DOI: 10.17747/2618-947X-2024-4-360-367
УДК: 004.01
JEL: M15

Compliance-risks in the operation of IT products

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

Abstract
The article discusses compliance risks that can arise during the operation of IT products in the market and cause unacceptable damage to IT organisations. To achieve this goal, the author of this article conducted a study of civil, administrative and criminal judicial practice, where one of the parties was an IT company (OKVED 62), including disputes related to the infringement of exclusive rights to IT products. Based on the research conducted, 12 compliance risks were identified, of which 6 were civil, 1 was administrative and 5 were criminal. An analysis of judicial practice has shown that the withdrawal, distribution and operation of IT products on the market without taking into account these requirements exposes IT companies to civil, administrative and/or criminal liability. In addition, as part of the work carried out, the dynamics of criminal offences in the field of computer information was analysed, where it was found that in the period 2022-2023. The increase in offences related to unauthorised access to electronic devices rose from 9,308 to 36,788 crimes (an increase of 74.6%). The results of the study highlited the urgent need for IT stakeholdes to develop effective and efficient preventive measures to influence identified compliance risks. For example, the development of measures related to the review of requirements for documentary support of IT projects, the form and content of IT products, and ways of protecting computer information.
Keywords: IT-subject, IT-product, IT-project, risk, compliance-risk, compliance-consequence.

For citation:
Nikolaenko V.S. (2024). Compliance-risks in the operation of IT products. *Strategic Decisions and Risk Management,* 15(4): 360-367. DOI: 10.17747/2618-947X-2024-4-360-367. (In Russ.)

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

运营 IT 产品的合规风险

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

简介
文章讨论了IT产品在市场运作过程中可能出现的合规风险，这些风险会对IT 产品造成不可接受的损害。为了实现这一目标，本文作者对民事、行政和刑事法院的实践进行了研究，其中一方当事人是信息技术主体（全俄罗斯经济活动分类手册62），包括研究与侵犯信息技术产品专有权有关的纠纷。根据所进行的研究，确定了 12 项合规风险，即 6 项民事风险、1 项行政风险和 5 项刑事风险。对司法实践的分析表明，在不考虑这些要求的情况下在市场上生产、销售和运营信息技术产品，会使信息技术主体面临民事、行政和/或刑事责任的威胁。此外，正在进行的工作分析了计算机信息领域刑事犯罪的趋势，发现在 2022 年至 2023 年期间，与未经授权访问电子设备有关的犯罪案件从 9 308 起增加到 36 788 起（增加了 74.6%）。研究结果表明，信息技术主体迫切需要制定切实有效的预防措施，以应对已发现的合规风险：例如，制定与核实信息技术项目文件支持要求、信息技术产品的形式和内容以及保护计算机信息的方法有关的措施。
关键词: IT 实体、IT 产品、IT 项目、风险、合规风险、合规后果。

供引用:
Nikolaenko V.S. (2024). 运营 IT 产品的合规风险。战略决策和风险管理, 15(4): 360–367. DOI: 10.17747/2618-947X-2024-4-360-367. (俄文)

致谢
这项工作是在国家任务 "科学 "的框架内进行的, FEWM-2023-0013项目。

Introduction

An analysis of the business activities of 495 IT enterprises in the Tomsk Oblast (OKVED 62) showed that during the creation of IT products within IT projects about 170 universal risks can occur [Nikolaenko, Sidorov, 2023]. An in-depth study of the nature of these risks allowed us to divide them into four groups: commercial risks (3%), project risks (33%), external environmental risks (37%) and compliance risks (27%)[1]. In addition, it was found that the occurrence of one compliance risk causes material damage to IT organisations in the average amount of 277,000 roubles. If two compliance risks occur during the implementation of an IT project, the damage increases to 554,000 roubles, if three - to 831,000 roubles, etc.

In this article, universal risks are understood as probable events that are relevant to IT projects regardless of their size, complexity, duration, types, approaches to creating IT products and number of participants [Paladino et al., 2009; Chapman, 2011; Aven, 2012; Brandas et al., 2012; Lee et al., 2013; De Baker et al., 2014; Mishra et al., 2014; Wieczorek-Kosmala, 2014; Beer et al., 2015; Luckmann, 2015]. Compliance risks are understood as probable events associated with the violation of current legislation, requirements of national standards and codes of conduct, which have legal consequences [Nikolaenko, 2024a].

The time for updating 170 risks in the study was limited to the following phases of the IT project lifecycle: requirements generation; development of the automated system concept; development of the technical specifications (hereafter referred to as TS); development of the draft design; development of the technical design; development of the working documentatio[2,3]. Compliance risks for the 'commissioning' and 'maintenance' phases were not identified due to the stated objectives of the study. However, it is important to note that information about the risks that may materialise during these phases and lead to compliance consequences is very important for IT organisations that plan to introduce, distribute and operate IT products on the market.

To confirm this, we can cite examples where the subject of the dispute was the exclusive rights to the created IT products. For example, in case No. A83-6393/2023[4] 1C LLC asked the court for compensation for infringement of exclusive rights in the amount of 268,000 roubles. In Case No. A81-11865/2022[5] 1C LLC and 1C-Soft LLC demanded payment of 4.7 million roubles from Partner JSC. In Case No. A50-4247/2023[6] 1C LLC claimed compensation in the amount of 684,000 roubles for the illegal use of IT products. In case No. A36-7440/2022[7] 1C LLC asked the court to protect the exclusive rights to IT products owned by 1C LLC and to recover 50,000 roubles from the infringer. Similar claims are registered in cases No. A35-7078/2022[8] and No. A08-16/2022[9]. In case No. A29-10372/2022[10] 1C LLC applied to the court for compensation for the illegal use of IT products in the amount of 342,000 roubles. In case No. A14-13243/2022[11] 1C LLC and 1C-Soft LLC claimed compensation from SpetsTekh-Stroy LLC for the illegal use of IT products in the amount of 2.4 million roubles.

An analysis of judicial practice also shows that there are frequent cases where the infringement of exclusive rights is converted into criminal liability. A clear example is case No. 1-209/2022[12], where the defendant copied a file of an IT product onto a USB drive without the proper permission of the copyright holder, 1C-Soft LLC, and performed numerous illegal installations, thereby obtaining commercial benefits. By his criminal actions, the defendant violated the constitutional right of the copyright holder to protect intellectual property, as provided for in Article 44, Part 1 of the Constitution of the Russian Federation[13], and caused damage to him in the amount of 4.2 million roubles.

Based on the above, it can be concluded that the purpose of this article is to identify compliance risks that may arise during the operation of IT products on the market It is important to note that in accordance with the provisions of Article 17 of the Federal Law 'On Information, Information Technologies and Protection of Information' No. 149-FZ[14] (hereinafter referred to as the 'Law'), offences in the sphere of information technologies are subject to disciplinary, civil, administrative and/or criminal liability. In order to achieve this objective, a study was made of the judicial practice in cases where the subject of the dispute was the infringement of rights to IT products or where one

[1] Nikolaenko V. (2023). Impeccable risk management: a textbook. Tomsk, TUSUR publishing house.
[2] GOST R 59793-2021 (2020). Information technology. Standards for automated systems. Automated systems. Stages of creation. Moscow, Standardinform.
[3] GOST R 57102-2016/ISO/IEC TR 24748-2:2011 (2016). Information technology. Systems and software engineering. Life cycle management. Part 2. Guide to the use of ISO/IEC 15288. Moscow, Standartinform.
[4] Decision of the Arbitration Court of the Republic of Crimea in Case No. A83-6393/2023 of 18.09.2023. https://clck.ru/36cnZT.
[5] Decision of the Arbitration Court of the Yamalo-Nenets Autonomous Okrug in Case No. A81-11865/2022 dated 13.08.2023. https://clck.ru/36cpoK.
[6] Decision of the Arbitration Court of Perm Krai in case No. A50-4247/2023 dated July 27, 2023. https://clck.ru/36cpzX.
[7] Decision of the Arbitration Court of the Lipetsk Region in case No. A36-7440/2022 dated 13.06.2023. https://clck.ru/36cq88.
[8] Decision of the Arbitration Court of the Kursk Region in case No. A35-7078/2022 dated 13.03.2023. https://clck.ru/36d5KQ.
[9] Decision of the Arbitration Court of the the Belgorod Region in case No. A08-16/2022 dated 07.11.2002. https://clck.ru/36d7n5.
[10] Decision of the Arbitration Court of the Kursk Region in case No. A29-10372/2022 dated 30.12.2002. https://clck.ru/36d5W7.
[11] Decision of the Arbitration Court of the Voronezh Region in case No. A14-13243/2022 dated 07.11.2022. https://clck.ru/36d7f5.
[12] Judgment of the Proletarsky District Court of Saransk, Republic of Mordovia, in case No. 1-209/2022, dated 09.07.2002. https://clck.ru/36eUWo.
[13] Constitution of the Russian Federation. https://clck.ru/MsKLk.
[14] The Federal Law 'On Information, Information Technologies and Protection of Information' No. 149-FZ of 27 July 2006. https://clck.ru/ggWjK.

of the parties was an IT company (OKVED 62).

1. Civil law risks

An analysis of arbitration court practice has shown that during the operation of IT products, as a rule, two types of risk events occur: risks related to the quality of the IT results of the work performed (rendered IT services, delivered IT goods) and risks related to the exclusive rights to the results of intellectual activity (hereinafter - RIA). According to Article 1261 of the Civil Code of the Russian Federation[15] An IT product is a RID [Kuznetsova et al., 2022]. Let us look at the content of these compliance risks in more detail.

The risk of discovering defects when using the results of the work performed (services rendered, goods delivered). The legislator understands a deficiency of work (service, product) as any non-compliance with mandatory requirements of laws, national standards, contract terms, etc. [Gayazov, 2022]. [Gayazov, 2022]. For example, if an IT product does not meet the stated requirements, it will be considered low quality, which can have negative compliance consequences for both the contractor (performer, supplier) and the customer. In particular, if it is established that the elimination of the defects will require significant costs or the nature of the defects is such that the defects will be discovered repeatedly, the customer (buyer) has the right to demand a refund of the previously paid amount [Mikhailenko, Kovaleva, 2021]. It is worth noting that the work [Nikolaenko, 2024b] notes that an IT product is a complex legal object consisting of two parts - an IT service and/or RIA (computer programs).

An illustrative example of the identification of defects during the operation of an IT product is Case No. A45-15497/2020[16], where a contract was concluded between Era LLC (the contractor) and Smartmedia LLC (the client), under which the contractor was obliged to perform and the client was obliged to pay for work on the creation of the Boom Boom mobile application on the Android and iOS platforms. During the "support" of the created IT product, the client identified a large number of software defects and requested the contractor to redo the work. The contractor refused to comply. In order to determine the nature of the defects, the court ordered an expert examination, which concluded that the result of the work performed partially complied with the terms of the contract, was of poor quality, and required the removal of the identified defects. As a result, the court decided to recover 133.7 thousand roubles from Era LLC.

Risk of copyright infringement. If individuals produce, distribute and operate IT products without the permission of copyright holders, these programmes are considered unlicensed (counterfeit) [Kopylov, 2019]. The use of such IT products is prohibited and may result in civil or administrative liability for legal entities and criminal liability for natural persons.

The consequences in the event of a risk of copyright infringement may be a ban on the use of the RIA by the copyright holder with subsequent recovery of damages (compensation) [Kotovshchikov, 2017]. In addition to the civil law consequences for the person who has infringed intellectual property rights, more serious compliance consequences may be imposed if, for example, the person has imported, sold or rented out counterfeit works in order to make a profit, or has provided false information about the copyright holders on copies of the works. If the fact of committing such an act is established, the subject will be brought to administrative responsibility in accordance with Article 7.12 of the Code of Administrative Offences of the Russian Federation[17].

An example is case 5-1637/2021[18], where the offender illegally exploited copyrighted items in business activities, namely the use of counterfeit IT products for Sony PlayStation 4 Pro consoles. The court found the offender guilty and sentenced him to an administrative fine of 15,000 roubles without confiscation of property.

It is important to note that the severity of the offence is increased if the subject appropriates authorship (plagiarism) and causes material damage to the author or copyright holder. In this case, the person may be held criminally liable in accordance with Article 146 of the Criminal Code of the Russian Federation[19]. For example, in case No. 1-108/2020[20] the defendant violated the exclusive rights of the copyright holder, 1C LLC, and caused property damage in the amount of 545.4 thousand roubles.

The risk that the copyright holder will prohibit the use of the RIA. According to Article 1252 of the Civil Code of the Russian Federation, if a subject violates the rights to intellectual property, the copyright holder has the possibility to stop illegal actions in the form of a direct prohibition. An example of the occurrence of such a risk is Case No. A53-23110/22[21], , in which Sistema-1 LLC asked the court to prohibit RSTU, the Federal State Budgetary Educational Institution of Higher Education, from illegally using the IT product LabWagon. After studying the case materials, the court dismissed the claims, concluding that an employee of

[15] Civil Code of the Russian Federation (CC RF). Commentary on the latest amendments (2019). Moscow, ABAK.
[16] Decision of the Arbitration Court of the Novosibirsk Region in case No. A45-15497/2020 dated 03.24.2022. https://clck.ru/36d7VV.
[17] Code of Administrative Offences of the Russian Federation (CAO RF) https://clck.ru/MsKtY.
[18] Decision of the Stavropol Industrial District Court No. 5-1637/2021 of 03.06.2021. https://clck.ru/36eUaL.
[19] Criminal Code of the Russian Federation (CC RF) of 13.06.1996. No. 63-FZ. https://clck.ru/ggWjK.
[20] Judgment of the Shpakovsky District Court of Stavropol Territory in case No. 1-108/2020 dated 24 September 2020. //sudact.ru/regular/doc/Tg3F5jz1VEox/.
[21] Decision of the Arbitration Court of the Rostov Region in case No. A53-23110/22 dated 07.06.2023. https://clck.ru/36cr8y .

Sistema-1 LLC was the author of LabWagon, but not the copyright holder. The court found that this employee created the disputed IT product as part of a work assignment when he was in an employment relationship with RSTU, the Federal State Budgetary Educational Institution of Higher Education.

The risk that the copyright holder will recover damages (compensation) for infringement of intellectual property rights. In addition to a direct prohibition to suppress actions that violate intellectual property rights, the copyright holder is given the opportunity to recover damages from the subject in the form of compensation for losses or payment of compensation in the range of 10 thousand to 5 million roubles [Shorokhov, 2020].

An illustrative example of the materialisation of the risk in question is Case No. A50-17729/2022[22], in which the copyright holder, 1C LLC, having established the fact of illegal use of its IT product, applied to the court for compensation from the individual entrepreneur Yazykova G.L. in the amount of 400,000 roubles.

It is worth noting that, in practice, cases of violation of the terms of license agreements are also common. For example, in case No. A67-8506/2018[23] SAB LLC asked the court to recover from NP Baikal-Tender a debt under the licence agreement in the amount of 3.5 million roubles.

The risk that the exclusive right to the intellectual property may not be recognised for the author. Failure to comply with the rules for the creation of intellectual property, for example, within the framework of labour relations between an employer and an employee, can lead to a negative scenario if the employer cannot prove that he is the copyright holder [Zaidova, 2021]. According to Article 1295 of the Civil Code of the Russian Federation, the exclusive right to a work for hire created by an employee within the framework of established work duties belongs to the employer.

An example of the materialisation of the risk in question is Case No. A40-90889/21-134-529[24], in which VIST Group JSC asked the court to prohibit the use of the ALTAN IT product. In support of its claims, VIST Group JSC referred to the fact that the IT product was developed by its former employees as part of their official duties. After reviewing the case materials, the court refused to grant the claims, stating that in order to establish the fact that the exclusive rights to the ALTAN programme belong to VIST Group JSC, it is necessary to confirm the fact that the employees were given a service contract. The court concluded that the IT product created was not a work for hire, and therefore JSC VIST Group was not the copyright holder of the ALTAN programme.

Risk of creating unwanted derivative works. According to Article 1270 of the Civil Code of the Russian Federation, the processing (modification) of IT products may lead to the creation of a derivative work, which is an independent object of copyright [Beskodarova, 2020]. This circumstance may lead to unwanted disputes. An example of such a conflict is Case No. A56-38522/2020[25], where Nmarket.PRO Rus LLC (the plaintiff) asked the court to jointly and severally recover damages in the amount of 2 million rubles from the owners of the website panpartner.ru. In support of its claims, the plaintiff argued that the software part of the search module website was its IT product. The court-appointed experts concluded that the total volume of the search engine module code was 2,669 lines, of which 589 lines (22%) were used by the site without modification and 1,522 lines (57%) were partially modified. Based on the experts' findings, the court concluded that the site's owners had illegally modified the search engine, thereby creating an unwanted derivative work.

2. Administrative risks

If an entity violates information security requirements during the creation and subsequent operation of IT products, for example, by using uncertified information systems, databases and other means of information security, the entity may be subject to administrative liability in accordance with Article 13.12 of the Code of Administrative Offences of the Russian Federation.

According to Article 21 of the Law No. 149-FZ, any information, including computer information, is subject to protection if its unlawful use may cause damage to its owner. This threat is eliminated through the use of protective measures: for example, IT units must obtain special licences that allow them to carry out information security activities.

A clear example of the occurrence of a risk associated with a violation of the requirements of the information protection rules is Case No. 5-300/2015[26]. The case documents show that during the inspection, InfoTelecom LLC failed to comply with the requirement to have qualified personnel on site. This fact was the basis for bringing the IT unit under administrative responsibility.

3. Criminal risks

According to the report on the state of criminality in 2022, 522.1 thousand crimes committed with the use of IT or in the field of computer information were registered in the Russian Federation - 26.5% of the total number of crimes. In 2023, 585.2 thousand such crimes

[22] Decision of the Perm Krai Arbitration Court in case No. A50-17729/2022 dated 28.12.2002. https://clck.ru/36d5id.
[23] Decision of the Arbitration Court of Tomsk Oblast in case No. A67-8506/2018 dated 15.11.2018. https://clck.ru/3957JU.
[24] Decision of the Moscow Arbitration Court No. A40-90889/21-134-529 dated 10/05/2023. https://clck.ru/36cmjw.
[25] Decision of the Arbitration Court of St Petersburg and Leningrad Region in Case No. A56-38522/2020 dated 14.04.2023. https://clck.ru/36d4mB.
[26] Order of the Sovietsky District Court of Bryansk in Case No. 5-300/2015 of 29.05.2015. https://clck.ru/36ZdQH.

were recorded - 34.3% of the total number of crimes[27]. An analysis of judicial practice has shown that the main criminal risks arising from the use of IT products relate to economic activity and computer information. Let us look at them in more detail.

The risk of theft of property by entering, deleting, blocking or modifying computer information, also known as fraud in the sphere of computer information (Article 159.6 of the Criminal Code of the Russian Federation). According to the Law No. 149-FZ, computer information is information stored in electronic devices and computer programs. This risk is characterised by the commission of an act connected with the input, deletion, blocking, modification of computer information for the purpose of stealing another person's property or acquiring the right to such property. According to the Russian Ministry of Internal Affairs, 334 cases of computer information fraud were registered in Russia in 2022, and 417 such crimes in 2023.

An example of illegal input of computer information is Case No. 1-422/2016[28], An example of illegal input of computer information is Case No. 1-422/2016, where the defendant, using the victims' mobile phones and SIM cards, repeatedly illegally withdrew funds from the victims' accounts by sending SMS messages.

Modification of computer information is the alteration of information in an electronic device or computer program. An example of illegal modification of computer information is case No. 1-26/2017[29], in which the defendant used the victim's mobile phone to make changes to the original state of bank card account data.

It is worth noting that computer information can be altered not only in electronic devices and computer programs, but also in databases. For example, in Case No. 1-30/2018[30] the defendant knowingly entered into the AIS-Tax database false information about the existing overpayment of VAT by a legal entity.

An example of another interference with the functioning of the means of storing, processing and transmitting computer information is presented in case No. 1-139/2016[31], where the defendant stole money through the personal account of the President-Service programme, using a login and password obtained by criminal means, by returning electronic travel documents at the ticket offices of the railway station.

Case No 1-48/2020 should be mentioned separately[32]. According to the case documents, the defendants and an unidentified person used illegally obtained login/password pairs to access the personal accounts of customers of the 'Kukuruza' multifunctional bonus payment card and carried out a number of operations to steal electronic money.

Risk of unauthorised access to computer information. Risk of unauthorised access to computer information. According to the Russian Ministry of Interior, 9,308 cases of unauthorised access to computer information were registered in Russia in 2022, and 36,788 such crimes were registered in 2023.

According to the Criminal Code of the Russian Federation, access to computer information by a person who does not have the right to receive and work with such information, in relation to which special protective measures have been taken to limit the circle of persons who have access to it, is recognised as illegal. If a subject performs illegal or unauthorised access, he/she may be criminally liable in accordance with Article 272 of the Criminal Code of the Russian Federation.

An example of unauthorised access to computer information is Case No. 1-190/2016[33]. According to the case documents, the defendant committed nine offences by installing counterfeit copies of IT products (Kompas-3D V16, CorelDRAW X6, Microsoft Windows 7 and Microsoft Office Professional Plus 2010) with the aim of selling and profiting from the sale of counterfeit copies of IT products. The total amount of material damage caused by the defendant to the copyright holders was 1.6 million roubles.

An example of the modification of computer information is case No. 1-257/2023[34], where the defendant, an office specialist, obtained unauthorised access through the 1C Retail programme and illegally issued SIM cards.

An example of the copying of computer information, i.e. the transfer of information to another medium while leaving the original information unchanged, is case no. 1-457/2022[35], where the defendant copied and transmitted the personal data of property owners in a chat room of an instant messaging service.

The risk of creating, using and distributing malicious computer programs. Malicious programs are computer viruses designed to cause the unauthorised destruction, blocking, alteration or copying of computer information. If a person uses and distributes malware, he or she may be prosecuted in accordance with Article 273 of the Criminal Code of the Russian Federation. According to the Ministry of Interior of the Russian Federation, in 2022, 200 cases of creation, use and distribution of

[27] Federal State Institution 'Central Information and Analysis Centre'. https://clck.ru/395A4r.
[28] Judgment of the Rudnichny District Court of Kemerovo, Kemerovo Oblast, Case No. 1-422/2016, dated 26 September 2016. https://clck.ru/395cv4.
[29] Judgment of the Bratsk City Court of the Irkutsk Region in Case No. 1-26/2017 of 22 September 2016. https://clck.ru/395d3Z.
[30] Judgment of the Leninsky District Court in Case No. 1-30/2018 of 11.04.2017. https://clck.ru/395dBV.
[31] Judgment of the Sinarsky District Court of Kamensk-Uralsky, Sverdlovsk Oblast, in Case No. 1-139/2016, dated 17 September 2016. https://clck.ru/395dKd.
[32] Judgment of the Kuibyshevsky District Court of Omsk in case No. 1-48/2020 dated 27.12.2019. https://clck.ru/395dPY.
[33] Judgement of the Severskiy City Court of the Tomsk Oblast in case No. 1-190/2016 dated 23.06.2016. https://clck.ru/36VDoX.
[34] Judgement of the Zlatoust City Court of the Chelyabinsk Region in the case No. 1-257/2023 of 11.04.2023. https://clck.ru/36UcMi.
[35] Judgement of the Kuznetsk district court of Penza Oblast in case No. 1-457/2022 dated 08.12.2022. https://clck.ru/36Ucs4.

malicious computer programs were registered in Russia (36.9% less than in 2021), in 2023 - 196 such crimes.

An example of the use of a computer virus to copy computer information is case number 1-226/2023[36], where the defendant used a virus to view video images from surveillance cameras and webcams on Internet users' personal computers and made unauthorised copies from those devices.

Case 1-355/2023 is an example of the neutralisation of protective equipment[37]. Neutralisation of security means is the negative impact on technical, cryptographic and other means with the aim of gaining unauthorised access to protected computer information. According to the complaint, the defendant illegally used the malicious program techsys.dll to neutralise the protection tools installed by the copyright holder.

The risk of violating the rules for operating means of storing, processing or transmitting computer information. According to the Criminal Code of the Russian Federation, liability for violating the rules of access and operation arises if the subject causes damage to the owner, the amount of which exceeds 1 million rubles. In this case, the subject may be held criminally liable in accordance with Article 274 of the Criminal Code of the Russian Federation.

A good example of the occurrence of the risk in question is Case No. 1-22/2021[38], where the defendants and an unidentified person developed plans to secretly steal money from ATMs in the Krasnoyarsk Territory and illegally entered the ATMs, violating the rules for their operation. To do this, they connected a laptop to the ATM and used malicious programs that caused the ATMs to continuously dispense all available cash. In total, the defendants made four connections and caused losses to the owners of 17.5 million roubles.

Risk of unlawful impact on the critical information infrastructure of the Russian Federation (hereinafter referred to as RF CII) According to Article 2 of the Federal Law 'On the Security of Critical Information Infrastructure of the Russian Federation' No. 187-FZ[39] (hereinafter referred to as Law 187-FZ), critical information infrastructure is the information systems of critical information infrastructure entities. A person who unlawfully interferes with critical information infrastructure may be criminally liable under Article 274.1 of the Criminal Code of the Russian Federation.

An example of risk materialisation is case 1-171/2023[40]. An examination of the case materials revealed that the defendants connected the mobile payment services to the subscriber numbers of PJSC VimpelCom, whose information infrastructure is an object of the critical information infrastructure of the Russian Federation. The illegal actions of the defendants violated the integrity and relevance of computer information. In order to localise the problem, PJSC VimpelCom was forced to suspend the MTopUp service on the territory of the Russian Federation.

Conclusion

As a result of the study, 12 compliance risks were identified - 6 civil, 1 administrative and 5 criminal. Separately, it is worth noting the dynamics of growth in offences committed using IT or in the field of computer information. In particular, in the period 2022-2023, the increase in offences related to unauthorised access to computer information and electronic devices rose from 9,308 to 36,788 cases, i.e. by 74.6%.

The results obtained indicate the need for IT entities to establish effective and efficient preventive measures to influence the identified compliance risks, such as compliance with and implementation of requirements for documentation support of IT projects, the form and content of IT products, and methods for protecting computer information. An analysis of legal practice has shown that the introduction, distribution and operation of IT products on the market without taking these requirements into account puts IT organisations at risk of undesirable compliance consequences.

References

Beskodarova V.S. (2020). Author's agreements. *Synergy of Sciences,* 45: 158-163. (In Russ.)

Gayazov I.R. (2022). On the issue of modifying computer programs. *Internauka,* 22-6(245): 21-32. (In Russ.)

Zaidova E.B. (2021). Problems of the efficiency model of granting real rights to a computer program through an author's order. *Scientific Research of the XXI Century,* 1(9): 331-334. (In Russ.)

Kopylov A.Yu. (2019). Basic qualifying characteristics of works as an object of copyright. *Issues of Russian and International Law,* 9(10-1): 106-112. (In Russ.)

[36] Judgement of Tula Proletarskiy District Court No. 1-226/2023 dated 31/08/2023. https://clck.ru/36UeQA.
[37] Verdict of the Novy Urengoy City Court of the Yamalo-Nenets Autonomous District in Case No. 1-355/2023 dated 27 September 2023. https://clck.ru/36UeHN.
[38] Judgement of the Sovietsky District Court of Krasnoyarsk in case No. 1-22/2021 from 03.06.2021. https://clck.ru/36Uezy.
[39] Federal Law of 26.07.2017 No. 187-FZ 'On the Security of Critical Information Infrastructure of the Russian Federation'. https://clck.ru/33sX2n.
[40] Judgement of the Vakhitovsky District Court of Kazan, Republic of Tatarstan in Case No. 1-171/2023 dated 02.11.2022. https://clck.ru/36UdEr.

Kotovshchikov A.V. (2017). Computer programs in the system of objects of object rights. In: *Current problems of graphic law and graphic legal proceedings:* 75-78. (In Russ.)

Kuznetsova K.O., Chernova E.A., Mayer V.R., Garifullin R.F. (2022). Information management. *Interscience,* 40-4(263): 54-55. (In Russ.)

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

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

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

Shorokhov D.A. (2020). Selection of software for creating a website. *Current Scientific Research in the Modern World,* 7-1(63): 219-226. (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: *Exploring the Information Frontier: International conference on information systems:* 1-18.

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

Chapman R. (2011). *Simple tools and techniques for enterprise risk management.* Chichester, Wiley.

De Baker 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. *Journal of the Southern African 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,* 16(1): 33. DOI: https://doi.org/10.3390/jrfm16010033.

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

Wieczorek-Kosmala M. (2014). Risk management practices from risk maturity models perspective. *Journal for East European Management Studies,* 19(2): 133-159.

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, Tomsk Polytechnic University (Tomsk, Russia); associate professor at the Department of Economics, Sociology, Political Science and Law, Siberian State Medical 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 S. 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（（俄罗斯，托木斯克）信息处理自动化系教授；托木斯克理工大学（俄罗斯，托木斯克）商学院副教授；西伯利亚国立医科大学（俄罗斯，托木斯克）经济学、社会学、政治学和法学系副教授。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 21.11.2024; revised on 18.12.2024 and accepted for publication on 22.12.2024. The author read and approved the final version of the manuscript.
文章于 21.11.2024 提交给编辑。文章于 18.12.2024 已审稿。之后于 22.12.2024 接受发表。作者已经阅读并批准了手稿的最终版本。