

УДК 005.8:004:005.334

DOI: 10.18799/26584956/2025/3/2022

Шифр специальности ВАК: 5.2.6



Анализ универсальных рисков в ИТ-проектах

В.С. Николаенко[✉]

Томский государственный университет систем управления и радиоэлектроники,

Россия, г. Томск

Национальный исследовательский Томский политехнический университет,

Россия, г. Томск

Сибирский государственный медицинский университет, Россия, г. Томск

Национальный исследовательский Томский государственный университет,

Россия, г. Томск

[✉]valentin.s.nikolaenko@tusur.ru

Аннотация. Проведенные исследования показывают, что во время создания ИТ-продуктов могут материализоваться 105 универсальных рисков. Также было обнаружено, что одним из критериев зрелости ИТ-субъекта является наличие результативных и эффективных мер превентивного воздействия на данные риски. **Цель:** проведение анализа ранее выявленных универсальных рисков, возникающих во время создания ИТ-продуктов в рамках выполнения спринтов, фаз жизненного цикла ИТ-проектов и (или) контрактов. **Методы:** теория управления рисками и ИТ-проектами. Анализ универсальных рисков был осуществлен с помощью методов 5W, SWIFT и коэффициентов Харрингтона. **Результаты:** ИТ-субъект должен заблаговременно, до заключения контракта, проводить экспресс-оценку универсальных рисков и превентивно воздействовать на них, в том числе за счет формализации в тексте контракта действий и (или) бездействий, которые должны выполнять заинтересованные стороны для элиминирования наиболее опасных рисков. Также были разработаны схемы причинно-следственных связей универсальных комплаенс- и проектных рисков, что позволило выявить часто встречаемые и наиболее опасные рисковые события. Благодаря созданным схемам был идентифицирован негативный сценарий, который продемонстрировал наихудший вариант развития событий во время выполнения ИТ-проектов. Данный сценарий дает возможность ИТ-субъектам заблаговременно разрабатывать меры «достойного» принятия рисков, не допуская наступления наиболее радикального исхода.

Ключевые слова: управление проектами, ИТ-продукт, ИТ-проект, ИТ-субъект, риск, универсальный риск, проектный риск

Благодарности: Работа выполнена в рамках государственного задания «Наука», проект FEWM-2023-0013.

Для цитирования: Николаенко В.С. Анализ универсальных рисков в ИТ-проектах // Векторы благополучия: экономика и социум. – 2025. – Т. 53. – № 4. – С. 1–19. DOI: 10.18799/26584956/2025/3/2022

UDC 005.8:004:005.334

DOI: 10.18799/26584956/2025/3/2022



Analysis of universal risks in IT projects

V.S. Nikolaenko[✉]

Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russian Federation

National Research Tomsk Polytechnic University, Tomsk, Russian Federation

Siberian State Medical University, Tomsk, Russian Federation

Tomsk State University, Tomsk, Russian Federation

[✉]valentin.s.nikolaenko@tusur.ru

Abstract. The study conducted shows that during the creation of IT products, about 105 universal risks can materialize. It was found out as well that one of the criteria for the maturity of an IT entity in terms of creating high-quality IT products as part of the implementation of IT projects is the presence of effective and efficient preventive measures against these risks. **The aim** of the research was to analyze 105 universal risks that arise during the creation of IT products within the framework of sprints, phases of the life cycle of IT projects and (or) contracts. **The methodological basis** of the study was the theory of risk management and IT projects. The analysis of universal risks was carried out using the 5W, SWIFT and Harrington coefficients methods. **The results** of the analysis showed that the IT entity must, in advance, before concluding a contract, conduct an express assessment of universal risks and preventively affect them, including by formalizing in the text of the contract actions and (or) inactions that stakeholders must perform to eliminating the most dangerous risks. Schemes of cause-and-effect relationships of universal compliance and project risks were also created, which made it possible to identify the most common and most dangerous risk events. The created schemes allowed us to identify a negative scenario that demonstrated the worst-case option during the implementation of IT projects. This scenario allows IT entities to develop measures for «decent» risk-taking in advance, preventing the most drastic outcome.

Keywords: project management, IT product, IT project, IT entity, risk, universal risk, project risk

Acknowledgements: The work was performed within the framework of the state task «Science», the FEWM-2023-0013 project.

For citation: Nikolaenko V.S. Analysis of universal risks in IT-projects. *Journal of Wellbeing Technologies*, 2025, vol. 53, no. 4, pp. 1–19. DOI: 10.18799/26584956/2025/3/2022

Введение

Исследование, проведенное в рамках научно-исследовательского гранта РФФИ № 16-36-00031 «мол_а» в 495 ИТ-субъектах Томской области (ОКВЭД класс 62)¹, позволило установить, что во время создания ИТ-продуктов могут материализоваться 105 универсальных рисков из которых 5 – коммерческие риски, 45 – комплаенс-риски и 55 – проектные риски [1]. Под *универсальными рисками* понимаются вероятные события, актуальные для ИТ-проектов (спринтов, фаз жизненных циклов, контрактов и др.), независимо от их масштабов, сложности, длительности (краткосрочные, среднесрочные, долгосрочные), типа (ПО, мобильное приложение и др.), концепций создания ИТ-продуктов (Waterfall, Agile) и численности участников [2].

¹ Грант РФФИ №16-36-00031 «мол_а». Управление рисками в ИТ-проектах. URL: https://www.rfbr.ru/project_search/324923/ (дата обращения 10.06.2025).

Под *коммерческими рисками* понимаются любые потенциальные угрозы, которые могут помешать заказчику и другим заинтересованным сторонам получить прибыль от эксплуатации созданного ИТ-продукта. Например, присутствие на рынке нежелательных производных произведений, «пиратство», а также запрет авторов и (или) правообладателей на использование ИТ-продуктов. Несмотря на малочисленность коммерческих рисков от общего объема рисков (4,7 %), материализация одного подобного риска способна нивелировать все затраченные ресурсы и усилия, нанеся заинтересованным сторонам катастрофический материальный ущерб.

В качестве примера наступления коммерческого риска можно привести дело № А56-38522/2020², где истец просил суд солидарно взыскать с владельцев сайта *panpartner.ru* компенсацию в размере 2 млн руб. В обосновании своих требований истец заявил, что программная часть сайта «поисковый модуль» является его ИТ-продуктом. Назначенные судом эксперты пришли к выводу, что общий объем кода «поискового модуля» составляет 2669 строк, из которых 589 строк (22 %) используются сайтом без изменений, а 1522 строк (57 %) изменены частично. На основании заключения экспертов суд пришел к выводу, что владельцы сайта незаконно модифицировали «поисковый модуль», создав тем самым нежелательное производное произведение.

Другим примером материализации коммерческого риска является уголовное дело № 1-190/2016³, где подсудимый в целях сбыта и получения прибыли осуществлял установку «пиратских» копий программ Компас-3D V16, CorelDRAW X6, Microsoft Windows 7 и Microsoft Office. Своими преступными действиями подсудимый причинил правообладателям ущерб на сумму 1,6 млн руб.

Ярким примером материализации коммерческого риска является уголовное дело № 1-209/2022⁴, где виновный без соответствующего разрешения правообладателя ООО «1С-Софт» скопировал на USB-носитель файл ИТ-продукта «1С:Предприятие» и осуществил множественное копирование. Своими преступными действиями подсудимый нарушил права правообладателя ООО «1С-Софт» и причинил ущерб на общую сумму 4,2 млн руб. Суд признал подсудимого виновным и назначил ему наказание в виде 2 лет условного лишения свободы с испытательным сроком на 1 год.

В качестве иных примеров, где субъекты извлекали прибыль от неправомерного использования ИТ-продуктов принадлежащих ООО «1С», можно привести дела № А83-6393/2023⁵, № А81-11865/2022⁶, № А50-4247/2023⁷, № А36-7440/2022⁸, № А35-7078/2022⁹, № А29-10372/2022¹⁰, № А50-17729/2022¹¹, № А14-13243/2022¹² и № А08-16/2022¹³.

² Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области по делу № А56-38522/2020 от 14.04.2023 г. URL: <https://clck.ru/36d4mB> (дата обращения 10.06.2025).

³ Приговор Северского городского суда Томской области по делу 1-190/2016 от 23.06.2016 г. URL: <https://clck.ru/36VDoX> (дата обращения 10.06.2025).

⁴ Приговор Пролетарского районного суда г. Саранск Республики Мордовия по делу № 1-209/2022 от 07.09.2022 г. URL: <https://clck.ru/36eUWo> (дата обращения 10.06.2025).

⁵ Решение Арбитражного суда Республики Крым по делу № А83-6393/2023 от 18.09.2023 г. URL: <https://clck.ru/36cpZT> (дата обращения 10.06.2025).

⁶ Решение Арбитражного суда Ямало-Ненецкого автономного округа по делу № А81-11865/2022 от 13.08.2023 г. URL: <https://clck.ru/36cpoK> (дата обращения 10.06.2025).

⁷ Решение Арбитражного суда Пермского края по делу № А50-4247/2023 от 27.07.2023 г. URL: <https://clck.ru/36cpzX> (дата обращения 10.06.2025).

⁸ Решение Арбитражного суда Липецкой области по делу № А36-7440/2022 от 13.06.2023 г. URL: <https://clck.ru/36cq88> (дата обращения 10.06.2025).

⁹ Решение Арбитражного суда Курской области по делу № А35-7078/2022 от 13.03.2023 г. URL: <https://clck.ru/36d5KQ> (дата обращения 10.06.2025).

¹⁰ Решение Арбитражного суда Курской области по делу № А29-10372/2022 от 30.12.2022 г. URL: <https://clck.ru/36d5W7> (дата обращения 10.06.2025).

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

Примером привлечения субъекта к административной является дело № 5-1637/2021¹⁴, где правонарушитель незаконно использовал игровые приставки SONY «PlayStation 4 Pro» и ИТ-продукты для них в компьютерном клубе «Colizeum». Суд признал правонарушителя виновным и назначил ему наказание в виде административного штрафа в размере 15 тыс. руб. без конфискации имущества.

Если рассматривать ситуацию, связанную с претензиями со стороны лиц, чьи права и интересы были нарушены, следует упомянуть дело № А40-81328/11¹⁵, где ИТ-субъект просил суд запретить использование его ИТ-продукта «HIST DoCoMo» иным лицам и возместить причиненный ущерб в размере 124,2 млн руб.

Одним из наиболее часто встречаемых комплаенс-рисков является возможность отказа заказчика принимать и (или) оплачивать выполненную ИТ-субъектом работу. Например, в деле № А22-1042/2020¹⁶ ИТ-субъект просил суд взыскать задолженность в размере 33,6 тыс. руб. В деле № А40-162480/13¹⁷ истец просил взыскать убытки в размере 567 млн руб. В деле № А67-8506/2018¹⁸ ИТ-субъект просил суд взыскать задолженность в размере 3,5 млн руб.

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

На основании вышесказанного логично предположить, что если на стороне ИТ-субъекта разработаны результативные и эффективные меры превентивного воздействия на универсальные риски, то это свидетельствует о его высокой зрелости. Отметим, что согласно ГОСТ Р ИСО/МЭК 33001¹⁹ под результативностью (effectiveness) понимается степень реализации запланированных мероприятий и достижения запланированных результатов. В соответствии с ГОСТ ISO 9000²⁰ под эффективностью (efficiency) понимается связь между достигнутым результатом и использованными ресурсами.

¹¹ Решение Арбитражного суда Пермского края по делу № А50-17729/2022 от 28.12.2022 г. URL: <https://clck.ru/36d5id> (дата обращения 10.06.2025).

¹² Решение Арбитражного суда Воронежской области по делу № А14-13243/2022 от 07.11.2022 г. URL: <https://clck.ru/36d7f5> (дата обращения 10.06.2025).

¹³ Решение Арбитражного суда Белгородской области по делу № А08-16/2022 от 07.11.2022 г. URL: <https://clck.ru/36d7n5> (дата обращения 10.06.2025).

¹⁴ Постановление Промышленного районного суда г. Ставрополя по делу № 5-1637/2021 от 03.06.2021 г. URL: <https://clck.ru/36eUaL> (дата обращения 10.06.2025).

¹⁵ Решение Арбитражного суда города Москвы по делу № А40-81328/11 от 07.04.2014 г. URL: <https://clck.ru/nTfSN> (дата обращения 10.06.2025).

¹⁶ Решение Арбитражного суда Томской области по делу № А22-1042/2020 от 24.06.2020 г. URL: <https://clck.ru/32S3kq> (дата обращения 10.06.2025).

¹⁷ Решение Арбитражного суда города Москвы по делу № А40-162480/13 от 16.05.2014 г. URL: <https://clck.ru/jfiJj> (дата обращения 10.06.2025).

¹⁸ Решение Арбитражного суда Томской области по делу № А67-8506/2018 от 15.11.2018 г. URL: <https://clck.ru/m2UKr> (дата обращения 10.06.2025).

¹⁹ ГОСТ Р ИСО/МЭК 33001-2017. Информационные технологии. Оценка процесса. Понятия и терминология. – М.: Стандартинформ, 2017. – 16 с.

²⁰ ГОСТ ISO 9000-2011. Системы менеджмента качества. Основные положения и словарь. – М.: Стандартинформ, 2020. – 28 с.

Сформулированное выше предположение о необходимости разработки результативных и эффективных мер превентивного воздействия на риски на стороне ИТ-субъекта может быть подтверждено полученными количественными результатами, согласно которым причиненный ущерб от наступления одного комплаенс-риска в среднем составляет 277 тыс. руб. [3]. Если во время выполнения ИТ-проекта материализуются два комплаенс-риска, то ущерб удваивается и составляет 544 тыс. руб., если наступает три комплаенс-риска – утраивается (831 тыс. руб.). Следовательно, если ИТ-субъект не имеет результативных и эффективных мер превентивного воздействия на универсальные риски, то успех выполнения ИТ-проекта будет зависеть не от добросовестности, надежности, квалифицированности и зрелости данного лица, а от размера его риск-аппетита.

На основании вышесказанного целью настоящей статьи является проведение анализа универсальных рисков, возникающих во время создания ИТ-продуктов в рамках выполнения спринтов, фаз жизненного цикла ИТ-проектов и (или) контрактов. Для достижения поставленной цели были решены следующие задачи:

- 1) проведен анализ 105 универсальных рисков методом 5W;
- 2) выполнен анализ 105 универсальных рисков методом SWIFT;
- 3) реализована качественная оценка рисков с использованием коэффициентов Харрингтона.

Методы исследования

Метод 5W – это метод, который направлен на выявление причин возникновения рисков и их источников [4, 5]. Впервые метод был предложен С. Тоёда с целью увеличения качества продукции организации «Тойота» [6]. В последующем метод стал использоваться и в других сферах, в том числе и в области ИТ. Суть метода заключается в ответе на вопрос «Почему существует вероятность материализации риска?». Если причина не была установлена, тогда вопрос задается повторно. Считается, что первопричина вызывающая наступление риска (источник риска), обнаруживается при пяти итерациях поиска ответа на вопрос «Почему?».

Для анализа рисков в методе SWIFT используются вопросы: «Что, если...?», «Что случится, если...?» и «К чему это приведет...?» [7]. Ответы на эти вопросы помогают установить причинно-следственные связи между рисками, создать схемы и спрогнозировать наиболее вероятные сценарии развития событий.

Оценивание вероятности наступления рисков и возможного влияния в случаях их материализации осуществлялось по средствам экспертного мнения и коэффициентов Харрингтона [8, 9]. Примеры коэффициентов представлены в таблице 1. Для экспертной оценки были отобраны 10 респондентов из различных ИТ-организаций Томской области^{21,22,23,24,25,26,27}, имеющих высшее специальное образование и опыт практической работы в области ИТ не менее четырех лет [10].

Каждый респондент давал три вида оценки для вероятности наступления риска (Likelihood) и возможного влияния в случае его материализации (Impact) для каждого рискованного события – оптимистическую, наиболее вероятную (реалистическую) и пессимистическую.

²¹ Официальный сайт ООО «Аксимедия Софт». URL: <https://clck.ru/Tz2vs> (дата обращения 10.06.2025).

²² Официальный сайт ООО «ЛидерГрупп». URL: <http://www.lidermgrupp.ru/> (дата обращения 10.06.2025).

²³ Официальный сайт ООО «Синтез интеллектуальных систем». URL: <http://ooosis.com/promo> (дата обращения 10.06.2025).

²⁴ Официальный сайт ООО «Спейс-О технологии». URL: <http://www.spaceotechnologies.com> (дата обращения 10.06.2025).

²⁵ Официальный сайт ООО «Телебриз». URL: <http://telebreeze.ru> (дата обращения 10.06.2025).

²⁶ Официальный сайт ООО «Контек Софт». URL: <http://www.contek.ru> (дата обращения 10.06.2025).

²⁷ Официальный сайт ООО «Сибэйдж». URL: <http://sibedge.com> (дата обращения 10.06.2025).

Затем полученные оценки рассчитывались по следующим формулам:

$$\text{Likelihood}_{ij} = \frac{O_i + 4R_i + P_i}{6};$$

$$\text{Impact}_{ij} = \frac{O_i + 4R_i + P_i}{6},$$

где O_i , R_i и P_i – оптимистическая, реалистическая и пессимистическая оценка вероятности наступления риска и его влияния в случае наступления; Likelihood_{ij} – расчетное значение вероятности наступления i -риска, по мнению j -эксперта; Impact_{ij} – расчетное значение влияния в случае наступления i -риска, по мнению j -эксперта; i – номер риска; j – номер эксперта.

Таблица 1. Коэффициенты Харрингтона
Table 1. Harrington Coefficients

Вероятность/ влияние Probabilit/ influence	Коэффициент Харрингтона Harrington coefficient	Комментарии Comments
Очень высокое Very high	5	Работы в ИТ-проекте полностью остановлены. Полученный ущерб сравним с общим бюджетом ИТ-проекта. Материализация риска в ИТ-проекте гарантирована Work on the IT project has been completely stopped. The damage received is comparable to the total budget of the IT project. Risk materialization in the IT-project is guaranteed
Высокое High	4	Работы в ИТ-проекте выполнены, но с большим опозданием. Риск материализуется, но имеется шанс его избежать The work in the IT project is completed, but with a significant delay. The risk materializes in the IT-project, but there is a chance to avoid it
Среднее Average	3	Задержка в выполнении работ. Шансы, что риск материализуется в ИТ-проекте либо не наступит, одинаковы Delay in execution of works. The chances that the risk will materialize in the IT project or will not occur are the same
Низкое Low	2	Работы в ИТ-проекте выполнены с небольшим опозданием. Остается вероятность материализации риска в ИТ-проекте The work in the IT project was completed with a slight delay. There remains a possibility of risk materialization in the IT project
Очень низкое Very low	1	Незначительное отставание от запланированных целей. Вероятность наступления риска в ИТ-проекте минимальна Minor delay from planned goals. The probability of risk occurrence in the IT project is minimal
Отсутствует Absent	0	Нет материального ущерба. Вероятность наступления риска в ИТ-проекте отсутствует There is no material damage. There is no probability of risk occurring in the IT project

Анализ 105 универсальных рисков ИТ-проектов

Исследование причин наступления универсальных рисков показало, что основными источниками на стороне ИТ-субъекта являются его работники, а именно руководитель проекта (36 %), системный аналитик (7 %), юрист (5 %), субподрядчик (2 %) и другие участники (17 %). Эти обстоятельства указывают на важность привлечения к созданию ИТ-продуктов квалифицированных работников, которые должны обладать необходимыми профессиональными компетенциями. В связи с этим автор настоящей статьи предлагает в качестве превентивной меры воздействия на универсальные риски проводить проверку работников ИТ-субъекта на соответствие требованиям профессиональных стандартов по коду 06 «Связь, информационные и коммуникационные технологии» в форме систематических аттестаций.

Немаловажно отметить, что анализ табл. 2 позволил установить, что среди источников универсальных рисков на стороне ИТ-субъектов были обнаружены «процессы» (10 %) и «проектные документы» (10 %). Данные обстоятельства указывают на необходимость включения в перечень критериев, определяющих зрелость ИТ-субъекта, степень освоения требований, декларирующих порядок выполнения процессов создания ИТ-продуктов, процессов управления ИТ-проектами, а также документального сопровождения этих процессов.

Таблица 2. Источники универсальных рисков
Table 2. Sources of universal risks

№	Название источника риска Name of the risk source	Доля Share, %	Комментарий/Comment
1	Пользователь User	1	Лицо (группа лиц), которое по завершении ИТ-проекта будет использовать в своих интересах созданный ИТ-продукт [11, 12] Group of people (a person) who, upon completion of the IT project, will use the created IT product to their advantage [11, 12]
2	Конкурент Competitor	1	Лицо (группа лиц), которое соперничает за лояльность конечного пользователя с ИТ-субъектом An entity (group of entities) that competes for the loyalty of an end user with an IT entity
3	Заказчик Customer	11	Лицо (группа лиц), которое выдает задание на создание ИТ-продукта и по завершении ИТ-проекта принимает и оплачивает результат выполненной работы A person (group of persons) who issues a task to create an IT product and, upon completion of the IT project, accepts and pays for the result of the work performed
4	ИТ-субъект IT entity	87	Лицо, которое принимает заказ на создание ИТ-продукта [13] A person who accepts an order to create an IT product [13]
4.1	Руководитель проекта Project manager	36	Специалист со стороны ИТ-субъекта, который отвечает за эффективное достижение целей проекта, в рамках утвержденных заказчиком требований, бюджетов и сроков [14, 15] A specialist from an IT entity who is responsible for the effective achievement of project goals, within the framework of the requirements, budgets and deadlines approved by the customer [14, 15]
4.2	Системный аналитик Systems analyst	7	Специалист со стороны ИТ-субъекта, который отвечает за выявление и формализацию функциональных, пользовательских и бизнес-требований [16] A specialist from an IT entity who is responsible for identifying and formalizing functional, user, and business requirements [16]
4.3	Юрист/Lawyer	5	Специалист со стороны ИТ-субъекта, который отвечает за правовую чистоту выполнения контракта A specialist from the IT entity who is responsible for the legal purity of the contract execution
4.4	Другие участники проекта Other project participants	17	Группа специалистов, которая собирается на период выполнения ИТ-проекта для создания ИТ-продукта [17, 18]. Команда ИТ-проекта может включать программистов, специалистов по тестированию, администраторов баз данных, специалистов по дизайну графических пользовательских интерфейсов и др. A group of specialists that gathers for the duration of an IT project to create an IT product [17, 18]. An IT project team may include programmers, testing specialists, database administrators, graphic user interface designers, etc.
4.5	Проектные документы Project documents	10	В соответствии с требованиями ГОСТ Р 59853 ²⁸ проектная документация включает проектно-сметную, рабочую, приемочную и эксплуатационную документацию In accordance with the requirements of SS R 59853 ²⁷ , design documentation includes design and estimate, working, acceptance and operational documentation

²⁸ ГОСТ Р 59853-2021. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. – М.: Российский институт стандартизации, 2021. – 16 с.

4.6	Процессы Processes	10	Согласно отечественным стандартам ГОСТ ISO 9000, ГОСТ Р ИСО/МЭК 21827 ²⁹ , ГОСТ Р ИСО/МЭК 33001, ГОСТ Р 54869 ³⁰ и ГОСТ Р ИСО/МЭК 15504-1 ³¹ под процессом необходимо понимать совокупность действий, которые направлены на достижение определенной цели According to domestic standards SS ISO 9000, SS R ISO/IEC 21827 ²⁸ , SS R ISO/IEC 33001, SS R 54869 ²⁹ and SS R ISO/IEC 15504-1 ³⁰ , a process should be understood as a set of actions aimed at achieving a specific goal
4.7	Субподрядчик Subcontractor	2	Если из условий контракта не вытекает обязанность ИТ-субъекта создать ИТ-продукт лично, то ИТ-субъект вправе привлечь к выполнению третье лицо, то есть субподрядчика If the terms of the contract do not imply the obligation of the IT entity to create the IT product personally, then the IT entity has the right to involve a third party, i.e. a subcontractor, in the performance

Кроме того, в процессе определения причин наступления рисков методом 5W было обнаружено, что основными источниками являются заказчик, пользователь, конкурент и ИТ-субъект. Согласно квалифицированным признакам, зафиксированным в PMBOK® Guide^{32,33,34}, данные обнаруженные юридические (физические) лица, активно участвующие в проекте либо чьи интересы затрагивают ход его выполнения, принято называть заинтересованными сторонами.

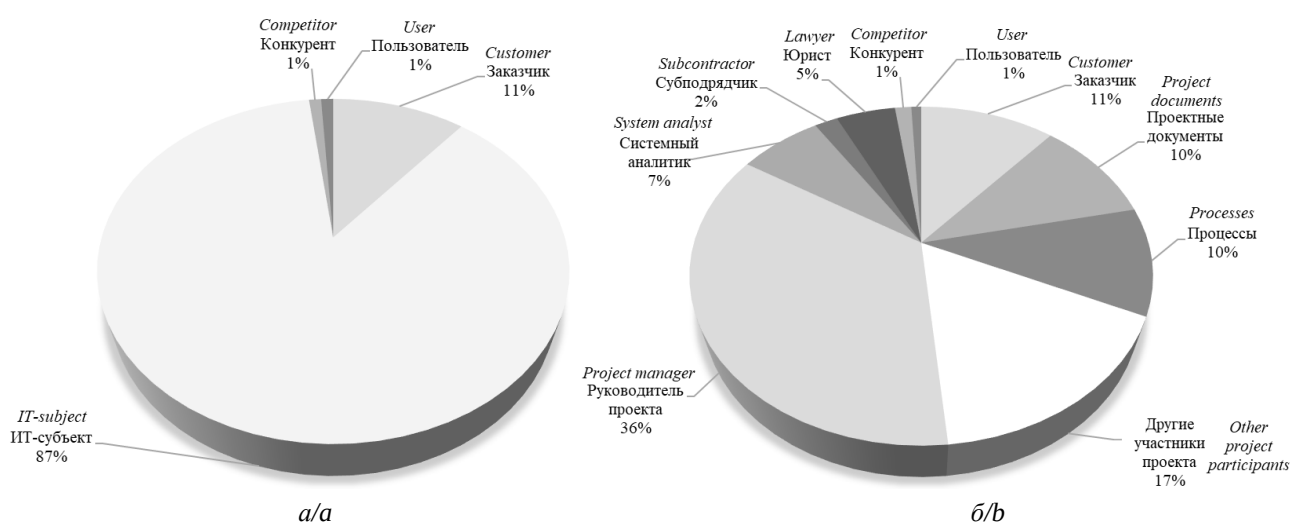


Рис. 1. Распределение источников универсальных рисков, возникающих во время создания ИТ-продуктов в рамках выполнения ИТ-проектов: а) по заинтересованным сторонам; б) с учетом декомпозиции ИТ-субъекта

Fig. 1. Distribution of sources of universal risks that arise during the creation of IT-products as part of the implementation of IT projects a) by stakeholders, b) taking into account the decomposition of the IT entity

²⁹ ГОСТ Р ИСО/МЭК 21827-2010. Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса. – М.: Стандартинформ, 2015. – 188 с.

³⁰ ГОСТ Р 54869-2011. Проектный менеджмент. Требования к управлению проектом. – М.: Стандартинформ, 2019. – 8 с.

³¹ ГОСТ Р ИСО/МЭК 15504-1-2009. Информационные технологии. Оценка процессов. Часть 1. Концепция и словарь. – М.: Стандартинформ, 2017. – 20 с.

³² Project management body of knowledge. Guide 4th edition (PMBOK-4). – Project Management Institute (PMI), 2008. – 506 p.

³³ Project management body of knowledge. Guide 5th edition (PMBOK-5). – Project Management Institute (PMI), 2013. – 616 p.

³⁴ Project management body of knowledge. Guide 6th edition (PMBOK-6). – Project Management Institute (PMI), 2017. – 756 p.

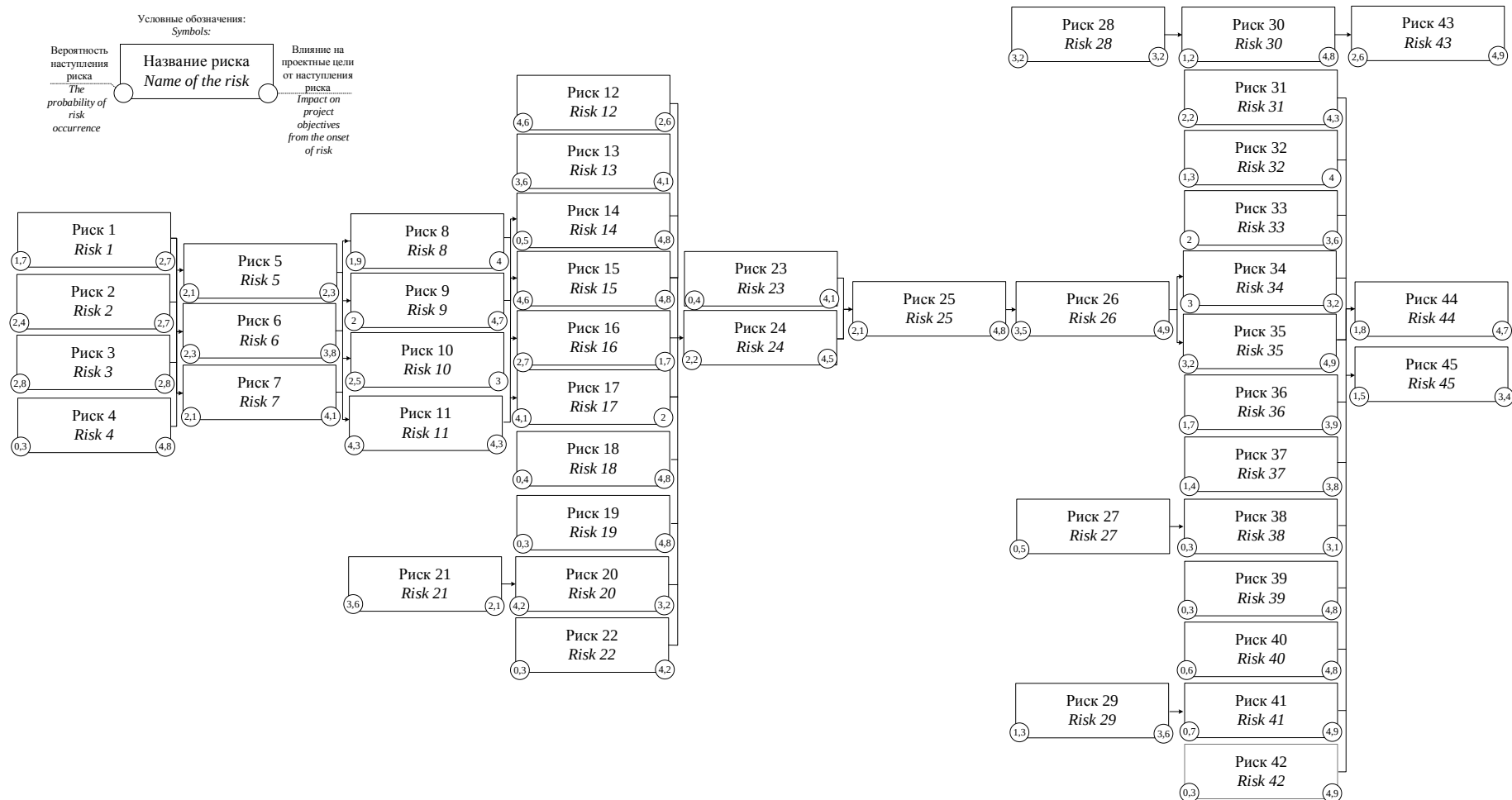


Рис. 2. Схема причинно-следственных связей универсальных комплаенс-рисков

Fig. 2. Scheme of causal relationships of universal compliance risks

Распределение источников универсальных рисков, возникающих во время создания ИТ-продуктов в рамках выполнения ИТ-проектов (рис. 1). Распределение на рис. 1, а наглядно показывает, что основными источниками универсальных рисков являются ИТ-субъект, который на заказ создает ИТ-продукт, а другой стороной – заказчик, который принимает результаты выполненных работ и оплачивает их, что подтверждает установленную ранее комплаенс-особенность разработки ИТ-продуктов, а именно «ИТ-проект – это гражданско-правовая сделка».

Необходимо подчеркнуть, что согласно действующему законодательству (гл. 37, 39 ГК РФ)³⁵ после подписания контракта ответственность за наступление всех последующих рисков несет ИТ-субъект. Однако, как показали результаты анализа универсальных рисков методом 5W, в действительности ИТ-субъект является источником универсальных рисков только на 87 %. Примерно 11 % рисков наступают по вине заказчика, 1 % конкурентов и 1 % пользователей, эксплуатирующих созданные ИТ-продукты. Это означает, что ИТ-субъект должен заблаговременно, до заключения контракта, проводить экспресс-оценку универсальных рисков и превентивно воздействовать на них, в том числе за счет формализации в тексте контракта действий и (или) бездействий (*ковенантов*), которые должны исполнять заинтересованные стороны для элиминирования наиболее опасных рисков либо их «достойного» принятия. Если сформулированное выше условие не будет выполняться, то при материализации рисков весь материальный и репутационный урон будет компенсировать сторона ИТ-субъекта.

В зависимости от особенностей создания ИТ-продуктов к числу заинтересованных сторон также могут быть отнесены руководитель продукта, спонсор проекта, генеральный подрядчик, владелец проекта и др. Согласно профессиональному стандарту код 06.012³⁶, *руководитель продукта (менеджер продукта) в области ИТ* – специалист, который осуществляет управление жизненным циклом ИТ-продуктов посредством организации их создания, вывода на рынок, продвижения, продаж и поддержки. *Спонсором проекта (куратором проекта)* является руководитель высшего звена, курирующий ИТ-проект со стороны подрядчика (исполнителя, поставщика) и обеспечивающий общий контроль [19, 20]. Согласно действующему законодательству сторона, которая на заказ выполняет работы, оказывает услуги и (или) предоставляет товары, может именоваться *генеральным подрядчиком, владельцем проекта и др.*

Анализ универсальных рисков методом SWIFT и их качественная оценка с помощью вербально-числовой шкалы Харрингтона позволили создать схемы причинно-следственных связей для комплаенс- и проектных рисков с указанием значений вероятностей наступления рисков и их возможного влияния в случаях материализации (рис. 2, 3, табл. 3–5). Благодаря созданным схемам было установлено следующее:

- **Связь между проектными и комплаенс-рисками.** Наступление проектных рисков оказывает влияние на цели ИТ-проекта (содержание, длительность, стоимость, качество), где наиболее опасными являются:
 - риск отсутствия знаний, навыков и опыта у руководителя проекта;
 - риск того, что руководитель проекта допустит ошибку при оценивании длительности проектных работ;
 - риск нерационального расходования ограниченных ресурсов проекта;
 - риск занятости руководителя проекта в других проектах;
 - риск изменения качества проекта;
 - риск изменения длительности проекта;
 - риск изменения стоимости проекта.

³⁵ Гражданский кодекс Российской Федерации (ГК РФ). Комментарий к последним изменениям. – М.: АБАК, 2019. – 752 с.

³⁶ Профессиональный стандарт 06.012 «Менеджер продуктов в области информационных технологий». URL: <https://clck.ru/PaFja> (дата обращения 10.06.2025).

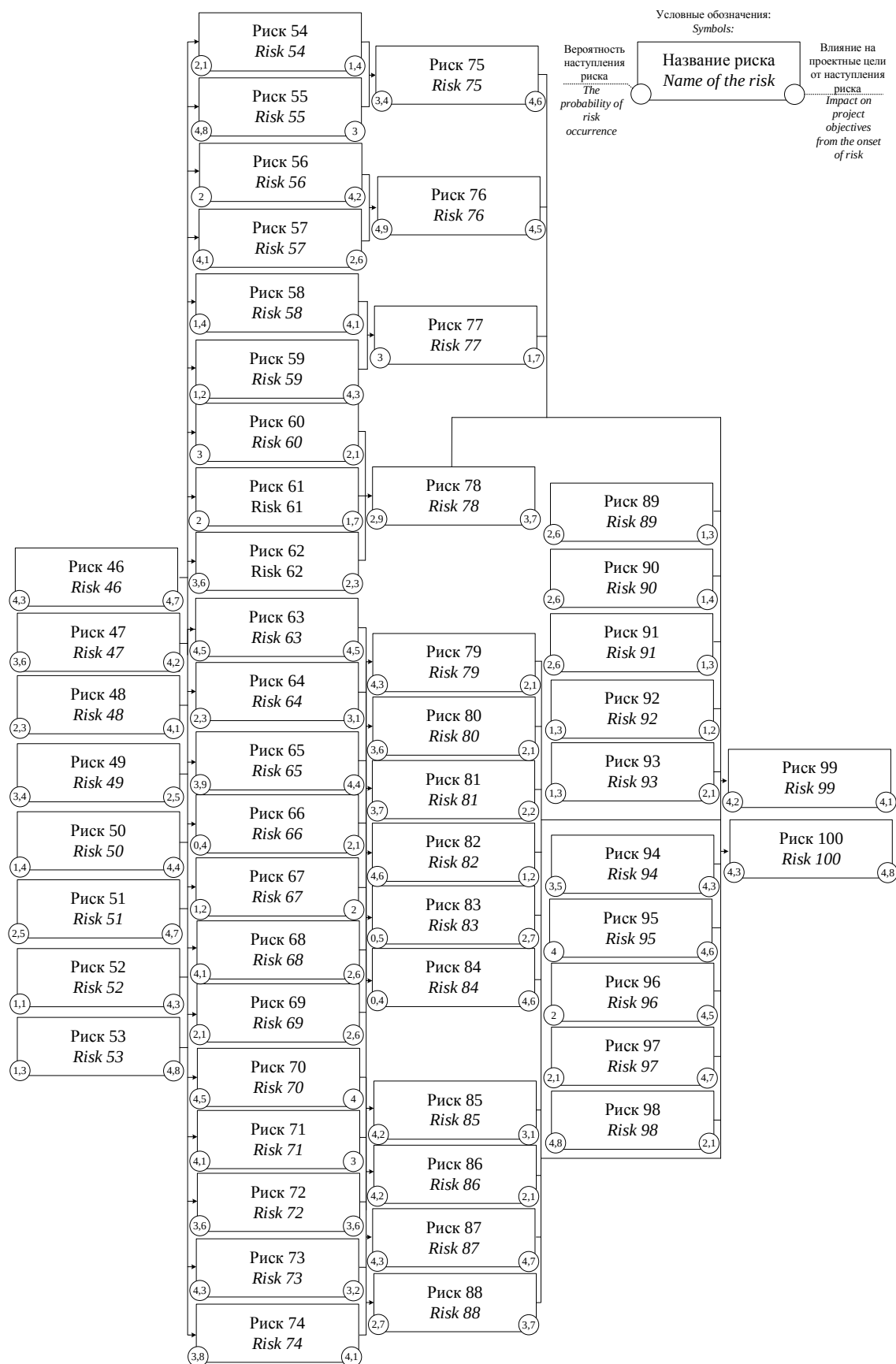


Рис. 3. Схема причинно-следственных связей универсальных проектных рисков
Fig. 3. Scheme of causal relationships of universal project risks

Таблица 3. Универсальные комплаенс-риски
Table 3. Universal compliance risks так много слова риск.

Номер риска Risk number	Описание риска Risk description
1	Риск отсутствия у заказчика корпоративной культуры, работников и опыта ведения деятельности в едином информационном пространстве The risk of the customer developing a corporate culture, manufacturers, and experience of operating in a single information space
2	Риск отсутствия у заказчика отлаженных корпоративных процедур по информационному взаимодействию The risk that the customer does not have well-established corporate procedures for information interaction
3	Риск отсутствия ключевых и квалифицированных специалистов на стороне заказчика The risk of missing key and qualified specialists on the customer's side
4	Риск реструктуризации заказчика/The risk of customer restructuring
5	Риск низкой вовлеченности заказчика в процесс выполнения работ The risk of low customer involvement in the work process
6	Риск отсутствия общего видения у заинтересованных сторон The risk of stakeholders not having a common vision
7	Риск того, что не все ключевые представители заказчика будут участвовать в создании проектных документов The risk that not all key representatives of the customer will participate in the creation of project documents
8	Риск того, что предмет договора будет сформулирован нечетко или оформлен неправильно The risk that the subject of the contract will be formulated vaguely or framed incorrectly
9	Риск допущения некорректных и неточных формулировок в тексте договора The risk of incorrect and inaccurate wording in the text of the agreement
10	Риск неверной квалификации вида сделки/The risk of incorrect qualification of the type of transaction
11	Риск того, что спецификация будет недостаточно полной, будет содержать недостоверные данные или не будет соответствовать национальным стандартам The risk that the specification will not be complete enough, will contain inaccurate data, or will not meet national standards
12	Риск отсутствия связи с заказчиком/The risk of lack of communication with the customer
13	Риск того, что заказчик вовремя не предоставит или вовсе не предоставит нужные данные для выполнения работ The risk that the customer will not provide the necessary data on time or not at all to complete the work
14	Риск того, что сделка между сторонами будет признана недействительной The risk that the transaction between the parties will be declared invalid
15	Риск изменения требований в процессе выполнения работ The risk of changing requirements during the execution of work
16	Риск того, что подрядчик не справится с обязательствами по договору The risk that the contractor will fail to meet its obligations under the contract
17	Риск выявления подрядчиком скрытых, не обнаруженных на этапе планирования источников дополнительных затрат The risk of the contractor identifying hidden sources of additional costs that were not discovered at the planning stage
18	Риск гибели и (или) повреждения электронного оборудования и другого имущества в результате пожара, затопления водой и т. д. The risk of death and/or damage to electronic equipment and other property as a result of fire, water flooding, etc.
19	Риск гибели и (или) повреждения электронного оборудования и другого имущества в результате противоправных действий третьих лиц The risk of death and/or damage to electronic equipment and other property as a result of illegal actions by third parties
20	Риск того, что результат, полученный субподрядчиком, не оправдает ожиданий всех заинтересованных сторон The risk that the result obtained by the subcontractor will not meet the expectations of all stakeholders

21	Риск отсутствия связи с субподрядчиком Risk of lack of communication with the subcontractor
22	Риск материализации обстоятельств непреодолимой силы, которые могут оказать значительное влияние на ход выполнения работ The risk of materialization of force majeure circumstances that may have a significant impact on the progress of work
23	Риск того, что подрядчик будет скрывать реальное положение дел или искажать факты The risk that the contractor will conceal the real state of affairs or distort the facts
24	Риск того, что подрядчик не выполнит свои обязательства по договору The risk that the contractor will not fulfill its obligations under the contract
25	Риск того, что работа не оправдает ожиданий заказчика The risk that the work will not meet the customer's expectations
26	Риск того, что заказчик откажется принимать выполненную работу The risk that the customer will refuse to accept the completed work
27	Риск того, что будут ограничения для последующих сублицензионных договоров The risk that there will be restrictions on subsequent sublicense agreements
28	Риск изменения норм действующего законодательства The risk of changing the norms of the current legislation
29	Риск нарушения исключительных прав на результаты интеллектуальной деятельности The risk of infringement of exclusive rights to the results of intellectual activity
30	Риск нарушения норм действующего законодательства The risk of violating the norms of current legislation
31	Риск распространения сведений, порочащих деловую репутацию подрядчика The risk of spreading information discrediting the contractor's business reputation
32	Риск промышленного шпионажа/The risk of industrial espionage
33	Риск утечки конфиденциальных данных/Risk of confidential data leakage
34	Риск просрочки оплаты за выполненную подрядчиком работу The risk of late payment for the work performed by the contractor
35	Риск того, что заказчик откажется платить за выполненную работу The risk that the customer will refuse to pay for the work performed
36	Риск того, что сделку нельзя будет расторгнуть досрочно и в одностороннем порядке The risk that the transaction cannot be terminated prematurely and unilaterally
37	Риск того, что стороны не смогут договориться о том, как делить сэкономленные деньги за уже выполненные работы The risk that the parties will not be able to agree on how to share the money saved for the work already done
38	Риск расторжения договора в «сублицензионной цепочке» договоров The risk of contract termination in the «sublicense chain» of contracts
39	Риск создания нежелательного производного произведения The risk of creating an undesirable derivative work
40	Риск взыскания правообладателем вознаграждения за использование его исключительных прав на результат интеллектуальной деятельности The risk of the rightholder collecting remuneration for the use of his exclusive rights to the result of intellectual activity
41	Риск того, что автор запретит использовать результаты интеллектуальной деятельности The risk that the author will prohibit the use of the results of intellectual activity
42	Риск того, что будет невозможно признать исключительное право на результат интеллектуальной деятельности за правообладателем (автором) The risk that it will be impossible to recognize the exclusive right to the result of intellectual activity for the copyright holder (author)
43	Риск получения штрафа за нарушение действующего законодательства The risk of receiving a fine for violating current legislation
44	Риск судебного иска от заказчика (подрядчика, исполнителя, поставщика) The risk of legal action from the customer (contractor, contractor, supplier)
45	Риск судебного иска от субподрядчика The risk of legal action from a subcontractor

Таблица 4. Универсальные проектные риски
Table 4. Universal project risks

Номер риска Risk number	Описание риска Risk description
46	Риск отсутствия знаний, навыков и опыта у руководителя проекта Risk of lack of knowledge, skills and experience of the project manager
47	Риск отсутствия у участников проекта знаний, навыков и опыта, необходимых для реализации требований The risk of the project participants' lack of knowledge, skills and experience necessary to implement the requirements
48	Риск отсутствия в проекте инструментария управления проектом The risk of missing project management tools in the project
49	Риск того, что информация о материализовавшихся рисках будет не сохранена The risk that information about materialized risks will not be saved
50	Риск привлечения в проект руководителя проекта, который имеет профессиональное образование в области управления проектами The risk of involving a project manager who has a professional background in project management in the project
51	Риск привлечения в проект руководителя проекта, который имеет опыт управления проектами более 2 лет The risk of involving a project manager who has more than two years of project management experience in the project
52	Риск того, что руководитель проекта будет самостоятельно подбирать команду The risk that the project manager will select the team independently
53	Риск того, что в проект будет привлечен высококвалифицированный работник The risk that a highly qualified employee will be involved in the project
54	Риск непонимания участниками проекта того, какой результат должен быть получен по завершении проекта The risk of project participants not understanding what result should be achieved at the end of the project
55	Риск того, что проектные работы окажутся гораздо сложнее, чем предполагалось The risk that the design work will turn out to be much more difficult than expected
56	Риск завышения качества/The risk of overestimation of quality
57	Риск того, что участники проекта допустят ошибки при его реализации The risk of making mistakes by the project participants during the project implementation
58	Риск конфликта интересов между заинтересованными сторонами Risk of conflict of interest between stakeholders
59	Риск конфликта между руководителем проекта и заинтересованными сторонами Risk of conflict between the project manager and stakeholders
60	Риск эффекта Кассандры/The risk of the Cassandra effect
61	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений The risk of prolonged coordination of information by stakeholders in the development of management decisions
62	Риск значительной временной задержки в получении ответов на задаваемые вопросы между участниками проекта The risk of a significant time delay in getting answers to the questions asked between the project participants
63	Риск того, что руководитель проектов допустит ошибку в оценке сроков выполнения задач The risk that the project manager will make a mistake in estimating the deadlines for completing tasks
64	Риск неправильного ранжирования задач/The risk of incorrect task ranking
65	Риск потери и (или) отсутствия контроля/The risk of loss and/or lack of control
66	Риск отсутствия заинтересованности у участников проекта в успешном завершении проекта The risk of project participants' lack of interest in the successful completion of the project
67	Риск отсутствия заинтересованности у руководителя проекта в успешном завершении проекта The risk of the project manager's lack of interest in the successful completion of the project
68	Риск низкой производительности труда у руководителя проекта The risk of low productivity for the project manager

69	Риск низкой производительности труда у участников проекта The risk of low productivity among the project participants
70	Риск того, что руководитель проекта допустит ошибку в оценке стоимости проектных работ The risk that the project manager will make a mistake in estimating the cost of the project work
71	Риск того, что руководитель проекта допустит неточность при оценке ресурсов The risk that the project manager will make inaccuracies in estimating resources
72	Риск того, что команда проекта неверно рассчитает объем работы и время, которое потребуется для выполнения задач The risk that the project team will incorrectly calculate the amount of work and the time it will take to complete the tasks
73	Риск того, что участники проекта неверно осуществлять дифференциацию задач There is a risk that the project participants will incorrectly differentiate tasks
74	Риск изменения состава участников проекта в процессе реализации проекта The risk of changing the project team during the project implementation process
75	Риск изменения содержания проекта/The risk of changing the content of the project
76	Риск изменения качества проекта/The risk of project quality changes
77	Риск негативной социально-психологической атмосферы The risk of a negative socio-psychological atmosphere
78	Риск недостатка коммуникаций между участниками проекта The risk of a lack of communication between the project participants
79	Риск того, что фактическое время работы участников проектов будет менее 8 часов в день The risk that the actual working hours of the project participants will be less than 8 hours per day
80	Риск неучета отпусков и государственных праздников при создании плана проекта The risk of not accounting for vacations and public holidays when creating a project plan
81	Риск простоя трудовых ресурсов/Risk of labor downtime
82	Риск нескоординированных действий участников проекта The risk of uncoordinated actions by project participants
83	Риск того, что в проекте будут участвовать более 6 человек The risk that more than 6 people will participate in the project
84	Риск привлечения в проект сторонних экспертов и советников The risk of involving third-party experts and advisors in the project
85	Риск отсутствия ресурсов, необходимых для выполнения проектных работ The risk of not having the resources needed to carry out the project work
86	Риск перегрузки трудовых ресурсов/Risk of labor overload
87	Риск нерационального расходования ограниченных ресурсов проекта The risk of irrational expenditure of limited project resources
88	Риск отсутствия резервов, необходимых для принятия материализовавшихся рисков The risk of not having the reserves necessary to take materialized risks
89	Риск отключения Интернета/The risk of Internet disconnection
90	Риск применения ранее не используемых технологий The risk of using previously unused technologies
91	Риск отключения электричества/Risk of power outage
92	Риск коллаборации руководителя проекта с участниками проекта The risk of collaboration between the project manager and the project participants
93	Риск использования устаревших технологий участниками проекта The risk of outdated technologies being used by project participants
94	Риск занятости участников проекта в других проектах The risk of employment of project participants in other projects
95	Риск занятости руководителя проекта в других проектах The risk of the project manager's employment in other projects
96	Риск ухода руководителя проекта из проекта The risk of the project manager leaving the project
97	Риск ухода ключевого работника из проекта/The risk of a key employee leaving the project
98	Риск ухода на больничный участника проекта The risk of a project participant going on sick leave
99	Риск изменения длительности проекта/The risk of changing the duration of the project
100	Риск изменения стоимости проекта/Risk of project cost changes

Таблица 5. Универсальные коммерческие (предпринимательские) риски**Table 5. Universal commercial risks**

Номер риска Risk number	Описание риска Risk description
101	Риск того, что выполненная работа не будет соответствовать ожиданиям клиента The risk that the work performed will not meet the client's expectations
102	Риск низкой вовлеченности клиента в процесс выполнения работы The risk of low client involvement in the work process
103	Риск того, что выполненная работа не принесет ожидаемый коммерческий эффект The risk that the work performed will not bring the expected commercial effect
104	Риск того, что конкуренты будут оказывать влияние на ход выполнения работы The risk that competitors will influence the progress of work
105	Риск того, что товары-субституты будут оказывать влияние на ход выполнения работы The risk that substitute products will affect the progress of work

Наступление этих проектных рисков значительно повышает вероятность изменения существенных условий контракта и провоцирует наступление комплаенс-рисков. Выявленные часто встречаемые и наиболее опасные проектные риски представляют определенную практическую ценность для ИТ-субъектов, так как их заблаговременное элиминирование снижает вероятность перехода отношений между заинтересованными сторонами в негативную комплаенс-плоскость.

- **Негативный сценарий развития событий.** Отсутствие квалифицированных работников приводит → к отсутствию общего видения итогового ИТ-продукта у заинтересованных сторон → к тому, что ТЗ и другие проектные документы являются неполными, недостоверными либо отсутствующими → к изменению требований в процессе создания ИТ-продукта → к неисполнению обязательств, предусмотренных контрактом → к отказу от исполнения условий контракта → к судебному разбирательству. Данный выявленный сценарий позволяет увидеть картину наихудшего варианта развития событий в рамках выполнения ИТ-проектов.

Требуется отметить, что ИТ-субъектам рекомендуется руководствоваться реестром универсальных рисков для оценки результативности и эффективности мер превентивного воздействия на них. Однако для элиминирования данных возможных универсальных проблем от ИТ-субъектов требуется проведение идентификации своих «универсальных» рисков, так как специфика создания ИТ-продуктов при выполнении спринтов, фаз жизненного цикла ИТ-проектов и (или) контрактов, а также факторы внешней среды будут оказывать воздействие не только на количество рисков, но и на значения их вероятностей и влияний.

Заключение

На основании проведенного анализа универсальных рисков с помощью методов 5W, SWIFT и коэффициентов Харрингтона были получены следующие результаты:

- Одним из критериев, оценивающих зрелость ИТ-субъекта, являются разработанные результативные и эффективные меры воздействия на универсальные риски. Было установлено, что одна из превентивных мер, обеспечивающих результативное и эффективное воздействие на подобные риски, – проверка работников ИТ-субъекта на соответствие требованиям профессиональных стандартов по коду 06 «Связь, информационные и коммуникационные технологии» в форме систематических аттестаций.

Кроме того, было установлено, что ИТ-субъект должен заблаговременно, до заключения контракта, проводить экспресс-оценку универсальных рисков и превентивно воздействовать на них, в том числе за счет формализации в тексте контракта действий и

(или) бездействий (ковенантов), которые должны выполнять заинтересованные стороны для элиминирования наиболее опасных рисков либо их «достойного» принятия. Другими критериями являются степень освоения требований, декларирующих порядок выполнения процессов создания ИТ-продуктов, процессов управления ИТ-проектами, а также степень освоения требований, закрепляющих документальное сопровождение этих процессов.

- Созданы схемы причинно-следственных связей универсальных комплаенс- и проектных рисков, что позволило выявить часто встречаемые и наиболее опасные рисковые события. Превентивное элиминирование данных рисков дают возможность ИТ-субъектам снизить вероятность перехода отношений между заинтересованными сторонами в негативную комплаенс-плоскость. Также благодаря созданным схемам был идентифицирован негативный сценарий, который показывает наихудший вариант развития событий во время выполнения ИТ-проектов. Выявленный сценарий дает возможность ИТ-субъектам заблаговременно разрабатывать меры «достойного» принятия рисков, не допуская наступления наиболее радикального исхода.

Полученные результаты выявляют необходимость проведения дальнейшего анализа бизнес-деятельности ИТ-субъектов в части освоения требований, декларирующих порядок выполнения процессов создания ИТ-продуктов, процессов управления ИТ-проектами, а также требований, закрепляющих документальное сопровождение этих процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Николаенко В.С. Негативные и позитивные риски в ИТ-проектах // Вестник московского университета. Серия 21: Управление (государство и общество). – 2018. – № 3. – С. 91–124.
2. Paladino B., Cuy L., Frigo M. Missed opportunities in performance and enterprise risk management // Journal of Corporate Accounting & Finance. – 2009. – № 20 (3). – P. 43–51. DOI: <https://doi.org/10.1002/jcaf.20483>.
3. Nikolaenko V., Sidorov A. Analysis of 105 IT project risks // Journal of Risk and Financial Management. – 2023. – Vol. 16. – Iss. 1. – article number 33. DOI: <https://doi.org/10.3390/jrfm16010033>. EDN: UOEIOH.
4. Wijayanti D., Sukwika T., Ramli S. Analisis Insiden Fatality Akibat Covid-19 Menggunakan Metode 5 Why, SCAT, BowTie, dan Interpretive Structural Model (ISM) // Jurnal Migasian. – 2022. – № 6 (1). – S. 84–92.
5. Ефимов В.В. Сборник методов поиска новых идей и решений управления качеством. – Ульяновск: УлГТУ, 2011. – 194 с.
6. Sahu R., Choudhari B. R., Yadav S. Usages of six sigma in library services // Conference: Library as a Medium of Communication. – 2022. URL: https://www.researchgate.net/publication/364011786_Usages_of_six_sigma_in_library_services (дата обращения 14.04.2025).
7. Card A., Ward J., Clarkson P. Beyond FMEA: the structured what-if technique (SWIFT) // Journal of Healthcare Risk Management. – 2012. – Vol. 31. – Iss. 4. – P. 23–29. DOI: <https://doi.org/10.1002/jhrm.20101>.
8. E-commerce sales revenues forecasting by means of dynamically designing, developing and validating a directed acyclic graph (DAG) network for deep learning / D. Petroşanu, A. Pirjan, G. Căruţaşu, A. Tăbuşcă, D. Zîră, A. Perju-Mitran // Electronics. – 2022. – Vol. 11. – Iss. 18. – article number 2940. DOI: <https://doi.org/10.3390/electronics11182940>.
9. Wind speed analysis of hurricane sandy / P. Martínez, I. Pérez, M. Sánchez, M. García, N. Pardo // Atmosphere. – 2021. – Vol. 12. – Iss. 11. – article number 1480. DOI: <https://doi.org/10.3390/atmos12111480>.
10. Николаенко В.С. Превентивный риск-менеджмент в ИТ-проектах // Государственное управление. Электронный вестник. – 2016. – № 55. – С. 76–96.
11. Миронов В. Профессия «бизнес-аналитик». – М.: Олимп-Бизнес, 2022. – 238 с.
12. Mazur K., Saleh M., Hornung M. Integrating life cycle assessment in conceptual aircraft design: a comparative tool analysis // Aerospace. – 2024. – Vol. 11. – Iss. 1. – article number 101. DOI: <https://doi.org/10.3390/aerospace11010101>.
13. Approach to formalizing software projects for solving design automation and project management tasks / A. Filippov, A. Romanov, A. Skalkin, J. Stroeve, N. Yarushkina // Software. – 2023. – Vol. 2. – Iss. 1. – P. 133–162. DOI: <https://doi.org/10.3390/software2010006>.
14. How to simplify life cycle assessment for industrial applications – a comprehensive review / S. Kiemel, C. Rietdorf, M. Schutzbach, R. Mieke // Sustainability. – 2022. – Vol. 14. – Iss. 23. – article number 15704. DOI: <https://doi.org/10.3390/su142315704>.

15. Mission-based cybersecurity test and evaluation of weapon systems in association with risk management framework / I. Kim, S. Kim, H. Kim, D. Shin // *Symmetry*. – 2022. – Vol. 14. – Iss. 11. – article number 2361. DOI: <https://doi.org/10.3390/sym14112361>.
16. Menezes T.A. Review to find elicitation methods for business process automation software // *Software*. – 2023. – Vol. 2. – Iss. 2. – P. 177–196. DOI: <https://doi.org/10.3390/software2020008>.
17. Automated cyber and privacy risk management toolkit / G. Gonzalez-Granadillo, S.A. Menesidou, D. Papamartzivanos, R. Romeu, D. Navarro-Llobet, C. Okoh, S. Nifakos, C. Xenakis, E. Panaousis // *Sensors*. – 2021. – Vol. 21. – Iss. 16. – article number 5493. DOI: <https://doi.org/10.3390/s21165493>.
18. Gupta V., Fernandez-Crehuet J.M., Hanne T. Freelancers in the software development process: a systematic mapping study // *Processes*. – 2020. – Vol. 8. – Iss. 10. – article number 1215. DOI: <https://doi.org/10.3390/pr8101215>.
19. Вигерс К., Битти Д. Разработка требований к программному обеспечению. – СПб.: БХВ, 2022. – 736 с.
20. Kuhail M.A., Lauesen S. User story quality in practice: a case study // *Software*. – 2022. – Vol. 1. – Iss. 3. – P. 223–243. DOI: <https://doi.org/10.3390/software1030010>.

Информация об авторе

Валентин Сергеевич Николаенко, кандидат экономических наук, доцент кафедры автоматизации обработки информации факультета систем управления Томского государственного университета систем управления и радиоэлектроники, Россия, 634050, г. Томск, пр. Ленина, 40; доцент отделения управления бизнесом и инновациями Бизнес-школы Национального исследовательского Томского политехнического университета, Россия, 634050, г. Томск, пр. Ленина, 30; доцент кафедры экономики, социологии, политологии и права Института интегративного здравоохранения Сибирского государственного медицинского университета, Россия, 634050, г. Томск, Московский тракт, 2; доцент кафедры управления качеством факультета инновационных технологий Национального исследовательского Томского государственного университета, Россия, 634050, г. Томск, пр. Ленина, 36; valentin.s.nikolaenko@tusur.ru

Поступила в редакцию: 19.06.2025

Поступила после рецензирования: 13.09.2025

Принята к публикации: 21.09.2025

REFERENCES

1. Nikolaenko V.S. Negative and positive risks in IT projects. *Bulletin of Moscow University. Series 21: Management (State and Society)*, 2018, no. 3, pp. 91–124. (In Russ.)
2. Paladino B., Cuy L., Frigo M. Missed opportunities in performance and enterprise risk management. *Journal of Corporate Accounting & Finance*, 2009, no. 20 (3), pp. 43–51. DOI: <https://doi.org/10.1002/jcaf.20483>.
3. Nikolaenko V., Sidorov A. Analysis of 105 IT Project Risks. *Journal of Risk and Financial Management*, 2023, vol. 16, Iss. 1, article number 33. DOI: <https://doi.org/10.3390/jrfm16010033>. EDN: UOEIOH.
4. Wijayanti D., Sukwika T., Ramli S. Analisis Insiden Fatality Akibat Covid-19 Menggunakan Metode 5 Why, SCAT, BowTie, dan Interpretive Structural Model (ISM). *Jurnal Migasian*, 2022, no. 6 (1), pp. 84–92.
5. Efimov V.V. *Collection of methods for searching for new ideas and solutions for quality management*. Ulyanovsk, Ulyanovsk State Technical University Press, 2011. 194 p. (In Russ.)
6. Sahu R., Choudhari B.R., Yadav S. Usages of six sigma in library services. *Conference: Library as a Medium of Communication*, 2022. Available at: https://www.researchgate.net/publication/364011786_Usages_of_six_sigma_in_library_services (accessed 14 April 2025).
7. Card A., Ward J., Clarkson P. Beyond FMEA: the structured what-if technique (SWIFT). *Journal of Healthcare Risk Management*, 2012, vol. 31, Iss. 4, pp. 23–29. DOI: <https://doi.org/10.1002/jhrm.20101>.
8. Petroșanu D., Pirjan A., Cărușu G., Tăbușcă A., Zirra D., Perju-Mitran A. E-commerce sales revenues forecasting by means of dynamically designing, developing and validating a directed acyclic graph (DAG) network for deep learning. *Electronics*, 2022, vol. 11, Iss. 18, article number 2940. DOI: <https://doi.org/10.3390/electronics11182940>.
9. Martínez P., Pérez I., Sánchez M., García M., Pardo N. Wind speed analysis of hurricane sandy. *Atmosphere*, 2021, vol. 12, Iss. 11, article number 1480. DOI: <https://doi.org/10.3390/atmos12111480>.
10. Nikolaenko V.S. Preventive risk management in IT-projects. *Public Administration. Electronic newsletter*, 2016, no. 55, pp. 76–96. (In Russ.)
11. Mironov V. *Profession «business analyst»*. Moscow, Olimp-Business Publ., 2022. 238 p. (In Russ.)
12. Mazur K., Saleh M., Hornung M. Integrating Life cycle assessment in conceptual aircraft design: a comparative tool analysis. *Aerospace*, 2024, vol. 11, Iss. 1, article number 101. DOI: <https://doi.org/10.3390/aerospace11010101>.

13. Filippov A., Romanov A., Skalkin A., Stroeve J., Yarushkina N. Approach to formalizing software projects for solving design automation and project management tasks. *Software*, 2023, vol. 2, Iss. 1, pp. 133–162. DOI: <https://doi.org/10.3390/software2010006>.
14. Kiemel S., Rietdorf C., Schutzbach M., Miehe R. How to simplify life cycle assessment for industrial applications – a comprehensive review. *Sustainability*, 2022, vol. 14, Iss. 23, article number 15704. DOI: <https://doi.org/10.3390/su142315704>.
15. Kim I., Kim S., Kim H., Shin D. Mission-based cybersecurity test and evaluation of weapon systems in association with risk management framework. *Symmetry*, 2022, vol. 14, Iss. 11, article number 2361. DOI: <https://doi.org/10.3390/sym14112361>.
16. Menezes T.A. Review to find elicitation methods for business process automation software. *Software*, 2023, vol. 2, Iss. 2, pp. 177–196. DOI: <https://doi.org/10.3390/software2020008>.
17. Gonzalez-Granadillo G., Menesidou S. A., Papamartzivanos D., Romeu R., Navarro-Llobet D., Okoh C., Nifakos S., Xenakis C., Panaousis E. Automated cyber and privacy risk management toolkit. *Sensors*, 2021, vol. 21, Iss. 16, article number 5493. DOI: <https://doi.org/10.3390/s21165493>.
18. Gupta V., Fernandez-Crehuet J.M., Hanne T. Freelancers in the software development process: a systematic mapping study. *Processes*, 2020, vol. 8, Iss. 10, article number 1215. DOI: <https://doi.org/10.3390/pr8101215>.
19. Wiegers K., Beatty D. *Development of software requirements*. St Petersburg, BKhV Publ., 2022. 736 p. (In Russ.)
20. Kuhail M.A., Lauesen S. User story quality in practice: a case study. *Software*, 2022, vol. 1, Iss. 3, pp. 223–243. DOI: <https://doi.org/10.3390/software1030010>.

Information about the author

Valentin S. Nikolaenko, Cand. Sc., Associate Professor, Tomsk State University of Control Systems and Radio-electronics, 40, Lenin avenue, Tomsk, 634050, Russian Federation; Associate Professor, National Research Tomsk Polytechnic University, 30, Lenin avenue, Tomsk, 634050, Russian Federation; Associate Professor, Siberian State Medical University, 2, Moskovsky Tract, Tomsk, 634050, Russian Federation; Tomsk State University, 36, Lenin avenue, Tomsk, 634050, Russian Federation; valentin.s.nikolaenko@tusur.ru

Received: 19.06.2025

Revised: 13.09.2025

Accepted: 21.09.2025