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

- Data in international trade
- Online anticompetitive practices
- Protection of personal data on the blockchain
- Preparing the workforce for the challenges of AI
- Rising cyber risks for SMEs

Monitoring No. 4 (16) (April 2025)

Monitoring **was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute)**:
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Ivan Ermokhin, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Olga Magomedova, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Kirill Chernovol, Researcher, International Best Practices Analysis Department, Gaidar Institute
Diana Golovanova, legal counsel, Economic Policy Foundation

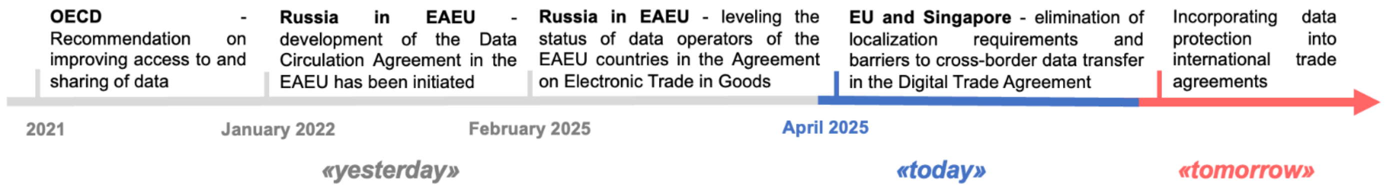
"April rain came for the first time,
But the wind carried the clouds away,
Leaving drops of fire
On the bare branches of the birch trees."
Samuil Marshak

In April 2025, there were 5 events that define the trends in the development of digital regulation in the world.

Trend № 1. Data in international trade

In April 2025, the EU and Singapore signed Digital Trade Agreement to remove measures that restrict cross-border data flows (such as requiring companies to store data on local servers or prohibiting the transfer of data abroad) and exchange customs information to facilitate digital trade.

Trend
Data in international trade



OECD - Recommendation on improving access to and sharing of data

Russia in EAEU - development of the Data Circulation Agreement in the EAEU has been initiated

Russia in EAEU - leveling the status of data operators of the EAEU countries in the Agreement on Electronic Trade in Goods

EU and Singapore - elimination of localization requirements and barriers to cross-border data transfer in the Digital Trade Agreement

Incorporating data protection into international trade agreements

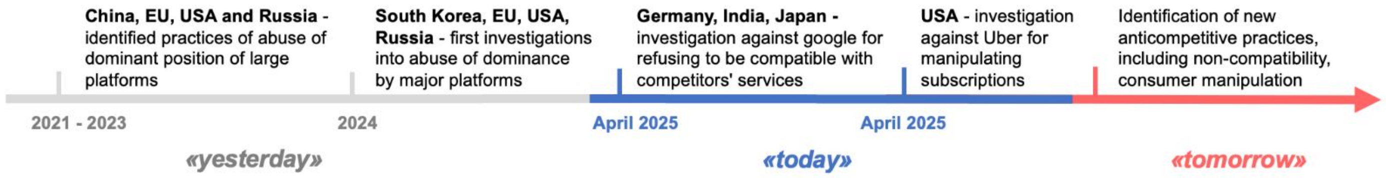
2021 January 2022 February 2025 April 2025

«yesterday» «today» «tomorrow»

Trend No. 2. Online anticompetitive practices

In April 2025, Germany completed investigations against Google for abuses in the market of mapping services, Japan and India recognized the refusal of compatibility with competitors' services as an anti-competitive practice due to the requirement to pre-install Google services on smartphones and smart TVs. In the US, an investigation against Uber for manipulating online subscriptions is completed.

Trend
Online anticompetitive practices



China, EU, USA and Russia - identified practices of abuse of dominant position of large platforms

South Korea, EU, USA, Russia - first investigations into abuse of dominance by major platforms

Germany, India, Japan - investigation against google for refusing to be compatible with competitors' services

USA - investigation against Uber for manipulating subscriptions

Identification of new anticompetitive practices, including non-compatibility, consumer manipulation

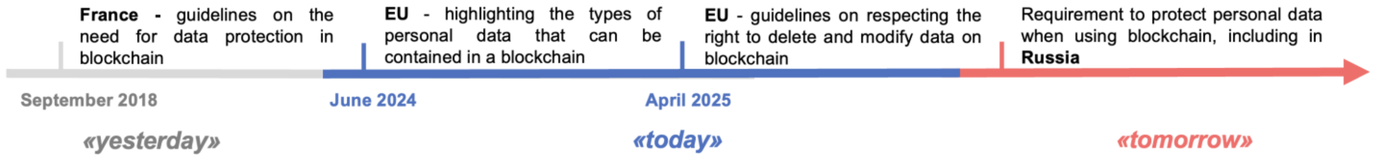
2021 - 2023 2024 April 2025 April 2025

«yesterday» «today» «tomorrow»

Trend No.3. Protection of personal data on the blockchain

In April 2025, the EU adopted guidelines on the use of blockchain technology for data protection, highlighting the risk that processing and storing data on blockchain limits the exercise of the data subject`s right to have their data erased and amended.

Trend
Protection of personal data on the blockchain



France - guidelines on the need for data protection in blockchain

EU - highlighting the types of personal data that can be contained in a blockchain

EU - guidelines on respecting the right to delete and modify data on blockchain

Requirement to protect personal data when using blockchain, including in **Russia**

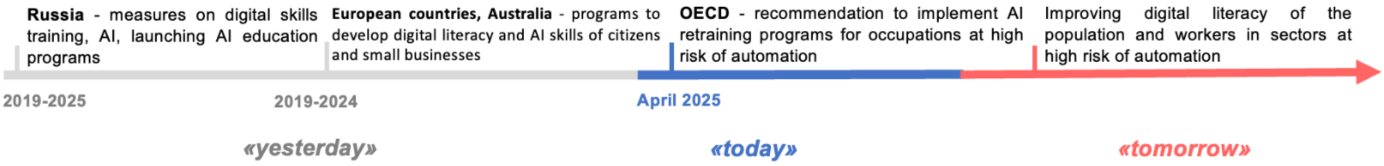
September 2018 June 2024 April 2025

«yesterday» «today» «tomorrow»

Trend No. 4. Preparing the workforce for the challenges of AI

In April 2025, the OECD published a report on the need to develop AI literacy, retraining workers for the rise of automation. Almost a third of all jobs in OECD countries already involve AI-enabled tasks, but only 1% of jobs require highly specialized AI skills.

Trend
Preparing the workforce for the challenges of AI



Russia - measures on digital skills training, AI, launching AI education programs

European countries, Australia - programs to develop digital literacy and AI skills of citizens and small businesses

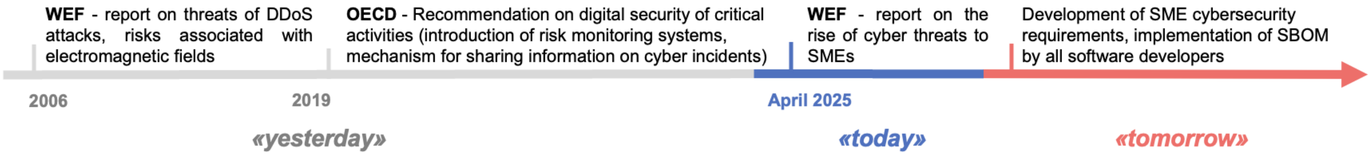
OECD - recommendation to implement AI retraining programs for occupations at high risk of automation

Improving digital literacy of the population and workers in sectors at high risk of automation

Trend No. 5. Rising cyber risks for SMEs

The WEF presented the Global Cybersecurity Outlook 2025 report, pointing out the growth of cyber risks to SMEs, the decreasing cost of cyber attacks due to AI, and the challenge of developing different country approaches to cybersecurity regulation.

Trend
Rising cyber risks for SMEs



WEF - report on threats of DDoS attacks, risks associated with electromagnetic fields

OECD - Recommendation on digital security of critical activities (introduction of risk monitoring systems, mechanism for sharing information on cyber incidents)

WEF - report on the rise of cyber threats to SMEs

Development of SME cybersecurity requirements, implementation of SBOM by all software developers

In April 2025, a number of innovations were introduced in Russia

1. Proposal to Introduce Profit Tax on Russian Multinational Companies

In April 2025, the media, citing the press service of the Russian Ministry of Finance, reported that the Ministry of Finance was discussing the introduction of the Qualified Domestic Minimum Top-Up Tax (QDMTT) rule into tax legislation. The rule is part of the OECD's Pillar 2[1] mechanism as part of the fight against the dilution of taxable bases and the diversion of profits from taxation. We have previously described the OECD Pillar 2 mechanism in Monitoring No. 1 (13) (January 2025).

The Ministry of Finance proposes that large multinational companies operating in Russia (having a subsidiary or parent company abroad) with annual revenues of at least €750 mn a year should pay profits tax in Russia at a rate of at least 15%, even if they have exemptions. The default rate in Russia is 25%. However, for example, accredited IT companies pay only 5% - so companies will have to pay an additional 10% on profits in Russia to reach the 15% level.

About 50 jurisdictions around the world have already established a rule: if a company pays too little tax in one country, the other country can collect the missing money itself (the so-called Undertaxed Profits Rule, UTPR). In order to prevent other countries from taking taxes from Russian companies, Russia wants to collect up to 15% tax itself. For example, a Russian IT-company is a member of an international group with a subsidiary in Germany, and it pays only 5% tax in Russia (it has a privilege), while the subsidiary company in Germany pays 15% tax. Under the new rule, the parent company in Russia will be obliged to pay an additional 10% (to make the total 15%), and if this rule does not exist, then in Germany (according to the “under-taxed profit rule”) the tax authorities will have the right to charge the company an additional profit tax equal to the 10% that the company did not pay in Russia.

To eliminate the risk of double taxation, the OECD has developed a special international report on GLoBE rules[2] (GLoBE Information Return, or GIR). A company completes the report once a year and submits it to the national tax authority, and then countries exchange these reports within the framework of bilateral agreements. So, if a Russian company files a GIR report, Germany will see that Russia has

[1] https://www.oecd.org/en/topics/sub-issues/global-minimum-tax/global-anti-base-erosion-model-rules-pillar-two.html

[2] GLoBE (Global Anti-Base Erosion) - international tax rules that require large TNCs to pay at least 15% income tax in each country where they operate.

already taken 15% tax from the parent company. The international information exchange system helps to check whether the tax has been calculated correctly.

Globally, Russia is following in the footsteps of the EU, the UK, Australia, and Canada, where similar "top-up taxes" have already been adopted or are nearing final approval. In these countries, tax benefits are gradually being transformed from rate reductions into subsidies or grants, which are not considered when calculating the effective GloBE rate. The Russian Ministry of Finance has not yet proposed similar compensatory measures.

2. Measures to counteract telephone fraud have been introduced

A new law on combating fraud by means of communication is adopted:[3]

- It is envisaged to create a state information system containing information on fraudsters and data on cellular numbers used for fraud. The system will be available only to law enforcement agencies, banks and telecommunications operators.
- New obligations are introduced for credit institutions with regard to restrictions on cash withdrawals in the event of fraud. Banks will have to verify customer requests for cash withdrawals according to criteria established by the Bank of Russia (not yet developed).
- A ban is introduced on the use of foreign messengers in the bank's interaction with clients.
- Bank customers are given the opportunity to appoint authorized persons (e.g., a relative) at their bank to confirm monetary transactions with their accounts.
- To protect customers, the law gives credit institutions and owners of aggregators (marketplaces) the right to use the Unified Biometric System to authenticate their clients or users[4] and obliges microfinance organizations to use biometrics when issuing loans in a remote format.

The law will take effect on June 1, 2025.

3. Approved rules for Roskomnadzor to recognize a website as a copy of a blocked website

The rules[5] were adopted to implement the procedure for restricting access to copies of websites that repeatedly host information prohibited in Russia (Article 15.6-1 of the Federal Law “On Information”). Signs of similarity between a copy of a website and the directly blocked website are highlighted:

- External similarities (what the interface looks like).
- Similarity of domain names, copy names, posted information.
- User account matching.
- Evidence of technical interaction between the copied site and the blocked site.
- Similar contact information for site administrators.

The list is not exhaustive, Roskomnadzor has the right to block a copy of a website on the basis of other similarities.

[3] Federal Law No. 41-FZ of 01.04.2025 “On the Creation of a State Information System to Counteract Offenses Committed with the Use of Information and Communication Technologies and on Amendments to Certain Legislative Acts of the Russian Federation”.

[4] P. 18 of Article 30 of the Federal Law “On Banks”, p. 1.4 of Article 9 of the Law “On Protection of Consumer Rights”.

[5] Decree of the Government of the Russian Federation No. 493 of 16.04.2025 “On Approval of the Rules for Adoption of a Motivated Decision on Recognition of a Site in the Information and Telecommunication Network ‘Internet’ as a Copy of a Blocked Site”.

.

Key aspects

1. Data in international trade

The EU and Singapore experience

In April 2025, the EU-Singapore Digital Trade Agreement was signed.[6] The parties agreed to:

1) Prohibit measures that restrict cross-border data transfers. For example, requiring the use of equipment located only in the EU without allowing the use of equipment in Singapore, or prohibiting EU companies from storing or processing data in Singapore, and vice versa.

2) Harmonize personal data protection regimes, taking into account the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[7] The Guidelines, for example, include the use limitation principle, i.e. data may only be used in accordance with the purpose for which consent has been given.

3) Develop open government data that could be used in the production of digital trade goods and services. The following criteria are established for them: machine-readable format; possibility to work with data (editing, copying, etc.); access to data through a user-friendly and freely available interface; placement of open data together with metadata; access to data on a free-of-charge basis, etc.

4) Develop single window systems to simplify the administration of digital trade.[8] It is envisaged to launch an information exchange between EU and Singapore customs authorities to facilitate the movement of e-commerce goods. For example, the exchange of customs information allows for the classification of goods by risk and the speeding-up of entry procedures for low-risk goods.

5) Counteract fraudulent practices against customers, such as advertising goods and services without the intention of supplying the goods (bait advertising).

Russia's experience

Russia has not yet concluded international agreements on digital trade to facilitate cross-border data flows. However, the EAEU is working on several such agreements.

For example, in 2022 work on a draft Agreement on Data Circulation in the EAEU was launched.[9] The text of the agreement is not yet available, but EAEU countries have national restrictions on data circulation (such as localization requirements in Russia and Kazakhstan). There is a lack of harmonization in data protection regimes, for example, the requirements for the format of consent are not harmonized (in Armenia and Belarus – formats are to be written and electronic, while in Russia and Kazakhstan any form is allowed).

In February 2025, the EAEU Agreement on Electronic Trade in Goods was approved.[10] To increase the transparency of e-commerce in the EAEU, the states are obliged to provide access to open data used in the sphere of mutual e-commerce - their list will be approved by the EAEC. The national regime of personal data legislation is established. However, the Agreement does not cover the issue of protection of e-commerce participants, for example, it does not contain restrictions on unfair commercial practices (such as misrepresentation of the price of goods), does not cover the problems related to cross-border data flows.

2. Online anticompetitive practices

The experience Germany

In April 2025, two abuse of dominance rulings were issued against Google in response to complaints from map service providers (like TomTom).

The first decision concerns Google Maps,[11] which offers mapping services such as map display (3D street views), route navigation, fixing and displaying locations on the map, etc. Third-party Android app developers can integrate such services into their apps - already

[6] https://data.consilium.europa.eu/doc/document/ST-5854-2025-INIT/en/pdf

[7] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[8] Note: Single window is an information system with a single entrance for exporters and importers to interact with authorities of different countries authorized in the field of foreign economic activity regulation.

.

[9] https://eec.eaeunion.org/news/v-eaes-pristupili-k-prakticheskoj-rabote-nad-soglasheniem-ob-oborote-dannyh-/

[10] https://www.alta.ru/tamdoc/25r00014/

[11] https://www.internationale-kartellkonferenz.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2025/B7-25-22_GMP.pdf?__blob=publicationFile&v=4

integrated into more than 10 million websites and mobile apps. At the same time, Google restricted the combination of Google Maps and map services from several providers (competitors of Google). Thus, developers were forbidden to:

1) Use maps, information about places on a map or other content other than that provided by Google.

2) Use services from other providers that are similar to or recreate the features of Google Maps.

3) Connect Google Maps and third-party mapping services if the application combines mapping services from different providers.

Google is recognized to be limiting the compatibility of Google Maps and competitors' mapping services.

The second proceedings relate to Google's abuses in the market of services for on-board car systems (route display screen, gesture control of services, voice assistants, etc.). Google sold a GAS package (Google Maps, Google Play and Google Assistant services) for cars to car manufacturers.

However, manufacturers could only connect the full GAS package (all 3 services), the services cannot be connected separately. For example, Google Maps can only be used with Google Play and Google Assistant.

The single GAS package also forces car manufacturers to connect the whole package without the option of linking Google services with similar services from other providers (like TomTom). In addition, Google limited the interoperability of its services with those of competitors, for example, the Google Assistant voice assistant did not interact with third-party mapping services and voice assistants.

The experience of Japan

In April 2025. The Japan Fair Trade Commission found that Google had entered into anticompetitive agreements with Android smartphone manufacturers and mobile network operators. The agreements included mandatory pre-installation of Google services.

Android smartphone manufacturers and mobile carriers could also generate some search advertising revenue if they fix Google Chrome as the default browser and don't integrate other developers' search engines.

Google must now remove the enumerated terms and conditions in the agreements, develop internal rules to ensure antitrust compliance.

The experience of India

In April 2025, the Competition Commission of India ruled against Google[12] for anti-competitive agreements with smart TV manufacturers. Manufacturers wishing to install the Google Play app store were required to:

1) Pre-install the full set of Google applications (Google TV Services and YouTube), which, for example, promoted YouTube and reinforced Google's dominance in the video hosting marketplace.

2) Do not use alternative versions of Android (forks[13]). This restricted the manufacturers' ability to develop and release devices on a modified Android operating system.

A settlement agreement was signed with Google to cancel these provisions, and Google must also pay a fine of about $2.4 mn.

The US experience

In April 2025, a District court in California issued an injunction against[14] the cab hailing and food delivery app Uber One. Uber offered a paid subscription, claiming that consumers would save up to $25 per month on rides and deliveries compared to those without subscription. However, it was revealed that:

1) There is no real evidence of savings of $25 per month.

2) Uber connected users to paid subscription without warning and without consent. For example, on the checkout screen, the user was automatically flagged that the user could save money with a free trial of Uber One. And if the checkbox was unchecked, it wasn't clear what was being canceled - the order or the subscription. And after 4 weeks, Uber automatically connected to paid subscription with periodic debiting of funds.

3) Uber notifies users 48 hours before the fee is charged that they can cancel their subscription, but due to unclear instructions on how to cancel subscription, users contacted

[12] https://www.cci.gov.in/antitrust/orders/details/1182/0

[13] Forks are modified versions of the operating system based on the original OS source code, but with changes in the interface, features or built-in services (can be used by device manufacturers as an alternative to the standard version of Android).

[14] https://www.ftc.gov/system/files/ftc_gov/pdf/uberonecomplaint.pdf

customer support, which, however, delayed responses for more than 48 hours, after which the fee was already charged.

Russia’s experience

Today in Russia, the FAS is focused on regulating dominant marketplaces. For example, by the end of March 2025, Ozon and Wildberries had to create a transparent discount mechanism for sellers. According to media reports,[15] the FAS should also define the criteria of “large” platforms and develop special antimonopoly requirements for marketplaces, such as restrictions for large platforms in terms of priority promotion of their own goods, the amount of investment in discounts, etc., as well as to establish a transparent mechanism of discounts for sellers.

3. Protection of personal data on the blockchain

The EU experience

In April 2025 the European Data Protection Board (EDPB) released Guidelines on the processing of personal data using blockchain technology[16] to comply with GDPR. The blockchain contains personal data because it stores the data of the participants in transactions (identifiers, IP addresses), data on the amounts of cryptocurrency, the goods purchased and so on. Although the data is encrypted,[17] its leakage cannot be excluded. According to Defillama, in April 2025, there were 8 hacks of blockchain networks with a damage cost of $113 million.[18] If data leakage occurs as a result of a hack, personal identifiers in the blockchain[19] can be used by attackers to access real personal data (such as passport information, payment information, etc.).

The technical properties of blockchain can pose risks to GDPR compliance. Data is replicated and transmitted simultaneously between participants on different computers on the blockchain network, and any changes or deletions are visible to all participants. Furthermore, if a transaction is made, the transaction data cannot be deleted unless the data is deleted by every participant in the chain on the blockchain. This is contrary to the principle of limiting data storage to the purpose of processing and limits the data subject's right to have the data deleted and rectified.

The EDPB offers the following recommendations for the use of blockchain:

– Use a private, authorized blockchain network. There are different types of blockchain, such as private and public. In a public blockchain (such as Bitcoin and Ethereum), each participant can see and create new blocks. In a private blockchain, there is a single central node that grants permission to other participants to participate: only selected nodes can read or create blocks. Therefore, in a private blockchain, data subjects are protected from possible access to their data.

– Only a hash that identifies an individual can be stored on the blockchain,[20] all other data can be stored privately off-chain. And if the data subject withdraws consent to data processing or wants, for example, wants to change the data, it is possible to delete the participant's hash in relation to individual transactions, making the data unidentifiable to the specific individual.

The EDPB recommends data controllers (similar to data controllers in Russia) to assess:

1) Whether the data on the blockchain will contain personal data.

2) Whether blockchain must be used or alternative technologies can be used.

3) What type of blockchain should be used.

4) Whether data will be stored on or off-chain.

Russia’s experience

In Russia, there is no specific regulation regarding the protection of personal data on the blockchain. At the same time, the Federal Act №152 “On Personal Data” (as well as the GPDR in the EU) establishes the obligation of the data controller (in the EU) to destroy or anonymize

[15] https://www.vedomosti.ru/business/articles/2025/02/26/1094482-fas-pridetsya-vnesti-novie-antimonopolnie-trebovaniya

[16] Blockchain is an electronic database (a single network) consisting of nodes (computers of each network participant) that maintain the network and validate transactions (e.g., Ethereum, Ripple, Solana, etc.). A blockchain network stores transaction data (e.g., the transfer of cryptoassets between participants) in the form of blocks, each linked to the previous one, connected into a single chain.

[17] With special encryption keys, i.e. certain alphanumeric characters - and only those with the encryption key have access to the data.

[18] https://defillama.com/hacks

[19] Blockchain Person Identifiers - records in the blockchain network related to a specific user (may contain information such as logins, passwords, passport data, payment information, etc.).

[20] Hashing is a cryptographic process of data encryption - converting raw data (e.g., a transaction or message) into a string of characters (a sequence of symbols and letters) according to a specified algorithm. The blockchain itself already shows the result of data encryption - the hash.

data once the purposes of its processing have been achieved.

Blockchain is rapidly developing in Russia. In April 2025, Rusnano announced the use of blockchain for a system of recording and storing data on its intellectual property rights to scientific developments.[21] However, there is a need for legal certainty regarding the use of the technology, including personal data.

4. Preparing the workforce for the challenges of AI

The OECD experience

In April 2025, the OECD released a report on training and adoption of AI technologies.[22] About one-third of jobs in OECD countries involve AI, and only 1% of jobs require highly specialized AI competencies (like skills in developing, customizing AI systems: machine learning, building and training models, working with big data, using frameworks[23] (like TensorFlow and PyTorch[24])).

The professions most affected by AI are those where more than 70% of employees have higher education - managers, IT specialists, scientists, accountants and translators. More than 90% of them are of working age.[25] However, there is no evidence of mass displacement of such workers as a result of AI implementation.[26] In general, for most workers, basic knowledge and skills in interacting with AI ("AI literacy") are sufficient: the ability to use AI tools in everyday tasks, understand their algorithms and assess the risks associated with their use.

Analysis of educational programs has shown that in Australia, Germany, Singapore and the US, only 0.3-5.5% of courses include modules on AI. The main focus is on training specialists in AI development, while programs to develop general AI literacy are less common.

The following trends in OECD countries can be identified:

– Building basic digital and AI literacy among a wide audience. For example, Austria is implementing the Digital Everywhere project: in 2024, 3,500 master classes on digital skills (including AI and cybersecurity) were held.

– Promoting AI and digital solutions for SMEs.

– Retraining workers at risk of automation. Singapore implements two-day courses on automation, cyber risk and analytics for low-skilled workers (in the food, textile and manufacturing industries), who are predominantly men without tertiary education and migrants.

– Training highly qualified specialists in AI and related fields. The UK implements Skills Bootcamps - 16-week courses on AI and digital technologies in cooperation with employers.

The OECD recommends developing AI skills through the following measures:

– Financial support: Subsidies, tax credits, training vouchers and grants for employers, especially for training workers at risk of automation.

– Non-financial measures: Career counseling, development of teacher training programs, creation of partnerships between universities and businesses.

– Lowering access thresholds: Simplifying entry requirements for AI courses.

– Developing general AI literacy initiatives through specialized short intensive courses.

– Integrating AI learning into HR strategies.

Russia's experience

In April 2025, a Rosbalt analysis showed that at least 10 mln Russians (cashiers, machine operators and middle-aged white-collar workers) are at risk of unemployment.[27] For example, FixPrice launched 5,800 self-service terminals, ensuring the processing of about a third of all transactions. Due to similar automation in other retail chains (Magnit and X5) around a million cashiers may be out of work.[28]

Russia is developing free or partially subsidized courses on digitalization. It is

[21] https://www.rusnano.com/news/20250421-gruppa-rosnano-rtsis-sozdayut-blokcheyn-infrastrukturu-dlya-ucheta-oborota-intellektualnykh-prav-na-razrabotki/

[22] https://www.oecd.org/en/publications/bridging-the-ai-skills-gap_66d0702e-en.html

[23] A framework is a set of out-of-the-box tools that help you quickly build and train AI models.

[24] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/who-will-be-the-workers-most-affected-by-ai_fb7fcccd/14dc6f89-en.pdf

[25] https://www.oecd.org/en/publications/who-will-be-the-workers-most-affected-by-ai_14dc6f89-en.html

[26] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/using-ai-in-the-workplace_02d6890a/73d417f9-en.pdf

[27] https://www.rosbalt.ru/news/2025-04-26/yaroslav-ignatovskiy-kak-vpishetsya-ii-v-rossiyskuyu-deystvitelnost-5377851

[28] https://companies.rbc.ru/news/NPD5d7jSuo/fix-price-vnedril-bolee-3-200-kass-samoobsluzhivaniya-v-2024-godu/

planned to train 600 thousand people by 2030, the Ministry of Digital Development, Communications and Mass Media is selecting organizations and programs to receive subsidies.[29]

5. Rising cyber risks for SMEs

In April, the WEF released the Global Cybersecurity Outlook 2025,[30] highlighting 3 cybersecurity challenges: (1) growing cyber risks for SMEs, (2) growing interest of organized crime groups in the cybercrime "marketplace" and the declining cost of AI attacks, and (3) differences in how countries approach cybersecurity regulation and the resulting increased cost of compliance.

The cyber resilience risks of large organizations are linked to the vulnerabilities of SME suppliers. This is the opinion of 54% of surveyed CEOs of large companies. By attacking the security system of an SME supplier, an attacker can gain access to the entire ecosystem of a large organization.

Another trend is the development of cooperation between cybercriminals and traditional criminal groups. For example, more than 220,000 people have been sold into slavery in online fraud "factories" in Southeast Asia. Such "factories" collect personal data, launch disinformation campaigns, and conduct social engineering (psychological manipulation of people to commit certain actions).

The development of generative AI reduces the cost of conducting a "successful" attack. In this case, criminals do not even try to hack into the IT infrastructure of organizations but use deepfakes and techniques to convince employees of organizations to make transactions in their favor. Last year alone, losses to individuals and companies from cyber fraud totaled $1 trillion, and some economies lost more than 3% of GDP.

Countries differ in their approaches to cybersecurity regulation, creating barriers to business. For example, OECD countries have different requirements for the timeframe for critical infrastructure operators to report cyber incidents, different requirements for software products to have SBOM,[31] and so on.

It is worth noting that the cybersecurity risks highlighted in 2025 echo the challenges that the WEF has been highlighting since 2022 (when the first Global Cybersecurity Outlook appeared). However, a retrospective analysis of WEF documents since 2006 shows that some risks have faded into the background over almost 20 years. For example, the threat of DDoS attacks was one of the most significant in 2013, but in 2025, it faded into the background. According to WEF surveys, only 6% of respondents consider this problem significant.

Russia's experience

The Russian market echoes the international trends and challenges listed in the WEF report. According to Solar Group (a major company in the cybersecurity market), in 2024 the company repelled more than 1.8 bn cyberattacks on clients' information systems, which is 2.4 times more[32] than in 2023.[33] The majority of cyberattacks in Russia are on SMEs - 81% (38% - small and 43% - medium-sized businesses).[34]

Russia is developing cybersecurity regulation. In April 2025, amendments were adopted establishing the obligation of critical infrastructure entities to use only domestic software, information about which is included in the Unified Register of Russian Computer Programs and Databases, and which complies with information protection requirements.[35] Such critical information infrastructure includes information systems and networks operating in the healthcare, transportation, communications, energy, banking, and industrial sectors.[36]

Unlike OECD countries, Russia has not introduced horizontal requirements for all software developers, such as SBOM - such requirements are still in force only for organizations that receive a license from the FSTEC (primarily for critical information infrastructure operators). The requirement for software products to have SBOM allows for a better assessment of software hacking risks.

[29] https://digital.gov.ru/activity/it-obrazovanie/kod-budushhego-ii

[30] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[31] Software Bill of Materials, a machine-readable list of all the libraries, frameworks, drivers, and other components from which the software is built - similar to the composition label on a food product.

[32] https://rt-solar.ru/analytics/reports/5335/

[33] https://rt-solar.ru/events/news/4991/?utm_source=chatgpt.com

[34] https://innostage-group.ru/press/news/eksperty-innostage-kiberatak-na-sredniy-i-malyy-biznes-v-2024-godu-stanet-sushchestvenno-bolshe/?utm_source=chatgpt.com

[35] Federal Law No. 58-FZ of 07.04.2025 "On Amendments to the Federal Law 'On the Security of Critical Information Infrastructure of the Russian Federation'".

[36] P. 8 Art. 2 Federal Law of 26.07.2017 No. 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation".