DOI: 10.17747/2618-947X-2025-2-125-133
УДК 004.01
JEL M15

Снижение рисков при создании ИТ-продуктов: формирование критериев добросовестности для ИТ-субъектов

В.С. Николаенко[1, 2, 3, 4]
[1] Томский государственный университет систем управления и радиоэлектроники (Томск, Россия)
[2] Томский политехнический университет (Томск, Россия)
[3] Сибирский государственный медицинский университет (Томск, Россия)
[4] Томский государственный университет (Томск, Россия)

Аннотация
В статье рассматривается суть и природа добросовестного поведения ИТ-субъектов, которые готовы гарантировать создание высококачественных ИТ-продуктов в рамках выполнения ИТ-проектов, а также снижение до минимальных значений вероятность наступления нежелательных комплаенс-последствий для всех участников отношений и иных заинтересованных сторон. Для достижения поставленной цели автором настоящей статьи был проведен анализ признаков добросовестного и недобросовестного поведения участников отношений, в том числе была изучена судебная практика, связанная с защитой прав от недобросовестного поведения контрагентов. На основании проведенного исследования были сформулированы критерии добросовестности ИТ-субъектов, а именно отсутствие умысла на причинение материального ущерба заинтересованным сторонам и наличие эффективной и результативной системы управления рисками. Было установлено, что наличие умысла на причинение вреда характеризуется не только текущим поведением ИТ-субъектов (включение в контракт явно обременительных условий, сознательное нарушение норм действующего законодательства, использование некомпетентности участников сделки им во вред и др.), но и недобросовестными действиями, которые они совершали ранее в прошлых сделках. Также было обнаружено, что ответственность за реализацию превентивных мер по митигации рисков возложена на сторону, которая берет на себя обязательства выполнить работу по созданию ИТ-продукта. В частности, проведенное исследование показало, что если ИТ-субъекты заблаговременно, до заключения контрактов, превентивно не воздействуют на 105 универсальных рисков, то во время выполнения работ заинтересованные стороны с большой вероятностью столкнутся с комплаенс-последствиями, которые смогут негативно повлиять на процесс достижения проектных целей и причинить этим сторонам значительный материальный ущерб.
Ключевые слова: ИТ-продукт, ИТ-проект, риск

Для цитирования:
Николаенко В.С. (2025). Снижение рисков при создании ИТ-продуктов: формирование критериев добросовестности для ИТ-субъектов. *Стратегические решения и риск-менеджмент,* 16(2): 125–133. DOI: 10.17747/2618-947X-2025-2-125-133.

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

Reducing risks when creating IT products: Developing integrity criteria for IT entities

V.S. Nikolaenko[1, 2, 3, 4]
[1] Tomsk State University of Control Systems and Radioelectronics (Tomsk, Russia)
[2] Tomsk Polytechnic University (Tomsk, Russia)
[3] Siberian State Medical University (Tomsk, Russia)
[4] Tomsk State University (Tomsk, Russia)

Abstract
The article examines the nature and essence of conscientious behaviour by IT entities willing to guarantee the production of high-quality IT products within the framework of projects and minimise the likelihood of undesirable consequences for all participants and other stakeholders. To achieve this goal, the article analyses the signs of good faith and unfair behaviour by parties involved in relationships, including judicial practice related to protecting rights against unfair conduct by counterparties. Based on this research, criteria were formulated for the integrity of IT entities, such as the absence of intent to cause material harm to interested parties and the existence of an effective risk management system. It was discovered that the intent to harm is not only characterised by the current practices of IT companies (including the use of clearly onerous terms in contracts, the deliberate violation of existing legislation, and the exploitation of the ignorance of transaction participants), but also by the unfair actions taken in previous transactions. It was also found that responsibility for taking preventative measures to reduce risks is assigned to the parties involved in producing an IT product. In particular, research has shown that if IT companies do not proactively influence other companies before entering into agreements, there may be no universal risks. However, during the course of work, the parties may face compliance issues that could negatively impact project goals and lead to significant financial losses for those parties.
Keywords: IT-product, IT-project, risk

For citation:

Nikolaenko V.S. (2025). Reducing risks when creating IT products: Developing integrity criteria for IT entities. *Strategic Decisions and Risk Management,* 16(2): 125-133. DOI: 10.17747/2618-947X-2025-2-125-133. (In Russ.)

Acnowledgements

The work was carried out within the framework of the state task «Science», project FEWM-2023-0013.

IT产品创建中的风险降低：IT实体诚信标准的形成

V.S. Nikolaenko[1, 2, 3]

[1] 托姆斯克国立系统管理与无线电电子大学 (俄罗斯，托姆斯克)
[2] 托姆斯克理工大学 (俄罗斯，托姆斯克)
[3] 西伯利亚国立医科大学 (俄罗斯，托姆斯克)

简介

本文探讨了信息技术主体诚信行为的本质和性质，这些主体随时准备保证在信息技术项目框架内创造高质量的信息技术产品，并将对所有关系参与者和其他利益相关者造成不良合规后果的可能性降至最低值。为了实现既定目标，本文作者分析了关系参与者善意和恶意行为的迹象，包括研究与保护权利免受对方恶意行为侵害有关的法院实践。在研究的基础上，制定了信息技术主体诚信的标准，即不存在对利益相关者造成重大损害的意图，以及存在切实有效的风险管理系统。研究发现，造成损害的意图不仅体现在信息技术主体当前的行为上（在合同中加入明显苛刻的条款、故意违反现行法律、利用交易参与者的无能损害自己的利益等），还体现在他们之前在过去的交易中实施的不公平行为上。研究还发现，实施预防性风险缓解措施的责任在于承诺执行工作以创建 IT 产品的一方。特别是，研究发现，如果 IT 利益相关方在签订合同之前不积极主动地应对 105 项普遍风险，那么在工作执行过程中，利益相关方极有可能遇到合规后果，从而对实现项目目标的进程产生负面影响，并给这些当事方造成重大的物质损失。

关键词: 信息技术产品、信息技术项目、风险

供引用:

Nikolaenko V.S. (2025). IT产品创建中的风险降低：IT实体诚信标准的形成。战略决策和风险管理, 16(2): 125–133. DOI: 10.17747/2618-947X-2025-2-125-133. (俄文)

致谢

这项研究是在国家任务 "科学 "项目FEWM-2023-0013下进行的。

Введение

Согласно постановлению пленума ВАС РФ от 12.10.2006 № 53[1] (далее – Постановление № 53) субъекты предпринимательской деятельности обязаны проявлять должную осмотрительность, то есть предпринимать действия по проверке надежности, зрелости и добросовестности потенциальных и действующих контрагентов во время заключения контрактов. Если субъекты не проявляют подобную осмотрительность, то они подвергают себя риску вступления в отношения с ненадежными, незрелыми и недобросовестными контрагентами, которые не смогут исполнить свои обязательства либо создадут продукты с дефектами и иными недостатками.

Отметим, что под недостатком результата выполненной работы (оказанной услуги, поставленного товара) законодатель понимает любое несоответствие обязательным требованиям нормативных актов, национальных стандартов, контрактов и др. [Гаязов, 2022]. Например, если продукт не отвечает заявленным требованиям, то он приобретает статус некачественного, что может повлечь наступление негативных комплаенс-последствий как для стороны подрядчика (исполнителя, поставщика), так и для стороны заказчика [Николаенко, 2024b]. В частности, если в силу статьи 475 ГК РФ[2] будет установлено, что для устранения недостатков требуются значительные затраты либо их характер таков, что дефекты обнаруживаются повторно, то заказчик (покупатель) может отказаться от исполнения контракта и потребовать возвращения ранее уплаченной им денежной суммы [Михайленко, Ковалева, 2021].

Под ИТ-субъектами в настоящей статье будут пониматься субъекты предпринимательской деятельности (ОКВЭД класс 62), занятые разработкой ИТ-продуктов и оказанием консультационных услуг в данной области [Николаенко, 2024a]. Под проектом, согласно PMBOK® Guide[3], необходимо понимать уникальный процесс, направленный на создание продукта и (или) оказание услуги в условиях, когда ресурсы ограничены, а сроки строго определены. В этой связи ИТ-проект – это уникальный процесс, который направлен на создание продукта и (или) оказание услуги в области информационных технологий (далее – ИТ-продукт) в условиях, когда ресурсы ограничены, а сроки строго определены.

Заметим, что помимо финансовых и репутационных потерь, выражающихся в нарушении сроков выполнения работ, поставках некомплектных и (или) некачественных товаров, выплатах неустоек, штрафов и т. д., субъекты предпринимательской деятельности также могут столкнуться с более тяжкими комплаенс-последствиями [Николаенко, 2024c]. В частности, если налоговым органом будет установлено, что субъект предпринимательской деятельности заключил контракт с контрагентом-однодневкой, то на этот субъект могут быть наложены санкции в форме отказа в возврате налога на добавленную стоимость, доначисления процентов по налогам и др. [Неуступова, Кузьмина, 2019].

[1] Постановление пленума ВАС РФ от 12.10.2006 № 53 «Об оценке арбитражными судами обоснованности получения налогоплательщиком налоговой выгоды». https://clck.ru/3Fkgje.
[2] Гражданский кодекс Российской Федерации (ГК РФ). Комментарий к последним изменениям (2019). Москва, АБАК.
[3] Project management body of knowledge. Guide 6th edition (PMBOK-6) (2017). Project Management Institute (PMI).

В качестве примера санкционирования субъекта предпринимательской деятельности из-за заключения контракта с недобросовестным налогоплательщиком следует привести постановление ФАС ПО от 15.03.2011 по делу № А65-15788/2010[4]. Согласно материалам дела заявитель просил суд признать незаконным решение о доначислении налога на прибыль в размере 827 тыс. руб., доначисления НДС в сумме 620 тыс. руб., начисления штрафа по пункту 1 статьи 122 НК РФ[5] за неуплату налога на прибыль и НДС в сумме 264 тыс. руб.

Другим примером является постановление ФАС ВВО от 28.01.2011 № Ф01-4843/2010 по делу № А29-3615/2010[6]. Заявитель просил суд признать недействительным решение налогового органа в части взыскания 2,9 млн руб. налога на прибыль и 2,2 млн руб. НДС.

Согласно постановлению ФАС ЗСО от 29.03.2011 по делу № А27-9150/2010[7] заявитель просил суд признать недействительным решение налогового органа в части доначисления ЕНВД в размере 328,8 тыс. рублей, пени – 113,7 тыс. рублей, штрафа – 43,3 тыс. рублей, единого налога – 459 тыс. рублей, пени – 122,2 тыс. рублей, штрафа – 81,5 тыс. рублей.

Несмотря на острую необходимость заключения контрактов с надежными, зрелыми и добросовестными контрагентами, Постановление № 53 не формализует каких-либо подходов и способов их проверки, предлагая субъектам предпринимательской деятельности самостоятельно разрабатывать методики исследования контрагентов в рамках собственной системы внутреннего контроля [Мурников и др., 2019]. Так, например, в работе [Востренков, Санина, 2024] отмечается, что для защиты своей экономической безопасности субъекты часто вынуждены инициировать создание отдельных специализированных подразделений (отделов экономической безопасности). Эти подразделения берут на себя функции по митигации рисков, связанных с заключением контрактов с ненадежными контрагентами и тяжкими комплаенс-последствиями, которые могут наступить по их вине. Отметим, что согласно ГОСТ Р ИСО 31000[8] под риском понимается вероятное событие, которое в случае своей материализации может оказать влияние на процесс достижения целей.

На основании сказанного логично предположить, что проверка контрагентов и оценка их надежности, зрелости и добросовестности должны являться неотъемлемой стадией предконтрактной работы субъекта предпринимательской деятельности [Туктарова и др., 2023]. В этой связи с целью улучшения механизма проверки надежности ИТ-субъектов, способных гарантированно создавать высококачественные ИТ-продукты в рамках выполнения ИТ-проектов (спринтов, фаз жизненных циклов, контрактов и др.), необходимо определить критерии добросовестности этих ИТ-субъектов.

Для достижения поставленной цели автором статьи были решены следующие задачи:

- идентифицированы признаки добросовестного и недобросовестного поведения участников отношений;
- формализованы критерии добросовестности ИТ-субъектов.

1. Признаки добросовестного и недобросовестного поведения

Анализ норм действующего законодательства показал, что фундаментом плодотворных и взаимовыгодных отношений между заинтересованными сторонами, занятыми созданием ИТ-продуктов в рамках выполнения ИТ-проектов (спринтов, фаз жизненных циклов, контрактов и др.), является их добросовестное поведение (статья 10 ГК РФ). Именно по этой причине проверку ИТ-субъекта на возможность гарантированного создания желаемых ИТ-продуктов необходимо начинать с проверки его добросовестности, невзирая на декларируемую законодателем презумпцию: согласно презумпции добросовестности любое лицо должно считаться добросовестным до тех пор, пока компетентным органом не будет доказано обратное. Правовое раскрытие презумпции добросовестности определено в статье 302 ГК РФ.

Действующее законодательство определяет добросовестность как принцип гражданского права, который предписывает участникам отношений учитывать права и интересы друг друга (статья 1 ГК РФ). Данный принцип налагает на участников отношений выполнение двух функций: первая направлена на построение плодотворных и взаимовыгодных отношений между заинтересованными сторонами, а вторая – на установление правовых границ и моральных ограничений [Кошурин, 2024].

Законодатель декларирует участникам отношений вести добросовестную деятельность и совершать добросовестные действия по отношению друг к другу. В частности, в силу пункта 2 статьи 434.1 ГК РФ участники отношений обязаны действовать добросовестно. Это означает, что, например, во время переговоров, выполнения работ, оказания услуг, поставки товаров и исполнения других обязательств участники отношений не вправе отступать от добросовестного поведения (пункт 3 статьи 432 ГК РФ) [Назарова, 2022]. Добросовестное поведение заинтересованных сторон является залогом стабильности, устойчивости и предсказуемости их отношений.

Стоит заметить, что нормы действующего законодательства не дают однозначного определения понятию «добросовестность», что является причиной многочисленных дискуссий. Например, А.А. Николаев в работе [Николаев, 2022] определяет добросовестность как императивное правило поведения участников отношений, которое регулирует баланс прав, обязанностей и устанавливает границы их деятельности. В работе Д.Н. Ревиной добросовестность характеризуется как критерий оценки поведения участника отношений [Ревина, 2019]. Усиливая данную точку зрения, В.В. Кошурин добавляет, что законодатель не закрепляет какой-либо перечень критериев, который бы позволил провести оценку добросовестности контрагента, однако формализует признаки, по которым можно осуществить квалификацию добросовестного или недобросовестного поведения контрагента [Кошурин, 2024]. Так, согласно постановлению пленума

[4] Постановление Федерального арбитражного суда Поволжского округа от 15.03.2011 по делу № А65-15788/2010. https://clck.ru/3FpteD.
[5] Налоговый кодекс Российской Федерации (НК РФ) от 31.07. 1998 № 146-ФЗ. https://clck.ru/3LyHqB.
[6] Постановление Федерального арбитражного суда Волго-Вятского округа от 28.01.2011 № Ф01-4843/2010 по делу № А29-3615/2010. https://clck.ru/3FpxEe.
[7] Постановление ФАС ЗСО от 29.03.2011 по делу № А27-9150/2010. https://clck.ru/3FpxGo.
[8] ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство (2020). Москва, Стандартинформ.

Верховного суда от 23.06.2015 №25 (далее – Постановление №25) поведение считается добросовестным, если в действиях контрагента присутствуют определенные признаки. Например, поведение контрагента считается добросовестным, если он[9]:

- учитывает права и законные интересы другой стороны;
- оказывает содействие другой стороне, в том числе помогает ей получить информацию, необходимую для выполнения работ, оказания услуг, поставки товаров и исполнения других обязательств (пункт 3 статьи 307 ГК РФ);
- предпринимает меры для предотвращения событий (рисков), которые могут причинить вред другой стороне, в том числе предупреждает контрагента о необходимости совершения им дополнительных действий, которые не указаны в договоре, но способны повлиять на качество конечного результата.

Когда лицо, вступившее в отношения, имеет умысел причинить вред и (или) злоупотребляет своим правом во вред другому лицу (пункт 1 статтьи 10 ГК РФ), подобное поведение считается недобросовестным. К признакам недобросовестного поведения могут быть отнесены действия контрагента, когда он:

- включает в контракт явно обременительные условия для другой стороны;
- сознательно нарушает нормы действующего законодательства, требования национальных стандартов и других нормативных актов;
- скрывает информацию, от которой зависит решение о заключении сделки;
- использует некомпетентность другой стороны ей во вред.

Важно подчеркнуть, что для признания действий какого-либо лица недобросовестными должно быть доказано, что у данного лица имелась цель причинить вред другому лицу. Кроме того, злоупотребление правом должно носить достаточно очевидный характер, а вывод о нем не должен являться следствием предположений. Именно по этой причине признание действий недобросовестными является компетенцией суда [Рыжих, 2020]. В работе М.Г. Назаровой [Назарова, 2022] отдельно подчеркивается, что двойственный характер добросовестности – формальный и нравственный – предоставляет судебному органу свободу в определении квалификации совершенных действий.

Признаки добросовестного и недобросовестного поведения представлены на рисунке.

Сложность проверки добросовестности потенциальных и действующих контрагентов отмечается в работе Е.Е. Богдановой [Богданова, 2016]. По мнению автора, сложность проверки обусловлена системой представлений о нравственном поведении участников гражданских правоотношений, которая сложилась в обществе. В своем исследовании Богданова приходит к выводу, что во время анализа деятельности контрагентов необходимо, в частности, оценивать их нравственность, используя понятия добра и зла.

Согласно требованиям Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» №44-ФЗ (далее – Закон №44-ФЗ)[10], добросовестность является одним из ключевых качеств участника закупки, который влияет на принятие решения о заключении контракта на закупку товаров, работ, услуг для обеспечения государственных и муниципальных нужд. В частности, участник закупки в течение трех лет до даты подачи заявки должен успешно реализовать не менее трех контрактов.

Недобросовестное поведение участника отношений может спровоцировать наступление тяжких комплаенс-последствий. Например, действующее законодательство предусматривает следующие средства защиты от недобросовестного поведения (эстоппель):

- контрагенту, который злоупотребляет своим правом, может быть отказано в защите этого права (пункт 2 статьи 10 ГК РФ);
- сделка, которая была заключена со злоупотреблением права, может быть признана недействительной (пункт 5 статьи 166 ГК РФ) [Черняткин, 2018]. Если заявле-

Рис. Признаки добросовестного и недобросовестного поведения участников отношений
Fig. Signs of bona fide and unfair behaviour of participants in relationships

Источник: составлено автором.

[9] Постановление пленума Верховного суда РФ от 23.06. 2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации». https://clck.ru/3EakXG.

[10] Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ. https://clck.ru/Nh6GG.

ние о недействительности сделки поступает от недобросовестного контрагента, то такое заявление не имеет правового значения;
- если контрагент, злоупотребив своим правом, причинил вред и материальный ущерб другой стороне, то эта сторона приобретает право на взыскание убытков (пункт 4 статьи 10 ГК РФ) [Филиппова, Жаркенова, 2018];
- если контрагент, которому выгодно наступление определенного условия сделки, действовал недобросовестно для материализации этого условия, то оно может быть признано ненаступившим (пункт 3 статьи 157 ГК РФ);
- если контракт направлен на обеспечение государственных (муниципальных) нужд, то лицо может быть включено в реестр недобросовестных подрядных организаций [Жуков, 2021].

В качестве примера недобросовестного поведения следует привести дело № А60-46975/2016[11], где ИТ-субъект воспользовался наработками ранее созданного ИТ-продукта, правообладателем которого он не являлся, и создал на его основе производное произведение (статья 1270 ГК РФ). Для признания установления факта недобросовестного поведения суд привлек эксперта. Согласно экспертному заключению, подавляющее количество функциональных блоков, связей и логических операций в оригинальном ИТ-продукте и в производном произведении являлись идентичными.

Другим примером недобросовестного поведения ИТ-субъекта является дело № А40-202764/2018[12]. В ходе судебного разбирательства было установлено, что ИТ-субъект пытался недобросовестно присвоить себе исключительные права на результаты интеллектуальной деятельности и объекты авторского права его бывших работников. В частности, ИТ-субъект предпринял действия по аннулированию свидетельства о государственной регистрации программы для ЭВМ, выданного Роспатентом, так как в этом документе было зафиксировано, что его бывшие работники являются авторами и правообладателями спорного ИТ-продукта.

Исследуя проблему недобросовестного поведения участников отношений, О.Е. Жульева приходит к выводу, что для митигации подобных проблем лицам необходимо предоставлять «заверение о добросовестности» либо включать дополнительные условия в текст контракта [Жульева, 2024]. По мнению Жульевой, эти ковенанты должны содержать информацию, подтверждающую официальный и налоговый статус участников отношений в гражданском обороте, наличие ресурсов для исполнения обязательств, а также готовность взаимодействовать с контролирующими органами.

По мнению автора настоящей статьи, позиция Жульевой, изложенная в ее работе, требует уточнения. В частности, согласно требованиям Закона №44-ФЗ правовой, налоговый и хозяйственный статусы участников закупки относятся к критериям, подтверждающим их надежность, а не добросовестность. Согласно ГОСТ 27.002[13] надежность – это свойство объекта выполнять заданные функции в установленных эксплуатационных пределах на определенном отрезке времени. В контексте экономических отношений между субъектами понятие «надежность» раскрывается как характеристика функционирования их системы финансово-хозяйственной деятельности.

Кошурин, проведя анализ судебной практики, пришел к выводу, что способом проверки добросовестности контрагента является анализ судебных решений с его участием [Кошурин, 2024]. Он утверждает, что проверку сведений о контрагенте необходимо осуществлять посредством изучения его правоустанавливающих документов, а при анализе судебной практики следует фокусировать внимание на мотивах и действиях, которые совершал контрагент во время спора.

2. Критерии добросовестности

На основании изложенного автор настоящей статьи считает, что основными критериями добросовестности ИТ-субъектов должны являться:

1. Отсутствие умысла на причинения материального ущерба и иного вреда заинтересованным сторонам. Наличие подобного умысла характеризуется не только текущим поведением ИТ-субъекта (включение в контракт явно обременительных условий, сознательное нарушение норм действующего законодательства, использование некомпетентности участников сделки им во вред и др.), но и недобросовестными действиями, которые он совершил ранее в прошлых сделках. Логично предположить, что одним из способов проверки умысла на причинения материального ущерба и иного вреда заинтересованным сторонам является проверка контрактов на наличие явно обременительных условий, а также анализ судебной практики и предписаний надзорных органов.

2. Наличие эффективной и результативной системы управления рисками (далее – СУР). Согласно действующему законодательству ответственность за реализацию превентивных мер по митигации рисков возложена на сторону подрядчика (исполнителя) (главы 37, 39 ГК РФ). Если подрядчик (исполнитель) заблаговременно, до заключения контракта, не оценивает риски и превентивно не воздействует на них, то во время выполнения работ с большой вероятностью участники сделки столкнутся с событиями, которые негативно повлияют на процесс достижения проектных целей, причинят им материальный ущерб либо иной вред. Это означает, что наличие СУР должно являться критерием, который способен легально установить добросовестность ИТ-субъекта. Нужно отметить, что согласно стандарту ГОСТ Р ИСО/МЭК 33001[14] результативность (effectiveness) определяется как степень реализации превентивных мер и достижения запланированных результатов. В соответствии с ГОСТ ISO 9000[15] под эффективностью (efficiency) следует понимать связь между достигнутым результатом и использованными ресурсами.

[11] Постановление суда по интеллектуальным правам по делу № А60-46975/2016 от 02.09.2022. https://clck.ru/3EbpVs.
[12] Постановление суда по интеллектуальным правам по делу № А40-202764/2018 от 01.08.2019. https://clck.ru/3EbodH.
[13] ГОСТ 27.002-2015. Надежность в технике. Термины и определения (2016). Москва, Стандартинформ.
[14] ГОСТ Р ИСО/МЭК 33001-2017. Информационные технологии. Оценка процесса. Понятия и терминология (2017). Москва, Стандартинформ.
[15] ГОСТ ISO 9000-2011. Системы менеджмента качества. Основные положения и словарь (2020). Москва, Стандартинформ.

Исследование, проведенное в рамках научно-исследовательского гранта РФФИ №16–36–00031 «мол_а» в 495 ИТ-субъектах Томской области (ОКВЭД класс 62), позволило установить, что во время создания ИТ-продуктов могут материализоваться порядка 105 универсальных рисков, из которых 5 – коммерческие, 45 – комплаенс-риски и 55 – проектные [Nikolaenko, Sidorov, 2023]. Под универсальными рисками понимаются вероятные события, актуальные для ИТ-проектов (спринтов, фаз жизненных циклов, контрактов и др.) независимо от их масштабов, сложности, длительностей (краткосрочные, среднесрочные, долгосрочные), типов (ПО, мобильное приложение, ИС и др.) и концепций создания ИТ-продуктов (Waterfall, Agile) [Paladino et al., 2009; Aven, 2012; Brandas et al., 2012; Lee, Baby, 2013; De Bakker et al., 2014; Mishra et al., 2014; Beer et al., 2015; Luckmann, 2015].

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 и т.п. Несмотря на небольшую долю в общем объеме рисков (4,7%), материализация одного коммерческого риска способна нивелировать все затраченные ресурсы и усилия, нанеся заинтересованным сторонам катастрофический материальный ущерб.

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.

Проектными рисками называют риски, наступление которых оказывает влияние на одну цель проекта либо на их совокупность. Данные риски, как правило, материализуются во время фазы жизненного цикла ИТ-проекта «Создание ИТ-продукта» из-за действий (бездействий) руководителя проекта, системного аналитика, юриста, субподрядчика и других участников проекта [Николаенко, 2025].

В свете сказанного можно заключить следующее. Если ИТ-субъекты намерены гарантировать создание высококачественных ИТ-продуктов и снижение до минимальных значений вероятности наступления нежелательных комплаенс-последствий для всех участников отношений и иных заинтересованных сторон, то на своей стороне они должны обеспечить митигацию 105 универсальных рисков. Превентивное элиминирование универсальных рисков может служить количественным и качественным подтверждением того, что на стороне ИТ-субъектов функционируют эффективные и результативные СУР. Так как в действиях этих субъектов присутствуют признаки добросовестного поведения, направленные на предотвращение событий, которые могут причинить вред заинтересованным сторонам, то это может свидетельствовать об их добросовестности.

Заключение

Таким образом, можно заключить, что если субъекты предпринимательской деятельности намерены заключать контракты на создание ИТ-продуктов, то для проявления должной осмотрительности им необходимо осуществлять экспертизу критериев добросовестности, таких как отсутствие умысла на причинение материального ущерба и иного вреда заинтересованным сторонам и наличие эффективной и результативной СУР. Как было отмечено ранее, выполнение этих критериев способствует повышению шансов на заключение контрактов с ИТ-субъектами, которые смогут обеспечить гарантированное создание высококачественных ИТ-продуктов в рамках выполнения ИТ-проектов (спринтов, фаз жизненных циклов, контрактов и др.) без наступления нежелательных комплаенс-последствий.

Стоит отметить, что рост вероятности успешного создания ИТ-продуктов базируется на механизме митигации 105 универсальных рисков. Результаты проведенного исследования показали, что если ИТ-субъекты заблаговременно, до заключения контрактов, не оценивают эти риски и превентивно не воздействуют на них, то во время выполнения работ с большой вероятностью они и заинтересованные стороны могут столкнуться с событиями, которые негативно повлияют на процесс достижения проектных целей.

В дальнейших исследованиях необходимо будет проанализировать механизм оценки зрелости ИТ-субъектов, так как именно высокий уровень зрелости показывает, насколько качественно и результативно ИТ-субъекты предпринимают действия по предотвращению событий (рисков), способных причинить вред заинтересованным сторонам. Исходя из этого, далее необходимо более подробно рассмотреть существующие способы определения уровня зрелости субъектов, занятых разработкой компьютерного программного обеспечения и оказанием консультационных услуг в данной области (ОКВЭД класс 62).

Литература

Богданова Е.Е. (2016). Принцип добросовестности: соотношение правовых и нравственных аспектов. *Lex russica (русский закон)*, 1: 177–182.

Востренков М.И., Санина Л.В. (2024). Обзор методов оценки надежности контрагентов, применяемых в организации. *Global and Regional Research*, 6(3): 120–129.

Гаязов И.Р. (2022). К вопросу о модификации программ для ЭВМ. *Интернаука*, 2–6(245): 21–32.

Жуков Ф.Ф. (2021). Реестр недобросовестных поставщиков и принцип добросовестности в гражданском праве. *Вестник Тверского государственного университета. Серия: Право,* 2(66): 15–20.

Жульева О.Е. (2024). Правовая характеристика заявлений о добросовестности в договорной практике. *Вестник ВИЭПП,* 1: 142–149.

Кошурин В.В. (2024). Критерии и методы определения добросовестности приобретателя: анализ теории и практики. *Вестник науки*, 4(73): 107–114.

Михайленко К.А., Ковалева К.А. (2021). Обзор и анализ развития программного обеспечения. В: *Актуальные проблемы науки и образования в условиях современных вызовов:* сборник материалов II Международной научно-практической конференции. Москва, Институт развития образования и консалтинга: 52–55.

Мурников И.В., Соловьюк Д.В., Кузьмина О.В., Федоренко И.В. (2019). Проблемы контроля надежности потенциального контрагента. *Учет, анализ и аудит: проблемы теории и практики,* 22: 144–149.

Назарова М.Г. (2022). Добросовестность участников возмездного оказания услуг в современных условиях. *Университетская наука,* 1(13): 345–347.

Неуступова А.С., Кузьмина Н.Д. (2019). Оценка надежности контрагента по хозяйственным операциям. *Современные проблемы инновационной экономики,* 6: 110–116.

Николаев А.А. (2022). Добросовестность как принцип гражданского права. Систематизация основных принципов добросовестности в гражданском праве. *Материалы Афанасьевских чтений,* 3(40): 76–79.

Николаенко В.С. (2024a). ИТ-продукт: уточнение понятия. *Векторы благополучия: экономика и социум,* 52(3): 136–145.

Николаенко В.С. (2024b). Комплаенс-особенности создания ИТ-продуктов в рамках выполнения ИТ-проектов. *Проблемы анализа риска,* 21(5): 97–107.

Николаенко В.С. (2024c). Комплаенс-риски эксплуатации ИТ-продуктов. *Стратегические решения и риск-менеджмент,* 15(4): 360–367.

Николаенко В.С. (2025). Анализ процессов создания ИТ-продуктов в рамках выполнения ИТ-проектов. *Проблемы анализа риска,* 22(1): 68–87.

Ревина Д.Н. (2019). Принцип добросовестности в деятельности Федеральной службы по интеллектуальной собственности. В: *Образовательная система в вопросах совершенствования правовой культуры.* Казань, СитИвент: 121–126.

Рыжих И.В. (2020). К вопросу о категории добросовестность в гражданском праве. *Вестник экономической безопасности,* 6: 106–109.

Туктарова П.А., Давлетшина С.М., Хамидуллина Д.И. (2023). Применение регрессионных моделей для определения надежности контрагента. *Информационные и математические технологии в науке и управлении,* 2(30): 121–128.

Филиппова Т.А., Жаркенова С.Б. (2018). Принцип добросовестности при исполнении обязательства. *Известия Алтайского государственного университета,* 6(104): 197–202.

Черняткин А.О. (2018). Добросовестность сторон при признании сделки недействительной. *Вопросы науки и образования,* 8(20): 92–93.

Aven T. (2012). The risk concept – Historical and recent development trends. *Reliability Engineering and System Safety,* 99: 33–44.

Beer M., Wolf T., Garizy T.Z. (2015). Systemic risk in IT portfolios – An integrated quantification approach. In: *Proceedings of the 36th International Conference on Information Systems (ICIS)*, Fort Worth, December 2015. Fort Worth, USA: 1–18.

Brandas C., Didraga O., Bibu N. (2012). Study on risk approaches in software development project. *Informatica Economica,* 16(3): 148−157.

De Bakker K., Boonstra A., Wortmann H. (2014). The communicative effect of risk identification on project success. *Project Organisation and Management,* 6: 138−156.

Lee O.-K.D., Baby D.V. (2013). Managing dynamic risks in global IT projects: Agile risk-management using the principles of service-oriented architecture. *International Journal of Information Technology & Decision Making,* 12: 1121−1150.

Luckmann J.A. (2015). Positive risk management: Hidden wealth in surface mining. *The Journal of The Southem Africa Institute of Mining and Metallurgy,* 115: 1027–1034.

Mishra A., Das S., Murray J. (2014). Managing risk in government information technology projects: Does process maturity matter? *Production and Operations Management,* 24(3): 365–368.

Nikolaenko V., Sidorov A. (2023). Analysis of 105 IT Project Risks. *Journal of Risk and Financial Management,* 33: 1–20.

Paladino B., Cuy L., Frigo M. (2009). Missed opportunities in performance and enterprise risk management. *Journal of Corporate Accounting & Finance,* 20(3): 43–51.

References

Bogdanova E.E. (2016). The principle of good faith: correlation of legal and moral aspects. *Lex russica (Russian Law),* 1: 177-182. (In Russ.)

Vostrenkov M.I., Sanina L.V. (2024). Review of methods for assessing the reliability of counterparties used in the organization. *Global and Regional Research,* 6(3): 120-129. (In Russ.)

Gayazov I.R. (2022). On the question of modifying computer programs. *Internauka,* 2-6(245): 21-32. (In Russ.)

Zhukov F.F. (2021). Register of unfair suppliers and the principle of good faith in civil law. *Bulletin of the Tver State University. Series: Law,* 2(66): 15-20. (In Russ.)

Zhulyeva O.E. (2024). Legal characteristics of declarations of good faith in contractual practice. *Bulletin of the RESPP,* 1: 142-149. (In Russ.)

Koshurin V.V. (2024). Criteria and methods for determining the buyer's integrity: analysis of theory and practice. *Bulletin of Science,* 4(73): 107-114. (In Russ.)

Mikhailenko K.A., Kovaleva K.A. (2021). Review and analysis of software development. In: *Actual problems of science and education in the context of modern challenges: Collection of materials II International Scientific and Practical Conference.* Moscow, Institute of Educational Development and Consulting: 52-55. (In Russ.)

Murnikov I.V., Solovyuk D.V., Kuzmina O.V., Fedorenko I.V. (2019). Problems of monitoring the reliability of a potential counterparty. *Accounting, Analysis and Audit: Problems of Theory and Practice,* 22: 144-149. (In Russ.)

Nazarova M.G. (2022). Integrity of participants in the paid provision of services in modern conditions. *University Science,* 1(13): 345-347. (In Russ.)

Neustupova A.S., Kuzmina N.D. (2019). Assessment of the counterparty's reliability in business transactions. *Modern Problems of the Innovative Economy,* 6: 110-116. (In Russ.)

Nikolaev A.A. (2022). Good faith as a principle of civil law. Systematization of the basic principles of good faith in civil law. *Materials of the Afanasyev Readings,* 3(40): 76-79. (In Russ.)

Nikolaenko V.S. (2024a). IT-product: Clarification of the concept. *Journal of Wellbeing Technologies,* 52(3): 136-145. (In Russ.)

Nikolaenko V.S. (2024b). Compliance-features of creating IT-Products within the framework of IT-projects. *Issues of Risk Analysis,* 21(5): 97-107. (In Russ.)

Nikolaenko V.S. (2024c) Compliance-risks in the operation of IT products. *Strategic Decisions and Risk Management,* 15(4): 360-367. (In Russ.)

Nikolaenko V.S. (2025). Analysis of the processes of creating IT-Products as part of the implementation of IT-projects. *Issues of Risk Analysis,* 22(1): 68-87. (In Russ.)

Revina D.N. (2019). The principle of good faith in the activities of the federal service for intellectual property. In: *Educational System for Improving Legal Culture.* Kazan, SitIvent: 121-126. (In Russ.)

Ryzhikh I.V. (2020). On the question of the category of good faith in civil law. *Bulletin of Economic Security,* 6: 106-109. (In Russ.)

Tuktarova P.A., Davletshina S.M., Khamidullina D.I. (2023). Using regression models to determine the counterparty's reliability. *Information and Mathematical Technologies in Science and Management,* 2(30): 121-128. (In Russ.)

Filippova T.A., Zharkenova S.B. (2018). The principle of good faith in the performance of obligations. *Proceedings of the Altai State University,* 6(104): 197-202. (In Russ.)

Chernyatkin A.O. (2018). Good faith of the parties when declaring a transaction invalid. *Issues of Science and Education,* 8(20): 92-93. (In Russ.)

Aven T. (2012). The risk concept - Historical and recent development trends. *Reliability Engineering and System Safety,* 99: 33-44.

Beer M., Wolf T., Garizy T.Z. (2015). Systemic risk in IT portfolios - An integrated quantification approach. In: *International Conference on information systems: Exploring the information frontier (ICIS),* Fort Worth, December 2015. Fort Worth, USA: 1-18.

Brandas C., Didraga O., Bibu N. (2012). Study on risk approaches in software development project. *Informatica Economica,* 16(3): 148-157.

De Bakker K., Boonstra A., Wortmann H. (2014). The communicative effect of risk identification on project success. *Project Organisation and Management,* 6: 138-156.

Lee O.-K.D., Baby D.V. (2013). Managing dynamic risks in global IT projects: Agile risk-management using the principles of service-oriented architecture. *International Journal of Information Technology & Decision Making,* 12: 1121-1150.

Luckmann J.A. (2015). Positive risk management: Hidden wealth in surface mining. *The Journal of The Southem Africa Institute of Mining and Metallurgy,* 115: 1027-1034.

Mishra A., Das S., Murray J. (2014). Managing risk in government information technology projects: Does process maturity matter? *Production and Operations Management,* 24(3): 365-368.

Nikolaenko V., Sidorov A. (2023). Analysis of 105 IT project risks. *Journal of Risk and Financial Management,* 33: 1-20.

Paladino B., Cuy L., Frigo M. (2009). Missed opportunities in performance and enterprise risk management. *Journal of Corporate Accounting & Finance,* 20(3): 43-51.

Информация об авторе

Валентин Сергеевич Николаенко

Кандидат экономических наук, доцент кафедры автоматизации обработки информации Томского государственного университета систем управления и радиоэлектроники (Томск, Россия); доцент Бизнес-школы Томского политехнического университета (Томск, Россия); доцент кафедры экономики, социологии, политологии и права Сибирского государственного медицинского университета (Томск, Россия); доцент кафедры управления качеством Томского государственного университета (Томск, Россия). ORCID: 0000-0002-1990-4443; Web of Science Researcher ID: J-8521-2015; SPIN: 9301-1835; Author ID: 745788; IRID: 283767926; Scopus Author ID: 57193434445.

Область научных интересов: риск-менеджмент, национальная безопасность, экономическая безопасность, информационное право и защита интеллектуальной собственности, гражданское право, управление проектами.

valentin.s.nikolaenko@tusur.ru

About the author

Valentin S. Nikolaenko

Candidate of economic sciences, associate professor at the Department of Automation of Information Processing, Tomsk State University of Control Systems and Radioelectronics (Tomsk, Russia); associate professor at the Business School of Tomsk Polytechnic University (Tomsk, Russia); associate professor at the Department of Economics, Sociology, Political Science and Law of Siberian State Medical University (Tomsk, Russia); associate professor at the Department of of Quality Management Tomsk State University (Tomsk, Russia). ORCID: 0000-0002-1990-4443; Web of Science Researcher ID: J-8521-2015; SPIN: 9301-1835; Author ID: 745788; IRID: 283767926; Scopus Author ID: 57193434445.

Research interests: risk-management, national security, economic security, information law and intellectual property protection, civil law, project management.

valentin.s.nikolaenko@tusur.ru

作者信息

Valentin Sergeyevich Nikolaenko

经济学副博士，托姆斯克国立系统管理与无线电电子大学信息处理自动化系副教授（俄罗斯，托姆斯克）； 托姆斯克理工大学商学院副教授 (俄罗斯，托姆斯克); 西伯利亚国立医科大学经济学、社会学、政治学和法律系副教授 (俄罗斯，托姆斯克); 托姆斯克国立大学质量管理系副教授（俄罗斯，托姆斯克）. ORCID: 0000-0002-1990-4443; Web of Science Researcher ID: J-8521-2015; SPIN: 9301-1835; Author ID: 745788; IRID: 283767926; Scopus Author ID: 57193434445.

科学研究兴趣领域: 风险管理、国家安全、经济安全、信息法和知识产权保护、民法、项目管理。

valentin.s.nikolaenko@tusur.ru

Статья поступила в редакцию 12.03.2025; после рецензирования 21.03.2025 принята к публикации 30.03.2025. Автор прочитал и одобрил окончательный вариант рукописи.

The article was submitted on 12.03.2025; revised on 21.03.2025 and accepted for publication on 30.03.2025. The author read and approved the final version of the manuscript.

文章于 12.03.2025 提交给编辑。文章于 21.03.2025 已审稿。之后于 30.03.2025 接受发表。作者已经阅读并批准了手稿的最终版本。