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

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 behavior of IT-entities that are willing to guarantee the production of high-quality IT-products within the framework of projects, as well as minimizing the likelihood of undesirable consequences for all participants and other interested parties. To achieve this goal, the article analyzes the signs of good faith and unfair behavior of parties involved in relationships, including judicial practice related to protecting rights from unfair conduct of counterparties. Based on this research, criteria were formulated for the integrity of IT-entities, such as the absence of intention to cause material harm to interested parties, and the existence of an effective risk management system. It was discovered that the intention to harm is characterized not only by the current behavior of IT-companies (including clearly burdensome terms in contracts, deliberate violation of current legislation, use of the incompetence of transaction participants for their own benefit, etc.), but also by unfair actions committed in previous transactions. It was also discovered that responsibility for taking preventive measures to reduce risks is assigned to parties undertaking work on producing an IT-product. In particular, research has shown that, if IT-companies do not proactively influence companies in advance before entering into agreements, there will be no universal risks, but during the performance of work, parties may face compliance consequences that could negatively affect project goals and lead to significant material losses for these 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。

Introduction

According to the Resolution of the Plenum of the Supreme Arbitration Court of the Russian Federation dated October 12, 2006, No. 53[1] (hereinafter referred to as Resolution No. 53), business entities are required to exercise due diligence when concluding contracts, i.e., take steps to verify the reliability and integrity of potential and current counterparts. If they fail to do so, they risk entering into relationships with unreliable and unscrupulous counterparts who will not fulfill their obligations or create products with defects.

It should be noted that the legislator considers a deficiency in the results of work performed (services rendered, goods delivered) to be any non-compliance with mandatory requirements of regulatory acts, national standards, contracts, etc. [Gayazov, 2022]. For example, if a product does not meet the stated requirements, it becomes low-quality and may entail negative consequences for both the contractor and the customer [Nikolaenko, 2024b]. In particular, if it is established by virtue of Article 475 of the Civil Code of the Russian Federation[2] that significant costs are required to eliminate defects or their nature is such that defects are discovered repeatedly, the customer (buyer) may refuse to perform the contract and demand a refund of money previously paid [Mikhailenko, Kovaleva, 2021].

In this article, IT entities are understood as business entities (OKVED class 62) engaging in the development of IT products and providing consulting services in this field [Nikolaenko, 2024a]. According to the PMBOK® Guide[3], a project is a unique process aimed at creating a product and/or providing a service under conditions where resources are limited and deadlines are strictly defined. In this regard, an IT project is a specific process aimed at developing an IT product (hereinafter referred to as 'the product') in the field of information technology under conditions of limited resources and strict deadlines.

It should be noted that, in addition to financial and reputational losses expressed in violation of deadlines for the performance of work, the delivery of incomplete or low-quality goods, and the payment of penalties and fines, business entities may face more serious consequences for compliance [Nikolaenko, 2024c]. In particular, if the tax authorities establish that a business has entered into a contract with a counterparty for one day, then sanctions may be imposed on that business in the form of refusal to refund VAT, additional interest on taxes, etc. [Neustupova, Kuzmina, 2019].

As an example of sanctions against a business entity for entering into a contract with a dishonest taxpayer, the ruling of the Federal Antimonopoly Service (FAS) of March 15, 2011, in case No. A65-15788/2010, should be cited[4]. According to the case materials, the applicant asked the court to declare the decision to charge income tax in an amount of 827 thousand rubles and VAT in an additional amount of 620 thousand rubles illegal, as well as to impose a fine under paragraph 1 of Article 122 of the Tax Code of the Russian Federation[5] in the amount of 264 thousand rubles for failure to pay taxes.

Another example is the ruling of the FAS VVO dated 28.01.2011 No. F01-4843/2010 in case No. A29-3615/2010[6]. The applicant asked the court to annul the tax authority's decision to collect RUB 2.9 million in income tax and RUB 2,2 million in VAT.

According to the ruling of the FAS WSO dated 29.03.2011, in case No. A27-9150/2010[7] the applicant requested the court to annul the decision of the tax authorities regarding the additional assessment of UTII amounting to 328.8 thousand rubles, penalties amounting to 113.7 thousand rubles and a fine amounting to 43.3 thousand rubles as well as a single tax amounting to another 459 thousand and penalties amounting again to 122.2 thousand and fines amounting once again to a total of 81.5 thousand.

Despite the urgent need to conclude contracts with reliable, mature and conscientious counterparts, Resolution No. 53 does not formalize any approaches or methods for their verification. Instead, it suggests that business entities should independently develop methods for researching counterparts within the framework of their own internal control systems [Murnikov et al., 2019]. For example, in the work by [Vostrenkov and Sanina, 2024], it is noted that entities are often forced to create separate specialised units in order to protect their economic security. These units take on the function of mitigating the risks associated with concluding contracts with unreliable counterparts and serious compliance consequences that may arise due to their actions. It should be noted

[1] https://clck.ru/3Fkgje.
[2] The Civil Code of the Russian Federation (Civil Code of the Russian Federation). Comment on the latest changes (2019). Moscow, ABAK.
[3] Project management body of knowledge. Guide 6th edition (PMBOK-6) (2017). Project Management Institute (PMI).
[4] https://clck.ru/3FpteD.
[5] https://clck.ru/3LyHqB.
[6] https://clck.ru/3FpxEe.
[7] https://clck.ru/3FpxGo.

that risk is understood in GOST R ISO 31000[8] as a probable event that, when it occurs, may affect the achievement of goals.

Based on the above, it is logical to assume that the verification of counterparties and the assessment of their reliability, maturity, and integrity should be an integral part of the pre-contractual work of a business entity [Tuktarova et al., 2023]. In this regard, in order to improve the mechanism for verifying the reliability of IT entities capable of creating high-quality IT products within the framework of IT projects (sprints, life cycle phases, contracts, etc.), it is necessary to define criteria for the integrity of these entities.

To achieve the stated goal, the author of the article solved the following tasks:

- signs of conscientious and dishonest behaviour of participants in relationships have been identified.
- criteria for the conscientiousness of IT entities have been formalised.

1. Signs of good faith and bad faith behaviour

An analysis of the current legislation has shown that the basis for fruitful and mutually beneficial relations between stakeholders involved in creating IT products within the framework of IT projects is their good faith (Article 10 of the Civil Code of the Russian Federation). For this reason, the verification of an IT entity's ability to create the desired IT product must begin with verifying its good faith regardless of any presumption declared by the lawmaker. According to the presumption of good faith, anyone must be considered to be acting in good faith until proven otherwise by a competent authority. The legal definition of the presumption is given in Article 302 of the Civil Code of the Russian Federation.

Current legislation defines good faith as a principle of civil law, which requires participants in relationships to take into account each other's rights and interests (Article 1 of the Civil Code of the Russian Federation). This principle imposes two functions on participants: the first is aimed at building fruitful and mutually beneficial relationships between interested parties; the second is aimed at establishing legal boundaries and moral restrictions. [Koshurin, 2024].

The legislator declares that the parties to the relationship must conduct bona fide activities and perform bona fide actions towards each other. In particular, by virtue of paragraph 2 of Article 434.1 of the Civil Code of the Russian Federation, the parties to the relationship are obliged to act in good faith. This means that, for example, during negotiations, performance of work, provision of services, delivery of goods and fulfillment of other obligations, the parties to the relationship have no right to deviate from bona fide behaviour (paragraph 3 of Article 432 of the Civil Code of the Russian Federation) [Nazarova, 2022]. The good faith behaviour of stakeholders is the key to stability, sustainability, and predictability in their relations.

It is worth noting that the current legislation does not provide an unambiguous definition of the concept of 'good faith'. This is the cause of numerous discussions, for example, A.A. Nikolaev defines good faith in [Nikolaev, 2022] as an imperative rule for the conduct of participants in relations, which regulates the balance of rights and obligations and establishes boundaries for their activities. In the work of D.N. Revina, conscientiousness is characterised as a criterion for assessing the behaviour of a person in a relationship [Revina, 2019]. Strengthening this point of view, V.V. Koshurin adds that the legislator does not establish a list of criteria to assess the counterparty's good faith. Instead, it formalises signs by which the good faith or bad faith of the party can be determined. [Koshurin, 2024]. Thus, according to Resolution No. 25 of the Plenary Session of the Supreme Court on 23 June 2015 (hereinafter referred to as Resolution No.25), conduct is considered to be good faith if certain signs are present in the actions of a counterparty. For example, behaviour by a counterparty is considered bona fide when[9]:

- the rights and legitimate interests of the other party are taken into account;
- assistance is provided to the other party, including helping them obtain information necessary for performing work, providing services, delivering goods, and fulfilling other obligations(Clause 3 of Article 307 of the Civil Code of the Russian Federation).
- measures are taken to prevent events that may harm other parties, including warning them about additional actions that are not specified in the contract and may affect the quality of the final result.

When a person who has entered into a relationship has the intent to cause harm and (or) abuses his/her right to the detriment of another person (Clause 1 of Article 10 of the Civil Code of the Russian Federation),

[8] GOST R ISO 31000-2019. Risk management. Principles and Guidelines (2020). Moscow, Standartinform.
[9] https://clck.ru/3EakXG.

such behaviour is considered unfair. Signs of unfair behaviour may include the actions of the counterparty when:

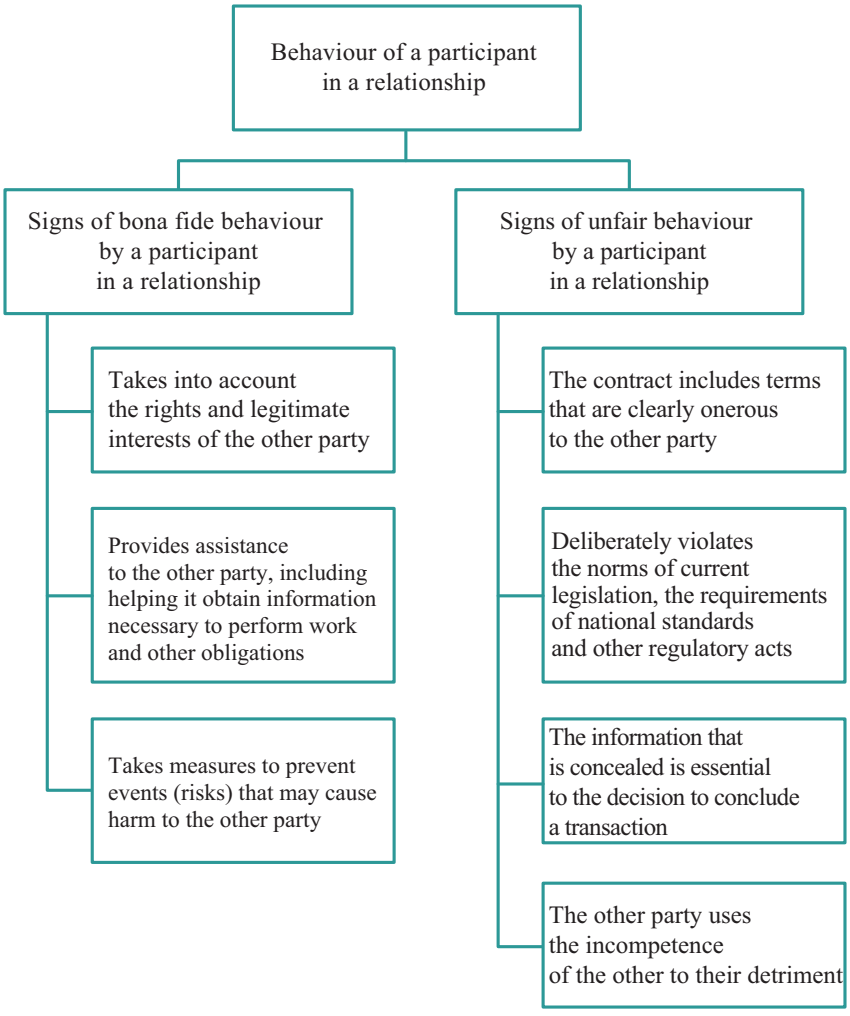
- the contract includes terms that are clearly onerous to the other party;
- the norms of current legislation, requirements of national standards and other regulations are deliberately violates;
- the information on which the decision to conclude a transaction depends is deliberately hidden;
- the incompetence of the other party is used to its detriment.

It is important to emphasise that, in order to recognise someone's actions as unfair, it must be proved that they had the intention to cause harm to another person. Additionally, the abuse of rights should be sufficiently obvious, and the decision about it should not be based on assumptions. For this reason, recognising actions as unfair is within the jurisdiction of the court [Ryzhikh, 2020]. In the work of M.G. Nazarov [Nazarov, 2022], it is emphasised separately that the dual nature of good faith - formal and moral - gives the court freedom to determine the qualification of actions committed.

Signs of bona fide and unfair behaviour are shown in the figure.

The complexity of checking the integrity of potential and current counterparts is noted in E.E. Bogdanova's work [Bogdanova, 2016]. According to the author, the complexity of the check is due to the system of ideas about the moral behavior of participants in civil legal relations that has developed in society. In her study, Bogdanova concludes that during the analysis of activities of counterparties, it is necessary to evaluate their morality, in particular, using the concepts of good and evil.

Fig. Signs of bona fide and unfair behaviour of participants in relationships



Source: compiled by the author.

According to the requirements of the Federal Law 'On the contract system in the sphere of procurement of goods, works, services to meet state and municipal needs' No. 44-FZ (hereinafter - Law No. 44-FZ)[10], good faith is one of the key qualities that influence the decision to enter into a contract for purchasing goods, works or services to meet state or municipal needs. Specifically, a prospective contractor must have successfully completed at least three projects within three years preceding the date of submission of an application.

Unfair conduct by one party to a relationship can lead to serious compliance consequences. For instance, current legislation provides for the following means of protection against unfair behaviour (estoppel):

- a counterparty who abuses their right may be denied the protection of this right (Clause 2 of Article 10 of the Civil Code of the Russian Federation).
- a transaction that was concluded in abuse of rights can be declared invalid (Clause 5 of Article 166 of the Civil Code of the Russian Federation) [Chernyatkin, 2018]. If a statement of invalidity of the transaction comes from a dishonest counterparty, then such statement has no legal force.
- if a counterparty has abused its rights and caused harm and material damage to another party, then that party acquires the right to recover damages (Clause 4 of Article 10 of the Civil Code of the Russian Federation) [Filippova, Zharkenova, 2018];
- if a counterparty who benefits from the occurrence of a certain condition in the transaction acts in bad faith to materialize that condition, it may be recognised as having not occurred (Clause 3 of Article 157 of the Civil Code of the Russian Federation).
- if a contract is aimed at meeting state (municipal) needs, then a person may be included in the register of unscrupulous contracting organisations [Zhukov, 2021].

An example of unfair behaviour is the case No. A60-46975/2016[11], in which an IT subject used developments of a previously created IT product that it was not the copyright holder for, and created a derivative work based on it (Article 1270 of the Civil Code of the Russian Federation). In order to recognise the unfairness of this behavior, the court appointed an expert. The expert's opinion stated that the vast majority of functional blocks, connections, and logical operations were identical in the original and derivative works.

Another example of unfair behaviour by an IT entity is case No. A40-202764/2018[12]. During the trial, it was established that the IT company attempted to unfairly appropriate exclusive rights to the results of intellectual activity and copyright objects of its former employees. In particular, the company took steps to cancel the state registration certificate for the computer program, issued by Rospatent. This document stated that the former employees were the authors and copyright holders of the product in question.

In studying the problem of unfair behaviour by participants in relationships, O.E. Zhulyeva concludes that in order to mitigate these problems, individuals should provide a 'guarantee of good faith' or include additional clauses in the contract [Zhulyeva, 2024]. According to Zhulyeva, these contracts should contain information confirming the official and tax status of participants in civil transactions, the availability of resources to fulfil obligations, as well as willingness to interact with regulatory authorities.

According to the author, Zhulyeva's position as set out in his work requires clarification. In particular, according to Federal Law No. 44-FZ, the legal and tax status of procurement participants is a criterion for their reliability, rather than good faith. As per GOST 27.002[13] reliability is an object's ability to perform specified functions within specified operational limits over a given period of time. In economic relations between entities, 'reliability' can be understood as a characteristic of their financial and economic activities system.

V.V. Koshurin, after analysing judicial practice, concluded that the method for verifying the good faith of a party is to analyse court decisions involving it [Koshurin, 2024]. He argues that verification of information about a counterparty should be carried out by studying their title documents, and when analyzing judicial practice, attention should be focused on the motives and actions taken by the counterparty during the dispute.

[10] https://clck.ru/Nh6GG.
[11] https://clck.ru/3EbpVs.
[12] https://clck.ru/3EbodH.
[13] GOST 27.002-2015. Reliability in technology. Terms and definitions (2016). Moscow, Standartinform.

2. Criteria of good faith

Based on the above, the author of this article believes that the main criteria for the integrity of IT entities should be:

1. Absence of intent to cause material damage or other harm to interested parties. The presence of such intent is characterised not only by the current behaviour of the IT subject (inclusion of clearly onerous conditions in the contract, deliberate violation of the norms of current legislation, use of the incompetence of the participants in the transaction to their detriment, etc.), but also by unfair actions that it has previously committed in past transactions. It is logical to assume that one way to check the intent to cause material damage or other harm to interested parties is by checking contracts for the presence of clearly onerous terms, as well as analysing judicial practice and decisions of supervisory bodies.

2. Availability of an effective and efficient risk management system (hereinafter referred to as RMS). According to current legislation, responsibility for implementing preventive measures to mitigate risks is assigned to the contractor (Chapter 37 and 39 of the Civil Code of the Russian Federation). If the contractor does not assess risks in advance before concluding a contract and does not proactively influence them, there is a high probability that during the execution of the work, the parties to the transaction will encounter events that negatively affect the achievement of project goals, causing material damage or other harm. Therefore, the presence of RMS should be a legal criterion for establishing the integrity of an IT company. It should be noted that, according to the standard GOST R ISO/IEC 33001[14] effectiveness is defined as the degree of implementation of preventive measures and achievement of planned results. In accordance with GOST ISO 9000[15] efficiency should be understood as the ratio between the achieved result and the resources used.

A study conducted within the framework of the research grant of the Russian Foundation for Basic Research No. 16-36-00031 'mol_a' in 495 IT entities of the Tomsk region (OKVED class 62) made it possible to establish that during the creation of IT products, about 105 universal risks can materialize, of which 5 are commercial, 45 are compliance risks and 55 are project risks [Nikolaenko, Sidorov, 2023]. Universal risks are understood as probable events that are relevant to IT projects (sprints, life cycle phases, contracts, etc.), regardless of their scale, complexity, duration (short-term, medium-term, long-term), type (software, mobile application, IS, etc.) or concept for creating IT products (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].

Commercial risks are understood as any potential threats that may prevent customers and other interested parties from benefiting from the use of the IT product. For example, unwanted derivative works, piracy, and other risks. Despite their small share in total risk (4.7%), one commercial risk could level out all resources and efforts spent, causing catastrophic damage to interested parties.

Compliance risks are understood as probable events related to the violation of the norms of current legislation, requirements of national standards and codes of conduct. A characteristic feature of compliance risks is legal consequences, expressed in sanctions from regulatory and supervisory authorities, industry associations, as well as individuals whose rights and interests have been violated.

Project risks are risks that affect one project's objective or combination of objectives. These risks typically materialize during the 'Creation of an IT Product' phase of the IT project lifecycle due to actions (or inactions) by the project manager, system analyst, legal counsel, subcontractor, and other project participants [Nikolaenko, 2025].

In light of the above, the following conclusions can be made. If IT entities intend to ensure the creation of high-quality IT products and reduce the probability of undesirable consequences for all parties involved in the relationship, they must mitigate 105 risks. The preventive elimination of these risks can serve as a quantitative and qualitative indicator that these entities have effective and efficient risk management systems in place. Since their actions indicate good faith behaviour towards preventing harm to interested parties, it may indicate their trustworthiness.

Conclusion

Thus, it can be concluded that if business entities intend to enter into contracts for the creation of IT products, they need to carry out a due diligence examination in order to ensure that there is no intent to cause material damage or other harm to stakeholders, and that there is an effective and efficient risk management system (RMS). As noted

[14] GOST R ISO/IEC 33001-2017. Information technology. Evaluation of the process. Concepts and terminology (2017). Moscow, Standartinform.
[15] GOST ISO 9000-2011. Quality management systems. Basic provisions and vocabulary (2020). Moscow, Standartinform.

earlier, compliance with these criteria increases the chances of successfully concluding contracts with IT entities who can ensure the creation of high-quality products within IT projects without undesirable consequences.

It is worth noting that the increase in the probability of successful creation of IT products is based on the mechanism of mitigating universal risks. The results of the study show that if IT companies do not assess these risks before entering into contracts and do not proactively influence them, there is a high probability that during the course of work they and the parties involved will encounter events that negatively affect the achievement of project goals.

In further studies, it will be necessary to analyse the mechanism for assessing the maturity of IT entities, as it is the high level of maturity that shows how well and effectively these entities take action to prevent events (risks) that could harm stakeholders. Based on this, it is necessary to examine in more detail existing methods for determining the level of maturity for entities engaged in computer software development and consulting services in this field (OKVED Class 62).

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.

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

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。