TECHNOLOGICAL BUSINESS STRATEGIES IN RUSSIA

TECHNOLOGICAL BUSINESS STRATEGIES IN RUSSIA

The study is prepared by the MWS Intelligence Team

Please send your questions, comments on this study or your ideas for collaboration to: Intelligence_Team@mts.ru

EXPERTS

Pavel Voronin

MWS CEO,
First Vice President of IT MTS

Igor Zarubinsky

MWS Executive Director,
CEO MWS Cloud

Denis Filippov

MWS AI CEO

Danila Egorov

MWS Cloud Director of Business Strategy

Mikhail Tutaev

Director of MWS Cloud Products

Polina Lee

Head of MWS Cloud Intelligence Team

Galina Gaydarhzhi

Business Analyst of MWS Cloud

CONTENTS

PREAMBLE

INTRODUCTION

TAXONOMY

METHODOLOGY

INTRODUCTION

Technologies in general and IT technologies for B2B are developing in large waves. The nineties were marked by the personal computer, software and operating systems for PCs. The 2000s was a time when corporations were ubiquitously implementing the internet and monolithic platforms. In the 2010s, companies migrated to the cloud. Each wave completely restructured the IT landscape.

> “ As one of the key bigtech companies in Russia, we see that AI agents are already radically changing the approach to business management, customer service and digital product development — from autonomous processing of routine tasks to support complex management decisions in real time. We create leading technologies: we develop the cloud, build platforms and data platforms, and release tools for developers so that AI agents can be integrated directly into business processes and their effect can be scaled to the entire economy.

Pavel Voronin
MWS CEO, First Vice President of IT MTS

In 2025, we are witnessing how a new technological wave — artificial intelligence — is rapidly shaping a new IT landscape. At the same time, clouds continue to grow, and the number of companies in Russia with more than 1 Petabyte of data has grown from 10 to 29 in just one year.

> “ The introduction of AI over the next 5 years will generate a new IT architecture where AI, platforms, and the cloud form a single technology stack. AI agents, digital employees, will be created on the basis of this stack. The product value will not be software as a tool, but the result of a business task itself. Software users will transform from task performers to agent managers. This will form a completely new technological economy.

Igor Zarubinsky
MWS Executive Director, CEO MWS Cloud

The creation of any technology begins with the client. It is our clients who tell us which product they need, point out the shortcomings and demand improvements. We are eternally grateful to the clients for this feedback. We believe that only deep knowledge of the client's tasks gives rise to great technologies. This year, we decided to focus on three technological areas that are changing most dynamically in Russia. These are clouds, artificial intelligence and cybersecurity. The study is based on responses from representatives of 700 Russian companies. We are very grateful to the participants for taking the time to provide us with the answers.

> “ At MWS, we follow an open approach, so we share the study results with you and make the study publicly available. We hope that the study will help you in your very difficult and very necessary work. Thank you for what you are doing!

Danila Egorov
MWS Cloud Director of Business Strategy

TAXONOMY

The basis of the approach used in the study was the structure of the IT market, which was first formed in the Prospects of the IT Market study. According to the MWS taxonomy, the entire market is segmented into 3 verticals: (1) Software, (2) Hardware, and (3) IT Services. Each of the verticals is decomposed into its component elements and includes solutions for each of the 3 main technological areas: clouds, cybersecurity and artificial intelligence.

From 2019 to 2024, the share of the Russian IT market in the global market was stable and ranged from 1.1% to 1.3%. Nevertheless, the ongoing digital transformation of key sectors of the economy contributes to the growth of IT penetration into the country's GDP. Between 2023 and 2024, the increase was 0.27 percentage points, which is higher than the same indicator for other countries.

The growth rate of the Russian IT market in 2019–2024 is comparable to global indicators. However, the cost structure differs significantly. Russia traditionally has a lower share of the Hardware vertical, largely due to the geographical and industrial specialization of other countries in the production of high—tech components, as well as the increasing role of software solutions. Additionally, the dynamics of the Hardware vertical is influenced by the ongoing transition of the business to cloud consumption models, which reduces the need to purchase its own computing power. The expansion and increased efficiency of cloud solutions are driving this trend, helping to optimize end-user capital expenditures.

> “ The Software vertical is showing steady growth, both in Russia and on the global market. The average annual increase in the share of this segment in the IT market is estimated at about 2% during 2019–2024. The main driver is the transition of business to subscription models, which make software more accessible to companies of different scales and reduce barriers to testing new technological solutions.
>
> 
>
> **Pavel Voronin**
> MWS CEO, First Vice President of IT MTS

The IT Services segment shows the lowest growth rates among the three key verticals. The dynamics of this trend are influenced by macroeconomic instability, saturation of individual markets, as well as a shift towards no-code and low-code solutions that partially displace traditional services. At the same time, it is expected that an increase in the number of cyber threats and the active development of artificial intelligence-based products may support the demand for IT services in the short term.

The cloud market deserves special attention: it is expected that by 2030 the share of this market from the entire IT market in Russia will reach 6%. High average annual growth rates in monetary terms (32% for the period 2021–2024) create the prerequisites for a noticeable development of the market in the medium term. Cloud solutions are becoming one of the key elements of the digital business transformation strategy in Russia, providing flexibility and reducing infrastructure costs.

The structure of the Russian IT market

	2023	2024	2025	2026	2027	2028	2029	2030
The size of the Russian market, bn rubles	**2 702**	**3 302**	**3 992**	**4 700**	**5 478**	**6 260**	**7 090**	**8 004**
Hardware, bn rubles	725	842	945	1 085	1 249	1 429	1 626	1 839
Software, bn rubles	1 063	1 404	1 816	2 236	2 686	3 105	3 548	4 031
IT-Services, bn rubles	913	1 056	1 231	1 379	1 543	1 726	1 916	2 134
Hardware, %	27%	25%	24%	23%	23%	23%	23%	23%
Software, %	39%	43%	45%	48%	49%	50%	50%	50%
IT-Services, %	34%	32%	31%	29%	28%	28%	27%	27%

The share of the cloud segment in the Russian IT market in 2023–2030

	2023	2024	2025	2026	2027	2028	2029	2030
Cloud's share in the Russian IT market	4.4%	5.1%	5.2%	5.3%	5.4%	5.6%	5.8%	6.0%

The IaaS/Paas subsegments are of particular interest in the development of cloud solutions. They account for about 65% of the total cloud solutions market and are the drivers of industry development. The growth in demand is provided not only by the increased demand for classical solutions, but also by the development of artificial intelligence technologies.

The penetration of the Russian IT market into the country's economy

2.2%
IT's share in Russia's GDP 2025

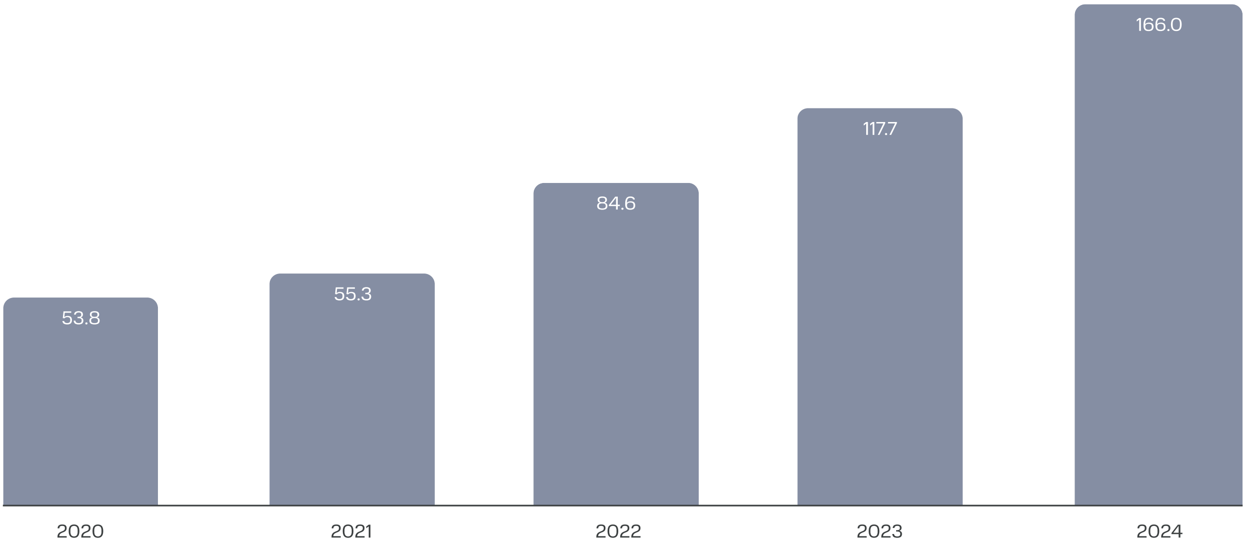
3.1%
IT's share in Russia's GDP 2030

The IaaS/PaaS subsegment is characterized by one of the highest growth rates in the structure of the Russian IT market. In 2021–2024, the average annual growth was about 30%, indicating the rapid spread of cloud technologies in the corporate sector. Nevertheless, the growth rate of IaaS/PaaS is showing a gradual slowdown, reflecting an increase in market maturity: in 2024, there was a 32% increase in volumes compared to the previous year.

For more information about the structure of the IT market, see the IT Market Prospects study.

The volume of the cloud segment in the Russian IT market

The market volume is indicated in bn rubles



> Despite the projected growth of all areas of the IT market in the medium term, today we are witnessing a qualitative change in its structure towards Software growth. The expected average annual growth rate of software in the period 2023–2030 is 20.6% per year, with the projected growth of the IT market by 17.4% per year, reflecting the transition of business to more flexible and economical consumption models. The accelerating digitalization of key industries creates the foundation for a steady increase in the share of IT in the country's economy. In our strategic vision, we put the understanding that "software eats the IT market."

Igor Zarubinsky
MWS Executive Director, CEO MWS Cloud

METHODOLOGY

This study is a logical continuation of the previous IT Market Prospects study and focuses on assessing the situation from the demand side. Its results will be especially useful to companies focused on improving efficiency through the introduction of digital technologies, in particular, to the teams of analytics, sales, product management, strategy and marketing, as well as key decision makers.

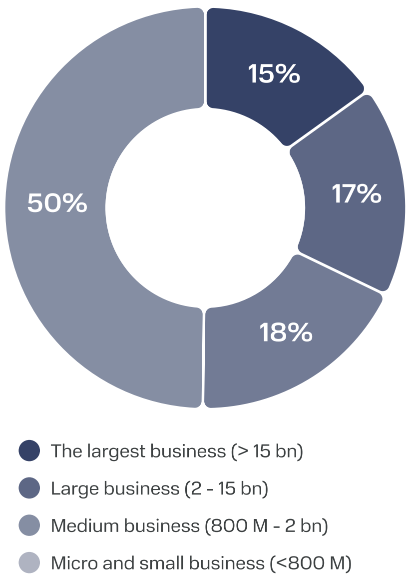
The study is based on a questionnaire survey of representatives of more than 700 Russian companies. In addition, in-depth interviews with some of the respondents were conducted to expand the understanding of certain aspects of the study.

The sample included only companies that confirmed the availability of budgets for the purchase, development, or use in business operations of at least one of three technologies: cloud solutions, cybersecurity, and artificial intelligence.

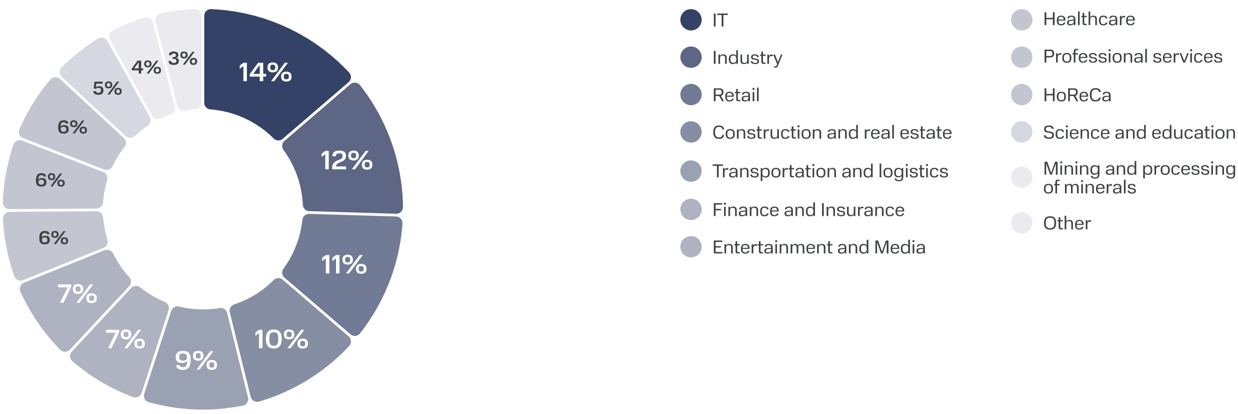
The study respondents represent different business segments in a balanced manner. Half of the sample consists of micro and small-sized companies, the remaining 50% are representatives of medium, large and largest businesses, and these shares are evenly distributed.

The structure of respondents by business segment

The revenue amount, rubles

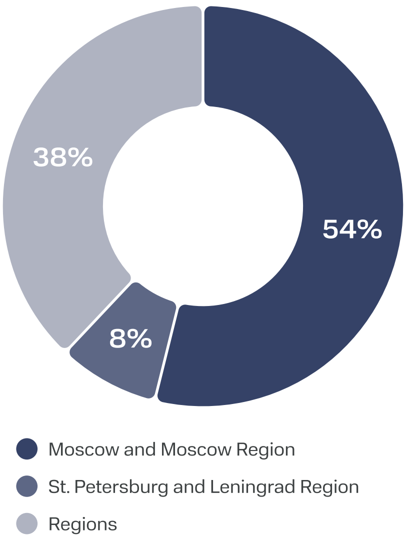


The structure of respondents by industry

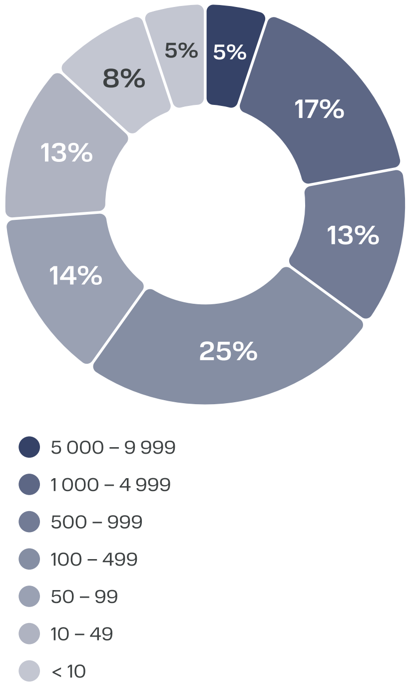


The majority of the respondent companies are located in Moscow and the Moscow region, but over a third of the respondents are represented by regional businesses, which provides a wide geographical coverage. The sample is also diverse in terms of personnel: 26% of companies are small businesses with fewer than 100 employees, the share of large companies (from 1 LLC to 4 999 employees) and the largest companies (from 5 LLC to 9 999 employees) is 13% and 17%, respectively.

The structure of respondents by the main office of the company



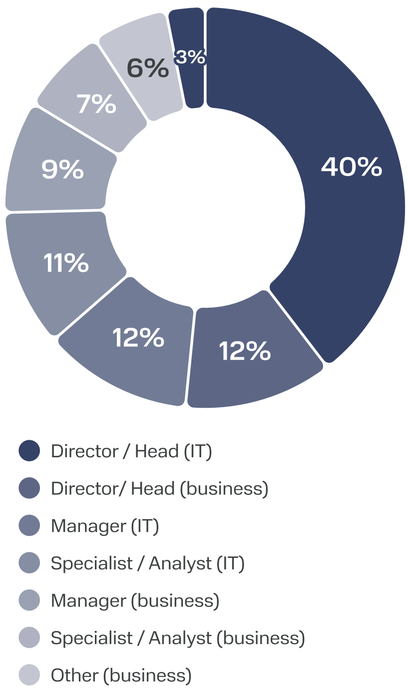
The structure of respondents by number of employees



The survey was conducted among specialists who are competent in the development of digital solutions. The selection of employees at different levels is determined by industry and business profile: the organization of digital transformation processes in companies strongly depends on their industry specifics and internal business processes. More than half of the participants represent senior management, which highlights the high level of expertise of the companies in the sample.

Thus, the sample structure provides representativeness for all Russian companies that are already implementing or using the technologies in question. The respondents' high level of competence guarantees the reliability of the collected data and allows them to draw informed conclusions about the current and potential demand for cloud solutions, cybersecurity technologies and artificial intelligence in Russian business.

The structure of respondents by position of the employee who took the survey



MTC WEB SERVICES

A bigtech company providing cloud and A1 services and platform solutions for various business tasks: from working with data to product development and process optimization

15
availability zones based on Tier III data centers

~ 280 000
kilometers of own communication channels

Standards support
UZ-1, GIS K1, 152-FZ, PCI DSS, GOST R 57580

No. 1
in the laaS Enterprise 2024 ranking

TOP-5
Russian-language AI solutions according to Mega's assessment

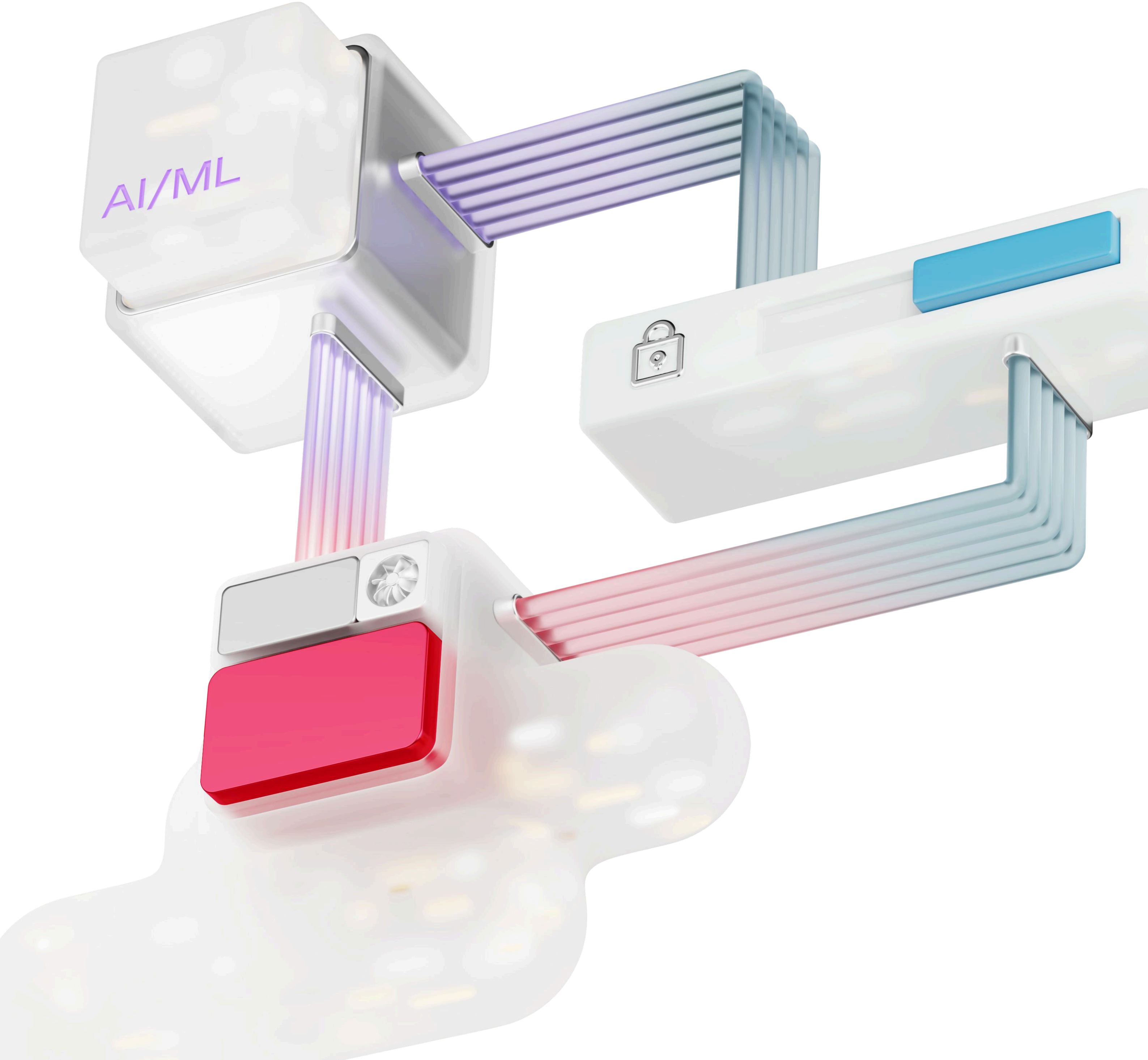
TOP-3
the NIST benchmark for the quality of face recognition algorithms

15 M
ecosystem users

No. 1
in the GPU CLOUD ranking

No. 1
LLM on coding accuracy in Russia

TECHNOLOGICAL BUSINESS STRATEGIES



IT BUDGETS

In 2024, the size of the IT budget of Russian companies averaged 2–3% of annual revenue, which is comparable to global practice: According to a Gartner study, in 2024, the median value of IT spending by firms around the world was 3.1% of revenue. In absolute terms, the majority (> 65%) of Russian companies surveyed have an annual IT budget of less than 100 M rubles, and only 14% of firms have it exceeding 1 bn rubles.

> The largest IT budget in 4 industries: IT, finance and insurance, mining and processing, entertainment and media

Respondents' IT budgets by industry

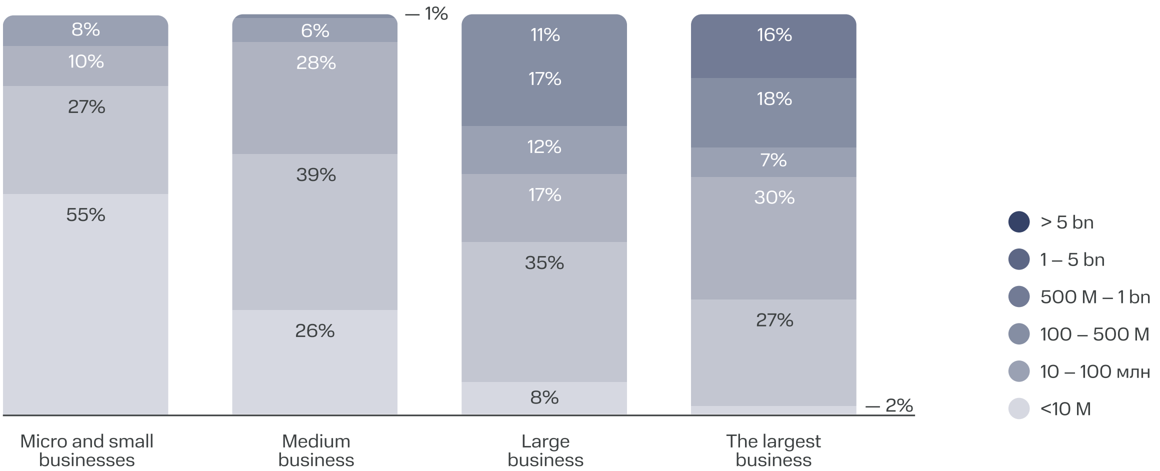
	< 10 M	10 – 100 M	100 – 500 M	500 M – 1 bn	1 – 5 bn	> 5 bn
IT	24%	28%	13%	13%	11%	10%
Finance and Insurance	33%	19%	11%	8%	20%	9%
Mining and processing of minerals	33%	32%	8%	7%	11%	9%
Entertainment and Media	22%	25%	36%	6%	3%	8%
Healthcare	33%	39%	15%	4%	4%	5%
Professional services	53%	25%	5%	12%	1%	4%
HoReCa	43%	30%	13%	6%	5%	3%
Science and education	37%	27%	20%	4%	3%	3%
Retail	54%	26%	8%	4%	4%	3%
Real Estate	54%	26%	9%	3%	5%	2%
Transportation and logistics	45%	23%	18%	10%	1%	2%
Industry	46%	37%	7%	6%	4%	2%

There remains a high level of differentiation in the distribution of IT budgets depending on the industry affiliation and size of the company. The largest IT costs are incurred by companies in the IT market, whose products are primarily based on digital solutions, as well as by the largest companies from traditional industries (industry, mining), which are also actively investing in tools to automate working processes and increase efficiency.

It is expected that the size of the IT budget is most closely related to the size of revenue: for the vast majority of companies (> 68%), micro and small-sized businesses (revenue < 800 M rubles) The IT budget does not exceed 10 M rubles, whereas the largest firms with revenues of > 15 bn rubles have a much greater variety of budget sizes. Thus, more than a third of the largest companies have an IT budget of more than 1 bn rubles. As revenue grows, the variability in the size of IT budgets increases, reflecting the complexity and versatility of the tasks that companies solve: from basic automation and support for existing IT infrastructure to the introduction of more advanced AI/ML solutions.

Respondents' IT budgets in business segment

Each column represents a business segment based on revenue. The colors indicate the size of the IT budget.



Effective management of the IT budget for most companies involves regular review, depending on changes in business priorities and the external environment. The majority of companies, regardless of the size of revenue (> 60%), adjust their IT budget from 1 to 2 times a year.

As the size of the company increases, the frequency of IT budget revisions also increases: among micro and small-sized businesses (revenue up to 800 M rubles), companies that adjust the IT budget less than once a year are most often found, which may indicate limited maturity and the need to use cost actualization mechanisms. At the same time, the largest companies (with revenues > 15 bn rubles) are most characterized by updating budgets on an annual basis, which may be due to a long cycle of coordination and approval of financial figures, as well as setting strategic goals for annual planning.

As part of the execution of IT budgets, the amount of costs for various technological solutions is unevenly distributed. According to the survey results, three key technology areas — cloud solutions, cybersecurity (CS) systems, and artificial intelligence (AI) — account for 17% of the total IT budgets of Russian companies.

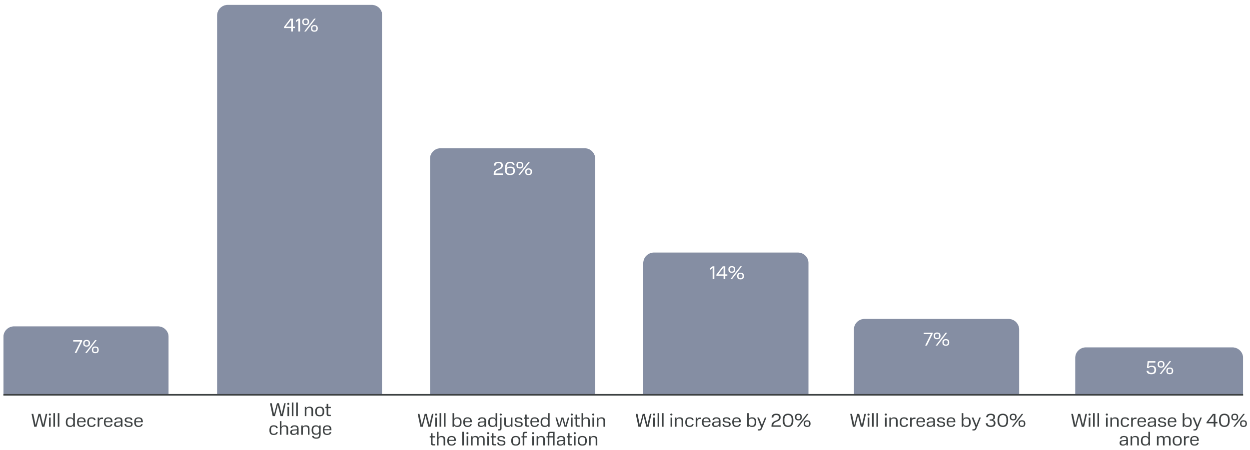
In terms of spending on these technological areas, domestic companies still lag behind international players, whose comparable costs can reach 50%. In addition, the structure of IT budgets in the world and in Russia also differs: cloud solutions occupy the leading positions in international practice, CS ranks second, and AI ranks third. In Russia, CS is the leader in terms of budget, clouds are in second place, and AI is in third. The differences may be related to the growing threats in the field of information security in Russia. The total number of cyber attacks is growing, DDoS attacks and attacks on major players with the aim of further compromising sensitive data are especially relevant, and the number of ARS groups attacking Russia and the CIS countries is also increasing. The answer to the increasing cyber threats is the complication of legislation: in 2024, 187-FZ and 152-FZ were tightened, and a new FSTEC regulation was developed.

Cloud technologies and cybersecurity have a non-linear distribution in the IT budget: their share increases by 1–2 percentage points with revenue growth, reaching a maximum for medium-sized companies (revenue from 800 M rubles to 2 bn rubles), after which the share of these technologies decreases. This trend may be due to the high minimum cost threshold required to deploy cybersecurity technologies and, at the same time, the relatively low cost of further scaling and maintaining operational solutions. The share of AI in the structure remains within 2–4% and has no significant differences depending on the size of the company's revenue.

> “ As threats become more complex and regulatory pressures increase, the market is already moving towards a more balanced allocation of investments between basic IT infrastructure, cybersecurity, and advanced digital solutions. At the same time, the contribution of the IT sector to global GDP reaches about 2.62% and exceeds the same indicator in Russia by 43%. To reach the appropriate level, it is necessary to accelerate the growth of investments primarily in the most promising areas of IT — cloud services and solutions based on artificial intelligence, which form a new level of business efficiency and manageability.

Igor Zarubinsky
MWS Executive Director, CEO MWS Cloud

Expected change in IT budgets in 2025 by business segment



Investments in cloud technologies, CS and AI are becoming a standard item of the IT budget in a wide variety of sectors — from retail to industry. This confirms the growing maturity of digital strategies and the spread of AI practices beyond IT and finance. The high level of investment in traditionally less digital industries indicates that technological development and economic transformation are accelerating — an important component of this area is the introduction of clouds, CS tools and AI.

Only 28% of the surveyed companies plan to expand the budget size for the technologies in question by more than the inflation rate. Artificial intelligence is the leading direction for expanding consumption.

Among all respondents, there is a direct relationship between the size of companies' revenue and the scale of the planned change in consumption: the higher the organization's income, the more often the company declares plans to increase investments and the greater the amount of growth. This pattern can be traced for all categories of technologies, with the exception of cloud solutions, where the potential volume of usage expansion remains more uniform depending on the size of the business. The largest increase in consumption is planned for AI, which is due to the low volumes of current implementation, as well as the significant expected potential to increase the efficiency of business processes in almost all industries.

TOP 5 industries in terms of cloud, CS, and AI costs in the IT budget

IT
Finance and Insurance
Entertainment and Media
Retail
Mining and processing of minerals

TECHNOLOGICAL BUSINESS STRATEGIES: CLOUD

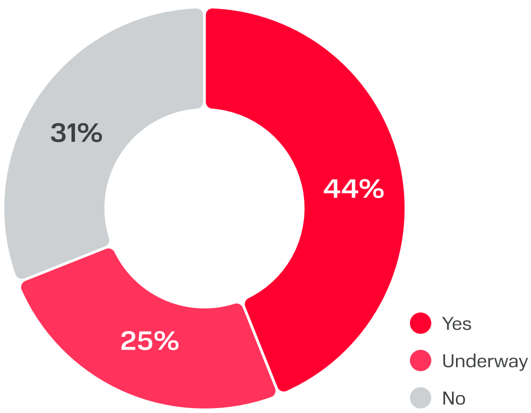
The strategy of implementing cloud technologies serves as a key indicator of the digital maturity of Russian companies and their readiness for transformation. Moving to the cloud is not only a technological choice, but above all a strategic one that affects a business' ability to adapt, reduce costs, and accelerate innovation.

44% of companies are implementing cloud technologies as part of a strategic approach, which indicates a developed but not yet saturated market for cloud solutions in Russia. This demonstrates a growing understanding of the value of clouds, from flexibility and scalability to cost optimization. These companies can be classified as "mature" cloud users. The availability of reserves in increasing the share of system consumers of cloud solutions creates a window of opportunity for cloud service providers.

A quarter of the companies are still in the process of forming a strategy, which indicates the stage of understanding and preparing the infrastructure. These companies are most likely already facing the needs of digital transformation, but have not yet moved to a systematic implementation. This category may be the most sensitive to external stimuli, both from regulators and from the point of view of market competition. It is this segment that will potentially become the next wave of demand for infrastructure, training and migration support.

Almost a third of companies do not have a cloud strategy at all. This may be due to several factors: (1) small or medium-sized businesses with insufficient resources or expertise, (2) companies operating in traditional or regulated industries (such as industry) where the transition to the cloud is complicated by security and regulations, (3) lack of understanding of the potential of clouds or resistance to changes at the management level.

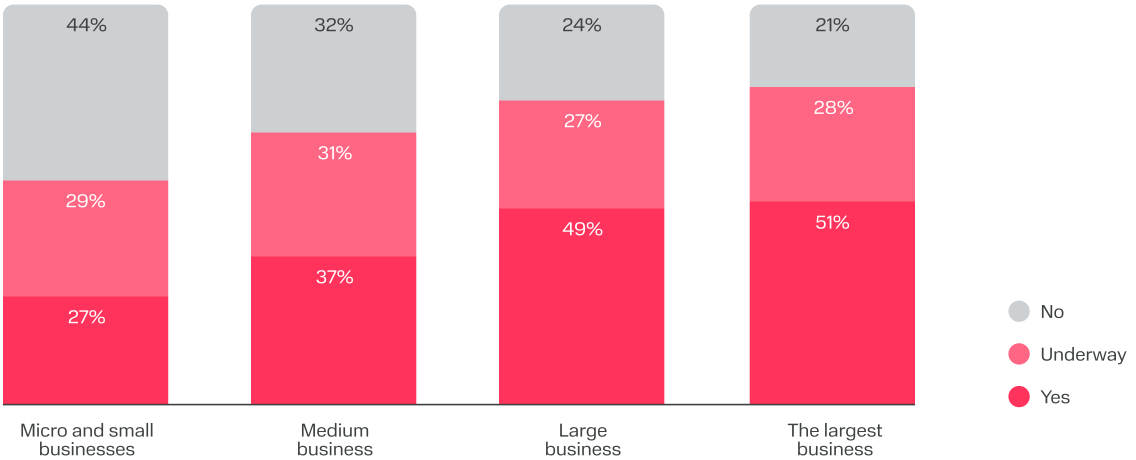
Having a strategy for implementing cloud technologies



The study shows a clear relationship between the size of companies' revenue and the availability of an already formed cloud strategy. This directly reflects differences in access to financial resources, the level of IT competencies, and the degree of digital maturity of the business.

The size of a company is directly proportional to the presence of a strategy. The largest business companies demonstrate the greatest involvement in the strategic planning of cloud initiatives (revenue over 15 bn rubles) — 51% of respondents noted the presence of a strategy here. For large enterprises (revenue from 2 to 15 bn rubles). This figure is slightly lower and amounts to 49%. Micro and small-sized businesses with revenues of up to 800 M rubles remain the least prepared — 44% of them do not have a cloud strategy at all, which is the lowest value of all the segments considered. Such a gap is most often associated with limited access to specialized IT expertise and the priority of solving current operational tasks over strategic initiatives.

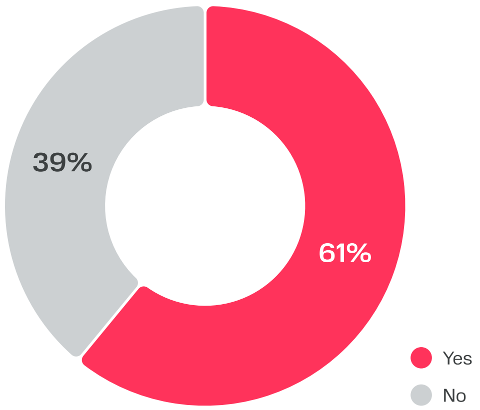
Having a strategy for implementing cloud technologies



From the point of view of having a cloud technology strategy, three key groups of industries can be distinguished: (1) Mature (more than 50% of companies have a cloud strategy). These industries demonstrate a high level of maturity in the field of cloud technologies. It is noteworthy that companies from this group also have a comparable level of strategies under development — about 16%, which indicates sustained attention to the topic and active work in this direction. These industries include IT, transport and logistics, industry, finance and insurance.
(2) Intermediate maturity (30–49% of companies have a strategy). Most of the industries from the scope of study belong to this group. From the point of view of the cloud strategy development process or lack thereof, there is an ambiguous and fragmented picture among these industries. Such industries are entertainment and media, healthcare, professional services, construction and housing and communal services. (3) Low level of strategic maturity (< 30% of companies have a strategy): More than 45–60% of companies from these industries do not have a cloud technology strategy at all. This may indicate both a more conservative approach and the presence of barriers (regulatory, technological, organizational) to the implementation of cloud solutions. These areas include HoReCa, science, and education.

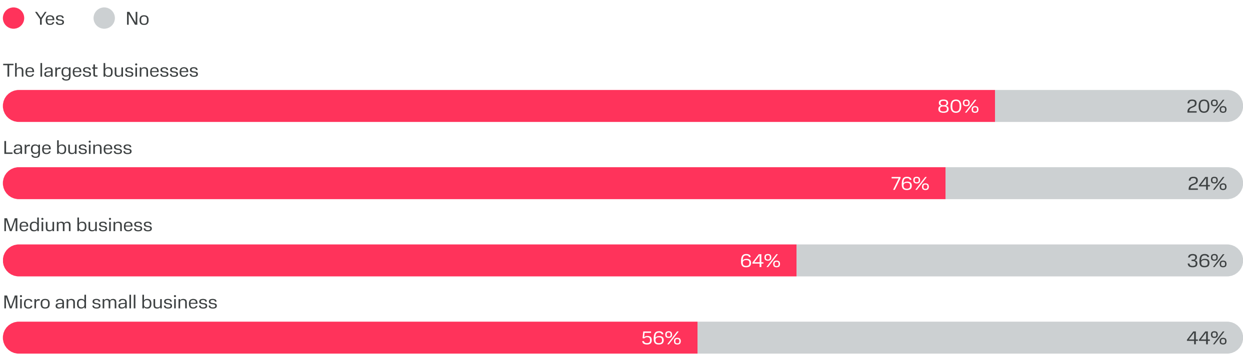
Cloud expertise is becoming one of the key indicators of a company's digital maturity and its ability to effectively scale infrastructure, manage risks, and implement a strategy for moving to hybrid and multicloud models. The difference between companies that already have and are only developing expertise in cloud solutions forms the boundary between organizations that are able to actively develop cloud architecture and those who still perceive the cloud as a potential vector of development rather than as a tool for system transformation. At the same time, the share of companies with a well-established cloud services development strategy is less than the share of companies with expertise. This means that some companies with expertise are still operating within a limited scenario field, without reaching the level of full-scale or comprehensive transformation of the IT landscape.

Having experience and expertise in working with cloud technologies



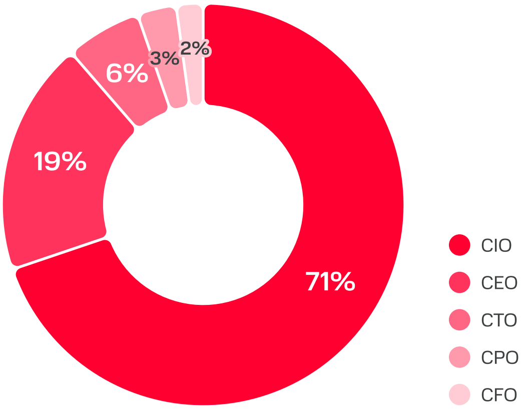
Having experience does not necessarily mean that the practitioners are mature. In many cases, we are talking about implementing separate services — backup, e-mail — without switching to advanced architectures using CI/CD, automated management, FinOps and SLA controls. The level of expertise in working with cloud technologies naturally increases with the growth of the size of companies, as large companies have more opportunities in terms of hiring and training employees. This distribution also reflects strategic priorities. Large businesses are more likely to launch large-scale digital initiatives, invest in DevOps and multicloud architectures, have dedicated IT departments and an informed IT strategy.

Having experience and expertise in working with cloud technologies in business segments



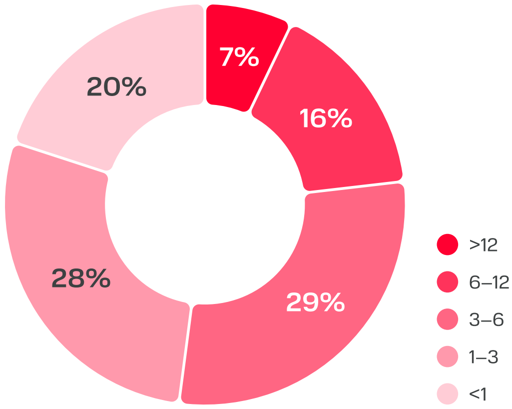
If we look at the industry cross-section, the picture turns out to be more fragmented. The leaders in cloud expertise are IT (90% have relevant expertise), finance (84%), media and entertainment (79%). The high level of engagement here is due either to the very nature of the industry (as in IT), or to the need for high-speed market response, flexibility in scaling, or compliance with high security standards. Thus, expertise in the field of clouds remains heterogeneous.

Key employees (KDM) in the process of migration to the cloud



Duration of the migration process to the cloud

Number of months



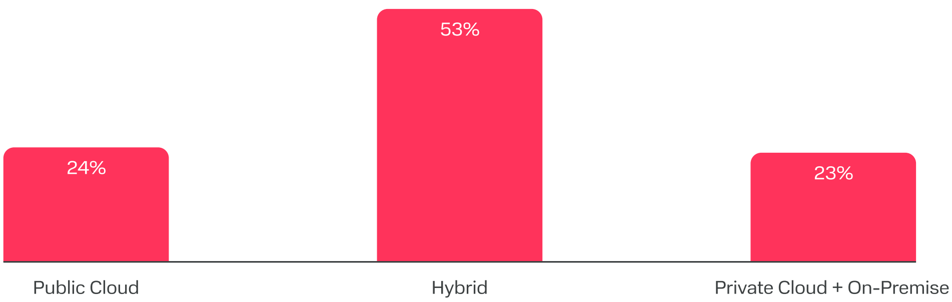
In most companies, decisions about moving to the cloud are made at the C-Level. In every fifth case, the decision to migrate is made directly by the CEO, which reflects the low level of strategic involvement of the top executive, although it is precisely this involvement that can contribute to IT and business synergy and accelerate transformation.

The analysis of migration dates demonstrates a significant dependence on the scale of the company and the complexity of the IT landscape. For 20% of companies, the process took less than a month, which may indicate a compact infrastructure and a limited amount of migration. The most common range was from 1 to 6 months (57% of companies), characterizing scenarios with a medium or high degree of transformation of the company's processes and restructuring of the architecture. At the same time, 23% spent more than six months migrating, which is typical for companies with a significant legacy volume, complex security requirements, or regulated segments.

> Multicloud is already here, 41% of companies use more than 1 provider

Types of infrastructure deployment

Multiple response



Public and multicloud approaches are in demand (36% each, respectively), reflecting the desire for flexibility, scalability, and risk diversification. Since the survey allowed for multiple choices, the data confirms the trend towards using combined architectures: most companies use multiple models at once to balance security, cost-effectiveness, and infrastructure sustainability. This indicates the maturity of IT strategies and a conscious approach to infrastructure architecture.

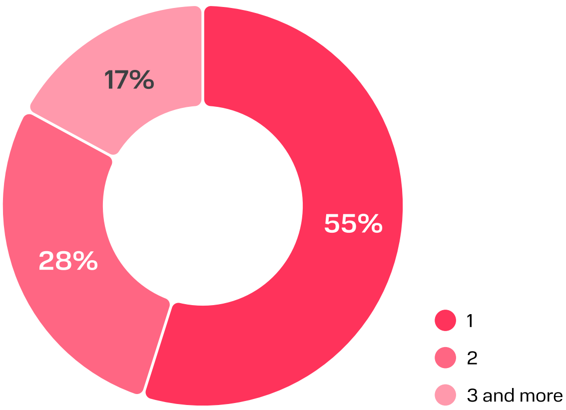
Large (2–15 bn rubles) and largest (> 15 bn rubles) companies more often prefer private installations and On-Premise solutions, emphasizing the importance of security, regulatory requirements and resilience to external risks (for example, sanctions or failures from external providers). Micro and small-sized businesses (up to 800 M rubles), in turn, are more flexible and ready for innovation, which makes them more willing to use public and multicloud solutions, minimizing infrastructure costs.

The larger the business, the more multicloud solutions

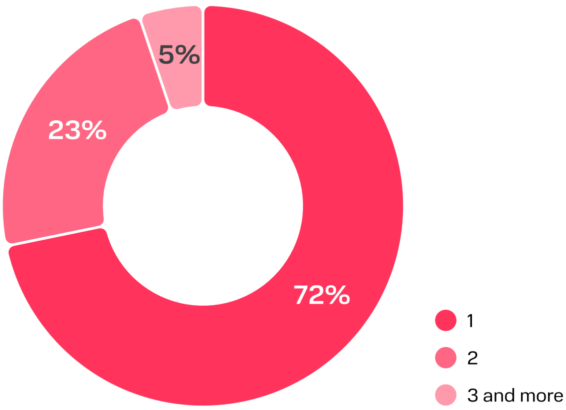
> “ Multicloud architecture is becoming the standard for mature companies. As the number of providers increases, so does the complexity of the infrastructure. This requires more highly qualified personnel, the development of DevOps/FinOps practices, and management automation. Companies choosing one provider rely on simplicity and economy. Those who use multiple approaches focus on sustainability, flexibility, and innovation, but face additional costs and challenges.

Mikhail Tutaev
Director of MWS Cloud Products

Number of Public Cloud providers used



Number of Private Cloud providers used



The singlecloud strategy is less typical for the Public Cloud: only 55% of companies choose it. The advantages are simplification of management, unification of processes and potential cost reduction due to the concentration of services at one provider. However, this model increases dependence on a single supplier, may limit flexibility and increase business risks.

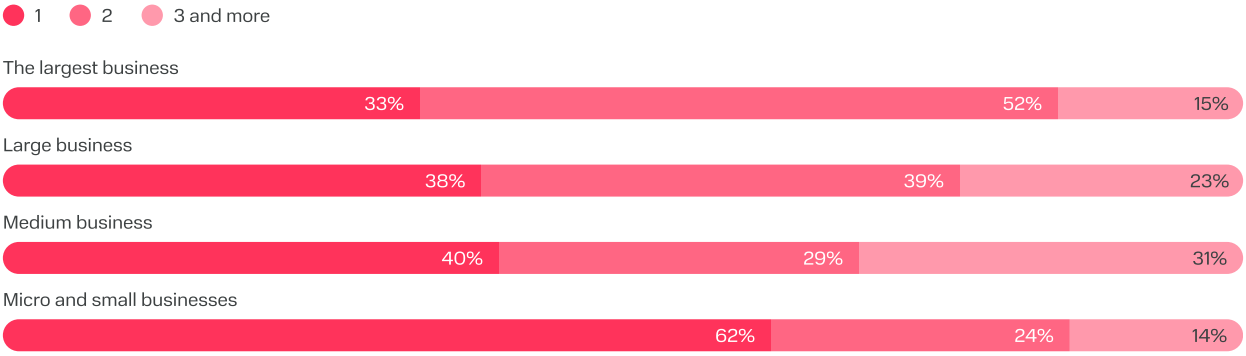
28% of companies use two providers, implementing elements of the multicloud approach to diversify risks, increase fault tolerance and access unique services from different platforms. 17% use three or more providers, which already reflects the more mature multicloud distributed architecture typical for organizations with advanced IT infrastructure. The segment of industries using the largest number of providers includes IT, finance and insurance, retail, industry and HoReCa.

Thus, the data obtained captures a multi-layered approach to cloud management and confirms that multi-cloud strategies are more common among technologically advanced companies interested in balancing fault tolerance, access to different services, and control over infrastructure.

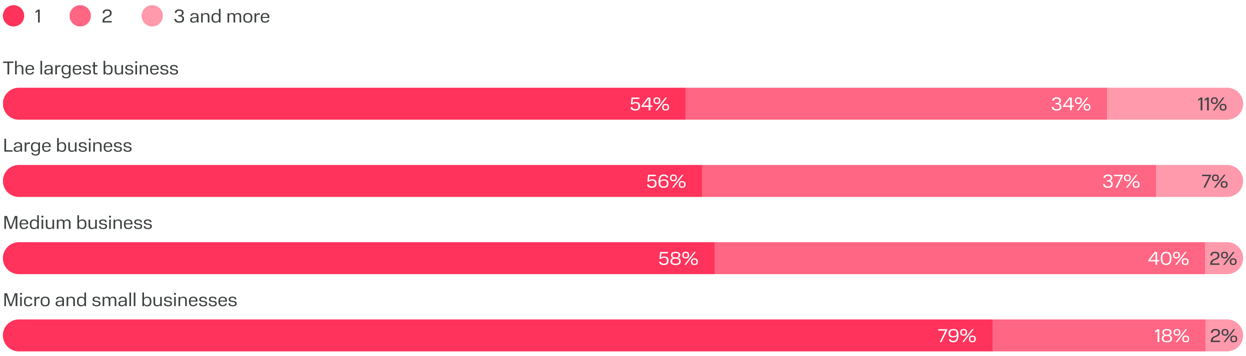
A similar situation is observed in the Private Cloud segment. For the majority of companies (72%), the choice of a single provider is typical, which ensures unified infrastructure management, SLA unification, and simplified solution support. This strategy allows us to focus on coordinating security requirements and regulatory aspects with one supplier, but at the same time increases dependence on the chosen partner.

23% of companies work with two providers, which may indicate a desire to minimize operational and technical risks, as well as take advantage of different technology stacks for different tasks. At the same time, multicloud in Private Cloud is more often motivated by reserving critical services and increasing fault tolerance.

Number of Public Cloud providers used by business segment



Number of Private Cloud providers used by business segment



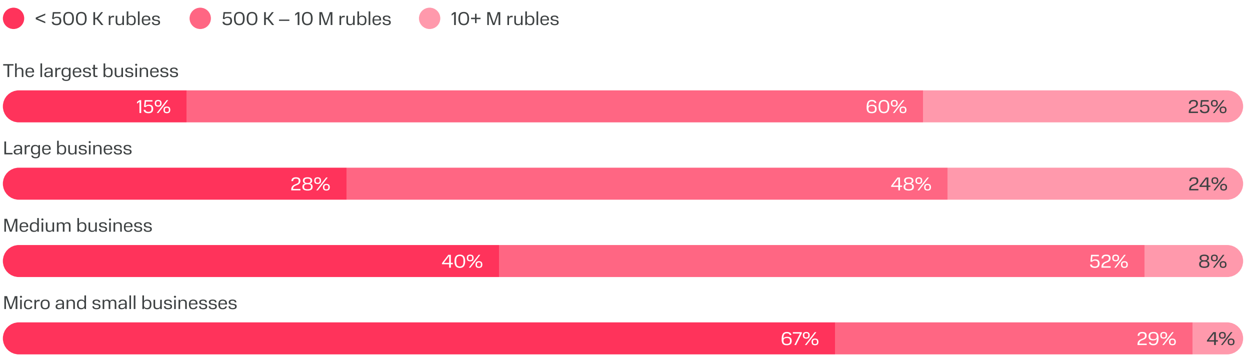
The data clearly demonstrates that the size of a business directly affects the application of the multicloud approach. Large companies are more likely to use products and services from multiple cloud providers. All companies except micro and small businesses are characterized by the active use of multiple public clouds: on average, 61% already work with two or more providers, and about 20% of medium and large businesses use the infrastructure of three or more suppliers. This indicates the high maturity of their cloud strategies. As a rule, such companies distribute tasks between providers by functional zones: some are used for data storage, others for analytics and AI, CI/CD or backup. This solution provides flexibility, fault tolerance, and supports business continuity.

At the same time, the business consciously reduces vendor lock-in risks by avoiding dependence on a single supplier. Multicloud enables load balancing, cost-based platform selection, and faster adoption of new technologies by SLAn. For these companies, multicloud is no longer just an element of infrastructure, but a tool for risk management, technological independence, and accelerating digital innovation.

The study confirmed a direct relationship between the size of a business and the scale of investments in cloud technologies. For micro and small businesses (revenue < 800 M rubles), minimal expenses are typical: about 67% spend less than 100 K rubles on clouds. This is due to both the scale of operations and the complexity of the structure, as well as the need to ensure fault tolerance, security, and work with big data. Large companies are building multi-cloud architectures, developing analytics, automation and High Performance Computing, and more often creating their own digital products, which requires significant investments and the introduction of container and AI services.

Small businesses, on the other hand, are limited to basic IT needs — virtual servers, storages, and SaaS for accounting and paperwork, which keeps costs low. In general, budgets of up to 2 M rubles are most typical for the market, reflecting moderate maturity and significant differentiation of needs.

Annual cloud costs by business segment



> The Russian cloud technology market is clearly shifting towards larger budgets, reflecting the growing maturity and strategic importance of cloud infrastructures for businesses. The corporate market is moving from a phase of point-to-point pilot implementations to a system transformation involving key processes and services. This means that there is a growing demand for integrated platforms capable of supporting complex multi-cloud and hybrid scenarios, providing fault tolerance at the level of business-critical applications, and offering transparent billing management mechanisms.

Polina Lee
Head of MWS Intelligence Team

Annual cloud costs by industry

	< 500 K	500 K – 10 M	10+ M
IT	32%	44%	24%
Finance and Insurance	40%	48%	12%
Retail	50%	39%	11%
Entertainment and Media	44%	46%	10%
HoReCa	53%	37%	10%
Science and education	44%	48%	10%
Construction and real estate	59%	34%	7%
Transportation and logistics	53%	41%	6%
Professional services	76%	19%	5%
Healthcare	74%	22%	4%
Mining and processing of minerals	49%	48%	3%
Industry	69%	30%	2%

The distribution of annual cloud costs by industry makes it possible to assess the maturity of cloud technology adoption and identify differences in the strategic approach between sectors. A significant part of the companies is still concentrated in the segment of minimum expenses — up to 500 K rubles per year. This is typical for industries such as professional services and healthcare, where clouds are used pointwise and do not become the core of the business model.

The industries where more than 10% of companies already spend over 10 M rubles a year demonstrate the greatest maturity: IT, finance and insurance, HoReCa, science and education. They are characterized by multicloud architectures, DevOps, and the use of clouds in mission-critical processes.

There are already companies with high cloud budgets in all industries, reflecting the differentiation that has begun: technology leaders are building complex consumption models, while most remain at the basic level. In the future, we can expect an increase in the share of large costs against the background of increased trust in the clouds, the development of our own expertise and adaptation to regulatory requirements.

57% of companies plan to increase their use of clouds, reflecting a moderate pace of deepening strategies, partly due to the saturation achieved and existing barriers. At the same time, 31% of respondents intend to develop private clouds, which confirms the growing demand for data control and compliance with localization and security requirements. Private solutions are increasingly becoming the core of hybrid strategies, complementing or replacing On-Premise infrastructure.

Public clouds are also in demand: 39% of companies plan to increase their use, considering them as a tool to reduce costs, accelerate digital projects and scale flexibly.

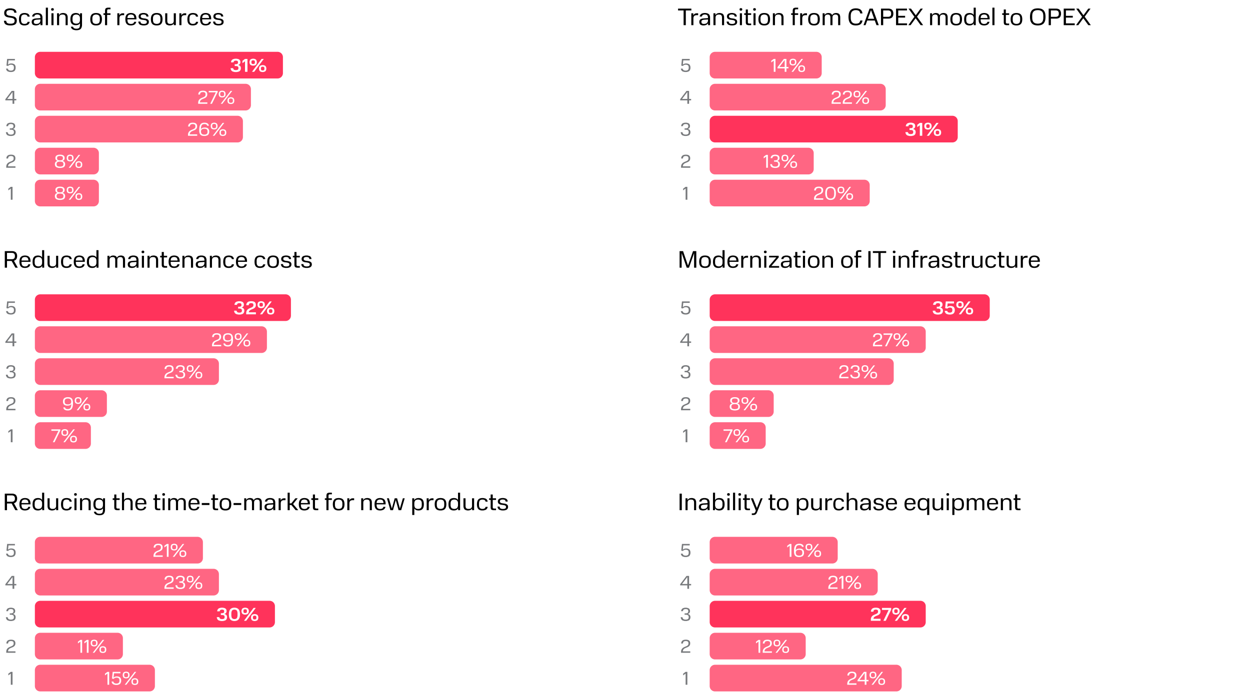
Thus, companies are building balanced approaches: with a priority on private for risk management and compliance, but with continued interest in public for optimization and rapid launch of initiatives, which supports the growth of hybrid and multi-cloud models.

> “ IT modernization, operational efficiency and strategic sustainability remain the key drivers of the transition to the cloud. Cloud solutions allow you to launch innovations without major investments, automate infrastructure, optimize costs, and adapt faster to external challenges. Together, these factors form a stable motivation for migration, with infrastructure modernization being the main reason for such projects.

Galina Gaydarhzhi
Business Analyst of MWS Cloud

Key factors in deciding whether to migrate to the cloud

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

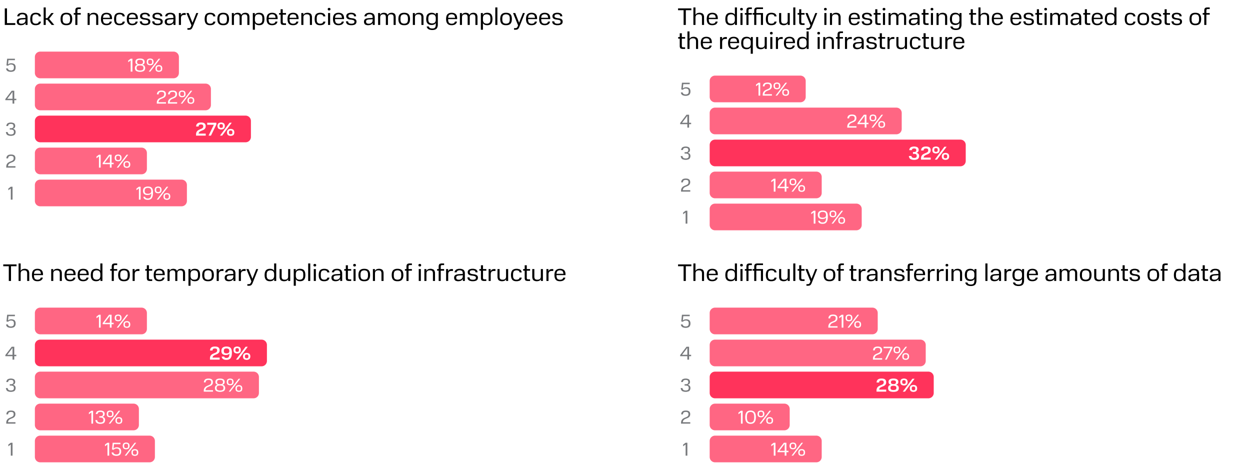


None of the barriers received the prevailing maximum ratings, which indicates that there are tools on the market to mitigate them. However, a number of problems remain relevant: technological, organizational, personnel and financial. Most often, companies note the difficulty of predicting cloud costs: almost 70% gave this barrier 3 points or higher, which indicates a lack of transparency and mature FinOps practices.

The additional costs of migration remain significant — temporary doubling of resources, payment for services and licenses, process adaptation, as well as the need to maintain local and cloud infrastructures in parallel, which increases the burden on budgets and teams.

Difficulties in the process of migration to the cloud [1/2]

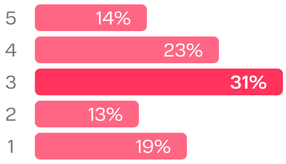
The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum



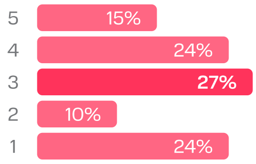
Difficulties in the process of migration to the cloud [2/2]

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

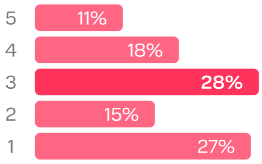
Additional costs at the stage of transferring systems to the Cloud



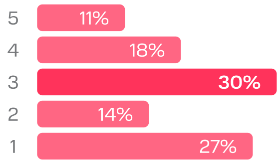
Inability to integrate used local solutions into the Cloud (outdated Software/Hardware)



Lack of vendor support during the migration process



Lack of migration roadmap



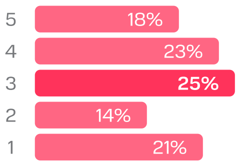
According to the survey, the additional costs of migrating to the cloud are not perceived by companies as a critical barrier, which indicates the maturity of the market and the willingness to include such costs in budgets. The cost of deploying test circuits is most often mentioned: 31% consider them of medium importance, while more than 56% consider them significant, reflecting the norm of pilot launches to reduce risks. Spending on upgrading the local infrastructure to prepare for integration with the clouds is of comparable importance.

This confirms that companies are increasingly planning budgets for pilots and On-Premise upgrades in advance, perceiving them as a natural part of migration rather than unplanned expenses.

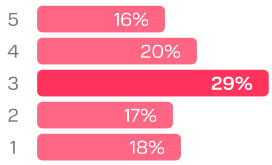
Additional costs during migration to the cloud

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

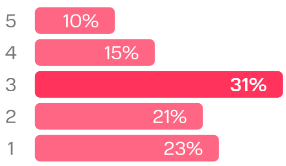
Retraining / hiring employees for high-quality work with the Cloud



Updating the local infrastructure



Deploying a test loop to verify the operability of the solution in question



Among the risks, companies attach the greatest importance to the threats of personal data leakage, trade secrets, cyber attacks and supplier withdrawal from the market. Information security issues are particularly acute for users of multi-cloud and hybrid models, which highlights the role of data protection in the design of such architectures. Banks show the greatest sensitivity.

The risk of the inability to upgrade equipment due to the departure of vendors or sanctions is highlighted separately: opinions are divided here, but for the hotel and restaurant business and industry this risk has become critical (40% gave the maximum rating), which underlines their vulnerability.

Budget overruns on clouds are less relevant for Russian companies (19%) compared to 69% worldwide, which is due to the lower prevalence of multi-cloud. As a result, companies are most focused on quality control and supply sustainability, while financial risks and incomplete services are seen more as manageable barriers.

Risks of migrating to the cloud

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

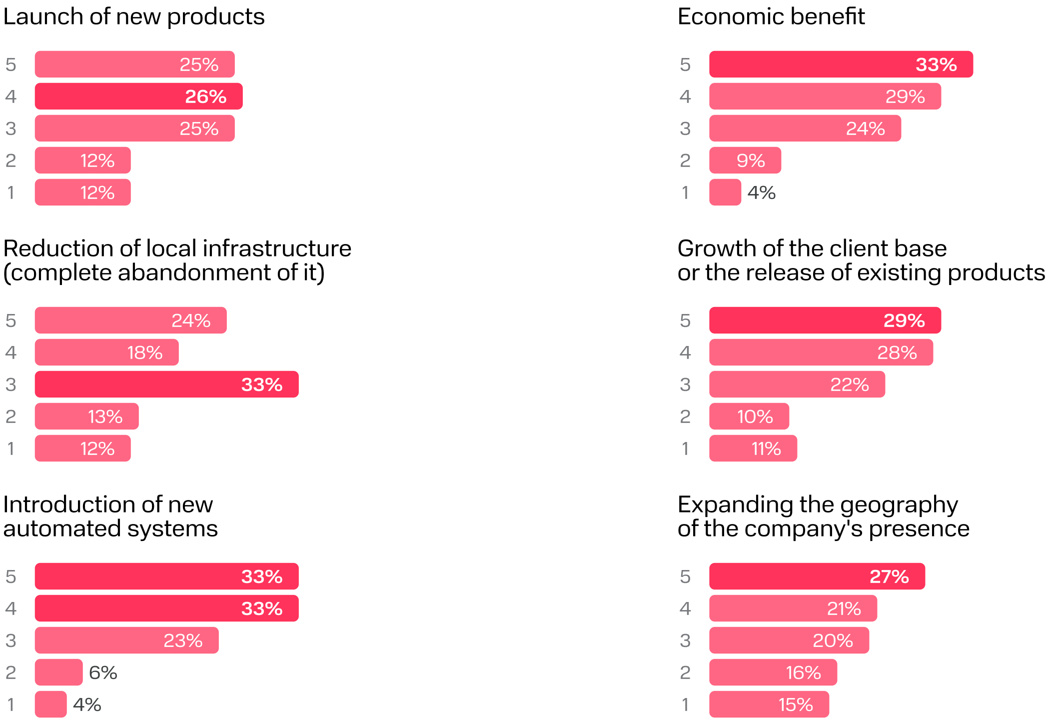
Cloud scaling decisions are increasingly being made not only for technical reasons, but also as part of a growth and digital transformation strategy. The main motivators were economic feasibility and the introduction of new automated systems — both factors were of maximum importance for 33% of companies. This confirms that clouds are increasingly being viewed as a tool for cost optimization, flexibility, and accelerated business model restructuring.

A similar trend is observed in the reduction of local infrastructure: 33% rated it at an average level, and another 40% assigned a high priority. This indicates a trend away from On-Premise in favor of clouds to reduce CAPEX and move to more manageable NUT models.

As a result, companies are increasingly using clouds as a means of strategic restructuring, which supports the growth of their share in IT budgets and shifts the focus from technical to business drivers.

Key factors when deciding to scale cloud consumption

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

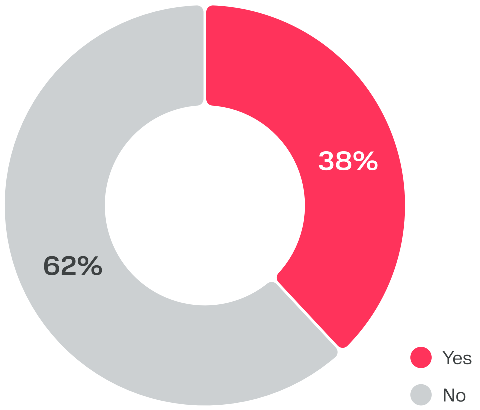


> The cloud technology market in Russia demonstrates a progressive transition from local IT initiatives to a strategic rethinking of business models. For most companies, cloud solutions are becoming not just a tool to optimize costs and accelerate the implementation of digital projects, but also a key element in increasing the sustainability and adaptability of the business. The predominance of private clouds is noticeable, reflecting the increasing demands for data control and compliance with industry and regulatory standards. At the same time, public clouds continue to play an important role in hybrid architectures, allowing companies to flexibly scale resources and quickly launch new initiatives without significant capital investments.

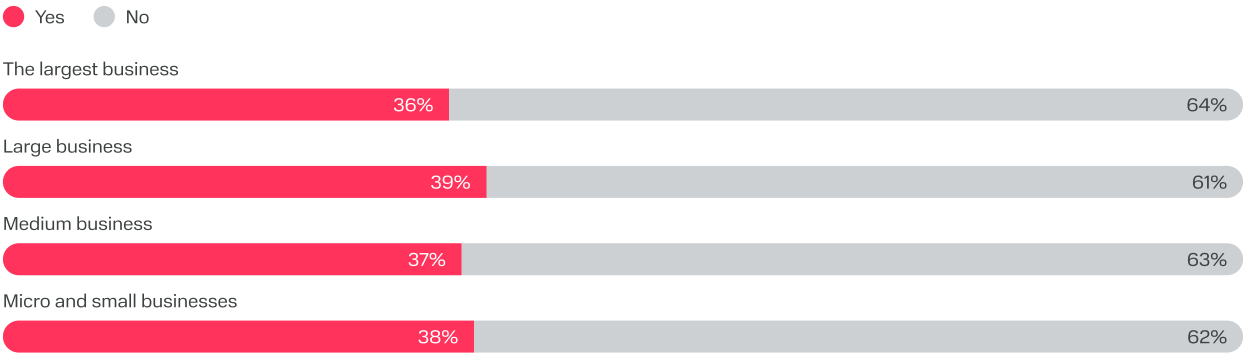
Danila Egorov
MWS Cloud Director of Business Strategy

Over the past few years, the problem of a shortage of qualified personnel has been actively discussed, but in the field of cloud technologies, more than 62% of companies have no problems hiring experts. The availability of hiring problems does not depend on the size of companies, which indicates a general shortage of specialists, regardless of the level of competence and salary. There is also little differentiation among industries in this indicator. Science, education, and industry are experiencing slightly greater difficulties.

Problems in hiring experts in the field of cloud technologies



Problems in hiring experts in the field of cloud technologies by segment



The issue of expertise is directly related to the prevalence of application software using the SaaS model. The share of SaaS solutions consuming remains low, at the level of 21–34%, depending on the business segment. Moreover, in medium and large businesses, these indicators are even lower than in small ones. This probably reflects a wariness of SaaS due to security, functionality limitations, and supplier lock-in. Instead, companies prefer to develop their own cloud environments or use IaaS/PaaS as more flexible platforms.

Thus, SaaS remains a point-to-point solution rather than a mass standard. Due to the lack of internal expertise, companies are actively using professional services. More than half of the respondents use technical support, 40% use staff training, and a third use outsourcing. This highlights that the cloud solutions market is developing not only through the sale of resources, but also through related services that accompany the entire migration cycle.

Professional services used by companies to develop cloud technologies

53% Technical support	40% Training
33% Outsourcing	19% Consulting (strategy)
11% Don’t use	

EXPANDING THE CAPABILITIES OF YOUR INFRASTRUCTURE

MWS CONTAINER PLATFORM

A reliable platform for the development and operation of container applications. It helps to innovate faster, carry out digital transformation and launch IT products.

by 40%
reduces the burden on IT teams

by 70%
accelerates the release of new applications and simplifies their operation

by 80%
automates manual operations

AI-CLOUD

Infrastructure and services for the implementation of AI technologies in business. The AI cloud effectively accelerates digital transformation and optimizes business processes

by 20%
Increased profits through more accurate strategic decisions using AI in data analysis

20–45%
improving the productivity of the development department when using code generation systems

by 60%
less time to process customer requests

MWS CLOUD PLATFORM

Reduce Time-to-Market and Improve Hybrid Infrastructure Capabilities

by 40%
Reducing infrastructure costs

by 50%
Time-to-Market acceleration

by 80%
reducing the likelihood of successful attacks due to cybersecurity systems

TECHNOLOGY INTRODUCTION: CLOUD

In this technology study, in addition to the overall assessment, which includes budgets, strategy, expertise, drivers, and barriers to implementation, it is critically important to additionally assess the consumption of relevant technology products.

For the transparency of the accumulated study results, the subsequent analysis is factual, without additional integral calculations. The conclusions and insights that accompany the data obtained in the framework of the study can be independently analyzed by the user of this report, since the indicators reflect the direct responses of the respondents. Thus, this block is an applied tool for making decisions about the consumption of the studied technologies.

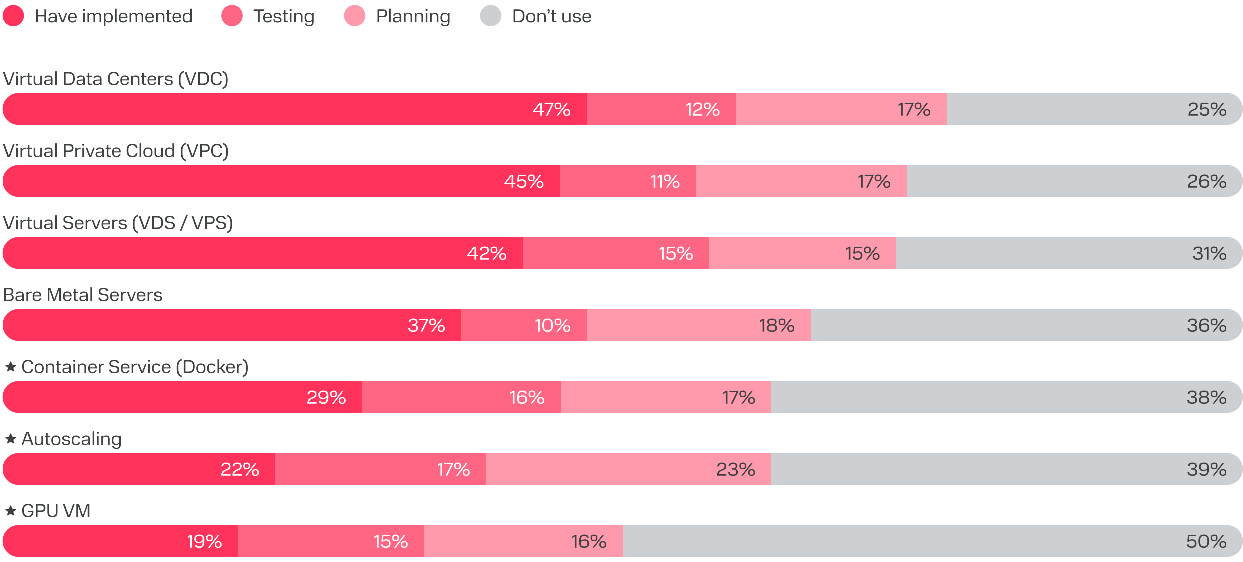
To evaluate among the obtained subcategories those products that have an increased growth potential, an approach called the "Formula for the growth potential of subcategories" was introduced. This formula is a comparison: on the one hand, the parameter "implemented", on the other hand, the sum of the parameters "testing" and "planning". Unlike the "don’t use" parameter, these values positively characterize the respondents' plans, which can be interpreted as a likely transition to the "implemented" status in the near future.

Have implemented < Testing + Planning = There is potential

Have implemented > Testing + Planning = Potential exhausted

The Product solutions section demonstrates classic product categories that belong to the segments Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Clouds are the foundation for complementary technologies, in particular for cybersecurity and artificial intelligence. Consequently, the high level of cloud development and consumption simplifies the process of testing and integrating more specialized technologies.

Computing



The most commonly used product subcategories are expected to be virtual data centers (VDC) and virtual private clouds (VPC), 47% and 45% of implementations, respectively. These solutions are a commodity for a significant number of companies from the survey of respondents, which correlates with open market data on consumption. Computing, along with other product categories in the IaaS segment, traditionally occupies the largest share in the revenue structure of cloud providers.

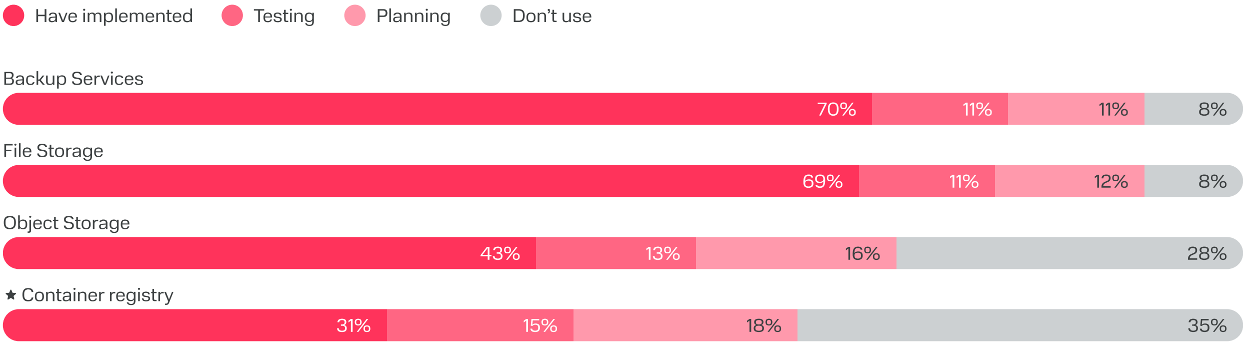
The analysis also supports the current thesis on the market about the high demand for both public and private installations. The largest cloud providers are actively responding to this trend by developing hybrid solutions.

Separately, we would like to draw attention to the product subcategory of container services (Docker), which are fully implemented by only a third of the surveyed companies, but also a third of users are already testing (16%), or have planned (17%) integration.

Despite the high relevance and widespread mention of AI technologies, the product subcategory related to computing for working with AI (GPU VM) is actually used by a relatively small number of companies surveyed. This is due to the fact that most corporate users work with AI tools at the assistant and business application levels. There is a high demand for GPUs, but this demand is supported by a limited number of customers interested in high-performance computing and often with their own AI development team. Only 31% of the companies surveyed have such a team. The active consumption of infrastructure solutions for AI tasks is not equally significant for different industries and market segments.

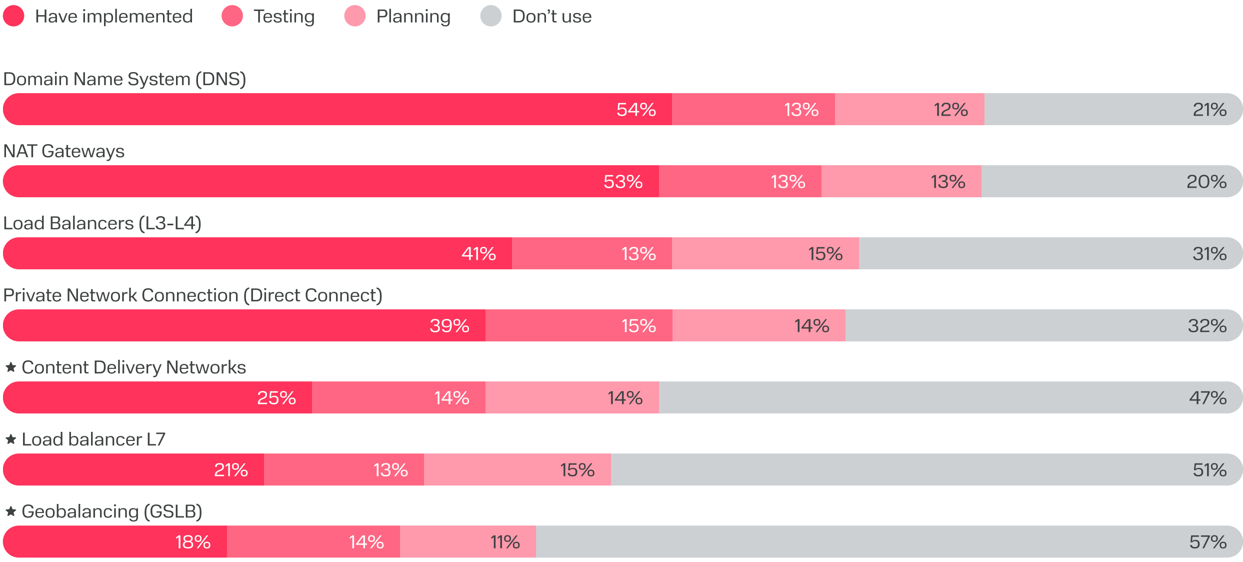
★ — high potential

Storage



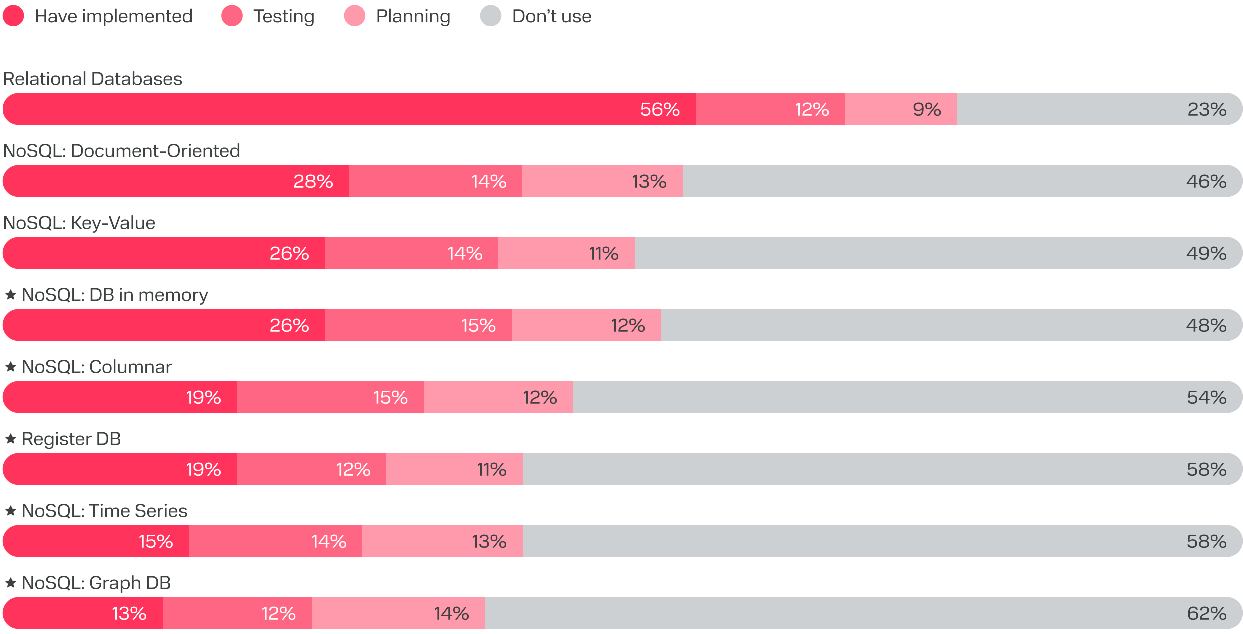
Storage is the basic product category for the vast majority of companies in the market. It can be unequivocally assessed that backup products, file storage, and virtual machine disks have become a commodity for the vast majority of corporate clients in Russia. There is a significant gap in the level of consumption between solutions that ensure the fulfillment of everyday tasks and specialized product subcategories — the level of consumption may differ by more than 2 times. But at the same time, object storages and container registries have high growth reserves: companies often note that they plan to use or test these products.

Network and Content Delivery



Often, companies that switch to the cloud do not customize individual network parameters, but use a comprehensive solution with standard settings. Private setup using individual products in this category is required for geographically distributed companies, for example, with a wide branch network. Such companies are often representatives of large and large businesses, for which the use of network products with fine-tuning is a standard scenario for cloud consumption. The use of these products is most typical for the IT and transport sectors.

Databases



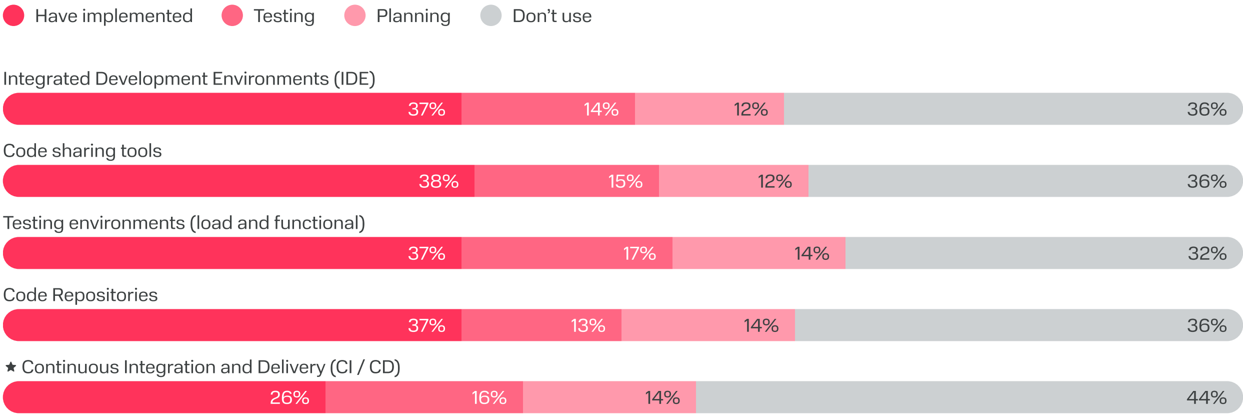
Databases are the most popular product category in the PaaS segment. Relational databases are expected to be the most implemented class of products among the analyzed ones, which is explained by their native application for most business application development scenarios. The second subcategory in terms of usage frequency is NoSQL databases (28% of implementations or 55% of positive responses combined), reflecting the growing interest in flexible, horizontally scalable solutions. At the same time, SQL remains the type of databases that the vast majority of companies have implemented or are considering implementing. This may reflect the difficulty of supporting new database formats and the lack of use cases for alternative solutions.

> “ The cloud market in Russia demonstrates high maturity in basic infrastructure solutions — virtual data centers, VPC and storage have become virtually the standard for most companies. At the same time, container services and AI infrastructure still cover a smaller part of the market, but they have significant growth potential: a third of companies have already implemented them, and a comparable proportion is testing or planning integration. Significant prospects are also visible for object storage and services around the management of containerized applications. This sets a double focus for further development: strengthening positions in mass IaaS solutions and parallel expansion of offerings for more advanced architectures and industry-specific cases.

Mikhail Tutaev
Director of MWS Cloud Products

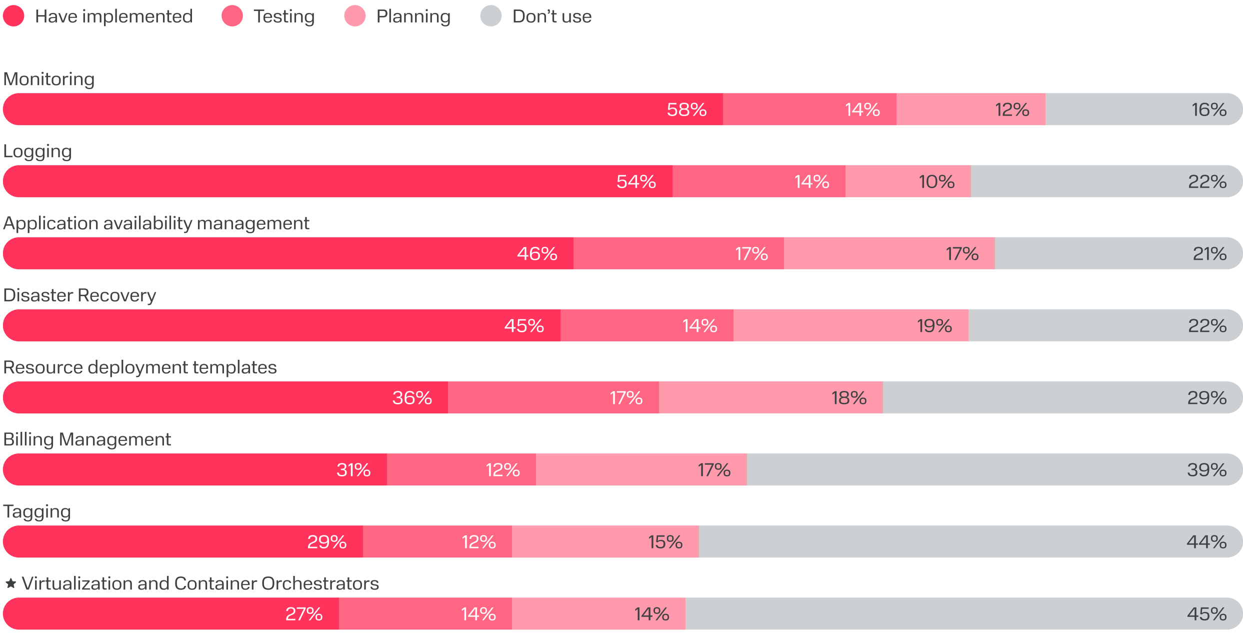
★ — high potential

Development Tools



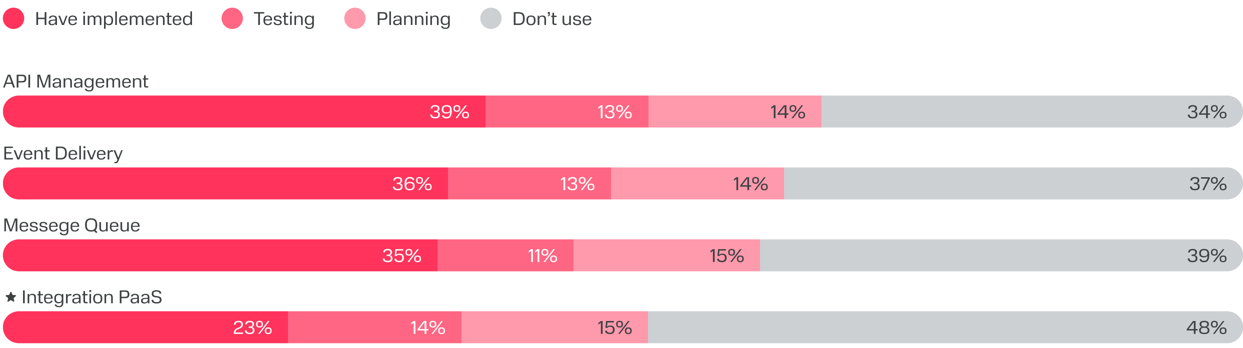
Development tools are one of the basic subcategories of the PaaS segment. The average values for the studied parameters are associated with the fact that these products are often integral components of the platform and are not isolated into separate products. The growth potential, which is reflected in the high values of testing and implementation planning (about 28% in total for the products under consideration), correlates with the growth rate of the platform solutions market in Russia. Continuous integration and content delivery (CI/CD) requires a high level of maturity of the development teams. Respondents from the survey of the studied companies noted this category less often than others.

Management Tools



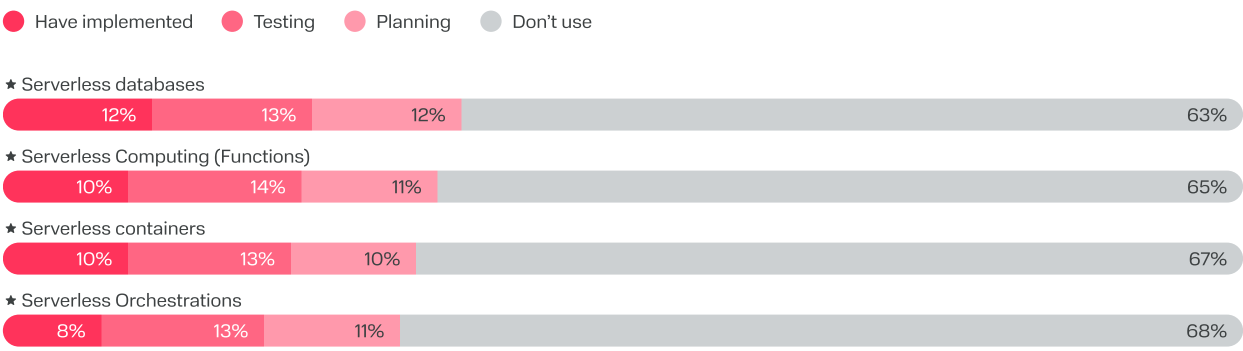
Product subcategories related to management tools are also, in a significant proportion of cases, an integral feature or functionality of the cloud provider's platform. However, unlike the Development Tools category, the survey respondents were significantly more likely to respond positively to these product subcategories. This illustrates the basic nature of the listed solutions for cloud clients. The particular importance of using these components can be observed in companies of large and large businesses, for which the stability of the infrastructure is of critical importance. The use of Disaster Recovery solutions additionally characterizes the maturity of companies' IT risk management.

Integration



These solutions are usually the basic components of the platforms. Comprehensive integration solutions are essential for large companies with a multi-layered enterprise architecture that implements complex integration scenarios and changes to business architecture, data architecture, application architecture, and technology stack. Advanced integration platform solutions, including those that support the transition from monolithic to component and microservice architectures. The diversity and maturity of integration products directly affects the technology contract between the supplier and the consumer, which ultimately affects availability, response time, bandwidth, and security-related constraints.

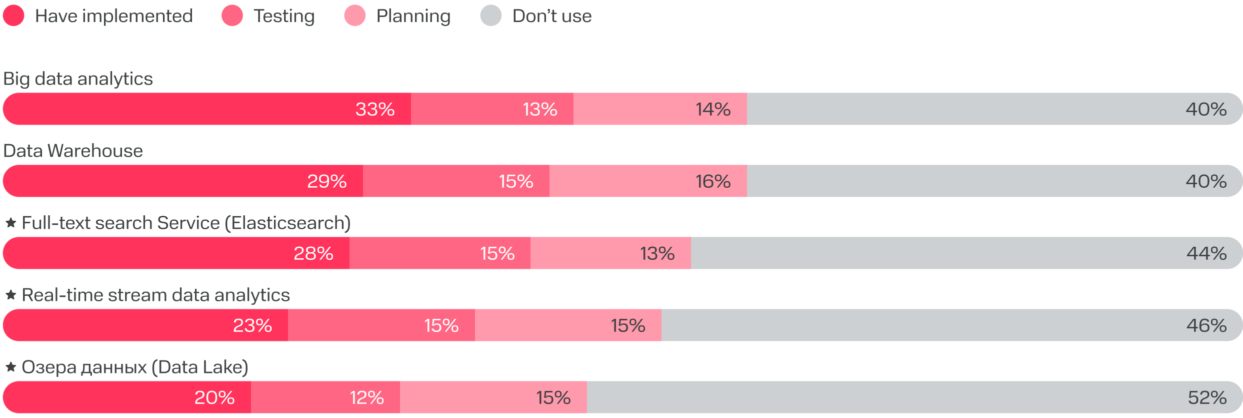
Serverless



The implementation of serverless solutions remains at the initial level, which indicates a large share of legacy architectures in the technology stack of companies, as well as a lack of DevOps/ cloud native practices, especially in comparison with foreign companies. Most of the surveyed companies not only do not use, but also do not plan to implement appropriate solutions. Low activity remains even at the testing level, which may indicate a low level of user awareness of the advantages of serverless, as well as insufficient competencies of employees to implement solutions of this class. An additional reason for the low level of demand may be the lack of relevant offers from a large number of providers.

★ — high potential

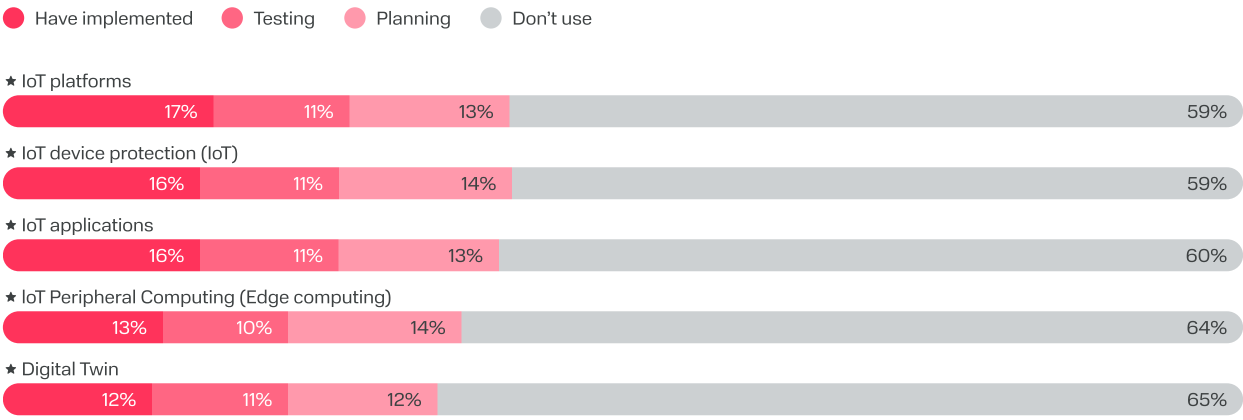
Analytics



Mature companies strive to develop a data-driven approach in their strategic activities and business operations. Difficulties in implementing this approach are often related to internal processes in companies and Data Governance methodology. However, if organizational and process barriers are overcome, then from a technological point of view, the implementation of the data-driven approach requires the availability of embedded basic IaaS and PaaS products, including those discussed earlier.

Data Warehouse is a common class of solutions, which, as a rule, begins the construction of advanced automated analytics. Solutions in the field of real-time analytics and the creation of DataLake are characterized by the predominance of companies testing and planning to use these products over those actually implementing them. These product subcategories are examples of integrations in companies with a developed approach to building analytics.

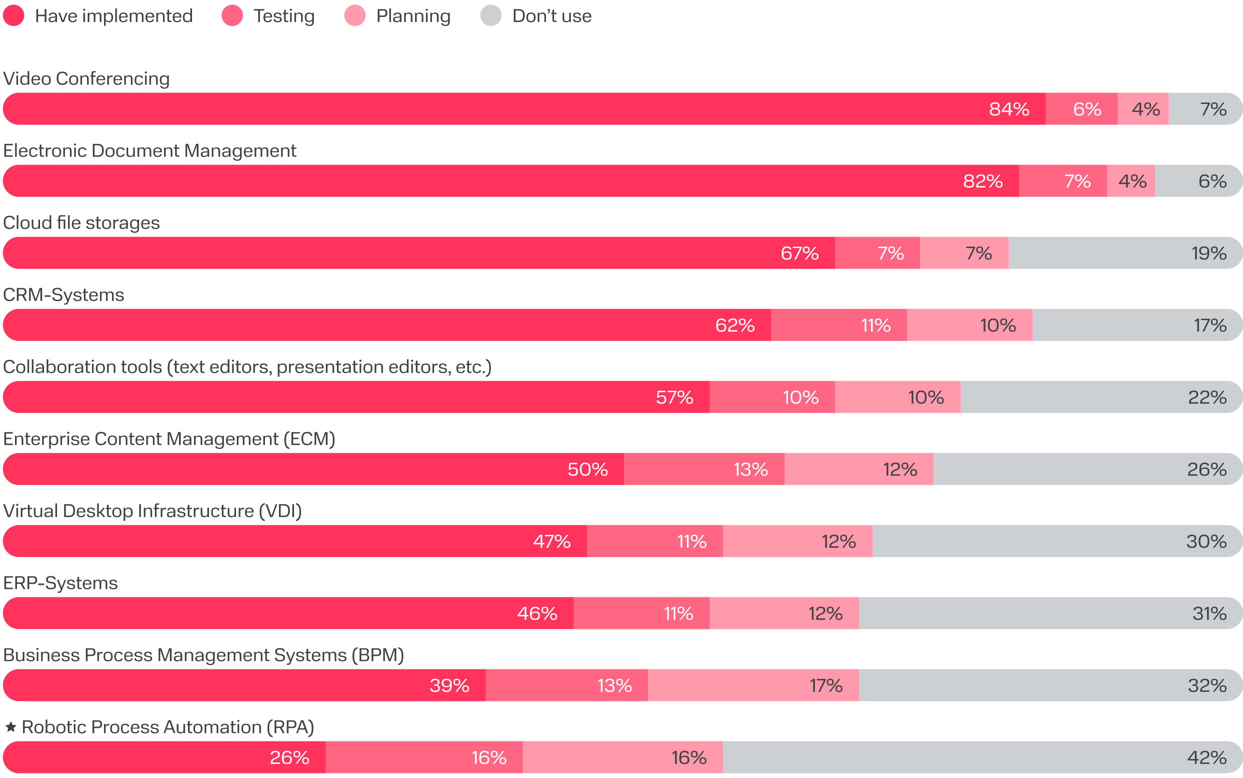
Internet of Things (IoT)



The Internet of Things is an end-to-end technology that includes software, hardware, and communication components. The implementation of solutions is impossible without at least partial use of the cloud infrastructure. According to the respondents, these practices are not widespread: in almost all areas, more than half of companies do not use IoT solutions at all, and two thirds of companies do not use the solution for digital twins. The Internet of Things remains popular mainly in industrial and logistics companies, while its maturity is extremely low in other industries.

Despite the fact that attacks on IoT systems are one of the fastest growing threat vectors, no more than 70% of companies that have implemented IoT platforms and applications use end device protection technologies. This trend may indicate a lack of device lifecycle management strategies in companies.

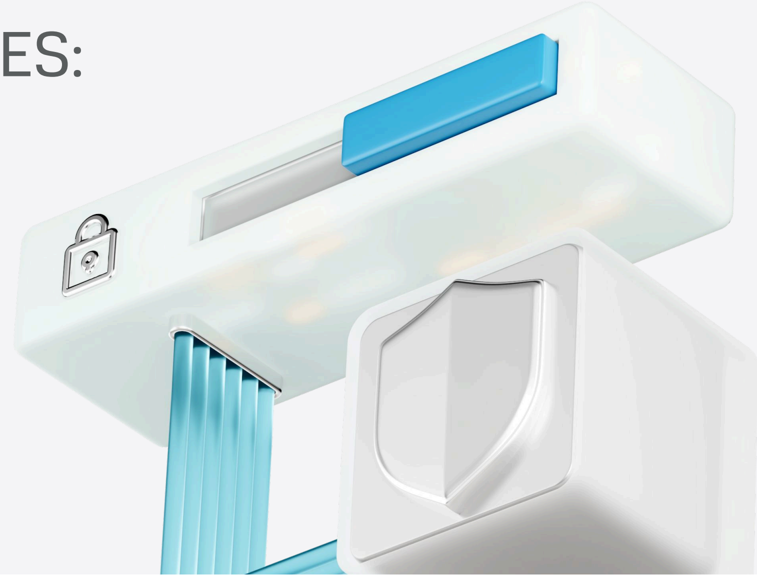
Business Applications



Business applications that belong to the SaaS segment are widespread, in high demand, and have begun to be native in many ways for companies. So, the vast majority of respondents in our survey scope have already noted the introduction of video conferencing, EDF, file storage, CRM systems and integrated collaboration tools, which usually include a wide range of functionality. Separately, we would like to draw attention to 2 product subcategories that have a high observed potential for further growth: Business Process Management Systems (BPM) and Robotic Business Process Automation (RPA). The high statistics of positive responses within these segments indicates the versatility of use regardless of industry and business segment.

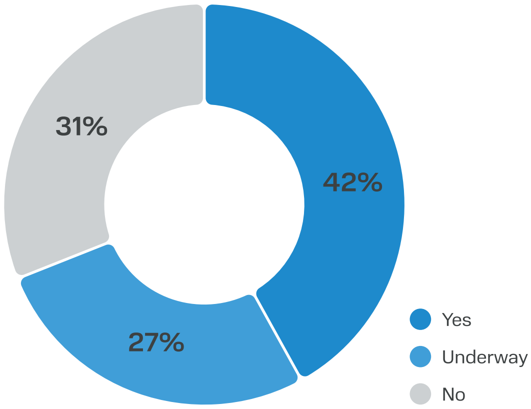
★ — high potential

TECHNOLOGICAL BUSINESS STRATEGIES: CYBERSECURITY



Information security is becoming an integral part of a sustainable digital infrastructure, necessary both for managing working processes and for effective work with big data and AI. According to the survey, 42% of companies already have a CS strategy, and another 27% are at the stage of developing it. This confirms that a systematic approach to vulnerability analysis and risk management is becoming more widespread. The focus is shifting towards broader systemic CS management in all segments, reflecting a market-wide focus on minimizing cyber risks and preparing the base for subsequent investment stages in digitalization.

Having a strategy for implementing CS

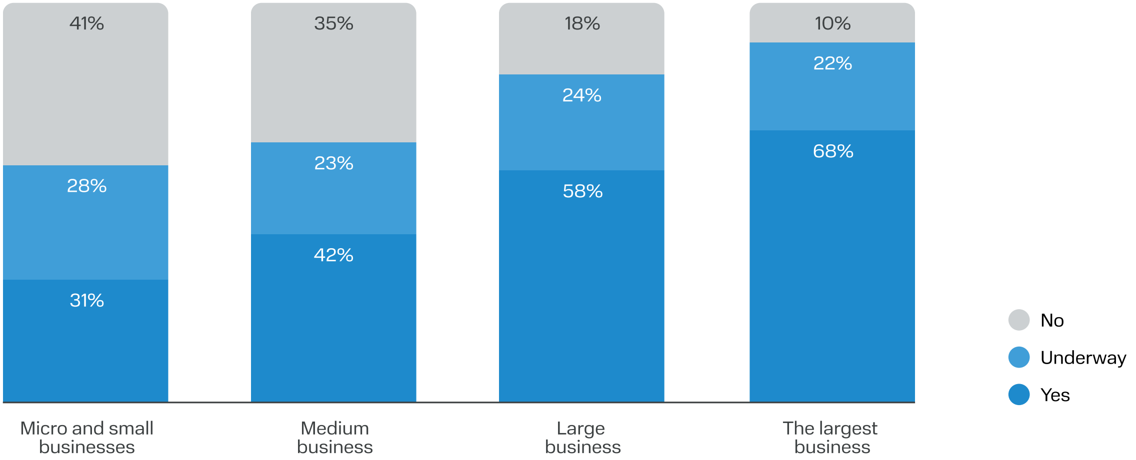


> “ Today, the market for cloud solutions for cybersecurity is demonstrating a qualitative shift — information security is no longer a local task of individual departments and is becoming the foundation of a sustainable digital ecosystem of companies. More and more organizations are approaching CS issues strategically, building systemic risk and vulnerability management models. This trend reflects the maturity of the market and the willingness of businesses to invest in long-term tools that ensure the reliability of big data processing and the implementing AI.

Mikhail Tutaev
Director of MWS Cloud Products

The dependence of the maturity level of CS strategies on the scale of the business can be traced quite clearly. Among the largest companies (with revenue > 15 bn rubles), a CS strategy is formed only in 68% of cases, while for enterprises with revenue < 800 M rubles, this figure is only 31%. At the same time, the development of CS strategies is almost equally typical for small and medium-sized companies. For them, this largely reflects the process of catching up and closing current vulnerabilities. At the same time, large companies often already have a targeted CS architecture, which reduces the proportion of those who are precisely at the stage of developing a strategy.

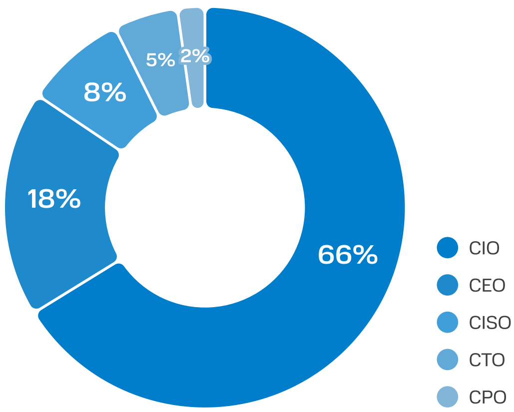
Strategy for implementing CS by segment



The greatest influence on decision-making in the field of information security, as in the case of cloud technologies, belongs to XU, the head of the IT department. He was named a key decision maker (KDM) by 66% of the companies surveyed. This confirms the continuing bias towards the IT domain, when the management of the CS is perceived primarily as the area of responsibility of the technical unit.

For most companies, the implementing information security tools process is quite fast: for 73%, it takes no more than six months. The most common period is from one to three months (31%), followed by a period of 3–6 months (24%).

Key employees (KDM) in the decision-making process on the implementating CS



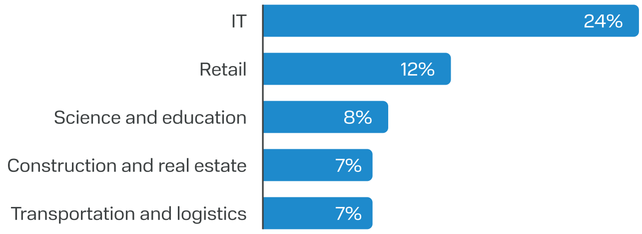
Such results demonstrate that for a significant part of the business, CS projects are implemented in a fairly short time, which may indicate either the typical nature of the solutions being implemented, or a high degree of their readiness for rapid integration into the existing infrastructure. The share of companies with CS projects lasting more than a year is only 14%, which underlines their exclusivity and probably indicates large-scale or specialized initiatives in large organizations.

The number of cyber attacks increased by 30% in 2025

The urgency of implementing security measures is determined not only by regulatory requirements. 35% of respondents experienced DDoS attacks in 2024.

At the same time, there is a direct relationship: the larger the company, the higher the probability of such an attack. Among large companies, about 50% were subjected to DDoS attacks, while among the respondents of the largest businesses, this figure reaches 60%.

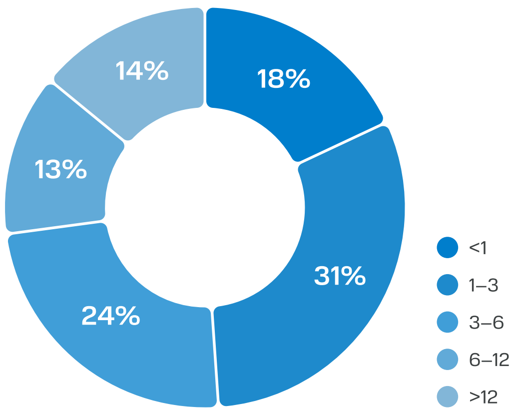
DDoS attacks in 2024 by industry



In 2025, an increase in cyber attacks was recorded by more than 25%. Cyber attacks on transport and industrial companies, as well as companies in the retail sector, have become the most widespread cases. Thus, one of the largest attacks on a telecom operator led to the disabling of key network elements and access restrictions for customers from 4 regions of the Russian Federation. Another attack was carried out on one of the major players in the industrial sector. The attackers hacked into internal services and restricted access to data. As a result, operational processes were stopped and logistics chains disrupted. The consequences of cyber attacks are not only disruption of business processes and compromise of enterprise data, but also additional checks by regulators, as well as the risks of criminal prosecution of top managers in the event of violations of the operation of information storage, processing or transmission facilities. According to the survey, industry specifics significantly influence the frequency of attacks: companies in the IT, retail, and scientific sectors were most frequently subjected to DDoS attacks. These data indicate that DDoS attacks remain a pressing threat to businesses, particularly large companies and certain industries. This highlights the importance of implementing effective cybersecurity measures to protect against such attacks.

The deployment of information security tools is most common in its own infrastructure: 43% of respondents use On-Premise solutions. This is due to the need for full control over the system and data, especially in the face of growing demands for confidentiality and compliance with regulatory standards. The hybrid cloud (32%) taked the second place, which more often allows you to maintain a balance between cost-effectiveness and reliability, including by processing sensitive data, including trade secrets and personal data of clients. This choice gives companies the opportunity to combine the advantages of cloud technologies with secure access management and data segmentation.

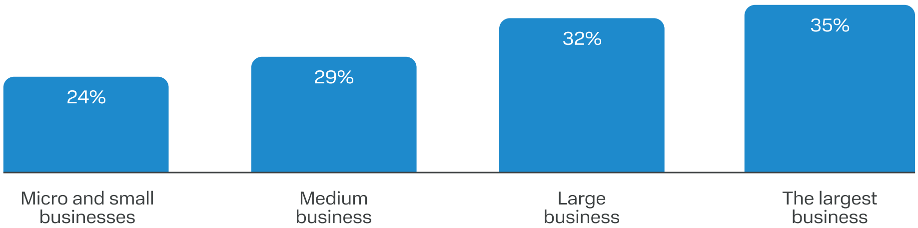
Duration of the implementing CS tools process in months



The share of using private and local solutions is increasing as the business size increases: among the largest companies (with revenue > 15 bn rubles) On-Premise and Private already use 50%. Large businesses are characterized by a more selective model of placing critical CS components outside of public infrastructures, which confirms the strategic priority of data protection and minimizing external risks.

Multi cyber security solutions are being developed

Share of CS tools used by companies in the cloud in business segment



As the scale of the business increases, the average share of CS tools deployed in the cloud also increases. For example, micro and small-sized business companies (with revenue < 800 M rubles) This share averages 24%, while for the largest enterprises it is already 35%. However, the vast majority of companies are characterized by a selective model of using cloud CS services: 79% of respondents have placed up to 30% of their CS tools in the cloud, which underlines the traditionally high importance of on-premises solutions for corporate security systems.

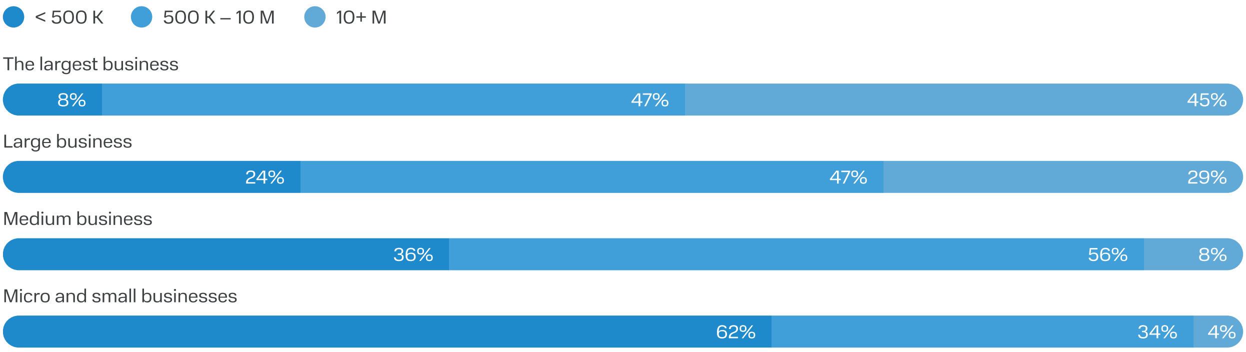
An industry breakdown shows that the leaders in terms of the share of CS tools in the cloud are IT, the entertainment and media segment, and science and education (with an average share of about 36%). This is due to the high digital maturity of these industries and the significant number of cloud services already embedded in their operational models. At the same time, transport and retail are also characterized by high values of this indicator (24–27%), reflecting the need for rapid scaling of CS tools to protect distributed infrastructure and client data.

The distribution of annual CS costs among companies of various sizes fully reflects the structure of corporate budgets. As revenue decreases, it is noticeable how the budget concentration shifts towards the lower ranges. For example, for the micro and small business segment, the main expenses are concentrated in the area of up to 500 thousand rubles, which confirms the more restrained capabilities of such companies in the field of CS and reflects the limited amount of investment in specialized tools.

The share of all CS tools used in the cloud by industry

	Average value
IT	36%
Retail	27%
Construction and real estate	19%
Transportation and logistics	24%
Professional services	23%

Annual CS costs in business segment



The greatest diversification of the ranges of annual cloud costs for information security is recorded in the IT and transportation industries. This demonstrates the extensive consumption pattern of CS solutions, from typical low-cost services for protecting communication channels and user devices to integrated incident monitoring and management systems at the infrastructure level.

The TOP 5 in terms of costs included IT, the financial sector, entertainment and media, mining and processing, and healthcare. These industries are characterized by a steady cost shift in the range of more than 10 M rubles, reflecting the mature demand for cloud CS services and the availability of regulations that require a systematic approach to protecting customer data and financial transactions.

From the point of view of risks and industry drivers, the distribution of costs looks logical: The IT industry invests in CS to protect its own platforms and customer data, finance and retail to minimize fraud threats and ensure regulatory compliance, and healthcare to protect intellectual property and clinical data. This distribution reflects not only the different levels of maturity of CS strategies, but also the specifics of the threats faced by the industry.

“

Despite the fact that on-premise installations still dominate — especially among the largest companies, where control and regulatory issues are most acute — the share of private and hybrid cloud models is growing. This reflects the business's desire to combine reliability and manageability with the scalability and flexibility of modern CS solutions. We see that the industries with high digital maturity and distributed infrastructure are showing the greatest interest in bringing CS functions to the cloud: IT, media, education, transport and retail. For such segments, cloud-based cybersecurity tools are becoming a key condition for maintaining smooth operations and protecting complex data processing chains. At the same time, the cost structure demonstrates a wide range of budgets, from basic security services to integrated incident management platforms, which confirms mature, segmented demand in the market.

Danila Egorov
MWS Cloud Director of Business Strategy

Annual CS costs by industry

	< 500 K	500 K – 10 M	10+ M
IT	33%	41%	26%
Finance and Insurance	47%	28%	25%
Entertainment and Media	27%	48%	25%
Mining and processing of minerals	43%	36%	26%
Healthcare	49%	40%	11%
Science and education	48%	44%	9%
Retail	56%	36%	8%
HoReCa	50%	45%	5%
Construction and real estate	59%	37%	4%
Industry	58%	37%	4%
Transportation and logistics	43%	53%	4%
Professional services	62%	36%	3%

Only 5% of the surveyed companies do not use the services of external providers of information security solutions, which indicates a high level of trust in specialized vendors and recognition of the importance of professional solutions in the field of data protection. At the same time, the remaining 95% of companies realize the need to integrate external solutions to ensure reliable protection of their digital infrastructures.

However, it is worth noting that some companies prefer to deploy information security tools locally. This may be due to the desire to maintain maximum control over the data and minimize the risks associated with the transfer of information to third parties. Local solutions may also be preferable for companies with high requirements for data security and confidentiality.

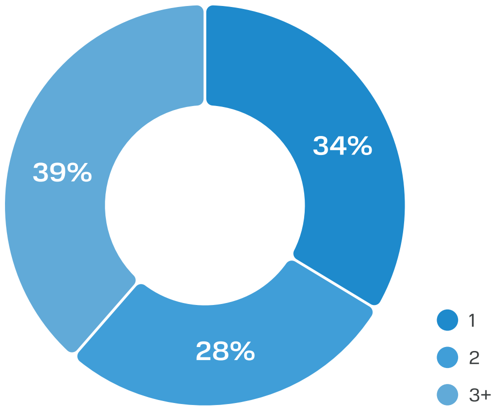
More than a third of respondents work with one vendor, which may indicate a desire to simplify management and integration of solutions, as well as trust in one trusted partner, which can be beneficial in terms of consolidating services and obtaining more favorable terms of service.

At the same time, 64% of the surveyed companies use the services of no more than two vendors. This approach allows you to combine best practices and technologies, adapting them to the specific needs of the company.

In general, these trends reflect a mature approach of companies to information security management, where the balance between the use of external resources and local solutions is determined by strategic priorities and specific business needs.

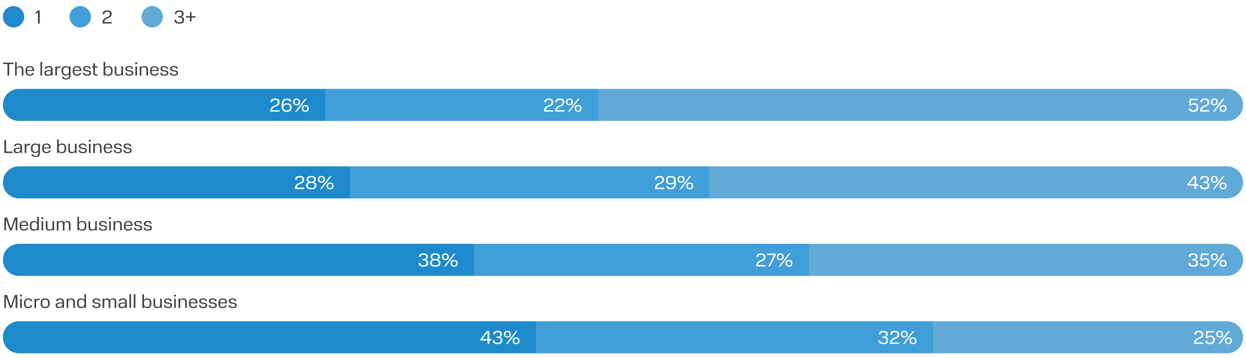
It is worth noting that large and large businesses use a large number of providers, and the number of providers increases in proportion to the size of the company.

Number of CS vendors used



> Companies are increasingly diversifying their cybersecurity risks by attracting multiple vendors

Number of CS vendors used in business segments



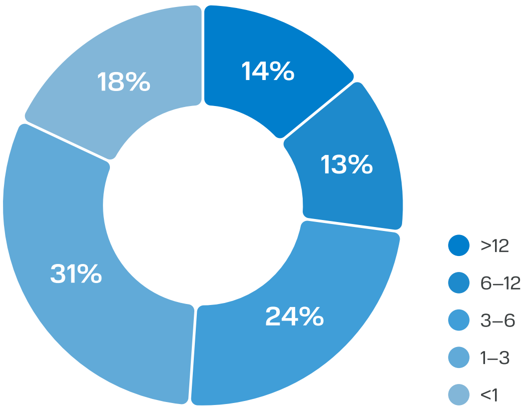
> For the Russian corporate sector, this pattern of choosing CS solutions illustrates the dominance of the "compliance-driven security" approach, where compliance with legislation and standards is the main goal. At the same time, such a strategy may deter investments in proactive cyber resilience technologies, which is important to take into account in the context of increasing complexity of cyber threats and the growing number of targeted attacks on large companies.

Polina Lee
Head of MWS Cloud Intelligence Team

For 55% of respondents, the process of implementing CS tools lasted up to six months. At the same time, most companies noted that the implementation took from 1 to 3 months. 14% of respondents stated that the process of implementing CS tools took more than a year. Long migration times can be associated with a number of factors, such as complex infrastructure, the need to integrate with multiple existing systems, or high security requirements. Companies that face longer deadlines may be undergoing large-scale upgrades or switching to more comprehensive and customized solutions, which requires significant time and resource costs.

Duration of the implementing CS tools process

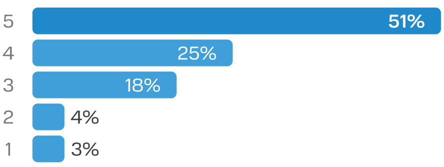
In months



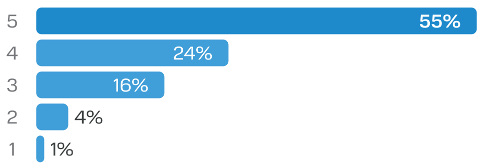
Key factors when deciding on the implementing CS tools

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

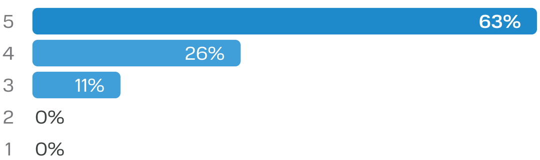
Compliance with information security legislation requirements



Ensuring the cyber resilience of the enterprise



Ensuring data protection from internal and external threats



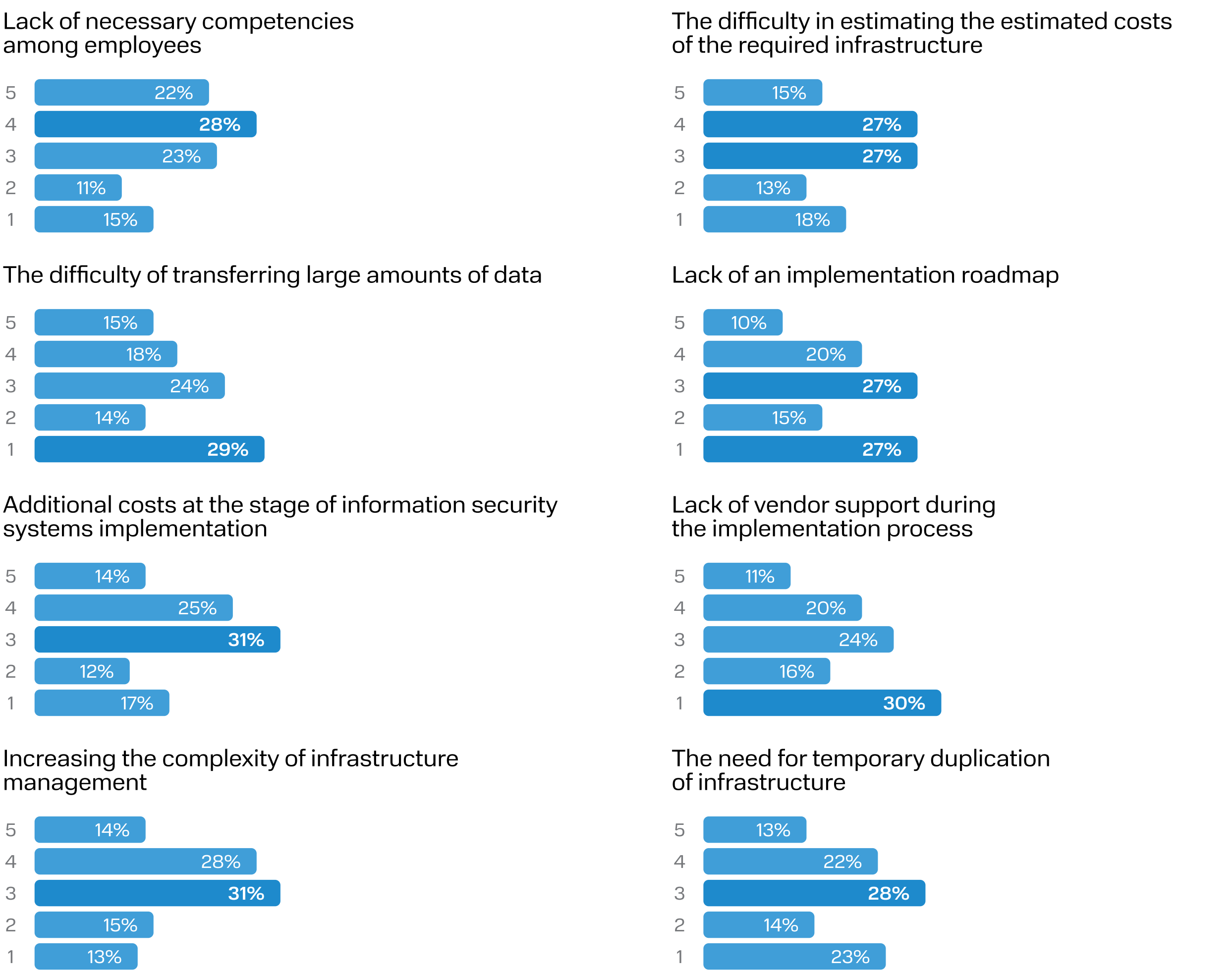
The majority of respondents consider the lack of necessary competencies among employees as the most critical factor complicating the process of implementing information security systems. This barrier consistently occupies a leading position in terms of the share of grades of 4 and 5 points, which indicates the significant role of human capital in the success of CS projects.

At the same time, factors such as the lack of vendor support during the implementation process, as well as the lack of full-fledged technical support programs for providers (ROS, Support, etc.), are evaluated much more mildly. For most companies, these difficulties have not become critical, which may indicate two trends. First, some companies prefer to develop their own competencies, minimizing external dependence and risks associated with the transfer of control over critical infrastructure. Secondly, there may be a concentration of demand for basic services that do not require deep customization or constant supplier support.

Separately, it is worth noting the factors "increasing the complexity of infrastructure management" and "additional costs during the implementation phase", which also remain sensitive factors for a significant proportion of respondents. Their comparatively high assessment of importance underscores the need for balanced budget planning and CS architecture during the transition to a more mature level of security.

Difficulties in the implementing CS tools process [1/2]

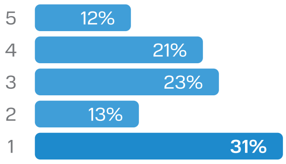
The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum



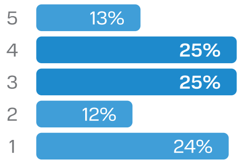
Difficulties in the implementing CS tools process [2/2]

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

Lack of technical support programs from the providers/vendors in question (ROS, Support, etc.)



Inability to integrate information security tools into used local solutions (outdated software/hardware)



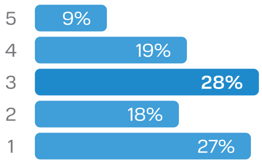
Additional costs associated with retraining or hiring employees for high-quality work with information security tools are most often mentioned by respondents and are distributed in the direction of high ratings of importance. This trend underlines that the personnel aspect continues to be one of the main items of additional costs in the framework of CS projects.

Updating the local infrastructure also occupies a prominent place in the cost structure, which logically reflects the need for technological modernization in the context of the introduction of more complex or resource-intensive CS systems.

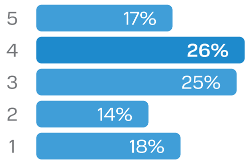
Дополнительные расходы в процессе внедрения средств КБ

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

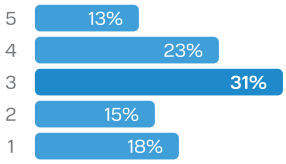
Deploying a test loop to verify the operability of the solution in question



Retraining / hiring of employees for high-quality work with information security tools



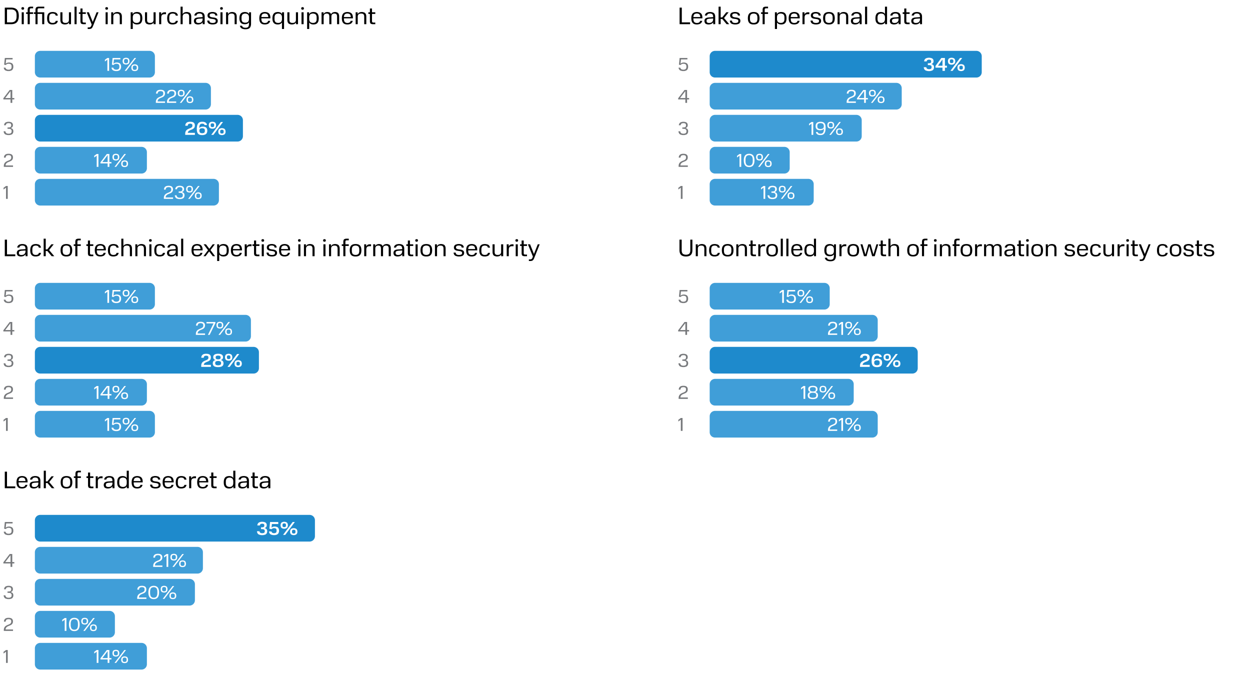
Updating the local infrastructure



Respondents are most critical of the risks associated with data leakage, both personal and trade secret data. These two risk groups collectively scored the largest share of ratings for the highest level of criticality (5): 35% of participants identified leaks of trade secrets as critical, and 34% of personal data leaks. This confirms the steady trend of increased attention to the protection of customer, partner, and confidential business information. The lack of technical expertise in information security is also perceived as an important risk, but more often receives moderate ratings (3 and 4), which indicates awareness of the problem, but without a pronounced crisis nature.

The criticality of the risk groups listed below when implementing CS tools

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

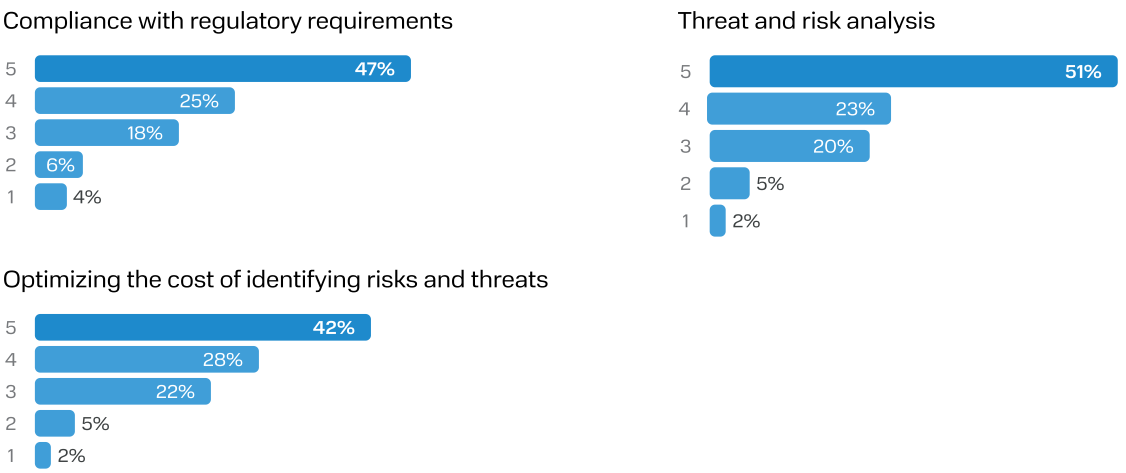


Threat and risk analysis is leading the way among the factors influencing decision-making on the implementing CS, with 51% of respondents calling it critically important. This distribution of responses highlights the companies' practical focus on understanding vulnerabilities and potential attack scenarios as the basis for forming an effective CS strategy.

Compliance with regulatory requirements also accounts for a significant share — 47% have placed this factor at the highest level of importance, reflecting regulatory pressure and the need to comply with industry standards and legislation in the field of information security.

The most important factors when making decisions about the implementing CS

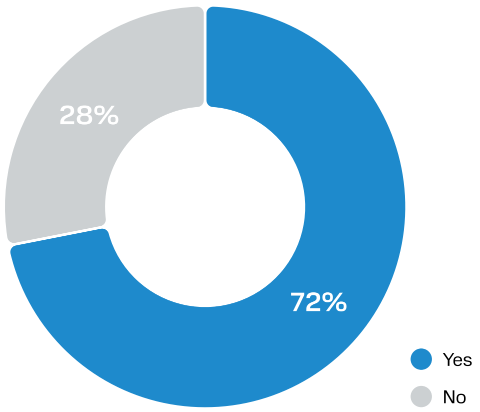
The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum



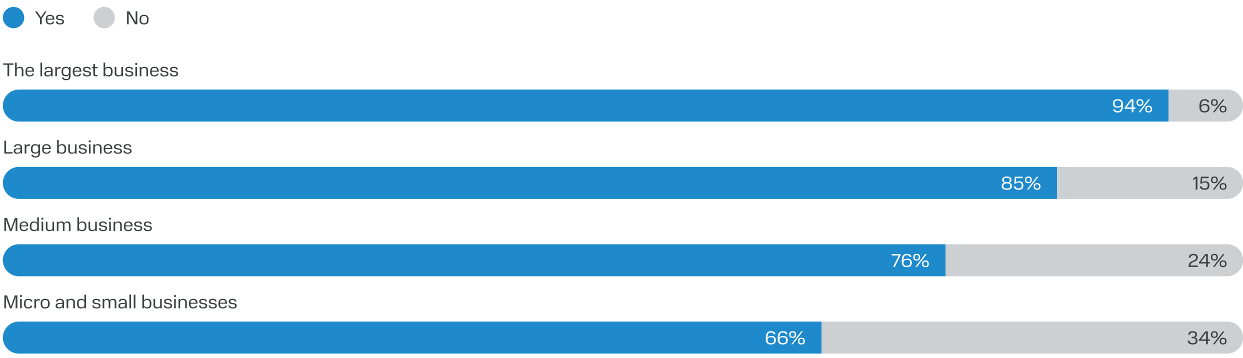
Only large and largest businesses have sufficient funding to hire the necessary specialists.

72% of companies already have experience and expertise in the field of cybersecurity. Such a high share confirms that CS issues are firmly on the corporate agenda of most market participants. The business segment structure shows that the higher the company's revenue, the higher the likelihood of having experience and competencies in the field of CS. Among companies with annual revenues of < 800 M rubles, 66% noted expertise in the CS, while among companies with higher revenues the share is growing, up to 94% for the largest business. This is logically explained by the ability of large companies to invest in specialized teams, training and development of CS processes.

Having experience and expertise in working with CS



Наличие опыта и экспертизы работы с КБ по сегментам бизнеса

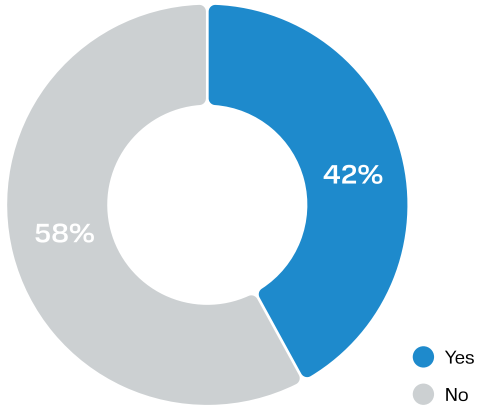


The largest concentration of expertise by industry is observed in IT (88%), mining (82%), finance and insurance (81%), as well as in healthcare and professional services. These industries are characterized by specific regulatory requirements, high risks of confidential data leaks, and the need to protect intellectual property and critical infrastructure. These factors directly affect the need to develop mature CS competence within companies. The presence of experience and expertise in the CS is not only an indicator of the maturity of technological risk management, but also reflects the specifics of industry regulations and business models. Less capital-intensive and less regulated sectors are characterized by a lower share of expertise, which indicates the potential for further development of CS practices and consulting services in these segments.

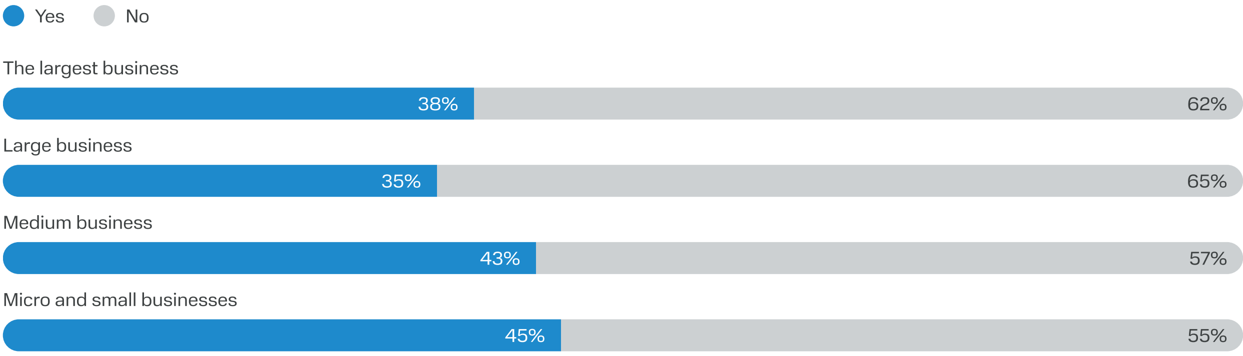
Despite the general experience of working with CS facilities, problems with hiring qualified employees are still a significant factor for the industry. 43% of respondents indicated problems in hiring experts in the field of CS, which is a significant indicator. At the same time, the presence of hiring problems does not correlate with the size of the business — companies from all business segments experience approximately similar hiring problems, which indicates the structural nature of the problem affecting both small businesses and large players.

From a technological point of view, the trend highlights the growing role of services that allow companies to compensate for the lack of their own competencies through ready-made managed security services and integrated provider expertise. In the long term, such models are becoming not just a technological option, but a strategic tool to close the critical shortage of personnel and accelerate the digital transformation of the business.

The presence of problems in hiring experts in the field of CS



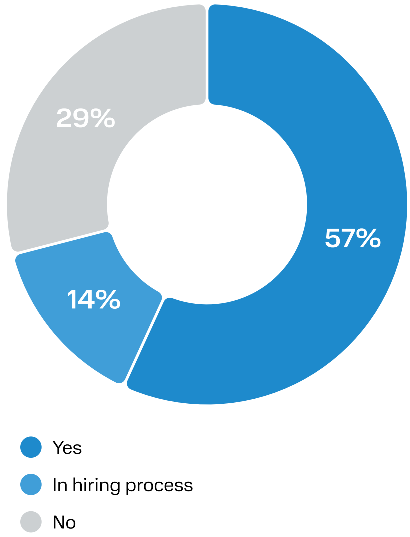
The presence of problems in hiring experts in the field of CS in business segments



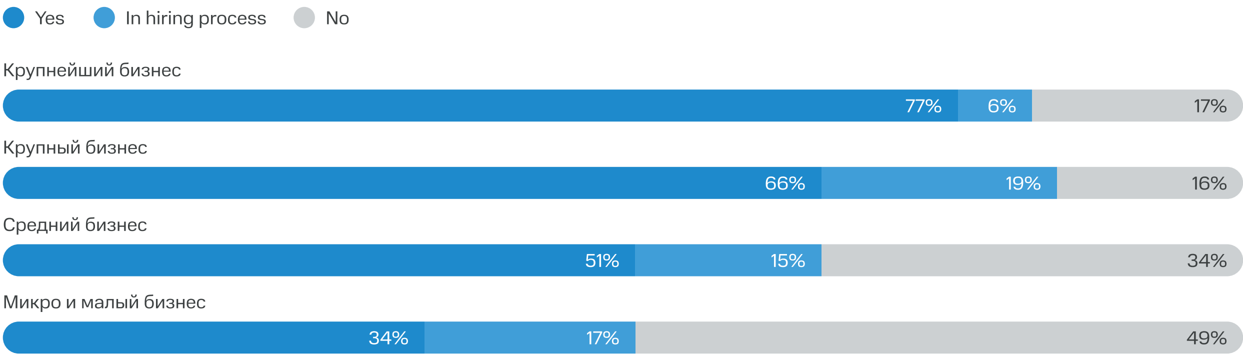
At the same time, having a full-fledged own team is also becoming more common. 57% of the surveyed companies already have their own cybersecurity team, while 14% are in the process of forming one. This indicates a growing recognition of the importance of cybersecurity in business. According to the survey results, it is expected that there is a direct correlation between the size of a company and the presence of its own cybersecurity team. Large companies with more complex IT structures are more likely to have their own teams.

Companies in the IT and pharmaceutical sectors are most often noted for having their own team. This is due to the fact that they process a large amount of data and are subject to significant regulatory requirements. However, even with in-house specialists, enterprises continue to rely on cloud security services to cover scalable tasks and meet growing regulatory standards. As a result, the market is moving towards combined models: its own CS competence centers are complemented by advanced cloud solutions, which creates demand for more flexible, integrated and industry-oriented services.

Having own cybersecurity team



Own cybersecurity team in business segments



Professional services for the development of cybersecurity mainly include technical support, training and auditing. These services are used by more than 40% of the surveyed companies. Technical support plays a key role in ensuring prompt incident response and vulnerability mitigation. Cybersecurity training increases employee awareness of potential threats and ways to prevent them. CS audit allows companies to systematically check and improve their protective measures. Overall, the data shows that companies are actively investing in key elements of cybersecurity, which is an important step to reduce risks and protect against cyber threats.

The list of professional services used for CS development

63%
Technical support

25%
Integration

CYBER PROTECTION OF THE CLIENT'S HYBRID INFRASTRUCTURE

Tools to protect against information security threats

Reduce the risk of cyber attacks by 80%

Reduce losses from any cyberattacks by 50%

24/7

perimeter monitoring and protection

500

active rules for analyzing and comparing IS events

>1500

sources of a wide range of information for data processing

300 Гбит/сек

active bandwidth for AntiDDoS

SOC

A comprehensive solution to increase the level of cybersecurity of the enterprise. By combining qualified specialists, innovative technologies and established processes, it provides comprehensive protection of the organization from cyber threats in real time. SOC monitors the state of the company's IT infrastructure around the clock and reduces the risks of hacks, theft of employee/client/user data, and other cyber threats that can bring the business to a standstill.

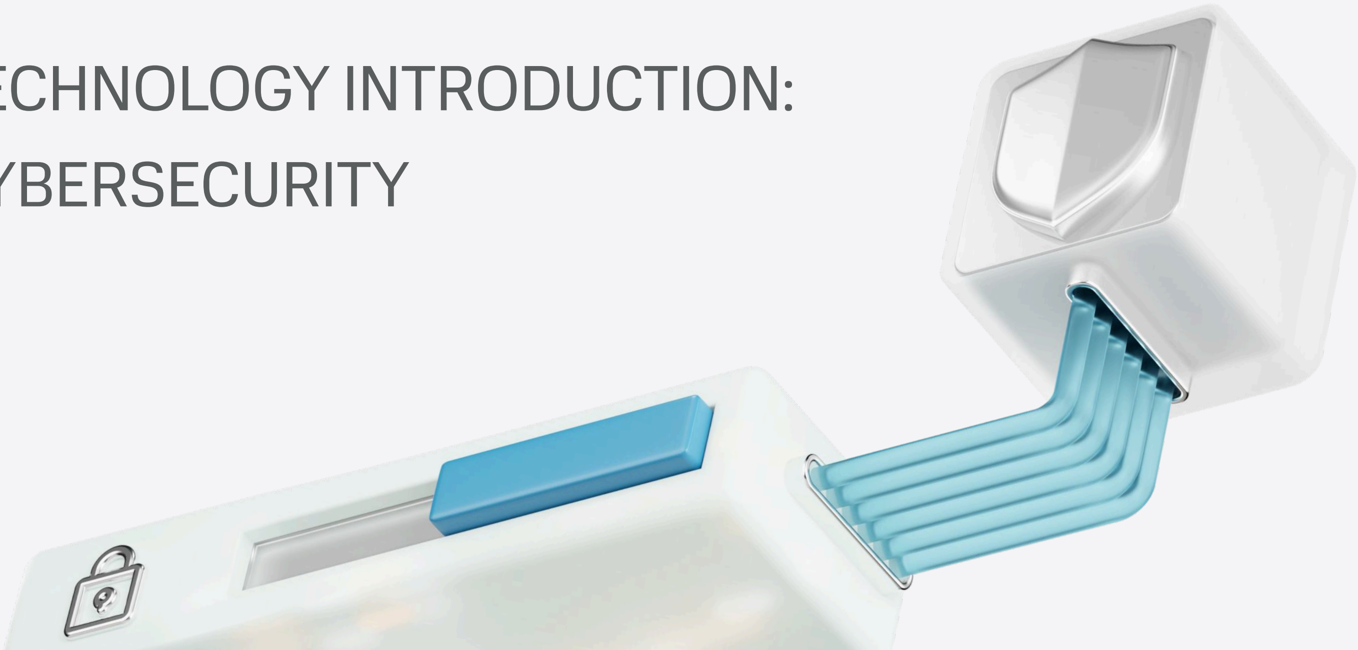
ANTI-DDOS

A comprehensive solution that blocks DDoS attacks on the customer's infrastructure and web resources. Protection against DDoS attacks is necessary for organizations whose activities are directly or indirectly related to the availability of systems on the Internet, and whose working processes are linked to remote access to their own and third-party resources.

WAF

A service to protect against attacks and vulnerabilities in web applications. You can use your profile page to set up your own policies and rules for protecting your resources.

TECHNOLOGY INTRODUCTION: CYBERSECURITY



This section demonstrates product categories related to information security technology. Due to the specifics of the study, the CS part focuses on the Software and IT Services verticals in the IT market, since these verticals make up the majority of the cybersecurity market in Russia in terms of amount. The hardware part of cybersecurity solutions is not the focus of our study, as it consists of highly specialized products, including analog solutions, and is not always associated with digital products. By analogy with the cloud, CS products can be divided into widespread ones, including those necessary to comply with legal requirements, and highly specialized ones that are in demand by companies to solve problems of increased complexity.

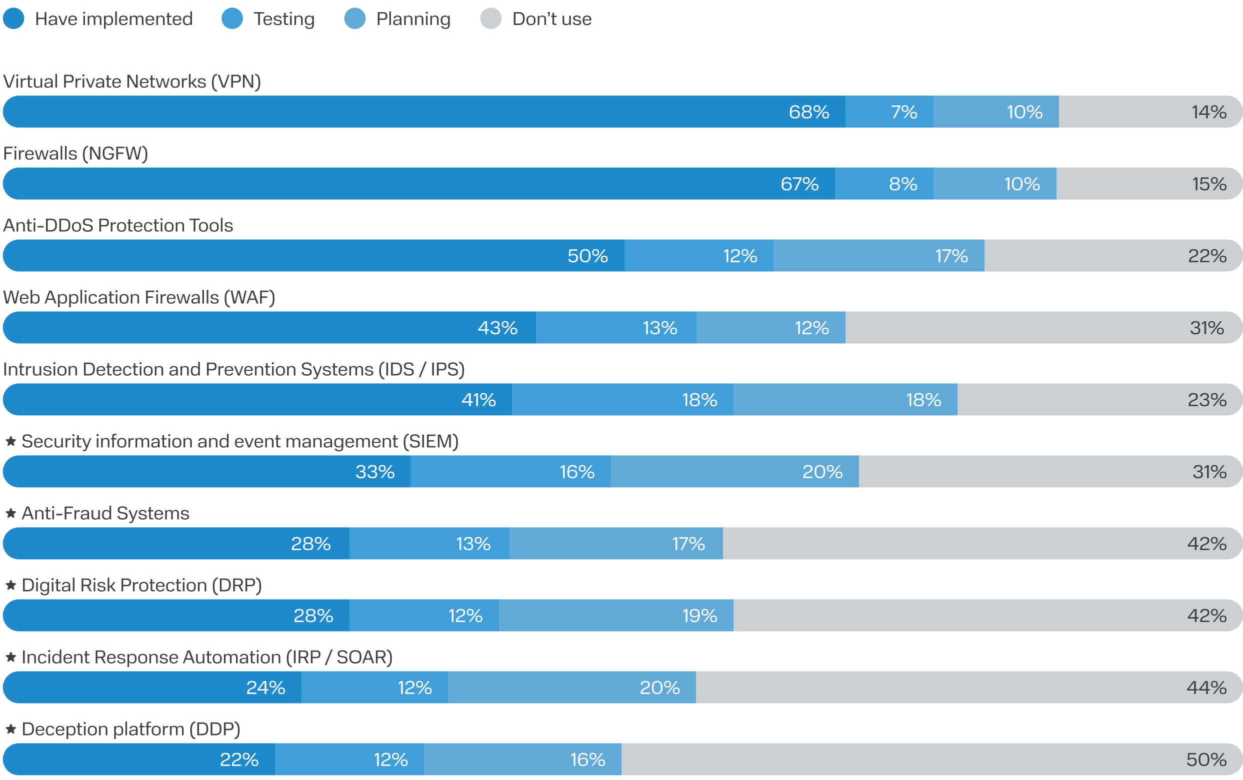
To evaluate among the obtained subcategories those products that have an increased growth potential, an approach called the "Formula for the growth potential of subcategories" was introduced. This formula is a comparison: on the one hand, the parameter "implemented", on the other hand, the sum of the parameters "testing" and "planning". Unlike the "don’t use" parameter, these values positively characterize the respondents' plans, which can be interpreted as a likely transition to the "implemented" status in the near future.

Have implemented < Testing + Planning = There is potential

Have implemented > Testing + Planning = Potential exhausted

According to these data, the product subcategory of Infrastructure Protection tools is the most promising (5 promising technologies out of 10). The high potential for further development of these areas is due both to technological trends (migration to the cloud, microservices, remote/ hybrid work, the transition from the traditional perimeter model to the Zero Trust model) and economic factors (increased losses from incidents, cyber risk insurance, lack of design specialists). Additional threats include not only a general increase in the number of cyber threats, but also factors such as accelerated development and delivery of software products, stricter regulatory requirements, and the overall transformation of the IT landscape. In these circumstances, investments in advanced application and infrastructure protection tools are becoming a key driver of reducing cyber risks and ensuring business continuity.

Infrastructure Protection Tools

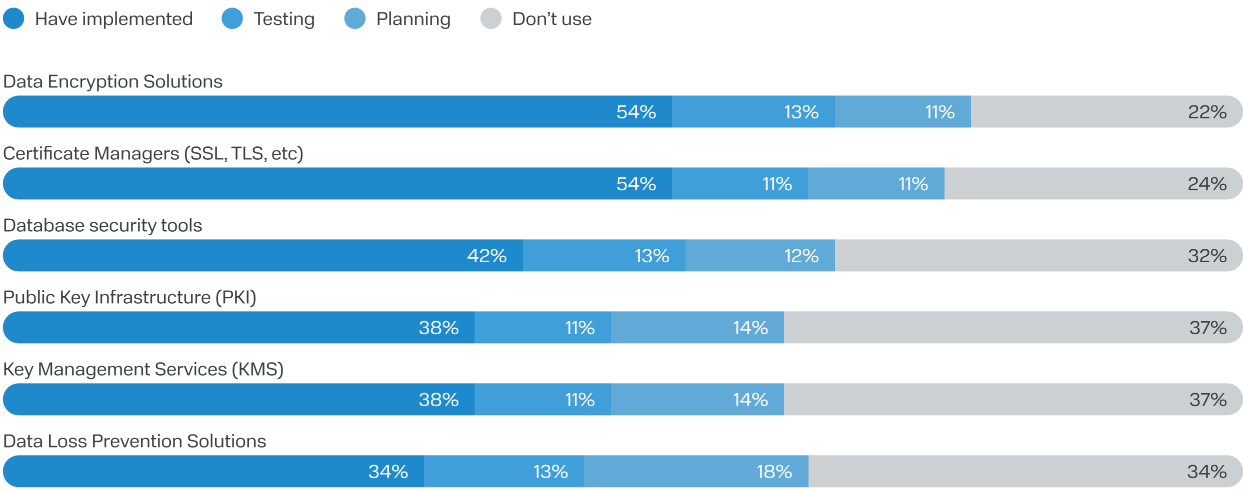


Information security solutions are the segment with the largest budget among the analyzed technologies. It is important to emphasize that this is due not just to formal compliance with legal requirements, but to a real threat to infrastructure security (among the largest businesses, more than 60% of the surveyed companies faced DDoS attacks during the year). Also, to strengthen protection against external threats, companies noted the frequent introduction of enterprise-class VPN services. Firewalls (NGFW) continue to be noted by companies as one of the most frequent products on the market (the implementation parameter was noted by 67%). Naturally, the high demand for the hardware and software supply model was largely recorded by companies of large and largest businesses.

The basic practice in holding companies is to have their own CS team (76% of the surveyed representatives of the largest businesses noted), however, hiring experts, including those responsible for protecting the basic infrastructure of the enterprise, still remains a significant problem (43% of respondents noted). This may be one of the reasons for the high proportion of those planning but not implementing solutions for many of the product subcategories.

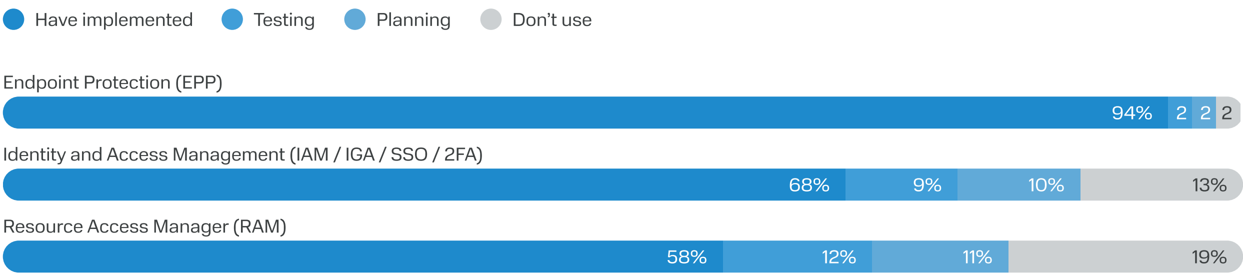
★ — high potential

Data Protection Tools



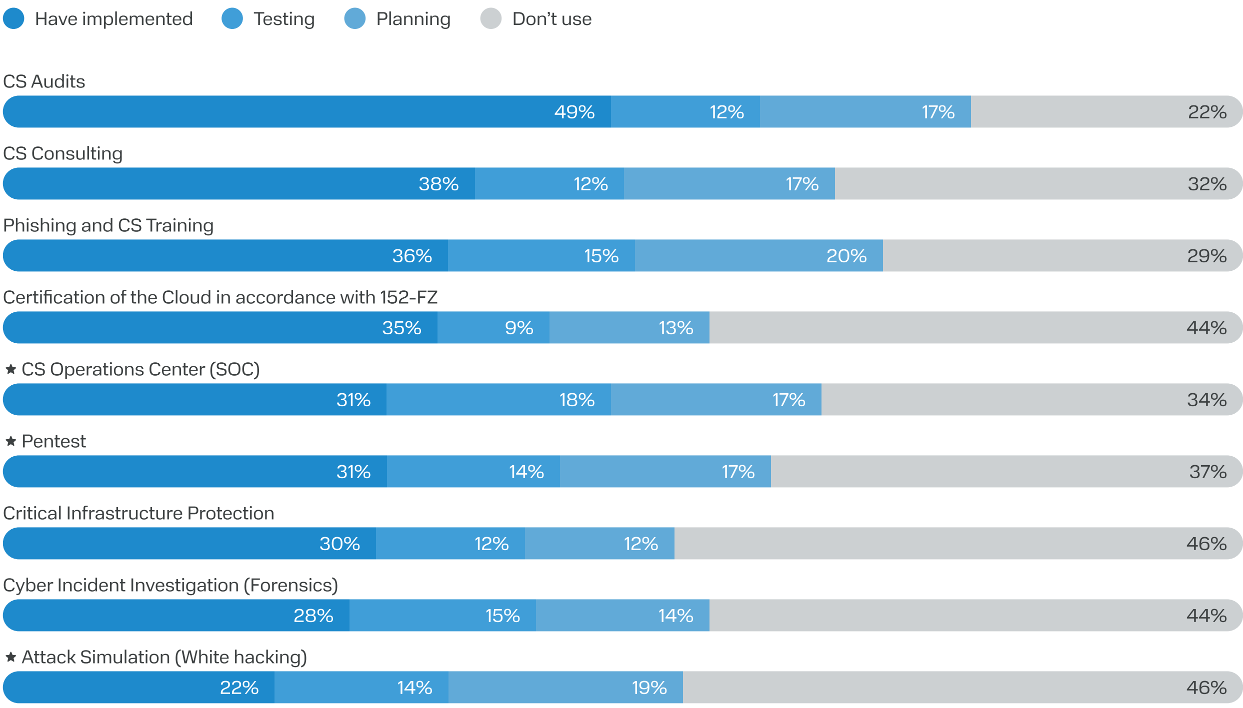
Protecting data from external and internal threats is a fundamental attribute of any corporation's business. The largest ecosystem-based Russian organizations, as well as government authorities, are regularly exposed to relevant risks, which poses not only a threat to internal operational processes, but also shareholder and reputational losses. Data encryption was noted by respondents as the most common data management tool, along with certification, access rights management, and other tools for responding to external threats. Separately, many respondents highlight DLP as a planned class of solutions for implementation, which is more in demand by large companies.

User and endpoint protection tools



Endpoint Protection has the highest adoption rate of all CS products under consideration — 94%, which indicates a high level of awareness about potential cyber threats. This class of solutions has become a commodity in the Russian market. As the complexity and number of cyber attacks increase, users respond to these risks by increasing their consumption of access control products.

Services in CS sphere

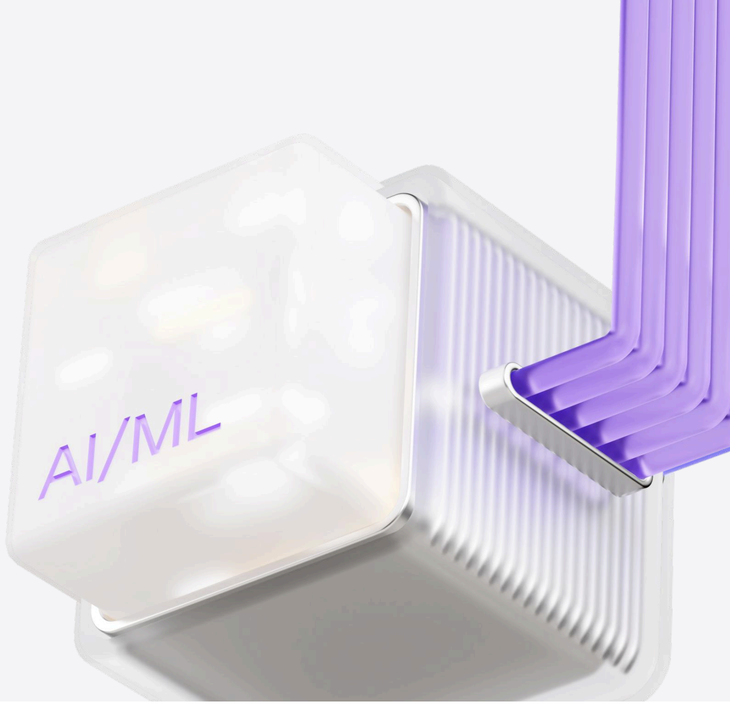


Software and IT Services together account for about 80% of the cybersecurity market in Russia. The vertical of IT Services is growing at an annual growth rate of more than 30%. These values correlate with the data on expectations of consumption volumes of the corresponding CS solutions in the sample of this study. Cybersecurity services are no less developed than software, which is due to a number of factors: difficulties in finding specialists, a lack of internal expertise, and the high cost of creating a company's own cybersecurity function.

The absolute leader in the share of service consumption is CS Audit, which is also conditioned by regulatory requirements and orders from the shareholders of the companies. Applying the previously formulated approach to identifying product subcategories with significant categories (the sum of responses for the "testing" and "planning" parameters is comparable to the value for the "implemented" parameter), the following categories can be noted in the IT Services part: Phishing, CS Training, CS Monitoring Center (SOC), as well as Pentest and White hacking.

★ — high potential

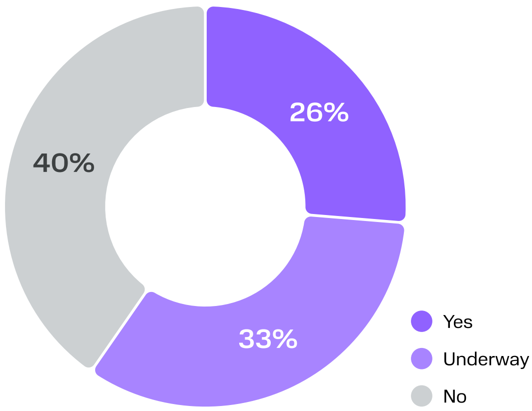
TECHNOLOGICAL BUSINESS STRATEGIES: ARTIFICIAL INTELLIGENCE



Having an implementing AI strategy allows companies to systematically approach the development of this area, integrating AI into the overall business architecture and ensuring a coordinated allocation of resources.

According to the data obtained, only 26% of respondents have an AI strategy, which is less than the share of implementing strategies for cloud solutions (44%) and cybersecurity (42%). At the same time, plans for developing an AI strategy stand out from a larger number of companies than plans for developing other strategies. The difference is due to the dynamic development of technology and the novelty of many AI solutions for a significant list of companies.

Having a strategy for implementing AI



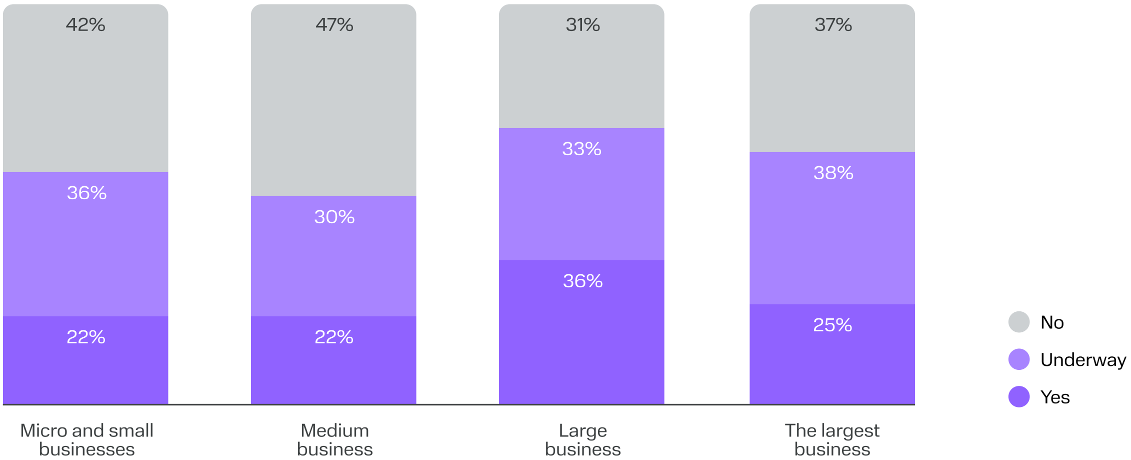
The leaders in terms of the developed AI strategy are large players with large resources and opportunities to invest in the development of their own AI products. At the same time, the share of the largest players with a developed strategy is smaller, which may be due to the length of the strategic planning cycle. Among the industrial leaders in terms of strategy, we can single out the IT sector, transport and logistics, as well as scientific organizations for which the use of AI is an applied necessity within the framework of processing large amounts of data.

> Ready-made AI strategies are not widespread, but they are actively being developed by players in all segments.

> We are seeing a paradigm shift: from universal generative intelligence, which can do everything and nothing for real, to specialized solutions that give measurable results. The era of application models created for specific tasks and industries is coming. Companies are realizing more and more clearly that simple integration takes too much time and resources, and the economic effect does not converge. Hence the new trend — platforms for creating and managing AI assistants. A class of solutions is being formed that allows businesses not just to use models, but to build a pipeline for creating their own AI products. Today, companies are moving to the next stage — their own AI transformation, to a business built on artificial intelligence.

Denis Filippov
CEO MWS AI LLC

Having an implementing AI strategy in business segments



In 67% of companies, the XU (IT head) plays a key role in the AI decision-making process, which is logically explained by their expertise in information technology, as well as a deep understanding of the infrastructural and architectural aspects of implementing AI solutions. The CEO is in second place in terms of engagement, with a score of 23%, reflecting the strategic importance of AI at the senior management level.

The remaining roles, including CISO, STO, and SRO, collectively account for less than 11%, which demonstrates the relatively limited involvement of specialized security, technical development, and product managers in the direct process of approving AI initiatives. These data emphasize that the implementing AI in most cases remains in the area of responsibility of the IT Directorate, with the support of top officials of companies in terms of strategic approval. This KDM structure can serve as a guideline for building client strategies and targeted communications when promoting AI solutions in the corporate market.

For the majority of respondents (55%), the implementation process takes from one to six months. The most common range is from 1 to 3 months (29%), which indicates the desire of companies to minimize the time needed to implement AI solutions and get the effect of their use as quickly as possible.

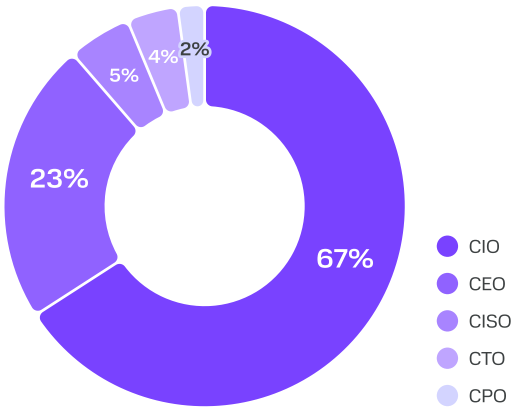
At the same time, for a significant proportion of organizations, the process is stretched over a longer period of time. These indicators may reflect either the high complexity of the solutions being implemented, or organizational barriers and the need for coordination at several levels of management.

Thus, the analysis obtained demonstrates that most companies are focused on relatively rapid implementing AI tools, but a significant part of projects are still characterized by long cycles of more than six months, which is important to take into account when planning resources and building project roadmaps for such solutions.

The most popular types of AI deployment among the surveyed companies were private and public cloud, which are used by 23% of respondents each. Local installations of AI workloads involve 20% of companies, while hybrid scenarios are less common so far — they are chosen by 13%.

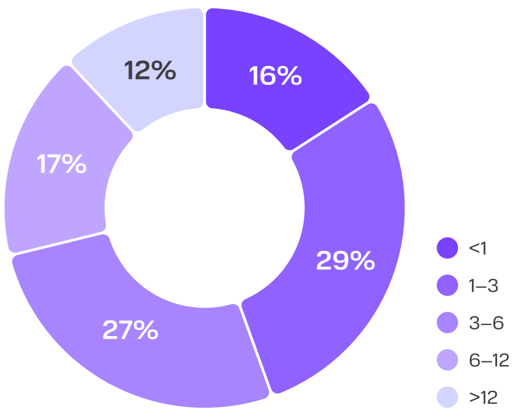
Such choice reflects the business's commitment to using cloud models to provide flexibility, scalability, and lower capital costs while maintaining control over critical processes and data in private infrastructures. Public clouds allow for faster adaptation and scaling of operations, which makes them attractive for tasks with variable or fast-growing workload. These data confirm the general trend towards the active use of cloud technologies to improve the efficiency and security of AI systems.

Key employees (KDM) in the decision-making process on the implementing AI



Duration of the implementing AI tools process

В месяцах

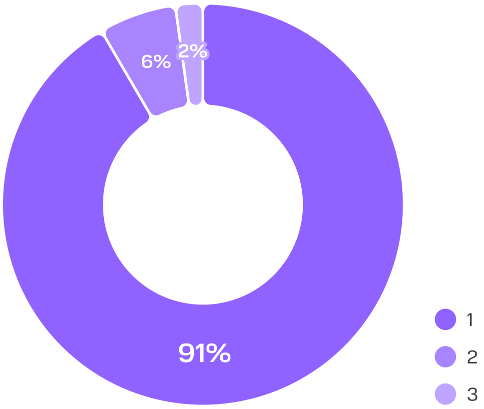


Number of AI vendors used in business segments

The majority of the surveyed companies (91%) cooperate with only one AI vendor. This model allows you to focus on adapting selected solutions to specific business needs, as well as simplify infrastructure management and reduce the risks associated with the compatibility of different platforms. The share of companies that cooperate with several vendors at once (2 or more) remains relatively low and totals about 9%, which indicates that the distribution of multi-vendor strategies in the AI market is still limited.

There is a clear trend: as the size of the business decreases, the proportion of companies that do not use AI at all increases. For the largest companies (> 15 bn rubles) The AI rejection rate is only 15%, whereas in the segment with revenue of 2–15 billion rubles. It is already 21%, and among companies with revenues of less than 800 M rubles — about 11%, but almost all of them are limited to a single supplier. The use of two or more AI vendors is typical for the most mature business segments: large and large companies with revenues of over 2 bn rubles.

Number of AI vendors used



Annual AI costs by industry

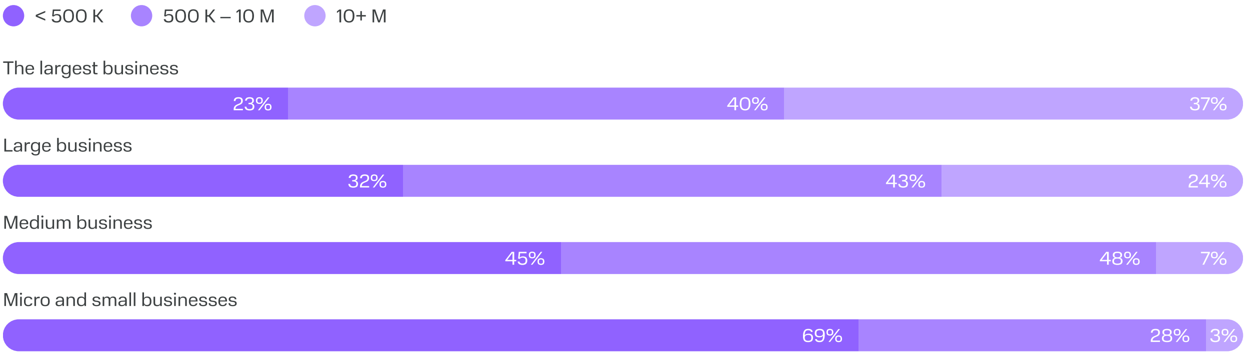
	< 500 K	500 K – 10 M	10+ M
IT	42%	30%	28%
Finance and Insurance	46%	34%	20%
Mining and processing of minerals	54%	27%	20%
Science and education	45%	41%	14%
Entertainment and Media	33%	58%	8%
Retail	56%	36%	8%
Professional services	82%	13%	6%
HoReCa	60%	35%	5%
Industry	67%	28%	5%
Transportation and logistics	55%	40%	5%
Healthcare	54%	42%	4%
Construction and real estate	66%	33%	1%

> At the current stage, AI is characterized by a monovendor approach: companies are just exploring the market.

AI costs are proportional to the size of the business. If the share of average costs is approximately equal for all segments except micro and small-sized businesses, then the share of costs over 10 M increases sharply for large and largest businesses. This separation is due to the presence of its own development team and the creation of custom solutions for this business segment. It is market leaders who form the bulk of the demand for large-scale AI initiatives and can afford to develop more capital-intensive projects.

Annual AI costs in business segment

The scales indicate the business segment according to revenue, the color indicates the amount of costs.



> AI is a big business, and it invests in the development and adaptation of solutions.

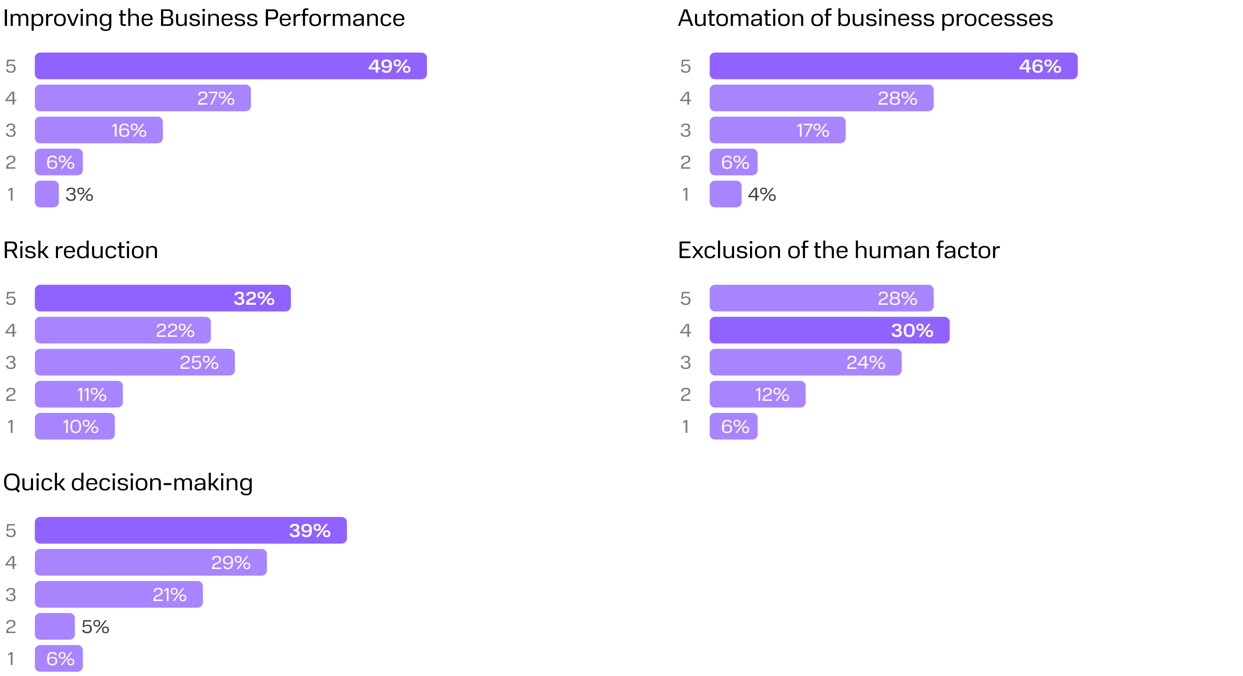
The largest volume of investments in AI is recorded in the IT, finance and insurance, mining and processing, retail, transport and logistics, as well as science and education. These industries exhibit a more distributed cost structure with a significant proportion of companies going beyond minimum budgets. The IT sector stands out in particular, where 29% of companies spend over 10 M rubles a year on AI, which is significantly higher than similar indicators in other industries. This is due to the high maturity of digital processes and the direct dependence of the business on technology.

Retail and transport are characterized by more moderate budgets, concentrated in the range of up to 20 M rubles per year, which is associated with the active use of AI for forecasting, supply chain management and personalization of services. The science and education sector also demonstrates a propensity to invest in the medium range, reflecting the challenges of processing large amounts of data and developing analytical platforms.

For most companies, the key factors in deciding whether to implement AI are improving business efficiency (49% noted this factor as the most important), automating business processes (46%) and making quick decisions (39%). These three areas form the basis of business motivation for investing in AI, reflecting companies' desire to reduce costs, increase operational speed and flexibility.

Key factors when deciding on the implementing AI

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

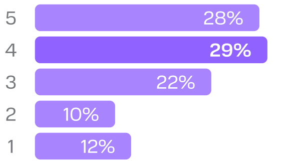


> Companies expect significant cost reductions from the introduction of AI, but fear the risks associated with data leaks.

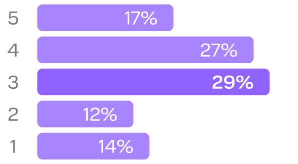
Difficulties in the implementing AI process [1/2]

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

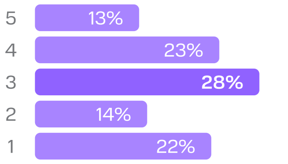
Lack of necessary competencies among employees



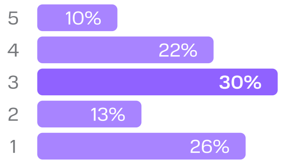
The difficulty in estimating the estimated costs of the required infrastructure



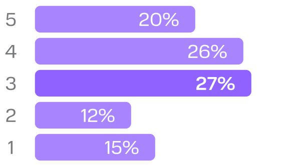
The need for temporary duplication of infrastructure



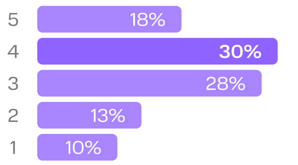
Lack of vendor support during the implementation process



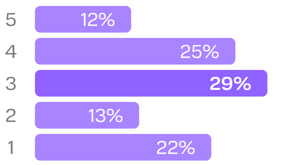
Additional costs at the stage of artificial intelligence implementation



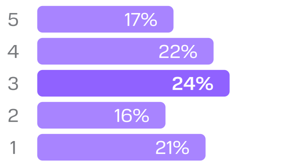
Search for AI-based solutions/tools on the market or their development



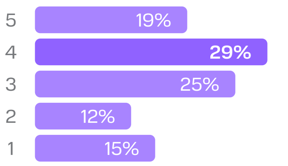
Lack of an implementation roadmap



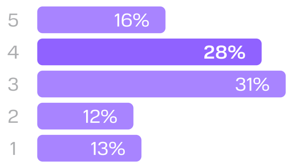
The difficulty of transferring large amounts of data



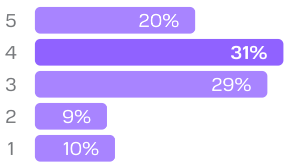
High financial costs



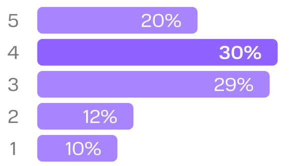
Scaling within an organization



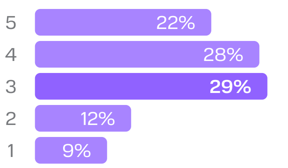
Creating the necessary data platform for working with AI



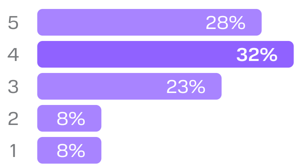
Changing familiar business processes to use AI effectively



Informing and training employees on AI issues



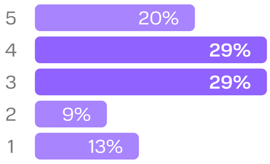
Achieving the required quality level of AI-based models



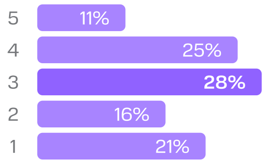
Difficulties in the implementing AI process [2/2]

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

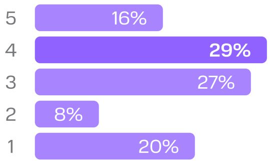
Forming a unified vision of key areas of AI use in the company



Lack of technical support programs from the providers/vendors in question (ROS, Support, etc.)



Inability to integrate artificial intelligence tools into used local solutions (outdated software/hardware)



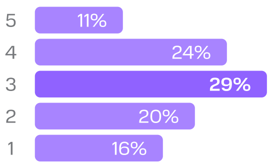
The difficulties accompanying implementing AI process are generally assessed by respondents at an average level of importance, which confirms the willingness of most companies to move towards AI integration, despite existing barriers. Companies are mostly willing to commit resources to overcoming organizational and technological barriers in order to obtain long-term benefits from using AI, but the issue of personnel training remains a key factor that requires priority attention when planning such projects.

The additional costs incurred in the implementing AI process are generally assessed by respondents at an average level of importance, which indicates the willingness of most companies to take these costs into account in their investment plans. The most frequently mentioned factor is retraining or hiring employees to ensure high-quality work with AI: 29% rated this item as the most important (4 out of 5), and another 19% gave the highest score. Personnel issues remain a key challenge for companies, requiring investments in competencies for the successful operation of AI solutions. This reflects previously identified barriers, such as a lack of technical expertise and risks associated with data management, including the threat of information and personal data leakage.

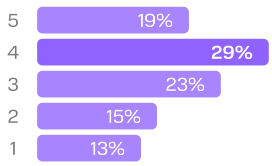
Additional costs in the implementing AI process

The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum

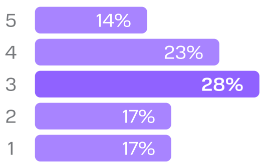
Deploying a test loop to verify the operability of the solution in question



Retraining / hiring employees for high-quality work with artificial intelligence



Updating the local infrastructure



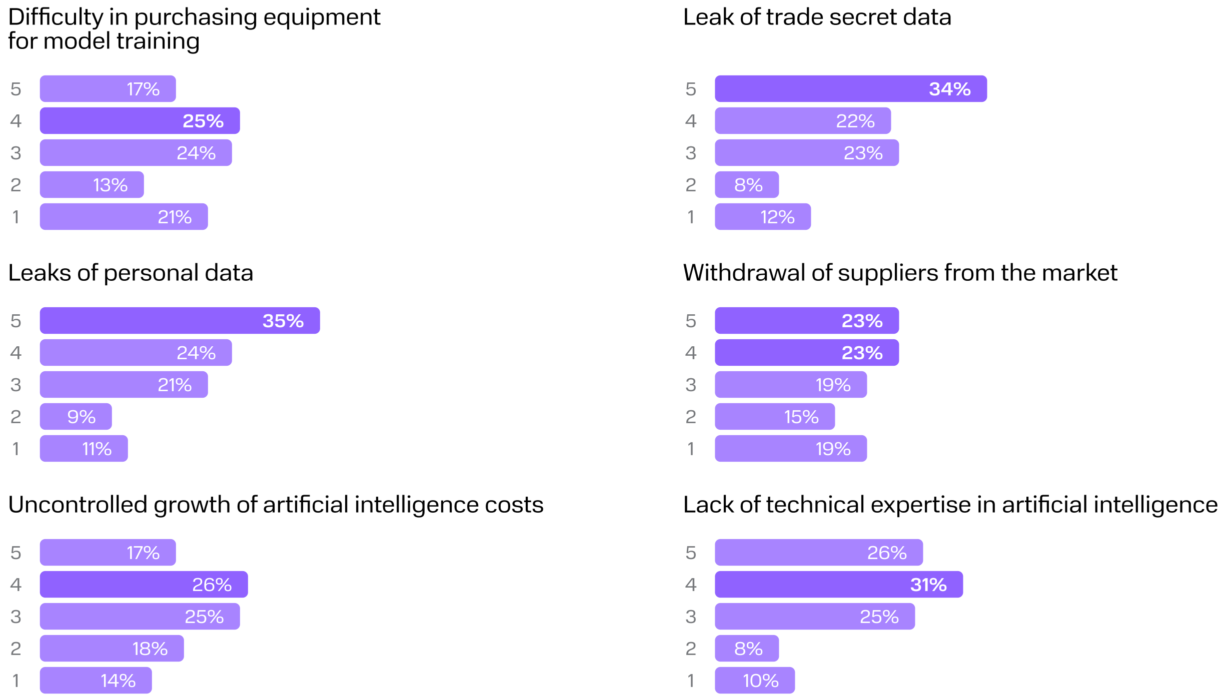
Among the critical risks associated with the introduction of AI, companies primarily identify the threat of data leaks — both personal (35% of the highest criticality ratings) and trade secrets (34%). This highlights the high sensitivity of businesses to security and confidentiality issues when implementing AI projects.

The lack of technical expertise in artificial intelligence also remains a significant barrier: 26% of respondents rated it as the most critical risk, while another 31% assigned a level of importance of 4 out of 5. Separately, concerns about the uncontrolled growth of AI costs are recorded, which confirms the need to build budget planning and FinOps practices for such projects.

The risks of suppliers leaving the market, difficulties in purchasing equipment for training models, and general infrastructure constraints remain less pronounced, but still relevant. These data indicate that for companies, data protection issues, the availability of competencies and cost transparency are still crucial when making decisions on the large-scale development of AI initiatives, despite the previously declared benefits in terms of optimizing routine tasks and increasing the efficiency of business processes.

The criticality of the risk groups listed below when implementing AI tools

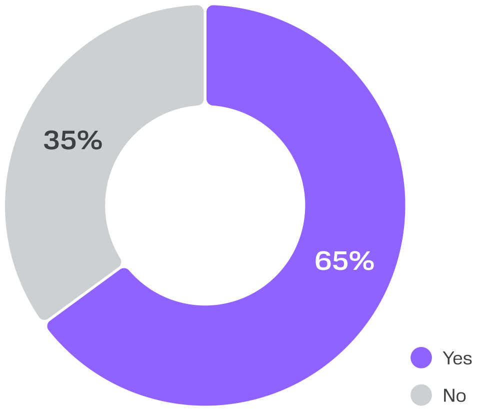
The respondent's score is from 1 to 5 points, where 1 point is the minimum influence of the factor, 5 is the maximum



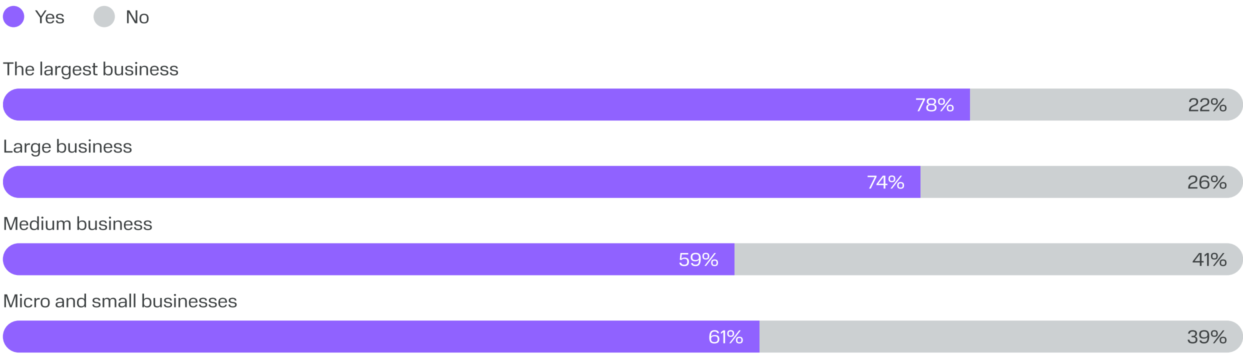
65% of the companies surveyed have experience and expertise in working with AI, which highlights the overall market movement towards the development of artificial intelligence technologies. At the same time, the data show a direct dependence of the level of accumulated competencies on the scale of the business: large companies more often have specialized teams and expertise in AI, which is associated with their ability to invest in the development of such competencies and maintain their own R&D centers.

In terms of industry, science, IT, and the entertainment and media segment are leading the way — in these industries, the share of companies with AI specialists exceeds 80%. This is largely due to the specifics of these industries, where working with big data, forecasting algorithms, and process automation has already become part of the operational model. Such results confirm the high importance of accumulating internal expertise for the successful implementation and scaling of AI solutions.

Having experience and expertise in working with AI



Having experience and expertise in working with AI in business segments

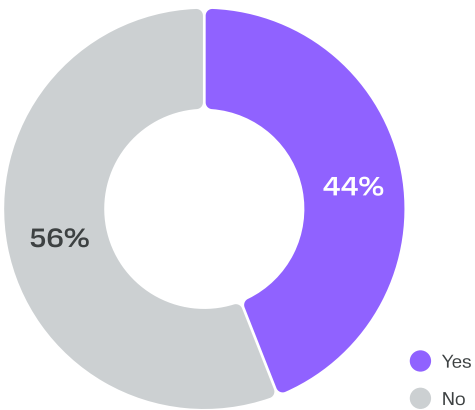


Despite the fact that a significant part of companies already have experience and expertise in the field of AI, problems with hiring qualified specialists remain for a significant part of the market: 43% of respondents noted difficulties in attracting AI experts. This indicator is approximately the same for all business segments in terms of revenue, which indicates the systemic nature of the lack of competencies in this area.

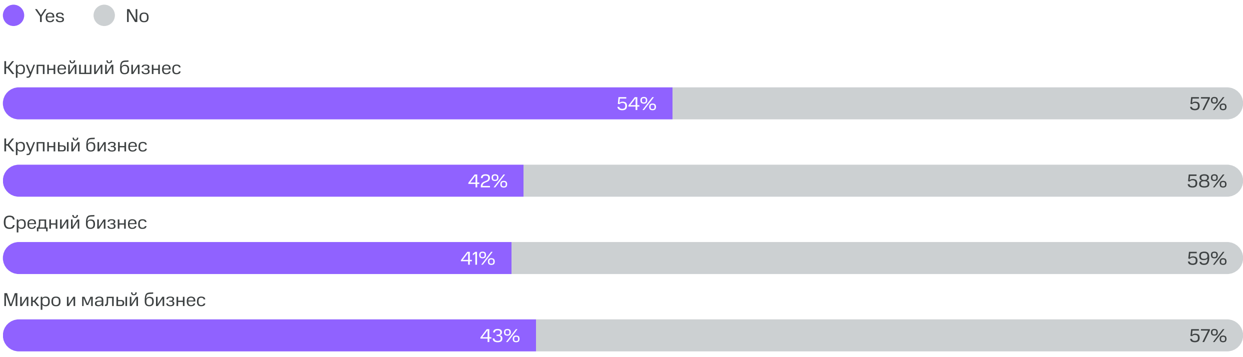
The problem of staff shortage is most acute in such industries as heavy industry (69%), construction and housing (61%), industry (60% each), as well as science and education (59%).

These industries are characterized by specific requirements for AI solutions, high regulatory barriers and the need for a deep understanding of industry processes, which complicates the search and integration of new specialists.

The presence of problems in hiring experts in the field of AI



The presence of problems in hiring experts in the field of AI in business segments

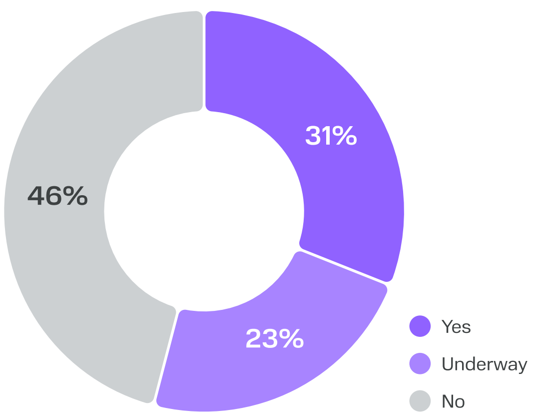


About a third of the respondents have their own team of developers and data scientists. The presence of such teams directly correlates with the level of maturity of approaches to artificial intelligence in a company and is most often found in organizations where an AI strategy has already been formed and which are in the phase of active or prolonged implementation of such solutions.

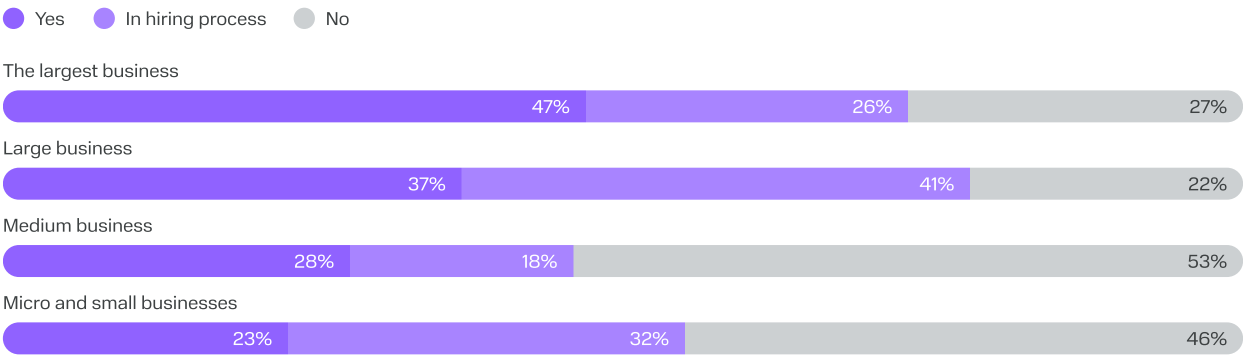
The analysis, depending on the duration of work with AI, shows a clear trend: the longer a company has been implementing AI, the more likely it is to have its own team. So, among companies that have been using AI for less than one year, only 29% have development teams, while among companies with more than 12 months of implementation experience, this share increases to 44%. This confirms that internal AI competencies are, in most cases, developed as practical experience with these technologies accumulates and projects become more complex.

It is also interesting that most of the companies in the process of creating such teams (through hiring or retraining employees) implement AI projects within 3–6 months. This may indicate that at this stage companies are beginning to face the need to move from pilot initiatives and the use of ready-made solutions to more complex scenarios that require the involvement of their own specialists to customize and refine models to suit the specifics of the business.

Own development team and data scientists



Own development team and data scientists in business segments



Overcoming the lack of internal competencies is carried out, among other things, through the use of professional services. The most popular services for the development of artificial intelligence among respondents are training and technical support, used by more than 30% of companies. While AI consulting is less widespread, only 17% of respondents use it. This may indicate a preference for companies to implement AI on their own, but using consulting services can help optimize and speed up the implementing AI process by providing valuable recommendations and best practices.

The list of professional services used for AI development

33%
Training

31%
Technical support

22%
Model training

18%
Integration

18%
Custom development of AI applications

17%
Consulting (strategy)

12%
Model inference

CLOSE THE NEED FOR AI SERVICES AND EXPERTISE

Sophisticated AI-based solutions with proven results

Profit growth by 20%

by making more precise strategic decisions through the use of AI in data analysis

20–45% increase in productivity of the development department

for processing customer requests

60% reduction in time

for processing customer requests

MWS GPT

A platform for working with large language models (LLM) for businesses

24 hours the period from the model's request to her work in the product	**2 years** saving labor costs for creating a similar platform solution	**All** existing models are available on the platform with the possibility of further training

MWS COSTUME AI

Individual development of AI solutions for the needs of a specific client

TECHNOLOGY INTRODUCTION: ARTIFICIAL INTELLIGENCE

The artificial intelligence section covers a wide range of technologies. The structure of the artificial intelligence market in this study is based on a general approach to the decomposition of the IT market. In this part, the focus is on the Hardware and Software verticals, which, in turn, are divided into three groups: (1) Computing technology, (2) AI-agents and applications, (3) AI-platforms. AI technologies are less developed among corporate clients regarding clouds and cybersecurity. Taking into account the size of the budget, the availability of a strategy and analytics of product consumption, it can be concluded that for many companies these solutions remain an experimental technology and are not massively integrated into corporate processes. Despite the dramatic attention from the professional community and widespread use by end users, solutions in the B2B segment still have great untapped potential.

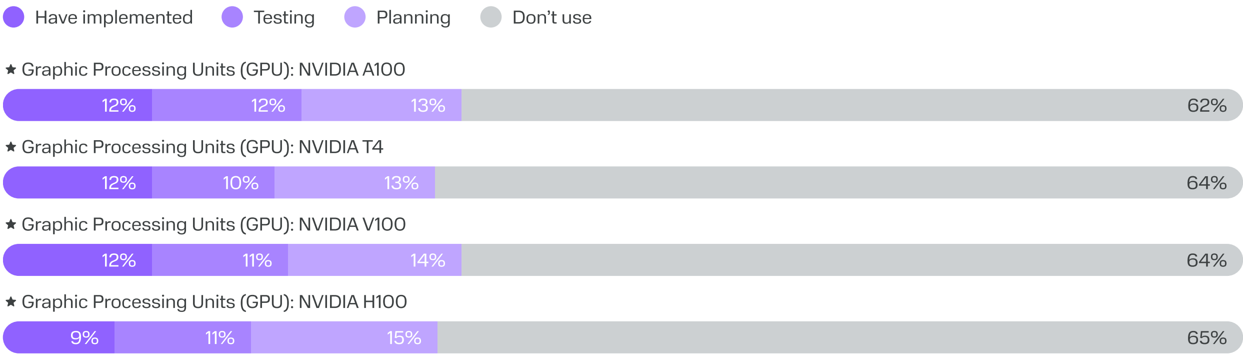
To evaluate among the obtained subcategories those products that have an increased growth potential, an approach called the "Formula for the growth potential of subcategories" was introduced. This formula is a comparison: on the one hand, the parameter "implemented", on the other hand, the sum of the parameters "testing" and "planning". Unlike the "don't use" parameter, these values positively characterize the respondents' plans, which can be interpreted as a likely transition to the "implemented" status in the near future.

Have implemented < Testing + Planning = There is potential

Have implemented > Testing + Planning = Potential exhausted

Assessment of the growth potential of subcategories, the assessment according to the above "Formula for the growth potential of subcategories" demonstrates the high prospects for the development of all groups of solutions, including both application software products and industry solutions. The high potential for the development of AI products is explained by the synergy of several megatrends, including the digitalization of business processes, the cheapening and development of machine learning tools, the exponential growth of data and the improvement of companies' competencies when working with them. This means that investing in AI will remain a strategic priority for all players who seek not only to support the business, but also to stay ahead of the market.

Computing Technology

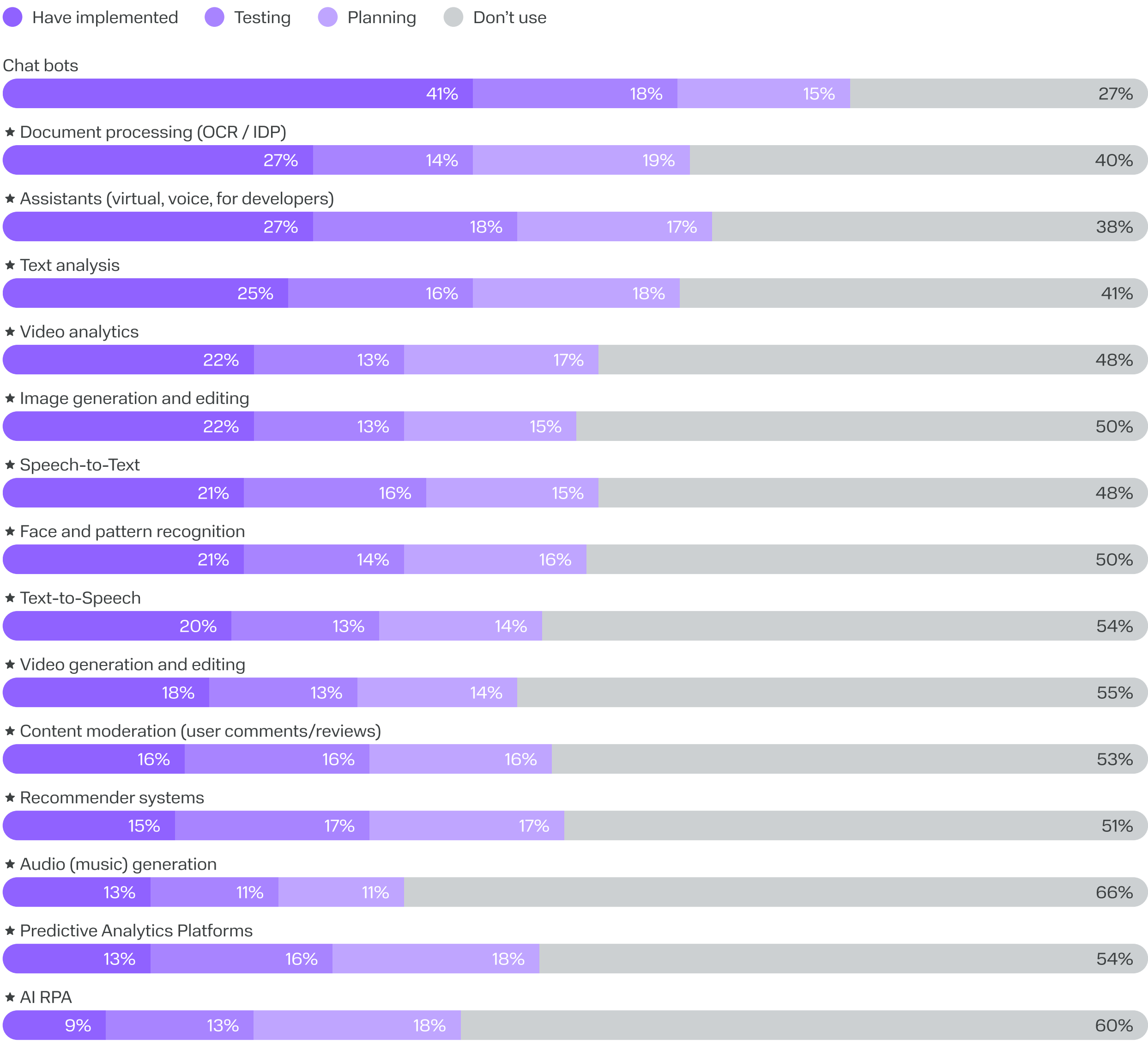


The demand for hardware for working with artificial intelligence-based solutions is formed mainly by companies of large and large businesses, as well as ecosystem companies. Additional demand is generated by specialized companies in IT, FinTech, E-Com, MarTech, EdTech, MedTech, InsureTech and other technology industries. Considering the obtained values for the parameters "testing" and "planning", insignificant percentages in the category "Computing technology" are observed in the total mass of respondents' responses. However, based on the previously proposed formula for assessing the potential of subcategories, it can be noted that respondents have high expectations for the consumption of these solutions.

For example, the implementation values for graphic processing units (GPUs) of different models are comparable to each other, which is still less than 5 times relative to classical computing (CPUs). The most popular graphics card is NVIDIA A100. The cost of this solution is about 1,5 times less than NVIDIA H100, which makes it more affordable for a wide range of companies, including medium and small-sized enterprises. New logistics supply chains for video cards have been formed, while there are problems with vendor technical support. From the point of view of demand, it is critically necessary for the end user of hardware solutions to compare the practical purpose with the models of various video cards.

★ —high potential

AI-Agents and applications

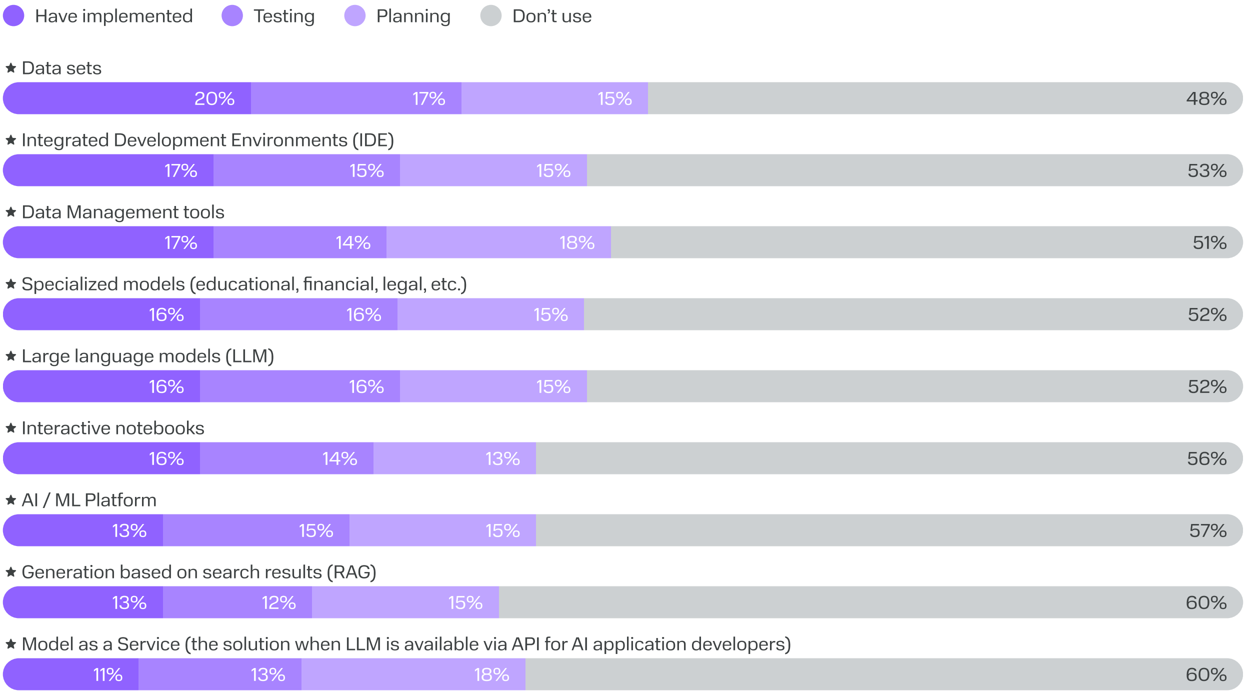


In contrast to the "Computing technology" category, the subcategories that relate to "A1 agents and applications" have demonstrated significantly higher adoption rates. This is particularly clearly demonstrated by the "Chatbots" subcategory, which is the only one among all the subcategories in AI technology within the framework of this study for which current implementation exceeds testing and usage planning. These solutions have been implemented by 41% of the respondent companies, against 18% and 15%, respectively, according to the answers "testing" and "planning". The remaining subcategories showed significant growth prospects in terms of the potential for further implementation. The widespread use of chatbots is associated not only with the low cost of implementation, but also mainly with the transparent value for businesses and end users.

The high percentages of positive responses in the "AI-agents and applications" category are due to the fact that a low entry threshold is typical for starting experiments with these AI solutions, including due to the use of a cloud-based delivery model for most of the products studied. Also, the positive attitude of market participants regarding AI solutions can be compared with the fact that developers of application software, cybersecurity solutions and platform solutions are actively striving to integrate products of these subcategories into their own end products.

The subcategories related to Natural Language Processing (NLP) and Computer Vision (CV) are more in demand relative to other solutions that are specialized and used to solve narrowly focused tasks, for example, Recommendation Systems, Predictive Analytics Platforms and AI RPA.

AI platforms



For all the listed subcategories, there is a relatively low level of current implementation (11–20%), but we can also note a high potential for further development, calculated as the sum of the responses "planning" and "testing" (27–32%).

Along with automated AI solutions that are delivered using the cloud model, large and major companies actively consume the services of consulting companies and system integrators. These market participants are actively implementing AI products, including providing training, technical support, model training, and more.

The respondents actively noted the development of a data-driven approach in their own companies, in particular, many highlighted the systematization of the process of accumulating business data. Not only advanced AI tools are crucial for the implementation of this approach, but also basic cloud-based, in particular, analytical tools, without which it is impossible to fully benefit from the use of AI.

The development of AI technologies is directly related to the penetration of certain subcategories into cloud technologies. There is a direct connection between these interdependent technologies. Further development of cloud computing and storage systems, as well as platform solutions, will significantly increase the availability of AI technologies and reduce barriers for all business segments and industries.

★ — high potential

CONCLUSION

“

Cloud technologies, cybersecurity, and artificial intelligence are not just developing in parallel — they form a closely interconnected ecosystem where the success of one area largely depends on the maturity of the others. Such synergetic growth is the basis for ensuring the competitiveness of both individual corporate customers and the national economy as a whole.

Cloud technologies, primarily the IaaS and PaaS segments, remain the most dynamically developing part of the Russian IT market. Cloud technologies continue to be the most dynamically developing part of the Russian IT market. In 2025, they will grow by 24% and reach 208 bn rubles. According to recent estimates, their combined share reached about 5,1% of the total market in 2024, and may exceed 5,2% in 2025. For a significant number of companies, virtual data centers and virtual private clouds have actually become an infrastructure standard — a commodity product. At the same time, the market is showing steady interest not only in public, but also in private and hybrid scenarios, which meets the growing demand for vendor lock-in manageability, customization and risk reduction. The largest clients are generating demand for multi-cloud models and are actively testing approaches that combine different providers to solve problems of fault tolerance and service differentiation.

Cybersecurity, in turn, is becoming an integral element of all digitalization strategies. In terms of supply, the domestic market already has a wide range of proprietary solutions covering most critical areas. This allows companies to ensure compliance with regulatory requirements and at the same time reduce dependence on foreign suppliers. In general, it can be noted that the cybersecurity sector in Russia is at the stage of technological stabilization, but retains the potential for evolutionary growth, primarily through the expansion of functionality, automation and the introduction of intelligent protection mechanisms.

The AI market in Russia is still at an earlier stage of the formation of sustainable corporate practices. Comparatively modest indicators of the implementation of high-performance computing infrastructures (GPU VM and NRS) are visible — the demand for these resources is mainly provided by companies with strong in-house Data Science teams, whose share is only a third of the market.

If we consider technologies from a product point of view, then AI stands out as having the greatest development opportunities. Solutions in this area have a high prospect of further development for most products (97% of areas have a high prospect of further development). Cloud technologies have a higher percentage of implementations, but at the same time, fewer areas with significant growth potential (only 42% of such areas). Cybersecurity technology showed the lowest reserves in the allocated subcategory (about 30% of areas have high growth potential). Such data may be related to the significant relevance of cybersecurity risks for Russian companies.

Based on the complementary product analytics of the offer, in particular, in cloud technologies, it should be noted that for the vast majority of product lines, domestic providers have a well-formed portfolio of solutions of their own design or modified open source. It seems that the current market supply is sufficient to meet not only basic technological needs, but also for experimental and innovative activities of companies.

Igor Zarubinsky
MWS Executive Director, CEO MWS Cloud

KEY TERMS

PUBLIC CLOUD

A cloud computing model in which the IT infrastructure (servers, data warehouses, networks) is owned and managed by a third-party provider, and resources are delivered over the Internet. Users (companies or individuals) share this infrastructure.

PRIVATE CLOUD

A cloud infrastructure deployed and used exclusively by a single organization. It can be physically located in the company's own data center (on-premise) or at a third-party provider, but all resources are completely isolated and intended for only one client

HYBRID CLOUD

An IT environment that combines a private cloud with one or more public clouds.

ON-PREMISE

A model in which the IT infrastructure (servers, software, networks) is deployed and managed directly on the company's territory, in its own data center.

MULTICLOUD

A strategy for using services from two or more public cloud providers at the same time.

MTC Web Services (MWS)

Cloud services and Enterprise-level products for AI-experiments and digital transformation of business. The company offers advanced technologies, in-depth expert review, comprehensive support and reliable infrastructure to help customers reach new heights. MWS solutions include: compute and storage services, infrastructure for training AI and ML models, databases, business applications, network services and solutions for developers

MWS Intelligence Team

The team is responsible for leadership in analytics and research in the Russian cloud market. We aggregate the best global and Russian practices in the field of clouds, artificial intelligence, cybersecurity and information technology in general