GAIDAR INSTITUTE FOR ECONOMIC POLICY

Monitoring international legal regulation trends for developing legislation in the digital economy in Russia

- Cybersecurity has become a barrier to trade
- How AI transforms labor market
- Recommendations for managing risks of agent AI
- Is it possible to recover abandoned bitcoins through courts?

Monitoring No.5 (29) (May 2026)

Monitoring has been prepared by a team of employees of the International Best Practices Analysis Department at the Gaidar Institute.
Associated authors: Maria Girich, Researcher, Ivan Ermokhin, Researcher, Antonina Levashenko, Senior Researcher, Olga Soldatkina, Researcher, Kirill Chernovol, Researcher, Diana Golovanova, Researcher

Cyberbarriers in trade

In May, 2026, the OECD issued a report considering how standards of cybersecurity become barriers for international trade.

Cybersecurity is a set of technologies and measures that prevent unauthorized access to networks, devices, and other digital infrastructure.

The OECD observes that fragmentation of cybersecurity regulation across countries leads to increased compliance costs for companies and reduces level of infrastructure security.

Thus, costs of the European companies for cybersecurity are estimated at **EUR 31.2 bn** annually. For example, the EU's Network and Information Security Directive (NIS2) has been in effect since 2023, requiring companies in critically important sectors to systematically manage cyber risks, prevent incidents, and promptly report incidents to the regulator. Growth of costs for companies who have already introduced cybersecurity measures is expected by **12%**, and by **22%** for those who have just come under the new regulation.

It is hard to disagree with the report's key findings. The digitalization of industries has hidden risks: now, a single cyberattack is enough to leave an entire city without power, as happened in Iran.

However, lack of common positions at the international arena can turn cybersecurity requirements into what the OECD calls “paperwork”: businesses are no longer so much concerned with ensuring security, as they are trying to comply with all the requirements. The cost of such compliance is also substantial: the OECD estimates these costs at **EUR 200–500.000** per company in the EU. In Russia such costs are estimated at **Rb 800.000** annually.

34%

Author: Ivan Ermokhin

SMEs in the EU lack means to comply with cybersecurity standards

The requirements as such become an instrument of trade protectionism. Thus, the WTO observe that **over 1/3** of all new trade disputes currently tackle cybersecurity issues. Therefore, imposition of high cybersecurity standards, including through requirements for equipment and software certification, localization of data storage, etc., may create more significant barriers to entry for foreign companies than direct restrictions on foreign investment. The cost of compliance for a foreign company may exceed the potential benefits of entering the formally open market for foreigners.

For instance, a series of bans imposed on Huawei in the American and European markets is a remarkable case. Restrictions affected government agencies' ability to purchase the Chinese company's equipment, as well as to use Huawei equipment for the development of 5G networks. The basis for restricting access was precisely the cybersecurity requirements that the company did not meet.

China is also not lagging behind in implementing cybersecurity standards, i.e., only in 2018, Technical Committee TC260 issued nearly **300** national cybersecurity standards, including requirements for software, routers, switches, and firewalls. In 2023, standards have been detailed with introduction of additional package of requirements TC260.

In Russia, the issue of international cooperation on cybersecurity is also raised at the EAEU, however, primarily in the context of information exchange within the Union (Article 23 of the EAEU Treaty), i.e., building a state IT infrastructure for interaction, rather than harmonizing requirements for business.

The OECD proposes reducing costs for companies' information security by developing common approaches to regulating the industry.

What is next?

Number of cybersecurity standards and their specification will grow along with increasing digitalization. Countries can use information security as a tool of trade protectionism. However, countries, where level of digitalization development, in particular, level of AI introduction, is high, may be interested in harmonization of cybersecurity standards. This will contribute to further expansion of companies in the international markets.

YESTERDAY

2010-s

Adoption of the first comprehensive cybersecurity laws

TODAY

2026

Growing cybersecurity requirements for a wider range of individuals, more detailed and more stringent

Over **110** countries adopted cybersecurity standards: **78%** countries adopted personal data security, and **63%** adopted incident notification rules

TOMORROW

Cybersecurity requirements will continue growing, but major economies will perceive information security requirements as a tool not only for protecting infrastructure, but also for trade policy

To replace natural intelligence

How AI transforms labor market: lawyers won't be left without work

Authors: Olga Soldatkina, Kirill Chernovol

In May 2026, a Court in China adjudged **RMB 260.000** ($ 38 400) as a compensation for an employee dismissed due to AI replacing his job functions. A technology company in Hangzhou attempted to replace a quality assurance specialist for large language models with an AI system, offering him a position with a **40%** lower salary. A court ruled the dismissal unlawful.

This case clearly demonstrates the conflict between two points of view on the role of AI in working process: AI enthusiasts, motivated by the need to optimize labor costs using AI, and AI skeptics supporting workers in the skills race with AI. However, according to the OECD, exposure to AI in manufacturing processes varies significantly across sectors and occupations.

65% *professions in the labor market are exposed to AI*

To measure the exposure to AI in the next 5-10 years, the OECD conducted a comparative analysis of the competencies of various professions with AI capabilities[1]: the greater the gap between AI capabilities and professional skills, the less susceptible the profession is to AI replacement. Conversely, if the gap is minimal, then human replacement is easy.

However, not everything is so clear-cut, as the profession involves solving a variety of multifaceted problems: some tasks, such as data processing, can be optimized using AI, while others, such as communications and people organization, cannot be solved without human intervention.

For this reason, lawyers and judges unexpectedly ended up in a group of professions least susceptible to AI replacement. Although this work is predominantly analytical, i.e., what AI does best. However, the need to make legally significant decisions makes lawyers indispensable.

Consequently, taking into account professional characteristics, according to some estimates, AI can fully replace only up to **15%** of existing professions, primarily in the fields of administration and document management.

However, working conditions will change for **50-65%** professions, especially in the field of education, healthcare, science, art, mass media, repair and technical support services.

This means that professions involving working in a standardized environment are most susceptible to replacement, but if creativity or social responsibility appear in a profession, then this already makes a human irreplaceable. However, contrary to the idea that physical labor is indispensable, the robotization of production should be taken into account: product packers, warehouse pickers, and parts assemblers are already at risk.

A complete list of professions that are most and least protected from competition with AI is presented in a special OECD platform.

The introduction of AI could have a positive impact on the Russian labor market. Sber estimates that robotics and generative AI could boost labor productivity **from 21% to 32%** by 2032.

[1] The comparison is made across nine areas of human activity: 1) communication; 2) social interaction; 3) problem solving; 4) creativity; 5) metacognition (understanding mental action); 6) knowledge, learning, and memory; 7) vision; 8) handling physical objects; 9) technical intelligence.

What is next?

If the OECD estimates are applied to Russia based on Rosstat's labor force survey data, approximately **2,1** mn people[1] will be in the "risk zone" by 2025, where AI or robots can confidently perform human-like tasks. These include employees in the information processing, accounting, and other office workers.[2]

The situation is somewhat better, but still critical (by now, AI has mastered only 1-2 skills required for the profession) for another **9.3 mn people**: these are salespeople, plant operators, textile workers, seamstresses, food industry workers, etc.[3] Cleaners, domestic helpers, and "business specialists" are still safe, while top managers and education workers are doing best.

YESTERDAY

Until 2026
The number of professions exposed to AI has grown as AI technologies have developed

Professions associated with routine work in a standardized environment (such as accounting) were susceptible to the influence of AI

TODAY

2026
In China, a court rules in favor of a worker replaced by AI; the OECD measures the exposure of professions to AI influence

AI is creating new professions related to servicing AI systems and increasing value of irreplaceable specialists, lawyers and medical officers

TOMORROW

AI is changing working conditions of most professions, but labor laws limit complete replacement of workers by AI

---

[1] The OECD considers office and manufacturing occupations, food preparation workers, textile workers, forestry workers, and sales workers to be the closest to what AI can already do.
According to Rosstat's 2025 labor force survey, approximately 11.36 mn people in Russia are employed in such occupations. This figure represents the number of workers in occupations whose tasks, according to the OECD, can already be performed by AI.

2 Number of employees involved in numerical data processing and inventory control: 1.081,451.
General clerical and office equipment maintenance workers: 529.960.
Other office workers: 487.502.
Total of all listed above workers: 1 081 451 + 529 960 + 487 502 = 2 098 913 people.

3 Operators of industrial plants and stationary equipment – 1 883 204 people.
Food, wood, textile, clothing and related industry workers – 1 641 286 people.
Assembly workers – 427 488 people.
Cooking assistants – 153 243 people.
Salespeople – 5 158 606 people
Total of all listed above workers:
1 883 204 + 1 641 286 + 427 488 + 153 243 + 5 158 606 = 9 263 827 people.

AI under cover

Initial recommendations for managing the risks of agent AI

Author:
Kirill Chernovol

This year marks 70 years since the term "artificial intelligence" was adopted by the scientific community. Interestingly, the author of the term, John McCarthy, died in the same year, 2011, when Apple launched its Siri voice assistant.

In May 2026, countries published the first regulatory measures for agent AI systems. Why and what is it?

Assume that we ask an AI to perform a market analysis. Generative AI without any additional tools will take information from the data it was trained on, compose a text similar to "market analysis," release it, and then "forget" both the task and its answer. Agent AI is a subset of generative AI that can "break down" a request into subtasks, plan what data to take and where to get it from, self-check, and produce a more "meaningful" result. Such AI independently decides which steps to perform within a task, and which data and applications to use.

A question arises: who is responsible for the damage caused by agent AI?

For example, a company's AI agent erroneously orders a shipment of goods. Can the company refuse the order because it was placed without human intervention? Should human approval of orders be mandatory? This is how agent AI differs from traditional AI systems: a human may lose control over the actions and decisions of an agent AI due to its high degree of autonomy, while the agent AI may go beyond its instructions and thereby cause harm.

Thus, in China, the PRC Position of the Cyberspace Administration notes that it is necessary to legally delineate which decisions agent AI can make only with human participation, which ones without it, and which ones cannot be transferred to AI at all.

Similarly, in Singapore, Model Guidelines for Governance of Agent AI recommend that before launching an agent AI, companies should determine what data it has access to, whether it can only read or also modify data, what it can do only with human approval, i.e. provide the minimum necessary access. For example, every time AI is going to use sensitive data, send messages, make payments, etc. It is also recommended to allow it to use only certain APIs[5], grant access to programs or data only temporarily, and forbid it to transfer its access rights to other AI systems.

56%

developers using AI agents in 2025, pointed to security risks and data leaks when using them

Another problem with agent AI is how to monitor their progress if they consist of several AI systems (a feature of AI agents is that one AI can delegate tasks to others), use different tools (e.g., email clients, instant messengers), delegate tasks to AI, etc. The chains of their actions are not always visible to the user: an agent AI can display a chain of its own actions, but what other agents or applications in the chain did is not visible. China proposes to develop the work of AI agents using blockchain to ensure that the actions of each agent are as transparent as possible.

Cyber security authorities in Australia, the US, Canada, New Zealand and Great Britain recommend in their Guidelines on agent AI introduction to developers of agent AI to Integrate special logs of interactions between agents into systems: if one agent delegates a task to another, the log should reflect who is the recipient, what actions were performed, what tools were used, etc.

Regulators in the respective countries also point to digital security risks, such as AI deleting data from other apps or overloading them with requests, etc. Thus, for instance: the incident concerning the Replit AI agent, which, during its operation, completely deleted the database of the developer who created the application using this agent. There are recommendations to test how agent AI behaves regarding the access to various external programs, creating AI agents that monitor the main AI to ensure it does no harm, and ensuring that the AI "keeps in mind" the goal, why it is doing this at every step of its work, etc.

In Russia, there are no initiatives yet to develop regulation of agent AI. However, for instance, the draft law on AI submitted by the Ministry of Digital Technology, Communication and Mass Media, could include provisions specifically addressing the risks of agent AI, establishing rules for developers to implement measures to monitor actions of agent AI, etc.

[5] a software interface that allows different applications to communicate and exchange data with each other

What is next?

Why is agent AI more dangerous than a simple chatbot? It can use programs you don't control. If it gets an access, the agent AI could accidentally delete your email, leak payment information, and even run the risk of common AI "hallucinations", distortion, and other risks.

In 2025, companies used about **28.6 mn** of AI agents; it is forecasted that by 2030 there will be more than **2.2 bn.**

YESTERDAY

February 2026
OECD report on AI agents

TODAY

May 2026
Recommendations of the PRC, Singapore, Australia, Great Britain, etc. on agent AI

TOMORROW

The OECD identifies factors that increase the risks of agent AI: delegation of tasks, reduction of human oversight and transparency, etc.:

Determination of agent AI risks: deleting, changing or transmitting data without permission, delegation of powers to other programs, going beyond the scope of assigned tasks and permitted actions

Introduction of agent AI security measures: maintain logs of actions of programs assigned to perform tasks; restrict the transfer of access rights to third parties or other programs, etc.

Abandoned bitcoins

Is it possible to recover abandoned bitcoins through the courts?

Authors: Ivan Ermokhin,
Diana Golovanova

In May 2026, an anonym using the pseudonym Noah Doe and two Wyoming companies (ABC Company and XYZ Company) filed a lawsuit in New York State Supreme Court seeking ownership of **39.069** inactive Bitcoin addresses. Plaintiffs claimed that, using the algorithm they developed, they identified addresses that had not been used for more than 5 years and therefore, in their opinion, could be considered abandoned. They therefore asked the court to recognize their ownership of these addresses and the bitcoins that are located there.
Under New York's Personal Property Law, title to lost property[1] valued at less than **$10** may be transferred to the finder if the finder has made a one-year effort to locate the owner.

As evidence, the plaintiff indicated that he handed over flash drives containing lists of found addresses to the police and notified the owners via blockchain messages. However, an independent expert hired by the plaintiff estimated the value of each address at less than $10, explaining that the plaintiff does not have access to the assets, that restoring the value is associated with high challenges, and that obtaining the value through such restoration is not guaranteed, although in fact, the addresses may contain bitcoins worth a larger amount.

$ 285 bn

may cost bitcoins at abandoned addresses

Thus, the plaintiff plans to acquire ownership only of the public addresses that are visible on the blockchain rather than of the bitcoins as such, and allow, for example, receiving transfers to such an address, but do not allow withdrawing cryptocurrency from such an address (since this requires a private key). Therefore, it is debatable whether a public address can be considered as found property if access to and disposal of bitcoins depends on availability of a public address as well as a private key.

New York has another law, the Unclaimed Property Act, which already includes provisions for unclaimed virtual currency: cryptocurrency may become state property if such cryptocurrency is held by an organization that operates in virtual currency (such as an exchange) and remains unclaimed for 5 years. However, this law is not entirely appropriate for the situation under consideration, since it regulates virtual currency held by an intermediary (for example, an exchange), while the lawsuit concern addresses without any intermediary at all.

Another legal question concerns whether it is possible to have separate ownership rights to a public address and a private key. And does ownership of a public address automatically mean ownership of a cryptocurrency that can only be used with the private key? Today, the legislation of countries does not directly answer this question.
In Russian law, digital currency is recognized as a set of electronic data (digital code or designation) that are contained in an information system and can be accepted as a means of payment or investment.[2]

Therefore, a public address or a private key can hardly be considered property on their own.

[1] Abandoned or lost property is the one that has been left by its owner and is then found by another person.

[2] Federal Law of 31.07.2020 No. 259-FZ.

What is next?

If the court upholds the claim, long absence of transactions with the crypto asset can be used as an argument in favor of its abandonment, although in practice the owner can simply hold the cryptocurrency and wait for its value to rise.
However, without a private key, the plaintiff will still not be able to transfer the bitcoins, but can rely on the court's decision if the assets start moving or enter the exchange.

Fun fact

In 2013, a Briton accidentally discarded a hard drive containing his private bitcoin key and then spent years trying to gain access through courts to the landfill where he claimed the drive was located. In January 2025, the court dismissed his claim, declaring that the claim had no real prospects, and that the hard drive, after being dumped in the landfill, became the property of the city council.
The **8 000 bitcoins** lost by Briton account for approximately **£ 600 mn**

YESTERDAY

Until 2026
Inactive bitcoin addresses have appeared and cannot be used without a private key

Part of bitcoins were actually lost: owners lost their private keys, stopped using the addresses, or cannot access them

TODAY

2026
The court is trying to recognize the ownership of inactive bitcoin addresses as abandoned property

A question remains as to what exactly can be considered property: a public address, a private key, or just cryptocurrency as a whole (all together)

TOMORROW

Special rules for lost cryptocurrency: when it can be considered lost, who can claim it, and how to distinguish loss of access from long-term storage

News in **May 2026,** that we found interesting.[1]

- A bill on robotics and autonomous unmanned systems has been submitted to the Russian State Duma. Robots and drones on the government's list will need to be registered, issued a "digital passport," transmit real-time location and parameters data to a unified state system, and, when interacting with humans, be warned that they are communicating with a robot.

- Ministry of Finance suggested to empower SMEs in Vietnam to use digital assets as collateral for bank loans instead of traditional collateral (such as real estate). However, SMEs account for more than **98%** of enterprises in Vietnam, but receive only about **19–20%** of the total volume of banking loans.

- In Russia, intermediary platforms should provide benefits to platform employees who have voluntary social or health insurance. The minimum benefit is set at 2.9% of the employee's income. This benefit may include, for example, additional payments, discounts on platform fees, and other benefits.

- Investigation has been started against Meta in Texas for a possible privacy violation. The company is developing a facial recognition feature called "Name Tag" for its AI glasses, which could automatically process human biometric data the user is looking at, including passersby. However, these individuals have not provided their agreement to the processing of their data.

[1] [1] Since 2025, the Gaidar Institute has been developing a digital platform for analyzing news in Russia and globally on the topic of digital economy regulation – DIgiReg. The news presented has been selected by experts, in part based on an analysis of the platform's data.

DIGEST