

*На правах рукописи*



**НИКОЛАЕНКО ВАЛЕНТИН СЕРГЕЕВИЧ**

**УПРАВЛЕНИЕ РИСКАМИ ИТ-ПРОЕКТОВ В ОРГАНИЗАЦИЯХ**

Специальность 08.00.05 – Экономика и управление народным хозяйством: Менеджмент  
(Процесс управления организацией, её отдельными подсистемами и функциями.  
Целеполагание и планирование в управлении организацией. Контроль, мониторинг и  
бенчмаркинг. Механизмы и методы принятия и реализации управленческих решений.  
Управление проектом. Управление знаниями. Риск-менеджмент. Управление производством.  
Современные производственные системы)

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени кандидата  
экономических наук

Томск – 2021

Диссертационная работа выполнена в отделении социально-гуманитарных наук Школы базовой инженерной подготовки Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский политехнический университет».

**Научный руководитель:**

доктор экономических наук, профессор Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский политехнический университет», Школа инженерного предпринимательства, профессор,

**Никулина Ирина Евгеньевна**

**Официальные оппоненты:**

доктор экономических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Вятский государственный университет», кафедра финансов и экономической безопасности, заведующий кафедрой,

**Каранина Елена Валерьевна**

кандидат экономических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Крымский федеральный университет имени В. И. Вернадского», кафедра бизнес-информатики и математического моделирования, доцент,

**Королев Олег Леонидович**

**Ведущая организация:**

Федеральное государственное бюджетное учреждение науки «Центральный экономико-математический институт Российской Академии наук»

Защита диссертации состоится «22» сентября 2021 года в 13-00 часов на заседании диссертационного совета Д 212.166.23 при Федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» по адресу: 603140, г. Нижний Новгород, пр. Ленина, д.27, Конференц-зал.

С диссертацией можно ознакомиться в библиотеке и на сайте <https://diss.unn.ru/1126> Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» по адресу: 603950, г. Нижний Новгород, пр. Гагарина, д.23, корп.1.

Автореферат разослан «09» сентября 2021 года

Ученый секретарь  
диссертационного совета,  
к.э.н., доцент



Макушева Ю. А.

## I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы диссертационного исследования.** Мировые и отечественные тренды перехода к постиндустриальному развитию обуславливают 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 посредством 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 благодаря принятым Указам Президента РФ от 09.05.2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» и от 21.07.2020 года № 474 «О национальных целях развития Российской Федерации на период до 2030 года», Распоряжению Правительства РФ от 28.06.2017 года № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”» и Постановлению Правительства РФ от 02.03.2019 года № 234 «О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации"», 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», 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, 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 оснащаться 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, что 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 разработанности научной 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»).

Необходимо отметить, что для достижения поставленной цели были 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, информационный менеджмент, производственный менеджмент, стратегический менеджмент, антикризисный менеджмент, а также кадровый 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»; Приказ Минкомсвязи России № 96 от 1 апреля 2015 года «Об утверждении плана импортозамещения программного обеспечения»; 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»; Постановление Правительства РФ №57 от 27 января 2017 года «О создании Российского фонда развития информационных технологий»; 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»; Sarbanes-Oxley Act; IRM; AIRMIC и ALARM (FERMA RMS); стандарт COSO «ERM Integrated Framework»; Australian Risk AS/NZS 4360:2004 и Handbook Risk Management Guidelines; 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 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 диссертации Паспорту научной специальности.** Диссертационная работа выполнена 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 и разработке теоретических положений и практических рекомендаций по управлению рисками ИТ-проектов, дополняющих теории проектного управления и риск-менеджмента.

**Наиболее существенные положения и научные результаты, полученные лично автором, 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) превосходя 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 рисков 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 относительно 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 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 рисков 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 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 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\_a); 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 положения диссертационной работы* рассмотрены, одобрены и *внедрены* хозяйствующими субъектами ИТ, 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 диссертации.** Диссертационная работа состоит из введения, трех глав, заключения, 11 приложений, библиографического списка из 227 наименований, включает 44 таблиц, 24 рисунка. Основное содержание работы изложено на 192 страницах машинописного текста.



## **II. ОСНОВНЫЕ ПОЛОЖЕНИЯ И РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ, 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) превосходя ранее запланированные результаты.**

На основании проведенного анализа было установлено, что в литературе нет общепринятой и устоявшейся трактовки термина «риск», что создает проблему интерпретации, определения и использования данного понятия в сфере информационных технологий (таблица 1).

Критическое осмысление обозначенных в таблице 1 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 сущность и содержание понятия «риск», и значительно ограничивает его практическое применение в сфере информационных технологий. В связи с этим автором диссертационного исследования была уточнена сущность и дополнено содержание понятия «риск в ИТ-проектах», трактуемого как 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.

Благодаря предложенному автором диссертационной работы уточнению и дополнению стало возможным выделение конкретных источников риска, актуальных для ИТ-проектов: подрядчик и (или) поставщик, право, рынок, заказчик ИТ-проекта, стихийные бедствия, пользователь ИТ-продукта, технология, проектный коллектив, руководитель ИТ-проекта, информация и коммуникационный канал. С определением конкретных источников риска была установлена их связь с фактором риска, совокупностью обстоятельств, которые, воздействуя на данные источники риска, увеличивают либо уменьшают вероятность наступления рискованного события. Стоит отметить, что фактор риска зависит 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).

Наличие благоприятных последствий по причине наступления риска, в свою очередь, послужило основанием для дифференциации рискованных событий на «негативные риски» и «позитивные риски». «Негативный риск» – это событие, которое может отрицательно повлиять на план проекта и на проектные цели, приводя к увеличению длительности проекта, увеличению стоимости проектных работ, уменьшению качества итогового

продукта. Под «позитивным риском» понимается событие, которое может положительно повлиять на план проекта и на проектные цели, предвосхищая запланированные результаты.

Таблица 1 – Основные точки зрения на определение термина «риск»

| №  | Дефиниция термина «риск»                                                                                                                                                                             | Источники                                                                                                    |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 1  | Влияние неопределенности на цели (стратегические, тактические, операционные и проектные)                                                                                                             | ГОСТ Р ИСО 31000-2010. Менеджмент риска: Принципы и руководство                                              |
| 2  | Угроза и (или) опасность                                                                                                                                                                             | И. Т. Балабанов, Д. М. Машков, С. Н. Митягов, Ю. В. Трифонов                                                 |
| 3  | Неопределенность                                                                                                                                                                                     | Д. И. Филимонов, В. Н. Бурков и Д. А. Новиков, И. И. Мазур и В. Д. Шапиро                                    |
| 4  | Условие или неопределенное событие, которое в случае наступления оказывает влияние хотя бы на одну цель проекта (длительность, стоимость, качество, содержание)                                      | Свод правил проектного управления Project Management Body of Knowledge (PMBOK® Guide)                        |
| 5  | Угроза и (или) возможность                                                                                                                                                                           | П. Сангхира                                                                                                  |
| 6  | Событие, которое одновременно несет угрозу, опасность, неопределенность и возможность                                                                                                                | PricewaterhouseCoopers                                                                                       |
| 7  | Вероятность недополучения доходов и (или) вероятность возникновения убытков                                                                                                                          | П. Г. Грабовый, С. Н. Петрова                                                                                |
| 8  | Численная мера опасности                                                                                                                                                                             | Е. И. Шохин                                                                                                  |
| 9  | Совокупность значений возможного ущерба в некоторой стохастической ситуации                                                                                                                          | В. Ю. Королев, В. Е. Бенинг, С. Я. Шоргин                                                                    |
| 10 | Возможность получения убытков от предпринимательской деятельности                                                                                                                                    | Гражданский кодекс Российской Федерации (ст.933 ГК РФ)                                                       |
| 11 | Действия, сделанные наудачу                                                                                                                                                                          | В. Даль                                                                                                      |
| 12 | Неопределенное событие или набор неопределенных событий                                                                                                                                              | Management of Risk: Guidance for Practitioners (M o R®)                                                      |
| 13 | Неопределенное событие или набор событий, которые в случае наступления, способно оказать влияние на процесс достижения целей                                                                         | PRojects IN Controlled Environments (PRINCE2®)                                                               |
| 14 | Искусственная экономическая категория, совокупно отражающая меру реальности нежелательного отклонения от цели хозяйственной деятельности предприятия и размер обусловленного этим отклонением ущерба | Р. М. Качалов                                                                                                |
| 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) |
| 16 | Вероятный неблагоприятный исход для субъекта                                                                                                                                                         | А. Г. Мадера                                                                                                 |

Термин «позитивный риск» (*positive risk*) упоминается во многих источниках. Так, например, У. Сторидж из Калифорнийского университета в Беркли, утверждает, что концепция «позитивного риска» сформировалась во многом благодаря правилам риск-менеджмента COSO ERM, опубликованным в 2004 году. В своде лучших практик управления проектами PMBOK® Guide 2017 года сказано, что целью управления проектными рисками является повышение вероятности и (или) влияния позитивных рисков и снижение вероятности и (или) влияния негативных рисков. Финансовый консультант Д. Дункельбергер определяет «позитивный риск», как вероятное событие, которое может оказать положительное влияние на проект. М. Карпентер, в своей работе утверждает, что о наступлении «положительного риска» можно говорить только тогда, когда полученный результат значительно предвосхитил ожидания. Риск-консультант Т. Дэвидсон, понимает под «позитивными рисками» шансы и возможности. Дж. А. Лакман в своих трудах не только активно использует термин «позитивный риск», но также предлагает алгоритм его использования при добыче полезных ископаемых. 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».



Рисунок 1 – Графическое представление взаимосвязи источника риска, фактора риска, риска и проблемной/благоприятной ситуации

Влияние материализовавшихся негативного и позитивного рисков в ИТ-проекте, можно охарактеризовать формулами 1 и 2, где  $Im_{negative}$  – 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,  $Im_{positive}$  – влияние в результате материализации позитивного риска,  $C_5$  – материальная польза, вызванная отклонением от запланированных проектных целей.

$$Im_{negative} = C_1 + C_2 + C_3 + C_4, \quad (1)$$

$$Im_{positive} = C_5 \quad (2)$$

В качестве примера наступившего 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. ( $Im_{negative}$ ).

Наглядным примером влияния материализованного позитивного риска на проектные цели ( $Im_{positive}$ ) 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*). Как правило, подобная замена приводит к значительному предвосхищению запланированных результатов, например, на 50 человеко-часов. Следовательно, влияние от материализации позитивного риска составит 42 500 руб. ( $C_5$ ).

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

- Во-первых, раскрывается сущность и природа рискового события, устанавливаются причины наступления риска, что дает возможность значительно повысить

результативность мер управленческого 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 методического 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. риск-ориентированный прогноз приобретает временной ориентир, что дает больше управленческой свободы ИТ-организациям, руководителям ИТ-проектов и проектным коллективам в выборе средств воздействия на данные рисковые события.

- В-четвертых, предложенная дефиниция уточняет сущность термина «неопределенность» и «риск-менеджмент». Так, 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 предсказуемым и прогнозируемым. Таким образом, с учетом приращения новых знаний в понимании природы риска под «риск-менеджментом» совокупность процессов по оценке негативных/позитивных рисков, принятия управленческих решений по разработке мер воздействия, мониторинга неидентифицированных рисков и контроля идентифицированных рисков.

**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.**

Диссертационное исследование показало, что многие международные ассоциации, институты, отечественные и зарубежные ученые глубоко и существенно изучили проблематику классификации рисков. Однако, несмотря на теоретическую проработанность вопроса, остается нерешенной проблема: как необходимо классифицировать риски в ИТ-проектах. Предлагаемые способы часто противоречат друг другу и имеют существенные недостатки. Нерешенность указанной проблемы оказывает отрицательное влияние на процессы управления рисками в ИТ-проектах, что приводит к низкому качеству идентификации негативных/позитивных рисковых событий, невыявлению скрытых и специфических рисков, частой потери управляемости по причине отсутствия стандартизированных мер превентивного воздействия на риски.

Стоит отметить, что, как правило, 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 была предложена классификация групп рисков, базирующаяся на классификационных признаках, актуальных для сферы ИТ – 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).

Таблица 2 – Классификация групп рисков в ИТ-проектах

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

Для апробации предложенной классификации групп рисков в ИТ-проектах были отобраны десять экспертов из различных ИТ-организаций (ООО «ЛидерГрупп», ООО «Синтез Интеллектуальных Систем», ООО «Спейс-О технологии», ООО «Аксимедия Софт», ООО «Телебриз», ООО «Контек Софт», ООО «Сибэйдж»). Все респонденты имели профессиональное образование и опыт работы в сфере информационных технологий не менее четырех лет.

В результате было выявлено 83 негативных риска и 16 позитивных рисков.

Среди негативных рисков были идентифицированы: риск изменения требований в процессе реализации ИТ-проекта; риск длительного изучения бизнес-процессов заказчика; риск несвоевременного завершения работы; риск отсутствия связи с субподрядом(-ами) и (или) поставщиком(-ами); риск низкого качества предоставляемых работ; риск отсутствия у коллектива знаний, навыков и опыта, необходимых для реализации требований ИТ-проекта, и др.

Основными позитивными рисками в ИТ-проектах являются: риск привлечения руководителя, имеющего опыт управления ИТ-проектами более 2-х лет; риск привлечения в проектный коллектив высококвалифицированного специалиста; риск уменьшения численности проектного коллектива до 6 человек; риск привлечения руководителя, который имеет профессиональное образование в области управления ИТ-проектами; риск



декомпозиции большого ИТ-проекта на малые, трудоемкостью не более 700 человеко-часов и др.

На базе идентифицированных рисков были разработаны иерархические структуры негативных и позитивных рисков (ИСР).

Полученные ИСР имеют большую практическую ценность для ИТ-организаций, руководителей ИТ-проектов и проектных коллективов, т.к. знание о потенциальных негативных и позитивных рисках помогает заблаговременно, до фазы организации и подготовки, предупредить деструктивные воздействия на проектные цели, разработать и реализовать превентивные меры, значительно повысить оперативность и качество идентификации рисков.

На основании проведенной апробации было установлено:

- Предложенная классификация рисков в ИТ-проектах повышает качество процесса идентификации рисков за счет выявления скрытых и специфических рисков событий. Кроме того, во время апробации разработанного методического инструментария управления рисками были обнаружены скрытые риски, которые могли бы быть не выявлены, если бы не была применена созданная классификация рисков в ИТ-проектах.

- Классификация способствует запуску процесса стандартизации мер превентивного воздействия на риски. Так, например, во время апробации разработанного методического инструментария управления рисками для определенных групп рисков создавались универсальные превентивные меры по их нивелированию, диверсификации, переносу и (или) ослаблению/усилению.

Благодаря классификации рисков были улучшены процессы мониторинга рисков и контроля рисков. В диссертационной работе показано, что если ИТ-организации, руководители ИТ-проектов и проектные коллективы обладают информацией о времени актуализации рисков относительно фаз жизненного цикла, то они могут заблаговременно мобилизовать материальные и временные резервы, либо, если данные рисковые события не были материализованы, высвободить зарезервированные ресурсы и уменьшить тем самым стоимость проектных работ.

Таким образом, совокупность полученных результатов от применения классификации рисков в ИТ-проектах повышает качество процесса идентификации рисков за счет выявления скрытых и специфических рисков событий, способствует запуску процесса стандартизации мер превентивного воздействия на рисковые события, улучшает мониторинг и контроль рисков.

**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.**

Несмотря на картографирование и обработку информации с помощью инструментов, рекомендованных сводом правил проектного управления PMBOK® Guide, таких как иерархическая структура рисков, ранжирование рисков и матрицы вероятностей наступления рисков и возможного влияния на проектные цели, в ИТ-проектах также требуется определять время актуализации рисков относительно фаз жизненного цикла проекта. Под фазой проекта в диссертационной работе понимается совокупность логически связанных операций, которые завершаются достижением одного или ряда запланированных результатов. Необходимо

отметить, что знание о времени материализации негативных/позитивных рисков способствует превентивной подготовке ИТ-организаций, руководителей ИТ-проектов и проектных коллективов к временным периодам, которые представляют наибольшую угрозу либо благоприятную возможность.

Исследования показали, что каскадная модель жизненного цикла может быть применима независимо от типа ИТ-проекта (*портал, сайт, ПО, мобильное приложение, корпоративная система, ERM-система*), его размера (*краткосрочный, среднесрочный, долгосрочный*) и сложности. В отличие от V-образной модели жизненного цикла, модели быстрой разработки приложений, инкрементной модели жизненного цикла и спиральной модели жизненного цикла Б. В. Боема, каскадная модель жизненного цикла состоит из универсальных последовательных фаз, таких как начало ИТ-проекта, организация и подготовка, выполнение работ, окончание ИТ-проекта, что и обусловило ее выбор при создании методики определения времени актуализации рисков.

По результатам анализа иерархических структур негативных и позитивных рисков, актуальных для ИТ-проектов, и фаз жизненного цикла было установлено, что наибольшая концентрация негативных рисков сосредоточена в фазе «выполнение работ» (рисунок 2), наибольшая концентрация позитивных рисков – в фазе «организация и подготовка». Также было установлено, что в ИТ-проектах существуют постоянные риски, которые имеют потенциал материализоваться в любой временной период существования ИТ-проекта.

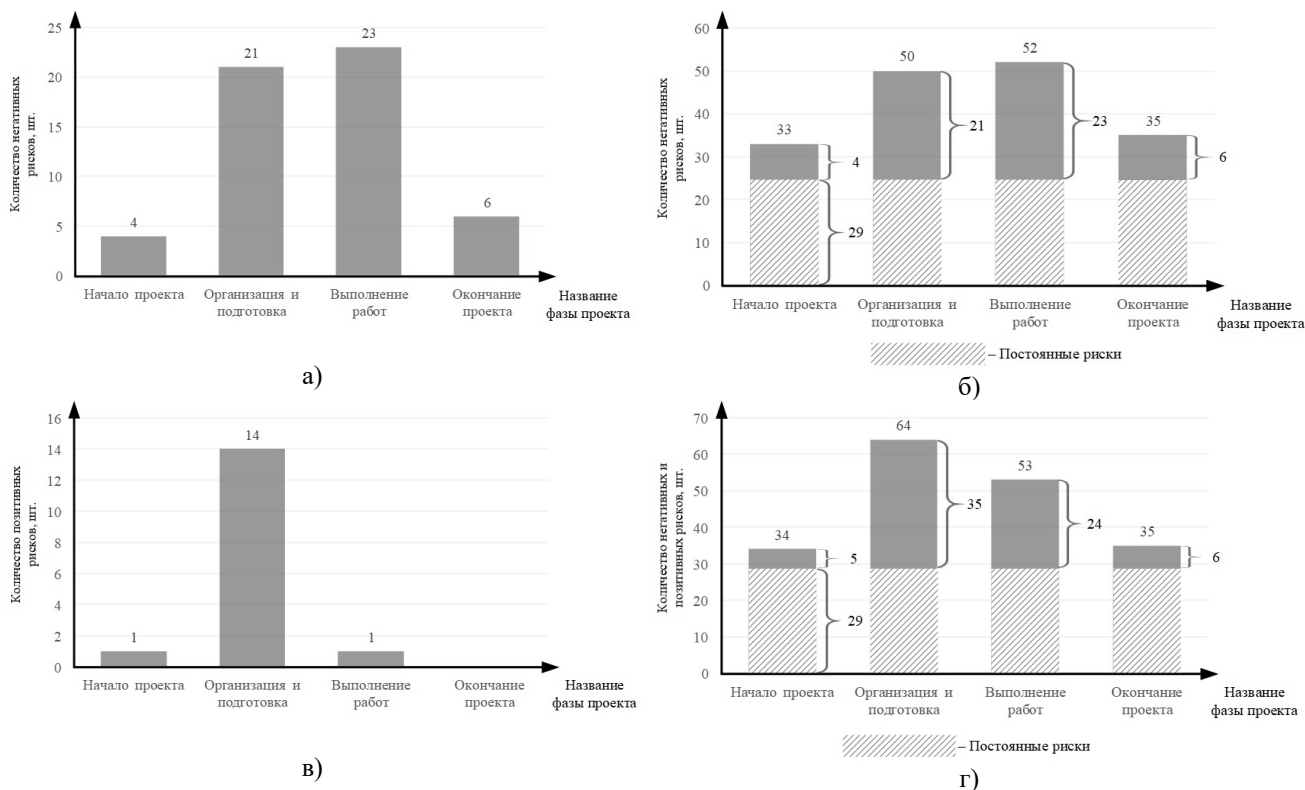


Рисунок 2 – **а)** количество негативных рисков, распределенных относительно фаз жизненного цикла ИТ-проекта, без учета постоянных рисков; **б)** количество негативных рисков, распределенных относительно фаз жизненного цикла ИТ-проекта, с учетом постоянных рисков; **в)** количество позитивных рисков, 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 наступления рисков и фазы наибольшей угрозы. Помимо прочего, обнаружение постоянных рисков позволяет формализовать методическую рекомендацию, сутью которой является обязательное формирование материальных и временных резервов на случай материализации данных рисков.

На основе полученных результатов автором диссертационного исследования была разработана методика определения времени актуализации (наступления) рисков относительно фаз жизненного цикла ИТ-проекта, сформулированы практические рекомендации для ИТ-организаций, руководителей ИТ-проектов и проектных коллективов о том, как необходимо определять время актуализации рисков относительно фаз проекта, выявлять наиболее благоприятные и опасные фазы и для каких постоянных рисков необходимо заблаговременно формировать материальные и временные резервы.

**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 относительно друга и идентифицировать наиболее значимые позитивные рисковые события, что существенно сокращает материальные и временные затраты на управление рисками ИТ-проектов в организациях.**

Как правило, идентифицированные негативные риски распределяются на три группы: катастрофические риски; умеренные риски; незначительные риски. Подобная группировка ранжирует негативные рисковые события, помогая проектным коллективам и руководителям ИТ-проектов в принятии управленческих решений в процессе создания мер воздействия. Также стоит отметить, что в отечественной и зарубежной литературе зачастую приводятся и рассматриваются только способы группировки негативных рисков.

Учитывая данное обстоятельство и полученные в ходе исследования аспекты касательно позитивной природы риска, был проведен анализ имеющихся способов группировки негативных рисков, по результатам которого был предложен авторский способ группировки позитивных рисков. Данный способ базируется на концепции, предложенной Т. Мерна и Ф. Ал-Хани. По их мнению, негативные риски необходимо распределять по четырем группам:

- Катастрофический риск или «тигр» – 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» – 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 «щенок» – 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» – 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.

Способ, предложенный Т. Мерна и Ф. Ал-Хани, обладает рядом преимуществ по сравнению с группировками, которые рекомендуют применять PMBOK® Guide, PRINCE2® и Н. Н. Талей. В частности:

- во-первых, оперативно выявляются наиболее опасные риски для ИТ-проектов;
- во-вторых, распределение рисков относительно друг друга дает возможность судить об общем состоянии ИТ-проекта в определенный момент времени;
- в-третьих, распознаются негативные риски, которые не представляют существенной угрозы для проектных целей, следовательно, не требуют дополнительных затрат для разработки мер превентивного воздействия и ресурсов для формирования резервов.

На основании вышесказанного автором диссертационного исследования был предложен способ группировки позитивных рисков, который обладает не менее значимыми преимуществами и включает в себя следующие группы:

- 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 заблаговременно 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%.

- 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»).

Предложенный способ группировки позитивных рисков позволяет оперативно получать информацию о позиционировании данных рисков друг относительно друга, выявлять рисковые события, которые не требуют разработки мер воздействия, а также идентифицировать наиболее важные и значимые позитивные риски, которые обладают потенциалом превосходить запланированные проектные цели.

Для апробации авторского способа группировки позитивных рисков было организовано экспертное оценивание. В экспертный состав вошли десять экспертов из различных ИТ-организаций (ООО «ЛидерГрупп», ООО «Синтез Интеллектуальных Систем», ООО «Спейс-О технологии», ООО «Аксимедия Софт», ООО «Телебриз», ООО «Контек Софт», ООО «Сибэйдж»). Следует отметить, что данная численность обусловлена двумя факторами: во-первых, возможностью верификации экспертных оценок; во-вторых, возможностью получения более достоверных оценок при большем количестве экспертных мнений. Все респонденты имели профессиональное образование и опыт работы в сфере информационных технологий не менее четырех лет. Оценивание включало в себя следующие этапы:

- формирование правил обработки экспертных мнений;
- оценивание 83 негативных рисков и 16 позитивных рисков;
- анализ и обработка экспертных мнений.

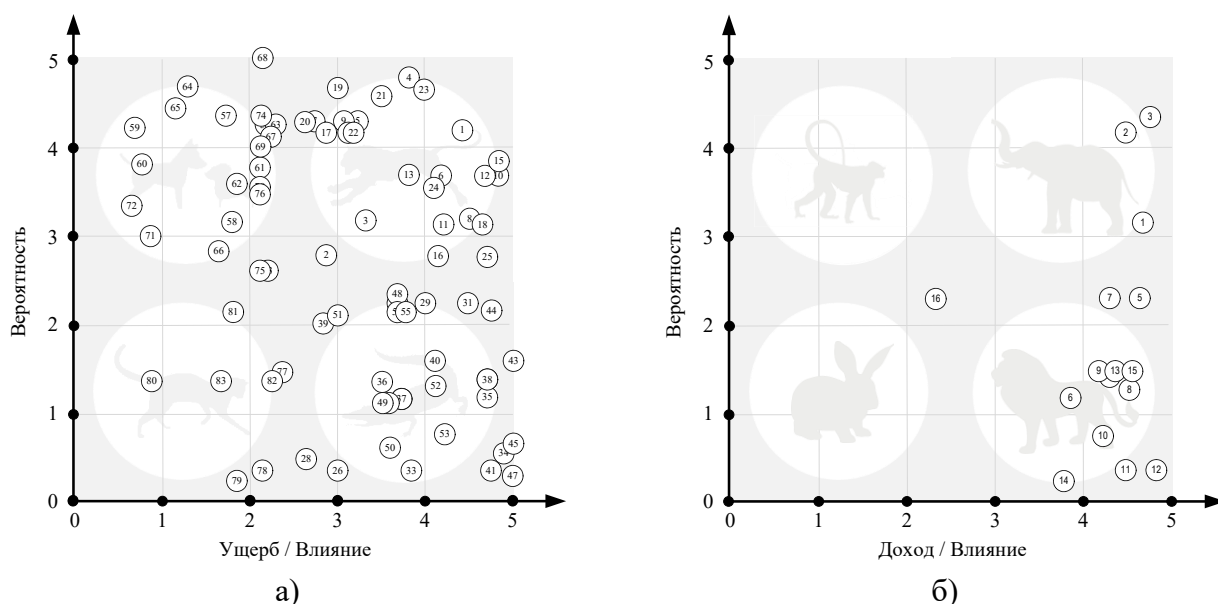


Рисунок 3 – а) способ группировки негативных рисков, актуальных для сферы ИТ, предложенный Т. Мерна и Ф. Ал-Хани, б) способ группировки позитивных рисков, актуальных для сферы ИТ<sup>1</sup>

Обработка экспертных мнений осуществлялась с помощью вербально-числовой шкалы и коэффициентов Харрингтона от 0 до 5, где 0 – нет вероятности/влияния, 5 – очень высокая вероятность/влияния. Эксперты оценивали два параметра риска: вероятность

<sup>1</sup> Степень вероятности наступления риска и степень влияния риска определяется с помощью коэффициентов Харрингтона, где 5 – очень высокая вероятность/влияние, 4 – высокая вероятность/влияние, 3 – средняя вероятность/влияние, 2 – низкая вероятность/влияние, 1 – очень низкая вероятность/влияние, 0 – нет вероятности/влияния.

наступления риска и его возможное влияние в случаях материализации. Для получения интегральных оценок использовался коэффициент Кендалла. Так, при полной согласованности экспертов их оценка вероятности наступления риска и его влияния заносилась в итоговый реестр. Интегральные оценки с низкой согласованностью или при ее отсутствии выносились на общее экспертное обсуждение, где респонденты принимали окончательное решение, какое значение вероятности/влияния следует внести в итоговый реестр.

В качестве объекта оценивания были выбраны отобранные ранее этими же экспертами 83 негативных риска и 16 позитивных рисков, актуальных для ИТ-проектов.

В результате апробации все негативные и позитивные рисковые события были распределены по группам. Было установлено, что к «тиграм» относится 25 негативных рисков, к «аллигаторам» – 30 негативных рисков, к «щеночкам» – 21 негативный риск, к «котяткам» – 7 негативных рисков, к «слонам» – 3 позитивных риска, к «львам» – 12 позитивных рисков и к «кроликам» – 1 позитивный риск (рисунок 3). Необходимо отметить, что для рисков, которые попадали в пограничное состояние между группами, окончательное решение о присвоении «группы риска» принималось респондентами на общем обсуждении.

Подобное графическое позиционирование негативных и позитивных рисковых событий друг относительно друга и знания о количестве «тигров», «аллигаторов» и «львов», актуальных для ИТ-проектов, имеет большую практическую ценность для ИТ-организаций, руководителей ИТ-проектов и проектных коллективов. Так, основываясь на данной информации, может быть формализована методическая рекомендация по формированию обязательных стимулирующих мер воздействия для 25 наиболее негативных рисков, относящихся к группе «тигры», для 30 негативных рисков – к группе «аллигаторы» и 12 позитивных рисков, которые относятся к группе «львы».

На основании проведенной апробации было установлено:

- во-первых, предложенный способ группировки рисков позволяет определять наиболее благоприятные позитивные риски, которые требуют дополнительных стимулирующих мер;
- во-вторых, способ группировки позитивных рисков оперативно идентифицирует наиболее значимые риски, существенно сокращая материальные и временные затраты на управление рисковыми событиями в ИТ-проектах;
- в-третьих, графическое представление позитивных рисков дает возможность ИТ-организациям, руководителям ИТ-проектов и проектным коллективам определить позиционирование рисковых событий друг относительно друга и судить об общем состоянии ИТ-проектов.

**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».**

В результате приращения знаний о природе риска, классификации групп рисков, актуальных для ИТ-проектов, методике определения времени актуализации рисков относительно фаз жизненного цикла, способе группировки позитивных рисков был обогащен классический инструментарий управления рисками, формализованный в ГОСТе Р ИСО 31000-2019 «Менеджмент риска: Принципы и руководство». Также в процессе анализа

методов оценки рисков, закрепленных в ГОСТе Р ИСО/МЭК 31010-2011 «Менеджмент риска: Методы оценки риска», было установлено, что общепринятые методы идентификации, анализа, оценивания и разработки мер воздействия на рисковые события требуют адаптации применительно к сфере информационных технологий. В связи с чем автором диссертационного исследования был выработан алгоритм управления рисками ИТ-проектов.

Созданный алгоритм был апробирован в семи ИТ-организациях и одиннадцати ИТ-проектах различной длительности, типов, численности проектных коллективов и способов реализации проектов (таблица 3). Данный алгоритм управления рисками ИТ-проектов базируется на национальном ГОСТе Р ИСО 31000-2019 «Менеджмент риска: Принципы и руководство» и включает в себя такие процессы, как идентификация рисков, анализ рисков, оценивание рисков, разработка мер воздействия на риски. Все процессы были адаптированы для сферы информационных технологий и обогащены знаниями, полученными в ходе диссертационного исследования.

Таблица 3 – ИТ-организации и ИТ-проекты, где была проведена экспериментальная апробация разработанного алгоритма управления рисками

| № | Название организации                 | Название проекта                 | Тип проекта | Способ реализации проекта | Количество человек в проекте | Планируемая длительность проекта, день | Размер проекта <sup>2</sup> |
|---|--------------------------------------|----------------------------------|-------------|---------------------------|------------------------------|----------------------------------------|-----------------------------|
| 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»                       | МП          | Waterfall                 | 7                            | 63                                     | Краткосрочный               |
| 5 | ООО «Контек Софт»                    | «Расчет и учет заработной платы» | ERM-система | Agile                     | 9                            | 294                                    | Среднесрочный               |
|   |                                      | «Портал логистики»               | Портал      | Agile                     | 6                            | 126                                    | Среднесрочный               |
|   |                                      | «Торговая площадка»              | ERM-система | Agile                     | 8                            | 231                                    | Среднесрочный               |
|   |                                      | «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                |

В результате апробации было установлено, что временной период, необходимый для применения алгоритма, составляет 8,2 ч.÷13,6 ч. Полученная информация может служить нормировочным критерием во время исполнения руководителем ИТ-проекта функции планирования. Также эмпирически доказано, что созданный алгоритм выявляет специфические и скрытые негативные и позитивные риски. Качество идентификации рисков проверялось по формуле 3, где  $k$  – показатель качества идентификации рисков;  $n_1$  – число

<sup>2</sup> К краткосрочным ИТ-проектам относятся проекты, трудозатраты которых составляют менее 700 человеко-часов, к среднесрочным – 700-2 500 человеко-часов, долгосрочным – более 2 500 человеко-часов.



наступивших неидентифицированных рисков;  $n_2$  – число наступивших идентифицированных рисков.

$$k = \frac{n_2}{n_1 + n_2}, \quad (3)$$

Анализ данных, представленных в таблице 4, показал:

- процесс идентификации рисков на основе разработанного алгоритма управления рисками ИТ-проектов обеспечивает высокое качество выявления как для негативных рисков, так и для позитивных, о чем свидетельствуют значения показателя  $k$ ;
- в долгосрочных ИТ-проектах возможна материализация неидентифицированных негативных рисков, в связи с чем ИТ-организациям, руководителям ИТ-проектов и проектным коллективам рекомендуется систематически повторять процесс выявления рисков с привлечением сторонних экспертов на более поздние фазы жизненного цикла (выполнение работ, завершение проекта).

Также в процессе апробации был определен экономический эффект от использования созданного алгоритма управления рисками ИТ-проектов. Для оценки экономической эффективности применялся затратный метод (формулы 4, 5 и 6, где  $E_p$  – экономический эффект от использования риск-менеджмента;  $C_p$  – затраты на риск-менеджмент;  $L_{\alpha_i}$  – фактические убытки от наступления  $i$ -го идентифицированного риска;  $H_{\alpha_i}$  – фактические расходы на обработку  $i$ -го идентифицированного риска;  $L_{\alpha_j}$  – фактические убытки от наступления  $j$ -го неидентифицированного риска;  $H_{\alpha_j}$  – 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 мероприятий «плана А» и «плана Б»).

$$E_p = R_p - C_p, \quad (4)$$

$$C_p = \left( \sum_{i=1}^N L_{\alpha_i} + \sum_{i=1}^N H_{\alpha_i} \right) + \left( \sum_{j=1}^K L_{\alpha_j} + \sum_{j=1}^K H_{\alpha_j} \right) \quad (5)$$

$$R_p = \sum_{i=1}^N M_{0_i} - \sum_{i=1}^N M_i \quad (6)$$

Таблица 4 – Оценка экономического эффекта от использования созданного алгоритма управления рисками ИТ-проектов

| №  | Название проекта                 | $C_p$ , день | $R_p$ , день | $E_p$ , день |
|----|----------------------------------|--------------|--------------|--------------|
| 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» | 43,2         | 336          | 292,8        |
| 7  | «Портал логистики»               | 10           | 135          | 125          |
| 8  | «Торговая площадка»              | 25,2         | 255          | 229,8        |
| 9  | «ТМЦ»                            | 5            | 67           | 62           |
| 10 | «DigitalTV»                      | 34,4         | 153          | 118,6        |
| 11 | «ERM-система»                    | 38,6         | 452          | 413,4        |

Таблица 5 – Результаты отклонений фактических длительностей ИТ-проектов от запланированной длительности

| №  | Название проекта                 | Планируемая длительность проекта, день | Фактическая длительность проекта, день | Отклонение фактической длительности проекта от запланированной длительности, день | Отклонение фактической длительности проекта от запланированной длительности, % |
|----|----------------------------------|----------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 1  | «Сайт ТГУ»                       | 126                                    | 189                                    | 63                                                                                | 33,3                                                                           |
| 2  | «МирКар»                         | 13                                     | 18                                     | 5                                                                                 | 27,8                                                                           |
| 3  | «HyperVibe»                      | 51                                     | 53                                     | 2                                                                                 | 3,8                                                                            |
| 4  | «Reading Log»                    | 56                                     | 67                                     | 11                                                                                | 16,4                                                                           |
| 5  | «CINEMOOD»                       | 63                                     | 63                                     | 0                                                                                 | 0,0                                                                            |
| 6  | «Расчет и учет заработной платы» | 294                                    | 336                                    | 42                                                                                | 12,5                                                                           |
| 7  | «Портал логистики»               | 126                                    | 135                                    | 9                                                                                 | 6,7                                                                            |
| 8  | «Торговая площадка»              | 231                                    | 255                                    | 24                                                                                | 9,4                                                                            |
| 9  | «ТМЦ»                            | 63                                     | 67                                     | 4                                                                                 | 6,0                                                                            |
| 10 | «DigitalTV»                      | 120                                    | 153                                    | 33                                                                                | 21,6                                                                           |
| 11 | «ERM-система»                    | 416                                    | 452                                    | 36                                                                                | 8,0                                                                            |

В ходе анализа данных (таблица 4) было установлено, что разработанный алгоритм управления рисками ИТ-проектов показал наилучшие экономические эффекты для большого проекта «ERM-система», средних проектов «Торговая площадка», «Расчет и учет заработной платы», «Портал логистики», «DigitalTV» и «Сайт ТГУ». Самые низкие показатели экономической эффективности наблюдались в малых ИТ-проектах, что может быть объяснено низкой стоимостью данных проектов и непродолжительным периодом разработки. В связи с этим можно заключить, что данный алгоритм в большей степени актуален для средних и больших ИТ-проектов, что подтверждают результаты отклонений фактических длительностей проектов от запланированных (таблица 5).

С учетом полученных результатов, предлагаемый алгоритм управления рисками может быть применен в любом ИТ-проекте независимо от типа, размера, численности проектного коллектива, способа управления проектами. Использование алгоритма гарантирует уменьшение фактической длительности и стоимости ИТ-проекта, путем превентивного воздействия на негативные/позитивные риски, способствует снижению отклонения фактических трудозатрат от запланированных, повышает шансы на успешное достижение проектных целей. Полученные эмпирические результаты подтверждены справками о внедрении диссертационного исследования, а созданный алгоритм управления рисками одобрен и внедрен в исследуемые хозяйствующие субъекты сферы ИТ. Положительные отзывы и позитивные эмпирические результаты предполагают, что созданный алгоритм обладает практической ценностью и эксплуатационным потенциалом, что является основанием для обогащения и дополнения ГОСТа Р ИСО 31000-2019 «Менеджмент риска: Принципы и руководство».

### III. ЗАКЛЮЧЕНИЕ

На основании обобщения основных результатов можно заключить, что цель диссертационного исследования достигнута. В диссертационной работе представлены разработанные автором: классификация рисков ИТ-проектов в организациях; методика определения времени актуализации рисков относительно фаз жизненного цикла с выявлением постоянных рисков, актуальных для сферы информационных технологий; группировка позитивных рисков; алгоритм управления рисками, который может быть использован в ИТ-проектах различной длительности, типов, численности проектных

коллективов и способов управления. Решены поставленные задачи: выявлены современные тенденции развития теории и практики управления ИТ-проектами и рисками в них; установлены характерные особенности негативных и позитивных рисков ИТ-проектов; проанализированы основные методы оценки рисков; разработана методика превентивного воздействия, мониторинга и контроля над негативными и позитивными рисками в ИТ-проектах; апробирован созданный методический инструментарий оценки, воздействия, мониторинга и контроля над негативными и позитивными рисками в семи ИТ-организациях и в одиннадцати ИТ-проектах.

Таким образом, результаты диссертационного исследования могут быть использованы в любом субъекте сферы ИТ, в том числе и национальных ИТ-проектах, таких как «Автоматизированная система управления транспортным комплексом», «АИС Маркировка», «ИТ-система обмена знаниями и технологиями в сфере сельского хозяйства», «ИТ-система социального обеспечения», «ИТ-система учета отходов», «ГИС-система Контингент», «Единый транспортный сервис в рамках противодействия незаконным финансовым операциям», «Автоматизированная система контроля применения контрольно-кассовой техники», а также в других 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», Распоряжения Правительства РФ от 28.06.2017 года № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»» и Постановления Правительства РФ от 02.03.2019 года №234 «О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации"».

#### **IV. ОСНОВНЫЕ НАУЧНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ**

##### **Публикации в рецензируемых научных журналах из перечня ВАК:**

1. Николаенко В. С. Проект отечественного стандарта управления рисками // Инновации в менеджменте. – 2020. - № 3 (25). – С.40-49. – 0,6 п. л. / 0,6 п. л.
2. Николаенко В. С. Риск, риск-менеджмент и неопределенность: уточнение понятий // Государственное управление. Электронный вестник. – 2020. - №81. – С.91-119. – 1,6 п. л. / 1,6 п. л.
3. Николаенко В. С. Риск-менеджмент как необходимый фактор для успешного завершения ИТ-проектов, реализуемых в рамках национальной программы «Цифровая экономика» // Государственное управление. Электронный вестник. – 2020. - №79. – С.271-295. – 1,4 п. л. / 1,4 п. л.
4. Николаенко В. С., Мирошниченко Е. А., Грицаев Р. Т. Модели зрелости управления проектами: критический обзор // Государственное управление. Электронный вестник. – 2019. – № 73. – С. 71-111. – 2,3 п. л. / 0,7 п. л.
5. Николаенко В. С. Негативные и позитивные риски в ИТ-проектах // Вестник московского университета. Серия 21: Управление (государство и общество). – 2018. – №3. – С. 91–124. – 1,9 п. л.
6. Никулина И. Е., Николаенко В. С. Государственное регулирование сферы информационных технологий в Российской Федерации // Государственное управление. Электронный вестник. – 2018. – № 67. – С. 137–149. – 0,7 п. л. / 0,4 п. л.
7. Никулина И. Е., Николаенко В. С. Становление и развитие концепций управления проектами и риск-менеджмента // Государственное управление. Электронный вестник. – 2018. – № 68. – С. 195–210. – 0,9 п. л. / 0,4 п. л.
8. Николаенко В. С. Разработка подходов классификации рисков в ИТ-проектах // государственное управление. Электронный вестник. – 2017. – № 61. – С. 36–54. – 1,1 п. л.
9. Николаенко В. С. Внедрение риск-менеджмента в ИТ-проекты // Государственное управление. Электронный вестник. – 2016. – № 54. – С. 63–88. – 1,5 п. л.
10. Николаенко В. С. Превентивный риск-менеджмент в ИТ-проектах // Государственное управление. Электронный вестник. – 2016. – №55. – С. 76–96. – 1,2 п. л.
11. Николаенко В. С. Разработка принципов управления ИТ-проектом // Вестник Томского государственного университета. – 2015. – № 390. – С. 155–160. – 0,3 п. л.

12. Николаенко В. С. Анализ инструментария по обеспечению функции управления рисками в ИТ-проектах // Государственное управление. Электронный вестник. – 2015. – №49. – С. 105–120. – 0,9 п. л.

**Публикации в научных изданиях, индексируемых в Scopus и Web of Science:**

13. Nikolaenko V. S., Petuhov O. N., Petukhova O. V., Romanovsky V. V. Special Aspects of Risk Management in IT-Projects // The 28<sup>th</sup> International Business Information Management Accusation Conference 2016 (IBIMA). – 2017. – P. 241–260. – 1,1 п. л. / 0,3 п. л.

14. Nikolaenko V. S. Riatshencev I. V. Development of Organizational Methods for Introduction of Risk Management in IT-Projects // International Conference «Responsible Research and Innovation». The European Proceeding of Social & Behavioral Science. – 2017. – Vol. XXVI. – P. 698–705. – 0,4 п. л. / 0,2 п. л.

**Учебные пособия:**

15. Николаенко В. С. Безупречный риск-менеджмент: рабочая тетрадь. – Тверь: Тверской филиал РАНХиГС; Томск. – 2018. – 92 с. – 5,3 п. л.

16. Николаенко В. С. Безупречный риск-менеджмент: практическое пособие. – Тверь: Тверской филиал РАНХиГС; Томск. – 2018. – 216 с. – 12 п. л.

**Публикации в других научных изданиях:**

17. 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. – 0,2 п. л. / 0,1 п. л.

18. Цуркан М. В., Николаенко В. С. Универсальная модель зрелости проектного управления: управление интеграцией проекта // Менеджмент сегодня. – 2019. – №2(160). – С. 150-157. – 0,4 п. л. / 0,2 п. л.

19. Дайбова К. Е., Николаенко В. С. Разработка инструментария оперативной идентификации рисков в ИТ-проектах // Ресурсоэффективным технологиям – энергию и энтузиазм молодых: сборник научных трудов VI Всероссийской конференции. – Томск: Изд-во Томского политехнического университета. – 2015. – С. 254–257. – 0,2 п. л. / 0,1 п. л.

20. Туманов М. С., Николаенко В. С. Сравнительный анализ ПО для управления рисками в ИТ-проектах // Ресурсоэффективным технологиям – энергию и энтузиазм молодых: сборник научных трудов VI Всероссийской конференции. – Томск: Изд-во Томского политехнического университета. – 2015. – С. 305–308. – 0,2 п. л. / 0,1 п. л.