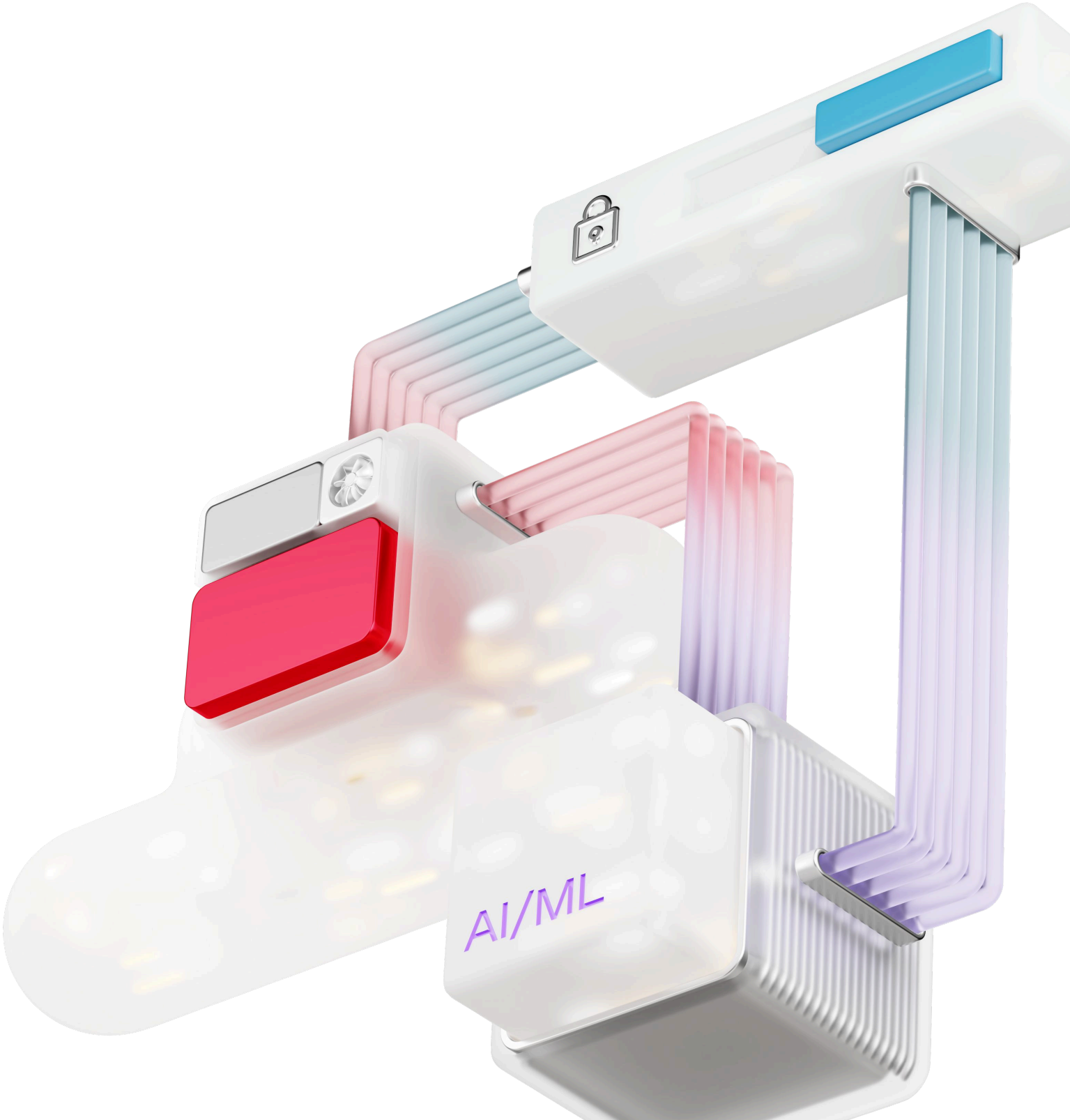
俄罗斯企业技术战略



俄罗斯企业技术战略

本报告由分析研究中心(MWS)编制

如对本研究有疑问和意见或有合作想法，请发送至邮箱：
Intelligence_Team@mts.ru

专家

Pavel Voronin

MWS 总经理

Igor Zarubinsky

MWS 执行董事，
MWS Cloud 首席执行官

Denis Filippov

MWS AI 总经理

Danila Egorov

MWS Cloud 业务战略总监

Mikhail Tutaev

MWS Cloud 产品总监

Polina Lee

MWS Cloud 分析与研究中心负责人

Galina Gaydarhzhi

MWS Cloud 业务分析师

目录

引论

前言

分类体系

方法论

前言

总体技术，尤其是面向 B2B 的 IT 技术，呈现出以“大浪潮”形式发展的特征。20 世纪 90 年代以个人计算机、软件以及 PC 操作系统为主要特征。21 世纪初期，企业普遍实施互联网技术并采用单体式平台。2010 年代，企业开始向云计算迁移。每一轮浪潮都彻底重塑了 IT 技术格局。

> “ 作为俄罗斯关键的大型科技公司之一，我们看到，AI 智能体已经在根本性地改变企业管理、客户服务以及数字产品发展的方式——从对日常事务的自主处理，到对复杂管理决策的实时支持。我们正在打造领先技术：发展云计算，构建平台与数据平台，推出开发者工具，使 AI 智能体能够直接部署到业务流程中，并将其影响力扩展至整个经济体系。

Pavel Voronin
MWS 总经理，MTS IT 第一副总裁

到 2025 年，我们观察到新一轮技术浪潮——人工智能——正在迅速塑造新的 IT 技术格局。与此同时，云计算持续增长，俄罗斯拥有超过 1 拍字节数据规模的企业数量在一年内从 10 家增长至 29 家。

> “ 未来五年内，人工智能的实施将催生一种新的 IT 架构，其中 AI、平台与云计算将形成统一的技术栈。在这一技术栈基础上，将创建 AI 智能体——数字化员工。产品价值将不再体现在软件这一工具本身，而体现在业务任务完成所带来的实际结果。软件用户将从任务执行者转变为智能体的管理者。这将形成一种全新的技术型经济。

Igor Zarubinskiy
MWS 执行董事，MWS Cloud 首席执行官

任何技术的创造都始于客户。正是客户向我们明确表达其产品需求，指出不足并提出改进要求。我们对客户的反馈表示由衷感谢。我们相信，只有对客户需求的深刻理解，才能孕育出卓越的技术。今年，我们决定聚焦于俄罗斯变化最为迅速的三大技术领域。

它们分别是云计算、人工智能和网络安全。本研究基于来自 700 家俄罗斯企业代表的调研反馈。我们衷心感谢所有参与者拨冗参与并提供宝贵意见。

> “ 在MWS，我们坚持开放原则，因此与您分享研究成果，并将研究报告向公众开放。我们希望本研究能够为您这项艰巨而又极其重要的工作提供切实帮助。感谢您所做的一切！

Danila Egorov
MWS Cloud 业务战略总监

分类体系

本研究所采用的方法基础是 IT 市场结构，该结构首次在《IT 市场前景》研究中提出。根据 MWS 的分类体系，整个市场被划分为三大垂直领域：（1）Software（软件），（2）Hardware（硬件），（3）IT-Services（IT 服务）。每一垂直领域均被进一步拆解，并涵盖三大核心技术方向的解决方案：云计算、网络安全和人工智能。

2019—2024 年期间，俄罗斯 IT 市场在全球市场中的占比保持稳定，约为 1,1%—1,3%。与此同时，关键经济领域持续推进的数字化转型，推动了 IT 在国家 GDP 中渗透率的提升。2023—2024 年期间，该指标增长了 0,27 个百分点，高于其他国家的同类水平。

2019—2024 年间，俄罗斯 IT 市场的增长速度与全球水平基本相当。但其支出结构存在显著差异。在俄罗斯，硬件领域的占比较低，这在很大程度上源于其他国家在高科技组件制造方面的地理和产业专业化，以及软件解决方案作用的不断增强。此外，企业持续向云消费模式转型，也影响了 Hardware 领域的动态，降低了对自有计算能力采购的需求。云解决方案的扩展和效率提升进一步强化了这一趋势，有助于终端用户。

> “ 软件纵向领域呈现出持续、稳定的增长态势——无论是在俄罗斯，还是在全球市场。2019—2024 年期间，该细分领域在 IT 市场中的占比年均增长约 2%。主要驱动力来自企业向订阅制模式的转型，这使软件对不同规模的企业更加可及，并降低了新技术解决方案试用的门槛。

Pavel Voronin
MWS 总经理，MTS IT 第一副总裁

IT 服务细分领域在三大核心垂直领域中表现出最低的增长速度。该领域的发展受到宏观经济不稳定、部分市场饱和，以及向 no-code 和 low-code 解决方案转移的影响，这些方案在一定程度上替代了传统服务。与此同时，预计网络威胁数量的增加以及基于人工智能产品的快速发展，将在短期内支撑对 IT 服务的需求。

云计算市场值得特别关注：预计到 2030 年，其在俄罗斯 IT 市场中的占比将达到 6%。以货币计算的高年均增长率（2021—2024 年期间为 32%）为市场在中期内的显著发展创造了条件。云解决方案正成为俄罗斯企业数字化转型战略的关键组成部分，为企业提供灵活性并降低基础设施成本。

俄罗斯 IT 市场结构

	2023 年	2024 年	2025 年	2026 年	2027 年	2028 年	2029 年	2030 年
俄罗斯市场规模, 十亿卢布	2 702	3 302	3 992	4 700	5 478	6 260	7 090	8 004
硬件，十亿卢布	725	842	945	1 085	1 249	1 429	1 626	1 839
软件，十亿卢布	1 063	1 404	1 816	2 236	2 686	3 105	3 548	4 031
IT服务，十亿卢布	913	1 056	1 231	1 379	1 543	1 726	1 916	2 134
硬件，%	27%	25%	24%	23%	23%	23%	23%	23%
软件，%	39%	43%	45%	48%	49%	50%	50%	50%
IT服务，%	34%	32%	31%	29%	28%	28%	27%	27%

2023–2030 年俄罗斯 IT 市场中云计算细分领域占比

	2023 年	2024 年	2025 年	2026 年	2027 年	2028 年	2029 年	2030 年
云计算在俄罗斯 IT 市场中的占比	4,4%	5,1%	5,2%	5,3%	5,4%	5,6%	5,8%	6,0%

在云计算解决方案的发展中，IaaS / PaaS 子细分领域尤为值得关注。该类解决方案约占整个云计算市场的 65%，是行业增长的核心驱动力。需求增长不仅来源于传统云解决方案需求的提升，也得益于人工智能技术的发展。

俄罗斯 IT 市场在国家经济中的渗透程度

2,2%
2025 年 IT 在俄罗斯 GDP 中的占比

→

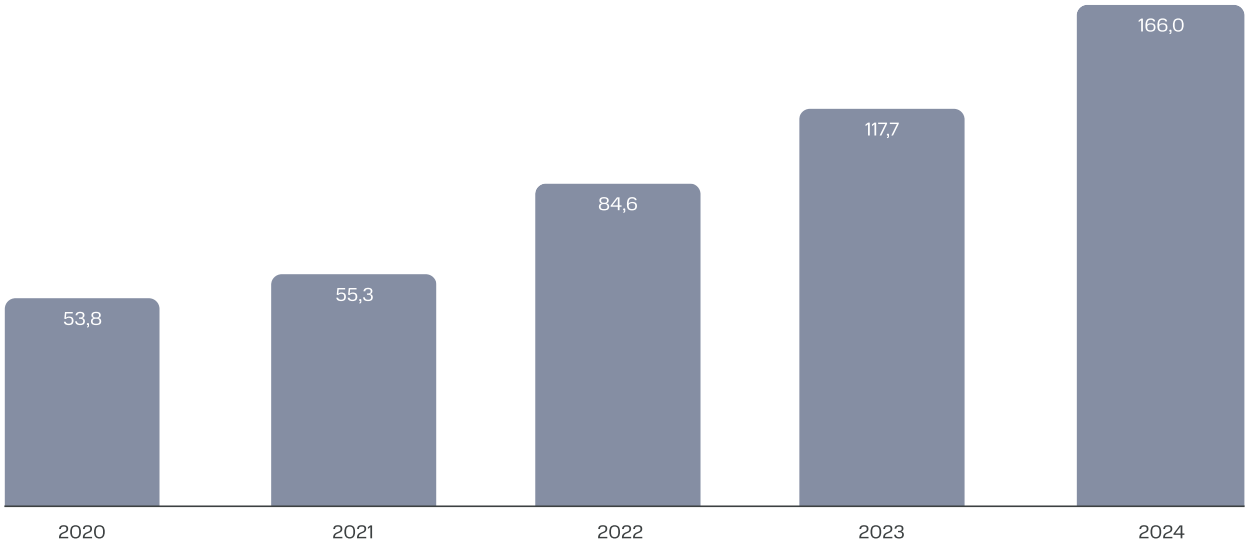
3,1%
2030 年 IT 在俄罗斯 GDP 中的占比

IaaS / PaaS 子细分领域在俄罗斯 IT 市场结构中表现出最高的增长速度之一。2021—2024 年期间，年均增长率约为 30%，表明云技术在企业领域的快速普及。与此同时，IaaS / PaaS 的增长速度呈现逐步放缓趋势，反映出市场成熟度的提升：2024 年市场规模较上一年增长 32%。

有关 IT 市场结构的更多内容，详见研究报告《IT 市场前景》。

俄罗斯 IT 市场中云计算细分领域规模

市场规模以十亿卢布计



> 尽管在中期内 IT 市场各方向均被预测将持续增长，但目前我们观察到其结构正发生质的变化，软件（Software）占比持续上升。预计 2023—2030 年期间，软件的年均增长率将达到 20,6%，而 IT 市场整体年均增长率为 17,4%，这反映了企业向更加灵活、经济的消费模式转型。关键行业数字化进程的加速，为 IT 在国家经济中的占比实现可持续增长奠定了基础。在我们的战略愿景中，我们坚持这样一个认知：“软件即 IT 市场”。

Igor Zarubinskiy
MWS 执行董事，MWS Cloud 首席执行官

方法论

本研究是此前《IT 市场前景》研究的逻辑延续，重点从需求侧对市场状况进行评估。研究结果将对致力于通过实施数字化技术提升效率的企业尤为有价值，尤其适用于分析、销售、产品管理、战略与市场营销团队，以及负责关键决策的管理层。

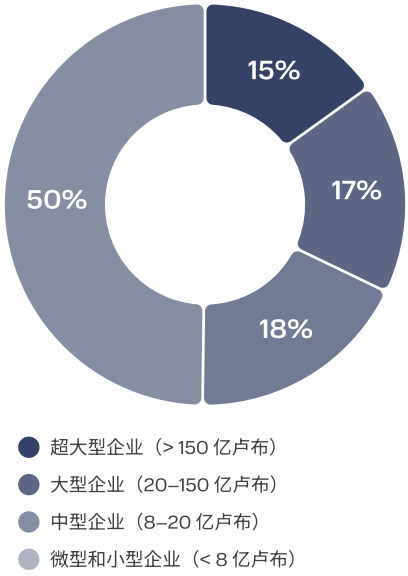
本研究以对 700 余家俄罗斯企业代表开展的问卷调查为基础。为进一步深化对部分研究议题的理解，研究团队还对部分受访者开展了深度访谈。

样本仅包括已确认在采购、发展或运营活动中至少一项投入预算的企业，该三项技术包括：云计算解决方案、网络安全和人工智能。

研究样本在不同业务规模的企业之间分布均衡。其中，微型和小型企业占样本的 50%，其余 50% 由中型、大型及超大型企业构成，且分布相对均衡。

按企业规模划分的受访者结构

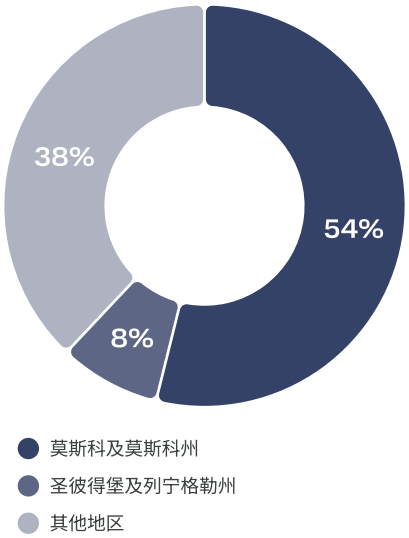
营业收入规模（卢布）



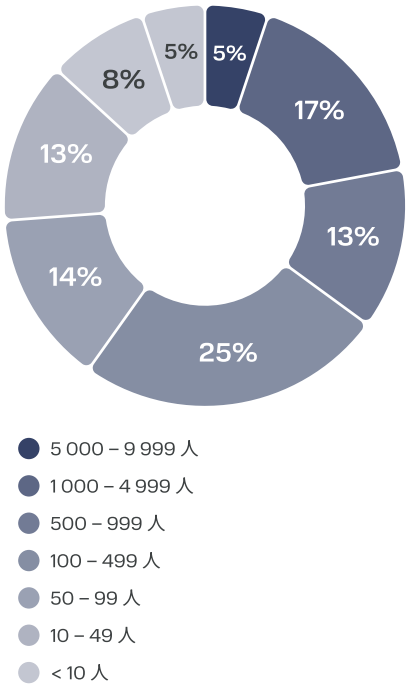
按行业划分的受访者结构

多数受访企业位于莫斯科及莫斯科州，但超过三分之一的样本来自地区性企业，从而确保了广泛的地域覆盖。从员工规模来看，样本同样具有多样性：26% 的企业属于员工人数少于 100 人的小型企业，大型企业（1 000–4 999人）和超大型企业（5 000–9 999 人）的占比分别为 13% 和 17%。

按公司总部所在地划分的受访者结构



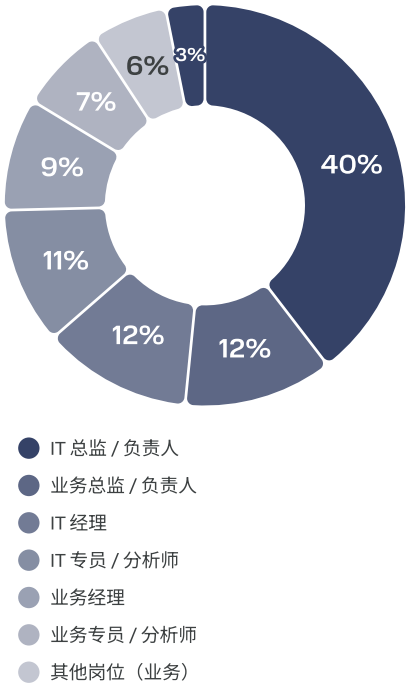
按员工人数划分的受访者结构



本次调研面向在数字化解决方案发展方面具备专业能力的人员开展。之所以覆盖不同层级的员工，是因为数字化转型的组织方式在很大程度上取决于行业特性及企业内部业务流程。超过一半的受访者来自高层管理团队，这凸显了样本企业代表所具备的高水平专业能力。

因此，该样本结构能够代表已实施或使用相关技术的俄罗斯企业整体情况。受访者所具备的高水平专业能力保证了数据的可靠性，并使研究团队能够就俄罗斯企业对云计算解决方案、网络安全技术及人工智能的当前与潜在需求作出有依据的判断。

按参与调研员工职务划分的受访者结构



MTC WEB SERVICES

大型科技公司，提供云计算与 AI 服务及平台化解决方案，覆盖多样化业务场景：从数据处理到产品开发与业务流程优化。

15 个

基于 Tier III 级数据中心的可用区

~ 280 000

公里的自有通信网络

支持标准

保护级别 -1、GIS K1、152-FZ、PCI DSS, 国家标准（GOST） R 57580

№ 1

2024 年企业级 IaaS 排名

前五

根据 Mera 评估，位列俄语 AI 解决方案

前三

在人脸识别算法质量方面，位列 NIST 基准测试

1,500 万

生态体系用户

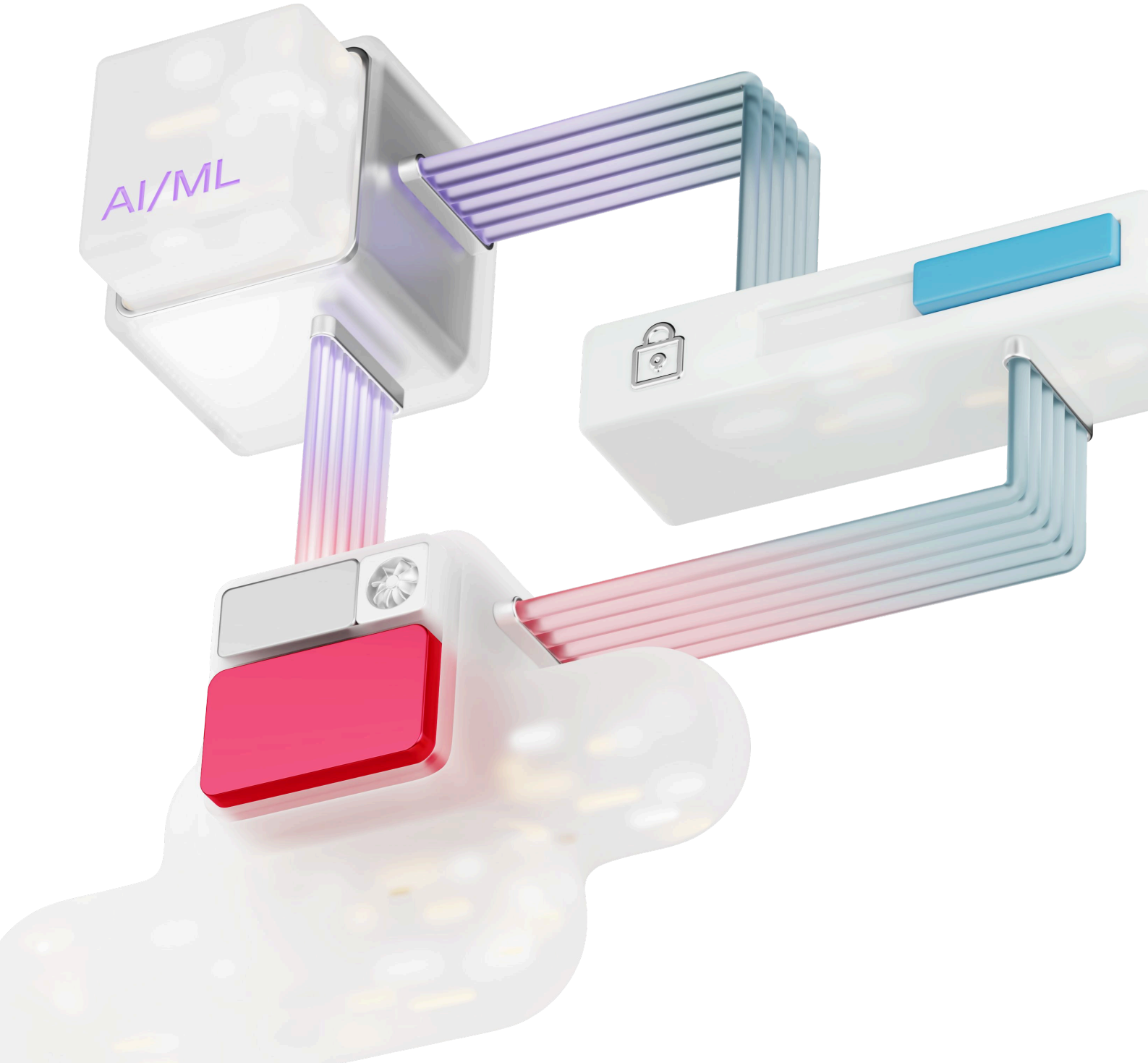
№ 1

GPU CLOUD 排名第 1

№ 1

俄罗斯代码生成准确率最高的大语言模型（LLM）

企业技术战略



IT 预算

2024 年，俄罗斯企业的 IT 预算平均占年收入的 2–3%，这一水平与全球实践基本一致。根据 Gartner 的研究，2024 年全球企业 IT 支出占收入的中位数为 3,1%。从绝对规模来看，超过 65% 的受访俄罗斯企业年度 IT 预算不超过 1 亿卢布，仅有 14% 的企业 IT 预算超过 10 亿卢布。

IT 预算规模最高的四大行业：IT、金融与保险、矿产资源开采与加工、娱乐与媒体

按行业划分的受访企业 IT 预算

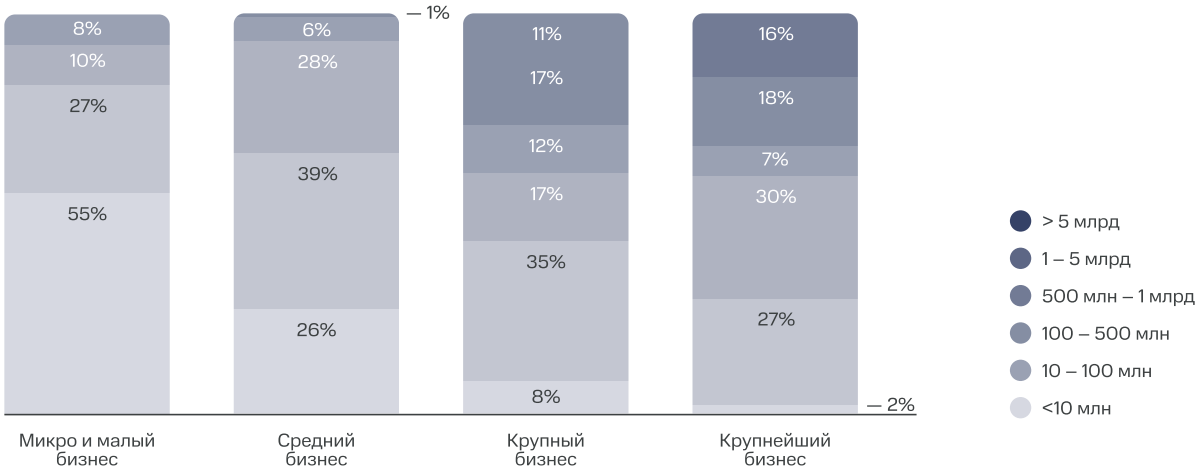
	< 1,000 万	1,000–1 亿	1–5 亿	5 亿–10 亿	10–50 亿	> 50 亿
IT	24%	28%	13%	13%	11%	10%
金融与保险	33%	19%	11%	8%	20%	9%
矿产资源开采与加工	33%	32%	8%	7%	11%	9%
娱乐与媒体	22%	25%	36%	6%	3%	8%
保健事业	33%	39%	15%	4%	4%	5%
专业服务	53%	25%	5%	12%	1%	4%
HoReCa	43%	30%	13%	6%	5%	3%
科学教育	37%	27%	20%	4%	3%	3%
零售业	54%	26%	8%	4%	4%	3%
房地产	54%	26%	9%	3%	5%	2%
交通与物流	45%	23%	18%	10%	1%	2%
工业	46%	37%	7%	6%	4%	2%

IT 预算在不同行业和企业规模之间仍呈现出高度分化。IT 市场企业（其产品主要基于数字化解决方案）以及传统经济领域中的超大型企业（如工业、矿产资源开采）承担了最高的 IT 支出。这些企业同时在生产自动化与效率提升工具方面持续加大投资。

如预期所示，IT 预算规模与企业收入规模高度相关：
对于绝大多数微型和小型企业（收入低于 8 亿卢布，占比超过 68%）IT 预算不超过 1,000 万卢布；而收入超过 150 亿卢布的超大型企业，其 IT 预算规模呈现出显著更高的多样性。例如，超过三分之一的超大型企业 IT 预算超过 10 亿卢布。随着收入规模的增长，IT 预算的差异性不断扩大，这反映了企业所面临任务的复杂性与多样性——从基础自动化与现有 IT 基础设施的维护，到更先进的 AI / ML 解决方案的实施。

ИТ-бюджеты респондетов по сегментам бизнеса

Каждый столбец — сегмент бизнеса на основе выручки, цветами обозначен размер ИТ-бюджета



对大多数企业而言，高效的 IT 预算管理意味着需根据业务重点和外部环境变化进行定期调整。无论收入规模如何，超过 60% 的企业每年会对 IT 预算进行 1–2 次调整。

随着企业规模的扩大，IT 预算的调整频率也随之提高：
在微型和小型企业（收入不超过 8 亿卢布）中，更常见的是一年调整次数少于一次的情况，这可能反映出数字化成熟度有限以及对成本更新机制的需求。而对于收入超过 150 亿卢布的超大型企业，年度预算更新最为常见，这可能与较长的财务审批周期以及年度战略规划目标的设定有关。

在 IT 预算执行过程中，不同技术方向的支出分布并不均衡。调研结果显示，在三大关键技术方向——云计算解决方案、网络安全系统以及人工智能——上的支出，占俄罗斯企业 IT 预算总额的 17%。

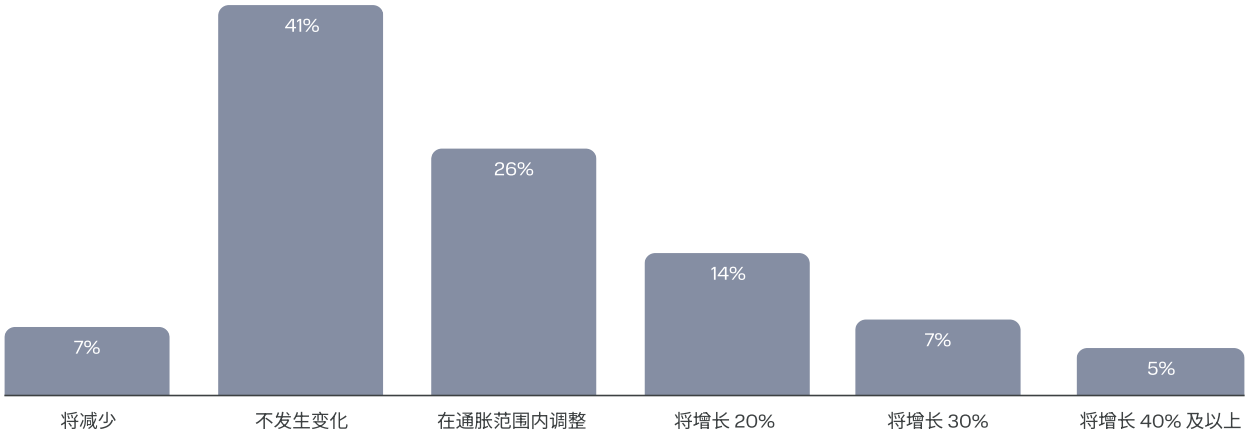
在上述技术方向的投入规模上，俄罗斯企业仍落后于国际同行，后者的相关支出占比可高达 50%。此外，全球与俄罗斯在 IT 预算结构上亦存在差异：在国际实践中，云计算支出居于首位，其次是网络安全，第三位为人工智能。而在俄罗斯，按预算规模排序，网络安全位居首位，其次是云计算，第三位为人工智能。这种差异可能与俄罗斯信息安全领域不断上升的风险有关。网络攻击总量持续上升，其中 DDoS 攻击以及针对大型企业、以窃取敏感数据为目的的攻击尤为突出，同时针对俄罗斯及独联体国家的 APT 组织数量也在增加。应对不断加剧的网络威胁，监管环境也随之趋严：2024 年，187-FZ 与 152-FZ 法规得到强化，同时出台了新的 FSTEC 监管规范。

云计算技术与网络安全在 IT 预算中的分布呈现非线性特征：
随着收入增长，其占比提高 1–2 个百分点，在中型企业（收入 8–20 亿卢布）中达到峰值，随后这些技术的占比出现下降。这一趋势可能源于网络安全技术在部署阶段所需的较高最低投入门槛，而其后续扩展与运行维护成本相对较低。人工智能在 IT 预算结构中的占比保持在 2–4% 区间，且与企业收入规模之间不存在显著差异。

> “ 在威胁形势加剧及监管压力增强的背景下，市场正逐步转向在基础 IT 基础设施、网络安全与先进数字化解决方案之间进行更加均衡的投资配置。与此同时，IT 行业对全球 GDP 的贡献约为 2,62%，比俄罗斯对应指标高出 43%。要达到这一水平，必须在最具前景的 IT 方向上实现超前投资增长，尤其是云服务和基于人工智能的解决方案，这些技术正在塑造企业效率与可管理性的全新水平。

Igor Zarubinskiy
MWS 执行董事，MWS Cloud 首席执行官

2025 年不同业务规模企业 IT 预算的预期变化



对云计算、网络安全和人工智能的投资正在成为各行业 IT 预算中的常规支出项目，从零售到工业领域皆是如此。这表明数字化战略日趋成熟，人工智能的应用实践正在向 IT 与金融以外的行业扩展。在传统上数字化程度较低的行业中，较高的投资水平表明技术进步与经济转型正在加速，其中云计算、网络安全和人工智能的实施是这一进程的重要组成部分。

仅有 28% 的受访企业计划将相关技术的预算增幅提高至高于通胀水平。人工智能是推动相关支出增长的首要方向。

在所有受访企业中，可以观察到企业收入规模与计划中的消费变化幅度之间存在直接相关性：企业收入越高，越倾向于制定扩大投资的计划，且增长幅度也越显著。这一规律适用于几乎所有技术类别，唯独云计算解决方案例外——其潜在使用扩展规模在不同企业规模之间分布相对均衡。人工智能被视为消费增长潜力最大的技术方向，这主要源于其当前实施水平仍然较低，同时在几乎所有行业中都具备显著提升业务流程效率的预期潜力。

在 IT 预算中云计算、网络安全与人工智能支出最高的五大行业

IT

金融与保险

娱乐与媒体

零售业

矿产资源开采与加工

企业技术战略云计算

云计算技术的实施战略是衡量俄罗斯企业数字化成熟度及其转型准备程度的关键指标。向云计算迁移不仅是技术决策，更是一项战略选择，直接影响企业的适应能力、成本控制以及创新速度。

44% 的企业已在战略层面实施云计算技术，这表明俄罗斯云计算市场正在发展，但尚未达到饱和状态。

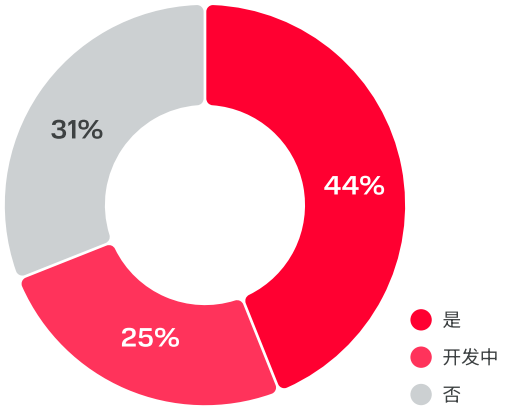
这反映出企业对云计算价值的认知不断提升，包括灵活性、可扩展性以及成本优化能力。此类企业可被视为“成熟的云计算用户”。在系统性使用云计算解决方案方面仍存在增长空间，这为云服务提供商创造了重要的发展窗口。

约四分之一的企业仍处于战略制定阶段，表明其正处在认知深化与基础设施准备期。这些企业很可能已感受到数字化转型的现实需求，但尚未进入系统化落地阶段。

该类企业对外部刺激最为敏感，无论是监管要求还是市场竞争压力。这一群体有望成为下一轮对基础设施、培训及迁移支持服务需求增长的主要来源。

近三分之一的企业尚未制定任何云计算战略。这一现象可能由以下因素导致：（1）资源或专业能力有限的中小企业；（2）来自传统或高度监管行业（如工业领域）的企业，其云迁移受到安全与合规限制；（3）对云计算潜力认知不足，或管理层对变革存在抵触。

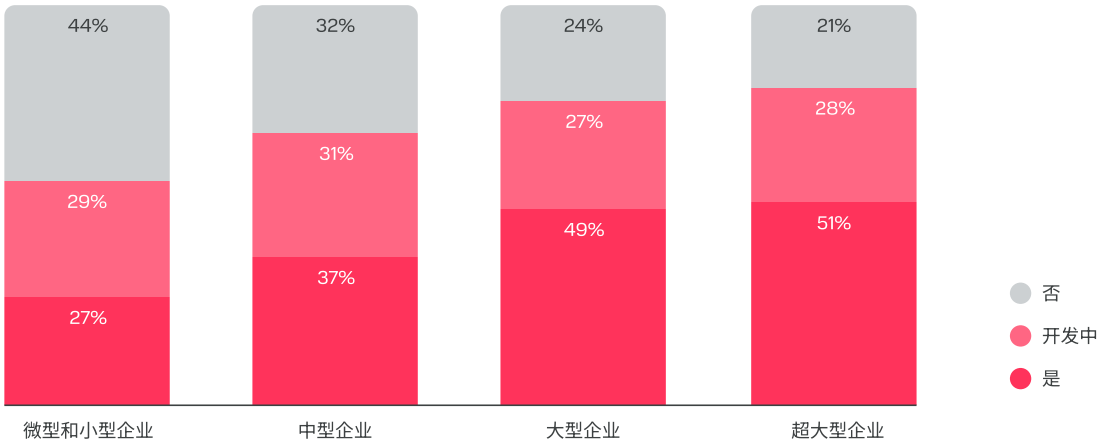
是否具备云计算实施战略



调研显示，企业收入规模与是否已形成云计算战略之间存在显著相关性。这直接反映了企业在资金获取能力、IT 能力水平以及数字化成熟度方面的差异。

企业规模与是否具备云计算战略呈正相关关系。在超大型企业（收入超过 150 亿卢布）中，对云计算战略规划的参与度最高，其中 51% 的受访者表示已具备相关战略。对于大型企业（收入 20–150 亿卢布），该比例略低，为 49%。准备程度最低的是微型和小型企业（收入不超过 8 亿卢布）：其中 44% 完全没有云计算战略，这是所有受分析业务规模中占比最高的。这种差距通常源于对专业 IT 能力的获取受限，以及企业更优先解决当前运营问题，而非推进长期战略举措。

是否具备云计算实施战略

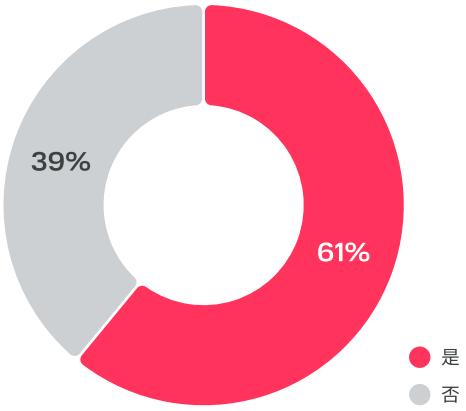


从云计算战略的具备情况来看，可将各行业划分为三大类:（1）成熟行业（超过 50% 的企业已具备云计算战略）。这些行业在云计算领域表现出较高的成熟度。值得注意的是，该组行业中处于战略制定阶段的企业比例也较为可观，约为 16%，表明其对云计算持续保持高度关注并积极推进相关工作。该类行业包括 IT、交通与物流、工业以及金融与保险。（2）中等成熟度（30–49% 的企业具备云计算战略）。该组涵盖了本次研究范围内的大多数行业。在这些行业中，云计算战略的制定与缺失并存，整体呈现出不均衡、碎片化的特征。该类行业包括娱乐与媒体、医疗健康、专业服务、建筑业及公用事业。（3）战略成熟度较低（云计算战略覆盖率低于 30%）：
在这些行业中，45–60% 以上的企业完全未制定云计算战略。这既可能反映出更为保守的经营方式，也可能表明在云计算落地过程中存在监管、技术或组织层面的障碍。

该类领域包括餐饮与酒店业（HoReCa）、科研与教育。

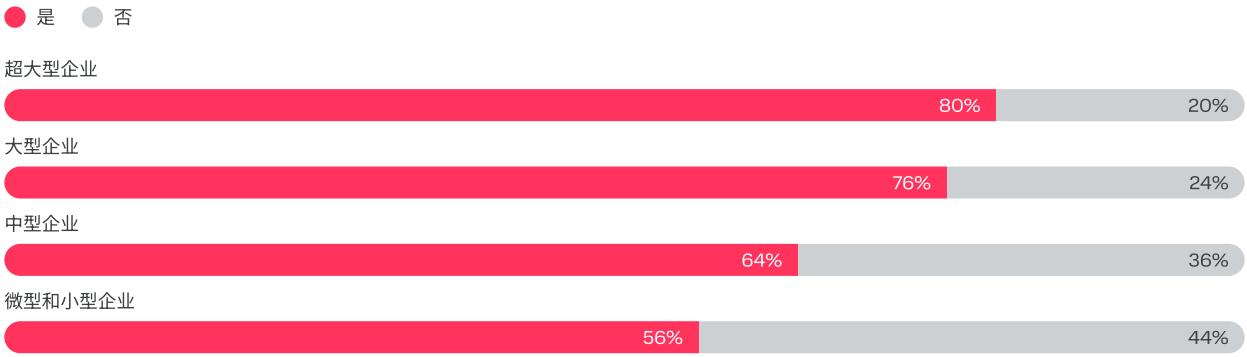
具备云计算专业能力已成为衡量企业数字化成熟度的关键指标之一，并直接关系到企业高效扩展基础设施、管理风险以及实施向混合云与多云模式转型战略的能力。在云计算解决方案方面，已具备成熟专业能力与仍处于能力建设阶段的企业之间，形成了一条明显分界线：前者能够主动构建和演进云架构，而后者仍将云计算更多视为潜在发展方向，而非系统性转型工具。同时，已形成云服务发展战略的企业比例，低于具备云计算专业能力的企业比例。这意味着，部分具备云计算能力的企业仍局限于有限的应用场景，尚未实现全面规模化或 IT 架构的系统性转型。

是否具备云计算实践经验与专业能力



具备实践经验并不必然意味着实践成熟。在许多情况下，企业仅实施了单点服务，如数据备份或企业邮箱，而尚未向采用 CI/CD、自动化运维、FinOps 以及 SLA 管理工具的先进架构转型。随着企业规模扩大，其云计算专业能力水平通常随之提升，因为大型企业在人才招聘与员工培训方面具备更强的资源优势。这一分布同样反映了战略优先级的差异.大型企业更频繁地推进大规模数字化项目，投资于 DevOps 与多云架构，设有独立的 IT 部门并具备清晰的 IT 战略。

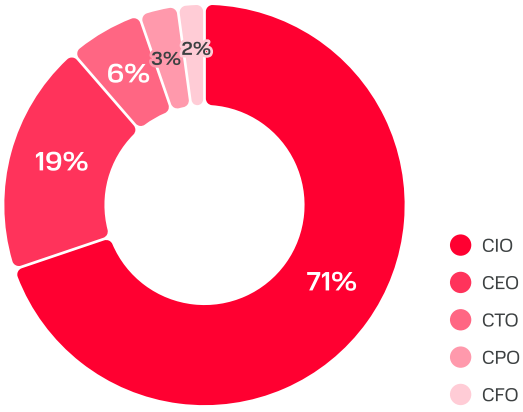
不同业务规模企业的云计算实践经验与专业能力



从行业维度来看，整体格局更加分散。在云计算专业能力方面，领先行业包括 IT（90% 的企业具备相关能力）、金融（84%）以及媒体与娱乐（79%）。这些行业的高参与度，要么源于其行业本身属性（如 IT 行业），要么来自对快速市场响应、灵活扩展能力或高安全标准的客观需求。

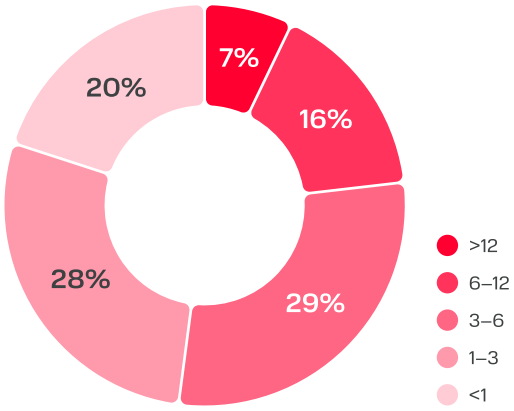
因此，云计算领域的专业能力在不同行业之间仍呈现出显著不均衡的状态。

云迁移过程中的关键决策人 (DMP)



云迁移周期

以月计



在大多数企业中，是否迁移至云计算的决策由 C 级管理层作出。

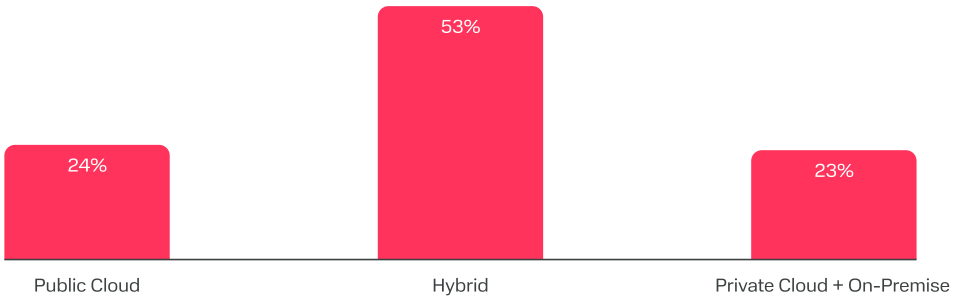
在约五分之一的案例中，云迁移决策由 CEO 直接作出，这表明最高管理者的战略参与度仍有限，而这种参与恰恰有助于促进 IT 与业务的协同并加速转型进程。

云迁移周期与企业规模及 IT 架构复杂度之间存在显著相关性。20% 的企业在一个月内完成迁移，这通常意味着其 IT 架构较为精简、迁移范围有限。最常见的迁移周期为 1–6 个月（占 57%），对应中等或较高复杂度的转型与架构重构场景。与此同时，23% 的企业迁移周期超过一年，这通常出现在 legacy 系统占比较高、安全合规要求严格或高度受监管的组织中。

Multicloud已成现实：41% 的企业使用多个云服务提供商

基础设施部署模式（多选）

多选



Public Cloud与多云模式的采用率均为 36%，这反映了企业对灵活性、可扩展性以及风险多元化的追求。由于本次调研允许多项选择，数据证实了采用组合式架构的趋势：多数企业同时使用多种部署模式，以在安全性、经济效率与基础设施稳定性之间实现平衡。这表明企业的 IT 战略已趋于成熟，并对基础设施架构采取了理性且有意识的规划方式。

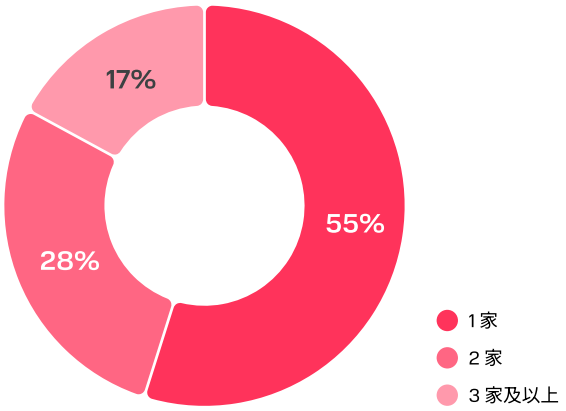
大型企业（收入 20–150 亿卢布）及超大型企业（收入超过 150 亿卢布）更倾向于选择私有部署及本地化（On-Premise）解决方案，强调安全性、监管合规要求以及对外部风险的抵御能力（例如制裁或外部云服务商故障）。相比之下，微型和小型企业（收入不超过 8 亿卢布）在基础设施选择上更具灵活性和创新意愿，因此更积极采用Public Cloud与多云解决方案，以降低基础设施成本。

企业规模越大，Multicloud解决方案的采用比例越高

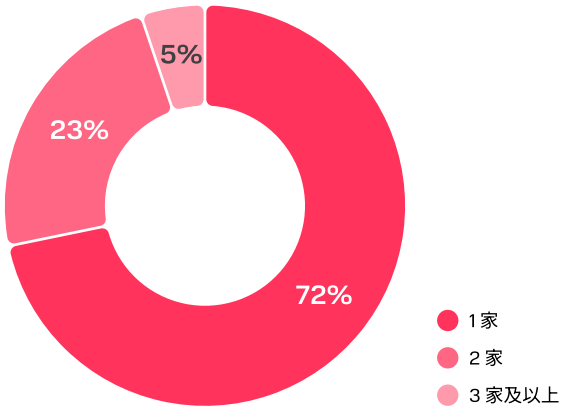
> 多云架构正逐步成为成熟企业的行业标准。随着云服务提供商数量的增加，基础设施的复杂性也随之提升。这对人员能力提出了更高要求，并推动 DevOps / FinOps 实践的发展以及运维管理自动化水平的提升。选择单一云服务商的企业通常更侧重架构简化与成本控制。而采用多云架构的企业则更注重系统韧性、灵活性与创新能力，但同时也面临更高的管理复杂度与额外成本。

Mikhail Tutaev
MWS Cloud 产品总监

使用的Public Cloud服务商数量



使用的Private Cloud服务商数量



在 Public Cloud 场景中，single-cloud 策略并不占主导地位，仅有 55% 的公司选择该模式。其优势在于简化管理、流程标准化，以及通过将服务集中于单一服务商来降低潜在成本。然而，该模式同时会加深对单一供应商的依赖，可能限制业务灵活性，并增加企业运营风险。

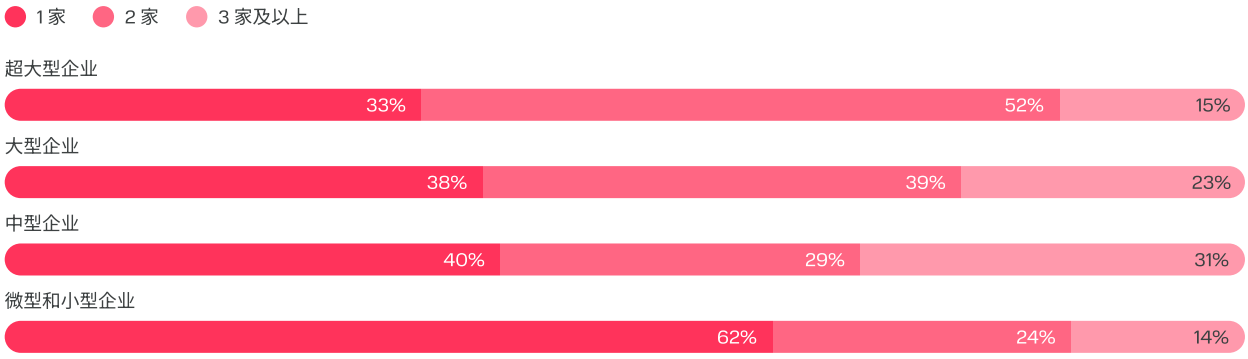
28% 的公司同时使用两家云服务商，通过引入 multicloud 元素实现风险分散、提升系统可靠性，并获取不同平台的差异化服务。17% 的公司使用三家及以上服务商，这已体现出更为成熟的分布式 multicloud 架构，通常出现在 IT 基础设施较为完善的组织中。使用云服务商数量最多的行业包括 IT、金融与保险、零售、工业以及 HoReCa。

因此，研究数据表明，企业在云环境管理方面采取了不同层级的策略，多云战略更常见于技术成熟度较高、力求在系统可靠性、多样化服务获取能力与基础设施可控性之间实现平衡的企业。

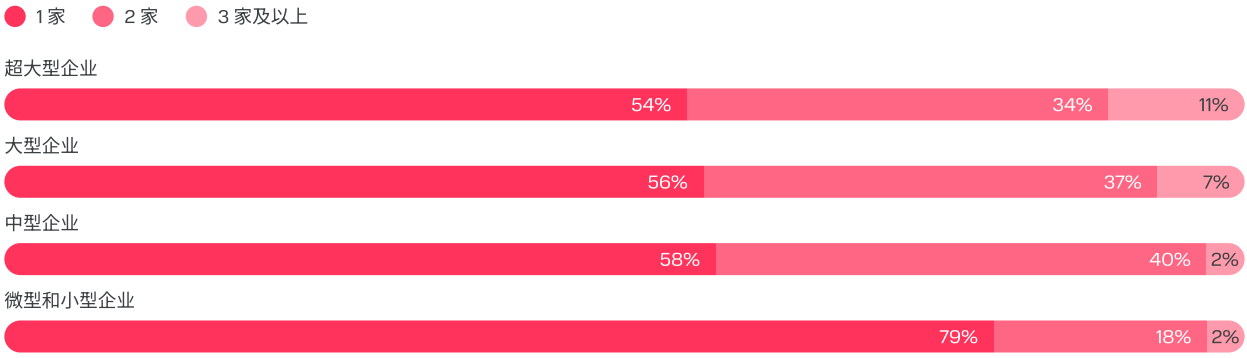
在Private Cloud领域也观察到类似情况。对大多数企业（72%）而言，选择单一服务商较为典型，这有助于实现基础设施的统一管理、SLA 的标准化以及运维工作的简化。该策略使企业能够在与单一供应商合作的情况下集中满足安全与监管要求，但同时也增加了对所选合作伙伴的依赖。

23% 的企业与两家服务商合作，这可能表明其力求降低运营和技术风险，并针对不同任务利用不同技术栈的优势。同时，Private Cloud环境中的多云部署通常出于关键服务备份以及提升系统可靠性的需求。

按业务规模划分的Public Cloud服务商使用数量



按业务规模划分的Private Cloud服务商使用数量



数据清楚表明，企业规模直接影响多云（Multicloud）策略的采用情况。大型企业更倾向于同时使用多家云服务商的产品和服务。除微型和小型企业外，大多数企业普遍积极使用多个Public Cloud平台：平均而言，61% 的企业已与两家及以上服务商合作，其中约 20% 的中型和大型企业使用三家及以上服务商的基础设施。这表明其云战略已具备较高成熟度。

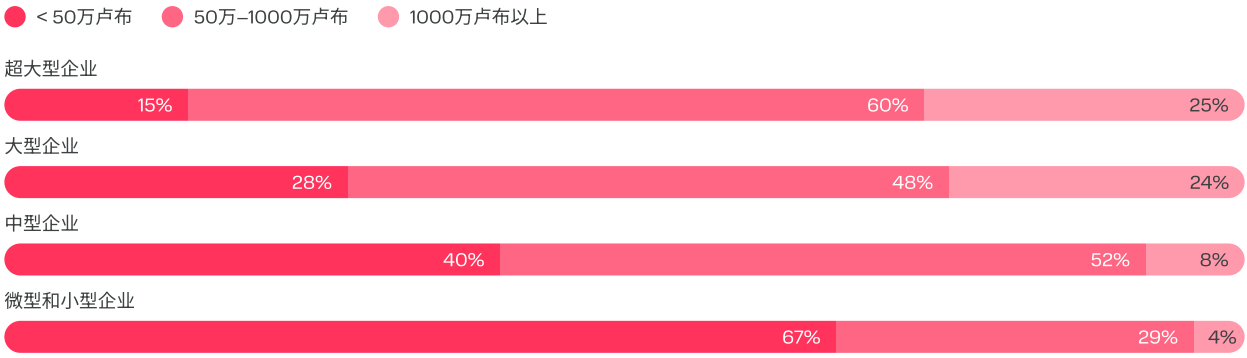
通常情况下，此类企业会按功能领域在不同服务商之间分配任务：部分用于数据存储，部分用于数据分析与人工智能、CI/CD，或用于备份恢复。这种方式能够提升灵活性和系统可靠性，并保障业务连续性。

同时，企业通过避免依赖单一供应商，有意识地降低供应商锁定风险。多云模式使企业能够进行负载均衡，基于成本和 SLA 选择平台，并更快地引入新技术。对于这些企业而言，多云已不再只是基础设施组成部分，而是用于风险管理、技术自主性以及加速数字创新的重要工具。

研究证实，企业规模与云技术投资规模之间存在直接关联。对于微型和小型企业（年收入低于 8 亿卢布）而言，云支出普遍较低：约 67% 的企业在云方面的投入低于 10 万卢布。这既与业务规模和组织结构复杂度有关，也与对系统可靠性、安全性及大数据处理能力的需求有关。大型企业则构建多云架构，发展数据分析、自动化以及高性能计算（HPC），并更频繁地开发自有数字化产品，这需要大量投资以及容器化服务和人工智能技术的引入。

相比之下，小型企业通常仅满足于基础 IT 需求，例如虚拟服务器、存储资源以及用于财务和文档管理的 SaaS 服务，从而将整体支出控制在较低水平。总体来看，市场中最具代表性的预算水平在 200 万卢布以内，这反映了整体数字化成熟度处于中等水平，同时企业需求差异显著。

按业务细分的年度云支出规模



> 俄罗斯云技术市场正明显向更大规模的预算迁移，这反映了企业对云基础设施的成熟度提升以及其战略重要性的增强。企业级市场正从局部试点阶段转向覆盖关键业务流程和服务的系统性转型。这意味着市场对综合型平台的需求持续增长，这类平台需要支持复杂的多云与混合云场景，在关键业务应用层面保障高可用性，并提供透明的成本管理机制。

Polina Li
MWS分析研究中心主任

按行业划分的年度云支出规模

	< 50 万卢布	50 万–1000万卢布	1000 万–1 亿
IT	32%	44%	24%
金融与保险	40%	48%	12%
零售业	50%	39%	11%
娱乐与媒体	44%	46%	10%
HoReCa	53%	37%	10%
科学教育	44%	48%	10%
房地产与建筑业	59%	34%	7%
交通与物流	53%	41%	6%
专业服务	76%	19%	5%
保健事业	74%	22%	4%
矿产资源开采与加工	49%	48%	3%
工业	69%	30%	2%

按行业划分的年度云支出结构有助于评估云技术落地的成熟度，并识别不同行业在战略路径上的差异。相当一部分企业仍集中在最低支出区间——每年不超过50万卢布。这一特征在专业服务、医疗健康等行业尤为明显，在这些领域中，云技术更多以局部应用的形式存在，尚未成为业务模式的核心。

成熟度最高的行业包括：IT、金融与保险、HoReCa、科研与教育——在这些行业中，超过10%的企业年度云支出已超过1000万卢布。这些行业普遍采用多云架构，积极推进 DevOps，并将云技术应用于关键业务流程。

在所有行业中均已出现云支出水平较高的企业，这表明市场开始出现分化：技术领先者正在构建更复杂的云使用模型，而大多数企业仍停留在基础应用阶段。未来，随着企业对云技术信任度的提升、自身能力的积累以及对监管要求的适应，高额云支出的占比有望进一步上升。

57%的企业计划扩大云技术的使用规模，这反映出云战略深化的节奏相对温和，部分原因在于市场逐步趋于饱和以及仍然存在的实施壁垒。同时，31%的受访企业计划发展Private Cloud，这表明企业对数据控制、本地化合规和安全要求的关注持续增强。Private Cloud解决方案正越来越多地成为混合云战略的核心，用于补充或替代本地部署（On-Premise）基础设施。

Public Cloud同样保持稳定需求：39%的企业计划扩大其使用规模，将其视为降低成本、加快数字化项目推进以及实现灵活扩展的重要工具。

总体来看，企业正在构建更加平衡的云策略：以Private Cloud作为风险管理和合规保障的优先选择，同时保留对Public Cloud的兴趣，用于优化成本和加速项目启动，从而推动混合云与多云模式的持续发展。

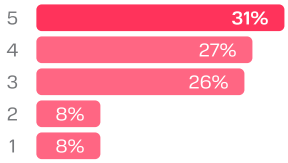
> “ 推动企业向云迁移的核心动力仍然是 IT 现代化、运营效率提升以及战略韧性增强。云解决方案使企业能够在无需大规模资本投入的情况下推进创新，实现基础设施自动化、优化成本，并更快速地应对外部变化。这些因素共同构成了持续而稳固的迁移动因，其中基础设施现代化是此类项目的首要驱动力。

Galinq Gaydarzhi
MWS Cloud 业务分析师

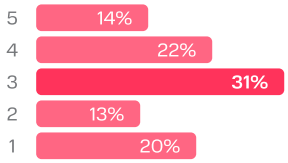
迁移至云计算的关键决策因素

受访者评分范围为1至5分，其中1分表示影响最小，5分表示影响最大

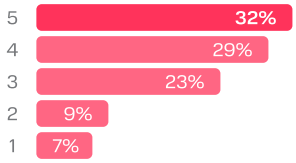
资源扩展能力



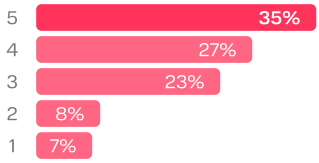
从 CAPEX 模式向 OPEX 模式转变



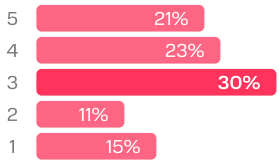
降低运维人力成本



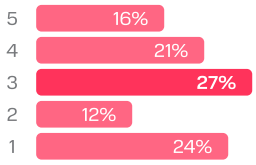
IT 基础设施现代化



缩短新产品的上市周期



无法采购设备



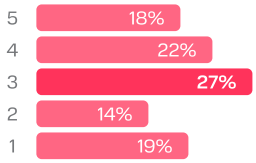
没有任何一项障碍因素获得压倒性的最高评分，这表明市场上已存在用于缓解这些问题的工具。然而，一些问题仍然具有现实意义，包括技术层面、组织层面、人力资源以及财务方面的问题。企业最常提到的问题是云支出预测的复杂性：近70%的受访者对此项障碍给出了3分及以上的评价，这表明当前在成本透明度和成熟的 FinOps 实践方面仍存在不足。

迁移过程中产生的额外成本依然显著，包括资源的阶段性双重投入、服务与许可费用、业务流程的适配，以及同时维护本地与云基础设施的需求，这些因素都会加重预算和团队的负担。

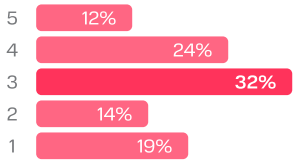
云迁移过程中的挑战 [1/2]

受访者评分范围为1至5分，其中1分表示影响最小，5分表示影响最大

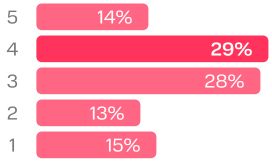
员工缺乏必要的专业能力



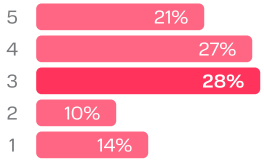
对所需基础设施预期成本的评估难度较高



需要在过渡阶段对基础设施进行临时性重复部署



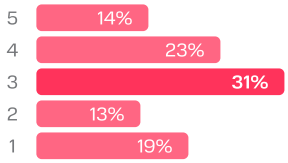
大规模数据迁移的复杂性



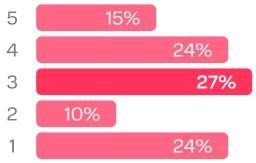
云迁移过程中的挑战 [2/2]

受访者评分范围为1至5分，其中1分表示影响最小，5分表示影响最大

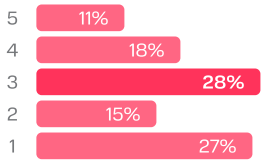
系统向云迁移阶段的额外成本



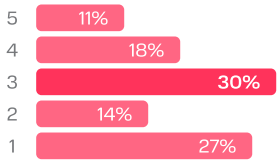
现有本地解决方案无法集成至云环境



迁移过程中缺乏厂商支持



缺乏清晰的迁移路线图



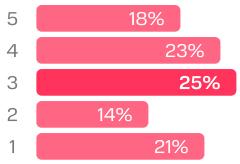
根据调研结果，企业并未将云迁移过程中产生的额外成本视为关键性障碍，这表明市场成熟度正在提升，企业已具备将相关支出纳入预算的能力。最常被提及的是测试环境部署成本：31% 的受访者认为其重要性处于中等水平，而超过 56% 的受访者认为其具有显著影响，这反映出通过试点项目降低风险的实践正在增加。与之同等重要的还有用于云集成准备的本地基础设施升级投入。

这表明，企业越来越倾向于提前规划试点和 On-Premise 升级预算，并将其视为云迁移的自然组成部分，而非临时性支出。

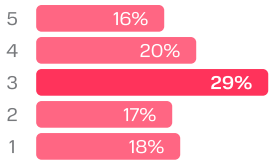
云迁移过程中的额外成本

受访者评分范围为1至5分，其中1分表示影响最小，5分表示影响最大

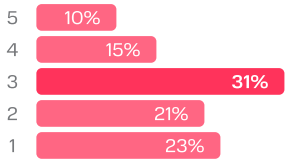
为高质量使用云环境而进行的员工再培训 / 招聘



本地基础设施升级



部署测试环境以验证所选解决方案的可行性



在各类风险中，企业最为重视的是个人数据泄露、商业机密泄露、网络攻击以及云服务商退出市场等威胁。对于采用多云和混合云架构的用户而言，信息安全问题尤为突出，这凸显了在设计此类架构时数据保护的重要性。其中，银行业表现出最高的敏感度。

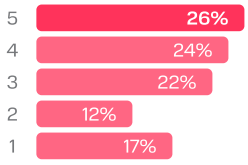
此外，由于供应商退出或制裁导致设备无法更新的风险也被单独指出。尽管对此看法不一，但在酒店餐饮业和工业领域，该风险被视为关键风险（40% 的受访者给予最高评分），这反映出这些行业的脆弱性。

与全球平均水平（69%）相比，俄罗斯企业对云成本超支的关注度较低（19%），这与多云架构的普及程度较低有关。总体来看，企业更关注网络安全和供应稳定性问题，而财务风险及服务功能不完整性则更多被视为可管理的障碍。

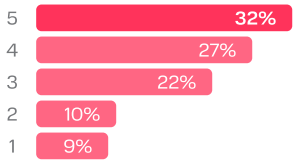
云迁移过程中的风险

受访者评分范围为1至5分，其中1分表示影响最小，5分表示影响最大

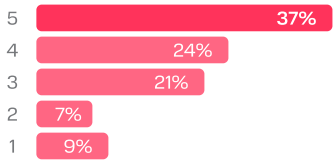
云服务商退出市场



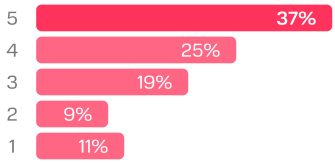
针对云服务商平台的网络攻击



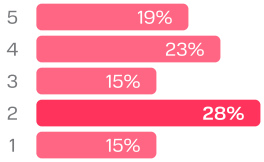
个人数据泄露



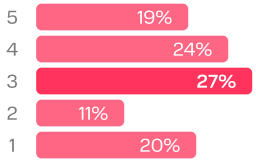
商业机密数据泄露



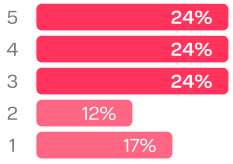
云基础设施成本的不可控增长



云服务商缺乏所需功能



因制裁导致供应商设备无法更新



关于云规模扩展的决策，越来越多地不仅基于技术因素，也被视为企业增长战略和数字化转型的一部分。经济可行性以及新型自动化系统的引入成为主要驱动因素，这两项因素均被 33% 的企业评为最高重要性。这表明，云技术正日益被视为实现成本优化、提升灵活性以及加速业务模式重构的重要工具。

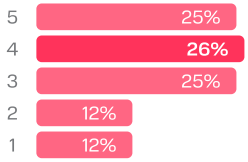
在缩减本地基础设施这一因素上也呈现出类似的趋势：33% 的受访者将其评为中等水平，另有 40% 赋予其较高优先级。这表明企业正逐步从 On-Premise 模式转向云计算，以降低 CAPEX，并过渡到更加可控、可管理的 OPEX 模型。

总体而言，企业正越来越多地将云作为战略重构的工具，这推动了云在 IT 预算中占比的增长，并将关注重点从技术因素转向业务驱动因素。

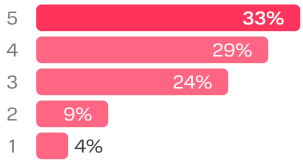
决定扩大云使用规模的关键因素

受访者评分范围为1至5分，其中1分表示影响最小，5分表示影响最大

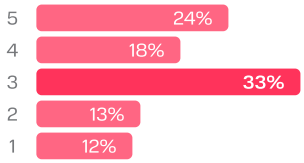
新产品发布



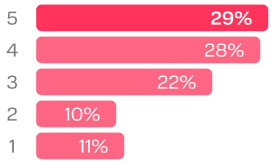
经济效益



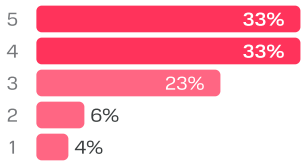
缩减本地基础设施（完全放弃）



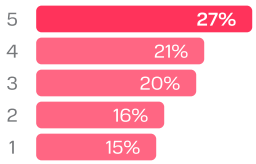
扩大客户基础 或提升现有产品产量



引入新的自动化系统



扩大公司的地域覆盖范围

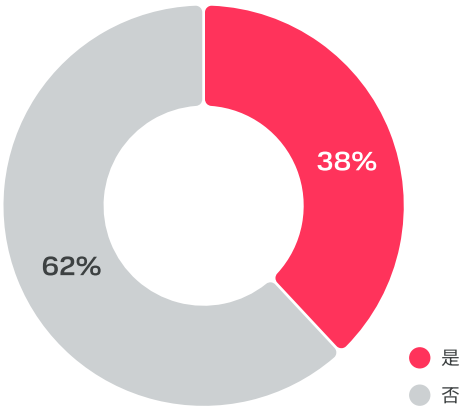


> “ 俄罗斯云技术市场正在逐步从本地 IT 举措转向对业务模式的战略性重塑。对于大多数企业而言，云解决方案已不再只是降低成本和加快数字化项目落地的工具，而是提升业务韧性和适应能力的关键要素。Private Cloud的占比明显更高，这反映出企业对数据控制以及行业和监管合规性的要求不断提升。同时，Public Cloud仍在混合架构中发挥重要作用，使企业能够灵活扩展资源，并在无需大量资本投入的情况下快速启动新举措。

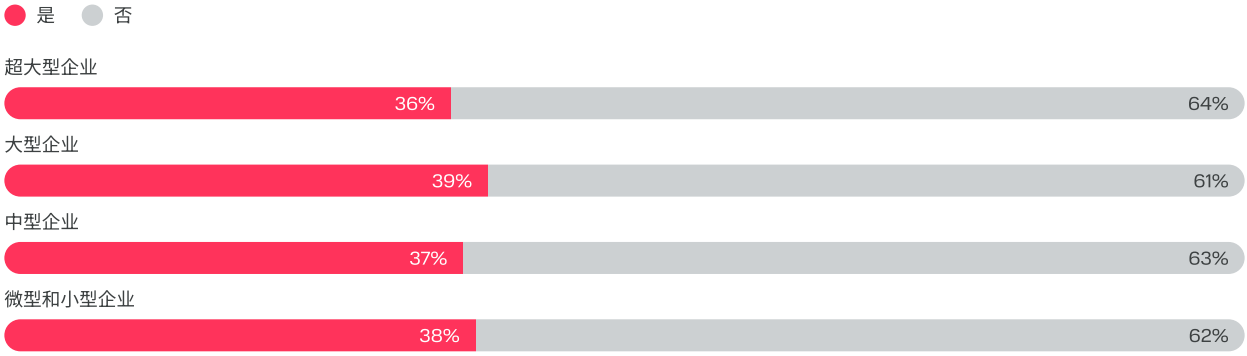
Danila Egorov
MWS Cloud 业务战略总监

近几年，关于高素质人才短缺的问题被广泛讨论，然而在云计算领域，超过 62% 的企业在招聘相关专家方面并未遇到困难。招聘困难与公司规模无关，这表明专业人才整体供给不足，与能力水平或薪酬水平无直接关联。在不同行业之间，该指标的差异同样不明显。相对而言，科研与教育领域以及工业领域面临的招聘困难略高。

云计算领域专家招聘是否存在问题



按业务规模划分的云计算专家招聘问题



专家能力问题与 SaaS 模式应用软件的普及程度直接相关。专家能力问题与 SaaS 模式应用软件的普及程度直接相关。采用 SaaS 解决方案的企业比例仍然偏低，根据业务规模不同，约为 21–34%。这可能反映出企业对 SaaS 在安全性、功能限制以及供应商绑定方面的谨慎态度。这可能反映出企业对 SaaS 在安全性、功能限制以及供应商绑定方面的谨慎态度。

因此，企业更倾向于构建自有云环境，或采用 IaaS / PaaS 作为更具灵活性的基础平台。在内部专业能力不足的背景下，企业积极借助专业服务。在内部专业能力不足的背景下，企业积极借助专业服务。超过一半的受访企业使用技术支持服务，40% 选择员工培训，约三分之一采用外包服务。

用于发展云技术的专业服务（企业使用情况）

53%
技术支持

40%
培训

33%
外包

19%
咨询（战略）

11%
未使用

MTS WEB SERVICES

拓展您的基础设施能力

MWS CONTAINER PLATFORM

用于开发和运行容器化应用的可靠平台。帮助企业更快引入创新、推进数字化转型并推出 IT 产品。

на 40% 将 IT 团队负载降低	на 70% 将新应用发布速度提升，并简化运维	на 80% 将人工操作自动化程度提升至	

AI-CLOUD

用于在业务中落地人工智能技术的基础设施与服务。AI 云可有效加速数字化转型并优化业务流程。

20% AI 云可有效加速数字化转型并优化业务流程	20–45% 使用代码生成系统后，研发团队生产效率提升	на 60% AI 云可有效加速数字化转型并优化业务流程。	

MWS云平台

将 Time-to-Market 缩短，并将混合基础设施能力提升

на 40% 基础设施成本降低	на 50% 产品上市速度提升	на 80% 通过网络安全系统，将成功攻击的概率降低	

技术落地：云计算

在本次技术研究中，除包含预算、战略、专业能力、实施驱动因素与障碍在内的总体评估之外，还尤为重要的是对相关技术产品的实际使用情况进行补充评估。

为确保研究结果的透明性与可比性，后续分析基于事实数据，不包含额外的综合计算。相关结论与洞察可由报告使用者独立分析，因为所有指标均直接来源于受访者的真实回答。因此，本模块可作为评估和决策相关技术使用情况的实用工具。

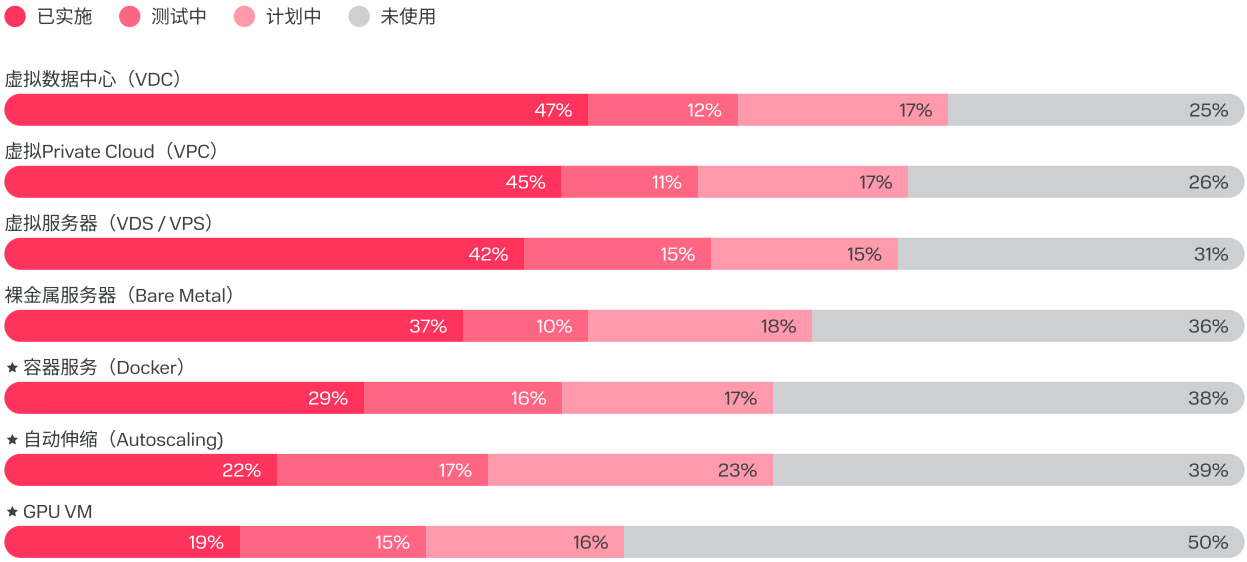
为评估各技术子类别中具备较高增长潜力的产品，引入了名为“子类别增长潜力公式”的方法。该公式将“已实施”这一指标，与“测试中”和“计划中”两项指标之和进行对比。不同于“未使用”这一参数，上述指标体现了受访者的积极规划，可被解读为在短期内向“已实施”状态转变的高概率。

已实施 < 测试中 + 计划中 = 存在增长潜力

已实施 > 测试中 + 计划中 = 增长潜力已被消耗

产品解决方案部分涵盖了经典的产品类别，分别对应基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。云计算是网络安全与人工智能等配套技术的基础。因此，云技术的高度发展与广泛应用显著降低了更专业技术在测试与集成过程中的复杂性。

计算



最常被使用的产品子类别符合预期，分别为虚拟数据中心（VDC）和虚拟Private Cloud（VPC），其实施比例分别为 47% 和 45%。对于受访样本中的大量企业而言，这类解决方案已成为标准化（commodity）产品，这一结论与公开市场的云计算消费数据高度一致。在云服务商的收入结构中，计算类产品与 IaaS 其他产品类别一道，长期占据最大比重。

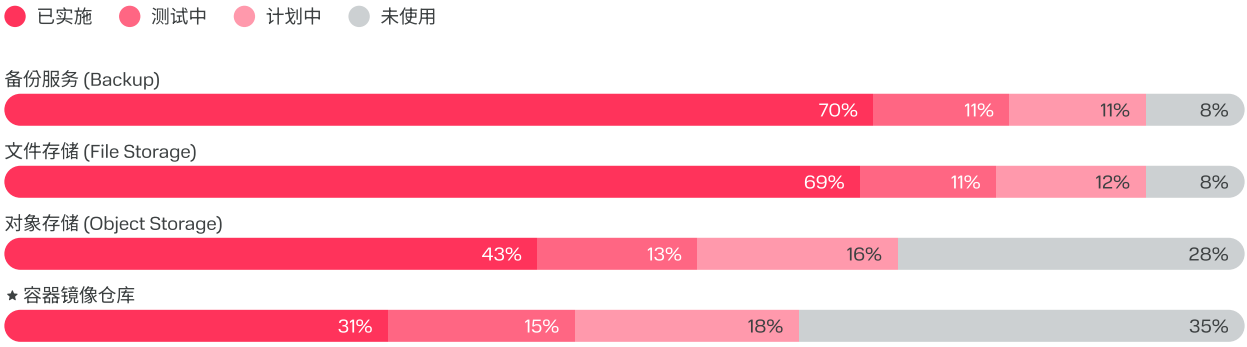
研究结果同样验证了当前市场上的一个关键趋势：无论是Public Cloud还是Private Cloud部署，均保持着较高需求。大型云服务提供商正积极响应这一趋势，加快混合云解决方案的发展。

值得单独关注的是容器服务（Docker）这一产品子类别。仅约三分之一的受访企业已完成全面部署，但另有约三分之一的企业已处于测试阶段（16%）或明确计划进行集成（17%）。

尽管人工智能技术具有高度关注度并被广泛讨论，但面向 AI 计算的产品子类别（GPU VM）在受访企业中的实际使用比例仍然相对有限。这主要源于多数企业当前主要在 AI 助手和业务应用层面使用人工智能工具。市场上确实存在对 GPU 的强烈需求，但这一需求主要来自对高性能计算有明确需求、且通常拥有自有 AI 研发团队的有限客户群体。调查显示，仅有 31% 的受访企业具备此类团队。因此，面向 AI 的基础设施型计算资源在不同行业和企业规模中，其重要性并不均衡。

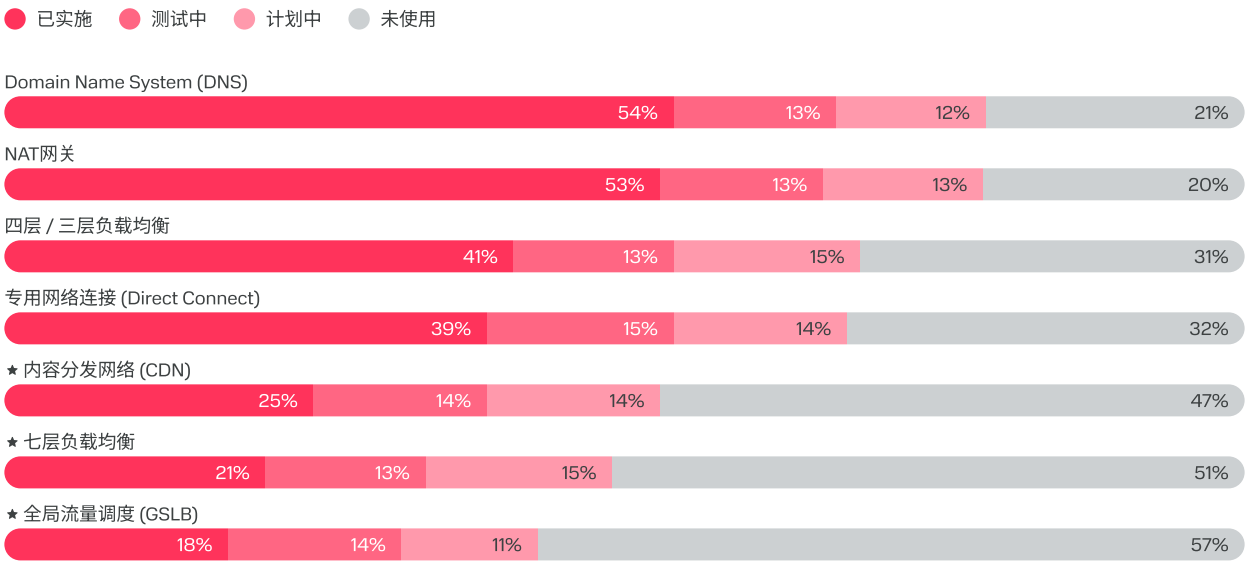
★ — 高增长潜力

存储



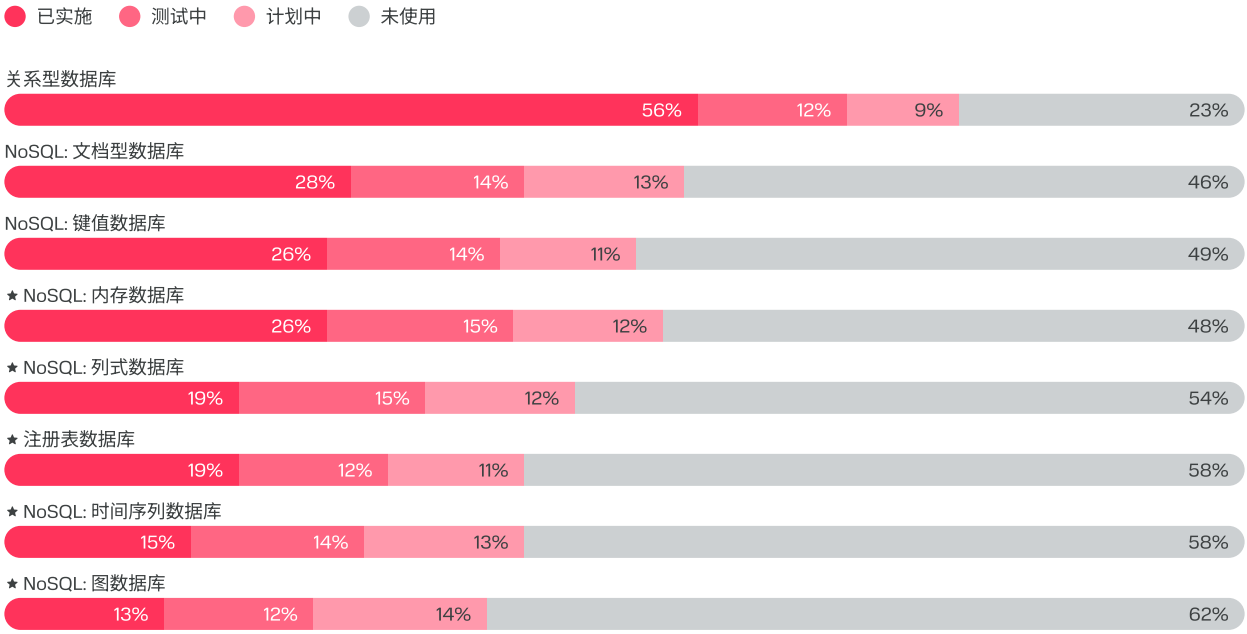
存储是当前市场中绝大多数企业的基础产品类别。可以明确指出，备份服务、文件存储以及虚拟机磁盘已成为俄罗斯大多数企业级客户的标准化产品。在满足日常业务需求的基础型解决方案与专业化产品子类别之间，消费水平存在显著差距，其使用比例差异可超过两倍。与此同时，对象存储和容器镜像仓库表现出较高的增长潜力：企业普遍表示已将这些产品纳入规划，或正处于测试阶段。

网络与内容分发



在向云迁移过程中，企业通常不会对单独的网络参数进行深度定制，而是采用具有标准配置的整体解决方案。该类别中对独立网络产品进行精细化配置，通常适用于地域分布广泛的企业，例如拥有大量分支机构的组织。此类企业多属于大型及超大型企业，对其而言，具备精细配置能力的网络产品已成为云使用的标准场景。上述网络与内容分发产品在 IT 行业和交通运输行业中的应用尤为典型。

数据库



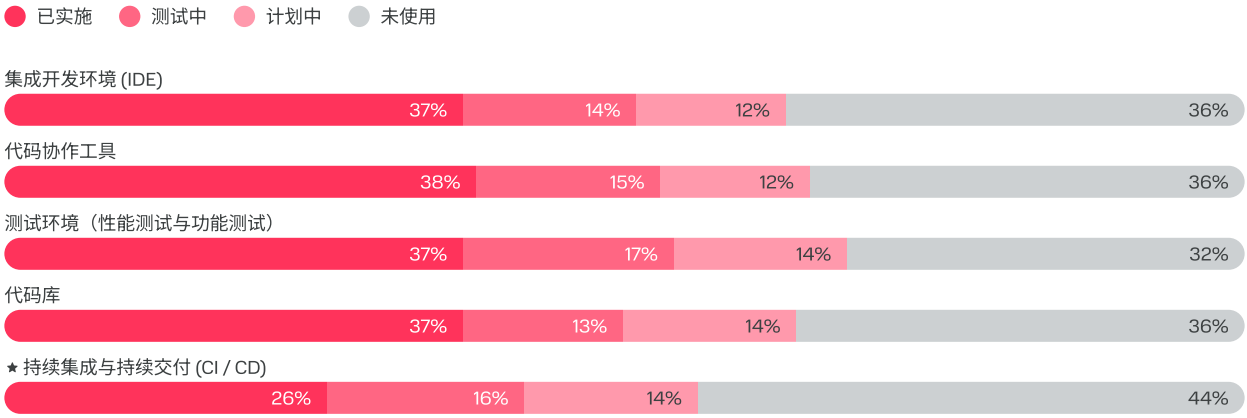
数据库是 PaaS 领域中最受欢迎的产品类别。关系型数据库如预期所示，是受访产品中实施比例最高的一类，这主要源于其在大多数业务应用开发场景中的原生适用性。使用频率排名第二的是 NoSQL 数据库（28% 已实施，或合计 55% 的正向反馈），这反映出市场对灵活、可横向扩展解决方案的兴趣增长。与此同时，SQL 仍然是绝大多数企业已经实施或正在考虑实施的数据库类型。这一现象可能反映出企业在支持新型数据库格式方面面临的复杂性，以及替代型数据库实际应用案例相对不足的问题。

> “ 俄罗斯云计算市场在基础型基础设施解决方案方面已表现出较高成熟度——虚拟数据中心、VPC 和存储已事实上成为大多数企业的标准配置。与此同时，容器服务和 AI 基础设施目前仍覆盖较小的市场份额，但具备显著的增长潜力：三分之一的企业已完成实施，另有相近比例的企业正处于测试或规划集成阶段。对象存储以及围绕容器化应用管理的相关服务同样展现出显著的发展前景。这为未来发展形成了双重重点：一方面巩固在通用型 IaaS 解决方案中的市场地位，另一方面并行扩展面向更复杂架构和特定行业场景的产品能力。

Mikhail Tutaev
MWS Cloud 产品总监

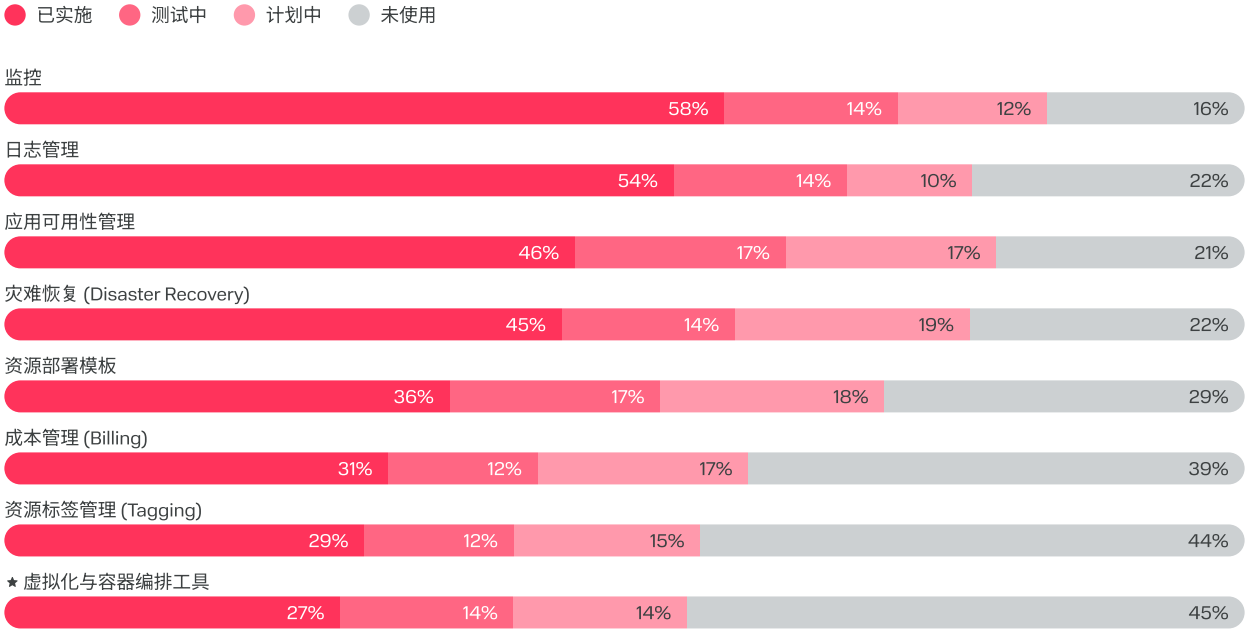
★ — 高增长潜力

开发工具



开发工具是 PaaS 领域中的基础性子类别之一。各项指标的中等水平，主要源于这些产品通常作为平台的内置组成部分存在，而非独立产品。从较高的测试与规划实施比例（相关产品合计约 28%）可以看出其增长潜力，这与俄罗斯平台型解决方案市场的增长速度相一致。持续集成与持续交付（CI / CD）对研发团队的成熟度要求较高。因此在本次调研企业中，该类别的采用频率相对低于其他工具。

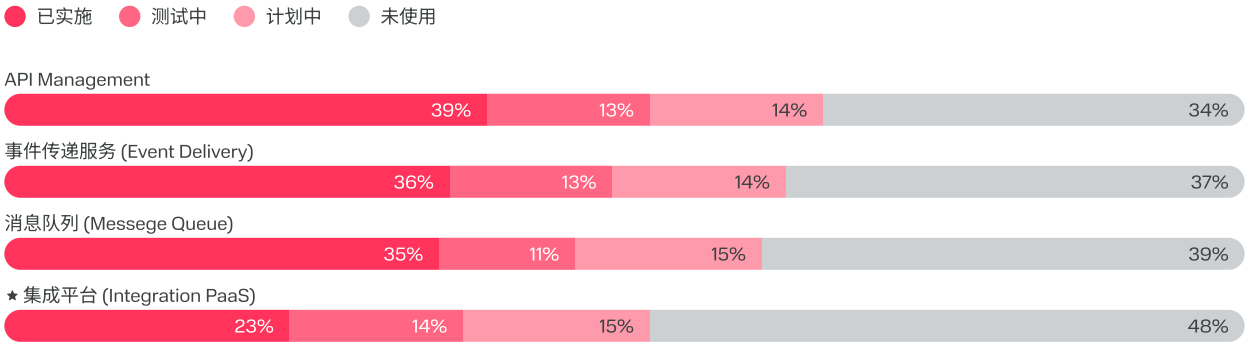
管理工具



管理类产品子类别在很大程度上同样作为云服务商平台的内置功能或属性存在。但与“开发工具”类别不同，受访企业对管理类工具的正向反馈明显更高。

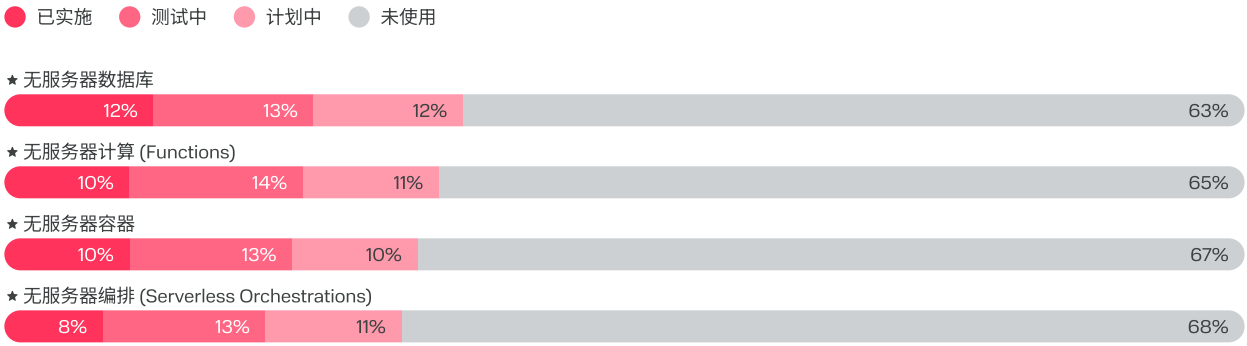
这表明上述解决方案对云计算客户而言具有基础性和必需性。在大型及超大型企业中，这些组件的重要性尤为突出，其基础设施稳定性具有关键意义。Disaster Recovery解决方案的应用进一步体现了企业在 IT 风险管理方面的成熟度。

集成



上述解决方案通常是平台的基础组成部分。对于拥有多层级企业架构的大型企业而言，集成类复杂解决方案是必不可少的，它们用于实现复杂的系统集成场景，以及对业务架构、数据架构、应用架构和技术栈的变更。成熟的集成平台解决方案支持企业从单体架构向组件化和微服务架构转型。集成产品的多样性与成熟度直接影响服务提供商与客户之间的技术契约，最终体现在系统可用性、响应时间、吞吐能力以及安全相关限制等方面。

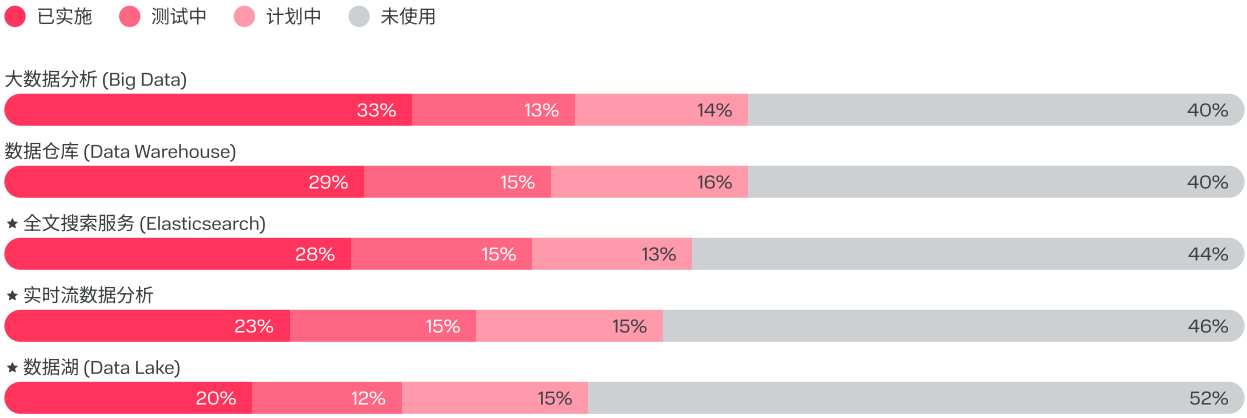
Serverless



无服务器（Serverless）解决方案的应用仍处于初级阶段，这表明企业技术栈中仍存在较高比例的遗留架构，同时在 DevOps/Cloud Native实践方面相对不足，尤其与海外企业相比更为明显。大多数受访企业不仅尚未使用相关解决方案，也未将其纳入未来规划。即使在测试阶段，该类技术的活跃度也较低，这可能反映出用户对 Serverless 优势认知不足，以及企业内部在该类解决方案实施方面的能力有限。此外，部分云服务商缺乏成熟的 Serverless 产品供给，也可能成为其市场需求不足的原因之一。

★ — 高增长潜力

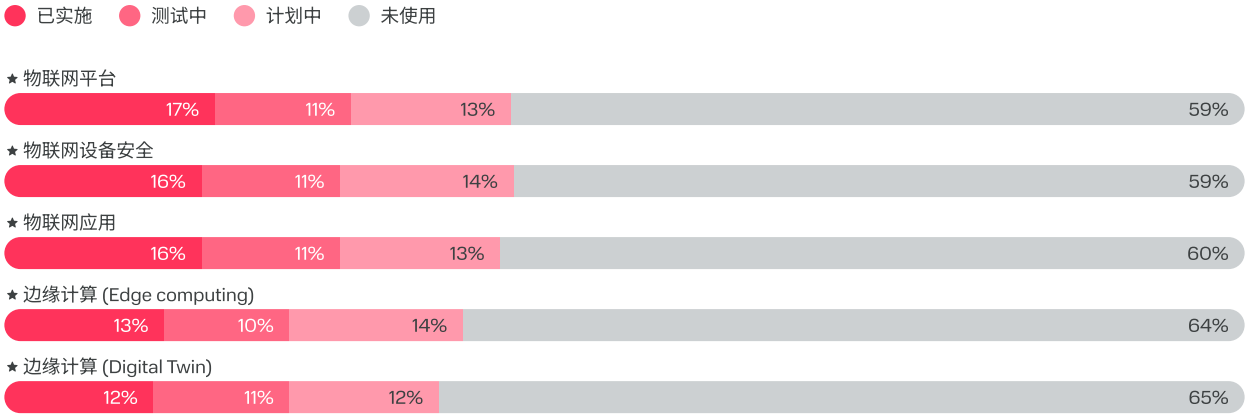
数据分析



成熟企业正在积极推进以数据驱动（data-driven）为核心的战略与运营模式。该模式的落地难点通常与企业内部流程以及数据治理（Data Governance）方法体系有关。一旦组织与流程层面的障碍被克服，从技术角度看，数据驱动模式的实现需要具备已部署的基础 IaaS 与 PaaS 产品，这些产品在前文已有所分析。

Data Warehouse 是构建成熟自动化分析体系的起点，也是最为普遍的解决方案类型。在实时分析和DataLake领域，测试阶段或规划阶段的企业数量明显高于已实际部署的企业。上述产品子类别通常出现在分析体系较为成熟、具备复杂集成能力的企业中。

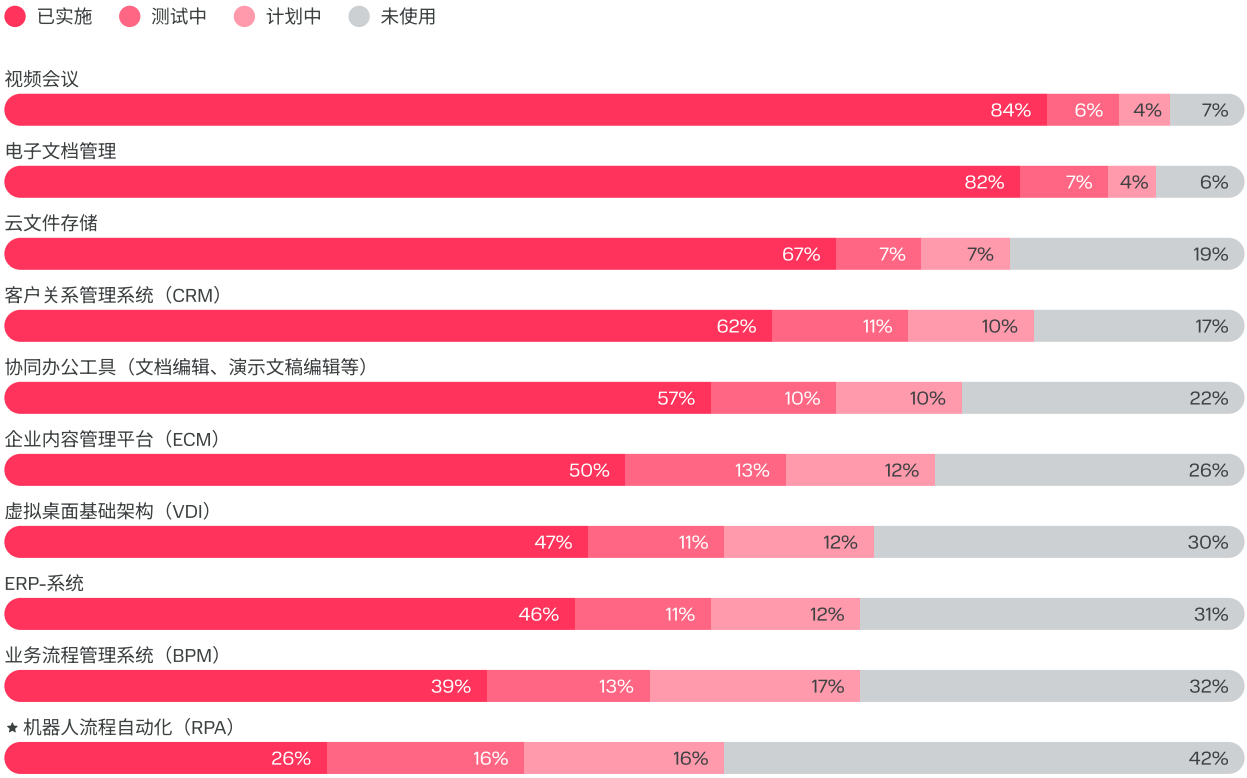
物联网 (IoT)



物联网是一项贯穿式技术，涵盖软件、硬件以及通信组件。物联网解决方案的实现至少需要部分依赖云基础设施。根据受访者反馈，物联网相关实践尚未形成规模化应用：在几乎所有方向上，超过一半的企业尚未使用 IoT 解决方案，而在数字孪生领域，约三分之二的企业尚未采用相关技术。目前，物联网主要应用于工业和物流行业，在其他行业中的成熟度仍然较低。

尽管针对 IoT 系统的攻击已成为增长最快的威胁之一，但在已部署物联网平台和应用的企业中，采用终端设备安全防护技术的比例仍不超过 70%。这一趋势可能表明，企业在设备全生命周期管理方面尚未形成系统性的战略。

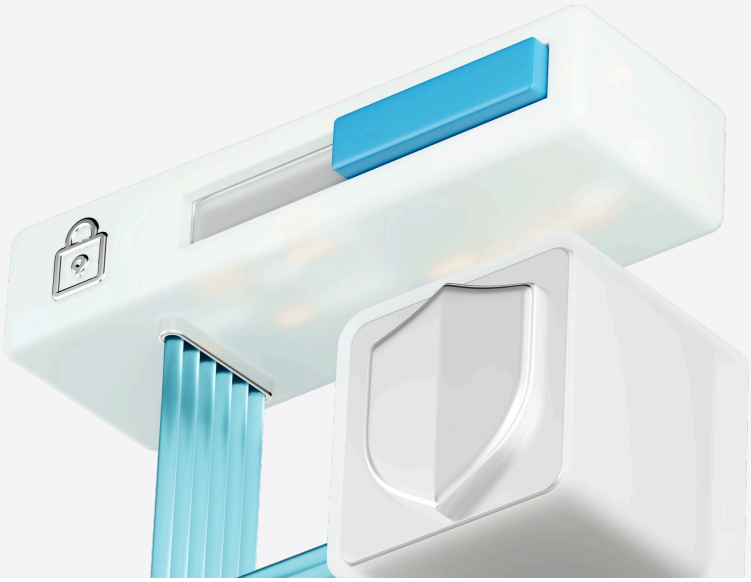
业务应用



属于 SaaS 领域的业务应用已被广泛采用，需求持续增长，并在许多企业中逐渐成为原生（原生云）解决方案。在本次研究中，绝大多数受访者已部署视频会议、电子文档管理、云文件存储、CRM 系统以及功能完善的协同办公工具，这类产品通常具备较为完整的功能体系。值得重点关注的两类产品子类别具备显著的增长潜力：业务流程管理系统（BPM）以及机器人流程自动化（RPA）。这些细分领域中较高的正向反馈比例表明，其应用具有高度通用性，基本不受行业属性或企业规模的限制。

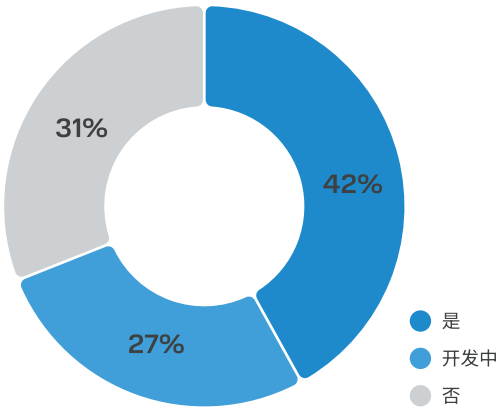
★ — 高增长潜力

企业技术战略：网络安全



信息安全保障正逐渐成为可持续数字基础设施中不可或缺的组成部分，该基础设施既是生产流程管理的必要条件，也是高效开展大数据与人工智能相关工作的关键基础。根据调查数据，42%的公司已经制定了完善的信息安全（网络安全）战略，另有27%的公司正处于该战略的制定阶段。这表明，对漏洞进行系统性分析并开展风险管理的做法正在得到越来越广泛的应用。关注重点正在向各业务细分领域中更为全面、系统化的网络安全管理转移，这反映了市场整体在降低网络风险以及为后续数字化投资阶段夯实基础方面的共识。

是否具备网络安全实施战略

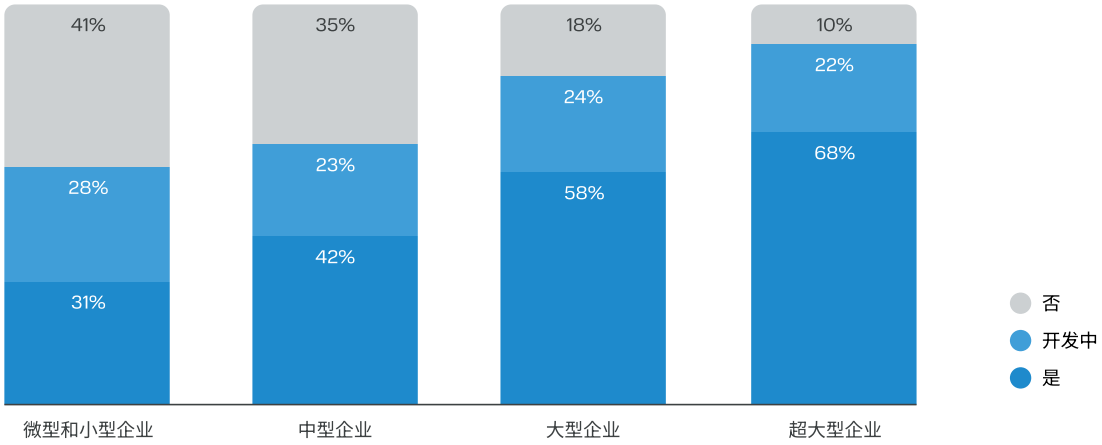


> 当前，面向网络安全的云解决方案市场正在发生质的转变——信息安全不再只是个别部门的局部任务，而是逐步成为企业可持续数字生态系统的基础。越来越多的公司以战略层面的方式应对网络安全问题，构建系统化的风险与漏洞管理模型。这一趋势反映了市场的成熟度，以及企业愿意投资于长期工具，以保障大数据处理的可靠性并推动人工智能的落地应用。

Mikhail Tutaev
MWS Cloud 产品总监

网络安全战略成熟度与企业规模之间的相关性表现得相当明显。在最大规模的企业中（年营收超过 150 亿卢布），仅有 68% 已形成网络安全战略；而在年营收低于 8 亿卢布的企业中，这一比例仅为 31%。与此同时，网络安全战略的制定在小型企业和中型企业中呈现出几乎相同的特征。对这些企业而言，这在很大程度上反映了其处于追赶式发展的过程，以及对现有漏洞的补齐与弥补。与此同时，大型企业往往已经构建了目标性的网络安全架构，这也使得仍处于战略制定阶段的企业比例相对较低。

按企业规模划分的网络安全实施战略

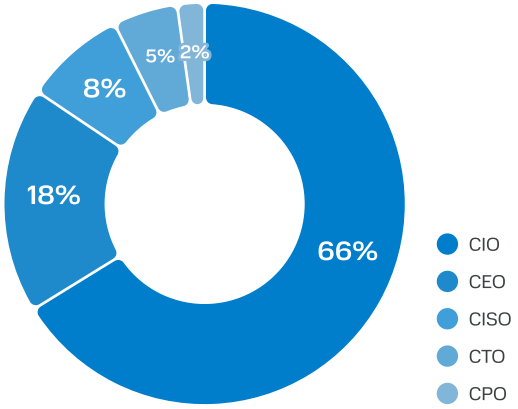


在信息安全领域的决策中，正如在云技术方面一样，影响力最大的是 CIO（首席信息官）——负责 IT 方向的管理者。其被认为是关键决策人 66% 的受访企业。

这表明仍然存在明显的 IT 导向，即网络安全管理主要被视为技术部门的责任领域。

对大多数企业而言，信息安全措施的实施过程相对较快：73% 的企业在不超过半年的时间内完成部署。最常见的实施周期为 1–3 个月（31%），其次为 3–6 个月（24%）。

在网络安全实施决策过程中发挥关键作用的人员

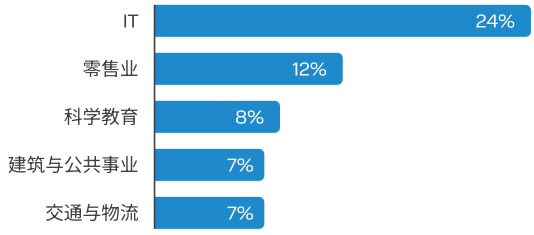


这些结果表明，对于相当一部分企业而言，网络安全项目能够在较短时间内完成实施，这可能说明所采用的解决方案具有较强的标准化特征，或具备较高的成熟度，能够快速集成到现有基础设施中。网络安全项目实施周期超过一年的企业占比仅为 14%，这凸显了此类项目的特殊性，并可能表明其多为大型组织中规模较大或高度专业化的举措。

2025 年网络攻击数量增长了 30%

安全防护手段的部署重要性不仅由监管要求决定。2024 年，35% 的受访企业曾遭遇 DDoS 攻击。同时可以观察到明显的相关性：企业规模越大，遭受此类攻击的概率越高。在大型企业中，约 50% 曾遭受 DDoS 攻击，而在超大型企业中，该比例高达 60%。

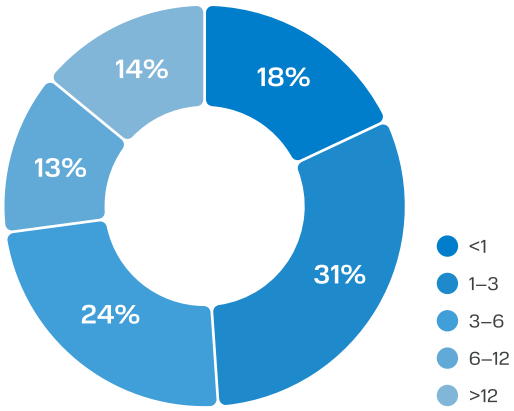
2024 年各行业遭受 DDoS 攻击情况



2025 年网络攻击数量同比增长超过 25%。影响最严重的案例主要集中在交通、工业企业以及零售行业。例如，对某大型电信运营商的一次重大攻击导致关键网络节点瘫痪，来自俄罗斯 4 个地区的客户访问受限。另一起针对大型工业企业的攻击破坏了内部系统，限制了数据访问。最终导致运营流程中断并扰乱了物流链条。网络攻击的后果不仅包括业务流程中断和企业数据泄露，还可能引发监管机构的额外审查，并在发现信息存储、处理或传输违规的情况下，给高层管理人员带来刑事责任风险。调查结果显示，行业特性对攻击频率具有显著影响：信息技术、零售和科研机构是最常遭受 DDoS 攻击的领域。这表明 DDoS 攻击仍然是企业，尤其是大型企业及特定行业面临的重要威胁，也凸显了部署有效网络安全防护措施的必要性。

信息安全系统的部署最常见于企业自有基础设施中：43% 的受访者采用 On-Premise 方案。这主要源于企业对系统和数据完全可控性的需求，尤其是在隐私保护和合规要求不断提高的背景下。其次是混合云（32%），该模式有助于在成本效率与可靠性之间取得平衡，尤其适用于处理敏感数据，包括商业机密和客户个人数据。这种选择使企业能够在享受云技术优势的同时，实现受控访问管理和数据分区隔离。

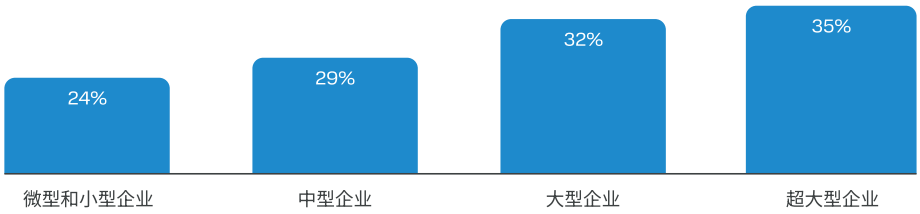
网络安全防护工具的实施周期 (以月计)



随着企业规模的扩大，私有化和本地化安全解决方案的使用比例不断上升。在营收超过150亿卢布的超大型企业中，采用 On-Premise 和 Private 部署模式的比例已达到 50%。大型企业在将关键网络安全组件部署至公有云时更加审慎，这体现了其在数据保护与外部风险最小化方面的战略优先级。

多云网络安全解决方案正在加速发展

按业务规模企业在云中使用的网络安全工具占比



随着企业规模的扩大，部署在云端的网络安全工具平均占比也随之提高。微型和小型企业（年营收低于 8 亿卢布）的云端安全工具占比平均为 24%，而在超大型企业中，该指标已达到 35%。但整体来看，大多数企业仍采取选择性上云策略：79% 的受访者仅将不超过 30% 的网络安全工具部署在云中，这凸显了本地化解决方案在企业安全体系中的长期重要性。

从行业维度来看，云端网络安全工具占比最高的行业包括信息技术、娱乐与媒体，以及科研与教育领域（平均约 36%）。这与上述行业较高的数字化成熟度以及云服务已深度融入其运营模式密切相关。与此同时，交通运输和零售行业的该指标同样处于较高水平（24–27%），反映出其在保护分布式基础设施和客户数据方面，对快速扩展网络安全能力的迫切需求。

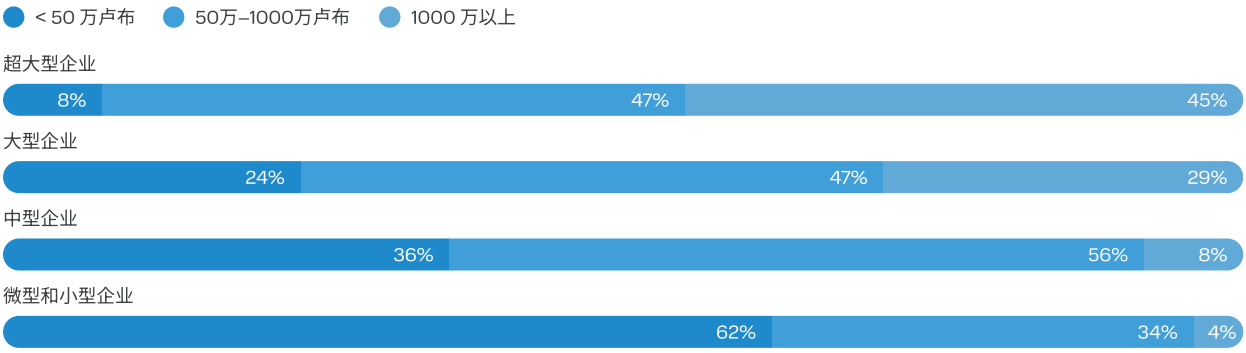
不同规模企业在网络安全（КБ）方面的年度支出分布，充分反映了其整体企业预算结构。随着营收规模的下降，安全预算明显向低投入区间集中。例如，在微型与小型企业中，主要网络安全支出集中在 50 万卢布以下，这表明此类企业在网络安全领域的投入能力相对有限，对专业化安全工具的投资规模也受到明显制约。

在信息技术和交通运输行业，云端网络安全年度支出区间呈现出最高的多样化特征。这表明这些行业在网络安全解决方案上的需求结构更加复杂，既包括用于通信链路和终端设备防护的基础型服务，也涵盖面向基础设施层面的综合监控与安全事件管理系统。

按行业云端网络安全投入占比 (占全部安全支出的比例)

	平均值
IT	36%
零售业	27%
建筑与公共事业	19%
交通与物流	24%
专业服务	23%

按业务规模企业的年度网络安全支出规模



在网络安全支出规模排名前五的行业中，分别为信息技术、金融行业、娱乐与媒体、资源开采与加工，以及医疗健康领域。这些行业普遍呈现出向 1000 万卢布以上投入区间稳定迁移的趋势，反映了其对云端网络安全服务的成熟需求，以及在客户数据和金融交易保护方面所面临的合规与制度性要求。

从风险特征和行业驱动因素的角度来看，网络安全支出的分布具有明显逻辑性：IT行业主要用于保护自身平台和客户数据；金融与零售行业侧重于防范欺诈风险和满足监管合规要求；医疗健康行业则重点保护知识产权和临床数据。该分布不仅体现了不同行业在网络安全战略成熟度上的差异，也反映了其所面临的特定安全威胁类型。

> “ 尽管本地部署方案仍然占据主导地位——尤其是在超大型企业中，出于更严格的监管要求和控制需求，这一趋势尤为明显——但私有云和混合云安全模式的占比正在持续增长。这反映出企业希望在保持可靠性和可控性的同时，引入具备更高扩展性和灵活性的现代网络安全解决方案。我们观察到，将网络安全功能迁移至云端的需求主要集中在数字化成熟度高、基础设施分布广泛的行业：IT、媒体、教育、交通和零售。对于这些行业而言，云端网络安全工具已成为保障业务连续性和复杂数据处理链路安全的关键条件。同时，支出结构呈现出从基础防护服务到综合安全事件管理平台的广泛预算区间，印证了市场已形成成熟且高度细分的需求格局。

Danila Egorov
MWS Cloud 业务战略总监

Годовой объем затрат на КБ по индустриям

	<50万卢布	50万–1000万卢布	1000 万以上
IT	33%	41%	26%
金融与保险	47%	28%	25%
娱乐与媒体	27%	48%	25%
矿产资源开采与加工	43%	36%	26%
保健事业	49%	40%	11%
科学教育	48%	44%	9%
零售业	56%	36%	8%
HoReCa	50%	45%	5%
房地产与建筑业	59%	37%	4%
工业	58%	37%	4%
交通与物流	43%	53%	4%
专业服务	62%	36%	3%

仅有 5% 的受访企业未使用外部信息安全解决方案提供商的服务，这表明企业对专业安全厂商具有高度信任，并普遍认可数据保护领域专业化解决方案的重要性。同时，其余 95% 的企业明确意识到，通过引入和集成外部安全解决方案，才能为自身数字基础设施提供可靠、系统性的防护。

然而需要指出的是，部分企业仍倾向于在本地部署信息安全解决方案。这通常与企业希望保持对数据的最大控制权、并尽量降低因将信息传递给第三方而带来的风险有关。对于在数据安全性和保密性方面要求较高的企业而言，本地化解决方案依然具有较强吸引力。

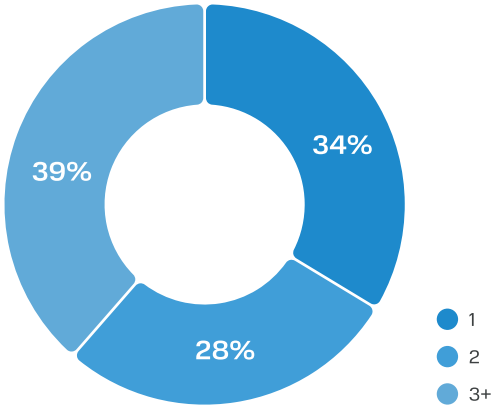
超过三分之一的受访企业仅与一家供应商合作，这可能反映出企业希望简化安全管理和系统集成流程，同时也体现了对单一、成熟合作伙伴的信任。从服务整合和获取更具优势的服务条件角度来看，这种模式往往具有一定的经济合理性。

与此同时，64%的受访企业仅使用不超过两家供应商的服务。这种做法使企业能够整合最佳实践与先进技术，并根据自身的具体需求进行灵活调整与适配。

总体来看，这些趋势反映出企业在信息安全管理方面日趋成熟，其在外部资源与本地解决方案之间的平衡选择，主要由战略优先级和业务自身的具体需求所决定。

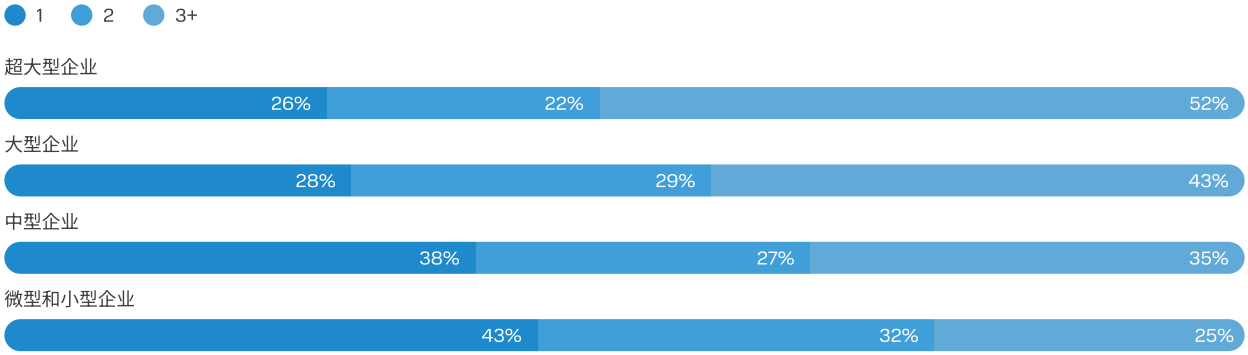
值得注意的是，大型及超大型企业通常会使用更多的安全服务提供商，并且供应商数量往往随着企业规模的扩大而相应增长。

网络安全供应商使用数量



企业正越来越多地通过引入多家供应商来分散网络安全风险

不同业务规模企业使用的网络安全供应商数量



“ 对于俄罗斯企业市场而言，此类网络安全解决方案的选择模式体现了（compliance-driven security)占据主导地位，其核心目标在于满足法律法规及行业标准的要求。同时，这种策略在一定程度上可能抑制对主动型网络韧性技术的投资，而在网络威胁日益复杂、针对大型企业的定向攻击数量不断增长的背景下，这一点尤需引起重视。

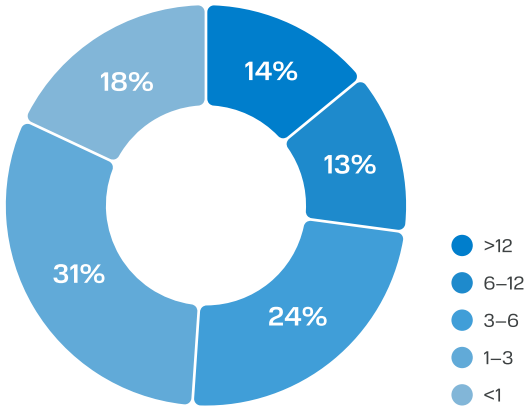
Polina Li
MWS Cloud 分析与研究中心负责人

55% 的受访企业表示，网络安全工具的实施周期不超过半年。其中，多数公司指出，实际部署时间为 1–3 个月。

另有 14% 的受访者表示，网络安全解决方案的实施过程持续超过一年。较长的实施周期通常与多种因素有关，例如复杂的基础设施架构、需要与大量现有系统进行集成，或对安全性提出较高要求。实施周期较长的企业，可能正在进行大规模的基础设施现代化改造，或向更加复杂、定制化的解决方案过渡，这类项目通常需要投入显著的时间和资源成本。

网络安全解决方案实施周期

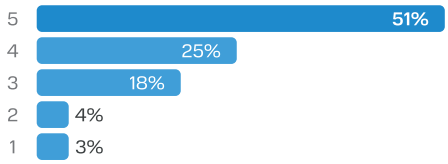
（以月计）



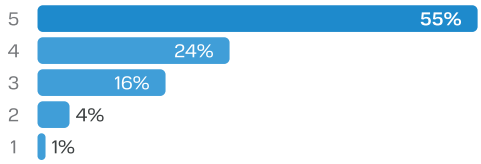
决定部署网络安全解决方案的关键因素

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

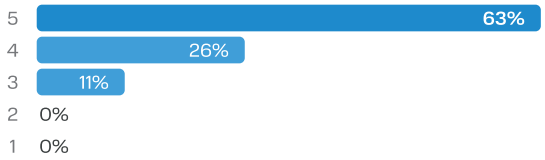
符合信息安全相关法律法规要求



保障企业的网络韧性



防范内部及外部威胁，保障数据安全



多数受访者认为，员工缺乏必要的专业能力是阻碍信息安全系统落地过程中最为关键的因素。该障碍在评分为4分和5分的比例中持续位居前列，表明人力资本在网络安全项目成功中发挥着决定性作用。

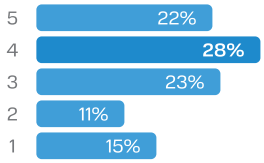
与此同时，“实施过程中缺乏厂商支持”以及“服务商未提供完整技术支持体系（如POC、Support等）”等因素的影响被评估得相对温和。对大多数企业而言，这些问题尚未构成关键障碍，这可能反映出两种趋势。其一，部分企业倾向于发展自身能力，以降低对外部供应商的依赖以及对关键基础设施控制权外移所带来的风险；其二，市场需求可能更多集中于不需要深度定制或持续厂商支持的基础型安全服务。

此外，“基础设施管理复杂度提升”和“实施阶段产生的额外成本”同样被相当一部分受访者视为重要影响因素。其较高的重要性评分凸显了在向更高成熟度安全水平迈进过程中，对网络安全预算与架构进行平衡规划的必要性。

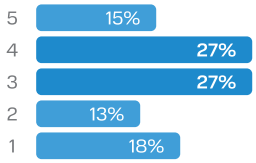
网络安全解决方案实施过程中的主要挑战

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

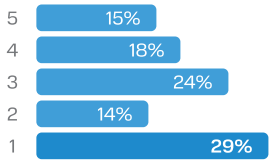
员工缺乏必要的专业能力



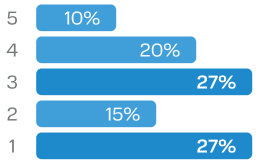
对所需基础设施预期成本的评估难度较高



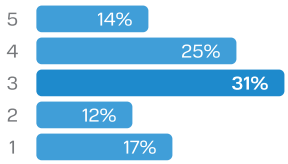
大规模数据迁移的复杂性



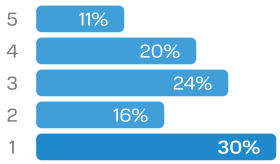
缺乏清晰的实施路线图



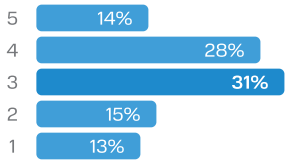
信息安全系统实施阶段的额外成本



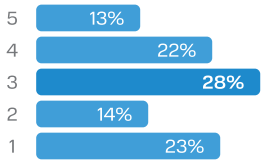
实施过程中缺乏厂商支持



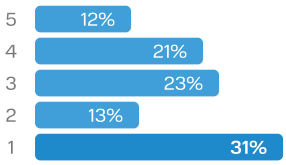
基础设施管理复杂度提升



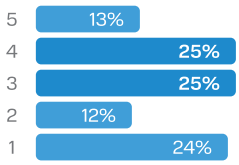
实施期间需要临时进行基础设施冗余



所考察的服务商 / 厂商缺乏完善的技术支持方案（如 POC、Support 等）



信息安全解决方案无法与现有本地系统集成（老旧软件 / 硬件）



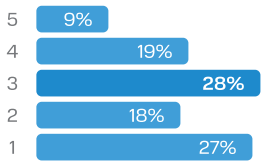
与员工再培训或招聘相关的额外支出，被受访者提及的频率最高，并且多集中在重要性较高的评分区间。这一趋势表明，在网络安全项目中，人力资源因素仍然是最主要的新增成本来源之一。

本地基础设施的更新同样在成本结构中占据重要位置，这也从侧面反映出，在部署更复杂或资源密集型网络安全系统时，技术升级具有客观必要性。

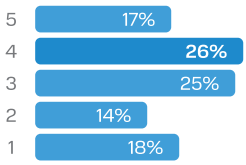
网络安全解决方案实施过程中的额外成本

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

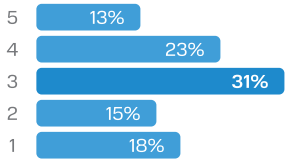
为验证所选解决方案可行性而部署测试环境



为高质量使用网络安全解决方案而进行员工再培训或招聘



本地基础设施的更新与升级

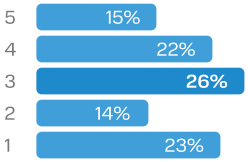


受访者对与数据泄露相关的风险表现出最高程度的敏感性——无论是个人数据还是商业机密数据。这两类风险在最高严重等级（5分）的评分中占据最大比例：35%的受访者认为商业机密泄露属于关键风险，34%认为个人数据泄露具有同等严重性。这表明企业对客户数据、合作伙伴信息以及商业敏感信息保护的关注持续提升。在信息安全领域技术能力不足同样被视为重要风险，但更多获得中等评分（3–4分），这说明企业已清楚认识到该问题的存在，但尚未将其视为迫在眉睫的危机。

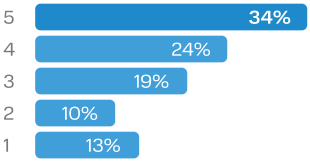
在实施网络安全解决方案过程中，下列风险类别的关键性评估

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

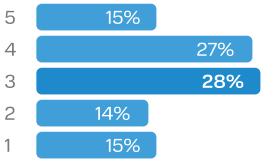
设备采购难度



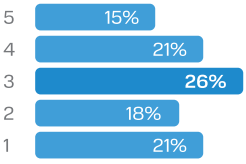
个人数据泄露



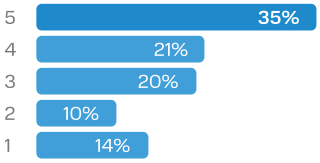
信息安全领域技术专业能力不足



信息安全投入成本的不可控增长



商业机密数据泄露



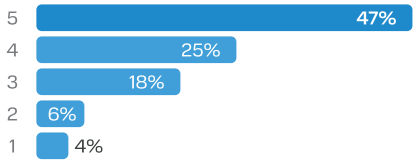
在影响网络安全解决方案决策的因素中，威胁与风险分析以微弱优势位居首位——51%的受访者认为该因素具有关键重要性。这样的结果表明，企业在制定网络安全战略时，越来越注重对系统脆弱性和潜在攻击场景的识别与理解，并将其作为构建有效安全体系的基础。

符合监管与合规要求同样占据重要位置——47%的受访者将该因素评为最高重要等级。这反映出监管压力的持续存在，以及企业在信息安全领域必须遵循行业标准和相关法律法规的现实需求。

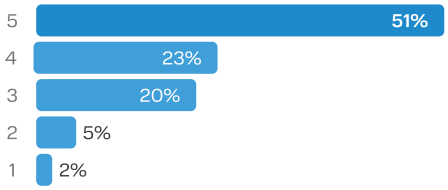
在网络安全解决方案决策过程中最重要的因素

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

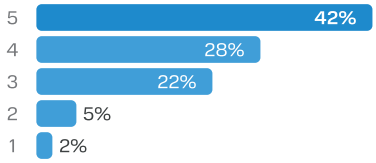
符合监管与合规要求



威胁与风险分析



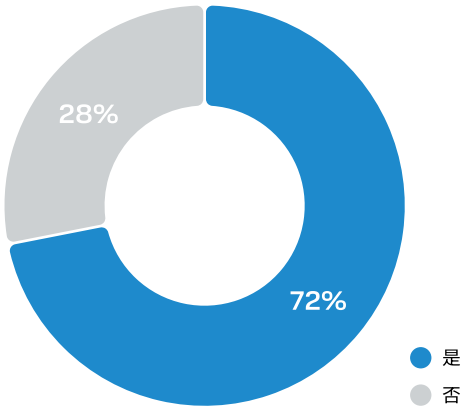
风险与威胁识别相关成本的优化



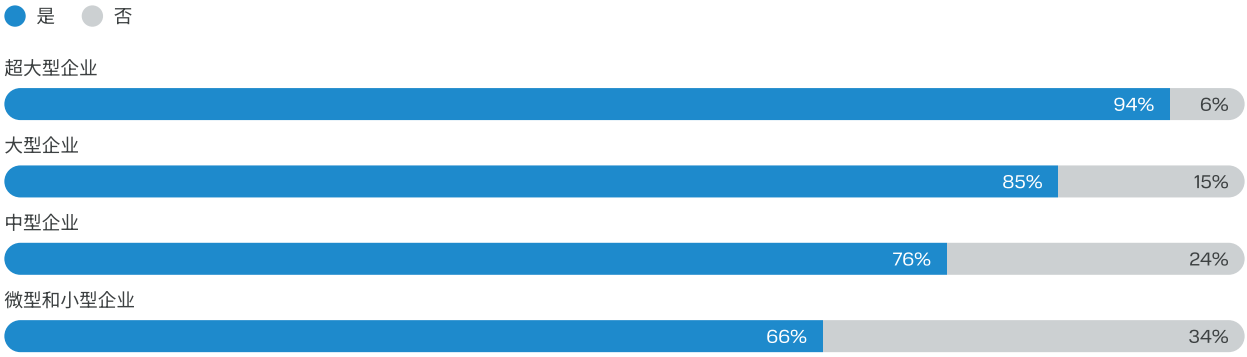
只有大型和超大型企业具备足够的资金用于招聘所需的专业人才

72%的企业已经具备网络安全领域的经验和专业能力。如此高的比例表明，网络安全问题已牢固地纳入大多数市场参与者的企业管理议程。按业务规模划分的结构显示，企业营收规模越高，其在网络安全领域具备经验和能力的可能性也越大。在年营收低于8亿卢布的企业中，66%的公司表示具备网络安全方面的专业能力；而在营收更高的企业中，这一比例持续上升，在超大型企业中高达94%。这在逻辑上源于大型企业具备更强的资源投入能力，能够建设专业团队，并持续进行网络安全相关的培训与流程优化。

是否具备网络安全相关经验与专业能力



按业务规模划分的网络安全经验与专业能力情况

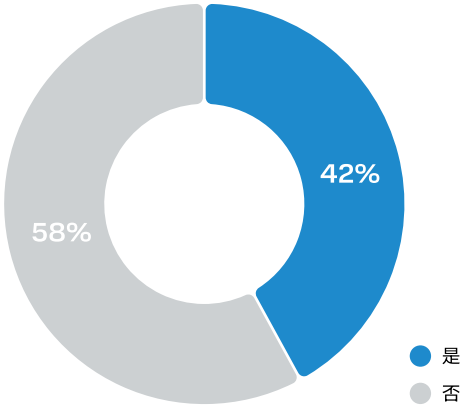


从行业角度来看，网络安全专业能力的最高集中度出现在信息技术行业（88%）、矿产资源开采行业（82%）、金融与保险行业（81%），以及医疗健康和专业服务领域。这些行业通常面临更为严格的监管要求、更高的敏感数据泄露风险，同时对知识产权和关键基础设施保护具有迫切需求。这些因素直接推动企业内部建立更加成熟的网络安全能力体系。网络安全经验与专业能力的存在，不仅是企业技术风险管理成熟度的体现，也反映了不同行业在监管环境和商业模式上的差异。对于资本密集度较低、监管程度相对较弱的行业而言，网络安全专业能力占比较低，这表明这些领域在网络安全实践和专业咨询服务方面仍具有较大的发展潜力。

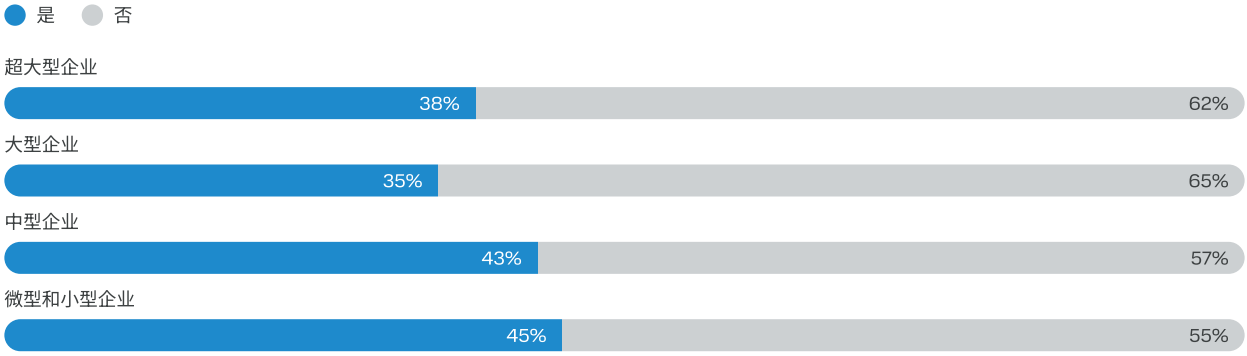
尽管整体上企业已具备使用网络安全工具的经验，但招聘合格专业人才的困难仍然是行业面临的重要问题。43%的受访企业表示在招聘网络安全专家方面存在困难，这一比例具有显著代表性。同时，招聘难题并不随企业规模变化而显著不同——各业务规模的企业普遍面临相似的招聘挑战。这表明该问题具有结构性特征，既影响中小企业，也影响大型企业。

从技术角度来看，该趋势凸显了托管式安全服务（Managed Security）以及服务商内置专业能力的重要性不断上升。这类服务帮助企业在自身能力不足的情况下，弥补网络安全专业人才的缺口。从长期来看，这些模式不再只是技术选择，而是成为弥补关键人才短缺、加速企业数字化转型的战略性工具。

是否存在网络安全专家招聘困难



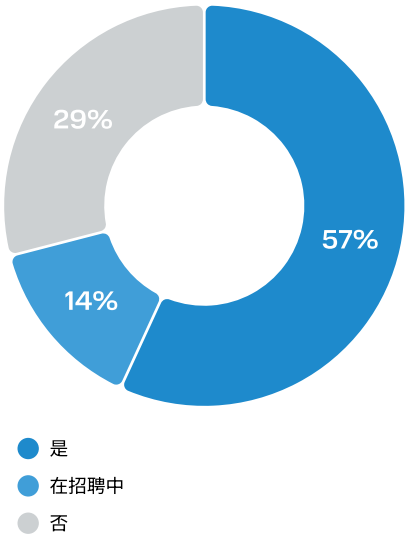
按业务规模划分的网络安全专家招聘问题情况



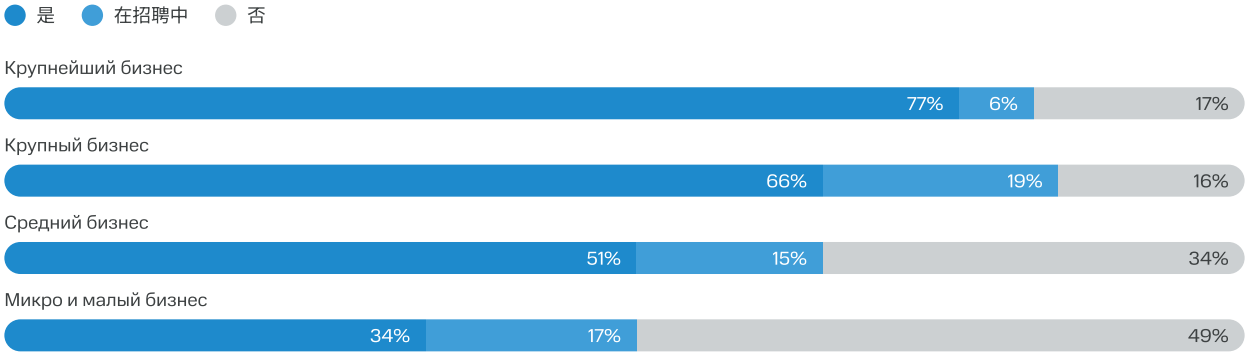
与此同时，拥有完整自有网络安全团队的企业比例也在持续上升。57%的受访企业已经建立了自己的网络安全团队，另有14%的企业正处于团队建设阶段。这表明企业对网络安全在业务中的重要性认知正在不断增强。调查结果显示，企业规模与是否拥有自有网络安全团队之间存在明显正相关关系。IT 架构更为复杂的大型企业，更倾向于组建并维持内部网络安全团队。

在信息技术和制药行业中，拥有自有网络安全团队的情况最为普遍。这主要源于这些行业需要处理大量数据，并受到较为严格的监管要求。与此同时，即便企业内部已经具备专业人员，仍然会依赖云端安全服务来应对可扩展性需求，并满足不断提升的合规标准。因此，市场正逐步向混合模式演进：企业内部的网络安全能力中心与先进的云安全解决方案相互补充，从而推动对更加灵活、综合性强且面向特定行业的安全服务的需求。

是否拥有自有网络安全团队



按业务规模划分的自有网络安全团队情况



用于提升网络安全能力的专业服务主要包括技术支持、培训和安全审计。超过40%的受访企业正在使用此类服务。技术支持在保障对安全事件的快速响应和漏洞修复方面发挥着关键作用。网络安全培训有助于提升员工对潜在威胁及其防范方式的认知。安全审计则帮助企业系统性地评估并持续改进其防护措施。总体来看，这些数据表明，企业正在积极投资于网络安全的核心要素，这是降低风险、防范网络威胁的重要一步。

用于网络安全能力建设的专业服务类型

63%	25%
技术支持	集成

MTS WEB SERVICES

客户混合基础设施的网络安全防护

用于防御信息安全威胁的工具

通过网络安全系统

за счёт систем кибербезопасности

将各类网络攻击造成的损失降低 50%

24/7

周界监控与防护

500 条

用于信息安全事件分析与关联的主动规则

>1500 个

用于数据处理的多源信息来源

300 Gbit/s

Anti-DDoS 防护的可用带宽能力

SOC（安全运营中心）

面向企业网络安全水平提升的综合解决方案。通过整合专业安全专家、创新技术与成熟流程，实现对网络威胁的实时、全方位防护。SOC 对企业 IT 基础设施进行 7×24 小时持续监控，有效降低入侵风险、员工/客户/用户数据泄露风险以及其他可能导致业务中断的网络威胁。

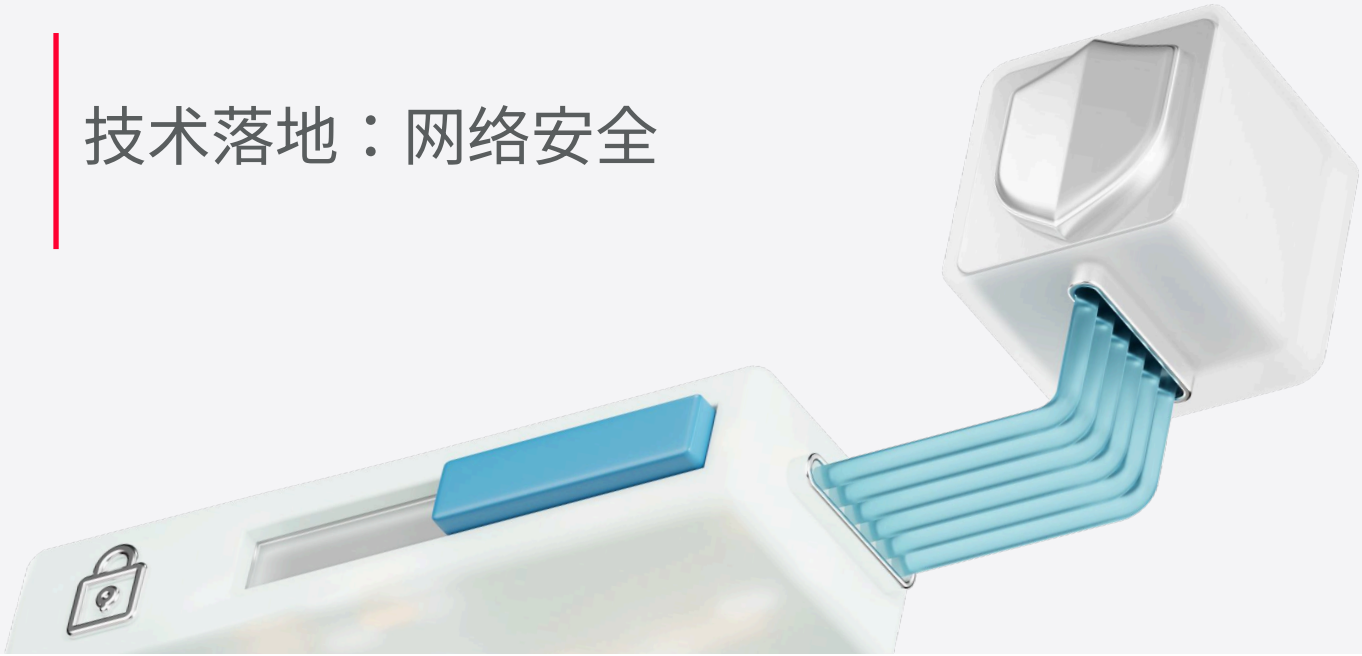
ANTI-DDOS

用于阻断针对客户基础设施及 Web 资源的 DDoS 攻击的综合解决方案。DDoS 防护对业务直接或间接依赖互联网系统可用性的组织至关重要，尤其适用于生产流程依赖远程访问自有或第三方资源的企业。

WAF（WEB 应用防火墙）

用于防御 Web 应用攻击与漏洞的安全服务。通过管理控制台，客户可自主配置安全策略与防护规则，保障自身资源安全。

技术落地：网络安全



本章节展示了信息安全技术相关的产品类别。鉴于本次研究的特点，在网络安全领域的分析重点集中于IT 市场中的 软件（Software）和 IT 服务（IT Services）垂直领域，因为从市场规模角度来看，这两类垂直领域构成了俄罗斯网络安全市场的主体。 网络安全领域中的硬件类解决方案未纳入本研究的重点范围，因为其主要由高度专业化的产品构成，其中包括部分模拟类解决方案，并且并不总是与数字化产品直接相关。 类比云计算领域，网络安全产品可划分为广泛应用的产品（其中包括满足法律法规合规要求所必需的解决方案）以及高度专业化的产品，后者主要被企业用于解决高复杂度场景下的安全问题。

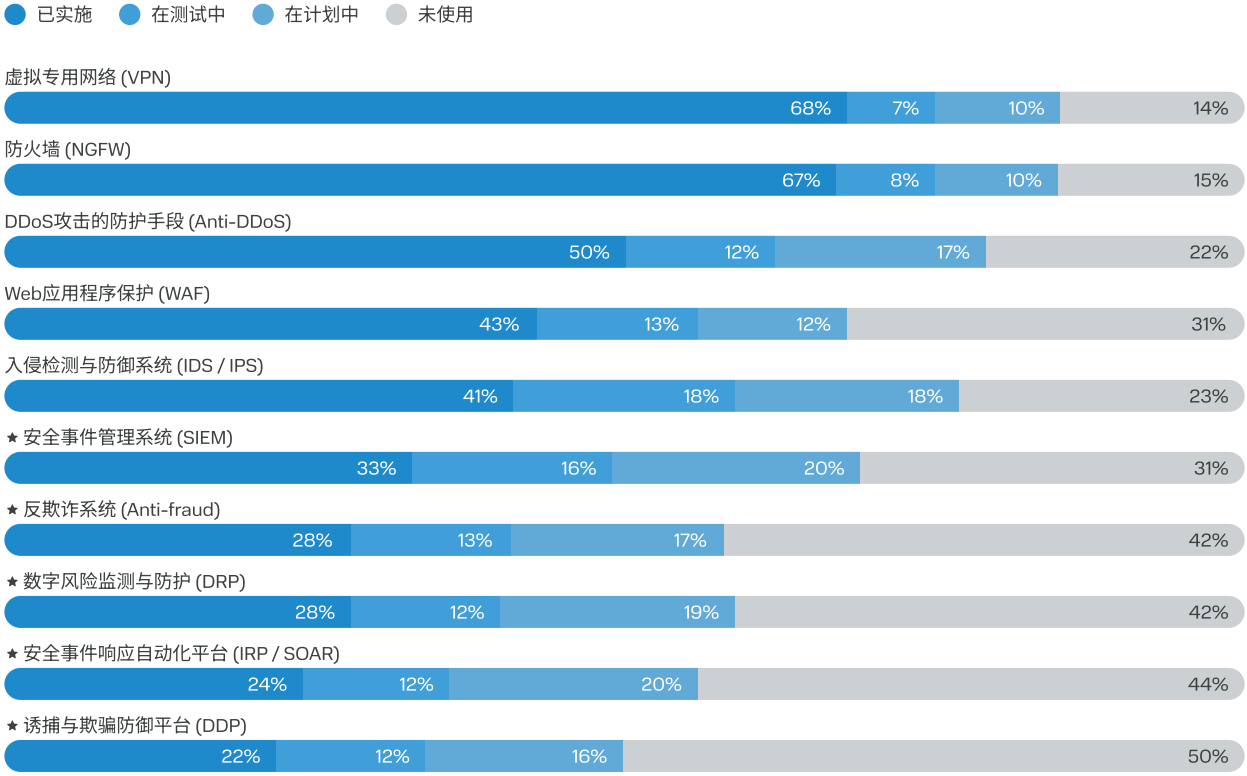
为评估各产品子类别中的高增长潜力方向，研究引入了名为“子类别增长潜力公式”的方法。该公式通过对比以下指标：一方面是“已实施”，另一方面是“正在测试”与“计划实施”两项指标之和。与“未使用”参数不同，这些数值能够正向反映受访企业的实施计划，可被解读为在近期内向“已实施”状态转化的较高可能性。

已实施 < 在测试中 + 在计划中 = 存在增长潜力

已实施 > 在测试中 + 在计划中 = 存在增长潜力

根据研究结果，最具发展前景的产品子类别为“基础设施安全防护工具”（在 10 项技术中占据 5 项高潜力方向）。该领域的高增长潜力同时受到技术趋势和经济因素的共同推动。 在技术层面，驱动因素包括：向云环境迁移、微服务架构、远程/混合办公模式的普及，以及从传统边界防护模型向 Zero Trust（零信任）模型的转变。在经济层面，影响因素包括：安全事件造成的损失增长、网络风险保险的发展以及网络安全专业人才的短缺。此外，风险的增长不仅源于网络威胁数量的持续上升，还包括软件产品开发与交付节奏加快、监管要求日益严格以及 IT 架构整体转型等因素。在此背景下，对先进的应用与基础设施安全防护手段进行投资，正成为企业降低网络风险、保障业务连续性的关键驱动力。

基础设施安全防护工具

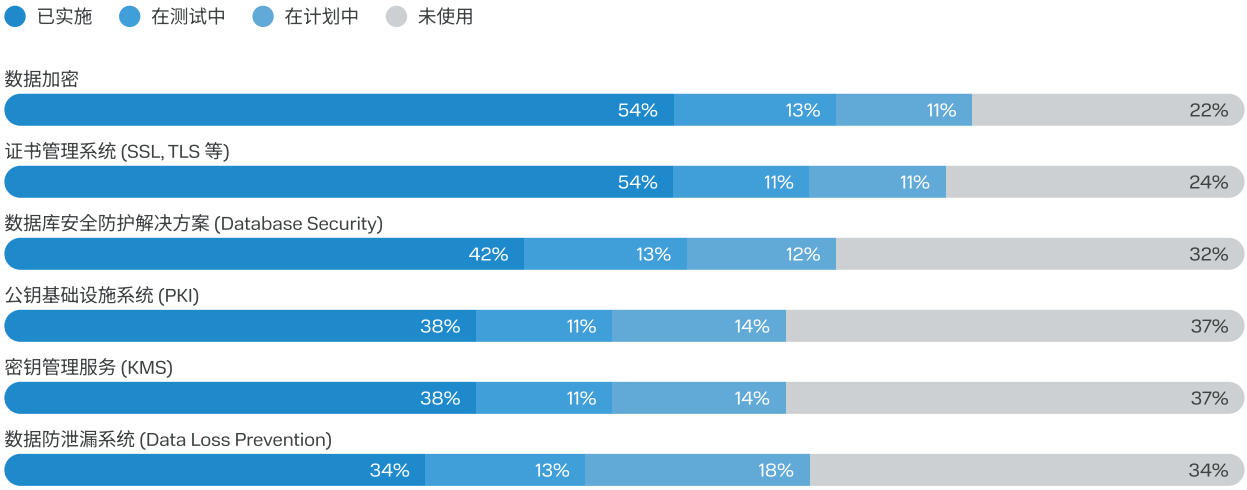


信息安全解决方案是本次分析技术中预算规模最大的领域。需要强调的是，这一趋势不仅源于对法律法规合规性的形式化要求，更源于对基础设施安全的现实威胁——在最大规模企业中，超过 60% 的受访公司在过去一年中遭遇过 DDoS 攻击。 此外，为加强对外部威胁的防护，企业普遍指出正在部署企业级 VPN 服务。下一代防火墙（NGFW）仍然是市场上使用最为广泛的产品之一（67% 的受访企业表示已实施）。可以预期的是，对软硬件一体化交付模式的高需求，主要集中在大型及超大型企业中。

在控股型企业中，拥有自有网络安全团队已成为一项基础实践（76% 的超大型企业受访代表对此予以确认）。然而，专业安全人才的招聘——包括基础设施安全方向的专家——仍然是一项突出挑战（43% 的受访企业指出该问题）。这一情况可能是多个产品子类别中“计划实施”比例较高、但尚未实际落地的重要原因之一。

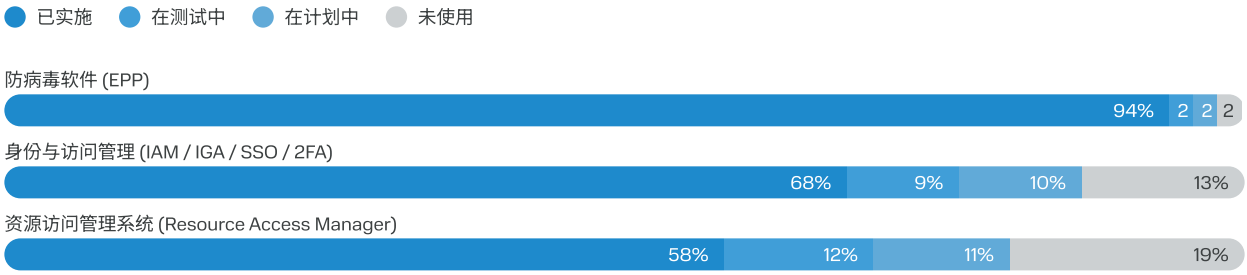
★ — 高增长潜力

数据安全防护工具



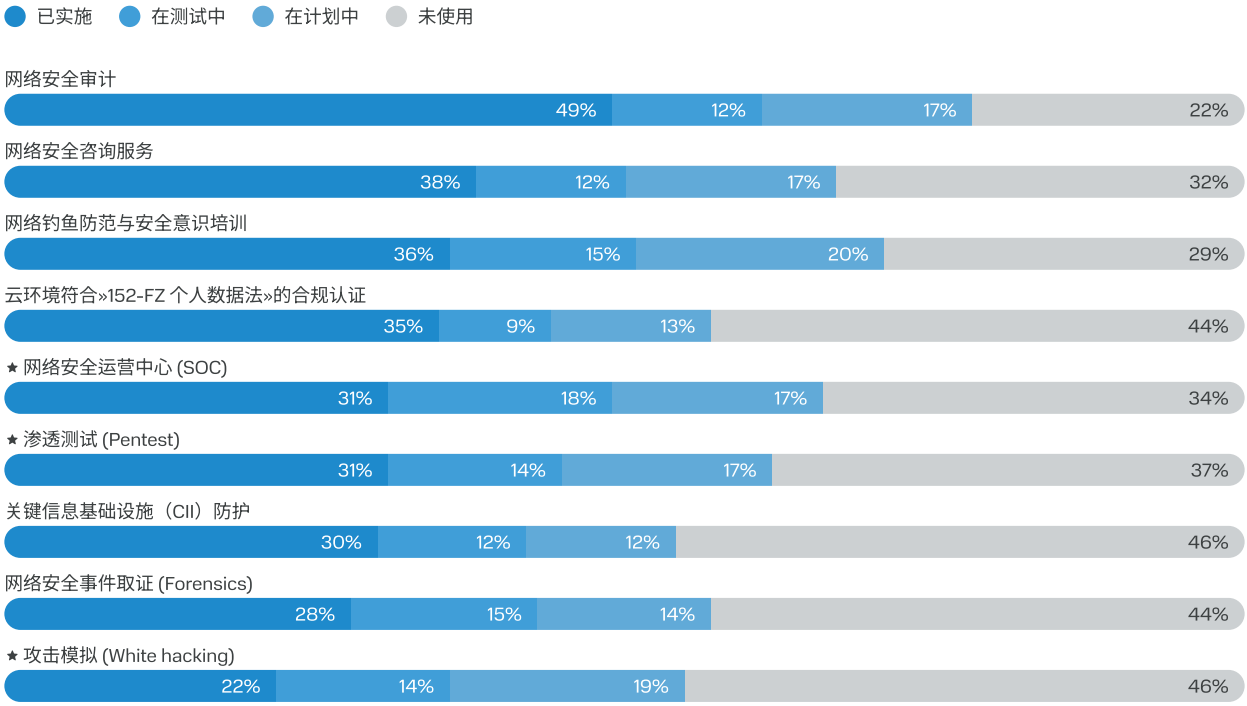
防范来自内部与外部的数据威胁是任何企业运营的基础性要素。大型生态型俄罗斯企业以及政府机构持续面临相关风险，这不仅会对内部运营流程造成冲击，还可能引发股东价值损失与声誉风险。受访者普遍将数据加密视为最为广泛应用的数据安全工具，与证书管理、访问权限控制以及其他应对外部威胁的安全机制并列。此外，许多受访者特别指出，DLP（数据防泄漏）是当前处于规划实施阶段的重要解决方案类别，该类产品在大型企业中的需求尤为突出。

用户与终端安全防护工具



在所有被分析的网络安全产品中，防病毒软件（EPP）的实施比例最高，达到 94%，这表明企业对潜在网络威胁具有较高的认知水平。该类解决方案已在俄罗斯市场形成标准化（commodity）产品形态。随着网络攻击复杂性和数量的不断增长，企业正通过扩大对访问控制与身份管理类产品的投入来应对相关风险。

网络安全服务

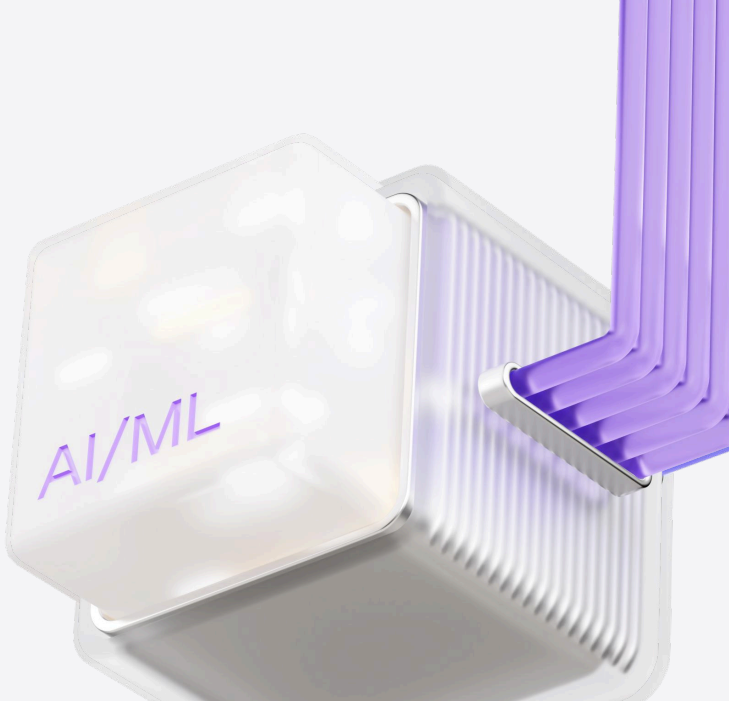


在俄罗斯网络安全市场结构中，软件（Software）与 IT 服务（IT-Services）两大垂直领域合计占比约 80%。其中，IT-Services 板块的年均增长率超过 30%。这一趋势与本研究样本中对相关网络安全解决方案消费规模的预期高度一致。相较于软件产品，网络安全服务的发展程度相对较低，主要原因包括：合格安全专家招聘难度较高，企业内部安全专业能力不足和建立自主网络安全职能体系的成本较高。

在各类网络安全服务中，网络安全审计在消费占比上处于绝对领先地位，这在很大程度上受到监管要求及公司股东层面合规指令的推动。按照此前用于识别高潜力产品子类别的方法（即“测试中”与“计划实施”的合计占比与“已实施”占比相当），在 IT-Services 领域中，可识别出以下具备显著增长潜力的服务类别：网络钓鱼防范与安全培训，网络安全运营中心（SOC），渗透测试（Pentest），攻击模拟（White Hacking）。

★ — 高增长潜力

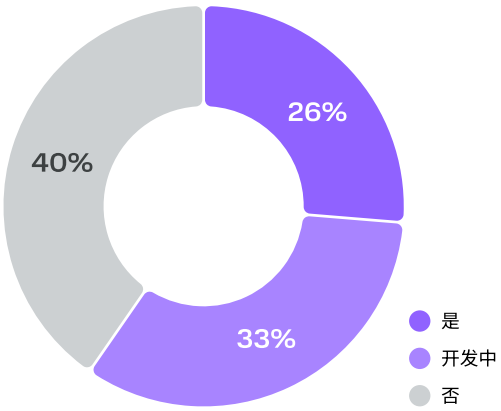
企业技术战略：人工智能



具备人工智能落地战略使企业能够以系统化方式推进该方向的发展，将 AI 融入整体业务架构，并实现资源的协调配置。

根据调研数据，仅有 26% 的受访企业已形成 AI 战略，该比例低于云计算战略（44%）和网络安全战略（42%）。与此同时，计划制定 AI 战略的企业数量高于其他战略方向。这一差异主要源于技术发展的高动态性，以及 AI 解决方案对大量企业而言仍具有较强的新颖性。

是否具备人工智能实施战略



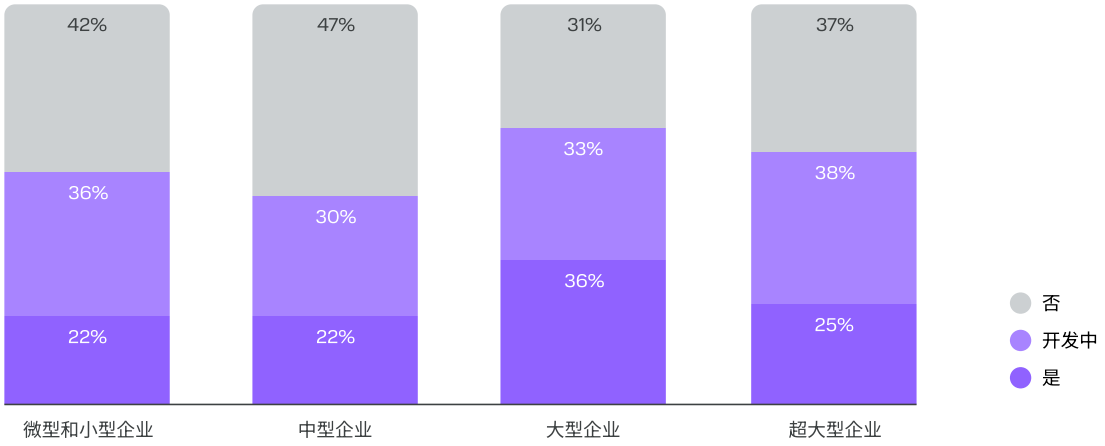
在 AI 战略成熟度方面，大型企业处于领先地位，其拥有更充足的资源和投资能力，用于自研 AI 产品的发展。而在规模最大的企业中，已形成完整 AI 战略的比例相对较低，这可能与其战略规划周期较长有关。从行业角度看，IT 行业、交通与物流领域以及科研机构在 AI 战略布局方面表现突出，这些行业在大规模数据处理流程中对 AI 的应用具有现实与刚性需求。

尽管成熟的 AI 战略尚未广泛普及，但各业务规模与行业的企业均在积极推进人工智能战略的制定

> 我们正在看到范式转移：从“样样都会、却难以真正落地”的通用生成式智能，转向能够产生可量化成果的专业化解决方案。面向具体业务场景和行业需求的应用型模型时代正在到来。企业愈发清晰地认识到，单纯的模型集成往往耗费大量时间和资源，而经济回报并不匹配。由此催生了新的趋势——用于构建和管理 AI 助手的平台型解决方案。一个新的解决方案类别正在形成，使企业不仅能够使用模型，更能够建立自有 AI 产品的持续生产流水线。当前，企业正迈入下一阶段——自主的 AI 转型，迈向以人工智能为核心构建的业务模式。

Denis Filippov
总经理
MWS AI 有限公司

按业务规模企业中 AI 落地战略的具备情况



在 67% 的企业中，围绕 AI 的决策主导权主要掌握在 CIO（首席信息官）手中，这在逻辑上源于其在信息技术领域的专业能力，以及对 AI 解决方案落地所涉及的基础设施和架构问题的深刻理解。CEO（首席执行官）以 23% 的参与度位居第二，体现出 AI 在最高管理层层面的战略重要性。

包括 CISO、CTO 和 CPO 在内的其他管理角色合计占比不足 11%，这表明在 AI 项目立项与决策过程中，安全、技术发展及产品负责人直接参与度相对有限。上述数据表明，AI 的落地在多数情况下仍主要由 IT 管理体系主导，并在战略层面获得公司高层的支持。该类决策结构可作为企业级 AI 解决方案制定客户策略与精准沟通方案的重要参考依据。

在多数受访企业中（55%），AI 解决方案的落地周期为 1 至 6 个月。其中，最常见的时间区间为 1–3 个月（29%），这表明企业普遍希望尽可能缩短 AI 项目的实施周期，以更快获得应用成效。

与此同时，仍有相当比例的组织面临更长的实施周期。这一现象可能反映出所部署解决方案本身的高度复杂性，或是企业内部存在组织层面的协调障碍，需要在多个管理层级之间进行决策与审批。

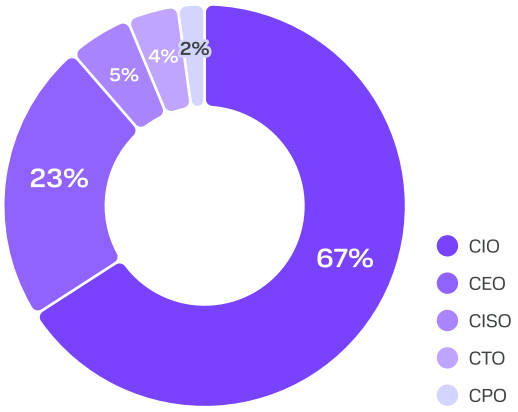
总体来看，相关分析显示，大多数企业倾向于较为快速地推进 AI 工具的落地，但仍有相当一部分项目具有超过半年的实施周期。在进行资源规划和制定 AI 项目路线图时，这一特征需要被充分考虑。

在 AI 的部署模式方面，受访企业中最常见的是私有云和公有云，两者各占 23%。约 20% 的企业采用本地部署 AI 负载，而混合云场景目前仍相对较少，仅有 13% 的企业选择该模式。

这一选择反映了企业希望通过云计算模型提升灵活性与可扩展性、降低资本性投入的同时，仍然在私有基础设施中保持对关键业务流程和核心数据的控制。

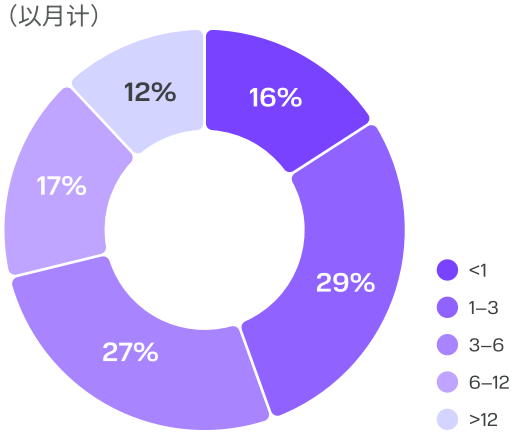
公有云能够支持更快速的业务适配与规模扩展，因此在负载波动或高速增长的应用场景中具备明显吸引力。相关数据进一步证实了企业正积极采用云技术，以提升 AI 系统的整体效率与安全性，形成清晰的行业发展趋势

在AI实施决策过程中发挥关键作用的人员



AI 解决方案实施周期

（以月计）

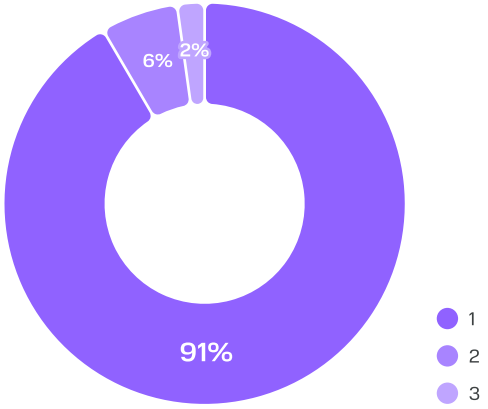


不同业务规模企业使用的AI供应商数量

多数受访企业（91%）仅与一家 AI 供应商合作。这种模式有助于企业将所选解决方案更好地适配自身的具体业务需求，同时简化基础设施管理，并降低因不同平台兼容性问题带来的风险。同时，与多家（2 家及以上）AI 供应商合作的企业比例仍然较低，总体约为 9%，这表明多供应商（multivendor）战略在 AI 市场中的普及程度仍然有限。

可以清晰观察到以下趋势：随着企业规模的缩小，完全不使用 AI 的公司占比逐步上升。在超大型企业（年营收超过 150 亿卢布）中，未采用 AI 的比例仅为 15%，而在年营收 20–150 亿卢布的企业中，该比例上升至 21%，在年营收低于 8 亿卢布的企业中，该比例约为 11%，但几乎所有这些企业仍然仅选择一家供应商。同时，使用两家及以上 AI 供应商主要出现在 AI 应用成熟度较高的企业群体中，即年营收超过 20 亿卢布的大型及超大型企业。

AI供应商使用数量



按行业年度AI支出规模

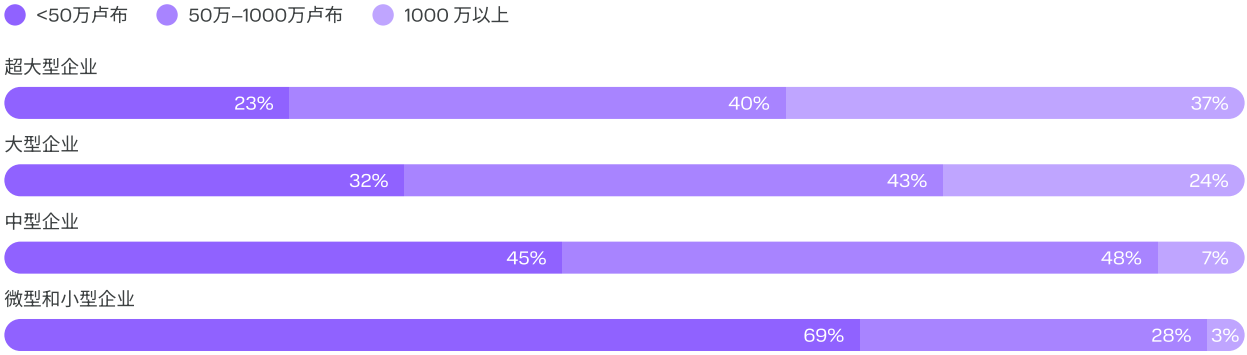
	< 50万卢布	50万–1000万卢布	1000 万以上
IT	42%	30%	28%
金融与保险	46%	34%	20%
矿产资源开采与加工	54%	27%	20%
科学教育	45%	41%	14%
娱乐与媒体	33%	58%	8%
零售业	56%	36%	8%
专业服务	82%	13%	6%
HoReCa	60%	35%	5%
工业	67%	28%	5%
交通与物流	55%	40%	5%
保健事业	54%	42%	4%
房地产与建筑业	66%	33%	1%

在当前阶段，人工智能领域呈现出明显的单一供应商（monovendor）模式：企业仍处于市场探索与初期应用阶段。

人工智能相关支出与企业规模呈正相关。如果不考虑微型和小型企业，各业务规模区间的中等支出占比大致相当，但在大型和超大型企业中，年支出超过1000万卢布的比例则显著上升。这种差异主要源于大型企业拥有自有研发团队，具备开发定制化解决方案的能力。正是市场领导者构成了对大规模 AI 项目的主要需求来源，并具备推进高资本密集型项目的能力。

按业务规模划分的 AI 年度支出规模

刻度表示按营收划分的业务规模，不同颜色表示对应的支出水平。



人工智能主要由大型企业推动，正是它们在解决方案的开发与适配方面进行核心投入

AI 投资规模最大的行业包括 IT、金融与保险、资源开采与加工、零售、交通与物流，以及科研与教育领域。这些行业的支出结构更加分散，其中相当一部分企业的投入已超出最低预算水平。尤为突出的是 IT 行业，其中 29% 的企业每年在人工智能方面的投入超过 1000 万卢布，显著高于其他行业的相应水平。这主要得益于 IT 行业数字化流程的高度成熟，以及业务对技术的直接依赖。

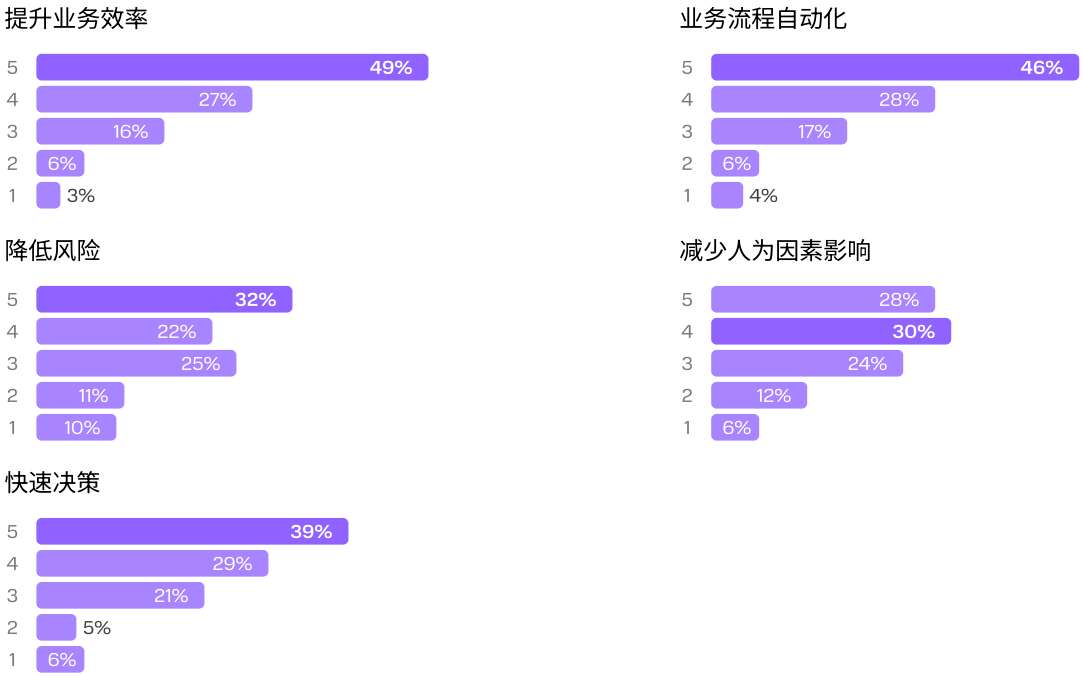
对于零售和交通运输行业而言，更为常见的是相对温和的预算，主要集中在每年不超过 2000 万卢布的区间，这与人工智能在需求预测、供应链管理以及服务个性化方面的广泛应用密切相关。科研与教育领域同样表现出对中等规模投资的倾向，这反映了其在大规模数据处理以及分析平台建设与发展方面的实际需求。

对于大多数企业而言，在决定是否引入人工智能时，关键因素包括提升业务效率（49%的受访者将该因素评为最重要）、业务流程自动化（46%）以及加快决策制定（39%）。

这三大方向构成了企业投资人工智能的核心业务动因，体现了企业降低成本、提升运营速度与灵活性的整体诉求。

企业在决定引入人工智能时的关键因素

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

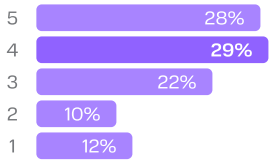


> 企业普遍预计引入人工智能将显著降低成本，但同时对与数据泄露相关的风险保持警惕。

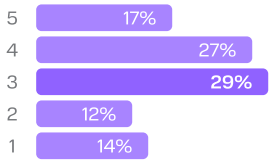
AI解决方案实施过程中的主要挑战 [1/2]

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

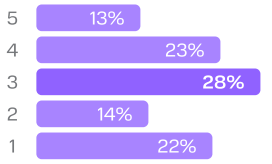
员工缺乏必要的专业能力



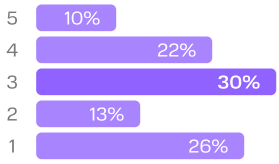
对所需基础设施预期成本的评估难度较高



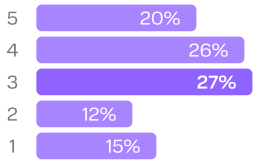
实施期间需要临时进行基础设施冗余



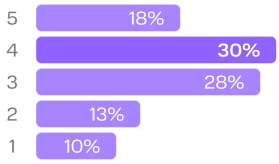
实施过程中缺乏厂商支持



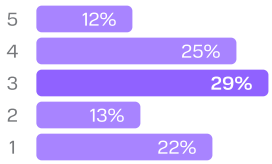
人工智能实施阶段产生的额外成本



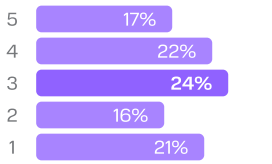
在市场上寻找基于人工智能的解决方案 / 工具或自行开发



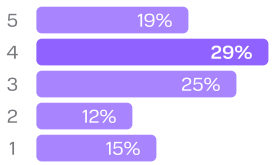
缺乏清晰的实施路线图



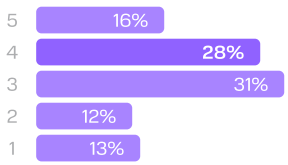
大规模数据迁移的复杂性



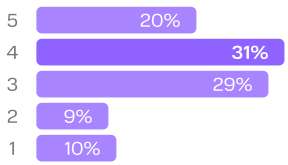
高额的财务投入



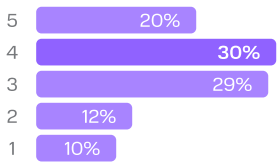
组织内部的规模化扩展难度



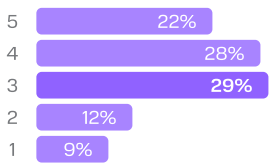
构建用于AI运行的必要数据平台



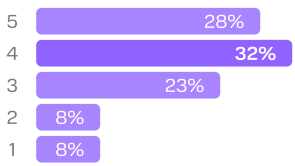
为高效使用人工智能而调整既有业务流程



对员工开展人工智能相关的培训与宣导



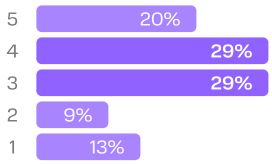
实现人工智能模型所需的质量水平



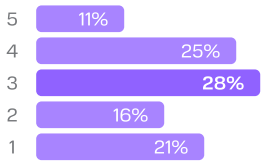
AI解决方案实施过程中的主要挑战 [2/2]

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

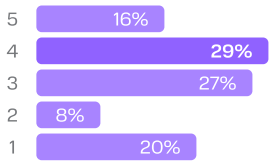
在公司内部形成关于人工智能关键应用领域的统一认知



所考察的服务商 / 厂商缺乏完善的技术支持方案（如 POC、Support 等）



AI工具无法与现有本地解决方案集成（老旧软件 / 硬件）



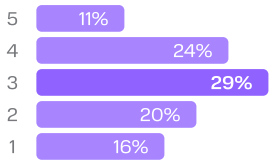
总体来看，受访者对人工智能实施过程中所面临的难点给予了中等重要性的评价，这表明尽管存在现实障碍，大多数企业仍然具备推进人工智能集成的意愿。总体而言，企业愿意为克服组织和技术层面的障碍投入资源，以获取人工智能应用所带来的长期收益，但人员培训问题仍是规划此类项目时需要优先关注的关键因素。

人工智能实施过程中产生的额外成本总体被受访者评估为中等重要性，这表明大多数企业已准备在其投资规划中纳入相关支出。最常被提及的因素是为保障人工智能高质量运行而进行员工再培训或招聘专业人才：29% 的受访者将该因素评为“非常重要”（4–5 分），另有 19% 给出了最高评分。对企业而言，最核心的挑战仍然是人才问题，需要持续投入以提升相关能力，从而确保人工智能解决方案的有效运行。这一结论与此前识别出的障碍相互呼应，包括技术专业能力不足以及与数据治理相关的风险，其中包括信息和个人数据泄露的威胁。

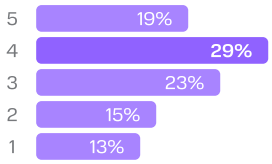
AI实施过程中的额外支出

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

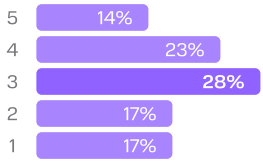
为验证所选解决方案可行性而部署测试环境



为保障人工智能高质量运行而对员工进行再培训 / 招聘专业人员



本地基础设施的更新与升级



在与人工智能实施相关的关键风险中，企业首先关注的是数据泄露风险——包括个人数据泄露（35% 的受访者给出最高严重性评分）以及商业机密泄露（34%）。这表明，在推进人工智能项目过程中，企业对安全性和数据保密问题具有高度敏感性。

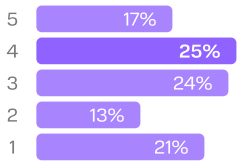
在人工智能领域，技术专业能力不足仍然是一个重要障碍：26% 的受访者将其评为最关键风险，另有 31% 给予了 5 分制中的 4 分重要性评价。同时，企业也对人工智能成本的不可控增长表示担忧，这进一步表明有必要为此类项目建立系统化的预算规划和 FinOps 管理实践。

风险表现相对不那么突出，但仍然具有现实意义的包括：供应商退出市场的风险、用于模型训练的设备采购难度，以及整体基础设施方面的限制。这些数据表明，对于企业而言，数据安全、相关能力的具备以及成本透明度，依然是决定是否推进大规模 AI 项目的关键因素，尽管此前已多次强调 AI 在优化日常任务和提升业务流程效率方面所带来的潜在收益。

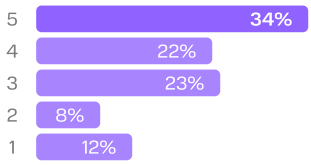
在实施AI解决方案过程中，下列风险类别的关键性评估

受访者评分范围为 1–5 分，其中 1 分表示影响最小，5 分表示影响最大

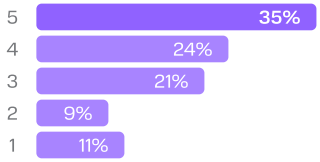
用于模型训练的设备采购难度



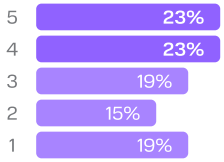
商业机密数据泄露



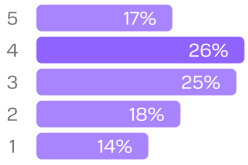
个人数据泄露



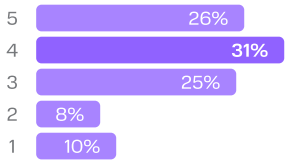
云服务商退出市场



AI相关成本的不可控增长



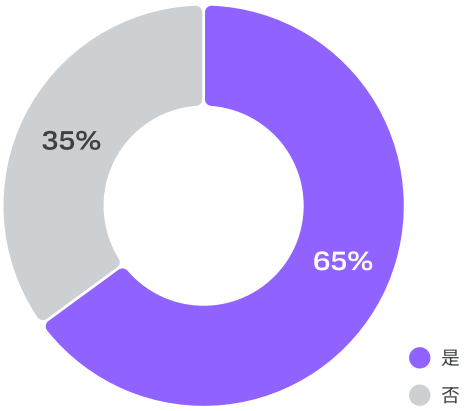
AI领域技术专业能力不足



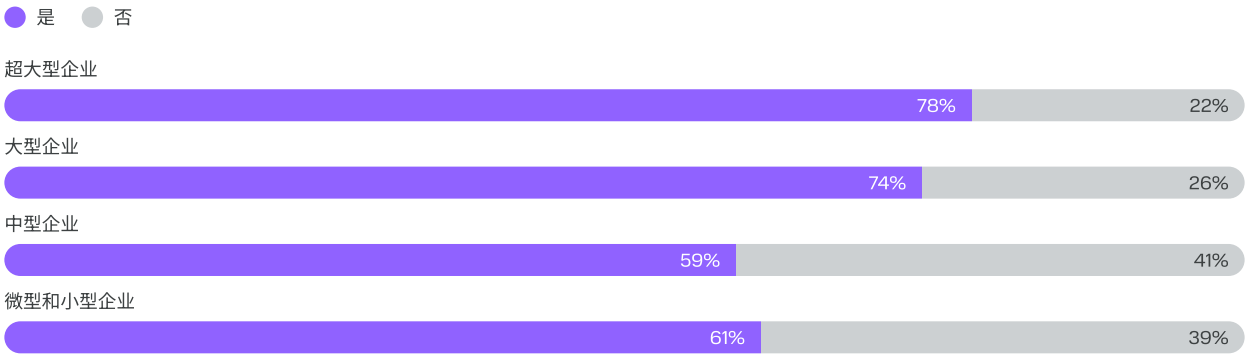
65% 的受访企业已具备人工智能应用经验与专业能力，这表明市场整体正持续向人工智能技术的应用与普及方向推进。 同时，数据也显示出能力积累水平与企业规模之间的直接相关性：大型企业更常拥有专业化的人工智能团队和相关经验，这与其在相关能力建设上的投资能力以及维持自有研发中心的资源条件密切相关。

在行业维度上，科研、IT 以及娱乐与媒体领域处于领先地位——在这些行业中，拥有 AI 专业人员的企业占比超过 80%。这在很大程度上源于这些行业的业务特性：大数据处理、预测算法和流程自动化已经成为其运营模式的组成部分。这些结果进一步证明，持续积累内部专业能力对于成功落地并规模化 AI 解决方案具有至关重要的意义。

是否具备AI相关经验与专业能力



按业务规模划分的AI经验与专业能力情况

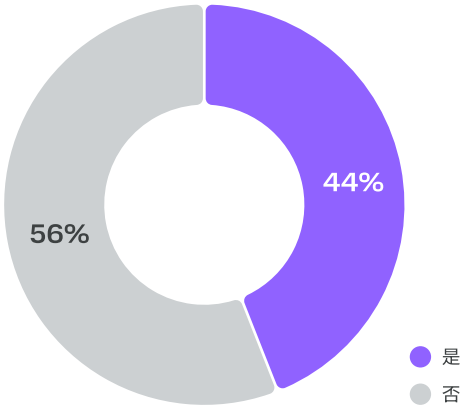


尽管相当一部分企业已经具备 AI 相关经验和专业能力，但高素质人才招聘依然是市场面临的重要问题：43% 的受访企业表示在吸引 AI 专家方面存在困难。该比例在不同收入规模的企业中基本一致，表明 AI 人才短缺具有明显的系统性特征。

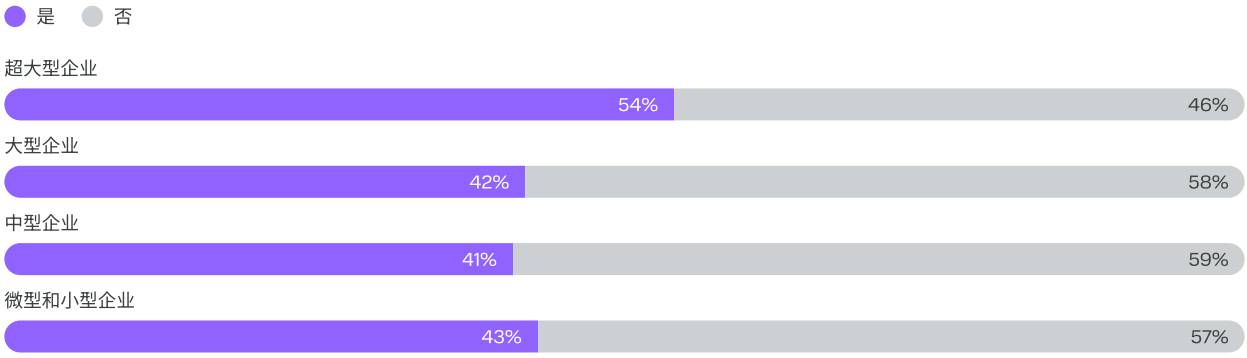
人才短缺问题在重工业（69%）、建筑与公共事业（61%）、制造业（60%）以及科研与教育领域（59%）表现得尤为突出。

这些行业对 AI 解决方案具有高度专业化要求，同时面临较高的监管门槛，并需要深入理解行业流程，从而显著增加了新专业人才的招聘与融合难度。

是否存在AI专家招聘困难



按业务规模划分的AI专家招聘问题情况

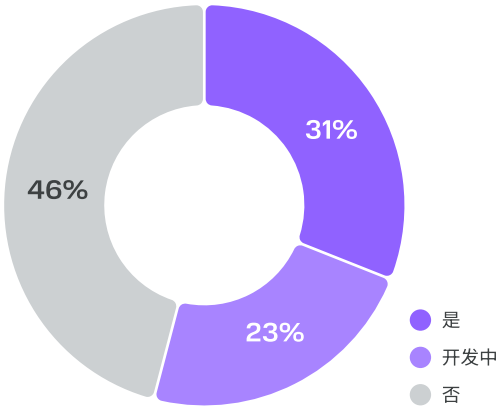


约三分之一的受访企业拥有自建的开发团队和数据科学家（Data Scientists）团队。此类团队的存在与企业在人工智能领域的方法成熟度呈现直接相关性，最常见于已经制定 AI 战略、并处于积极或持续实施阶段的企业。

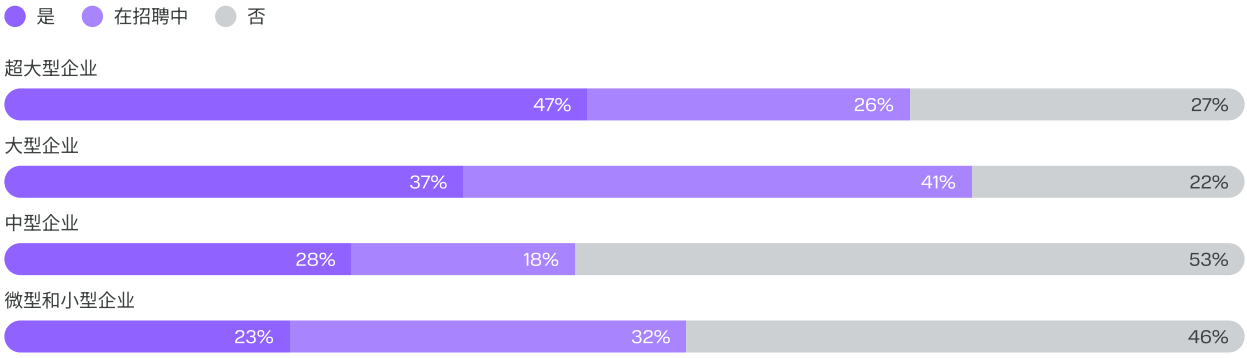
基于 AI 应用时长的分析显示出明确趋势：企业从事 AI 实施的时间越长，拥有自有团队的可能性就越高。例如，在 AI 使用时间不足一年的企业中，仅有 29% 拥有开发团队，而在实施经验超过 12 个月的企业中，该比例上升至 44%。这表明，在大多数情况下，AI 内部能力是在不断积累相关技术实践经验以及项目复杂度提升的过程中逐步形成的。

同样值得注意的是，大多数正处于团队建设阶段（通过招聘或员工再培训）的企业，其 AI 项目实施周期集中在 3–6 个月。这可能意味着，在这一阶段，企业开始从试点项目和标准化解决方案转向更复杂的应用场景，这些场景需要依靠内部专家对模型进行定制化配置和深度优化，以适应具体业务需求。

自有开发团队与数据科学家(Data Scientists)团队



按业务规模划分的自有开发团队与Data Scientists团队情况



弥补内部能力不足在一定程度上通过使用专业服务来实现。在受访企业中，用于人工智能发展的最常见服务是培训和技术支持，使用比例均超过 30%。相比之下，AI 咨询服务的普及程度较低，仅有 17% 的受访企业使用该类服务。这可能表明企业更倾向于自主推进 AI 的实施，但引入咨询服务有助于优化并加快 AI 落地进程，同时提供有价值的建议与最佳实践。

用于AI能力建设的专业服务类型

33%
培训

31%
技术支持

22%
模型训练

18%
集成

18%
定制化 AI 应用开发

17%
咨询（战略）

12%
模型推理

MTS WEB SERVICES

全面满足企业在 AI 服务与专业能力方面的需求

基于 AI 的成熟解决方案，具备可验证的实际成效

利润提升 20%

通过在数据分析中引入 AI，实现更精准的战略决策

研发部门生产效率提升 20–45%

在客户请求处理环节

时间缩短 60%

在客户请求处理环节

MWS GPT

面向企业的大语言模型（LLM）应用平台

24 小时	2 年	全部	
从模型申请到投入生产环境的周期	从模型申请到投入生产环境的周期	平台支持所有主流模型，并提供再训练能力	

MWS COSTUME AI

根据具体客户需求进行 AI 解决方案的定制化开发

技术落地：人工智能

人工智能章节涵盖了广泛的技术领域。本研究中人工智能市场的结构构建基于对 IT 市场进行通用拆分的方法。在本章节中，分析重点集中于硬件与软件两大技术纵向领域，并进一步划分为三类：（1）计算硬件；

（2）AI 智能体与应用；（3）AI 平台。与云计算和网络安全相比，企业客户在人工智能技术方面的发展仍相对滞后。综合预算规模、战略规划以及产品使用分析情况可以得出结论：对许多企业而言，相关 AI 解决方案仍处于实验阶段，尚未被大规模整合进企业核心流程。尽管专业领域高度关注人工智能，且在终端用户层面已广泛普及，但在 B2B 领域，相关解决方案仍具备巨大的未释放潜力。

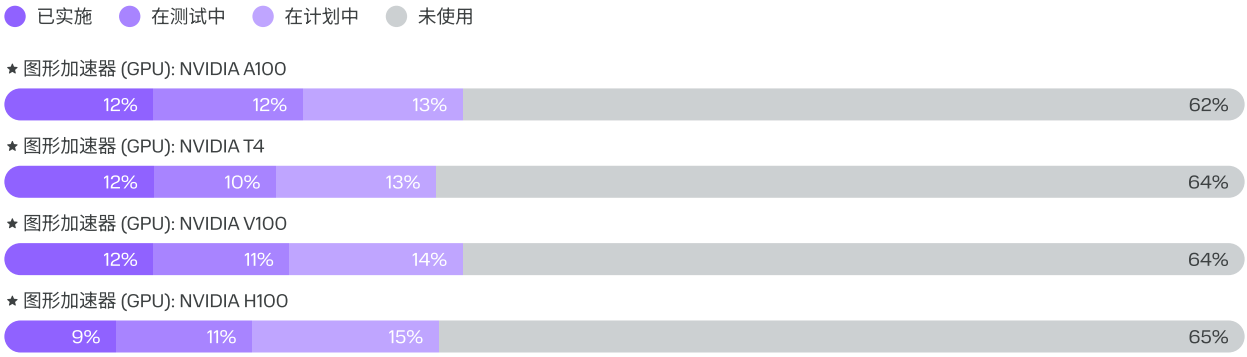
为评估各技术子类别中具备较高增长潜力的产品，引入了名为“子类别增长潜力公式”的方法。该公式通过对比以下指标：一方面是“已实施”，另一方面是“正在测试”与“计划实施”两项指标之和。与“未使用”参数不同，这些数值能够正向反映受访企业的实施计划，可被解读为在近期内向“已实施”状态转化的较高可能性。

已实施 < 在测试中 + 在计划中 = 存在增长潜力

已实施 > 在测试中 + 在计划中 = 增长潜力已被消耗

基于上述“子类别增长潜力公式”的评估结果显示，所有解决方案类别均具备较高的发展前景，包括通用应用型软件产品和行业垂直解决方案。AI 产品的高增长潜力源于多重宏观趋势的协同作用，包括业务流程数字化、机器学习工具的成本下降与能力提升、数据规模的指数级增长，以及企业在数据应用方面能力的持续提升。这意味着，人工智能投资将持续成为所有市场参与者的战略重点，尤其是那些不仅希望维持业务运转、更致力于实现市场领先的企业。

计算设备

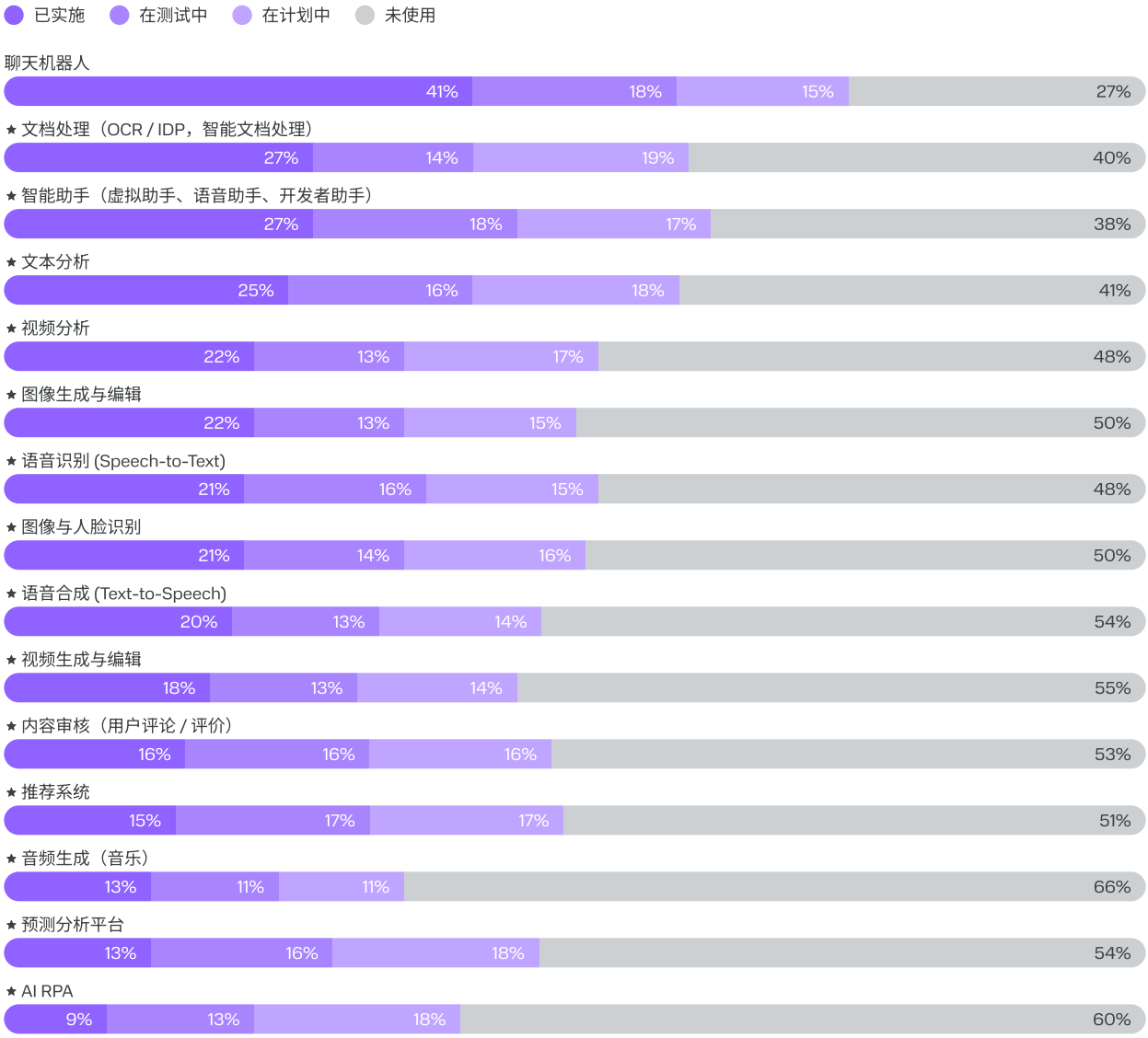


面向人工智能解决方案的硬件需求主要由大型及超大型企业以及生态型企业所驱动。此外，IT、金融科技（FinTech）、电子商务（E-Com）、营销科技（MarTech）、教育科技（EdTech）、医疗科技（MedTech）、保险科技（InsurTech）等技术行业的专业公司也形成了额外需求。从“测试中”和“计划中”两项指标来看，在“计算设备”类别中，受访者整体占比仍然较低。然而，基于此前提出的子类别增长潜力评估公式，可以看出受访者对该类解决方案的未来使用预期较高。

例如，不同型号 GPU 的部署比例彼此接近，但与传统 CPU 计算相比仍低约五倍。当前最受欢迎的显卡型号为 NVIDIA A100。该方案的价格约为 NVIDIA H100 的三分之二，使其对包括中小企业在内的更广泛企业群体更具可及性。尽管新的显卡供应链已逐步形成，但厂商在技术支持方面仍存在一定问题。从需求角度来看，硬件解决方案的终端用户在选择不同显卡型号时，必须将具体应用目标与设备性能进行严格匹配。

★ — 高增长潜力

AI 智能体与应用

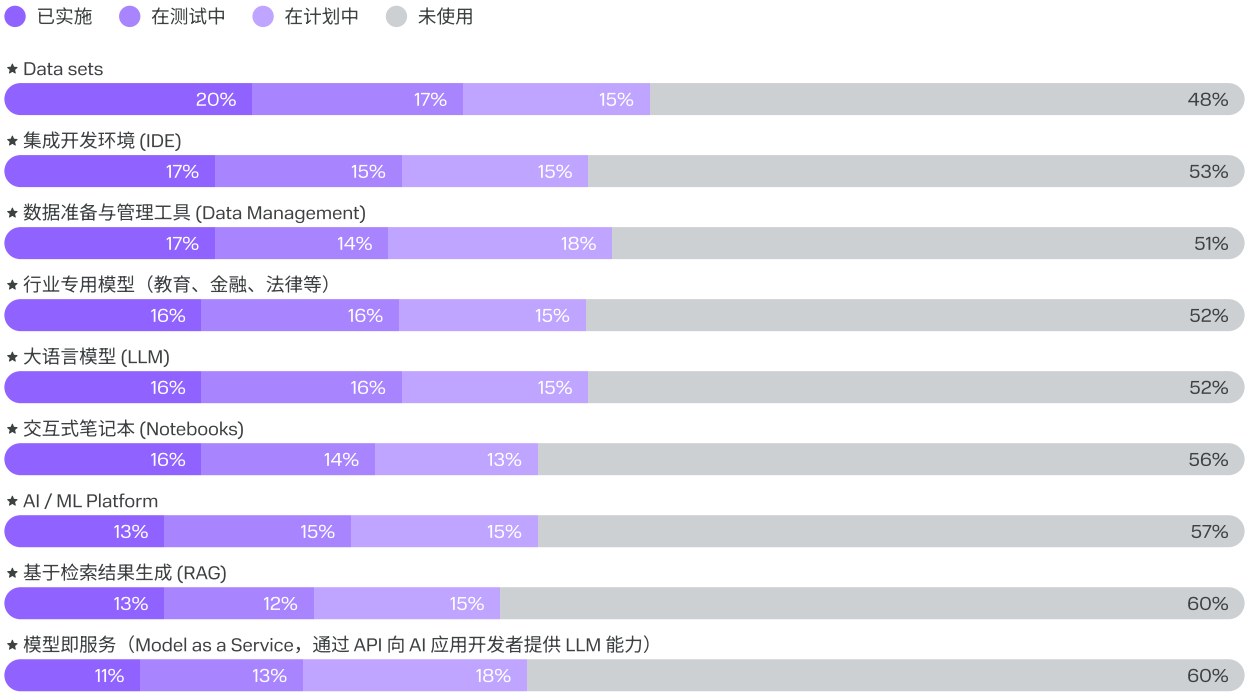


与“计算设备”类别相比，属于“AI 智能体与应用”的子类别展现出显著更高的部署水平。其中，“聊天机器人”子类别表现尤为突出，是本次研究中唯一一个“已部署”比例高于“测试中”和“计划中”的 AI 技术子类别。根据受访者反馈，该类解决方案已在 41% 的企业中部署，而“测试中”和“计划中”的比例分别为 18% 和 15%。其余子类别根据进一步部署潜力公式，均展现出显著的增长前景。聊天机器人的广泛应用不仅源于较低的部署成本，更主要在于其对企业和终端用户所带来的价值高度清晰且可量化。

“AI 智能体与应用”类别中较高的正向反馈比例，主要源于该类 AI 解决方案在试点和实验阶段具有较低的进入门槛，这在很大程度上得益于多数受研究产品采用云交付模式。此外，市场参与者对 AI 解决方案的积极态度，也与应用软件开发商、网络安全解决方案提供商及平台型厂商积极将上述子类别产品集成至自身终端产品中密切相关。

与其他具有高度专业化、用于解决特定垂直场景问题的解决方案（如推荐系统、预测分析平台和 AI RPA）相比，属于自然语言处理（NLP）和计算机视觉（CV）的子类别表现出更高的市场需求。

AI平台



在所有列示的子类别中，当前部署水平整体较低（11–20%），但“计划中”与“测试中”两项合计显示出较高的后续发展潜力（27–32%）。

除以云交付模式提供的自动化 AI 解决方案外，大型及超大型企业还在积极使用咨询公司和系统集成商提供的专业服务。上述市场参与者积极推进 AI 相关产品落地，并提供包括培训、技术支持、模型训练等在内的配套服务。

受访者普遍指出，其所在企业正在积极推进数据驱动（data-driven）发展路径，尤其强调了业务数据积累过程的系统化。实现该路径的关键不仅在于先进的 AI 工具，还依赖于基础云能力，尤其是分析工具；缺乏这些基础能力，将难以充分释放 AI 应用价值。

AI 技术的发展与其各子类别向云技术渗透密切相关。在此可观察到多种数据相关技术之间的直接相互依赖关系。云计算与存储系统以及平台型解决方案的进一步发展，将显著提升 AI 技术的可获得性，并降低其在各业务规模与行业中的应用门槛。

★ — 高增长潜力

结论

“

云计算技术、网络安全与人工智能并非只是并行发展，而是共同构建起一个高度互联的生态体系，其中任何一个领域的成功在很大程度上取决于其他领域的发展成熟度。这种协同式增长是保障单个企业客户以及国家整体经济竞争力的重要基础。

云计算技术，尤其是 IaaS 和 PaaS 细分领域，仍然是俄罗斯 IT 市场中发展最为迅速的组成部分。云计算技术仍然是俄罗斯 IT 市场中发展最为迅速的领域。

到 2025 年，该市场规模将增长 24%，达到 2080 亿卢布。根据最新评估结果，2024 年其合计占比约为整体市场规模的 5,1%，并有望在 2025 年超过 5,2%。对于相当数量的企业而言，虚拟数据中心和虚拟私有云事实上已成为一种基础设施标准，即通用化（商品化）的产品。与此同时，市场不仅对公有云方案保持稳定兴趣，也同样关注私有云与混合云场景，这符合企业对可控性、定制化能力以及降低供应商锁定（vendor lock-in）风险的不断增长需求。超大型客户正在推动对多云模型的需求，并积极测试融合多家云服务提供商的方案，以实现高可用性目标并实现服务差异化。

网络安全反过来正逐渐成为所有数字化战略中不可或缺的核心要素。从供给侧来看，国内市场已具备覆盖大多数关键领域的、自主研发解决方案的完整产品线。这使企业能够满足监管机构的合规要求，同时降低对外国供应商的依赖。总体而言，可以认为俄罗斯网络安全领域正处于技术稳定阶段，但仍保留演进式增长潜力——主要体现在功能扩展、自动化水平提升以及智能化防护机制的引入。

俄罗斯的人工智能市场目前仍处于构建稳定企业级实践的早期阶段。高性能计算基础设施（GPU 虚拟机与 HPC）的部署水平仍然相对有限——对这类资源的需求主要来自拥有强大自有数据科学团队的企业，而这类企业在整体市场中的占比仅约为三分之一。

从产品视角来看，人工智能被认为是具备最大增长与发展潜力的技术方向。该领域的解决方案对大多数产品而言具备较高的后续发展前景（其中 97% 的技术方向被认为具有较高的发展潜力）。云计算技术的落地比例更高，但具备显著增长潜力的细分方向数量相对较少（此类方向仅占 42%）。在所划分的子类别中，网络安全技术展现出的增长储备最为有限（仅约 30% 的方向被认为具备较高的增长潜力）。这些数据可能与网络安全风险对俄罗斯企业具有高度现实性和紧迫性密切相关。

基于对供给侧产品的补充性分析，尤其是在云计算领域，可以指出，在绝大多数产品方向上，国内服务提供商已形成由自主研发解决方案或经过深度改造的开源方案所构成的成熟产品组合。可以认为，当前市场供给不仅足以满足基础性的技术需求，也能够支持企业开展实验性与创新性活动。

Igor Zarubinskiy
MWS 执行董事，MWS Cloud 首席执行官

关键术语

公有云

一种云计算模式，其中 IT 基础设施（服务器、数据存储、网络）由第三方服务提供商拥有并负责管理，资源通过互联网向用户提供。用户（企业或个人）共享使用该基础设施。

私有云

仅由单一组织部署并使用的云基础设施。该基础设施可以物理部署在企业自有的数据中心（本地部署，on-premise），也可以部署在第三方服务提供商处，但所有资源均完全隔离，仅供单一客户使用。

混合云

一种将私有云与一个或多个公有云相结合的 IT 环境。

ON-PREMISE

一种部署模式，其中 IT 基础设施（服务器、软件、网络）直接部署并运行在企业自身场地内的自有数据中心，由企业自行管理。

MULTICLOUD

同时使用两个或以上公有云服务提供商服务的战略模式。

MWS CONTAINER PLATFORM

Надёжная платформа для разработки и эксплуатации контейнерных приложений. Помогает быстрее внедрять инновации, проводить цифровую трансформацию и запускать ИТ-продукты

на 40% снижает нагрузку на ИТ-команды	на 70% ускоряет выпуск новых приложений и упрощает их эксплуатацию	на 80% автоматизирует ручные операции	

AI CLOUD

Инфраструктура и сервисы для внедрения технологий ИИ в бизнес. ИИ-облако эффективно ускоряет цифровую трансформацию и оптимизирует бизнес-процессы

на 20% растёт прибыль за счёт более точных стратегических решений благодаря использованию ИИ при анализе данных	20–45% повышение производительности отдела разработки при использовании систем генерации кода	на 60% меньше времени на обработку обращений клиентов	

ВИРТУАЛЬНАЯ ИНФРАСТРУКТУРА С GPU

Готовая масштабируемая виртуальная инфраструктура для размещения любых информационных систем клиента, разработки и тестирования ПО, а также облачные серверы на базе NVIDIA для ускорения высоконагруженных вычислений и машинного обучения

≥5 минут на развертывание инфраструктуры	15 15 зон доступности	30% сокращение расходов на ИТ-инфраструктуру	

MTC Web Services (MWS)

面向人工智能实验与企业数字化转型的企业级云服务与产品。公司提供先进技术、深度专业能力、全面支持以及可靠的基础设施，助力客户实现新的业务高度。MWS 的解决方案包括计算与存储服务、用于 AI 和 ML 模型训练的基础设施、数据库、业务应用、网络服务以及面向开发者的解决方案。

MWS Intelligence Team

该团队负责在俄罗斯云计算市场中的分析与研究领导地位。我们整合全球及俄罗斯在云计算、人工智能、网络安全以及整体信息技术领域中的最佳实践。