краткосрочного ИТ-проекта «CINEMOOD» – 10,6%, краткосрочного ИТ-проекта «МирКар» – 17,6%. В тоже время доля «тигров» для краткосрочного ИТ-проекта «Регламентация ведения номенклатуры ТМЦ» равна 39,1%, среднесрочных ИТ-проектов «Торговая площадка» – 43,5% и «Портал логистики» – 37,2%. Наиболее опасным из исследуемых ИТ-проектов стал среднесрочный ИТ-проект «Сайт ТГУ», где доля катастрофических рисков была равна 60%.

В исследуемых ИТ-проектах была отмечена высокая доля непредсказуемых негативных рисков. В 9 ИТ-проектах количество «аллигаторов» превысило 20%, в 5 ИТ-проектах – 30%, в 2 ИТ-проектах –

40%. Причем выявлено, что в ИТ-проектах достаточно высоки доли незначительных негативных рисков. Например, в краткосрочных ИТ-проектах «HyperVibe», «Reading Log» и «CINEMOOD» доля «котят» составила 43,9%, 37,9% и 39,4% соответственно. Самой малозначительной группой стали «щеночки», их доля в исследуемых ИТ-проектах не превысила 6%.

Таблица 3.4 – Группировка негативных рисков в исследуемых ИТ-проектах согласно способу, предложенному Т. Мерта и Ф. Ал-Хани

№	Название ИТ-проекта	Тигры, шт.	Аллигаторы, шт.	Щеночки, шт.	Котята, шт.
1	«Сайт ТГУ»	33	15	6	1
2	«МирКар»	9	31	1	10
3	«HyperVibe»	14	16	2	25
4	«Reading Log»	17	17	2	22
5	«CINEMOOD»	7	31	2	26
6	«Расчет и учет заработной платы в научно-технических учреждениях»	17	27	4	21
7	«Портал логистики»	29	29	3	17
8	«Торговая площадка»	30	16	4	19
9	«Регламентация ведения номенклатуры ТМЦ»	27	22	5	15
10	«DigitalTV»	29	10	10	4
11	«ERM-система»	2	1	7	65

Группировка позитивных рисков осуществлялась согласно авторскому способу и показала, что несмотря на значительное количество в среднесрочных и долгосрочных проектах позитивных рисков, большая их часть не нуждается в разработке мер воздействия (таблица 3.5). Например, в ИТ-проекте «Сайт ТГУ» было выявлено 5 «слонов», 5 «обезьян» и 2 «кролика». Однако 2 «львам» (риск того, что руководитель проекта получит прямой канал коммуникаций с ректором ТГУ; риск переезда одного представителя со стороны заказчика в офис ООО «Синтез Интеллектуальных Систем» на время реализации проекта) требовалась разработка мер воздействия с целью увеличения вероятности их материализации.

Таблица 3.5 – Группировка позитивных рисков в исследуемых ИТ-проектах согласно авторскому способу

№	Название ИТ-проекта	Слоны, шт.	Львы, шт.	Обезьяны, шт.	Кролики, шт.
1	«Сайт ТГУ»	5	2	5	2
2	«МирКар»	0	0	0	0
3	«HyperVibe»	0	0	0	0
4	«Reading Log»	0	0	0	0
5	«CINEMOOD»	0	0	0	0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	3	3	1	1
7	«Портал логистики»	2	0	1	0
8	«Торговая площадка»	2	2	0	1
9	«Регламентация ведения номенклатуры ТМЦ»	2	2	0	0
10	«DigitalTV»	0	0	0	0
11	«ERM-система»	2	5	2	0

Похожие выводы были сделаны коллективами ИТ-проектов «Расчет и учет заработной платы в научно-технических учреждениях», «Торговая площадка», «Регламентация ведения номенклатуры ТМЦ» и «ERM-система». Команды этих проектов предпочли уделить большее внимание рискам относящимся к группе «львы» и пренебречь рисками из остальных групп.

Матрицы вероятностей материализации негативных (позитивных) рисков и возможных влияний представлены в Приложениях В и Г.

Процесс воздействия на риски. Группировка рисковых событий значительно снизила расход ресурсов на разработку мер воздействия, т. к. проектные средства фокусировались только на группы, которые были способны оказать значительное влияние на стоимость, сроки, содержание и качество проектов (рисунок 3.4). Поэтому среди негативных рисков особый интерес для коллективов представляли события, которые относились к «тиграм» и «аллигаторам», среди позитивных рисков – ко «львам». Иными словами, разрабатывая меры планов превентивного воздействия на риски и меры планов принятия рисков, проектные команды применяли адаптированные автором диссертационного исследования методы для сферы информационных технологий. Рисками из остальных групп коллективы

пренебрегли, посчитав их незначительными и неспособными оказывать значительного влияния на проектные цели.

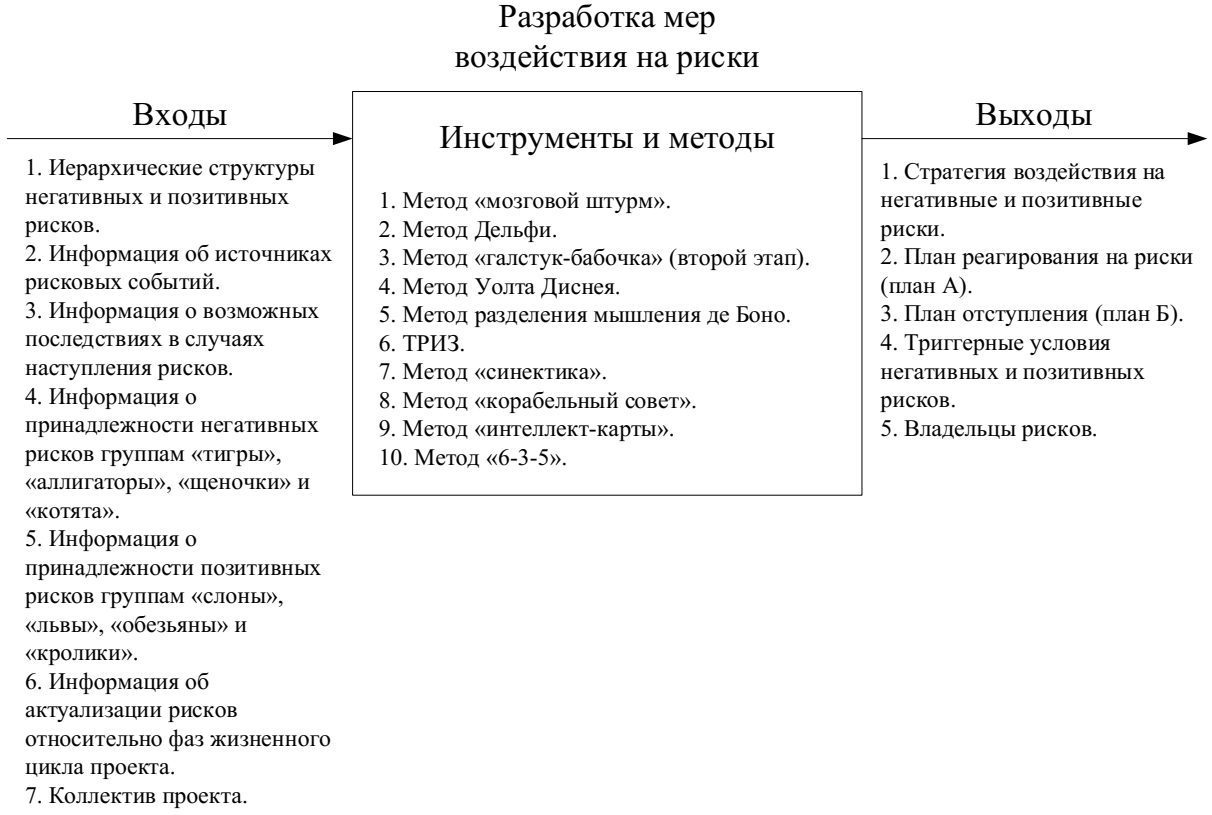


Рисунок 3.4 – Процесс разработки мер воздействия на риски в ИТ-проектах

В конечном счете для рисковых событий, относящихся к группам «тигры», «аллигаторы» и «львы», коллективами проектов были разработаны меры воздействия, которые вошли в планы превентивного воздействия на риски и планы принятия рисков. С целью обеспечить контроль над данными рисками в процессе реализации проектов были сформулированы показатели наступления рисков – триггерные условия. В частности, триггерное условие риска «заказчик будет не удовлетворен содержанием разработанного ИТ-продукта» ИТ-проекта «МирКар» было формализовано следующим образом: «во время диалога с заказчиком прозвучит фраза «Я же вам говорил!»». Также было установлено, что исполнение одного превентивного мероприятия из «плана А» может нивелировать или ослабить несколько

негативных рисков. Например, мера воздействия «разработать спецификацию проекта, согласно стандартам ГОСТ Р ИСО/МЭК 29155-1-2016 Системная и программная инженерия» в проекте «DigitalTV» дало возможность нивелировать или ослабить риск нечетко сформулированных целей, риск отсутствия проектной документации, риск несоответствия полученных результатов изначальным требованиям, риск низкого качества разработанного ИТ-продукта, риск того, что коллективу будет непонятно, какой продукт должен получиться по завершении проекта.

Таблица 3.6 – Планы реагирования на риски, триггерные условия и планы принятия рисков в исследуемых ИТ-проектов

№	Название ИТ-проекта	«План А»	Триггерные условия	«План Б»
1	«Сайт ТГУ»	Разработан	Разработаны	Разработан
2	«МирКар»	Разработан	Разработаны	Не разработан
3	«HyperVibe»	Разработан	Разработаны	Не разработан
4	«Reading Log»	Разработан	Разработаны	Не разработан
5	«CINEMOOD»	Разработан	Разработаны	Не разработан
6	«Расчет и учет заработной платы в научно-технических учреждениях»	Разработан	Разработаны	Разработан
7	«Портал логистики»	Разработан	Разработаны	Разработан
8	«Торговая площадка»	Разработан	Разработаны	Разработан
9	«Регламентация ведения номенклатуры ТМЦ»	Разработан	Разработаны	Не разработан
10	«DigitalTV»	Разработан	Разработаны	Разработан
11	«ERM-система»	Разработан	Разработаны	Разработан

В ходе апробации было установлено, что коллективы краткосрочных ИТ-проектов, таких как «МирКар», «HyperVibe», «Reading Log», «CINEMOOD», «Регламентация ведения номенклатуры ТМЦ» отказались от разработки мер планов принятия рисков (таблица 3.6). Проектные команды объясняют отказ от «плана Б» следующим образом:

- *во-первых*, их проекты находятся в зоне относительной безопасности, т. к. доля успешно завершенных краткосрочных проектов согласно статистическим данным равна 76% [63, 64];
- *во-вторых*, количество сотрудников в коллективах варьируется от 4 до 7 человек, что также увеличивает шансы на успешные исходы [63, 64];
- *в-третьих*, руководители заложили временные и финансовые резервы на случаи форс-мажорных обстоятельств.

Таблица 3.7 – Время потраченное на выполнение процессов идентификации, анализа, оценивания и разработки мер воздействия на риски

№	Название ИТ-проекта	Название процесса риск-менеджмента				
		Идентификация рисков, час	Анализ рисков, час	Оценивание рисков, час	Разработка мер воздействие на риски, час	Итого, час
1	«Сайт ТГУ»	5	3	0,3	4	12,3
2	«МирКар»	4	1	0,2	3	8,2
3	«HyperVibe»	4	2	0,2	3	9,2
4	«Reading Log»	4	2	0,2	3	9,2
5	«CINEMOOD»	4	2	0,3	3	9,3
6	«Расчет и учет заработной платы в научно-технических учреждениях»	4	2	0,3	4	10,3
7	«Портал логистики»	4	0	0,3	4	8,3
8	«Торговая площадка»	4	2	0,2	4	10,2
9	«Регламентация ведения номенклатуры ТМЦ»	4	2	0,2	2	8,2
10	«DigitalTV»	4	3	0,3	4	11,3
11	«ERM-система»	7,2	4	0,4	2	13,6

Таким образом, время потраченное на выполнение процессов разработанного инструментария управления рисками ИТ-проектов в организациях составило 8,2 часов ÷ 13,6 часов (таблице 3.7). Среднее значение времени, которое было потрачено на выполнение процессов риск-

менеджмента, равно 10 часов. Иными словами, во время планирования руководителям проектов необходимо резервировать 8 часов ÷14 часов для того, чтобы провести идентификацию, анализ, оценивание и разработку мер воздействия на риски.

На основании анализа данных можно сделать вывод, что наиболее трудоемкими являются процессы идентификации (4 ч. ÷ 7,2 ч.) и воздействия на риски (2 ч. ÷ 4 ч.), где разработка мер «плана Б» увеличивала продолжительность данного процесса примерно на 1 час. Самым оперативным стал процесс оценивания за счет использования качественных методов (0,2 ч. ÷ 0,4 ч.). Отметим, что на трудоемкость процессов риск-менеджмента существенного влияния не оказали размер, тип, количество сотрудников и способ управления проектами. Например, трудоемкость долгосрочного ИТ-проекта «ERM-система» больше малого ИТ-проекта «Регламентация ведения номенклатуры ТМЦ» всего на 5,4 часа.

Таблица 3.8 – Материализовавшиеся негативные риски в исследуемых ИТ-проектах

№	Название ИТ-проекта	Материализовавшиеся негативные риски				
		Тигры, шт.	Аллигаторы, шт.	Щеночки, шт.	Котята, шт.	Итого, шт.
1	«Сайт ТГУ»	2	1	1	0	4
2	«МирКар»	5	1	0	0	6
3	«HyperVibe»	4	0	0	0	4
4	«Reading Log»	1	1	0	0	2
5	«CINEMOOD»	2	0	1	0	3
6	«Расчет и учет заработной платы в научно-технических учреждениях»	6	2	0	1	9
7	«Портал логистики»	2	1	1	0	4
8	«Торговая площадка»	3	0	1	0	4
9	«Регламентация ведения номенклатуры ТМЦ»	1	0	0	0	1
10	«DigitalTV»	17	0	3	1	21
11	«ERM-система»	0	0	1	0	1

Результаты материализованных негативных и позитивных рисков в исследуемых проектах с учетом их групп представлены в таблицах 3.8 и 3.9. Одними из самых нерезультативных мер воздействия «плана А» оказались мероприятия проведенные в ИТ-проекте «DigitalTV», где из 29 «тигров» материализовались 17. Для борьбы с последствиями руководителем проекта были применены меры «плана Б», однако из-за того, что проблемы наступили почти одновременно, отклонение фактической длительности от запланированной все же составило 21,6% (таблица 3.10). Самое значительное отклонение от запланированной длительности было зафиксировано в ИТ-проекте «Сайт ТГУ» – 33,3%. Наиболее эффективные меры воздействия на риски зарегистрированы в ИТ-проектах «Регламентация ведения номенклатуры ТМЦ» – 1 «тигр» из 27, «Reading Log» – 1 «тигр» из 17, «Портал логистики» – 2 «тигра» из 29, «HyperVibe» – 4 «тигра» из 14. Матрицы вероятностей и влияний реализовавшихся негативных рисков представлены в Приложении Д.

Таблица 3.9 – Материализовавшиеся позитивные риски в исследуемых ИТ-проектах

№	Название ИТ-проекта	Материализовавшиеся позитивные риски				
		Слоны, шт.	Львы, шт.	Обезьяны, шт.	Кролики, шт.	Итого, шт.
1	«Сайт ТГУ»	5	2	5	0	12
2	«МирКар»	0	0	0	0	0
3	«HyperVibe»	0	0	0	0	0
4	«Reading Log»	0	0	0	0	0
5	«CINEMOOD»	0	0	0	0	0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	3	3	1	0	7
7	«Портал логистики»	2	2	1	0	5
8	«Торговая площадка»	2	2	0	0	4
9	«Регламентация ведения номенклатуры ТМЦ»	2	2	0	0	4
10	«DigitalTV»	0	0	0	0	0
11	«ERM-система»	2	5	2	0	9

Данные из таблицы 3.9 показывают, что разработанные и реализованные меры воздействия на позитивные риски группы «львы», способствовали увеличению вероятности материализации этих событий. В исследуемых проектах материализовались все выявленные риски данной группы. Также отмечено, что риски групп «слоны» и «обезьяны» материализовались без каких-либо дополнительных стимулирующих мер.

Таблица 3.10 – Результаты отклонений фактической длительности исследованных ИТ-проектов от запланированной длительности

№	Название ИТ-проекта	Фактическая длительность ИТ-проекта, дней	Отклонение фактической длительности проекта от запланированной длительности, дней	Отклонение фактической длительности проекта от запланированной длительности, %
1	«Сайт ТГУ»	189	63	33,3
2	«МирКар»	18	5	27,8
3	«HyperVibe»	53	2	3,8
4	«Reading Log»	67	11	16,4
5	«CINEMOOD»	63	0	0,0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	336	42	12,5
7	«Портал логистики»	135	9	6,7
8	«Торговая площадка»	255	24	9,4
9	«Регламентация ведения номенклатуры ТМЦ»	67	4	6,0
10	«DigitalTV»	153	33	21,6
11	«ERM-система»	452	36	8,0

Как видно из таблицы 3.10 отклонение фактической длительности от запланированной в краткосрочных ИТ-проектах «МирКар», «HyperVibe», «Reading Log» и «Регламентация ведения номенклатуры ТМЦ» составило 3,8% ÷ 27,8%. Краткосрочный ИТ-проект «CINEMOOD», несмотря на материализовавшихся двух «тигров» был завершен согласно установленному сроку. Для среднесрочных ИТ-проектов «Сайт ТГУ», «Расчет и учет заработной платы в научно-технических учреждениях», «Портал логистики»,

«Торговая площадка» и «DigitalTV» наблюдаются более значительные отклонения – до 33,3%. В долгосрочном ИТ-проекте «ERM-система» зафиксировано отклонение 8%. Данный показатель может быть объяснен тем, что в проекте было обнаружено только 3 негативных риска, 2 «тигра» и 1 «аллигатор».

Также установлено, что время необходимое на проведение процессов идентификации рисков, анализа рисков, оценивания рисков и разработки мер выявления на риски прямо пропорционально размерам ИТ-проектов. Например, для краткосрочных ИТ-проектов этот показатель варьируется от 1,6% до 2,3%. В среднесрочных ИТ-проектах и долгосрочном ИТ-проекте доля времени затраченного на процессы управления рисками уменьшается до 0,4%.

Таким образом, анализ релевантных данных, полученных в ходе апробации, проведенной в 11 ИТ-проектах различного размера, типа, способа и численности проектных команд позволяет сделать ряд выводов, а именно:

- *Во-первых*, показатели отклонения, информация о материализовавшихся негативных рисках и позитивных рисках говорят о том, что материализация незначительного количества негативных рисков способно увеличить длительность исполнения проектов до 33,3%. Логично предположить, что при отсутствии работы с позитивными рисками был бы значительно увеличен разрыв между фактической длительностью проекта и запланированной длительностью проекта. В связи с этим сформулирована рекомендация для руководителей ИТ-проектов, суть которой заключается в планировании временных резервов для случаев наступления катастрофических и непредсказуемых рисков, исходя из расчета среднего арифметического отклонения длительности на 13,2%.
- *Во-вторых*, полученные иерархические структуры негативных и позитивных рисков, группы негативных и позитивных рисков, матрицы вероятности и влияния и др. показывают, что разработанный инструментарий

управления рисками в ИТ-проектах учитывает особенности сферы информационных технологий, интегрируясь в любой проект.

- *В-третьих*, общее время использования процессов риск-менеджмента, таких как идентификация, анализ, оценивание, разработка мер воздействия на подготовительных фазах проекта занимает от 8 часов до 14 часов, что позволяет предположить, что применение данных процессов при последующих внедрениях займет не более двух рабочих дней. Согласно опросу, 14 часов для выполнения процессов риск-менеджмента является приемлемой длительностью, чтобы менеджмент ИТ-организаций и руководители ИТ-проектов стали использовать разработанный автором диссертационного исследования инструментарий риск-менеджмента.
- *В-четвертых*, созданный инструментарий управления рисками ИТ-проектов в организациях успешно использовался в проектах разрабатываемых по *waterfall* и *agile*. Иными словами, в процессе апробации в исследуемых проектах не возникло противоречий между разработанным инструментарием риск-менеджмента и способами управления проектами, такими как *waterfall* и *agile*.

3.3. Оценка результативности применения инструментария управления рисками в ИТ-проектах

Оценка результативности применения разработанного инструментария управления рисками в ИТ-проектах проводилась сопоставлением результатов, полученных в ходе апробации, с результатами исследований предшественников. В связи с чем в данном параграфе предприняты попытки оценить качество процесса идентификации рисков и доказать, что использование разработанного инструментария управления рисками в ИТ-проектах является экономически оправданным.

Оценка качества процессов идентификации рисков в исследуемых ИТ-проектах проводилась посредством аудита, материализовавшихся неидентифицированных и идентифицированных рисков. Неидентифицированными рисками называются негативные и позитивные риски, которые не были зафиксированы в реестрах рисков. Отметим, что негативные и позитивные события, которые были выявлены в процессе мониторинга рисков отнесены к идентифицированным рискам, т. к. эти события выявлялись во время исполнения процессов риск-менеджмента. В связи с этим качество идентификации рисков в ИТ-проектах может быть проверено с помощью формулы [211, 212]:

$$k = \frac{n_2}{n_1 + n_2}, \tag{3.1}$$

где k – показатель качества идентификации рисков, n_1 - число материализовавшихся неидентифицированных рисков, n_2 - число материализовавшихся идентифицированных рисков.

Формула 3.1 дает возможность оценить насколько качественно руководители и проектные коллективы выполнили процессы идентификации рисков. Например, если выполняется условие $n_1 \geq n_2$, то процесс идентификации рисков был выполнен неудовлетворительно. Следовательно,

если показатель $k = 1$, то можно сделать вывод, что в процессе реализации ИТ-проектов не наступило ни одного «риска-невидимки», т. е. все наступившие негативные и позитивные риски были выявлены во время выполнения процессов идентификации и мониторинга.

Таблица 3.11 – Материализовавшиеся неидентифицированные и идентифицированные негативные риски в исследуемых ИТ-проектах

№	Название ИТ-проекта	n_1	n_2	k
		Материализовавшиеся неидентифицированные негативные риски, шт.	**Материализовавшиеся идентифицированные негативные риски, шт.**	**Показатель качества идентификации рисков**
1	«Сайт ТГУ»	0	4	1,0
2	«МирКар»	0	6	1,0
3	«HyperVibe»	0	4	1,0
4	«Reading Log»	0	2	1,0
5	«CINEMOOD»	0	3	1,0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	0	9	1,0
7	«Портал логистики»	0	4	1,0
8	«Торговая площадка»	0	4	1,0
9	«Регламентация ведения номенклатуры ТМЦ»	0	1	1,0
10	«DigitalTV»	0	21	1,0
11	«ERM-система»	15	1	0,1

Результаты неидентифицированных и идентифицированных негативных и позитивных рисков материализовавшихся в исследуемых ИТ-проектах представлены в таблицах 3.11 и 3.12.

Таблица 3.12 – Материализовавшиеся неидентифицированные и идентифицированные позитивные риски в исследуемых ИТ-проектах

№	Название ИТ-проекта	n_1	n_2	k
		Материализовавшиеся неидентифицированные позитивные риски, шт.	**Материализовавшиеся идентифицированные позитивные риски, шт.**	**Показатель качества идентификации рисков**
1	«Сайт ТГУ»	0	12	1,0
2	«МирКар»	0	0	0
3	«HyperVibe»	0	0	0
4	«Reading Log»	0	0	0
5	«CINEMOOD»	0	0	0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	0	7	1,0
7	«Портал логистики»	0	5	1,0
8	«Торговая площадка»	0	4	1,0
9	«Регламентация ведения номенклатуры ТМЦ»	0	4	1,0
10	«DigitalTV»	0	0	0
11	«ERM-система»	0	9	1,0

Как видно из таблицы 3.11 в десяти ИТ-проектах показатель $k = 1$. Логично предположить, что высокое качество выявления рисковых событий в данных ИТ-проектах было обеспечено благодаря применению адаптированных методов идентификации рисков для сферы информационных технологий (см. таблицу 2.1). Однако, несмотря на высокий уровень показателей в ИТ-проекте «ERM-система» все же материализовалось 15 негативных рисков, которые не были выявлены во время процессов идентификации и мониторинга. Отметим, что впоследствии эти неидентифицированные риски оказали неблагоприятное влияние на проект и привели к увеличению его длительности на 36 дней. Низкое качество идентификации и мониторинга рисков может быть объяснено

размерами ИТ-проекта. Планируемая длительность реализации составляла 416 рабочих дней, т. е. проект должен был разрабатываться более одного года. Долгий срок реализации привел к появлению непредвиденных трудностей, сопряженных с заданиями, где необходимо было привлекать дополнительные ресурсы, в том числе сотрудников работающих удаленно. Кроме того, в проекте были зафиксированы конфликты между руководителем и участниками проекта.

Анализ данных таблицы 3.12 показал, что показатель качества идентификации позитивных рисков $k = 1$. Из чего следует, что адаптированные методы идентификации позволяют руководителям ИТ-проектов и проектным коллективам выявлять максимально возможное количество позитивных рисковых событий с приемлемым уровнем качества.

Таким образом, подводя итог оценки качества идентификации рисков в ИТ-проектах можно сделать вывод, что процессы их выявления и мониторинга в рамках разработанного инструментария управления рисками дают возможность руководителям и коллективам находить негативные, позитивные и уникальные рисковые события в краткосрочных и среднесрочных ИТ-проектах с приемлемым уровнем качества. В долгосрочных ИТ-проектах, где наблюдается всплеск наступивших неидентифицированных негативных событий, автор диссертационного исследования рекомендует руководителями систематически повторять процесс выявления рисков на этапах реализации и завершения жизненного цикла, привлекая к работе в том числе и сторонних экспертов.

Далее обратим внимание на то, что несмотря на различные размеры, типы, способы управления ИТ-проектами, присутствует тождественность среди некоторых рисков. В таблицах 3.13 и 3.14 представлены рисковые события, которые чаще остальных материализовывались в исследуемых ИТ-проектах. Например, в процессе анализа таблицы 3.13 было обнаружено, что риск «отставание от запланированных сроков» материализовался во всех исследуемых ИТ-проектах, несмотря на разработанные и реализованные

меры воздействия. Анализ материализовавшихся негативных рисков, представленных в таблице 3.13, также позволил установить связь между результатами, полученными в ходе апробации разработанного инструментария управления рисками и данными зарубежных ученых. Например, тождественность наблюдается для таких рисков, как низкая производительность труда и изменение требований в процессе реализации ИТ-проекта. Стоит отметить, что в трудах Т. Аддисона и С. Валлабха [213], К. Д. Стивенса и С. Фовелла [214], М. Самнера [215] не упоминается о рисках, связанных с отставанием от запланированных сроков, хотя в их работах присутствуют ссылки на затруднения, которые влияют на длительность ИТ-проектов (см. Приложение Ж). В частности, Т. Аддисон и С. Валлабх описывают риск того, что сроки реализации и бюджеты ИТ-проекта могу быть «нереальными». В статье М. Самнера отмечается, что часто ИТ-проекты оказываются гораздо сложнее, чем планировалось изначально [215].

Таблица 3.13 – Материализовавшиеся негативные риски

№	Название риска	Количество совпадений, шт.
1	Риск отставания от запланированных сроков	11
2	Риск изменения требований в процессе реализации проекта	9
3	Риск неудовлетворенности заказчика сроками реализации проекта	8
4	Риск низкой производительности труда	7
5	Риск допущения ошибок при оценивании сроков	3
6	Риск занятости руководителя на других проектах	3
7	Риск допущения ошибок при реализации проекта *(bugs)*	2
8	Риск ухода на «больничный»	2
9	Риск допущения ошибок при оценивании	2
10	Риск простоя за-за того, что заказчик неоперативно дает ответы на задаваемые вопросы	1

Большая часть негативных рисков, представленных в таблице 3.13 не упоминается в трудах Т. Аддисона, С. Валлабха, К. Д. Стивенса, С. Фовелла и М. Самнера. Низкий уровень совпадений может быть объяснен спецификой объектов исследования. В частности, К. Д. Стивенс и С. Фовелл

рассматривают ИТ-проекты, которые разрабатывались для Австралийского оптового финансового рынка, М. Самнер исследует факторы риска для ERP-проектов, Т. Аддисон и С. Валлабх анализируют ретро-риски, которые наступали в ИТ-проектах с 1991 г. до 2002 г. [213, 214, 215].

Таблица 3.14 – Материализовавшиеся позитивные риски

№	Название риска	Количество совпадений, шт.
1	Риск того, что у руководителя будет профессиональное образование в области управления проектами	6
2	Риск того, что у руководителя будет опыт управления проектами более двух лет	6
3	Риск того, что руководитель будет самостоятельно формировать коллектив проекта	6
4	Риск того, что в состав проектной команды будет привлечен высококвалифицированный специалист (старший разработчик)	6
5	Риск того, что в проект будут привлечены тестировщики	4
6	Риск того, что в проект будет привлечен системный аналитик	3
7	Риск того, что для проекта будут созданы устав, спецификация, техническое задание и другие документы	3
8	Риск того, что заказчик сделает предоплату	2
9	Риск того, что представитель заказчика будет входить в состав коллектива разрабатывающего проект	2
10	Риск привлечения пользователя к процессу разработки	2

В таблице 3.14 представлены материализовавшиеся позитивные риски в исследуемых ИТ-проектах. Анализ показал, что на количество позитивных рисков влияет специфика и уникальность ИТ-проектов. Например, возможность привлечения представителя заказчика в состав коллектива присутствовала только в проектах «МирКар» и «Сайт ТГУ». Часто встречаемыми позитивными рисковыми событиями были только риски, сопряженные с профессиональным образованием и опытом руководителей ИТ-проектов.

На основании полученных данных, представленных в таблицах 3.13 и 3.14, можно заключить:

- *во-первых*, негативные события схожи друг с другом и мало зависят от размеров ИТ-проектов, их типов и способов управления ИТ-проектами;
- *во-вторых*, конкордантность с рисками, которые упоминаются в трудах Т. Аддисона, С. Валлабха, К. Д. Стивенса, С. Фовелла и М. Самнера дает возможность предположить, что разработанный инструментарий управления рисками может применяться в международных ИТ-проектах [213, 214, 215];
- *в-третьих*, наличие и количество позитивных рисков зависят от особенностей и специфики ИТ-проектов.

Следующим этапом оценки результативности является сопоставление результатов, полученных в ходе апробации разработанного инструментария управления рисками в ИТ-проектах, с данными международной научно-консультационной организации The Standish Group [63, 64]. В 2014 году The SG было проведено крупномасштабное исследование, где анализировались отчеты более 50 000 проектов, разрабатываемых в сфере информационных технологий. По окончании исследования экспертами The Standish Group были получены данные относительно того, насколько фактические сроки проектов превышают запланированные, определены доли успешных и незавершенных ИТ-проектов, а также установлена зависимость между успешными исходами и используемыми способами управления проектами. Результаты отклонений ИТ-проектов от запланированных длительностей представлены в таблице 3.15. Обращает на себя внимание, что большинство ИТ-проектов, согласно данным The SG, отклоняются от запланированных длительностей примерно на 101-200%, что может говорить о низком уровне риск-менеджмента в данных ИТ-проектах. Это значительно отличается от результатов, полученных автором диссертационного исследования во время апробации. В частности, в исследуемых ИТ-проектах отклонение от запланированной длительности не превысило 33,3%. В 80% случаев отклонение от запланированной длительности было менее 20%. В связи с

этим логично предположить, что разработанный инструментарий управления рисками дает возможность снизить величину отклонения от запланированных длительностей и не допустить ее увеличение на 50%, 100% и 400%.

Таблица 3.15 – Отклонение от запланированных длительностей в ИТ-проектах

№	Отклонение от запланированных длительностей	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	менее 20%	13,9	80
2	21-50%	18,3	20
3	51-100%	20,0	0
4	101-200%	35,5	0
5	201-400%	11,2	0
6	более 401%	1,1	0

Далее рассмотрим сведенья о том, какое распределение получили успешно завершенные ИТ-проекты, ИТ-проекты в которых были зафиксированы проблемы и незавершенные ИТ-проекты (таблица 3.16). Стоит сказать, что исследуемые ИТ-проекты признавались руководителями и заказчиками успешными только в тех случаях, когда отклонение от запланированных длительностей не превышало 10%, иначе ИТ-проекты относились к группе, где присутствовали трудности. Из материалов, представленных в таблице 3.16, видно, что доля успешных ИТ-проектов, согласно данным The Standish Group, составила 29%. Доля же успешных исходов в исследуемых ИТ-проектах – 54,5%. Подобное различие может быть объяснено тем, что в исследуемых ИТ-проектах был использован инструментарий управления рисками, который позволил руководителям контролировать события, имеющие потенциал значительного негативного и позитивного влияния. Отметим, что подобное регулирование не позволило полностью избежать трудностей, что подтверждает доля проблемных проектов – 45,5%.

Таблица 3.16 – Сравнительный анализ успешно завершенных ИТ-проектов, незавершенных ИТ-проектов и ИТ-проектов, где проблемы повлекли изменение запланированных целей

№	Статус ИТ-проекта	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	Успешные ИТ-проекты	29	54,5
2	Незавершенные ИТ-проекты	19	0
3	ИТ-проекты, в которых проблемы повлекли изменение запланированных целей	52	45,5

Таблица 3.17 – Сравнительный анализ успешных исходов краткосрочных ИТ-проектов, незавершенных краткосрочных ИТ-проектов и краткосрочных ИТ-проектов, где проблемы повлекли изменение запланированных целей

№	Статус ИТ-проекта	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	Успешные ИТ-проекты	76	60
2	Незавершенные ИТ-проекты	4	0
3	ИТ-проекты, в которых проблемы повлекли изменение запланированных целей	20	40

Таблица 3.18 – Сравнительный анализ успешных исходов среднесрочных и долгосрочных ИТ-проектов, незавершенных среднесрочных и долгосрочных ИТ-проектов и среднесрочных и долгосрочных ИТ-проектов, где проблемы повлекли изменение запланированных целей

№	Статус ИТ-проекта	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	Успешные ИТ-проекты	10	50
2	Незавершенные ИТ-проекты	38	0
3	ИТ-проекты, в которых проблемы повлекли изменение запланированных целей	52	50

Несмотря на преимущества использования разработанного инструментария управления рисками в ИТ-проектах, дальнейший сравнительный анализ краткосрочных ИТ-проектов показал (таблица 3.17), что в краткосрочных ИТ-проектах доля успешного завершения, согласно данным The Standish Group равна 76%. В то время, как доля успешных исходов в исследуемых ИТ-проектах составила 60%. Однако далее доля успешно завершенных среднесрочных и долгосрочных ИТ-проектов, согласно данным The Standish Group, уменьшается до 10%. Результаты же, полученные в ходе апробации, показывают, что в исследуемых среднесрочных и долгосрочных ИТ-проектах доля успешных исходов равна 50%. Вследствие этого можно заключить, что использование разработанного автором диссертационного исследования инструментария управления рисками более актуально для среднесрочных и долгосрочных ИТ-проектов. Среди причин незначительного позитивного эффекта от использования разработанного инструментария в краткосрочных ИТ-проектах могут быть названы следующие причины:

- материализовавшиеся «тигры» и «аллигаторы» в краткосрочных ИТ-проектах оказали большее влияние на проектные цели (содержание, длительность, стоимость и качество ИТ-проектов), чем в среднесрочных и долгосрочных ИТ-проектах;
- в краткосрочных ИТ-проектах руководители приняли решения не разрабатывать меры «планов Б».

Также процесс сопоставления данных, полученных The Standish Group и данных, полученных автором диссертационного исследования, показал, что эффективность использования разработанного инструментария риск-менеджмента не имеет прямой зависимости от количества человек в ИТ-проекте. Хотя, согласно данным The Standish Group шансы на успешное завершение ИТ-проектов выше, если количество сотрудников не превышает шести человек (таблице 3.19). Доля успешных исходов для подобных проектов равна 67%. Численность сотрудников в исследуемых ИТ-проектах

варьировалась от 4 до 10 человек, при этом доля успешно завершенных ИТ-проектов составила 54,5%. Из чего следует, что разработанный инструментарий управления рисками может применяться в ИТ-проектах численностью до десяти человек, не оказывая значительного влияния на успешные исходы.

Таблица 3.19 – Сравнительный анализ успешно завершенных ИТ-проектов, незавершенных ИТ-проектов и ИТ-проектов, где проблемы повлекли изменение запланированных целей (команда проекта не превышает шести сотрудников)

№	Статус ИТ-проекта	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	Успешные ИТ-проекты	67	54,5
2	Незавершенные ИТ-проекты	5	0
3	ИТ-проекты, где проблемы повлекли изменение целей	28	45,5

В аналитических отчетах The Standish Group также рассматриваются статистические данные относительно зависимости между используемыми способами управления ИТ-проектами и успешными исходами. Как видно из таблиц 3.20 и 3.21 доли успешно завершенных ИТ-проектов, разрабатываемых по *agile* и *waterfall*, тождественны. Причем данные, полученные автором диссертационного исследования в ходе апробации (доля успешных ИТ-проектов, разрабатываемых по *agile*, равна 40%, по *waterfall* – 50%), схожи с данными, полученными The Standish Group (доля успешных проектов, разрабатываемых по *agile*, равна 46%, по *waterfall* – 47%). Отличия наблюдаются только для случаев, когда ИТ-проекты не были завершены. Критически осмыслив результаты можно заключить, что разработанный инструментарий управления рисками не противоречит способам управления ИТ-проектами, которые базируются на каскадном и итеративном способах управления проектами, что в свою очередь, удовлетворяет требованию

предъявляемому к разработанному инструментарию управления рисками, менеджментом ИТ-организаций и руководителями ИТ-проектов.

Таблица 3.20 – Сравнительный анализ успешно завершенных ИТ-проектов, незавершенных ИТ-проектов и ИТ-проектов, где проблемы повлекли изменение запланированных целей, разрабатываемых по *agile*

№	Статус ИТ-проекта	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	Успешные ИТ-проекты	46	40
2	Незавершенные ИТ-проекты	6	0
3	ИТ-проекты, где проблемы повлекли изменение запланированных целей	47	60

Таблица 3.21 – Сравнительный анализ успешно завершенных ИТ-проектов, незавершенных ИТ-проектов и ИТ-проектов, где проблемы повлекли изменение запланированных целей, разрабатываемых по *waterfall*

№	Статус ИТ-проекта	Данные полученные The Standish Group, %	Данные полученные автором диссертационного исследования, %
1	Успешные ИТ-проекты	49	50
2	Незавершенные ИТ-проекты	8	0
3	ИТ-проекты, где проблемы повлекли изменение запланированных целей	43	50

Таким образом, сравнительный анализ данных, полученных международной научно-консультационной организацией The Standish Group и автором диссертационного исследования позволяет сделать следующие выводы:

- использование инструментария управления рисками в ИТ-проектах снижает отклонение длительности от запланированных результатов и препятствует более значительным отклонениям;

- созданный инструментарий увеличивает шансы на успешное завершение ИТ-проектов с 29% до 54,5% благодаря тому, что руководители и проектные коллективы могут управлять негативными и позитивными рисками;
- разработанный инструментарий управления рисками более результативен в среднесрочных и долгосрочных ИТ-проектах;
- благодаря использованию риск-менеджмента численность сотрудников в ИТ-проектах может быть увеличена до десяти человек, не оказывая существенного негативного влияния на проектные цели (содержание, длительность, стоимость и качество проекта);
- эмпирически доказано, что разработанный инструментарий управления рисками не противоречит способам управления ИТ-проектами, таким как *waterfall* и *agile*, что удовлетворяет требованию, которое предъявляется менеджментом ИТ-организаций и руководителями ИТ-проектов.

Далее рассмотрим экономический эффект от использования управления рисками в проектах, разрабатываемых в сфере информационных технологий. Наиболее распространенным способом оценки экономической эффективности риск-менеджмента является затратный метод, где рассчитывается превышение результативности риск-менеджмента над понесенными затратами согласно формулам [211, 212]:

$$E_p = R_p - C_p, \tag{3.2}$$

$$C_p = \left(\sum_{i=1}^{N} L_{\alpha_i} + \sum_{i=1}^{N} H_{\alpha_i} \right) + \left(\sum_{j=1}^{K} L_{\alpha_j} + \sum_{j=1}^{K} H_{\alpha_j} \right), \tag{3.3}$$

$$R_p = \sum_{i=1}^{N} M_{0_i} - \sum_{i=1}^{N} M_i, \tag{3.4}$$

где E_p экономический эффект от использования риск-менеджмента; C_p – затраты на риск-менеджмент; L_{α_i} – фактические убытки от наступления i-го

идентифицированного риска; H_{α_i} – фактические расходы на обработку i-го идентифицированного риска; L_{α_j} – фактические убытки от наступления j-го неиндентифицированного риска; H_{α_j} – фактические расходы на обработку j-го неидентифицированного риска; N – количество идентифицированных рисков; K – количество неидентифицированных рисков, R_p – результат управления рисками; M_{0_i} – вероятные потери от наступления i-го идентифицированного риска без проведения мер «плана А» и «плана Б»; M_i – вероятные потери от наступления i-го идентифицированного риска после проведения мер «плана А» и «плана Б».

В таблице 3.22 представлены результаты расчетов затрат на управление рисками, потерь от использования риск-менеджмента и понесенных затрат в исследуемых ИТ-проектах. Отметим, что данные расчетов затрат фактических убытков от наступлений идентифицированных рисков, фактических расходов на обработку идентифицированных рисков, фактических убытков от наступлений неидентифицированных рисков, фактических расходов на обработку неидентифицированных рисков, вероятные потери от материализации идентифицированных рисков БЕЗ ПРОВЕДЕНИЯ мер «планов А» и мер «планов Б», вероятные потери от наступлений идентифицированных рисков ПОСЛЕ ПРОВЕДЕНИЯ мер «планов А» и мер «планов Б» приводятся в Приложении З.

Обратим внимание, что позитивный экономический эффект характеризуется превышением результатов управления рисками над расходами в процессе управления, т. е. $R_p > C_p$. Если затраты на управление рисками C_p превышают результаты от использования риск-менеджмента R_p, то можно говорить о том, что использование риск-менеджмента является экономически неоправданным.

Таблица 3.22 – Оценка экономического эффекта использования разработанного инструментария управления рисками в исследуемых ИТ-проектах

№	Название ИТ-проекта	C_p	R_p	E_p
		Затраты на управление рисками, дней	**Результат управления рисками, дней**	**Превышение результативности управления рисками над затратами, дней**
1	«Сайт ТГУ»	64,5	189	124,5
2	«МирКар»	6	18	12
3	«HyperVibe»	3,1	53	49,9
4	«Reading Log»	12,1	67	54,9
5	«CINEMOOD»	1,1	63	61,9
6	«Расчет и учет заработной платы в научно-технических учреждениях»	43,2	336	292,8
7	«Портал логистики»	10	135	125
8	«Торговая площадка»	25,2	255	229,8
9	«Регламентация ведения номенклатуры ТМЦ»	5	67	62
10	«DigitalTV»	34,4	153	118,6
11	«ERM-система»	38,6	452	413,4

В ходе анализа данных, представленных в таблице 3.22, было установлено, что разработанный инструментарий управления рисками показал наибольший экономический эффект для долгосрочного ИТ-проекта «ERM-система», среднесрочных ИТ-проектов «Торговая площадка», «Расчет и учет заработной платы в научно-технических учреждениях», «Портал логистики», «DigitalTV» и «Сайт ТГУ». Самые низкие показатели экономической эффективности наблюдались в краткосрочных ИТ-проектах. В связи с этим базируясь на выводах, сделанных в ходе исследования и результатах расчета превышения результативности риск-менеджмента над понесенными затратами можно заключить, что разработанный автором диссертационного исследования инструментарий управления рисками в большей степени актуален для среднесрочных и долгосрочных ИТ-проектов. Низкий уровень результативности в краткосрочных ИТ-проектах может быть

объяснен тем, что время потраченное на реализацию процессов риск-менеджмента не зависело от размеров ИТ-проектов.

Таким образом, в ходе оценивания результативности созданного инструментария управления рисками в ИТ-проектах можно сделать следующие выводы:

- *во-первых*, адаптированный для сферы ИТ инструментарий управления рисками дает возможность руководителям и коллективам идентифицировать негативные, позитивные и уникальные риски в краткосрочных и среднесрочных ИТ-проектах. Для долгосрочных проектов автор диссертационного исследования рекомендует систематически повторять выявление рисков во время разработки ИТ-проекта, привлекая к работе в том числе и сторонних экспертов;
- *во-вторых*, установлено, что негативные рисковые события, которые чаще остальных рисков материализуются в ИТ-проектах, в большинстве случаев схожи друг с другом и мало сопряжены с размерами, типами, способами управления ИТ-проектами. Показано, что наличие и количество позитивных рисков зависят от особенностей и специфики ИТ-проектов;
- *в-третьих*, обнаруженная связь между негативными рисками, полученными в ходе апробации и рисками, которые были получены Т. Аддисоном, С. Валлабхом, К. Д. Стивенсом, С. Фовеллом и М. Самнером, дает возможность предположить, что разработанный инструментарий управления рисками является универсальным и может применяться в международных ИТ-проектах;
- *в-четвертых*, сравнительный анализ данных, полученных международной научно-консультационной организацией The Standish Group и автором диссертационного исследования показал, что разработанный инструментарий управления рисками снижает отклонение длительностей от запланированных результатов до 33,3%, увеличивает шансы на успешное

завершение среднесрочных и долгосрочных ИТ-проектов, а также не противоречит способам управления проектами;

- *в-пятых*, обнаружено, что экономический эффект прямо пропорционален размерам ИТ-проектов. Это позволило установить, что использование риск-менеджмента является экономически оправданным в среднесрочных и долгосрочных ИТ-проектах. Однако несмотря на низкий позитивный эффект в краткосрочных проектах, результаты от использования риск-менеджмента превысили понесенные затраты.

Выводы по третьей главе:

1. В рамках диссертационного исследования проведенный анализ деятельности и финансового состояния семи ИТ-организаций позволил установить, что трудности, с которыми сталкиваются ИТ-организации во многом связаны с материализацией негативных рисков. Установленная связь позволила сделать вывод, что многих проблем можно было бы избежать превентивно нивелируя, ослабляя и эскалируя негативное влияние рисковых событий. Обнаружено, что в исследуемых организациях отсутствует инструментарий идентифицирующий и стимулирующий наступление позитивных рисков. Также основываясь на анализе причин низкой популярности риск-менеджмента в ИТ-организациях и ИТ-проектах сформулированы требования, предъявляемые к инструментарию управления рисками ИТ-проектов в организациях.

2. Апробация показала, что адаптированные методы для сферы информационных технологий были успешно внедрены в исследуемые ИТ-проекты независимо от их размеров, типов, численности коллективов и способов реализации ИТ-проектов.

3. Эмпирически доказано, что инструментарий риск-менеджмента, использующий авторские разработки дает возможность руководителям ИТ-проектов и проектным коллективам идентифицировать уникальные и специфические негативные (позитивные) риски, оперативно проводить анализ и оценивание рисков, разрабатывать меры воздействия на рисковые

события, базируясь на одной из стратегий управления, а также обеспечивать мониторинг и контроль рисков с учетом особенностей ИТ-проектов, в свою очередь, является основанием для приращения научных знаний в области риск-менеджмента и дополнения ГОСТа Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство».

4. Сравнительный анализ данных, полученных международной научно-консультационной организацией The Standish Group и автором диссертационного исследования, продемонстрировал, что разработанный инструментарий управления рисками снижает отклонение длительностей от запланированных результатов, увеличивает шансы на успешное завершение в среднесрочных и долгосрочных ИТ-проектах, не противоречит способам управления ИТ-проектами. Установлена связь между негативными рисками, полученными в ходе апробации и рисковыми событиями, которые были описаны иностранными учеными, на основании чего сделано предположение, что созданный инструментарий универсален и может применяться в международных ИТ-проектах.

5. Подтвержден положительный экономический эффект, где результаты от использования риск-менеджмента превышают понесенные затраты в краткосрочных, среднесрочных и долгосрочных ИТ-проектах, на основании чего сделан вывод, что применение созданного инструментария управления рисками ИТ-проектов в организациях является экономически оправданным.

ЗАКЛЮЧЕНИЕ

В качестве **научной гипотезы** диссертационного исследования было выдвинуто предположение о том, что реализация ИТ-проектов происходит под воздействием как негативных, так и позитивных рисков, которые могут быть оценены посредством специального инструментария управления ими. Главная идея диссертационной работы базируется на результатах анализа современного состояния мировой и ответственной экономики, действующего законодательства, государственных интересов на рынке информационных технологий, сводов лучших управленческих практик и стандартов управления проектами, характеристик деятельности и финансового положения ИТ-организаций, а также на анализе обобщенного передового опыта в области риск-менеджмента. Полученные автором диссертационного исследования результаты подтверждают выдвинутое предположение о том, что фазы жизненного цикла ИТ-проектов в организациях подвержены значительному влиянию негативных и позитивных рисков, которые могут быть выявлены, проанализированы и оценены с помощью специального адаптированного инструментария управления рисками.

По завершению исследования автором настоящей диссертационной работы были получены следующие **научные результаты**:

1. Уточнены понятия «риск», «управление рисками в ИТ-проектах» и «неопределенность». В частности:

- *во-первых*, представлено новое содержание термина «риск», под которым понимается возможное событие, которое порождается конкретными источниками (источники риска), материализация которого под воздействием определенных факторов (факторы риска) способно оказать негативное (позитивное) влияние на запланированные проектные цели (содержание, длительность, стоимость и качество проекта), побуждая наступление проблемных (благоприятных) ситуаций;

- *во-вторых*, усовершенствована дефиниция «управление рисками в ИТ-проектах». Под «риск-менеджментом в ИТ-проектах» понимается совокупность процессов по оценке негативных (позитивных) рисков, управленческие решения по разработке мер воздействия, мониторинг неидентифицированных рисков и контроль идентифицированных рисков. Вновь предложенная дефиниция понятия «управление рисками в ИТ-проектах» существенно отличается от ныне существующих, так как включает в себя понятие «позитивный риск», управление которым, как показали результаты настоящего диссертационного исследования, может положительно влиять на план проекта и на проектные цели, предвосхищая ранее запланированные результаты;
- *в-третьих*, уточнено содержание понятия «неопределенность». Автором диссертационного исследования было установлено, что под «неопределенностью» следует понимать совокупность стохастических событий, наступление которых невозможно прогнозировать, а под «риском» следует понимать совокупность конкретных источников риска, факторов риска и проблемных (благоприятных) ситуаций.

2. Установлено, что зарубежные и отечественные ученые расходятся во мнениях относительно способов классификации рисков. Отсутствие универсального способа группировки рисков, специфика сферы информационных технологий, практическая значимость ранжирования рисков побудили автора диссертационной работы создать способ классификации рисков основываясь на таких классификационных признаках, как среда, внешний и внутренний проектные источники, срочность риска, негативный и позитивный аспекты риска, уровень управления риском, фазы жизненного цикла и проектные цели. Предложенная автором настоящего диссертационного исследования классификация рисков ИТ-проектов в организациях способствует обнаружению специфических и скрытых рисковых событий, стимулирует развитие стандартизации мер

управленческого воздействия на риски, улучшает мониторинг и контроль рисков, а также рационализует функцию планирования в ИТ-проектах.

3. Обнаружено, что классический набор инструментов предлагаемый PMBOK® Guide для обработки информации о рисках не соответствует области информационных технологий. PMBOK® Guide не рассматривает и не предлагает инструментов определения времени актуализации рисков. Решая данную проблему автор диссертационного исследования предложил методику определения времени актуализации рисков относительно фаз жизненного цикла ИТ-проекта с выявлением постоянных рисков, способных материализоваться на любом этапе реализации проекта. Предлагаемый методический инструментарий дает возможность получать исчерпывающую информацию о вероятных событиях, способных оказать значительное влияние на проектные цели, а также идентифицировать наиболее опасные временные периоды.

4. Обоснован способ группировки позитивных рисков с представлением в нем: «слонов», как созидательных рисков; «львов», как непредсказуемых рисков; «обезьян», как часто встречаемых рисков; «кроликов», как незначительных рисков. Данный способ группировки позитивных рисков совершенствует и дополняет классическую группировку рисков, позволяет идентифицировать позитивные риски требующие дополнительных стимулирующих мер воздействия, получать информацию о позиционировании позитивных рисков друг относительного друга и выявлять наиболее значимые позитивные рисковые события, что существенно сокращает материальные и временные затраты на управление рисками ИТ-проектов в организациях.

5. Разработан и научно обоснован инструментарий управления рисками ИТ-проектов в организациях, который применим для ИТ-проектов различной длительности, типов, численности проектных коллективов, а также способов управления ИТ-проектами, учитывающий негативные и позитивные аспекты природы риска, оперативно реализующий базовые

процессы риск-менеджмента, снижающий отклонение фактических трудозатрат от запланированных.

Адаптация методов применяемых для разработки мер воздействия на риски позволила усовершенствовать метод «галстук-бабочка» (второй этап). Анализ данного метода показал, что в классическом исполнении он сфокусирован на работе с негативными рисками. Используя свойства метода устанавливать связь между источниками рисков и проблемными (благоприятными) ситуациями, автор диссертационного исследования улучшил алгоритм данного метода включая «стимулирующие меры» и «меры усиления», которые способствуют качественному анализу позитивных рисков, а также стимулирует процесс создания результативных мер воздействия на позитивные риски.

Кроме того, автором диссертационной работы предложен способ мониторинга и контроля рисков с помощью триггерных условий. Способ базируется на стандартах проектного управления, где после разработки части программного кода, коллективы во время ретроспективного анализа обсуждают значимые события. Было установлено, что подобный способ мониторинга и контроля рисков обеспечивает плавную интеграцию созданного инструментария управления рисками в ИТ-проекты, не вызывая конфликтов с используемыми классическими способами управления проектами, такими как *agile* и *waterfall*.

Проведенная апробация авторского инструментария управления рисками в семи ИТ-организациях показала, что трудности, с которыми встречаются данные организации имеют общие источники рисков. Обнаруженная связь позволила сделать вывод, что проблем с которыми сталкиваются исследуемые ИТ-организации можно избежать, если превентивно нивелировать и ослаблять негативное влияние рисков, порождаемых общими источниками рисков.

Кроме того, проведенный автором диссертационного исследования анализ причин низкой популярности риск-менеджмента в ИТ-организациях и

ИТ-проектах позволил сформулировать требования к инструментарию управления рисками. Было установлено, что ИТ-организации готовы применять риск-менеджмент, если:

- *во-первых*, инструментарий управления рисками не будет противоречить способам реализации ИТ-проектов;
- *во-вторых*, инструментарий риск-менеджмента будет интегрироваться в любой ИТ-проект независимо от его размера, типа, численности коллектива и способа управления ИТ-проектом;
- *в-третьих*, в процессе идентификации будут выявляться негативные, позитивные и уникальные риски;
- *в-четвертых*, процессы управления рисками будут выполняться оперативно;
- *в-пятых*, инструментарий управления рисками будет показывать позитивный экономический эффект.

Апробация авторского инструментария управления рисками показала, что адаптированные методы для сферы информационных технологий были успешно внедрены в ИТ-проекты независимо от их размеров, типов, численности коллективов и способов управления ИТ-проектами. Эмпирически доказано, что разработанный инструментарий выявляет уникальные негативные и позитивные риски, обеспечивает оперативное выполнение процессов риск-менеджмента, а также учитывает особенности сферы ИТ при мониторинге и контроле рисков. Более того, был отмечен положительный экономический эффект от использования данного инструментария.

Полученные экспериментальные данные показали, что применение разработанного инструментария управления рисками значительно снижает фактическое отклонение от запланированных длительностей в среднесрочных и долгосрочных проектах, что было подтверждено в рамках сравнительного анализа и сопоставления результатов, полученных ранее

предшественниками. На основании этого можно сделать вывод о том, что созданный инструментарий обладает высоким практическим потенциалом, в свою очередь, является основанием для приращения научных знаний в области риск-менеджмента и дополнения ГОСТа Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство».

Обобщая основные результаты можно заключить, что **цель** диссертационного исследования направленная на создание инструментария управления рисками ИТ-проектов в организациях, включающая в себя идентификацию, анализ, оценивание вероятностей материализации рисков и их возможного влияния, мониторинг и контроль рисков, а также разработку мер превентивного воздействия (мер «плана А») и мер принятия рисков (мер «плана Б»), достигнута.

Таким образом, можно заключить, что результаты диссертационного исследования могут быть использованы в любом субъекте сферы ИТ, в том числе и национальных ИТ-проектах, таких как «Государственная информационная система ”Моя школа”», «АИС Маркировка», «ИТ-система обмена знаниями и технологиями в сфере сельского хозяйства», «ИТ-система социального обеспечения», «ИТ-система учета отходов», «Единый транспортный сервис в рамках противодействия незаконным финансовым операциям», «Автоматизированная система контроля применения контрольно-кассовой техники», а также в других ИТ-проектах, инициированных в рамках Указа Президента РФ от 09.05.2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» и от 07.05.2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Владинец Н. И., Ильичев Л. И., Левитас И. Я., Мазур П. Ф., Меркулов И. Н., Моросанов И. А., Мякота Ю. К., Панасян С. А., Рудников Ю. М., Слуцкий М. Б., Якобс В. А. Народный комиссариат связи СССР. Большой филателистический словарь; под общ. ред. Н. И. Владинца и В. А. Якобса. – М.: Радио и связь, 1988. – 320 с.

2. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. – URL: http://minsvyaz.ru (дата обращения 30.03.2021 г.).

3. Беркун С. Искусство управления IT-проектами. – СПб.: Питер, 2014. – 255 с.

4. Официальный сайт Федеральной службы государственной статистики [Электронный ресурс]. – URL: http://www.gks.ru (дата обращения 30.03.2021 г.).

5. Официальный сайт «1С» [Электронный ресурс]. – URL: http://1c.ru (дата обращения 30.03.2021 г.).

6. Официальный сайт «БОСС. Кадровые системы» [Электронный ресурс]. – URL: http://www.bosshr.ru/ (дата обращения 30.03.2021 г.).

7. Официальный сайт «Группа ИНЭК-ИТ» [Электронный ресурс]. – URL: http://inec.ru (дата обращения 30.03.2021 г.).

8. Официальный сайт «Отдел кадров плюс» [Электронный ресурс]. – URL: http://www.okpartner.ru (дата обращения 30.03.2021 г.).

9. Официальный сайт «Assessment Tools» [Электронный ресурс]. – URL: http://learnware.ru (дата обращения 30.03.2021 г.).

10. Официальный сайт «Oracle» [Электронный ресурс]. – URL: https://www.oracle.com (дата обращения 30.03.2021 г.).

11. Официальный сайт «АиТ СОФТ» [Электронный ресурс]. – URL: http://www.aitsoft.ru (дата обращения 30.03.2021 г.).

12. Официальный сайт «Платон» [Электронный ресурс]. – URL: http://platon.ru (дата обращения 30.03.2021 г.).

13. Официальный сайт Федеральной службы по регулированию алкогольного рынка [Электронный ресурс]. – URL: https://egais.ru/ (дата обращения 30.03.2021 г.).

14. Васильев А. А. Информационные технологии в управлении // Перспективы науки и образования. – 2015. – №4 (16). – С. 76-82.

15. Золотов А. В. Сокращение рабочего дня как основа обеспечения занятости в цифровой экономике // Экономика и предпринимательство. – 2019. – №5(106). – С. 293-296.

16. Официальный сайт «CNews Analytics» [Электронный ресурс]. – URL: http://www.cnews.ru (дата обращения 30.03.2021 г.).

17. Официальный сайт «Gartner» [Электронный ресурс]. – URL: http://www.gartner.com (дата обращения 30.03.2021 г.).

18. Официальный сайт Министерства экономического развития Российской Федерации [Электронный ресурс]. – URL: http://economy.gov.ru (дата обращения 30.03.2021 г.).

19. Официальный сайт «IDC» [Электронный ресурс]. – URL: http://idcrussia.com (дата обращения 30.03.2021 г.).

20. Официальный сайт «McKinsey & Company» [Электронный ресурс]. – URL: http://www.mckinsey.com (дата обращения 30.03.2021 г.).

21. Федеральный закон РФ № 244-ФЗ от 28 сентября 2010 года «Об инновационном центре «Сколково» [принят Государственной Думой 21 сентября 2010 года. Одобрен Советом Федерации 22 сентября 2010 года] // Российская газета – Федеральный выпуск . – 30.09.2010. – № 5299 (220).

22. Федеральный закон РФ № 254-ФЗ от 21 июля 2011 года «О внесении изменений в Федеральный закон «О науке и государственной научно-технической политике» [принят Государственной Думой 06 июля 2011 года] // Российская газета – Федеральный выпуск. – 26.07.2011. – №5537 (161).

23. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Приказ Минкомсвязи России № 96 от 1 апреля 2015 года «Об утверждении плана импортозамещения программного обеспечения» [Электронный источник]. – URL: https://clck.ru/TyyjN (дата обращения 30.03.2021 г.).

24. Официальный сайт Правительства Российской Федерации. Постановление Правительства Российской Федерации № 1236 от 16 ноября 2015 года «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [Электронный источник] – URL: https://clck.ru/EhDkh (дата обращения 30.03.2021 г.).

25. Федеральный закон от 29 июня 2015 г. N 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статья 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [принят Государственной думой 19 июня 2015 года. Принят Советом Федерации 24 июня 2015 года] // Российская газета – Федеральный выпуск. – 06.07.2015. – № 6716 (145).

26. Официальный сайт Единого реестра российских программ для электронных вычислительных машин и баз данных [Электронный ресурс]. – URL: https://reestr.digital.gov.ru/reestr/?name= (дата обращения 30.03.2021 г.).

27. Официальный сайт Правительства Российской Федерации. Постановление Правительства РФ №57 от 27 января 2017 года «О создании Российского фонда развития информационных технологий» [Электронный источник]. – URL: https://clck.ru/EhDkh (дата обращения 30.03.2021 г.).

28. Официальный сайт Президента Российской Федерации. Указ Президента РФ №203 от 9 мая 2017 года «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»

[Электронный источник]. – URL: https://clck.ru/EXaJo (дата обращения 30.03.2021 г.).

29. Официальный сайт Правительства Российской Федерации. Распоряжение Правительства РФ №1632-р от 27 июля 2017 года «Об утверждении программы Цифровая экономика Российской Федерации» [Электронный источник]. – URL: https://clck.ru/EhDkh (дата обращения 30.03.2021 г.).

30. Трофимов О. В., Саакян А. Г. Функционирование промышленных предприятий в условиях цифровой экономики // Фундаментальные исследования. – 2018. – № 8. – С. 122-126.

31. Масютин С. А., Гуськова И. В. Промышленность России в цифровой экономике: тенденции и возможности // Экономика и предпринимательство. – 2018. – №11(100). – С. 238-242.

32. Морозова Г. А., Лапаев Д. Н. Цифровая экономика как основа ускорения развития РФ // Актуальные вопросы экономики, менеджмента и инноваций. – 2018. – С. 173-174.

33. Иванов А. А., Яшин С. Н., Иванова Н. Д. Анализ современного состояния и формирования цифровой экономики России // Цифровая трансформация экономики и промышленности. – 2019. – С. 104-113.

34. Яшин С. Н., Коробова Ю. С., Борисов С. А. Совершенствование системы стратегического планирования инновационного развития промышленного предприятия в условиях цифровой экономики // Управление инновациями: вызовы и возможности для отраслей и секторов экономики. – 2019. – С. 281-291.

35. Официальный сайт «EY» [Электронный ресурс]. – URL: http://www.ey.com (дата обращения 30.03.2021 г.).

36. Никулина И. Е., Николаенко В. С. Государственное регулирование сферы информационных технологий в Российской Федерации // Государственное управление. Электронный вестник. – 2018. – № 67. – С. 137–149.

37. Официальный сайт «The Standish Group» [Электронный ресурс]. – URL: https://standishgroup.com/ (дата обращения 30.03.2021 г.).

38. Lee O.-K. D., Baby D V. Managing dynamic risks in global IT projects: agile risk-management using the principles of service-oriented architecture // International Journal of Information Technology & Decision Making. – 2013. – Vol.12. − №6. – P. 1121−1150.

39. Корнилов Д. А., Корнилова Е. В. Криптовалюты и токенизация бизнеса // Вестник НГИЭИ. – 2019. – №5(96). – С. 107-118.

40. Project management body of knowledge. Guide 4th edition (PMBOK-4). – Project Management Institute (PMI), 2008. – 506 p.

41. Project management body of knowledge. Guide 5th edition (PMBOK-5). – Project Management Institute (PMI), 2013. – 616 p.

42. Project management body of knowledge. Guide 6th edition (PMBOK-6). – Project Management Institute (PMI), 2017. – 756 p.

43. Organizational Project Management Maturity Model (OPM3). – Project Manadgement Inctitute, 2003. – 195 p.

44. Официальный сайт Международной ассоциации управления проектами «IPMA International Project Management Association» [Электронный ресурс]. – URL: http://www.ipma.world (дата обращения 30.03.2021 г.).

45. Официальный сайт «Project Management Institute» [Электронный ресурс]. – URL: https://www.pmi.org (дата обращения 30.03.2021 г.).

46. Постановление Правительства РФ от 15.10.2016 года № 1050 «Об организации проектной деятельности в Правительстве Российской Федерации» [Электронный источник]. – URL: https://clck.ru/Tz2Mp (дата обращения 30.03.2021 г.).

47. Individual Competence Baseline for Project, Programme & Portfolio Management (ICB). Version 4.0. – International Project Management Association, 2015. – 432 p.

48. Organisation Competence Baseline for Developing Competence in Managing by Projects (OCB). Version 1.1. – International Project Management Association, 2016. – 112 p.

49. Project Excellence Baseline for Achieving Excellence in Projects and Programmes (PEB). Version 1.0 – International Project Management Association, 2016. – 113 p.

50. Gilb T. Principles of Software Engineering Management. – Addison-Wesley Professional, 1988. – 464 p.

51. Бахтизин В. В. Технология разработки программного обеспечения. – Минск: БГУИР, 2010. – 267 с.

52. Managing Successful Projects with PRINCE2. – TSO, 2017. – 412 p.

53. Официальный сайт «Microsoft Solution framework» [Электронный ресурс]. – URL: https://www.microsoftpressstore.com (дата обращения 30.03.2021 г.).

54. Официальный сайт Международной организации по стандартизации «International Organization for Standardization» [Электронный ресурс]. – URL: https://www.iso.org/ru/home.html (дата обращения 30.03.2021 г.).

55. Бек К. Экстремальное программирование: разработка через тестирование. – СПб.: Питер, 2003. – 216 с.

56. Кон М. Scrum. Гибкая разработка ПО. – М.: Вильямс Издательский дом, 2011. – 576 с.

57. ГОСТ Р 54869-2011. Проектный менеджмент. Требования к управлению проектом. – М.: Стандартинформ, 2012. – 11 с.

58. ГОСТ Р 21500-2014. Руководство по проектному менеджменту (ISO 215000:2012. Guidance on project management). – М.: Стандартинформ, 2015. – 52 с.

59. Никулина И. Е., Николаенко В. С. Становление и развитие концепций управления проектами и риск-менеджмента // Государственное управление. Электронный вестник. – 2018. – № 68. – С. 195–210.

60. Boehm B.W. Software Engineering Economics // Englewood Cliffs. – NJ.: Prentice-Hall. – 1981. – P. 1−42.

61. Hoda R. Self-Organizing Agile Teams: A Grounded Theory. – Victoria University of Wellington, 2011. – 262 p.

62. Brandas C., Didraga O., Bibu N. Study on risk approaches in software development project // Informatica Economica. – 2012. – Vol. 16. – №3. – P. 148−157.

63. The CHAOS Manifesto. – The Standish Group, 2013. – 48 p.

64. The CHAOS Manifesto. – The Standish Group, 2014. – 16 p.

65. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ISO 31000:2009. Risk management – Principles and guidelines (IDT). – М.: Стандартинформ, 2012. – 19 с.

66. Балабанов И. Т. Риск-менеджмент. – М. : Финансы и статистика, 1996. – 192 с.

67. Машков Д. М. Научные подходы к управлению рисками промышленных предприятий // Инженерный вестник Дона. – 2014. – Том 31. – №4-1. – С. 65.

68. Филимонов Д. И. Классификация рисков кадровой безопасности в деятельности IT-структур // Экономика и предпринимательство. – 2017. – № 5-1 (82-1). – С. 682-685.

69. Бурков В. Н., Новиков Д. А. Как управлять проектами. – М.: Синтег, 1997. – 188 с.

70. Мазур И. И., Шапиро В. Д. Управление проектами. – М.: Высшая школа, 2001. – 502 с.

71. Sanghera P. PMP exam in depth, second edition: project management professional study guie for the PMP exam. – Course technology, a part of Cengage Learning, 2010. – 592 p.

72. Официальный сайт «PricewaterhouseCoopers» [Электронный ресурс]. – URL: http://www.pwc.ru (дата обращения 30.03.2021 г.).

73. Грабовый П. Г., Петрова С. Н. и др. Риски в современном бизнесе. – М.: Издательство «Алане», 1994 г. – 200 с.

74. Шохин Е. И. Финансовый менеджмент. – М.: ИД ФБК-ПРЕСС, 2002. – 408 с.

75. Королев В. Ю., Бенинг В. Е., Шоргин С. Я. Математические основы теории риска. – М. : Физматлит, 2011. – 620 с.

76. Гражданский кодекс Российской Федерации от 30 ноября 1994 года №51-ФЗ. Принят Государственной Думой 21 октября 1994 года. – 688 с.

77. Даль В. И. Толковый словарь живого великорусского языка. – М.: Цитадель, 1998. – 11465 с.

78. Management of Risk: Guidance for Practitioners. – The Office of Government Commerce, 2010. – 160 p.

79. Качалов Р.М. Управление хозяйственным риском. – М.: Наука, 2002. – 192 с.

80. Enterprise Risk Management. Integrating with Strategy and Performance. – Committee of Sponsoring Organizations of the Treadway Commission, 2017. – 16 p.

81. Мадера А. Г. Риски и шансы. Неопределенность, прогнозирование и оценка, 2014. – М.: Красанд. – 448 с.

82. Мадера А. Г. Принятие решений в условиях неопределенности при актуализации в будущем множества возможных шансов и рисков // Экономические науки. – 2014. – №4. – С. 136-140.

83. Фадейкина Н. Эволюция взглядов на категории «риск» и «неопределенность» в экономической науке // Риск: ресурсы, информация, снабжение, конкуренция. – 2013. – № 3. – С. 202-208.

84. ISO 31000:2009. «Risk Management – Principles and Guidelines», 2009. – 24 p.

85. ISO 31000:2018 Risk management – Guidelines. 2th edition. – International Organization for Standardization, 2018. – 19 p.

86. Vaníčková R. Application of PRINCE2 Project Management Methodology // Studia Commercialia Bratislavensia. – 2017. – No.10(38). – P. 227–238.

87. Качалов Р. М. Управление экономическим риском: Теоретические основы и приложения: монография. – М.; СПб.: Нестор-История, 2012. – 248 с.

88. Paladino B., Cuy L., Frigo M. Missed opportunities in performance and enterprise risk management // Journal of Corporate Accounting & Finance. – 2009. – No. 20(3). – P. 43–51.

89. Рудаков Д. В., Михайлова М. Е. Проблемы риск-менеджмента предприятий в России // Динамика систем, механизмов и машин. – 2012. – №4. – С. 37-39.

90. Божко Л. М. Риск-менеджмент в управлении организационными изменениями на основе маркетингового подхода // Вестник Астраханского государственного технического университета. Серия: Экономика. – 2014. – №1. – С. 22-28.

91. Болова И. С., Морозова В.Д. Этапы внедрения системы риск-менеджмента на предприятии в современных условиях // Современные проблемы науки и образования. – 2014. – №3. – С. 379.

92. Борисоглебская Л. Н., Емельянов С.Г. Риск-менеджмент российской экономики // Научные ведомости Белгородского государственного университета. Серия: История. Политология. Экономика. Информатика. – 2007. – Том 2. – №3. – С. 154-158.

93. Давидянц Т. Э. Риск-менеджмент как система стратегического управления предприятием // Журнал правовых и экономических исследований. – 2012. – №1. – С. 140-144.

94. Ермасова Н. Б. Риск-менеджмент организации. – М.: Издательство торговая корпорация «Дашков и К», 2012. – 308 с.

95. Mishra A., Das S., Murray J. Managing Risk in Government Information Technology Projects: Does Process Maturity Matter? // Production and Operations Management. – 2014. – No. 24(3). – P. 365−368.

96. Internal Control – Integrated Framework. Guidance on Monitoring Internal Control Systems, 2008. – Vol. 3. – 117 p.

97. Гиндикин С. Г. Рассказы о физиках и математиках. – М.: МЦНМО, 2001. – 448 с.

98. Aven T. The risk concept – historical and recent development trends // Reliability Engineering and System Safety. – 2012. – Vol. 99. – P. 33-44.

99. Никулина И. Е., Николаенко В. С. Хронология развития риск-менеджмента // Синергия науки и практики в контексте инновационных прорывов в развитии экономики и общества: национальные и международные аспекты: сборник научных статей по итогам Международной научно-практической конференции. 9-10 декабря 2019 года. Санкт-Петербург. – СПб. : Изд-во СПбГЭУ, 2019. – С.262-264.

100. Никулина И. Е., Николаенко В. С. Становление и развитие концепций управления проектами и риск-менеджмента // Государственное управление. Электронный вестник. – 2018. – № 68. – С. 195-210.

101. Смит А. Исследование о природе и причинах богатства народов. – М.: Эксмо, 2016. – 1056 с.

102. Аникин А. В. Джон Стюарт Милль. Юность науки: Жизнь и идеи мыслителей-экономистов до Маркса. – М. : Политиздат, 1975. – 384 с.

103. Найт Ф. Х. Риск, неопределенность и прибыль. – М. : Дело, 2003. – 360 с.

104. Нейман Дж. фон, Моргенштерн О. Теория игра и экономическое поведение. – М. : Наука, 1970. – 708 с.

105. ГОСТ Р 51901.11-2005 (МЭК 61882:2001) Hazard and operability (HAZOP studies) – Application guide (MOD). – М.: Стандартинформ, 2006. – 46 с.

106. ГОСТ Р 51901.3-2007 (МЭК 60300-2:2004) Руководство по менеджменту надежности. Dependability management – Part 2: Guidelines for dependability management (MOD). – М.: Стандартинформ, 2008. – 50 с.

107. ГОСТ Р 51901/12-2007 (МЭК 60812:2006) Метод анализа видов и последствий отказов. IEC 60812:2006. Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) (MOD).). – М.: Стандартинформ, 2008. – 40 с.

108. ГОСТ Р 51901.14-2007 (МЭК 61078:2008) Структурная схема надежности и булевых методов. Analysis techniques for dependability – Reliability block diagram and Boolean methods (MOD).). – М.: Стандартинформ, 2008. – 24 с.

109. ГОСТ Р ИСО/МЭК 16085-2007 Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения. ISO/IEC 16085:2006. System and software engineering – Life cycle processes – Risk management (IDT). – М.: Стандартинформ, 2008. – 31 с.

110. ГОСТ Р 31010-2011 Методы оценки риска. ISO/IEC 31010:2009. Risk management – Risk assessment techniques (IDT). – М.: Стандартинформ, 2012. – 74 с.

111. ГОСТ Р 51901.21-2012 Менеджмент риска. Реестр риска. Общие положения. – М.: Стандартинформ, 2014. – 16 с.

112. ГОСТ Р 51901.22-2012 Менеджмент риска. реестр Риска. Правила построения. – М.: Стандартинформ, 2014. – 20 с.

113. ГОСТ Р 51901.23-2012 Менеджмент риска. Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска. – М.: Стандартинформ, 2014. – 35 с.

114. Stevens K. J., Fowell S. Perspective on E-Business Software Project Risk // 7th Pacific Asia Conference on Information Systems. – 2003. – P. 95−107.

115. Белых В. С. Правовое регулирование предпринимательской деятельности в России. – М.: Монография, 2005. – 430 с.

116. Трифонов Ю. В., Фомина Е. А. Методика оценки рисков автоматизации при реализации инвестиционных проектов малыми и средними предприятиями // Бизнес-тренды: цифровые технологии в менеджменте. – 2019. – С.13-18.

117. Битнер Г. Г. Теория вероятностей / Г. Г. Битнер. – Ростов н/Д: Феникс, 2012. – 329 с.

118. Ключников В. О. Идентификация рисков ИТ-проектов // Государственное управление. Электронный вестник. – 2009. – № 20. – С. 1−7.

119. Ключников В. О. Опционный метод управления рисками в инвестиционных ИТ-проектах // Вестник Московского университета. Серия 21: Управление (государство и общество). – 2010. – № 1. – С. 69-78.

120. Ключников В. О. Реальные опционы в проектах информационных технологий // Российское предпринимательство. – 2011. – № 12-2. – С. 118-124.

121. Никонов В. А. Управление рисками. Как больше зарабатывать и меньше тратить. – М. : Альпина Паблишерз, 2009. – 285 с.

122. Поляков А.А., Ключников В. О. Опционный метод управления рисками в инвестиционных ИТ проектах // Вестник Московского университета. Серия 21: Управление (государство и общество). – 2010. – № 1. – С. 69-78.

123. Поляков А. А. Информационные системы в управлении // Вестник Московского университета. Серия 21: Управление (государство и общество). – 2006. – № 3. – С. 21-39.

124. Ефимов В. В. Сборник методов поиска новых идей и решений управления качеством. – Ульяновск: УлГТУ, 2011. – 194 с.

125. Crawley F., Tyler B. Hazard identification methods. Institute of Chemical Engineers, 2003.

126. Card A., Ward J., Clarkson P. Beyond FMEA: the structured what-if technique (SWIFT) // Healthcare Risk Manage. – 2012. – Vol. 31. – P. 23–29.

127. Губанов Р. С. Разработка стратегии риск-менеджмента // Горный информационно-аналитический бюллетень (научно-технический журнал). – 2008. – №7. – С. 63-67.

128. Рэдхэд К., Хьюс С. Управление финансовыми рисками. – М.: Инфра-М, 1996. – 288 с.

129. Яроцкая Е. В. Управление имущественными рисками предприятия: монография / Е. В. Яроцкая; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2011. – 131 с.

130. Официальный сайт «Innovation games» [Электронный ресурс]. – URL: http://www.innovationgames.com (дата обращения 30.03.2021 г.).

131. Авдошин С.М., Песоцкая Е. Ю. Информатизация бизнеса. Управление рисками, 2011. – М.: ДМК Пресс. – 176 с.

132. Песоцкая Е. Ю. Управление рисками в ИТ-проектах // Альманах современной науки и образования. – 2008. – №1(8). – С. 157−159.

133. Песоцкая Е. Ю. Управление рисками при внедрении ИТ-проектов // Успехи современного естествознания. – 2008. − №1. – С. 11−13.

134. Lewis S., Smith K. Lessons Learned from Real World Application of the Bow-tie Method // 6th Global Congress on Process Safety. – 2010. – P. 1−20.

135. Ishikawa K. Guide to quality control. – Asian Productivity Organization, 1986. – 226 p.

136. Пестерева Е. Канбан и «точно вовремя» на Toyota: Менеджмент начинается на рабочем месте. – М. : Альпина Паблишер, 2015. – 214 с.

137. Панде П. Что такое «шесть сигм»? Революционный метод управления качеством. – М.: Альпи-на Бизнес Букс, 2006. – 158 с.

138. Домащенко Д. В. Управление рисками в условиях финансовой нестабильности / Д. В. Домащенко, Ю. Ю. Финогенова, 2010. – М.: Магистр: ИНФРА. – 238 с.

139. Тарасенко Ф. П. Прикладной системный анализ. – М: КНОРУС, 2010. – 224 с.

140. Мадорская Ю. М. Повышение точности и сокращение времени планирования в процессах управления проектами по разработке программного обеспечения // Международная техническая конференция «Технические науки: проблемы и перспективы» Санкт-Петербург. – 2011. – С. 92-99.

141. Raymond E. The Art of Unix Programming, 2003. – Addison-Wesley. – 549 p.

142. Джеффрис Р., Андерсон Э., Хендриксон Ч., Джеффрис Р. Э. Extreme Programming Installed, 2000. – Addison-Wesley Professional. – 288 p.

143. Официальный сайт «Manifesto for Agile Software Development» [Электронный ресурс]. – URL: http://agilemanifesto.org (дата обращения 30.03.2021 г.).

144. Феонова М. Р. Управление персоналом: Методология анализа качества рабочей силы. – М.: Наука, 2001. – 214 с.

145. Адлер Ю. А., Маркова Е. В., Грановский Ю. В. Планирование эксперимента при поиске оптимальных условий. – М.: Наука, 1976. – 280 с.

146. Талеб Н. Н. Одураченные случайностью. Скрытая роль шанса в бизнесе и жизни. – М. : Манн. Иванов и Фербер, 2011. – 320 с.

147. Талеб Н. Н. Антихрупкость. Как извлечь выгоду из хаоса / Нассим Николас Талеб; пер. с англ. Н. Караева. – М. : КоЛибри, Азбука-Аттикус, 2016. – 768 с.

148. Талеб Н. Н. Черный лебедь. Под знаком непредсказуемости – 2-е изд., доп. / Нассим Николас Талеб ; пер. с англ.. – М. : КоЛибри, Азбука-Аттикус, 2015. – 736 с.

149. The Department of Defense (DoD) United States of America. Risk Management Guide for DOD Acquisition, 2006. – Sixth Edition. – Version 1.0. – 34 p.

150. Merna T., Al-Thani F. Corporate risk management. – John Wiley & Sons, Ltd, 2008. – 2nd ed. – 443 p.

151. Волкова Ю. П., Олейникова Е. А., Филин С. А., Пирогов М. В. Инвестиционная политика современной России: Коллективная монография. – М. : РЭА им. Г.В. Плеханова, 2001. – 401 с.

152. Мильнера Б., Лииса Ф. Управление современной компанией. – М. : ИНФРА-М, 2001. – С. 350.

153. Колесник Д. Н. Практические аспекты внедрения информационных систем оценки деятельности предприятия. Журнал школы IT-менеджмента «Системы управления бизнес-процессами» [Электронный источник]. – URL: http://journal.itmane.ru/node/820 (дата обращения 30.03.2021 г.).

154. Полковников А. В., Дубовик М. Ф., Песоцкая Е. Ю. Материалы к курсу «Управление рисками проекта». – М.: Ланит, 2001. – 105 с.

155. Ехлаков Ю. П. Классификация и описание рискообразующих факторов при создании программных продуктов // Управление, вычислительная техника и информатика. – 2013. - №3. – С. 124−128.

156. Волков И. В. Карта рисков российского медиабизнеса // Российской предпринимательство. – 2010. – №7(1). – С. 119-128.

157. Beer M., Wolf T., Garizy T. Z. Systemic risk in IT portfolios – An integrated quantification approach // 2015 international Conference on Information Systems: Exploring the Information Frontier. – 2015. – P. 1-18.

158. Barton T., Shenkir W., Walker P. Improving Board Risk Oversight. Through Best Practices. – Institute of Internal Auditors Research Foundation, 2011. – 81 p.

159. Чемоданова Ю. В., Макушева Ю. А., Сорокина К. В. Проблемы киберугроз в свете риска менеджмента и безопасности организации // Экономические исследования и разработки, 2019. – №5. – С.162-168.

160. Горшкова Л. А., Давыдова Д. М. Угрозы и условия устойчивого развития организации // Теория и практика общественного развития, 2015. – №16. – С.51-54.

161. Николаенко В.С. Разработка подходов классификации рисков в ИТ-проектах // Государственное управление. Электронный вестник. – 2017. – № 61. – С. 36-54.

162. Гага В. А., Козлова С. А., Тютюшев А. П., Ярославцева Е. Н. Российские системы распознавания и сопровождения лидера. – Томск: Изд-во Том. ун-та, 2011 – 196 с.

163. De Baker K., Boonstra A., Wortmann H. The Communicative Effect of Risk Identification on Project Success // Project Organisation and Management. – 2014. – Vol. 6. – No. ½. – P. 138−156.

164. De Bakker K. Dialogue on Risk. Effects of Project Risk Management on Project Success. – University of Groningen, 2011. – 222 p.

165. De Bakker K. Risk Management Planning – How Much is Good Enough? // Presented at the Fifth European Project Management Conference. – 2002. – P. 1−5.

166. De Bakker K., Boonstra A., Wortmann H. Does Risk Management Contribute to IT Project Success? A Mete-Analysis of Empirical Evidence // International of Project Management. – 2010. – P. 1−23.

167. Официальный сайт ООО «Аксимедия Софт». [Электронный ресурс]. – URL: https://clck.ru/Tz2vs (дата обращения 30.03.2021 г.).

168. Официальный сайт ООО «ЛидерГрупп» [Электронный ресурс]. – URL: http://www.lidermgrupp.ru/ (дата обращения 30.03.2021 г.).

169. Официальный сайт ООО «Синтез интеллектуальных систем». [Электронный ресурс]. – URL: http://ooosis.com/promo (дата обращения 30.03.2021 г.).

170. Официальный сайт ООО «Спейс-О технологии» [Электронный ресурс]. – URL: http://www.spaceotechnologies.com (дата обращения 30.03.2021 г.).

171. Официальный сайт ООО «Телебриз» [Электронный ресурс]. – URL: http://telebreeze.ru (дата обращения 30.03.2021 г.).

172. Официальный сайт ООО «Контек Софт» [Электронный ресурс]. – URL: http://www.contek.ru (дата обращения 30.03.2021 г.).

173. Официальный сайт ООО «Сибэйдж» [Электронный ресурс]. – URL: http://sibedge.com (дата обращения 30.03.2021 г.).

174. Полонский А. Ю., Васильев М. М. Анализ методологий разработки программного обеспечения // Аллея науки. – 2018. – Том 1. – № 6(22) – С. 1084-1094.

175. Balaji S., Sundararajan Murugaiyan M. Waterfall Vs V-Model Vs Agile: A Comparative on SDLC // International Journal of Information Technology and Business Management. – 2012. – Vol. 2. – No. 1. – P. 26−30.

176. Ching Gu V., Hoffman J. J., Cao Q., Schniederjans M.J. The effects of organizational culture and environmental pressures on IT project performance: A moderation perspective // International Journal of Project Management. – 2014. – No. 32. – P. 1170−1181.

177. Митяков Е. С., Митяков С. Н. Оценка рисков в задачах мониторинга угроз экономической безопасности // Труды НГТУ им. Р. Е. Алексеева. – 2018. – №1(120). – С.44-51.

178. Болкунова Ю. Н. Организация службы защиты информации в системе риск-менеджмента // Финансы и кредит. – 2012. – №16 (496). – С. 58-62.

179. Казарцева О. А., Бойко В. В. Особенности управления виртуальным предприятием: риск-менеджмент // Вестник Волгоградского государственного университета. Серия 9: Исследования молодых ученых. – 2013. – №11. – С. 217-220.

180. Альтшуллер Г. С. Алгоритм изобретения. – М.: Московский рабочий, 1973. – 296 с.

181. Альтшуллер Г. С. Найти идею. Введение в ТРИЗ – теорию решения изобретательских задач. – М. : Альпина Паблишер, 2015. – 402 с.

182. Орлов М. Основы классической ТРИЗ. – М. : СОЛОН-ПРЕСС, 2006. – 432 с.

183. Надеждин Н. Я. Уолт Дисней: Все это начато одной мышью. – М. : Майор: Осипенко, 2010. – 192 с.

184. De Bono E. Six thinking hats. – Little, Brown Book Group Limited, 1985. – 207 p.

185. Николаенко В.С. Негативные и позитивные риски в ИТ-проектах // Вестник Московского университета. Серия 21: Управление (государство и общество). – 2018 - №3. – С. 91-124.

186. Бьюзен Т. Научите себя думать. – Минск: Попурри, 2014. – 224 с.

187. Бьюзен Т. Супермышление. – Минск: Попурри, 2014. – 272 с.

188. Федоров К. П. Применение ТРИЗ для решения проблем лингвистики средствами информационных технологий // Современные тенденции развития науки и производства. Сборник материалов VII Международной научно-практической конференции. – 2017. – С. 31-34.

189. Селиховкин И. Управление ИТ-проектом. Эффективная система «с нуля» в любой организации. – СПб. 2010. – 90 с.

190. Селюков В.К., Гончаров С.Г. Управление рисками. Ипотечная сфера. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2001. – 360 с.

191. Николаенко В.С. Превентивный риск-менеджмент в ИТ-проектах // Государственное управление. Электронный вестник. – 2016. – № 55. – С. 76-96.

192. Демарко Т., Листер Т. Человеческий фактор: успешные проекты и команды. – СПб.: Символ-Плюс, 2009. – 256 с.

193. Демарко Т. Вальсируя с медведями: управление рисками в проектах по разработке программного обеспечения. – М.: Компания p.m.Office, 2005. – 196 с.

194. Йордон Э. Путь камикадзе. Как разработчику программного обеспечения выжить в безнадежном проекте. – М.: Лори, 2012. – 256 с.

195. Гостяева Ю. Ю., Щетинина Е. Д. Основные приемы риск-менеджмента при принятии управленческих решений // Социально-гуманитарные знания. – 2014. – №8. – С. 258-265.

196. Официальный сайт «RiskTrack» [Электронный ресурс]. – URL: http://www.risktrak.com (дата обращения 30.03.2021 г.).

197. Официальный сайт «OpenPlanProfessional» [Электронный ресурс]. – URL: http://openplanprofessional.com (дата обращения 30.03.2021 г.).

198. Официальный сайт «RiskRadar» [Электронный ресурс]. – URL: http://www.riskradarprogram.com (дата обращения 30.03.2021 г.)

199. Официальный сайт «Risk Register» [Электронный ресурс]. – URL: http://incom.com.au (дата обращения 30.03.2021 г.).

200. Официальный сайт «RiskGap» [Электронный ресурс]. – URL: http://riskgap.ru (дата обращения 30.03.2021 г.).

201. Брукс П. Метрики для управления ИТ-услугами. – М.: Альпина Бизнес Букс, 2008. – 283 с.

202. Никулина И. Е., Тарабановский А. А. «Мониторинг-анализ» и «мониторинг-критерий» в системе финансового планирования автономного образовательного учреждения высшего профессионального образования // Фундаментальные исследования. – 2009. – №5. – С. 140-141.

203. Сидоренко А., Демиденко Е. Как создать ценность для бизнеса от риск-менеджмента 2.0. – 47 с.

204. Кузнецов В. П. Специфика оценки эффективности инвестиций ИТ-компаний // На страже экономики. – 2017. – №1(1). – С. 26-34.

205. Официальный сайт АО «Интерфакс» [Электронный ресурс]. – URL: http://www.interfax.ru/ (дата обращения: 30.03.2021 г.).

206. Официальный сайт Арбитражного суда Томской области [Электронный ресурс]. – URL: https://tomsk.arbitr.ru/ (дата обращения: 30.03.2021 г.).

207. Официальный сайт Территориального органа Федеральной службы государственной статистики по Томской области [Электронный ресурс]. – URL: https://tmsk.gks.ru/ (дата обращения: 30.03.2021 г.).

208. Новицкий Н. И. Организация, планирование и управление производством. – М.: Финансы и статистика, 2007. – 576 с.

209. Павлов В., Хозяинов С. Производственно-финансовые риски предприятия // РИСК: Ресурсы. Информация. Снабжение. Конкуренция. − 2000. − №5-6. – С. 50−56.

210. Официальный сайт Федерального государственного унитарного предприятия «Главный межрегиональный центр обработки и распространения статистической информации Федеральной службы государственной статистики» [Электронный ресурс]. – URL: http://gmcgks.ru (дата обращения 30.03.2021 г.).

211. Макарова В. А. Анализ и оценка экономической эффективности риск-менеджмента // Эффективное антикризисное управление. – 2015. – № 3 (90). – С. 72-83.

212. Макарова В. А. Формирование системы риск-менеджмента на предприятии // Вестник Псковского государственного университета. Серия: Экономика. Право. Управление. – 2014. – №4. – С. 98-108.

213. Addison T., Vallabh S. Controlling Software Project Risks – an Empirical Study of Methods used by Experienced Project Managers // Proceedings of SAICSIT. – 2002. – P. 128−140.

214. Stevens K. J., Fowell S. Perspective on E-Business Software Project Risk // 7th Pacific Asia Conference on Information Systems. – 2003. – P. 95−107.

215. Sumner M. Risk factors in enterprise-wide/ERP projects // Journal of Information Technology. – 2000. − №15. – P. 317−327.

216. William Storage. Chief Science Officer [Электронный ресурс]. – URL: https://www.quora.com/profile/William-Storage (дата обращения: 30.03.2021 г.).

217. David Dunkelberger. Enterprise Risk Management [Part III]: 5 Examples of Positive Risk [Электронный ресурс]. – URL: https://www.ispartnersllc.com/blog/erm-5-examples-of-positive-risk/ (дата обращения: 30.03.2021 г.).

218. Carpenter M. T. The Risk-Wise Investor: How to Better Understand and Manage Risk. – Wiley, 2009. – 254 p.

219. Taylor Davidson. Owner (Neil Benton Arts & Entertainment), Risk Management, Insurance, Marketing [Электронный ресурс]. – URL: https://www.quora.com/profile/Taylor-Davidson-6 (дата обращения: 30.03.2021 г.).

220. What are examples of positive risk? Quora [Электронный ресурс]. – URL: https://www.quora.com/What-are-examples-of-positive-risk (дата обращения: 30.03.2021 г.).

221. Luckmann J. A. Positive risk management: hidden wealth in surface mining // Surface Mining 2014 Conference. – 2014. – P. 113–124.

222. Luckmann J. A. Positive risk management: hidden wealth in surface mining // The Journal of The Southem Africa Institute of Mining and Metallurgy. – 2015. – Vol. 115. – P. 1027-1034.

223. Hillson D. Effective Opportunity Management for Projects, Exploiting Positive Risk. – New York: Taylor & Francis, 2004. – 340 p.

224. Дмитриев И.О., Николаенко В.С. Лидерство, как позитивный риск, наступление которого необходимо для успешного завершения ИТ-проекта // Современные проблемы и тенденции развития экономики, управления и информатики в XXI веке. Сборник научных статей по материалам научно-практической конференции с международным участием. ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» под редакцией Шаминой Л.К., Шаш Н.Н., Соснило А.И., Соловьевой Е.О., Пузанова О.П., Креера М.Я., Чирковой М.Ю., Волокобинского М.Ю., Майоровой Е.Ю. – 2016 – С. 12-16.

225. Бетенекова Н. В., Николаенко В. С. Обобщение структуры проектной документации // Государство и бизнес. Современные проблемы экономики. Информационный издательский учебно-научный центр «Стратегия будущего». – 2017. – С. 224-228.

226. Бетенекова Н. В., Николаенко В. С. Уточнение терминологической базы, используемой в проектной деятельности // Развитие методологии современной экономической науки и менеджмента. Материалы I Междисциплинарной Всероссийской научно-практической конференции. Севастополь. – 2017. – С. 227-232.

227. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2020. – 19 с.

ПРИЛОЖЕНИЕ А. Опросный лист

Вопросы, задаваемые экспертам в процессе выявления негативных рисков:

1. Будут сомнения в успешном завершении проекта?
2. Будут нечетко сформулированы цели проекта (не по S.M.A.R.T.)?
3. Руководитель будет не заинтересован в успешном завершении проекта?
4. Будет отсутствовать план-график проекта?
5. В проекте будет отсутствовать техническое задание?
6. Будет отсутствовать общее виденье конечного продукта у участников проекта?
7. Будет отсутствовать устав проекта?
8. Будет отсутствовать спецификация проекта?
9. По факту проект заказчика будет значительно сложнее, чем предполагалось изначально (на понимание бизнес-процессов заказчика уйдет «колоссальное» количество времени)?
10. В проекте будут выявлены скрытые, т.е. не обнаруженные на этапе планирования источники дополнительных затрат?
11. Руководитель завысит требования, предъявляемые к качеству проекта? (Перфекционизм Стива Джобса в проекте «Apple Liza»)
12. Изменятся требования в процессе реализации проекта?
13. Разработанный продукт не будет пользоваться спросом у конечного потребителя?
14. Будет отставание от запланированных сроков?
15. Полученные результаты будут не соответствовать изначальным требованиям?
16. Разработанный продукт не будет соответствовать требованиям, которые описаны в уставе проекта, спецификации проекта и техническом задании?

17. Заявленные требования невозможно будет реализовать?

18. Руководитель сделает ошибочную оценку сроков, необходимых для реализации проекта?

19. Руководитель сделает ошибочную оценку человеческих ресурсов, необходимых для реализации проекта?

20. У руководителя проекта не будет хватать знаний и навыков, необходимых для реализации требований проекта?

21. Из проекта может уйти руководитель?

22. Разработанный продукт будет низкого качества?

23. Заказчик откажется от полной (частичной) предоплаты?

24. Заказчик не сможет оплатить трудозатраты проектной команды, работающей по системе оплаты T&M?

25. Заказчик будет не удовлетворен работой участников проекта?

26. Заказчик будет не удовлетворен работой руководителя проекта?

27. В проекте будет отсутствовать финансирование?

28. Заказчик будет не удовлетворен качеством разработанного продукта?

29. Заказчик будет не удовлетворен сроками реализации проекта?

30. Заказчик будет не удовлетворен содержанием разработанного продукта?

31. Руководитель будет занят на других проектах?

32. Участники проектной команды будут заняты на других проектах?

33. Будут не учтены отпуска и государственные праздники при создании план-графика проекта?

34. В проекте будет использоваться классический способ реализации проекта (*agile, waterfall* и др.)?

35. В проекте будет задержка в выплатах заработной платы?

36. Фактическое «чистое» время работы сотрудника будет менее 8 часов в день (рабочее время расходуется на социальные сети, YouTube и др.)?

37. У команды проекта будет не хватать знаний и навыков, необходимых для реализации требований проекта?

38. Проектной команде будет непонятно, какой продукт должен получиться по завершении проекта?

39. Проектная команда будет не заинтересована в успешном завершении проекта?

40. Кто-то будет умышленно вредить проекту?

41. Будет низкая производительность проектной команды?

42. Участники проектной команды будут иметь низкую мотивацию?

43. Участники проектной команды могут заболеть?

44. У участников проекта могут быть форс-мажорные обстоятельства?

45. Из проекта могут уйти ключевые сотрудники?

46. Будет перегрузка людских ресурсов (переработка, работа сверхурочно и т. п.)?

47. Будет низкая загрузка человеческих ресурсов?

48. В процессе реализации проекта может измениться состав участников проектной команды?

49. Будет негативная социально-психологическая атмосфера внутри проектной команды?

50. Будут не скоординированы действия проектной команды?

51. Проектная команда будет допускать ошибки при реализации проекта *(bugs)*?

52. Субподрядчики могут вовремя не завершить работу?

53. Субподрядчики могут не выйти на связь?

54. Предоставляемый субподрядчиками сервис будет низкого качества?

55. Заказчик может не выйти на связь?

56. Проектной команде будет не доступна актуальная информация, необходимая для реализации проекта?

57. Будет переизбыток каналов коммуникаций, доносящих актуальную информацию?

58. Будет недостаток коммуникаций между участниками проекта?

59. Будет большая временная задержка в получении ответов на задаваемые вопросы между участниками проекта?

60. Будет большая временная задержка в получении ответов на задаваемые заказчику проекта вопросы?

61. Будут использоваться устаревшие технологии?

62. Будет поломка оборудования?

63. Будет неэффективно использоваться инструментарий управления проектами (диаграмма Ганта, Microsoft Project 2010 и др.)?

64. В проекте будут применяться ранее не используемые технологии?

65. Будет отключение электричества?

66. Будет отключение интернета?

67. Будут использоваться чужие авторские права?

68. Будут допущены ошибки при составлении договора, заказа и т. п. (с заказчиками, субподрядчиками и др.)?

69. Будет промышленный шпионаж?

70. Будет ограбление офиса?

71. Будет утечка конфиденциальных данных?

72. От заказчика может быть судебный иск?

73. От субподрядчика может быть судебный иск?

74. Проект может пострадать от действий конкурентов?

75. На проект могут оказать негативное влияние геополитические факторы, например, такие как политика, география, демография, экономика и т. п.?

76. На проект могут оказать негативное влияние стихийные бедствия, например, такие как пожар, наводнение, ураган и т. п.?

77. Будут изменения в налоговом законодательстве?

78. Будут штрафы со стороны фискальных органов государства?
79. Будет изменение валютного курса?

ПРИЛОЖЕНИЕ Б. Объекты исследования

Описание деятельности ИТ-организаций и характеристика исследуемых ИТ-проектов

ООО «Синтез Интеллектуальных Систем» (SIS).

ООО «Синтез Интеллектуальных Систем» специализируется на разработке веб-сайтов и мобильных приложений, работающих на платформах *Android* и *iSO*. В перечень выполняемых работ организации входят работы по созданию программных продуктов на ИТ-платформе Битрикс 24. Для внедрения разработанного автором диссертационного исследования инструментария управления рисками, специалистами ООО «Синтез Интеллектуальных Систем» был выбран проект «Сайт ТГУ». Количество участников проекта составило 6 человек, в число которых входили руководитель проекта, дизайнер, старший разработчик *(Senior Developer)* и 3 разработчика *(Middle Developers)*.

ООО «Лидер Групп».

В портфолио веб-студии ООО «Лидер Групп» входит более 100 успешно реализованных проектов, связанных с разработкой CRM-систем, ERP-систем, CMS-систем, мобильных приложений, сайтов и т. п. Апробация разработанного автором диссертационного исследования инструментария управления рисками проходила в ИТ-проекте «МирКар». Целью ИТ-проекта «МирКар» являлось создание и запуск корпоративного сайта для сети автомоек. В состав проектной команды входили руководитель проекта, дизайнер и 2 разработчика *(Middle Developers)*. Необходимо отметить, что разработка сайта являлась стандартной задачей для команды ООО «Лидер Групп», т. е. в ИТ-организации имелись шаблоны дизайна и программного кода.

ООО «Спейс-О Технологии» (Space-O Technologies).

Перечень оказываемых услуг и подрядных работ международного центра автоматизации ООО «Спейс-О Технологии» включает в себя дизайн, разработку мобильных приложений, сайтов и программного обеспечения для автоматизации бизнес-процессов. Специалистами ООО «Спейс-О Технологии» были выбраны 2 ИТ-проекта «HyperVibe» и «ReadingLog», для которых было решено провести внедрение разработанного автором диссертационного исследования инструментария управления рисками. Оба ИТ-проекта были связаны с разработкой ПО для автоматизации автономных устройств. В состав ИТ-проекта «HyperVibe» вошли 6 сотрудников – руководитель проекта, дизайнер, 3 разработчика *(Middle Developers)*, специалист, ответственный за тестирование программного кода. В состав ИТ-проекта «ReadingLog» вошли руководитель проекта, 3 разработчика *(Middle Developers)*. Одним из обязательных условий заказчика была работа по системе оплаты *Fixed Price*, где бюджет ИТ-проекта утверждается на этапе планирования.

ООО «Аксимедиа Софт» (Aximedia Soft).

Специализация компании ООО «Аксимедиа Софт» – это разработка мобильных приложений для Android и iOS. Помимо разработки программ для мобильных устройств ООО «Аксимедиа Софт» принимает заказы на разработку веб-серсисов. С 2010 года было реализовано более 50 успешно завершенных ИТ-проектов, связанных со сферами телекоммуникаций, ритейла, медицины и автотранспорта. В 2015 году ООО «Аксимедиа Софт» вошла в ТОП-100 лучших мобильных разработчиков в рейтинге Tagline.

История становления компании началась с реализации онлайн-сервиса по обработке видео и аудиофайлов. Данный проект победил в конкурсе «СТАРТ» Фонда Бортника, получил 1 млн. руб. По завершении проекта на рынок было выпущено мобильное приложение «Slide Show Creator» для

создания слайд-шоу из фотографий и музыки. За 3 года приложение набрало более 3 миллионов скачиваний.

Для внедрения разработанного автором диссертационного исследования инструментария управления рисками, специалистами ООО «Аксимедиа Софт» был выбран ИТ-проект по разработке мобильного приложения «CINEMOOD». Пользователем данного приложения являются дети, пользующиеся пико-проекторами «МУЛЬТиКУБИК». ИТ-проект включал в себя разработку мобильного приложения для пико-проектора и мобильное приложение для дистанционного управления. В проекте использовались технологии *Java* и *Android SDK*. В состав ИТ-проекта вошли: руководитель проекта, дизайнер, аналитик, 3 разработчика *(Middle Developers)* и специалист, ответственный за тестирование программного кода.

ООО «Контек Софт» (Contek Soft).

Основными направлениями деятельности компании ООО «Контек Софт» являются разработка ИТ-решений:

- для управления научной деятельностью, дополнительным образованием и интеллектуальной собственностью для вузов и научно-промышленных предприятий;
- для информационной безопасности. В данной сфере специалистами ООО «Контек Софт» реализовано более 30 проектов.

Для внедрения разработанного автором диссертационного исследования инструментария управления рисками, специалистами ООО «Контек Софт» были выбраны ИТ-проекты «Расчет и учет заработной платы в научно-технических учреждениях» («РЗП»), «Портал логистики», «Торговая площадка», «Регламентация ведения номенклатуры ТМЦ» («ТМЦ»).

Пользователями ИТ-проекта «РЗП» являлись высшие учебные заведения и научно-технические организации. В состав проектной команды

входило 9 человек: руководитель проекта; аналитик; дизайнер; старший разработчик *(Senior Developer)*; 4 разработчика *(Middle Developers)*; специалист, ответственный за тестирование программного кода. Запланированная длительность составила 294 дня. Для реализации проекта использовалась итеративная разработка. Необходимо отметить, что при итеративной разработке чаще всего используют систему оплаты *Time & Material*, где бюджет проекта формируется в зависимости от количества затраченного времени и ресурсов в процессе реализации проекта. Однако для данного проекта была использована система оплаты *Fixed Price*. Это связано с тем, что заказчиком данного проекта выступало государственное учреждение.

ИТ-проект «Портал логистики» реализовывался посредством *agile*, используя систему оплаты *Time & Material*. В состав проектной команды входило 6 сотрудников, в частности руководитель проекта, аналитик, дизайнер, старший разработчик *(Senior Developer)* и специалист, ответственный за тестирование программного кода.

ИТ-проект «Торговая площадка» реализовывался посредством *agile* и оплачивался по *Time & Material*. В состав проекта входили руководитель проекта, аналитик, дизайнер, старший разработчик *(Senior Developer)*, 2 разработчика *(Middle Developers)* и специалист, ответственный за тестирование программного кода.

Для реализации ИТ-проекта «ТМЦ» применялся *agile*, но т. к. заказчиком являлось государственное учреждение, бюджет проекта формировался по системе *Fixed Price*. В число участников проектной команды входили руководитель проекта, старший разработчик *(Senior Developer)*, 2 разработчика *(Middle Developers)*, специалист, ответственный за тестирование программного кода.

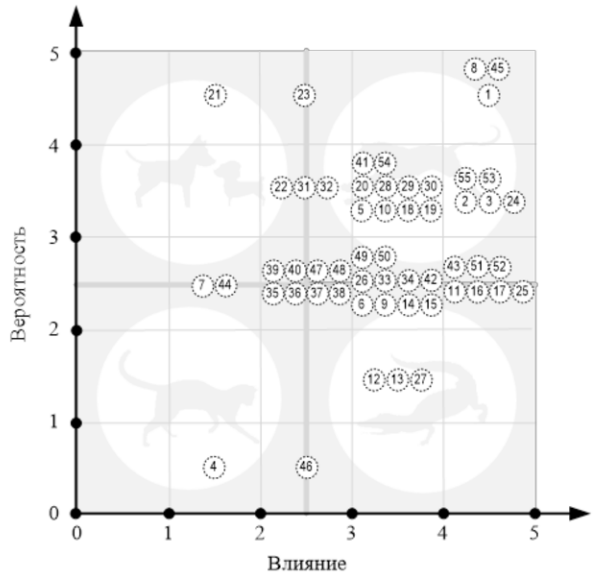
ООО «Телебриз» (Telebreeze).

Международная организация ООО «Телебриз» была основана в 2011 году. Штат сотрудников на момент внедрения риск-менеджмента составлял 19 человек. ООО «Телебриз» специализируется на разработке и реализации программных продуктов для IPTV/OTT. Для внедрения разработанного автором диссертационного исследования инструментария управления рисками, специалистами ООО «Телебриз» был выбран внутренний проект компании «DigitalTV». Для реализации проекта были привлечены 10 сотрудников, руководитель проекта, старший разработчик *(Senior Developer)*, 7 разработчиков *(Middle Developers)* и специалист, ответственный за тестирование программного кода.

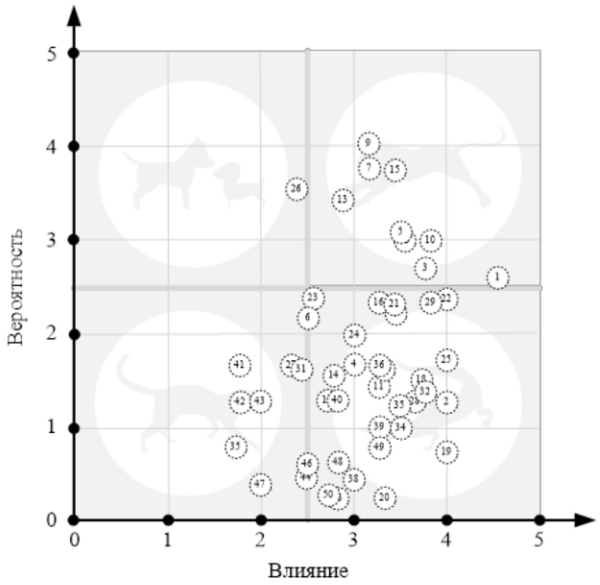
ООО «Сибэйдж» (SibEDGE).

Специализацией ООО «Сибэйдж» является разработка и реализация CRM-систем, ERP-систем, CMS-систем для нефтегазового комплекса, а также разработка портальных решений и реализация собственных продуктов, таких как «Система управления инженерными проектами» и «Система управления рабочим временем». Для внедрения разработанного автором диссертационного исследования инструментария управления рисками, специалистами ООО «Сибэйдж» был выбран ИТ-проект «EAM-система». Целью данного проекта являлась оптимизация управления физическими активами и режимами их работы. В состав проектной команды вошли: руководитель проекта; аналитик; 2 старших разработчика *(Senior Developers)*; 3 разработчика *(Middle Developers)*; специалист, ответственный за тестирование программного кода.

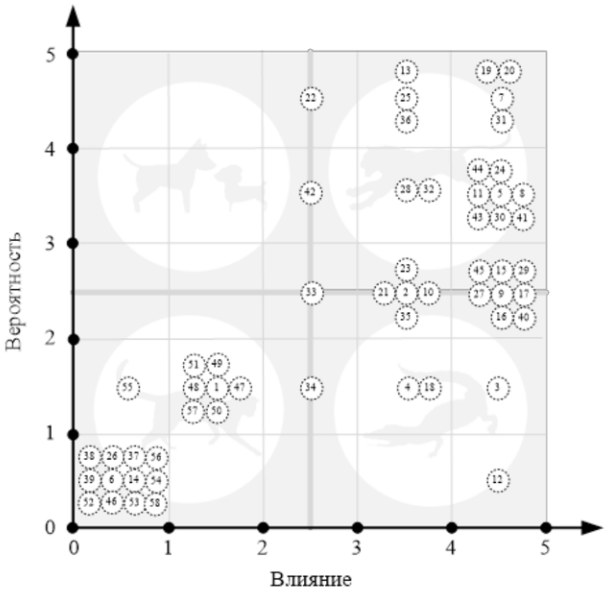
ПРИЛОЖЕНИЕ В. Матрицы вероятностей/влияния негативных рисков



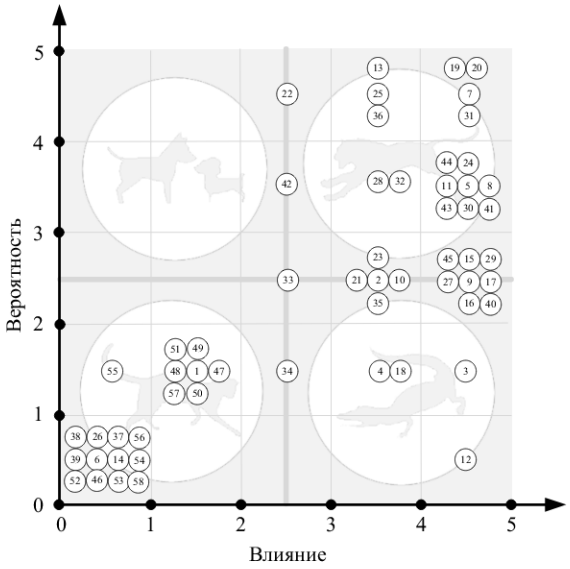
а)



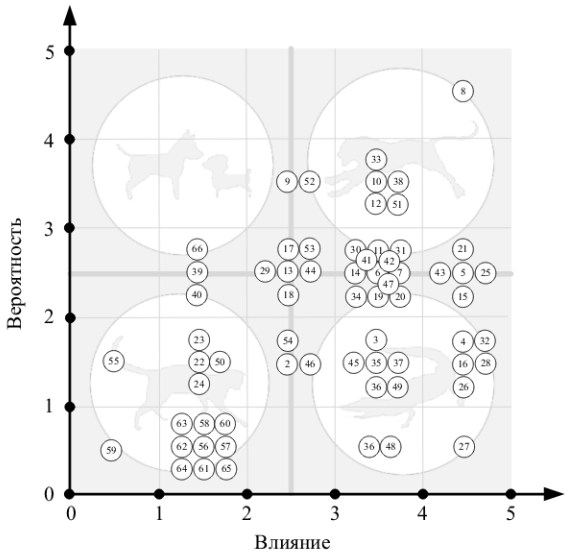
б)



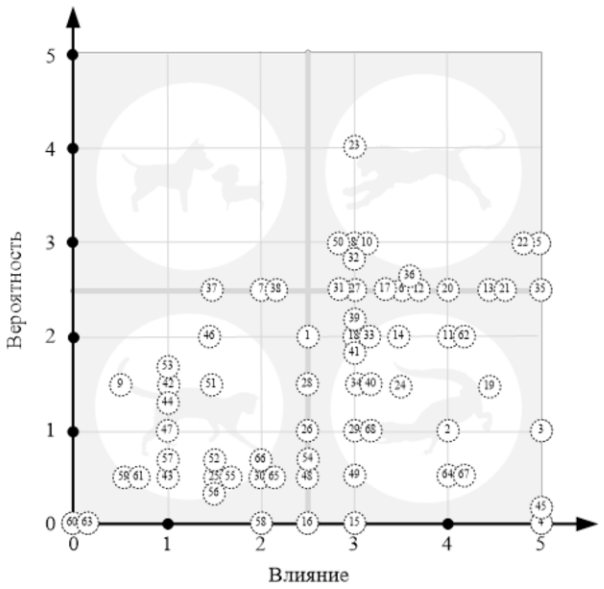
в)



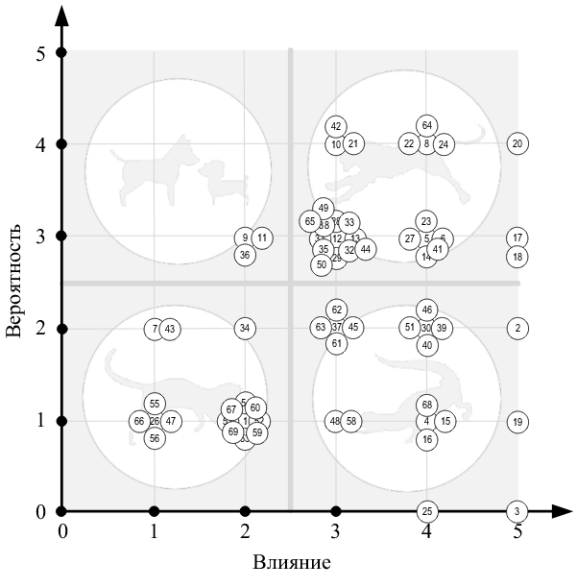
г)


Вероятность
Влияние

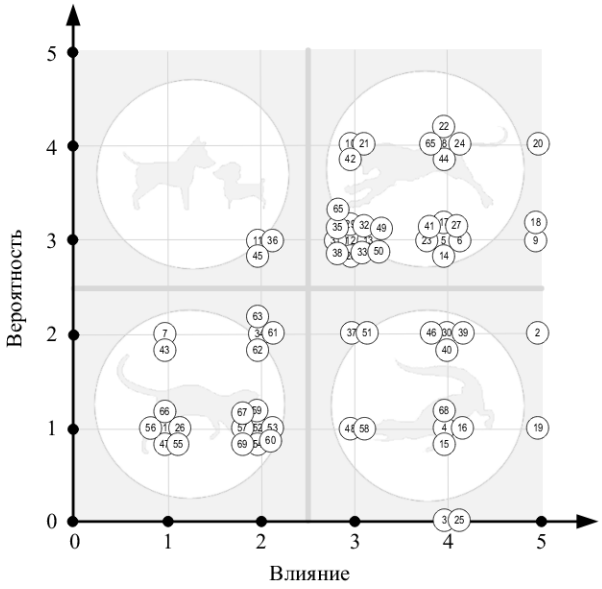
д)


Вероятность
Влияние

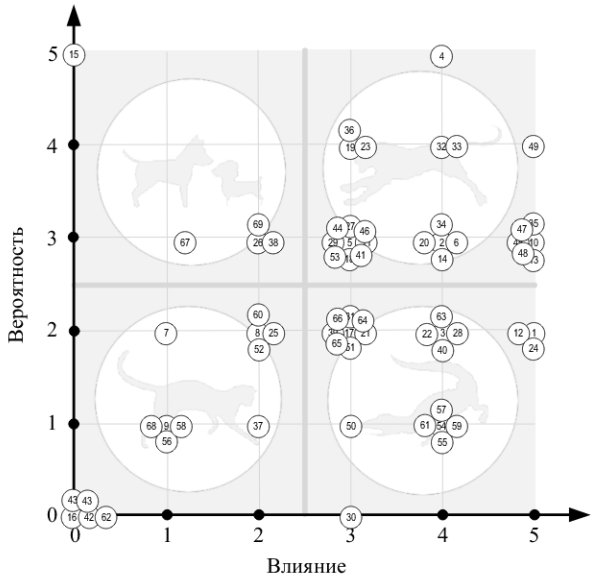
е)


Вероятность
Влияние

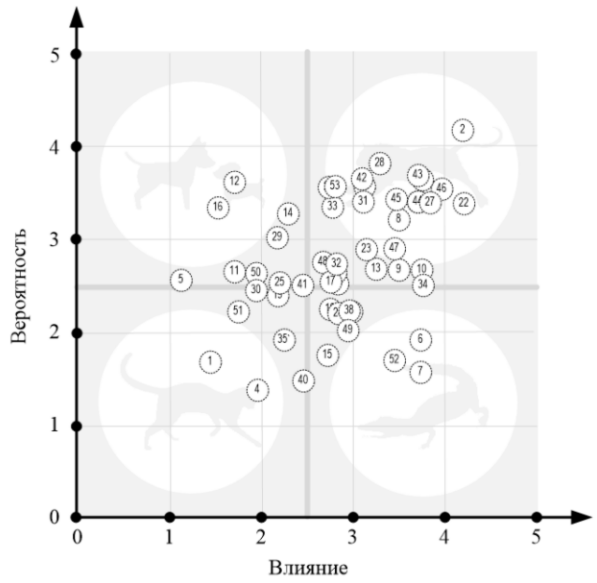
ж)


Вероятность
Влияние

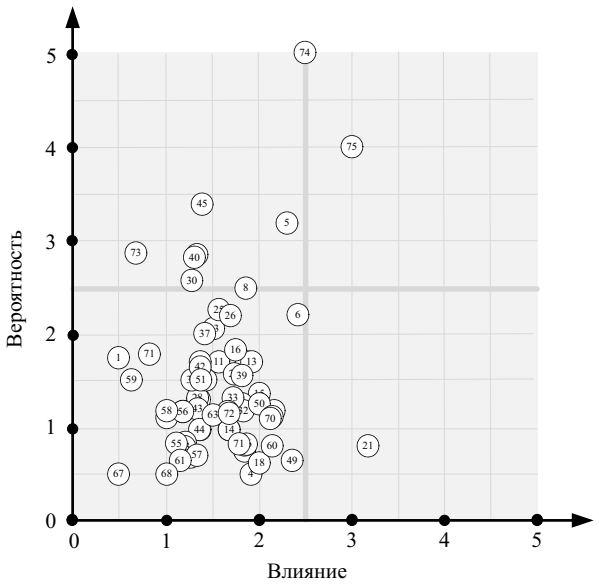
з)


Вероятность
Влияние

и)


Вероятность
Влияние

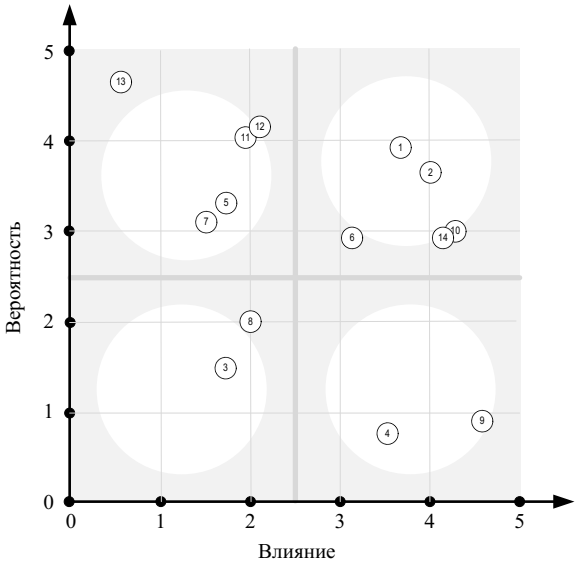
к)



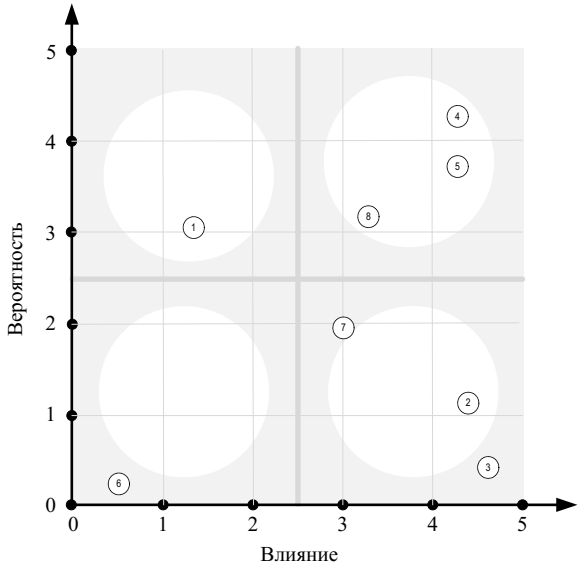
л)

Рисунок. Матрицы вероятностей и влияния негативных рисков: а) «Сайт ТГУ»; б) «МирКар»; в) «HyperVibe»; г) «Reading Log»; д) «CINEMOOD»; е) «РЗП»»; ж) «Портал логистики»; з) «Торговая площадка»; и) «ТМЦ»; к) «DigitalTV»; л) «ERM-система»

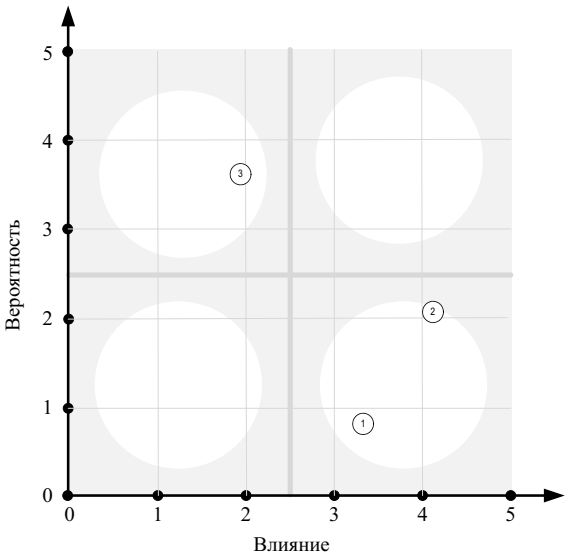
ПРИЛОЖЕНИЕ Г. Матрицы вероятностей/влияния позитивных рисков



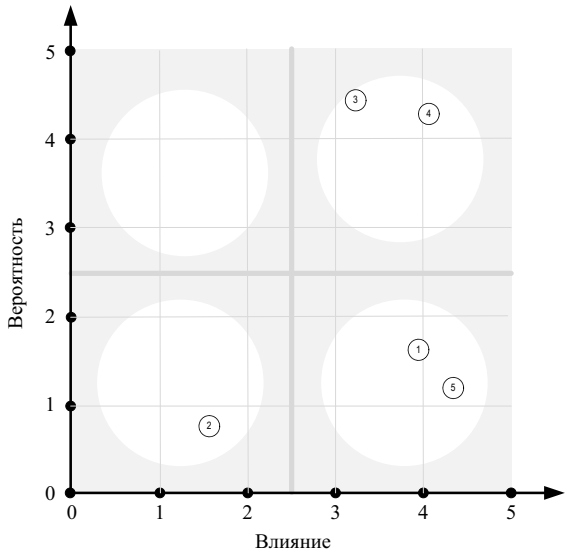
а)



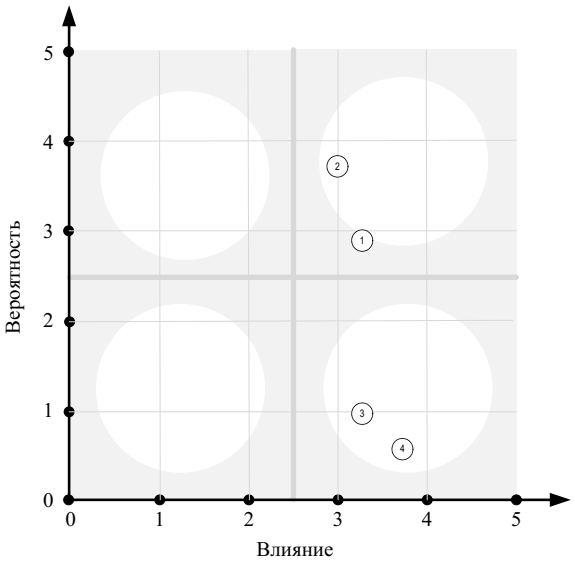
б)



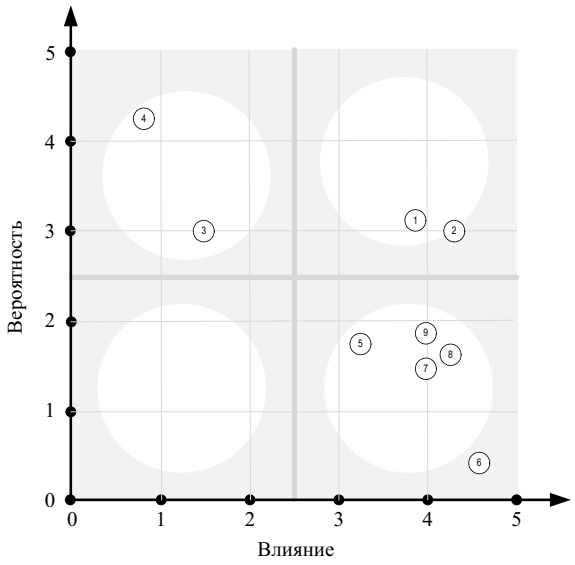
в)



г)



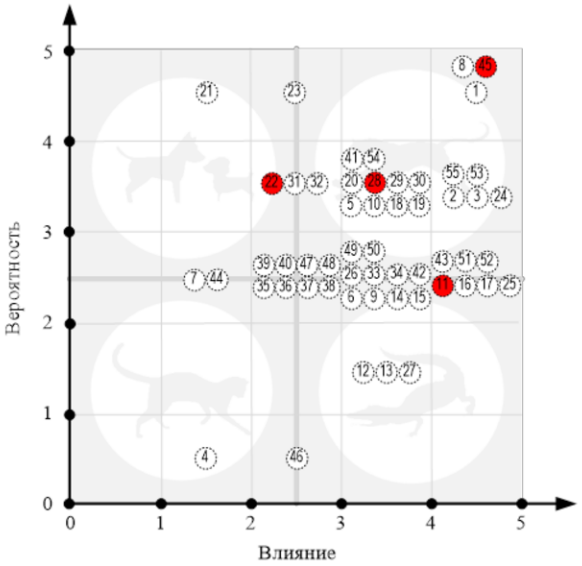
д)



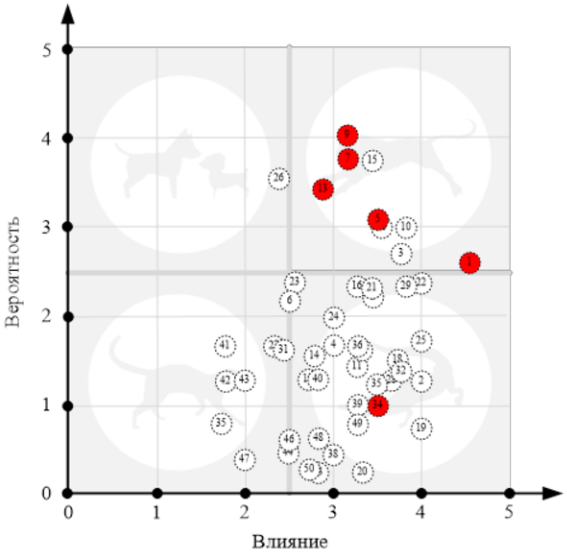
е)

Рисунок. Матрицы вероятностей и влияния позитивных рисков: а) «Сайт ТГУ»; б) «РЗП»»; в) «Портал логистики»; г) «Торговая площадка»; д) «ТМЦ»; е) «ERM-система»

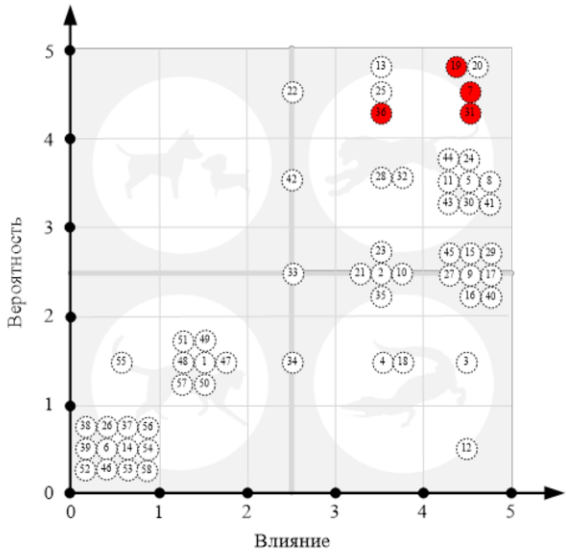
ПРИЛОЖЕНИЕ Д. Матрицы вероятностей/влияния наступивших негативных рисков



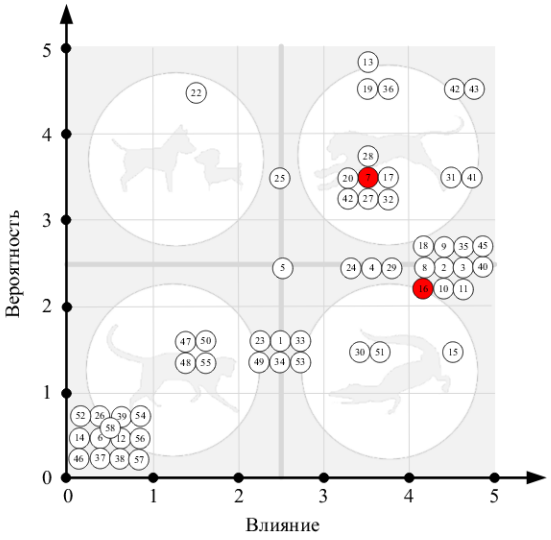
а)



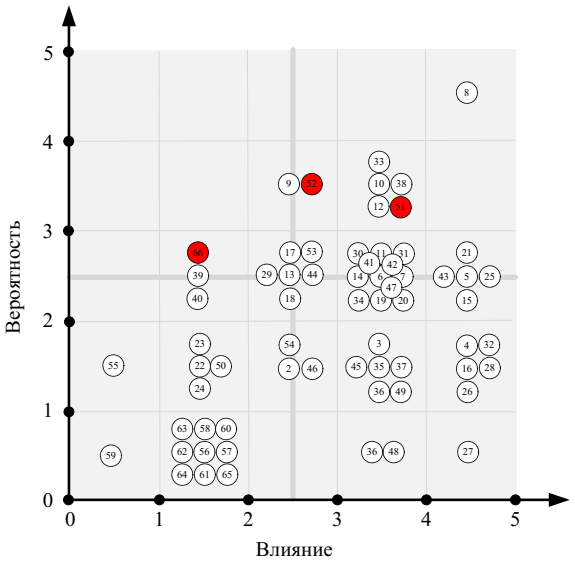
б)



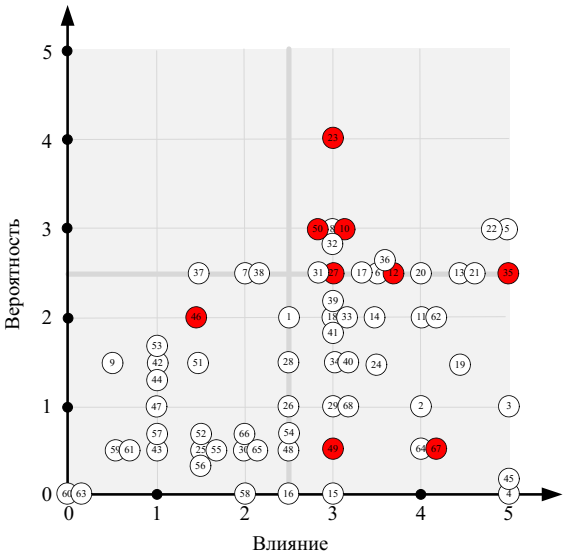
в)



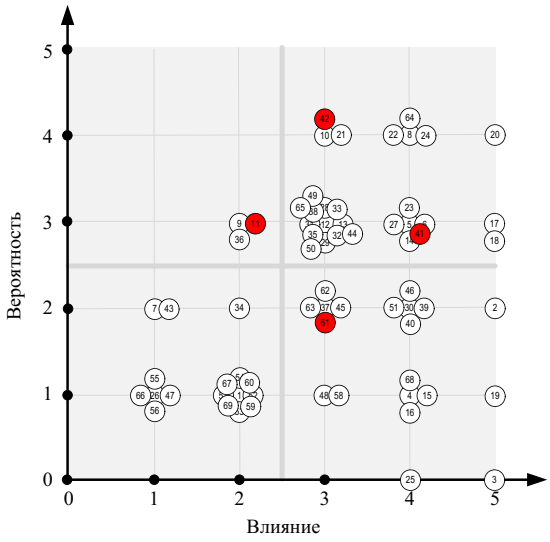
г)


Вероятность
Влияние

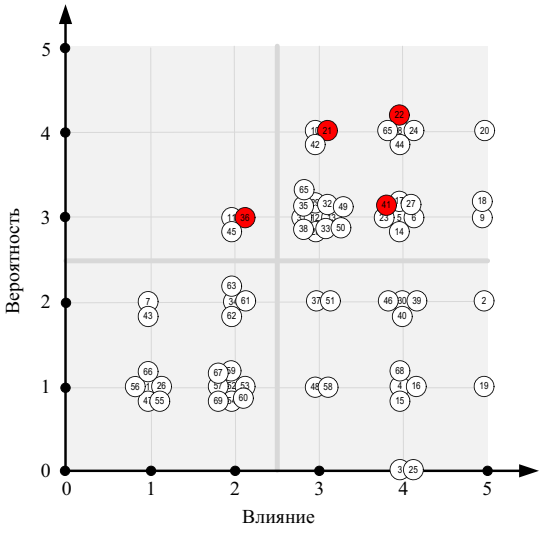
д)


Вероятность
Влияние

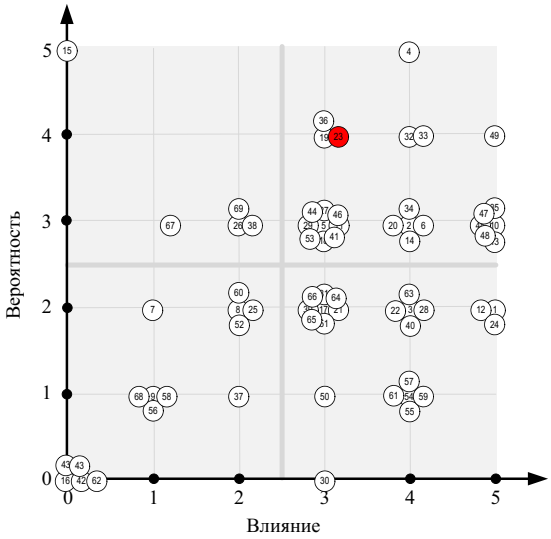
е)


Вероятность
Влияние

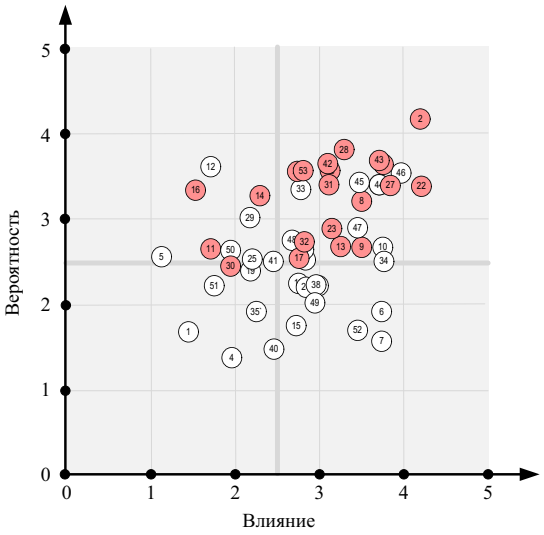
ж)


Вероятность
Влияние

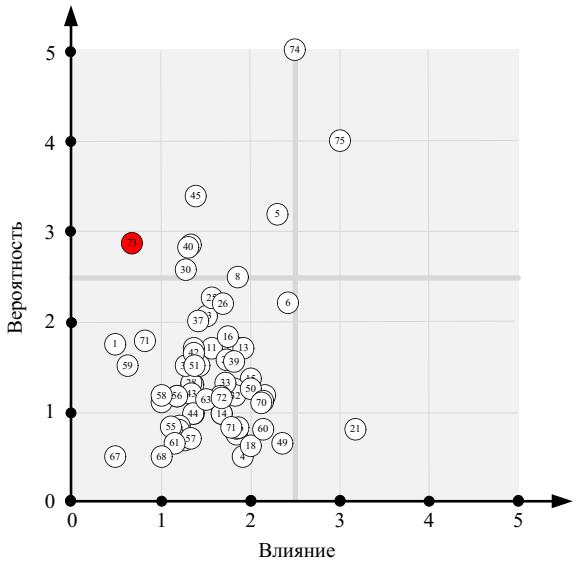
з)


Вероятность
Влияние

и)


Вероятность
Влияние

к)



л)

Рисунок. Матрицы вероятностей и влияния наступивших негативных рисков: а) «Сайт ТГУ»; б) «МирКар»; в) «HyperVibe»; г) «Reading Log»; д) «CINEMOOD»; е) «РЗП»; ж) «Портал логистики»; з) «Торговая площадка»; и) «ТМЦ»; к) «DigitalTV»; л) «ERM-система»

ПРИЛОЖЕНИЕ Е. Справки об использовании результатов диссертационного исследования

ООО "ЛидерГрупп"

125466, г. Москва, ул. Юровская, д. 92, офис 1
634009, г. Томск, пер. Совпартшкольный, 13, офис 407
8 (495) 922-3072, +7 (3822) 30-30-82, develop@luny.ru

СПРАВКА

об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ИТ-проекте «МирКар», разрабатываемый компанией ООО «Лидер Групп»

Компания ООО «Лидер Групп» работает в сфере информационных технологий, предлагая высокотехнологичные решения для крупного и среднего бизнеса. В портфолио ООО «Лидер Групп» входит свыше двухсот успешно завершенных ИТ-проектов связанных с CRM, ERP, CMS, мобильными приложениями, адаптивными сайтами и т.п.

Предложенное в диссертационном исследовании Николаенко В.С. методическое обеспечение по внедрению риск-менеджмента в ИТ-проект было использовано ООО «Лидер Групп» на этапе планирования и составления план-графика работ для проекта «МирКар». Целью внедрения риск-менеджмента являлось повышение степени управляемости и увеличение вероятности успешного завершения проекта «МирКар».

Специалистами ООО «Лидер Групп» отмечается, что внедрение риск-менеджмента в проект «МирКар» ослабило влияние и уменьшило вероятность наступления негативных «катастрофических» рисковых событий, а также способствовало формированию культуры управления рисками в компании.

Генеральный директор ООО «Лидер Групп» Славнин Д.Э.
Менеджер проекта «МирКар»

14 сентября 2015 г.

.sis СИНТЕЗ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ
ГОРОД ТОМСК
+7 (3822) 78-90-76
INFO@OOOSIS.COM
HTTP://OOOSIS.COM

СПРАВКА

об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ООО «СИС» по внедрению системы управления рисками для ИТ-проекта
«Сайт Томского государственного университета»

Организация ООО «СИС» (Синтез интеллектуальных систем) работает в сфере информационных технологий, оказывает услуги по созданию, внедрению, развитию различных по сложности информационных систем, в частности осуществляет разработку и внедрение индивидуальных автоматизированных систем управления и их отдельных компонентов (модулей).

Предложенная в диссертационном исследовании Николаенко В.С. система управления рисками для проектов, разрабатываемых в сфере информационных технологий была использована ООО «СИС» на этапе планирования и составления план-графика работ для проекта «Сайт Томского государственного университета», сокращенно «Сайт ТГУ». Целью внедрения являлось повышение степени управляемости и увеличение вероятности успешного завершения проекта.

Специалистами ООО «СИС» отмечается, что внедрение системы управления рисками в проект «Сайт Томного государственного университета» способствовало: ликвидации, ослаблению и нивелированию негативных «катастрофических», «часто встречаемых» и «непредсказуемых» рисков; реализации позитивных рисков, оказавших благоприятное влияние на успешное завершение проекта; формированию культуры управления рисками в организации.

Генеральный директор ООО «СИС» Манжетов И.
Менеджер проекта «Сайт ТГУ» Нестерович Р.

18 февраля 2015 г.

SPACE TECHNOLOGIES

Общество с ограниченной ответственностью "Спейс-О Технологии"
ИНН 7017330063 КПП 701701001
634029, Россия, Томская область, г. Томск, пр. Фрунзе, д.25
+7 (3822) 22-89-90

Исх. № 85
От «18» НОЯБРЯ 2015 г.

СПРАВКА
об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ИТ-проектах, разрабатываемых центром автоматизации
ООО «Спейс-О Технологии»

Компания ООО «Спейс-О Технологии» работает в сфере информационных технологий, предлагая высокотехнологичные решения для крупного и среднего бизнеса. В портфолио ООО «Спейс-О Технологии» входит свыше двухсот успешно завершенных ИТ-проектов связанных с CRM, ERP, CMS, мобильными приложениями, адаптивными сайтами и т.п.

Предложенное в диссертационном исследовании Николаенко В.С. методическое обеспечение было внедрено в организацию ООО «Спейс-О Технологии». По итогам внедрения специалистами ООО «Спейс-О Технологии» было принято решение по дальнейшему использованию данного методического обеспечения в остальных ИТ-проектах. Отметим, что целью внедрения риск-менеджмента являлось повышение степени управляемости и увеличение вероятности успешного завершения ИТ-проектов в организации ООО «Спейс-О Технологии».

Специалистами ООО «Спейс-О Технологии» отмечается, что внедрение риск-менеджмента в ИТ-проекты ослабило влияние и уменьшило вероятность наступления негативных «катастрофических» рисковых событий, а также способствовало формированию культуры управления рисками в организации.

Генеральный директор ООО «Спейс-О Технологии» Ерин Е.А.

Менеджер проектов ООО «Спейс-О Технологии» Шахтин А.А.

17 ноября 2015 г.

«Спейс-О Технологии»

Aximedia

Общество с ограниченной ответственностью «Аксимедиа Софт»

Юр. адрес: 634021, г. Томск, улица Герцена, 74/2
ИНН 7017267855 КПП 701701001 ОГРН 1107017014862
Р/с 40702810006290004813 в ПАО «Томскпромстройбанк»
К/с 30101810500000000728 БИК 046902728
www.aximediasoft.com

СПРАВКА
об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ИТ-проекте «Cinemood», разрабатываемого
ООО «Аксимедиа Софт»

Компания ООО «Аксимедиа Софт» работает в сфере информационных технологий свыше 5 лет, разрабатывая мобильные предложения для Android, iPhone и iPad. В портфолио «Аксимедиа Софт» входит свыше тридцати успешно завершенных проектов.

Предложенное в диссертационном исследовании Николаенко В.С. методическое обеспечение было внедрено в проект «Cinemood». По итогам внедрения специалистами ООО «Аксимедиа Софт» было принято решение по дальнейшему использованию данного методического обеспечения в остальных ИТ-проектах. Отметим, что целью внедрения риск-менеджмента являлось повышение степени управляемости и увеличение вероятности успешного завершения ИТ-проектов в организации ООО «Аксимедиа Софт».

Специалистами ООО «Аксимедиа Софт» отмечается, что внедрение риск-менеджмента в ИТ-проект «Cinemod» ослабило влияние и уменьшило вероятность наступления негативных «катастрофических» рисковых событий, а также способствовало формированию культуры управления рисками в организации.

Генеральный директор ООО «Аксимедиа Софт»

Сапунков Глеб Геннадьевич _____

Менеджер проектов ООО «Аксимедиа Софт»

Ветошкин Илья Сергеевич _____

01 февраля 2016 г.

TELEBREEZE

СПРАВКА

об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ИТ-организации «Телебриз»

Компания «Телебриз» работает в сфере информационных технологий, устанавливает оборудование для IP телевиденья, принимает и кодирует сигналы со спутников, доставляет контент по конечных пользователей, обеспечивает техническую поддержку.

Предложенное в диссертационном исследовании Николаенко В.С. методическое обеспечение было внедрено в организацию «Телебриз». По итогам внедрения специалистами «Телебриз» было принято решение по дальнейшему использованию данного методического обеспечения в остальных ИТ-проектах. Отметим, что целью внедрения риск-менеджмента являлось повышение степени управляемости и увеличение вероятности успешного завершения проектов в организации «Телебриз».

Специалистами «Телебриз» отмечается, что внедрение риск-менеджмента ослабило влияние и уменьшило вероятность наступления негативных «катастрофических» рисковых событий, а также способствовало формированию культуры управления рисками в организации.

Генеральный директор «Телебриз» Песегов Николай Сергеевич
Менеджер проектов «Телебриз» Песегов Николай Сергеевич
01 февраля 2016 г.

contek
SOFT

ООО «Контек-Софт»
Россия, 634055, г. Томск, Развития пр., д. 3,
тел.: (3822) 701-404, факс: 701-403
e-mail: info@contek.ru, http://www.contek.ru
ИНН/КПП 7017065538//701701001
ОГРН 1037000099245

Справка

об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ИТ-проекты «Портал логистики», «Торговая площадка», «Регламентация ведения номенклатуры ТМЦ», «Расчет и учет заработной платы в научно-образовательных учреждениях», разрабатываемый компанией ООО «Котек-Софт»

Компания ООО «Котек-Софт» работает в сфере информационных технологий, предлагая высокотехнологичные решения для крупного и среднего бизнеса. В портфолио ООО «Котек-Софт» входит свыше двухсот успешно завершенных ИТ-проектов связанных с CRM, ERP, CMS, мобильными приложениями, адаптивными сайтами и т.п.

Предложенное в диссертационном исследовании Николаенко В.С. методическое обеспечение по внедрению риск-менеджмента в ИТ-проект было использовано ООО «Контек-Софт» на этапе планирования и составления план-графиков работ для проектов «Портал логистики», «Торговая площадка», «Регламентация ведения номенклатуры ТМЦ», «Расчет и учет заработной платы в научно-образовательных учреждениях». Целью внедрения риск-менеджмента являлось повышение степени управляемости и увеличение вероятности успешного завершения проектов «Портал логистики», «Торговая площадка», «Регламентация ведения номенклатуры ТМЦ», «Расчет и учет заработной платы в научно-образовательных учреждениях».

Специалистами ООО «Котен-Софт» отмечается, что внедрение риск-менеджмента в проекты «Портал логистики», «Торговая площадка», «Регламентация ведения номенклатуры ТМЦ», «Расчет и учет заработной платы в научно-образовательных учреждениях» ослабило влияние и уменьшило вероятность наступления негативных «катастрофических» рисковых событий, а также способствовало формированию культуры управления рисками в компании.

Генеральный директор ООО «Котек-Софт» Соснин В.Н.

Менеджер проекта «Портал логистики» Корнев Д.Н.

Менеджер проекта «Торговая площадка» Корнев Д.Н.

Менеджер проекта «Регламентация ведения номенклатуры ТМЦ» Сыродой В.В.

Менеджер проекта «Расчет и учет заработной платы в научно-образовательных учреждениях» Распопов В.В.

SibEDGE

ООО «Сибэдж», LLC «SibEDGE»
634006, Томск, ул. Пушкина, 75
тел: (3822) 701 841
www.sibedge.com
contacts@sibedge.com

ОГРН 1127017015179
ИНН/КПП 7017307138 / 701701001
РЕГ.НОМЕР 7000037783

«06» февраля 2017 г.

СПРАВКА
об использовании результатов диссертационного исследования
Николаенко Валентина Сергеевича
в ИТ-проектах, разрабатываемых ИТ-организацией ООО «Сибэдж»

Компания ООО «Сибэдж» работает в сфере информационных технологий, разрабатывая и предлагая высокотехнологичные решения для крупного и среднего бизнеса. В портфолио ООО «Сибэдж» входит свыше двухсот успешно завершенных ИТ-проектов: системы документооборота, организации процессов и взаимодействия сотрудников, мобильные приложения, приложения для нефтедобывающих компаний и другие.

Предложенное в диссертационном исследовании Николаенко В.С. методическое обеспечение было внедрено в организацию ООО «Сибэдж». По итогам внедрения специалистами ООО «Сибэдж» было принято решение по дальнейшему использованию данного методического обеспечения в остальных ИТ-проектах. Отметим, что целью внедрения риск-менеджмента являлось повышение степени управляемости и увеличение вероятности успешного завершения проектов.

Специалистами ООО «Сибэдж» отмечается, что внедрение риск-менеджмента в ИТ-проекты ослабило влияние и уменьшило вероятность наступления негативных «катастрофических» рисковых событий, а также способствовало формированию культуры управления рисками в организации.

Директор ООО «Сибэдж» Калинин А. В.

Руководитель проектов ООО «Сибэдж» Алеутдинов О. В.

ПРИЛОЖЕНИЕ Ж. Часто встречаемые негативные риски

Таблица. Часто встречаемые риски, выявленные Т. Аддисоном и С. Валлабхом

Номер риска	Название негативного риска
Риск 1	Риск того, что цели будут непонятны
Риск 2	Риск того, что сроки реализации проекта и бюджеты будут «нереальными»
Риск 3	Риск отсутствия заинтересованности в успешном завершении проекта у руководителя
Риск 4	Риск низкой вовлеченности пользователя
Риск 5	Риск отсутствия необходимых знаний и навыков
Риск 6	Риск отсутствия эффективного способа управления проектом
Риск 7	Риск непонимания требований
Риск 8	Риск завышения качества проекта *(gold plating)*, или «золотая сервировка»
Риск 9	Риск постоянного изменения требований
Риск 10	Риск неправильной разработки функциональности программного обеспечения
Риск 11	Риск невыполнения обязательств субподрядчиками
Риск 12	Риск низкой производительности труда
Риск 13	Риск использования новых технологий
Риск 14	Риск отсутствия управления ожиданиями пользователей

Таблица. Часто встречаемые риски, выявленные К. Д. Стивенсом и С. Фовеллом [181]

Номер риска	Название негативного риска
Риск 1	Риск отсутствия заинтересованности в успешном завершении проекта у руководителя
Риск 2	Риск отсутствия спроса у пользователей
Риск 3	Риск непонимания требований разработчиками
Риск 4	Риск низкой вовлеченности (отсутствия) пользователя
Риск 5	Риск отсутствия управления ожиданиями пользователей
Риск 6	Риск изменения целей проекта
Риск 7	Риск отсутствия необходимых знаний и навыков у коллектива
Риск 8	Риск отсутствия «заморозки» требований *(frozen requirements)*
Риск 9	Риск использования новых технологий
Риск 10	Риск недостаточного укомплектования проекта сотрудниками
Риск 11	Риск конфликта между заинтересованными сторонами проекта

Таблица. Часто встречаемые риски, выявленные М. Самнером [182]

Номер риска	Название негативного риска
Риск 1	Риск отказа от проектирования бизнес-процессов
Риск 2	Риск отсутствия заинтересованности в успешном завершении проекта у руководителя
Риск 3	Риск отсутствия соответствующих мастер-классов
Риск 4	Риск ухода из проекта ключевых сотрудников
Риск 5	Риск отсутствия соответствующих мастер-классов
Риск 6	Риск того, что по факту проект окажется гораздо сложнее
Риск 7	Риск отсутствия управления ожиданиями клиентов
Риск 8	Риск отсутствия интеграции с другими платформами
Риск 9	Риск отсутствия надлежащей структуры управления
Риск 10	Риск отсутствия внутренней экспертизы
Риск 11	Риск отсутствия лидера
Риск 12	Риск отсутствия бизнес-аналитика
Риск 13	Риск снижения качества работы
Риск 14	Риск отсутствия необходимой информации в проектной документации
Риск 15	Риск отсутствия стандартизации и дисциплины
Риск 16	Риск неэффективных коммуникаций

Таблица. Факторы влияющие на успех ИТ-проектов, по мнению специалистов The Standish Group [62, 63]

Номер риска	Факторы, влияющие на успех ИТ-проекта
Риск 1	Риск того, что требования будут неполны
Риск 2	Риск отсутствия пользователей в процессе реализации проекта
Риск 3	Риск нехватки ресурсов
Риск 4	Риск отсутствия управления ожиданиями заказчиков, пользователей и т. п.
Риск 5	Риск отсутствия заинтересованности в успешном завершении проекта у руководителя
Риск 6	Риск изменения требований в процессе реализации проекта
Риск 7	Риск отсутствия планирования
Риск 8	Риск отсутствия управления
Риск 9	Риск использования новых технологий

ПРИЛОЖЕНИЕ 3. Ущерб от материализации выявленных рисков

Таблица. Расчеты затрат фактических убытков от наступлений идентифицированных рисков, фактических расходов на обработку идентифицированных рисков, фактических убытков от наступлений неидентифицированных рисков, фактических расходов на обработку неидентифицированных рисков в исследуемых ИТ-проектах.

№	Название проекта	Ущерб от материализации идентифицированных рисков, дней	Расходы на обработку идентифицированных рисков, дней	Ущерб от материализации неидентифицированных рисков, дней	Расходы на обработку не выявленных рисков, дней
1	«Сайт ТГУ»	63	1,5	0	0
2	«МирКар»	5	1	0	0
3	«HyperVibe»	2	1,1	0	0
4	«Reading Log»	11	1,1	0	0
5	«CINEMOOD»	0	1,1	0	0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	42	1,2	0	0
7	«Портал логистики»	9	1	0	0
8	«Торговая площадка»	24	1,2	0	0
9	«Регламентация ведения номенклатуры ТМЦ»	4	1	0	0
10	«DigitalTV»	33	1,4	0	0
11	«ERM-система»	0	1,5	36	1,1

Таблица. Расчеты вероятных потерь от наступлений идентифицированных рисков без проведения мер «плана А» и «плана Б», а также вероятных потерь от наступлений идентифицированных рисков после проведения мер «плана А» и «плана Б» в исследуемых ИТ-проектах

№	Название проекта	Вероятные потери от материализации выявленных рисков **без мер** «плана А» и «плана Б», дней	Вероятные потери от материализации выявленных рисков **с мерами** «плана А» и «плана Б», дней
1	«Сайт ТГУ»	189	0
2	«МирКар»	18	0
3	«HyperVibe»	53	0
4	«Reading Log»	67	0
5	«CINEMOOD»	63	0
6	«Расчет и учет заработной платы в научно-технических учреждениях»	336	0
7	«Портал логистики»	135	0
8	«Торговая площадка»	255	0
9	«Регламентация ведения номенклатуры ТМЦ»	67	0
10	«DigitalTV»	153	0
11	«ERM-система»	452	0

ПРИЛОЖЕНИЕ И. Патент

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

ПРИЛОЖЕНИЕ К. Ранжирование негативных и позитивных рисков ИТ-проектов

Таблица. Ранжирование негативных рисков ИТ-проектов, где алл. – группа риска «аллигатор», щен. – «щеночек»

№	Название риска	Вер-ть	Ущерб	Группа риска
1	Риск изменения требований в процессе реализации ИТ-проекта	4,2	4,4	Тигр
2	Риск того, что по факту ИТ-проект будет значительно сложнее, чем предполагалось изначально	2,8	2,9	Тигр
3	Риск длительного изучения бизнес-процессов заказчика	3,1	3,4	Тигр
4	Риск несвоевременного завершения работы	4,8	3,9	Тигр
5	Риск отсутствия связи с субподрядом(-ами) и (или) поставщиком(-ами)	4,3	3,2	Тигр
6	Риск низкого качества предоставляемых работ	3,7	4,2	Тигр
7	Риск того, что фактическое время работы коллектива будет менее 8 часов в день	4,3	2,7	Тигр
8	Риск отсутствия у коллектива знаний, навыков и опыта, необходимых для реализации требований ИТ-проекта	3,1	4,5	Тигр
9	Риск отсутствия актуальной информации, необходимой для разработки ИТ-проекта	4,3	4,1	Тигр
10	Риск отсутствия знаний, навыков и опыта у руководителя ИТ-проекта	3,7	4,9	Тигр
11	Риск ухода руководителя ИТ-проекта	3,1	4,3	Тигр
12	Риск ухода ключевых сотрудников	3,6	4,8	Тигр
13	Риск перегрузки людских ресурсов (переработка, работа сверхурочно и т. п.)	3,8	3,9	Тигр
14	Риск допущения ошибок коллективом в вопросах управления временем	4,1	3,1	Тигр
15	Риск нечеткой формулировки целей ИТ-проекта (не по *S.M.A.R.T.*)	3,9	4,9	Тигр
16	Риск отсутствия плана-графика	2,8	4,1	Тигр
17	Риск ошибочной оценки сроков, необходимых для реализации ИТ-проекта	4,1	2,9	Тигр
18	Риск ошибочной оценки ресурсов, необходимых для реализации ИТ-проекта	4,6	3,1	Тигр
19	Риск ошибочной оценки бюджетов, необходимых для реализации ИТ-проекта	4,6	3	Тигр
20	Риск занятости руководителя ИТ-проекта на других проектах	4,3	2,6	Тигр
21	Риск занятости участников коллектива на других ИТ-проектах	4,6	3,5	Тигр
22	Риск отсутствия устава ИТ-проекта	4,2	4,1	Тигр
23	Риск изменения состава участников проектной команды в процессе реализации ИТ-проекта	4,7	4	Тигр
24	Риск низкой производительности труда руководителя ИТ-проекта	3,5	4,1	Тигр
25	Риск низкой мотивации руководителя ИТ-проекта	2,8	4,7	Тигр
26	Риск временной задержки в получении ответов на задаваемые вопросы между участниками проекта	0,4	3	Алл.
27	Риск поломки оборудования	1,2	3,6	Алл.
28	Риск неэффективного использования инструментария управления проектами (диаграмма Ганта, *Microsoft Project* и т. п.)	0,4	2,6	Алл.
29	Риск применения ранее не используемых технологий	2,3	4	Алл.
30	Риск отсутствия классического способа реализации проекта (*agile, waterfall* и др.)	2,3	3,7	Алл.
31	Риск низкого качества разработанного продукта	2,3	4,5	Алл.
32	Риск допущения ошибок при заключении договора(-ов) и других юридических документов	1,4	4,6	Алл.
33	Риск промышленного шпионажа	0,3	3,9	Алл.
34	Риск ограбления	1,5	4,9	Алл.
35	Риск утечки конфиденциальных данных	1,3	4,8	Алл.
36	Риск судебного иска от заказчика(-ов)	1,4	3,5	Алл.
37	Риск судебного иска от субподрядчика(-ов), поставщика(-ов) и т. п.	1,2	3,8	Алл.

Окончание таблицы

№	Название риска	Вер-ть	Ущерб	Группа риска
38	Риск получения штрафа(-ов) со стороны фискальных государственных органов	1,4	4,8	Алл.
39	Риск влияния от действий конкурентов	2	2,7	Алл.
40	Риск отсутствия спроса у конечного потребителя	1,7	4,1	Алл.
41	Риск использования чужих авторских прав	0,3	4,8	Алл.
42	Риск неудовлетворенности заказчика работой руководителя проекта	1,1	3,6	Алл.
43	Риск неудовлетворенности заказчика качеством разработанного продукта	1,7	5	Алл.
44	Риск неудовлетворенности заказчика сроками реализации ИТ-проекта	2,1	4,8	Алл.
45	Риск неудовлетворенности заказчиком содержанием ИТ-продукта	0,6	5	Алл.
46	Риск влияния геополитических факторов	0,2	5	Алл.
47	Риск влияния стихийных бедствий (пожар, наводнение, ураган и т. п.)	0,2	5	Алл.
48	Риск отсутствия необходимых ресурсов	2,4	3,7	Алл.
49	Риск умышленного вредительства ИТ-проекту	1,1	3,5	Алл.
50	Риск низкой загрузки человеческих ресурсов	0,6	3,6	Алл.
51	Риск того, что заказчик не сможет оплатить трудозатраты коллектива, работающего по системе оплаты *T&M*	2,1	3	Алл.
52	Риск отсутствия финансирования	1,4	4,1	Алл.
53	Риск задержки выплаты заработных плат	0,8	4,2	Алл.
54	Риск неправильного ранжирования задач руководителем ИТ-проекта	2,1	3,7	Алл.
55	Риск отсутствия технического задания	2,1	3,8	Алл.
56	Риск выявления скрытых, не обнаруженных на этапе планирования источников дополнительных затрат	4,3	2,2	Щен.
57	Риск завышения качества руководителем ИТ-проекта	4,4	1,7	Щен.
58	Риск изменения в налоговом законодательстве	3,1	1,8	Щен.
59	Риск изменения валютного курса	4,2	0,6	Щен.
60	Риск изменения банковских процентных ставок	3,8	0,8	Щен.
61	Риск отсутствия связи с заказчиком	3,8	2,1	Щен.
62	Риск временной задержки в получении ответов на задаваемые заказчику проекта вопросы	3,6	1,9	Щен.
63	Риск непонимания у коллектива того, какой продукт должен получиться по завершении ИТ-проекта	4,2	2,3	Щен.
64	Риск ухода на «больничный»	4,7	1,3	Щен.
65	Риск форс-мажоров	4,4	1,1	Щен.
66	Риск неэффективного использования инструментария управления проектами (диаграмма Ганта, *Microsoft Project* и т. п.)	2,8	1,7	Щен.
67	Риск отсутствия спецификации ИТ-проекта	4,1	2,2	Щен.
68	Риск отставания от запланированных сроков	5	2,1	Щен.
69	Риск не учета отпусков и государственных праздников при создании плана-графика ИТ-проекта	4	2,1	Щен.
70	Риск нескоординированных действий проектной команды	3,5	2,1	Щен.
71	Риск низкой производительности труда проектной команды	3	0,9	Щен.
72	Риск низкой мотивации проектной команды	3,4	0,6	Щен.
73	Риск негативной социально-психологической атмосферы внутри коллектива	2,6	2,2	Щен.
74	Риск допущения ошибок при реализации ИТ-проекта *(bugs)*	4,4	2,1	Щен.
75	Риск недостатка коммуникаций между участниками проекта	2,6	2,1	Щен.
76	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений	3,4	2,1	Щен.
77	Риск использования устаревших технологий	1,5	2,4	Котенок
78	Риск отключения электричества	0,3	2,1	Котенок
79	Риск отключения интернета	0,2	1,9	Котенок
80	Риск переизбытка каналов коммуникаций, доносящих актуальную информацию	1,4	0,8	Котенок
81	Риск отсутствия у коллектива заинтересованности в успешном завершении ИТ-проекта	2,1	1,8	Котенок

Окончание таблицы

№	Название риска	Вер-ть	Ущерб	Группа риска
82	Риск отсутствия общего видения конечного ИТ-продукта	1,4	2,2	Котенок
83	Риск отсутствия полной (частичной) предоплаты	0,4	1,7	Котенок

Таблица. Ранжирование позитивных рисков ИТ-проектов

№	Название риска	Вер-ть	Доход	Группа риска
1	Риск привлечения руководителя, который имеет опыт управления проектами более 2-х лет	3,1	4,6	Слон
2	Риск того, что для ИТ-проекта будет создано техническое задание	4,1	4,5	Слон
3	Риск использования плана-графика (диаграмма Ганта, сетевого графика и т. п.)	4,3	4,7	Слон
4	Риск полной (частичной) предоплаты	1,5	4,3	Лев
5	Риск привлечения высококвалифицированного специалиста в проектную команду	2,3	4,7	Лев
6	Риск уменьшения численности коллектива ИТ-проекта до 6 человек	1,1	3,8	Лев
7	Риск того, что руководитель ИТ-проекта имеет профессиональное образование в области управления проектами в сфере информационных технологий	2,4	4,4	Лев
8	Риск привлечения руководителя, который имеет профессиональное образование в области управления проектами	1,3	4,5	Лев
9	Риск того, что для ИТ-проекта будет создан Устав проекта	1,5	4,1	Лев
10	Риск того, что для ИТ-проекта будет создана спецификация продукта	0,8	4,3	Лев
11	Риск того, что для ИТ-проекта будет создано технико-экономическое обоснование (ТЭО)	0,3	4,5	Лев
12	Риск того, что для ИТ-проекта будет создан план управления рисками	0,3	4,9	Лев
13	Риск декомпозиции большого ИТ-проекта на краткосрочные, трудоемкостью не более 700 человеко-часов	1,5	4,3	Лев
14	Риск того, что к процессу оценивания будут приглашены сторонние эксперты	0,3	3,8	Лев
15	Риск использования классического способа реализации проекта (*agile, waterfall* и др.)	1,5	4,6	Лев
16	Риск сотрудничества *(collaboration)* между руководителем ИТ-проекта и коллективом (групповое одобрение, реализация индивидуальных идей и т. п.)	2,3	2,4	Кролик

ПРИЛОЖЕНИЕ Л. Актуализация негативных и позитивных рисков ИТ-проектов

Таблица. Актуализация негативных рисков ИТ-проектов

№	Название риска	Фаза жизненного цикла
1	Риск отсутствия общего видения конечного ИТ-продукта	Начало проекта
2	Риск отсутствия полной (частичной) предоплаты	Начало проекта
3	Риск допущения ошибок при заключении договора(-ов) и других юридических документов	Начало проекта
4	Риск отсутствия финансирования	Начало проекта
5	Риск неправильного ранжирования задач руководителем ИТ-проекта	Организация и подготовка
6	Риск отсутствия технического задания	Организация и подготовка
7	Риск длительного изучения бизнес-процессов заказчика	Организация и подготовка
8	Риск отсутствия знаний, навыков и опыта, необходимых для реализации требований ИТ-проекта у коллектива	Организация и подготовка
9	Риск нечеткой формулировки целей ИТ-проекта (не по *S.M.A.R.T.*)	Организация и подготовка
10	Риск отсутствия плана-графика	Организация и подготовка
11	Риск ошибочной оценки сроков, необходимых для реализации проекта	Организация и подготовка
12	Риск ошибочной оценки ресурсов, необходимых для реализации проекта	Организация и подготовка
13	Риск ошибочной оценки бюджетов, необходимых для реализации проекта	Организация и подготовка
14	Риск отсутствия устава ИТ-проекта	Организация и подготовка
15	Риск неэффективного использования инструментария управления проектами (диаграмма Ганта, *Microsoft Project* и т. п.)	Организация и подготовка
16	Риск применения ранее не используемых технологий	Организация и подготовка
17	Риск отсутствия классического способа реализации проекта (*agile, waterfall* и др.)	Организация и подготовка
18	Риск неэффективного использования инструментария управления проектами (диаграмма Ганта, *Microsoft Project* и т. п.)	Организация и подготовка
19	Риск отсутствия спецификации ИТ-проекта	Организация и подготовка
20	Риск завышения качества руководителем ИТ-проекта	Организация и подготовка
21	Риск использования чужих авторских прав	Организация и подготовка
22	Риск не учета отпусков и государственных праздников при создании плана-графика ИТ-проекта	Организация и подготовка
23	Риск нескоординированных действий проектной команды	Организация и подготовка
24	Риск использования устаревших технологий	Организация и подготовка
25	Риск длительного изучения бизнес-процессов заказчика	Организация и подготовка
26	Риск изменения требований в процессе реализации ИТ-проекта	Выполнение работ
27	Риск того, что по факту ИТ-проект будет значительно сложнее, чем предполагалось изначально	Выполнение работ
28	Риск переизбытка каналов коммуникаций, доносящих актуальную информацию	Выполнение работ

Окончание таблицы

№	Название риска	Фаза жизненного цикла
29	Риск отсутствия у коллектива заинтересованности в успешном завершении ИТ-проекта	Выполнение работ
30	Риск того, что фактическое время работы коллектива будет менее 8 часов в день	Выполнение работ
31	Риск отсутствия актуальной информации необходимой для разработки ИТ-проекта	Выполнение работ
32	Риск перегрузки людских ресурсов (переработка, работа сверхурочно и т. п.);	Выполнение работ
33	Риск допущения ошибок коллективом в вопросах управления временем	Выполнение работ
34	Риск занятости руководителем ИТ-проекта на других проектах	Выполнение работ
35	Риск занятости участников коллектива на других проектах	Выполнение работ
36	Риск изменения состава участников проектной команды в процессе реализации ИТ-проекта	Выполнение работ
37	Риск низкой производительности труда руководителя ИТ-проекта	Выполнение работ
38	Риск низкой мотивации руководителя ИТ-проекта	Выполнение работ
39	Риск неудовлетворенности заказчика работой руководителя проекта	Выполнение работ
40	Риск низкой загрузки человеческих ресурсов	Выполнение работ
41	Риск отсутствия необходимых ресурсов	Выполнение работ
42	Риск непонимания у коллектива того, какой продукт должен получиться по завершении ИТ-проекта	Выполнение работ
43	Риск выявления скрытых, не обнаруженных на этапе планирования источников дополнительных затрат	Выполнение работ
44	Риск низкой производительности труда проектной команды	Выполнение работ
45	Риск низкой мотивации проектной команды	Выполнение работ
46	Риск негативной социально-психологической атмосферы внутри коллектива	Выполнение работ
47	Риск допущения ошибок при реализации ИТ-проекта *(bugs)*	Выполнение работ
48	Риск отставания от запланированных сроков	Выполнение работ
49	Риск низкого качества предоставляемых работ	Окончание проекта
50	Риск низкого качества разработанного продукта	Окончание проекта
51	Риск неудовлетворенности заказчика качеством разработанного продукта	Окончание проекта
52	Риск неудовлетворенности заказчика сроками реализации ИТ-проекта	Окончание проекта
53	Риск неудовлетворенности заказчиком содержанием ИТ-продукта	Окончание проекта
54	Риск того, что заказчик не сможет оплатить трудозатраты коллектива, работающего по системе оплаты *T&M*	Окончание проекта
55	Риск несвоевременного завершения работы	Все фазы жизненного цикла
56	Риск отсутствия связи с субподрядом(-ами) и (или) поставщиком(-ами)	Все фазы жизненного цикла
57	Риск ухода руководителя ИТ-проекта	Все фазы жизненного цикла
58	Риск ухода ключевых сотрудников	Все фазы жизненного цикла
59	Риск временной задержки в получении ответов на задаваемые вопросы между участниками проекта	Все фазы жизненного цикла
60	Риск поломки оборудования	Все фазы жизненного цикла
61	Риск промышленного шпионажа	Все фазы жизненного цикла
62	Риск ограбления	Все фазы жизненного цикла
63	Риск утечки конфиденциальных данных	Все фазы жизненного цикла

Окончание таблицы

№	Название риска	Фаза жизненного цикла
64	Риск судебного иска от заказчика(-ов)	Все фазы жизненного цикла
65	Риск судебного иска от субподрядчика(-ов), поставщика(-ов) и т. п.	Все фазы жизненного цикла
66	Риск получения штрафа(-ов) со стороны фискальных государственных органов	Все фазы жизненного цикла
67	Риск влияния от действий конкурентов	Все фазы жизненного цикла
68	Риск отсутствия спроса у конечного потребителя	Все фазы жизненного цикла
69	Риск влияния геополитических факторов	Все фазы жизненного цикла
70	Риск влияния стихийных бедствий (пожар, наводнение, ураган и т. п.)	Все фазы жизненного цикла
71	Риск умышленного вредительства ИТ-проекту	Все фазы жизненного цикла
72	Риск задержки выплаты заработных плат	Все фазы жизненного цикла
73	Риск изменения в налоговом законодательстве	Все фазы жизненного цикла
74	Риск изменения валютного курса	Все фазы жизненного цикла
75	Риск изменения банковских процентных ставок	Все фазы жизненного цикла
76	Риск отсутствия связи с заказчиком	Все фазы жизненного цикла
77	Риск временной задержки в получении ответов на задаваемые заказчику проекта вопросы	Все фазы жизненного цикла
78	Риск ухода на «больничный»	Все фазы жизненного цикла
79	Риск форс-мажоров	Все фазы жизненного цикла
80	Риск недостатка коммуникаций между участниками проекта	Все фазы жизненного цикла
81	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений	Все фазы жизненного цикла
82	Риск отключения электричества	Все фазы жизненного цикла
83	Риск отключения интернета	Все фазы жизненного цикла

Таблица. Актуализация позитивных рисков ИТ-проектов

№	Название риска	Фаза жизненного цикла
1	Риск привлечения руководителя, который имеет опыт управления проектами более 2-х лет	Начало проекта
2	Риск того, что для ИТ-проекта будет создано техническое задание	Организация и подготовка
3	Риск использования плана-графика (диаграмма Ганта, сетевого графика и т. п.)	Организация и подготовка
4	Риск полной (частичной) предоплаты	Организация и подготовка
5	Риск привлечения высококвалифицированного специалиста в проектную команду	Организация и подготовка

Окончание таблицы

№	Название риска	Фаза жизненного цикла
6	Риск уменьшения численности коллектива ИТ-проекта до 6 человек	Организация и подготовка
7	Риск того, что руководитель ИТ-проекта имеет профессиональное образование в области управления проектами в сфере информационных технологий	Организация и подготовка
8	Риск привлечения руководителя, который имеет профессиональное образование в области управления проектами	Организация и подготовка
9	Риск того, что для ИТ-проекта будет создан Устав проекта	Организация и подготовка
10	Риск того, что для ИТ-проекта будет создана спецификация продукта	Организация и подготовка
11	Риск того, что для ИТ-проекта будет создано технико-экономическое обоснование (ТЭО)	Организация и подготовка
12	Риск того, что для ИТ-проекта будет создан план управления рисками	Организация и подготовка
13	Риск декомпозиции большого ИТ-проекта на краткосрочные, трудоемкостью не более 700 человеко-часов	Организация и подготовка
14	Риск того, что к процессу оценивания будут приглашены сторонние эксперты	Организация и подготовка
15	Риск использования классического способа реализации проекта (*agile, waterfall* и др.)	Организация и подготовка
16	Риск сотрудничества *(collaboration)* между руководителем ИТ-проекта и коллективом (групповое одобрение, реализация индивидуальных идей и т. п.)	Выполнение работ