DOI: 10.17747/2618-947X-2025-3-275-287
UDC 338.2

Artificial Intelligence adoption: Drivers and barriers to development

M.P. Loginov[1, 2, 3]
N.V. Usova[1, 2, 3]
P.A. Kukanova[3]
S.A. Alekseeva[3]
[1] Ural State University of Economics (Yekaterinburg, Russia)
[2] Ural Federal University(Yekaterinburg, Russia)
[3] RANEPA, Ural Institute of Management(Yekaterinburg, Russia)

Abstract

The article explores the challenges to Russia's economic security caused by the development and implementation of artificial intelligence (AI) in the context of digital transformation and global technological competition. The purpose of the study is to identify the most significant threats to the country's economic security in the context of the popularisation of AI technologies and propose measures aimed at addressing them, taking into account the current situation. To achieve this goal, the authors analysed the dynamics of the Russian AI market, its structure by industry and growth rates, as well as the main external and internal risks associated with the use of AI technologies. Special attention is paid to the trends in the development of the AI market, cyber threats, economic and cyber espionage, proliferation of deepfakes, and problems of technological dependence on foreign suppliers and sanctions pressure. Internal challenges include staff shortages, polarisation of digitalisation in industries, concentration of resources in large companies, and lack of regulatory oversight. It is shown that these factors significantly limit the development potential of the domestic AI market and create prerequisites for economic and technological vulnerability in the country. The article suggests measures to minimise threats, including the development of domestic solutions, decentralisation of resources, annual monitoring of digital maturity and digital literacy in industries, the use of various mechanisms to support small and medium-sized businesses depending on the industry affiliation and the role of a company in a particular market. It also proposes improvement of the regulatory framework, relaxation of regulations, and provision of comfortable working conditions for IT specialists in Russia, as well as training of qualified personnel. The conclusion is drawn about the need for a comprehensive approach to ensuring Russia's economic security in the context of the rapid development of artificial intelligence. The results obtained can be applied both in the practical activities of organisations using AI technologies and in the activities of government authorities to develop strategic and other policy documents for the development of the AI market.

Keywords: cyber threats, cyberattacks, deepfakes, digital technologies, and technological security

For citation:

Loginov M.P., Usova N.V., Kukanova P.A., Alekseeva S.A. (2025). Artificial Intelligence adoption: Drivers and barriers to development. *Strategic Decisions and Risk Management,* 16(3): 275-287. DOI: 10.17747/2618-947X-2025-3-275-287. (In Russ.)

AI采用：发展的驱动和障碍因素

M.P. Loginov[1, 2, 3]
N.V. Usova[1, 2, 3]
P.A. Kukanova[3]
S.A. Alekseeva[3]
[1] 乌拉尔国立经济大学（俄罗斯，叶卡捷琳堡）
[2] 俄罗斯联邦第一任总统鲍里斯·叶利钦乌拉尔联邦大学（俄罗斯，叶卡捷琳堡）
[3] 罗斯联邦总统国民经济和行政学院乌拉尔分院（俄罗斯，叶卡捷琳堡）

简介

本文研究了在数字化转型与国际技术竞争背景下，人工智能（AI）的发展与应用对俄罗斯经济安全构成的威胁。本研究旨在识别人工智能（AI）技术应用背景下对国家经济安全构成的最重大威胁，并制定相应的风险消减措施。　　　本文作者分析了俄罗斯人工智能（AI）市场的动态变化、行业结构及增长趋势，并重点研究了与AI技术应用相关的主要外部和内部风险。研究特别关注AI市场的发展趋势、网络威胁、经济间谍与网络间谍活动、深度伪造（Deepfake）技术扩散，以及对外国供应商的技术依赖问题和制裁压力等挑战。研究分析了内部挑战：人才短缺、各行业数字化进程不均衡、资源向大型企业过度集中，以及法规监管不足等问题。研究表明，这些因素严重制约了俄罗斯国内人工智能（AI）市场的发展潜力，并可能引发国家经济与技术层面的脆弱性。　　　文章提出了一系列风险消减措施，包括：发展本国解决方案，推动资源去中心化、建立行业数字化成熟度与数字素养年度监测机制、根据企业所属行业及其在特定市场中的角色实施差异化中小企业扶持政策、完善法规体系、吸引海外人才回流，以及为在俄境内工作的IT领域专家提供舒适工作条件并培养高素质专业人才。研究结论指出，在人工智能（AI）迅猛发展的背景下，必须采取综合措施保障俄罗斯经济安全。研究成果既可供应用AI技术的各类组织在实际工作中参考，也能为政府部门在制定人工智能市场发展战略及其他规划文件时提供决策依据。

关键词：网络威胁、网络攻击、深度伪造、数字技术、技术安全

供引用:

Loginov M.P., Usova N.V., Kukanova P.A., Alekseeva S.A. (2025). AI采用：发展的驱动和障碍因素。 战略决策与风险管理, 16(3): 275–287. DOI: 10.17747/2618-947X-2025-3-275-287. (俄文)

Introduction

As human society evolves, it creates and improves its methods of attack and defense. Similarly, the current development of artificial intelligence (AI) can be compared to the invention of the bow and arrow, which led to the creation of the long arm, significantly changing human life. The development of 'long arm' never stops and the evolution of offensive weaponry continues. While modern AI is still at the stage of choosing between a bow and an arrow, humanity is essentially developing its 'smart arms' or 'digital heads'. The future development of AI technologies and their potential consequences cannot be accurately predicted over the long term. However, it is crucial to address the issue of 'shielding', that is, protecting against the threats posed by AI now, as the current 'long arm' could potentially plunge the planet into chaos and destroy humanity.

To defend against AI threats, we need to take multiple approaches:

– Ensuring the stability of AI against external and internal threats, such as electronic worms, viruses, and Trojans;
– Detecting and preventing constitutional AI, implementing code insertions to prevent it from committing illegal actions, and training it not to commit illegal acts when time limits or conditions are met;
– Technologies using AI as a countermeasure to prevent illegal actions that threaten human life and state security;
– Training, certifying, and approving AI technologies for market use in accordance with security requirements;
– Parity between national systems using AI and foreign ones.

The authors examine the threats to Russia's economic security associated with the active development and implementation of AI technologies in the country's economy. These threats are particularly significant at the current stage of digital transformation and ensuring technological sovereignty amid international competition in this area. The study aims to identify the most significant threats and propose measures to mitigate them given the current situation.

To achieve these goals, the authors consistently address tasks such as analysing the Russian AI market, identifying the main risks and challenges associated with the use of AI, and proposing measures to minimise identified threats.

In terms of methodology, a retrospective analysis of data characterising the state of AI market development in Russia and cyberattacks in Russia is conducted. Analysis of external and internal threats associated with implementation of AI at national level is performed. This made it possible to identify problems of developing 'smart hand' or 'digital head' and, based on application of synthesis, propose set of measures aimed at solving 'shield' problem.

1. Theoretical aspects of the study

Recent years have seen growing interest in research not only in the digital economy, but also in one of its key technologies, artificial intelligence. Given the multifaceted nature of this issue, we are interested in examining artificial intelligence specifically as a potential threat to Russia's economic security. Therefore, this study focuses on the work of leading Russian scholars.

For example, A.S. Danchenko notes that 'digitalisation has become the most important driver of the modern economy and a condition for ensuring economic security, determining the importance of technological and innovative solutions in all sectors of the national economy' [Danchenko, 2024].

In his analysis of the technical aspects of AI, A.A. Balashov highlights the potential for increased unemployment due to technological advancements, as well as concerns regarding cybersecurity threats and the spread of misinformation. He also discusses the possibility of government agencies utilising 'profiling,' which raises questions about its safety and ethical implications [Balashov, 2023].

At the same time, ensuring economic security should include not only technical and information support, but also the digital competence of employees and management, as well as legal protection through improving existing legal norms [Mamontova, 2022].

Research into AI technologies for economic security reveals the transformation and increasing sophistication of crime methods driven by technological advances. At the same time, AI systems have significant potential to identify risks associated with ensuring a country's economic security [Dyatlova, Svirina, 2024].

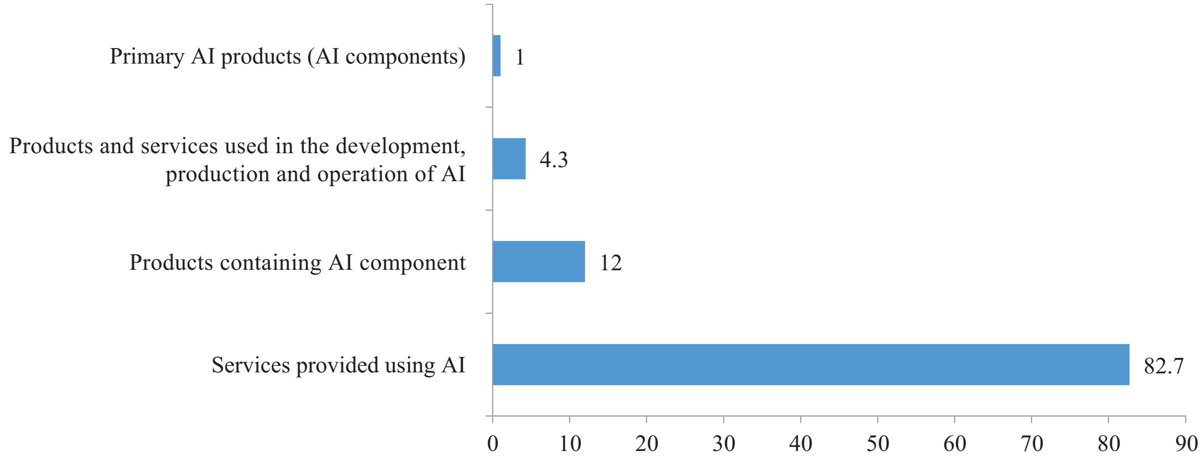
Aspects of AI, such as the digital shadow economy [Obukhova, Piyaltsev, 2021] and the use of AI technologies in assessing the level of economic security at the national level have also been studied [Balashov, 2024].

Based on the results of assessing the state's economic security during large-scale implementation of neural networks in various sectors of the national economy, it was noted that there are threats related to the banking sector when working with artificial intelligence, such as AI malfunctions and damage to customers and the bank itself [Mankovsky, 2023].

I.N. Romanova, examining the risks and threats of AI technology implementation, notes that the main threats include: complete dependence on computers; errors and failures in intelligent information systems; the unpredictability of intelligent robots; the lack of security; threat to information privacy; impossibility of accountability; and creation of artificial superintelligence. As a response, she proposes closer cooperation between government and AI developers; socially responsible behavior by developers; involvement of top scientists and experts; application of best international security practices [Romanova, 2021].

A set of mechanisms have been identified through which AI technologies can contribute not only to reducing the level of risk but also to increasing the resilience of the economic system: forecasting based on neural networks, monitoring and optimisation of business processes, rationalisation of risk management systems,

Fig. 1. The structure of soled goods, works and services related to AI technologies by type of good and service, 2023 (%)



Source: [Artificial Intelligence.., 2025].

and modeling the dynamics of complex socio-economic systems [Barakin, Shailieva, 2023].

One cannot but agree that 'one of the key areas for AI use in Russia's economic security is its application to the analysis and forecasting of macroeconomic processes. Modern machine learning algorithms allow for processing vast volumes of data and identifying patterns that might escape human analysis' [Smorodina et al., 2024].

In general, the main barriers to digitalisation of the Russian economy and implementation of AI include lack of investment resources, infrastructure limitations, insufficient legal regulations, shortage of specialised personnel, and fears and tensions in society caused by the expectation of possible structural unemployment [Elin et al., 2024].

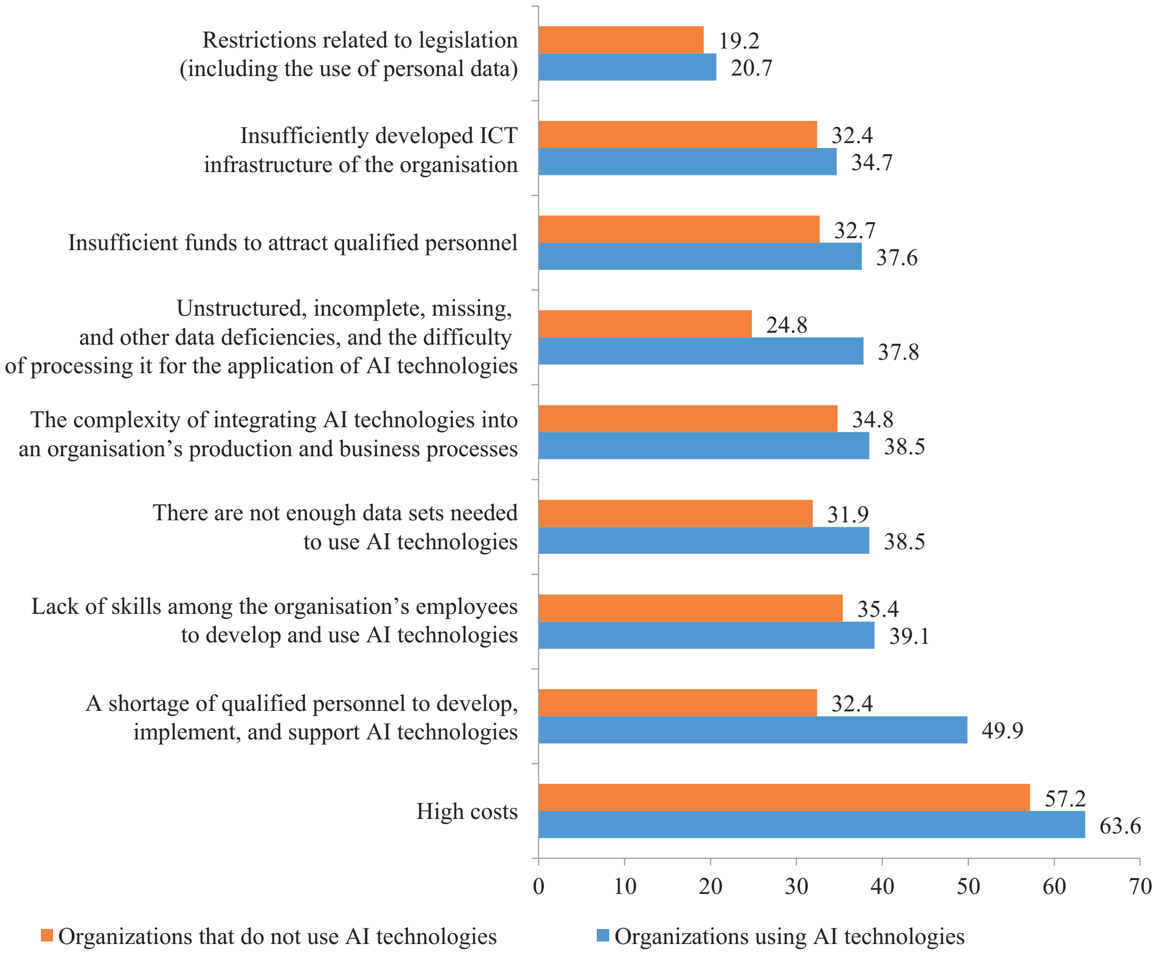
As can be seen from the results of the review of scientific papers conducted, there is still a gap in research on AI technologies with regard to national economic security.

2. The current state of demand for AI technologies in Russia

The Russian artificial intelligence market has shown steady and rapid growth in recent years. According to various analytical agencies, the market size was estimated at approximately 80-90 billion rubles in 2021, and by 2022 it had grown to 647 billion rubles, an 17% increase. In 2023, the market reached 900 billion rubles, with a year-on-year increase of 37%. Estimates of the Russian AI market size vary: the NTI Competence Center at MIPT estimates it at 130-160 billion rubles; Smart Ranking estimates it at about 305 billion rubles and TAdviser estimates around 320 billion. Meanwhile, investments in AI grew 36% in 2014, reaching 304 billion roubles [Borovkov et al., 2024].

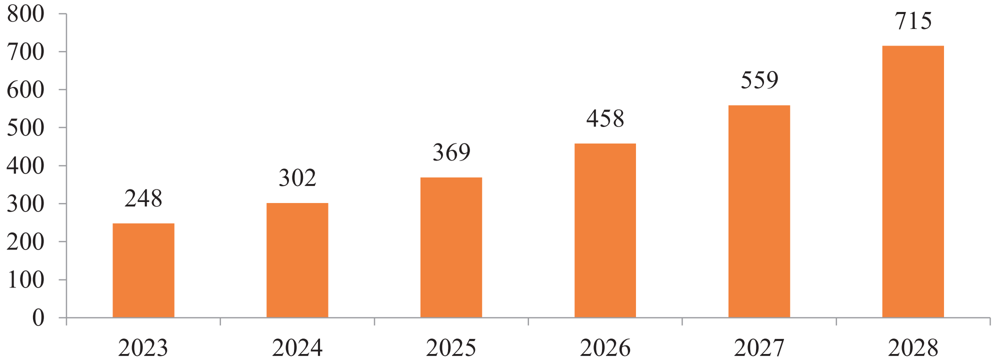
According to forecasts from experts at NTI Safenet and the NTI Competence Center, revenue from the Russian AI project market is expected to grow to 600-800 billion rubles by 2025, representing a two to three-fold increase compared to 2024. The contribution of

Fig. 2. Barriers to AI adoption by organisations, 2023
(% of respondents' answers)



Source: [Artificial intelligence.., 2025].

Fig. 3. Forecast for the development of the Russian cybersecurity market
(billion rubles)



Source: Forecast for the development of the cybersecurity market in the Russian Federation for 2024-2028. https://www.csr.ru/upload/iblock/f14/bnl532lqmqd0u23s1ftuzw4n3ycm1to1.pdf.

the AI sector to Russia's GDP could reach up to 2% [Borovkov et al., 2024].

Of interest is the structure of sales of goods, works, and services related to AI technologies (Figure 1), as well as barriers to the use of AI by organisations (Figure 2).

As Figure 1 shows, the AI market is growing based on AI-enabled services (82.7%). In turn, primary AI products as well as goods and services used in the development, production and operation of AI do not significantly impact market structure, accounting for 1% and 4.3% respectively.

Regarding barriers for companies using AI technologies, the most significant ones are: high costs (cited by 63.6% of respondents), a shortage of qualified personnel to develop, implement and support the operation of AI technologies (49.9%), and a lack of skills among organisation's employees to develop and use AI technologies (39.1%).

For companies that do not use AI technologies, the most significant barriers include high costs (57.2%), lack of skills among organisation's employees to develop and use AI (35.4%) and difficulty integrating AI into production and business processes (34.8%).

Financial services lead the way in AI adoption by industry, with 95% of organisations already using it, followed by higher education (72%) and information and communication technology (70%). Manufacturing is lagging behind, with only 16% having adopted AI.

Table
Assessing the impact of factors on the growth of the cybersecurity market
(% changes based on current weighted average estimates from the expert community)

Factor	Year				
	2024	2025	2026	2027	2028
Rising cyberattacks	3	3	3	3	3
Departure of foreign vendors	3	3	3.5	3.1	3
Sanctions and related restrictions	0	0	0	0	0
Responsibility of top officials of organisations for ensuring information security	3	4	4	4	4
Ban on foreign software in critical information infrastructure facilities	3	3	4	5	5
Financial support measures	3.7	3.6	3.8	3.7	4.1
Non-financial support measures	2.3	2.4	2.5	2.6	2.8
Tightening of information security requirements	3.4	3.2	3.5	3.6	3.7
Total market growth (year-on-year)	21.4	22.3	24.3	25	24.8

Source: Forecast for the development of the cybersecurity market in the Russian Federation for 2024-2028. https://www.csr.ru/upload/iblock/f14/bnl532lqmqd0u23s1ftuzw4n3ycm1to1.pdf.

According to data presented at the 2025 St. Petersburg International Economic Forum[1], среди 100 крупнейших российских компаний внедрили43% of the top 100 Russian companies have implemented AI in at least one business function, an increase of 23% compared to 2019. More than half of large companies (54%) are using generative AI.

At the same time, AI technologies provide certain competitive advantages for companies and industries, as well as the economy of the country as a whole. However, they also pose a number of threats that can be minimised through knowledge of these threats at the corporate, industrial, and national levels.

Let's look at the economic consequences and cybersecurity issues through the lens of cyberattacks, as a factor hindering the development and active implementation of AI technologies in various elements of the country's economic system.

In 2024, Russian businesses faced a sharp increase in cyber threats, many of which were created using artificial intelligence. Attackers actively used AI to develop sophisticated and effective attacks, using phishing campaigns, ransomware and deepfakes. This led to significant financial losses, destabilising corporate IT infrastructures and undermining the stability of corporate systems. Companies had to significantly increase their cybersecurity budgets and reduce user trust in digital services as a result.

Companies operating in the financial, telecommunications, and retail sectors remain particularly vulnerable to cyber threats due to the high level of digitalisation and vulnerability of their IT systems. Active integration of artificial intelligence into fraudulent schemes and automated attacks complicates the defense process significantly, necessitating the use of innovative information security methods. Measures are being discussed in response to these threats, including criminal liability for the use of AI in fraudulent schemes [Gashi et al., 2024].

The economic impact of the misuse of artificial intelligence technologies includes both direct losses from ransomware (which increased by 44% in 2024) and indirect losses due to data breaches, damage to companies' reputations, and system recovery costs. The introduction of AI into cyberattacks creates new types of threats - intelligent malware that adapts to defense systems, requiring continuous improvements in cybersecurity methods.

In this regard, as previously noted, an important component of ensuring economic security is the identification and prohibition of malicious AI containing various types of backdoors in the code and training for committing illegal actions when certain times or conditions occur.

Figure 3 shows the forecasted values of the national cybersecurity market from 2023 to 2028.

The data presented in Figure 3 suggests that the Russian cybersecurity market is expected to grow significantly by 188.3% in 2028 compared to 2023, according to forecasts from the Center for Strategic Research, which predicts annual growth of 22-28%. Therefore, it is of interest to study the results of a survey conducted among representatives of key market players in Russia, including vendors and distributors, to assess the impact of various factors on the growth of the cybersecurity market.

As can be seen from the data presented in Table, the importance of banning foreign software on critical information infrastructure facilities is increasing, followed by a decrease in the importance of financial support measures, tighter information security requirements, and an increase in the number of cyberattacks, according to experts.

3. External threats to economic security associated with AI

One of the key external threats to Russia in the AI sector is technological dependence on foreign suppliers of hardware and software.

Sanction restrictions significantly hinder access to advanced computing power, specialised processors, and software platforms necessary for training and operating neural networks. This hinders the development of domestic AI technologies, reduces the competitiveness of Russian companies in the global market, and increases the risk of technological backwardness [Tulunbasova, 2024]. Under sanctions pressure, Russia is forced to actively develop its own solutions and infrastructure. Creating a fully-fledged, closed AI ecosystem, however, requires time and significant investment. Technological dependence, at the same time, creates vulnerabilities that could be exploited by external actors to restrict access to critical resources and technologies.

External threats to economic security also include cyber espionage, economic espionage and AI-enabled data leaks.

Cyberespionage and economic espionage are interconnected and complementary threats that take on new dimensions and complexity through the use of AI. Attackers use automated AI tools to conduct reconnaissance attacks, significantly lowering the barrier to entry and increasing the speed and effectiveness of cyberespionage [Varavva, 2023].

According to Bi.Zone2, the share of intelligence attacks on Russian companies' web resources has increased by 220% in Russia in the second half of 2024

[1] https://forumspb.com/programme/business-programme/145548/.

[2] https://bi.zone/news/dolya-razvedyvatelnykh-atak-s-tselyu-poiska-uyazvimostey-saytov-vyrosla-na-220/.

compared to the first half. AI-enabled cyberattacks aim to obtain strategically valuable information, including trade secrets, technological innovations, and economic data. Attackers can use AI to quickly process large amounts of data and identify vulnerabilities in digital systems. They can also automate unauthorised access and data leaks.

The use of AI in economic espionage is becoming a key threat to national security. Foreign entities are gaining tools to quickly analyse the economic situation in Russia, identify vulnerabilities, and then use the resulting information to strengthen their own market positions. In this context, Russian companies and government organisations must strengthen data protection measures, implement advanced cybersecurity solutions, and refine strategies to counter new types of digital threats.

At the current stage of AI development and implementation, one of the main threats to information security is deepfakes - fake audio and video materials created using AI. Voices and appearances of famous people are imitated to spread false information, claims, and even ‘evidence’ of non-existent events.

There has been a significant increase in the use of deepfakes in information attacks. From 2023 to 2024, the number of such cases increased by 150%. This figure could triple by 2026. At the 2025 St Petersburg International Economic Forum, it was noted that deepfakes have the potential to manipulate public opinion and undermine trust in government institutions. They could also destabilise the political situation and create fertile ground for the spread of fake news, which could lead to mass protests and social conflicts. This could even lead to interference in the internal affairs of states.

To counter this threat, a comprehensive approach is needed. It includes the development and implementation of advanced methods for automatic detection and verification of digital content. Modern AI-powered algorithms can analyse video and audio recordings with up to 95% accuracy, identifying signs of forgery. However, technological measures alone are not enough. A strengthened legal framework for liability for creation and distribution of deepfakes, as well as international cooperation to share experiences and coordinate efforts, are also needed.

With AI technologies rapidly advancing and cyber threats growing, countering deepfakes has become a priority for ensuring information security and maintaining social stability in Russia and around the world.

4. Internal threats to economic security associated with AI

To ensure the country’s economic security, one of the main internal barriers to AI development in Russia is the acute shortage of qualified personnel in this field. This hinders large-scale implementation of technologies and creates dependence on foreign specialists.

By 2030, the shortage of qualified AI specialists in Russia could reach critical proportions. According to estimates from the Digital Economy non-profit, the demand for AI developers will exceed 70,000 people, while the annual university graduation rate is only around 4,500 specialists. In certain industries such as metallurgy and mechanical engineering, there is a shortage of personnel with AI skills reaching 55-65%. This is forcing industrial companies to compete with IT giants such as Sberbank and Yandex, which offer higher salaries, for talent [Akaev et al., 2024].

Due to a shortage of specialists, many IT initiatives at industrial enterprises remain at the pilot stage and are not systematically implemented, hindering digitalisation and optimisation of production processes. In 2023, due to personnel shortages, financial barriers and insufficient digital infrastructure, only 25% of manufacturing companies used AI technologies[3].

There is also a severe shortage of information security experts, which complicates the development and implementation of secure AI systems. Without reliable protection, AI technologies remain vulnerable, creating additional risks for businesses and governments.

The talent shortage is exacerbated by the emigration of IT specialists after 2022, while the influx of young talent is slow and fails to compensate for the loss. Furthermore, sanctions and Russia’s technological isolation limit access to advanced computing power and modern processors, further hindering AI development. This leads to the country’s technological backwardness and dependence on foreign technologies and specialists.

One of the national approaches to ensuring the availability of skilled labor is to increase the number of state-funded places at leading universities in the country, which have undergone a competitive selection process and received government support for implementing top-tier education programmes. Universities are required to admit a sufficiently large number of students each year, which will significantly increase the number of qualified graduates.

Close attention is also paid to the development of cyber schools offering free and accessible courses in programming, AI-powered technology development, and related fields. These initiatives aim to make training in modern technology more accessible to a wider audience. Partnerships with leading IT companies play a key role

[3] https://forumspb.com/programme/business-programme/145548/.

in creating relevant curricula, providing internships, and grant support, ensuring a high level of training and the competitiveness of graduates.

The shortage of personnel in the fields of AI and information security is a key factor slowing Russia's technological development and large-scale implementation of AI, and requires urgent and systematic measures from government and business.

The implementation of AI in the Russian economy is highly polarised. The uneven adoption of digital technologies and automation across various sectors of the Russian economy creates internal contradictions, reduces overall productivity and competitiveness. While IT, telecommunications and some energy sectors actively embrace digital solutions and implement AI, manufacturing, a key sector of the economy, significantly lags behind. As noted in [Matyushkina, Seregina, 2023], in 2022, the manufacturing industry recorded a low level of AI implementation (approximately 16%). This is explained by high costs, worn-out equipment, personnel shortages, and insufficient government funding for digitalisation. These factors have led to polarisation in efficiency and innovation development between different industries.

The backwardness of traditional sectors, which accounts for a significant share of GDP and employment, negatively impacts overall labour productivity and the economy's innovative potential. This limits Russia's ability to enter new markets and maintain international competitiveness. The technological gap leads to uneven development across regions and industries, which in turn exacerbates socioeconomic inequality. More digitally advanced companies and regions gain competitive advantages, while those lagging behind face the risk of stagnation and job losses [Ibragimov, Dushenin, 2021].

To improve competitiveness and ensure the sustainable development of the Russian economy, it is essential to close the gap in artificial intelligence (AI) adoption across industries. This can be accomplished through annual monitoring of digital maturity and digital literacy in industries, followed by the development and implementation of a series of government measures. The monitoring process will enable us to track trends in specific industries and, in certain cases, take targeted measures to address identified issues. Overall, enhancing competitiveness and ensuring the sustainable development of the national economy require comprehensive measures: modernisation of production, investment in digital infrastructure, training of qualified personnel, and stimulation of innovation in traditional sectors. Together, these measures will create a balanced and efficient economy capable of competing successfully in the global market.

A negative aspect that poses a significant threat to Russia's economic security is the concentration of resources in large corporations for the development of new technologies. As of 2024, there were approximately 540 companies working on AI in the country, with a significant number located in Moscow. This has led to regions that are not among the leaders suffering from a lack of investment, qualified specialists and necessary infrastructure. This hinders their digital transformation and economic growth.

Small and medium-sized enterprises (SMEs) face significant barriers to using advanced AI technologies. The high development and implementation costs of such solutions prevent them from automating processes, increasing productivity, and expanding their operations [Kondrashov et al., 2025]. This also exacerbates economic inequality and weakens the competitiveness and stability of the economy as a whole.

Of particular importance is the more equitable distribution of limited resources among regions and companies through the use of various support mechanisms, depending on the industry and the role of the company in the market. Large businesses undoubtedly provide significant revenue streams for budgets at various levels, but small and medium-sized businesses face oligopolisation and even monopolisation of certain markets. This leads to restrictions for them, as well as a deterioration in consumers' positions in the market, due to narrowing their choice of goods and services they can purchase.

Another challenge facing AI development in Russia in 2025 is the lack of a clear and comprehensive regulatory framework. This creates multiple risks and slows down digital transformation in key economic sectors.

A major challenge is the absence of a clear definition for artificial intelligence (AI) in Russian legislation at the federal level. Despite the fact that the concept of AI has been enshrined in the decree of the President of the Russian Federation and the national strategy for the development of AI until 2030, there is no legal definition for AI in the Civil Code of Russia, which creates uncertainty and hinders effective regulation.

Experts note that we talk a lot about AI, but there is no legislative regulation, confirming that the legal framework seriously lags behind technological developments in this area. This lack of clarity has led to confusion and uncertainty among stakeholders, including businesses, government agencies, and researchers [Kondrashov et al., 2025].

Currently, gaps in the regulation of personal data protection when using AI exacerbate privacy concerns. Existing personal data legislation does not take into account the specifics of processing by machine learning systems, creating legal uncertainty for companies implementing such solutions. Although work is currently underway to create a standard for personal data for AI systems, it must be acknowledged that this process is progressing rather slowly.

The lack of effective measures to prevent AI abuse is creating opportunities for cybercriminals. The increasing number of cyberattacks using AI, such as deepfakes and automated fraud, demands urgent legislative action. The Russian Ministry of Digital Development has proposed introducing criminal responsibility for AI-related crimes in 2025. However, experts warn of the risk of unfair prosecution due to a lack of clear criteria for determining malicious AI behaviour.

5. Measures to minimise threats

A priority area for ensuring Russia's economic security is the development of domestic AI solutions.

To stimulate innovation and the development of competitive technologies, the state supports the creation of research centers. Currently, 12 centers are operating, focusing on cutting-edge developments in the field of strong, ethical and industry-specific AI. This facilitates the formation of a sustainable ecosystem of domestic AI solutions, reducing dependence on foreign technologies and mitigating the risk of technological backwardness.

The use of domestic software is aimed not only at ensuring the stability of AI, but also at identifying and prohibiting malicious AI.

State grants and support programs for AI startups help small and medium-sized businesses to implement innovations, facilitating market diversification and the development of regional centers of excellence. The development of domestic AI platforms and solutions becomes a key tool for minimising internal threats and enhancing the country's economic security.

The next area of AI threat mitigation is personnel training. In Russia, personnel training is considered one of the key measures to minimise the risks associated with the development of IT and AI in the country. Thus, the Russian Ministry of Digital Development, Communications and Mass Media has initiated new training programmes (Top-IT and Top-AI), effective September 1st, 2025. These programs are aimed at training developers of IT solutions and specialists in AI.

Another important area of focus in terms of human resources is the return of relocated workers and the provision of comfortable working conditions for IT specialists working in Russia.

To successfully develop and implement modern technologies, it is essential to establish a government oversight system. This system should include regulations for the safe use of AI technologies, ethical standards, and certification procedures for Russian systems. By doing so, we can ensure the reliability and transparency of these technologies, as well as eliminate potential risks and increase trust among economic actors. At SPIEF 2025, a proposal was made to mandate the labeling of AI-generated content. This initiative aims to promote greater transparency and accountability in the digital space. By providing clear information about the origin of content, users can make informed decisions about whether to trust it.

A key component of state policy in this area is the federal project 'Artificial Intelligence', implemented as part of the national project 'Digital Economy'. As of 2024, 839 grants have been awarded for AI technology development under this project and 857 startups have received state support. This demonstrates widespread support for innovative initiatives. Between 2019 and 2023, 19.4 billion rubles have been allocated for the development of artificial intelligence. These funds have created conditions for industry growth and implementation of advanced solutions in various economic sectors [Kondrashov et al., 2025].

It is advisable to conduct annual monitoring of digital maturity and digital literacy in industries. This measure will allow for prompt response to challenges within a particular industry.

As noted previously, there are a number of gaps in the legal framework, further reinforcing the importance of improving the regulatory framework. This includes with regard to AI-enabled technological solutions used to commit illegal acts. Collectively, these gaps exacerbate existing threats to human life, the security of the state and infrastructure, as well as the functioning of various systems, territories and enterprises.

Various mechanisms must be applied to support small and medium-sized businesses in implementing and applying AI technologies in their operations. These mechanisms will vary depending on the industry of the company and its role in the market.

Together, these measures form the foundation for the safe, ethical, and responsible development of artificial intelligence in Russia, ensuring economic stability and sustainable digital growth.

We also emphasise international partnership in the field of AI as a means to ensure Russia's economic security. The free flow of information contributes to economic and social development, education, and democratic governance. Significant progress in information technology and telecommunications development and implementation has also created new opportunities for illegal activities, particularly criminal misuse of information technology [Larionova, 2024]. To mitigate the risks associated with AI development and use, it is essential to support international cooperation in security for new technologies. Despite the sanctions imposed on Russia in 2022, cooperation with friendly countries enables the exchange of advanced knowledge, successful approaches, and new technologies to protect countries.

For example, the Shanghai Cooperation Organisation (SCO) serves as an important platform for coordinating efforts in the field of information security. Its members have signed an agreement on cooperation in international information security, which entered into force in 2011. Russia, China, Kazakhstan, and Tajikistan have ratified this agreement, creating a legal basis for the prompt exchange of information on cyber threats. The SCO plans to sign a roadmap for developing cooperation with the CSTO and the CIS by the end of 2025, which will strengthen regional coordination in combating cybercrime.

In December 2024, Russian President Vladimir Putin announced the creation of the international AI Alliance Network to unite specialists from friendly countries. In January 2025, the president instructed the government to establish closer cooperation with China in the field of artificial intelligence. China is becoming a key partner for Russia in technology exchange, joint development of AI projects, and overcoming technological limitations.

Today, it is essential to align approaches towards ethical norms and standards in the field of AI technology. This will create a stable and secure environment for all economic actors and ensure the global application of these technologies. A global partnership in AI security will not only protect Russian digital systems, but also strengthen trust between states, essential for stable technological development and economic security.

Conclusion

An analysis of the state of artificial intelligence development and its impact on Russia's economic security reveals a complex and multifaceted picture of contemporary challenges and opportunities. The Russian AI market is demonstrating impressive growth dynamics. In 2024, growth was 22.8% compared to 2023, and by 2025 it is projected to reach 22.2%. Subsequent projected annual growth rates range from 22.1% to 27.9%. At the same time, the development of this industry is accompanied by serious internal and external threats to the country's economic security, requiring a comprehensive and systematic approach to mitigate them.

External threats related to technological dependence on foreign suppliers and sanctions pressure remain a key risk factor. Restricted access to advanced computing power and specialized equipment creates long-term obstacles to Russia's integration into global technological chains. Of particular concern are AI-enabled cyberattacks, which reached a record 1.8 billion cases in 2024, and deepfake fraud, which increased 2.3-fold compared to the previous year.

Internal threats are no less critical, and include an acute shortage of skilled labour. This could reach 2-3 million specialists in industry by 2030. The uneven adoption of AI across industries (only 16% of manufacturing companies used AI technologies in 2022, and 25% used them in 2023) creates imbalances in the economy. The concentration of resources in large companies, particularly in the Moscow region, where 68% of Russian AI companies are located, exacerbates regional disparities, and hinders the formation of a coherent innovation ecosystem.

To minimise the identified threats, Russia is implementing a range of measures, including the development of domestic solutions. A priority is training personnel through new 'Top-IT' and 'Top-AI' programs that will launch in 2026 to address the shortage of specialists. Regulations in this area include the development of a first bill on voice privacy and mandatory labeling of AI content to ensure the safe development of these technologies.

Thus, the proposed set of measures aims to address the 'shield' problem. In order to ensure sustainable economic growth for the Russian Federation during the era of digital transformation, it is necessary to wisely use the potential of artificial intelligence, while simultaneously minimising associated risks. Technological independence and economic security in the field of AI can only be achieved through comprehensive development of domestic research, training of qualified specialists, establishment of clear legal regulations and expansion of international cooperation. The ability of Russia to quickly and effectively respond to challenges associated with AI development will determine its competitiveness and long-term economic well-being.

References

Akaev A.A., Devezas T.K., Korablyov V.V., Sarygulov A.I. (2024). Critical technologies and prospects for Russia's development under economic and technological constraint. *Terra Economicus,* 22(2): 6-21. (In Russ.)

Balashov A.A. (2023). The development of artificial intelligence: Threats and opportunities for Russia's economic security. *International Scientific Research Journal,* 10(136). DOI: 10.23670/IRJ.2023.136.56. (In Russ.)

Balashov A.A. (2024). Conceptual foundations of the use of artificial intelligence to assess the level of economic security of the state. *Digital Modeling of the Economy,* 1: 74-79. (In Russ.)

Barakin B.S., Shailieva M.M. (2023). The role of artificial intelligence in strengthening economic security: From theory to practical application. *Human. Society. Inclusion,* 4(56): 64-71. (In Russ.)

Borovkov A.I., Rozhdestvensky O.I., Pavlova E.I. (2024). Analysis of the market for simulation process and data management systems (SPDM Systems) within the 'Technet' NTI Program. Expert-Analytical Report. St. Petersburg, St. Petersburg State Politechnical University. (In Russ.)

Varavva M.Y. (2023). The personnel gap: The scale and factors of the shortage of IT personnel in Russia. *Bulletin of the Plekhanov Russian University of Economics,* 4: 171-180. (In Russ.)

Danchenko A.S. (2024). Trends and prospects for the development of the digital economy in ensuring the economic security of the country. *Original Research,* 14(3): 247-252. (In Russ.)

Dyatlova A.F., Svirina M.V. (2024). Artificial intelligence technologies in the field of economic security. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* 2: 227-232. DOI: 10.24412/2073-0454-2024-2-227-232. (In Russ.)

Elin K.M., Usova N.V., Loginov M.P. (2024). Artificial intelligence technologies in the digital model of the national economy. *AlterEconomics,* 21(4): 723-747. DOI: 10.31063/AlterEconomics/2024.21-4.5. (In Russ.)

Ibragimov N.M., Dushenin A.I. (2021). Uneven development of the spatial economy of the Russian Federation and differentiation of growth factors. *The World of Economics and Management,* 21(2): 5-29. (In Russ.)

Artificial Intelligence in Russia: Development and Application (2025). Moscow, National Research University Higher School of Economics. (In Russ.)

Kondrashov P.E., Petrunin Yu.Y., Popova S.S. (2025). Regulation of the development and application of artificial intelligence: Problems and directions of development. *Bulletin of the Moscow University. Series: Management (State and Society)*, 1: 3-19. (In Russ.)

Larionova M.V. (2024). Problems of regulation of digital platforms: Difficulties and opportunities for international cooperation. *Bulletin of International Organizations: Education, Science, New Economy,* 19(2): 4. (In Russ.)

Mamontova S.V. (2022). Economic and information security in the digital economy. *Region: Systems, Economics, Management,* 4(59): 145-153. DOI: 10.22394/1997-4469-2022-59-4-145-153. (In Russ.)

Mankovsky E.R. (2023). Prospects for the impact of artificial intelligence on the economic security of the state. *Fundamental and Applied Research of the Cooperative Sector of the Economy,* 3: 140-146. DOI: 10.37984/2076-9288-2023-3-140-146. (In Russ.)

Matyushkina I.A., Seregina M.Yu. (2023). Digital transformation of manufacturing enterprises. *Economics. Sociology. Law,* 2(30): 19-25. DOI: 10.22281/2542-1697-2023-02-02-19-25. (In Russ.)

Obukhova A.S., Piyaltsev A.I. (2021). Digital shadow economy: A threat to economic security. *Proceedings of the Southwestern State University. Series: Economics. Sociology. Management,* 11(1): 82-89. (In Russ.)

Romanova I.N. (2021). Introduction of artificial intelligence technologies: Analysis of probable risks and possible threats. *Materials of the Ivanov Readings,* 4(35): 15-18.

Smorodina E.P., Sidnev M.D., Reushenko A.A., Smorodin M.A. (2024). The role and development of artificial intelligence in ensuring Russia's economic security. *Digital and Endustry Economics,* 3(35): 121-128.

Tulunbasova N.A. (2024). The impact of economic espionage on the Internet on the economic security and development of national economies (The experience of the USA and China). *Economic Bulletin of ICS RAS,* 5(1): 3-11. DOI: 10.25728/econbull.2024.1.1-tulunbasova.

Gashi S., Imaralieva T., Abdykadyrov S. (2024). Research on the impact of artificial intelligence on financial security in the context of modern technological challenges. *Interdisciplinary Journal of Applied Science,* 8(13).

About the authors

Mikhail P. Loginov

Doctor of economic sciences, associate professor, professor, Department of Finance, Money Circulation and Credit, Ural State University of Economics (Yekaterinburg, Russia); Department of Management, School of Management and Interdisciplinary Studies, Institute of Economics and Management, Ural Federal University (Yekaterinburg, Russia); professor, Department of Economic Theory, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia). SPIN: 8796-0033; ORCID: 0000-0003-0831-3004; Scopus ID: 57204101945; Researcher ID: V-2947-2017.
Research interests: digitalisation, financial markets, project management.
port-all@mail.ru

Natalia V. Usova

Doctor of economic sciences, associate professor, professor, Department of Economic Theory, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia); professor, Department of Marketing and International Management Ural State University of Economics (Yekaterinburg, Russia); associate professor, Department of Marketing, School of Economics and Management, Institute of Economics and Management, Ural Federal University (Yekaterinburg, Russia). SPIN: 7098-2046; ORCID: 0000-0002-7575-6078; Scopus ID: 57219834561.
Research interests: services, digitalisation, marketing.
nata-ekb-777@yandex.ru

Polina A. Kukanova

Student, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia).
Research interests: digitalisation, economic security.
Kukanovapolina@mail.ru

Svetlana A. Alekseeva

Student, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia).
Research interests: digitalisation, economic security.
svetlana_alex177@icloud.com

作者信息

Mikhail P. Loginov
经济学博士，副教授，乌拉尔国立经济大学货币流通与信贷教研室教授（俄罗斯，叶卡捷琳堡）；俄罗斯联邦第一任总统鲍里斯·叶利钦乌拉尔联邦大学经济与管理学院管理与跨学科研究系教授（俄罗斯，叶卡捷琳堡）；俄罗斯联邦总统国民经济和行政学院乌拉尔分院经济理论教研室教授（俄罗斯，叶卡捷琳堡）. SPIN: 8796-0033; ORCID: 0000-0003-0831-3004; Scopus ID: 57204101945; Researcher ID: V-2947-2017.
研究领域： 数字化、金融市场、项目管理。
port-all@mail.ru

Natalia V. Usova
经济学博士，副教授，罗斯联邦总统国民经济和行政学院乌拉尔分院经济理论教研室教授（俄罗斯，叶卡捷琳堡）; 市场营销与国际管理教研室教授，乌拉尔国立经济大学（俄罗斯，叶卡捷琳堡）; 俄罗斯联邦第一任总统鲍里斯·叶利钦乌拉尔联邦大学经济与管理学院市场营销教研室副教授. SPIN: 7098-2046; ORCID: 0000-0002-7575-6078; Scopus ID: 57219834561.
研究领域： 服务领域、数字化、市场营销。
nata-ekb-777@yandex.ru

Polina A. Kukanova
罗斯联邦总统国民经济和行政学院乌拉尔分院的学生（俄罗斯，叶卡捷琳堡）。
研究领域： 数字化、经济安全。
Kukanovapolina@mail.ru

Svetlana A. Alekseeva
罗斯联邦总统国民经济和行政学院乌拉尔分院的学生（俄罗斯，叶卡捷琳堡）。
研究领域： 数字化、经济安全。
svetlana_alex177@icloud.com

The article was submitted on 17.07.2025; revised on 13.08.2025 and accepted for publication on 21.08.2025. The authors read and approved the final version of the manuscript.
文章于 17.07.2025 提交给编辑。文章于 13.08.2025 已审稿。之后于 21.08.2025 接受发表。作者已经阅读并批准了手稿的最终版本。