



2022年 全国网民网络安全感满意度 调查专题报告

行业发展报告专题

(行业发展与生态建设、新技术应用与网络安全、科技创新与人才培养)

复旦大学网络空间国际治理研究基地

2022年11月

本报告数据来源于 2022 网民网络安全感满意度调查活动，任何组织和个人 引用本报告中的数据和内容须注明来源出处。

组委会欢迎有关研究机构合作，深入挖掘调查数据价值，有需要者请与组委会秘书处联系。

报告查询(总报告及区域、专题、行业报告):网络安全共建网:www.iscn.org.cn “网安联”公众号:



2022 年全国网民网络安全感满意度 “行业发展报告” 专题调查报告

复旦大学网络空间国际治理研究基地

2022 年 10 月

目录

一、前言	1
二、主要发现	2
2.1 网络安全状况总体较为稳定，相较于去年有不同程度改善	2
2.2 网络安全监管力度较强，细分领域问题仍较为突出	2
2.3 网络安全产品与服务发展政策环境整体偏佳，产业链供应问题需重视	2
2.4 信息技术产品自主可控生态较完善，关键产品国产化配套取得成效	2
2.5 加快研发迭代网络安全新技术、新产品，加强人才队伍建设	2
2.6 网络安全测评机构数量充足，测评细分服务需求旺盛	2
2.7 网络安全未来发展较乐观，行业发展制约因素较集中	3
2.8 信创、工控、物联网等领域技术应用和安全风险较高	3
2.9 人工智能（AI）期待度较高，发展阻力较大	3
2.10 区块链和大数据普及推广程度偏低，落地应用问题较多	3
2.11 数字政府与智慧城市新技术应用受到好评，网络安全保障需加强	3
2.12 网络安全科研经费预算水平欠佳，主要依靠市场力量	4
2.13 网络安全科研课题立项和管理欠佳，科研工作多方面仍需改善	4
2.14 安全领域教育培训工作亟需加强	4
2.15 网络安全专业人才评价和队伍建设存在问题，专业人才待遇不高	4
三、从业人员基本情况	5
3.1 从业人员基本情况	5
四、网络安全行业发展主问卷分析	9
4.1 网络安全感知	9
4.2 网络黑产	12
4.3 网络安全治理	15
五、专题分析	19
5.1 行业发展与生态建设	19
5.2 新技术新应用与网络安全	30
5.3 科技创新与人才培养	40
六、结论	50

一、前言

随着网络信息社会发展，互联网已与人民群众日常生活密不可分。网络在提供各种生活便利和沟通便捷的同时，网络威胁也在增长：网络攻击、病毒传播、垃圾邮件等屡见不鲜；利用网络进行诈骗、盗窃、敲诈勒索、窃密等案件逐年上升，严重影响网络的正常秩序，损害网民权益；网上色情、暴力等不良和有害信息的传播，正在严重危害青少年的身心健康。如何加强网络安全社会治理、保障广大人民群众上网用网安全，日益成为社会广泛关注的重大问题。开展网络安全满意度调查，旨在进一步贯彻习近平总书记关于“网络安全为人民，网络安全靠人民”网络强国的重要思想，切实落实《网络安全法》及相关法律法规，增强网民的网络安全意识和防范能力，促进互联网企业履行社会责任，提升网民网络安全感和满意度，最大限度调动网民参与网络生态治理的自觉性和主动性，助力政府相关部门积极探索网络治理规律，提高综合治理的成效和水平。

网民网络安全感满意度调查的宗旨就是要坚持面向网民大众，目的是让大家有话可以说，让政府主管部门可以倾听和了解网络安全在网民中的感受、网民的诉求和存在的问题。同时也向广大网民宣传网络安全的相关政策、法律和知识。

为充分发挥网络安全社会组织在网络空间建设中的作用，切实履行网络社会组织的社会责任，全面提升社会组织服务国家及地方政府网络安全建设水平，促进全国网络安全事业的发展，从 2018 年开始由全国多家网络安全社会组织联合发起了每年一度的全国网民网络安全感满意度调查活动，调查活动及其报告引起社会巨大反响。2022 年度全国网民网络安全感满意度调查活动在抗击新冠疫情取得阶段性胜利和国际形势跌宕起伏，复杂多变的背景下进行，具有特别的意义。本年度调查活动由全国 135 家网络安全行业协会及相关社会组织联合发起，公安部网络安全保卫局作为指导单位对活动给予了大力的支持。活动组委会在总结过去几年的网民网络安全感满意度调查活动经验基础上，今年的调查活动在活动组织、品牌建设、推广发动、研究规划、问卷设计等方面进行了多方面的创新和改进，取得显著的效果，活动影响力和问卷数量实现跨越式增长。

本报告是基于 2022 年度网民网络安全感满意度调查活动收集回来的有效问卷数据，经过整理、统计、分析后编写形成的。报告力求全面、客观地反映参与调查的行业从业人员的真实感受，为有关各方提供参考。

二、 主要发现

本次活动共收回从业人员版网民网络安全感满意度调查问卷有效问卷 465679 份。经过对调查数据统计、分析后，有以下主要发现：

2.1 网络安全状况总体较为稳定，相较去年有不同程度改善

(1) 全国范围内，63.99%从业人员对网络安全状况的评价较为积极；同时，有 78.11%的从业人员认为 2022 年的网络安全状况相比较 2021 年有不同程度的改善。

(2) 网络黑产发展势头受到一定遏制，有 36.5 的从业认为认为网络黑产发展有不同程度的减少；作为比较，有 32.12%的从业人员认为网络黑产发展势头有所上升。从业人员认为，整治网络黑产的关键入手点是信息、流量和帐号。

2.2 网络安全监管力度较强，细分领域问题仍较为突出

(3) 大多数从业人员对目前的网络安全监管力度给予积极评价，其中表示监管力度非常强的占比 21.66%，比较强的占比 33.73%。

(4) 在调查从业人员认为目前最突出的网络安全问题时，网络诈骗（59.71%）和数据泄露（57.57%）的投票数偏高，比排名第三的选项至少高 20%个百分点。从业人员认为目前维护网络安全最需采取的措施是加强网络安全法制建设（63.80%）。

2.3 网络安全产品与服务发展政策环境整体偏佳，产业链供应问题需重视

(5) 超过一半的从业人员对目前的网络安全产品与服务发展政策环境评价持正向态度（51.29%），较多的从业人员认为网络安全需求出现增长的迹象（55.4%），但是仅有不到一半的人对经济环境评价为正向态度（48.44%）。

(6) 在调查从业人员察觉到的信息技术产业供应链安全问题的威胁时发现，22.36%的人认为安全威胁非常高；认为安全威胁比较高的人占比最多，达 34.21%，两者相加超过半数（56.57%）。

2.4 信息技术产品自主可控生态较完善，关键产品国产化配套取得成效

(7) 超过半数的从业人员对于目前信息技术产品自主可控生态完善程度评价较为积极（59.11%），超过 60%的人都认为其工作单位的关键信息技术产品国内配套能够在不同程度上满足要求，数据显示目前关键信息技术产品的国产化、国产配套工作取得一定成效。

2.5 加快研发迭代网络安全新技术、新产品，加强人才队伍建设

(8) 对于网络安全产品与服务存在的问题，从业人员认为最突出的是体验差（59.84%）；同时，只有不到一半的从业人员认为目前的网络安全新技术、新产品的研发能适应网络安全形势发展的需要（49.08%）。

(9) 在专题调查中，有 58.57%的从业人员表示所在单位的网络安全岗位数量有一定程度增长，但是对于行业内网络安全技术人才数量的评估，只有 20.13%的人认为非常充足，22.88%的人认为比较充足。数据显示，需要进一步加强网络安全行业的技术人才队伍建设。

2.6 网络安全测评机构数量充足，测评细分服务需求旺盛

(10) 只有不到一半的从业人员表示目前测评机构的数量是充足的(49.06%)，当前网络安全测评机构数量还有进一步增加的空间。在调查从业人员认为所在单位还需要测评机构提供哪些服务时，安全监理(62.76%)和安全运维(52.64%)的需求较为强烈，超出第三名将近 20 个百分点。

2.7 网络安全未来发展较乐观，行业发展制约因素较集中

(11) 参与调查的从业人员对网络安全行业未来一年发展趋势的评价，给予正向态度的超过半数(56.35%)，在进一步分析制约网络安全行业发展的主要因素中，从业人员认为排名前 3 的是：人才(75.20%)、技术(65.08%)和政策(59.79%)。

2.8 信创、工控、物联网等领域技术应用和安全风险较高

(12) 在调查信创领域存在的新技术应用问题时，排名最高的 3 项分别是：价格贵，成本高(63.81%)、技术不成熟，稳定性、兼容性不足(56.84%)、系统不够安全(51.52%)；在调查工控领域存在的网络安全问题时，排名最高的 3 项分别是：核心技术自主可控度不高(65.89%)、资产暴露数量多(57.48%)、工控领域网络安全监管力度不够(56.76%)；在调查物联网安全风险主要存在哪些方面时，排名最高的 3 项分别是：信息安全风险高(65.58%)、物联网使用人员易误操作(62.28%)、物联网设备不安全(52.09%)。

2.9 人工智能(AI)期待度较高，发展阻力较大

(13) 在调查的从业人员最期待人工智能(AI)在哪些领域发挥优势时，排名最高的 3 项均超过 50%，分别是：交通(60.51%)、教育(54.19%)和医疗(52.55%)。但是在进一步分析人工智能应用发展面临的阻力时，有 4 项均超过 50%：社会接受(59.58%)、安全隐私问题(58.98%)、技术有待成熟(52.29%)、投资不足(51.38%)。

2.10 区块链和大数据普及推广程度偏低，落地应用问题较多

(14) 总体上从业人员对于区块链的了解程度是非常欠佳的，从业人员表示非常了解区块链的只有 17.12%，表示了解的只有 19.08%，给予积极态度的占比不到半数(36.2%)。同时，从业人员普遍反馈，区块链的标准规范、应用场景、技术和安全均有待成熟。

(15) 从业人员有 47.64%表示所在单位已经应用大数据技术，不足半数，同时仍有 25.97%的人表示没有应用。在调查的从业人员认为当前大数据技术应用存在的问题时，以下 3 项投票率较高：管理层尚未决定布局(57.44%)、专业人员匮乏(49.42%)、缺少数据共享政策规范支持(45.90%)。

2.11 数字政府与智慧城市新技术应用受到好评，网络安全保障需加强

(16) 参与调查的从业人员对于数字政府和智慧城市中新技术的应用效果评价时，超过半数的人给予积极态度(51.24%)，在进一步调查从业人员认为数字政府和智慧城市新技术应用存在问题的主要原因时，排名前 3 的是：过度强调数字化技术，忽略弱势群体对传统服务的需要(49.34%)、技术不成熟，不实用(41.07%)、核心技术和关键产品自主可控(39.44%)。

(17) 在调查从业人员对加强新技术应用网络安全保障的建议时，排名前 3 的是：强化标准引领，构建安全评估体系(72.91%)；加强自主创新，加快技术研发(69.48%)；健全行业监管，加大执法与惩戒力度(59.59%)。

2.12 网络安全科研经费预算水平欠佳，主要依靠市场力量

(18) 在调查从业人员所在单位网络安全领域的专门科研经费预算时，评价持正向态度的不足半数（43.54%）。具体而言，17.03%的人认为预算充裕，26.51%的人认为预算较充裕；另外，有 9.53%的人表示其单位没有专门的预算经费，17.81%的人表示预算较少。

(19) 通过科技创新与人才培养专题调查发现，只有 10.18%的单位政府支持网络安全科研专门经费占比超过 50%，12.84%的单位占比在 30%~50%之间，获得政府支持比例超过 30%的单位不足 25%。

2.13 网络安全科研课题立项和管理欠佳，科研工作多方面仍需改善

(20) 对于从业人员所在单位的网络安全科研课题立项和管理满意度，持有积极态度的不足半数（47.79%），另外持有负面态度的占比 32.16%。数据显示，从业人员对于所在单位网络安全科研课题立项和管理方面的满意度不高。

(21) 在调查从业人员认为网络安全科研工作开展在哪些方面需要改善时，排名前 3 的选项是：立项评选（57.49%）、课题规划（54.93%）、经费管理（50.25%）。

(22) 专题调查中，对于网络安全方面的科研成果转化的满意度，持有积极态度的不足半数（46.77%），另外持有负面态度的占比 23.7%。数据显示，从业人员对于网络安全方面的科研成果转化的满意度不高。同时，在进一步调查科研成果转化不满意的原因时，排名前 3 的选项是：成果保护（72.80%）、保障服务（61.46%）。

2.14 网络安全领域教育培训工作亟需加强

(23) 从业人员对于网络安全领域继续教育培训服务供给评价，持有积极态度的不足半数（33.79%），另外持有负面态度的占比 33.32%。数据显示，网络安全领域继续教育培训服务供给市场还有较大的深耕提升空间。

(24) 从业人员认为网络安全领域继续教育培训服务供给最大的问题是培训监管不到位（55.64%）。

(25) 在进一步调查从业人员认为网络安全继续教育领域存在的科目缺失或不足时，有 3 个选项的投票率超过 50%：计算机网络安全管理（69.82%）、网络安全检测与方法技术（61.34%）、网络安全协议与标准（52.60%）。

(26) 从业人员表示，他们在过去的一年接受过的网络安全培训，最多的 3 项是：本单位组织的培训（63.84%）、专业机构组织的培训（61.54%）、参加相关专业论坛和研讨会等（59.34%）。

2.15 网络安全专业人才评价和队伍建设存在问题，专业人才待遇不高

(27) 在调查从业人员认为网络安全专业人才评价和队伍建设方面存在的问题时，以下 3 项超过 50%：任职资格管理不完善（54.21%）、专业不对口（53.61%）、实训环境不足（51.94%）。

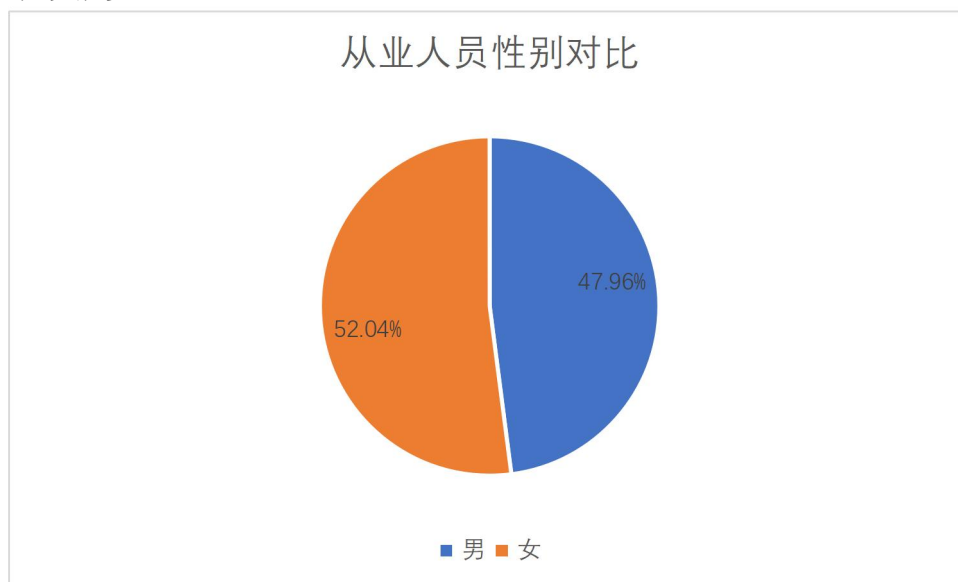
(28) 在调查从业人员单位内部网络安全专业人才待遇时发现，持有积极评价的不足半数（37.43%），另外有 33.31%的人认为其单位内部网络安全专业人才待遇是偏低的。数据显示，网络安全专业人才待遇不高。

三、 从业人员基本情况

3.1 从业人员基本情况

(1) 性别分布

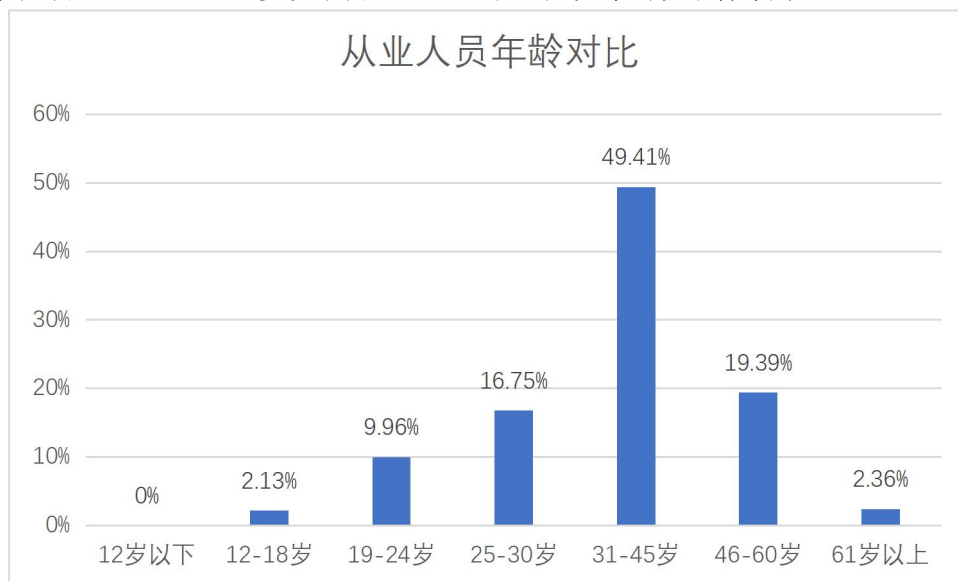
参与本次调查的从业人员中男性占 47.96%，女性网民占 52.04%，从数据上女性从业人员居多。



图表 3.1-1：从业人员性别对图

(2) 年龄对比

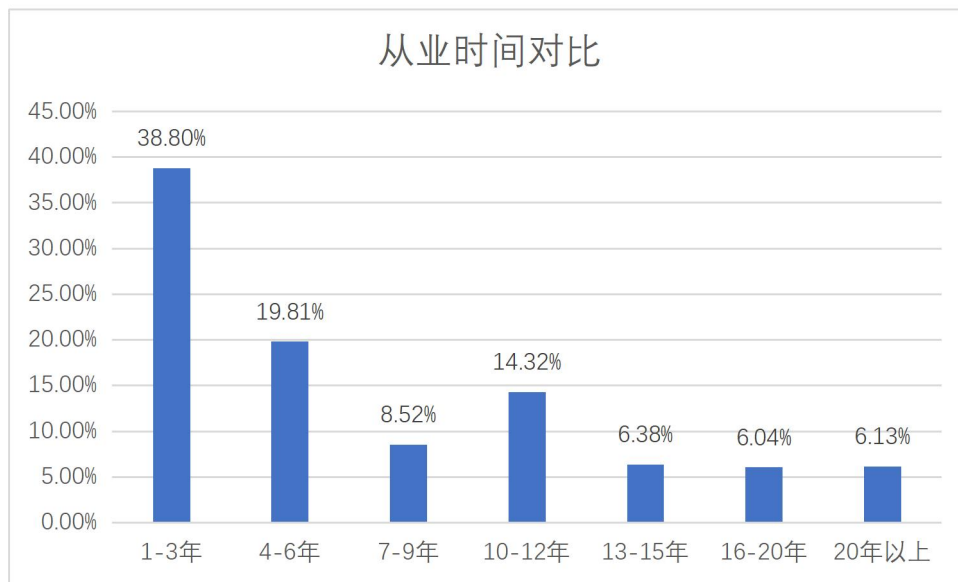
参与调查的从业人员中处于中年人的占大多数，其中，12 岁到 18 岁占 2.13%，19 岁到 24 岁占 9.96%，25 岁到 30 岁占 16.75%，31 岁到 45 岁占 49.41%，即 30 岁以下年轻人占约 28.84%。45 岁以下占 78.25%，从业人员年龄以中青年为主。



图表 3.1-2：从业人员年龄对比

（3）从业时间对比

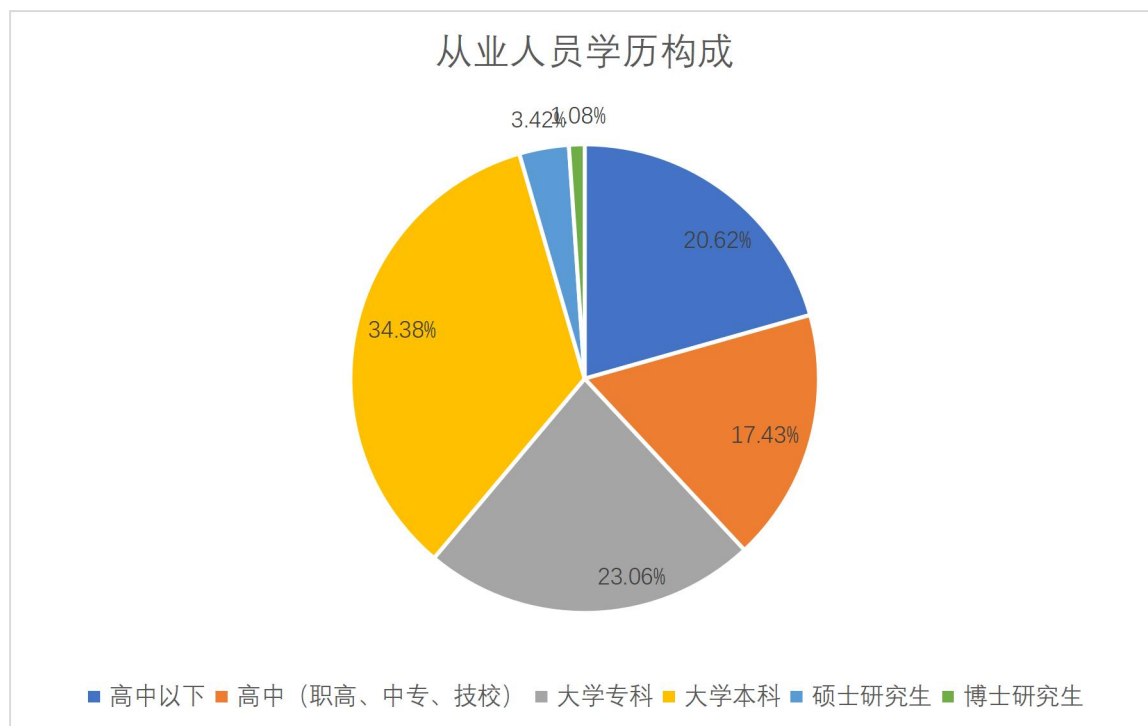
从业人员中从业时间在 12 年及以下的占大多数，其中，1-3 年的占 38.8%，4-6 年的占 19.81%，7-9 年的占 8.52%，10-12 年的占 14.32%，即从业时间在 12 年及以下的人数占 81.45%。



图表 3.1-3：从业时间对比

（4）学历构成

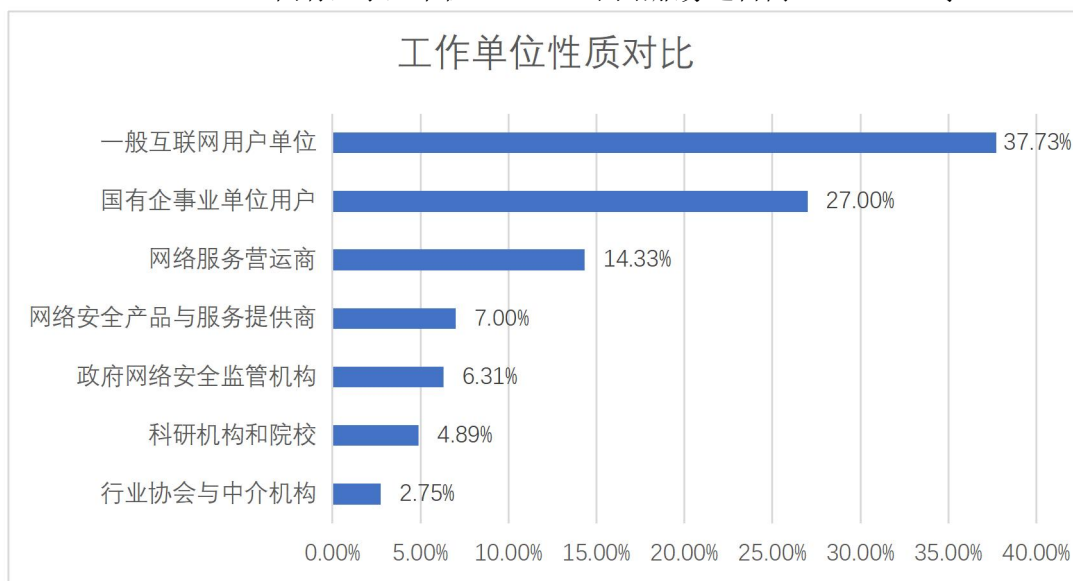
参与调查的从业人员中大学本科的人数最多，占 34.38%，其次是大专学历，占 23.06%，大专以上学历为 61.94%，反映出参加本年度调查问卷的被访者文化水平较高。



图表 3.1-4：学历构成

（5）工作单位性质对比

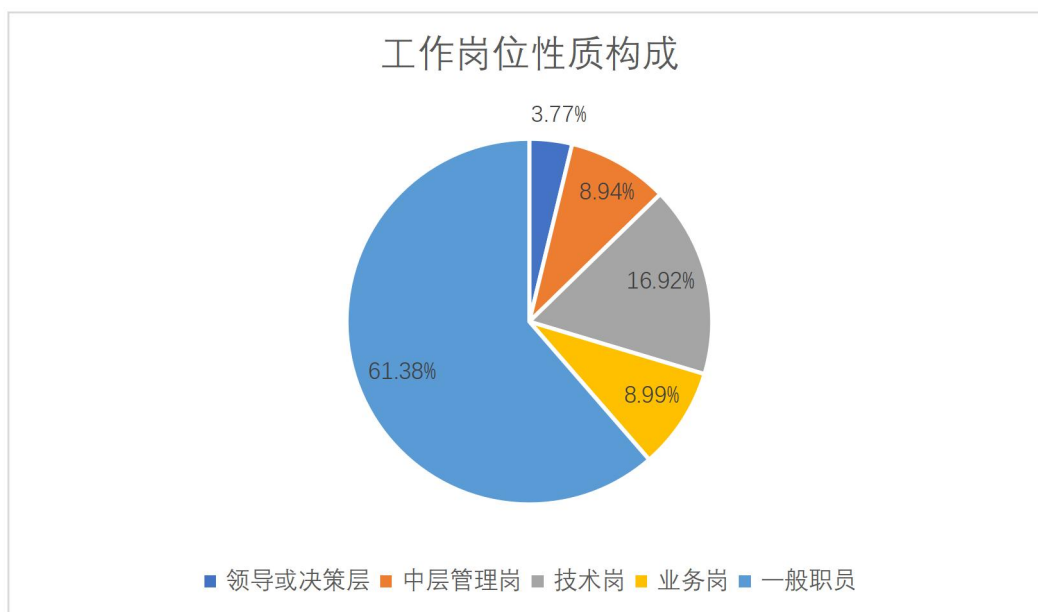
参与调查的从业人员的工作单位占比排名前三的是：一般互联网用户单位（37.73%）、国有企事业单位（27%）、网络服务运营商（14.33%）等。



图表 3.1-5：工作单位性质对比

（6）工作岗位性质构成

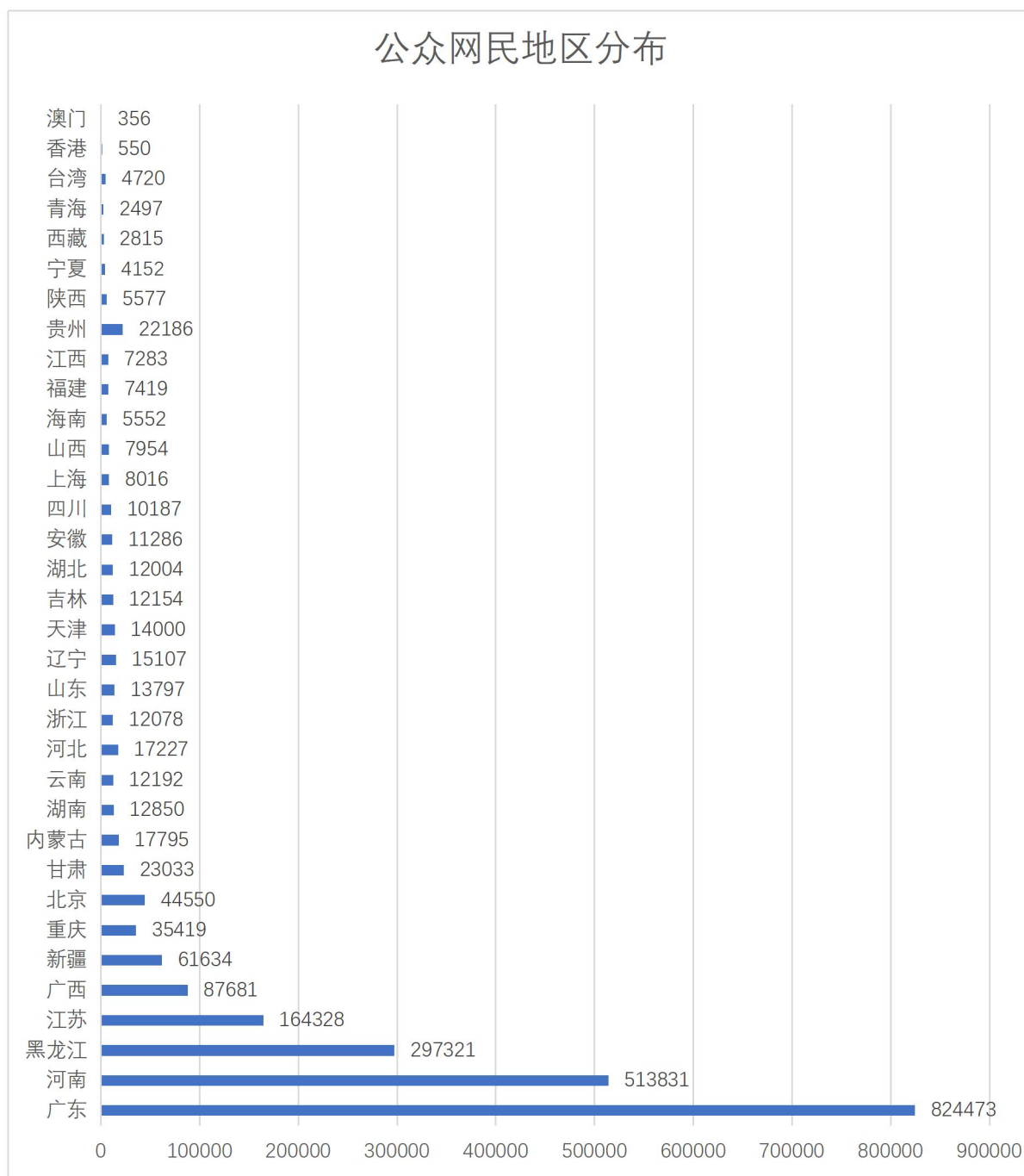
参与调查的从业人员以一般职员居多，技术岗（16.92%）、业务岗（8.99%）和一般职员（61.38%）等基层岗位，共计占比 87.29%。体现了调查活动开展的真实客观性。



图表 3.1-6：工作岗位性质构成

(7) 地区分布

参与本次调查的从业人员来自全国各省、直辖市、自治区和港澳台地区等，其中广东、河南、黑龙江、江苏、广西、新疆、重庆、北京、甘肃、内蒙古的有效答卷数量排列前 10 位。各地区分布情况如下图：



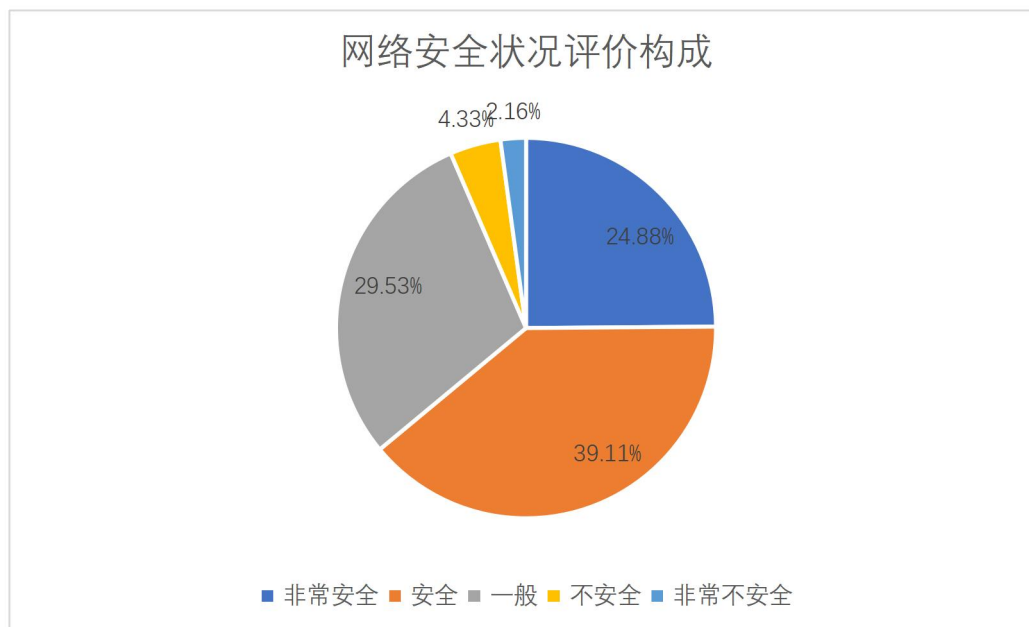
图表 3.1-7：从业人员地区分布

四、 网络安全行业发展主问卷分析

4.1 网络安全感知

（1）网络安全状况评价构成

大部分从业人员对网络安全状况的评价较为积极（63.99%），其中，有 24.88%的从业人员感到非常安全，有 39.11%的从业人员感到安全。

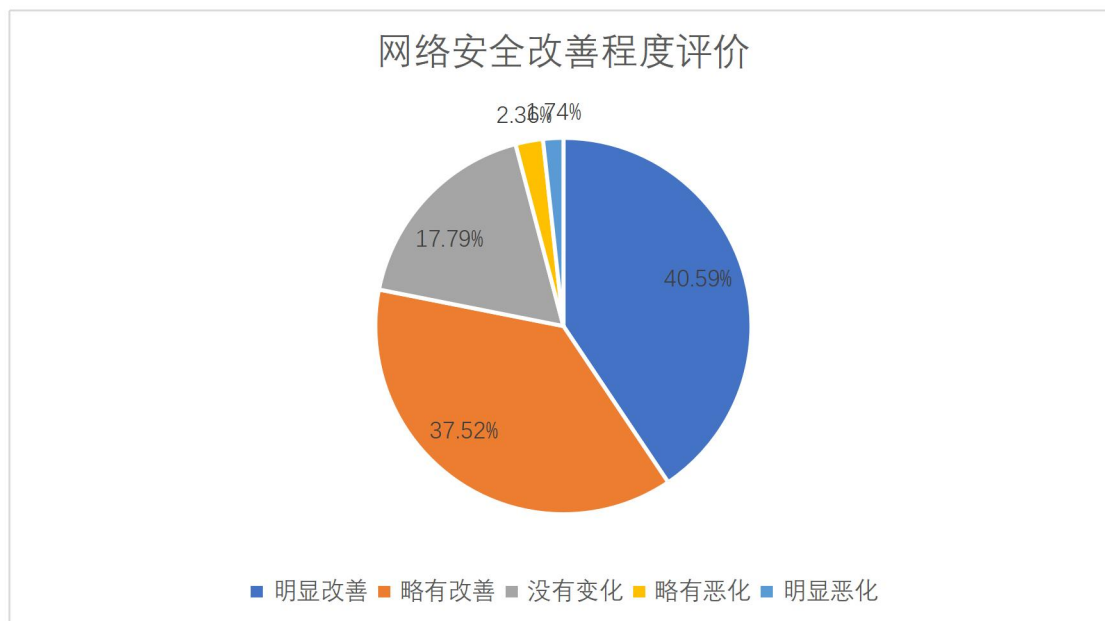


图表 4.1-1：网络安全状况评价构成

（图表数据来源：从业人员版主问卷第 7 题：您认为当前网络安全状况如何？）

（2）本年度网络安全改善程度评价

大部分从业人员对网络安全改善程度的评价较为积极，认为同去年相比，本年度的网络安全状况有所改善。其中，有 40.59%的从业人员认为有明显改善，另外有 37.52%的从业人员认为略有改善。

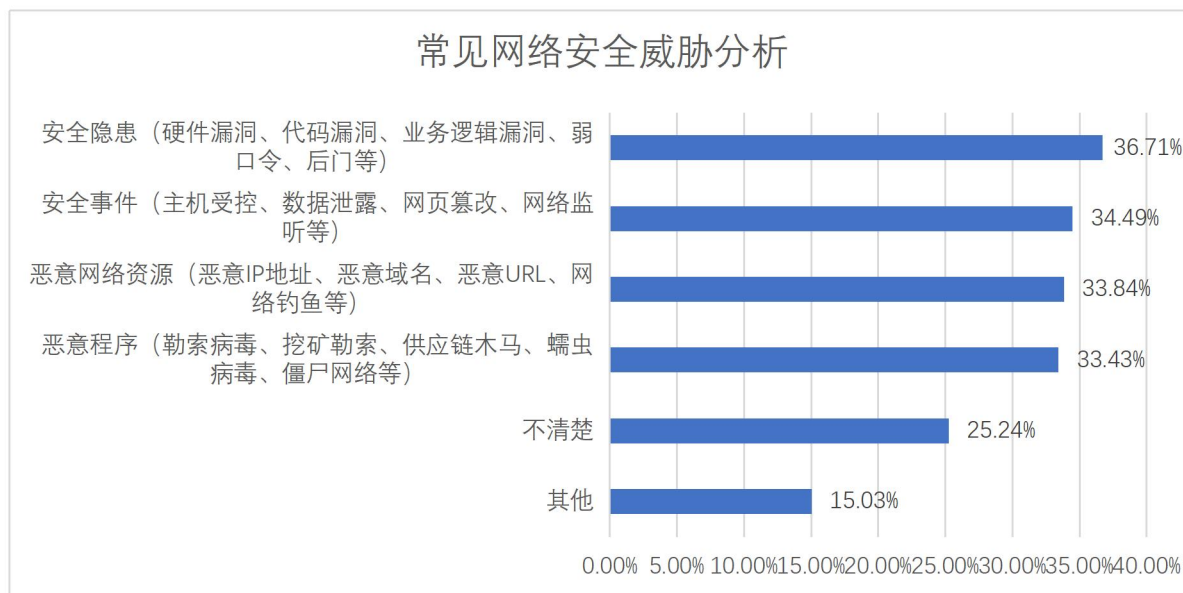


图表 4.1-2：网络安全改善程度评价

（图表数据来源：从业人员版主问卷第 8 题：与去年相比，您认为当前网络安全状况是否有变化？）

（3）常见网络安全威胁分析

从业人员认为，最常见的三大网络安全威胁分别是：安全隐患（36.71%）、安全事件（34.49%）、恶意网络资源（33.84%）。数据显示降低网络安全威胁的首要方式，是要提升主体自身的网络安全防护和网络安全合规整改。

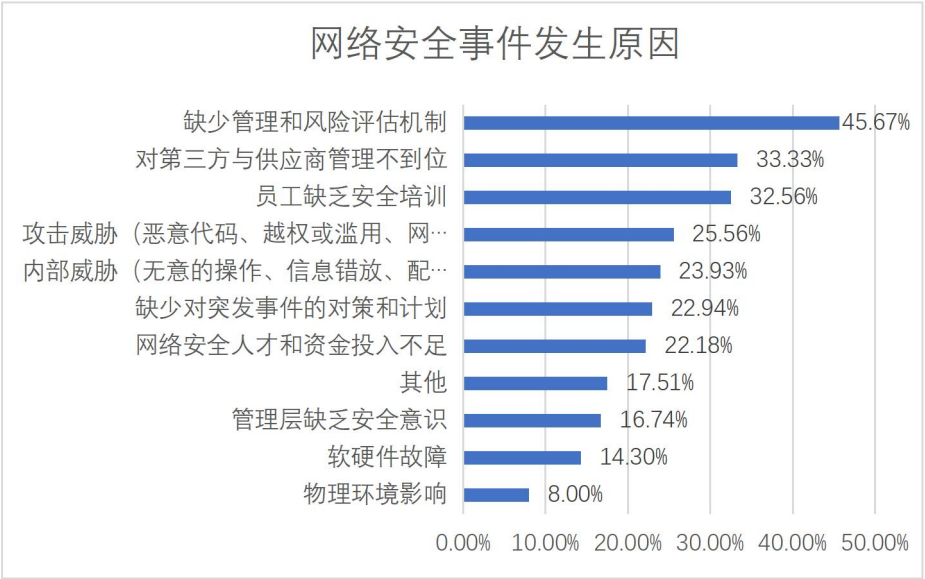


图表 4.1-3：常见网络安全威胁分析

（图表数据来源：从业人员版主问卷第 9 题：您在工作中最常面对和处理的网络安全威胁是？）

（4）网络安全事件发生原因

从业人员认为，最常见的三大网络安全威胁分别是：缺少管理和风险评估机制（45.67%）、对第三方与供应商管理不到位（33.33%）、员工缺乏安全培训（32.56%）。

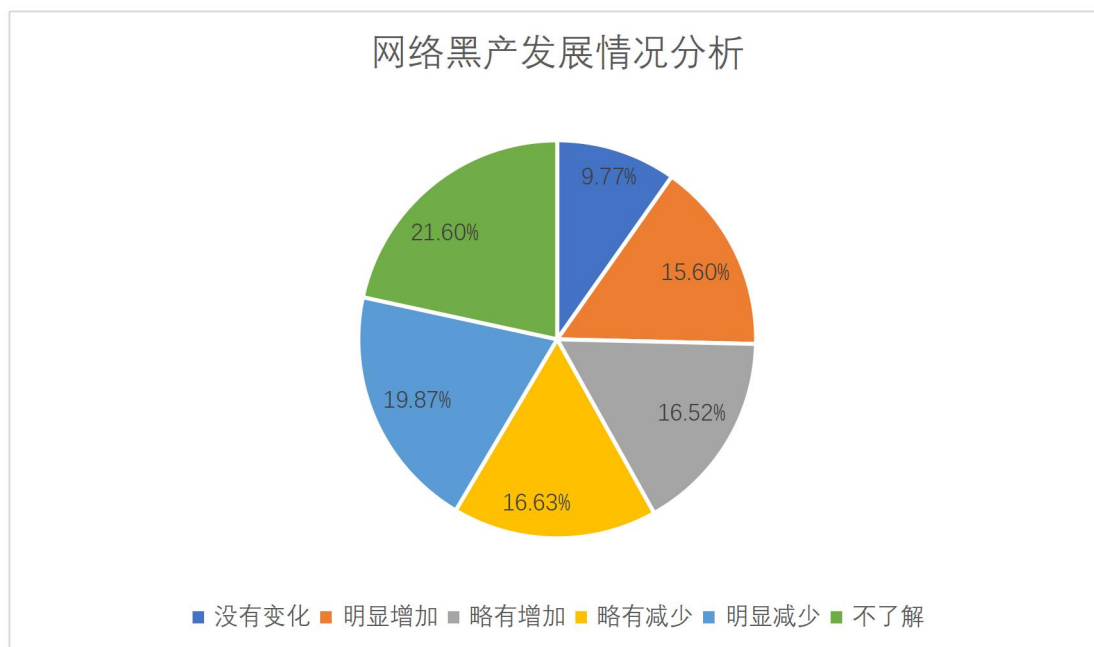


图表 4.1-4：网络安全事件发生原因
（图表数据来源：从业人员版主问卷第 10 题：您认为造成网络安全事件频繁出现的主要原因是？）

4.2 网络黑产

（1）网络黑产发展情况分析

参与调查的从业人员有 32.12%（明显增加 15.6%、略有增加 16.52%）认为近年来网络黑产发展势头有所上升，有 36.5%（明显减少 19.87%、略有减少 16.63%）的从业人员认为网络黑产发展有不同程度的减少。综上说明，近年来有关部门对于网络黑产的整治工作取得一定的成效。

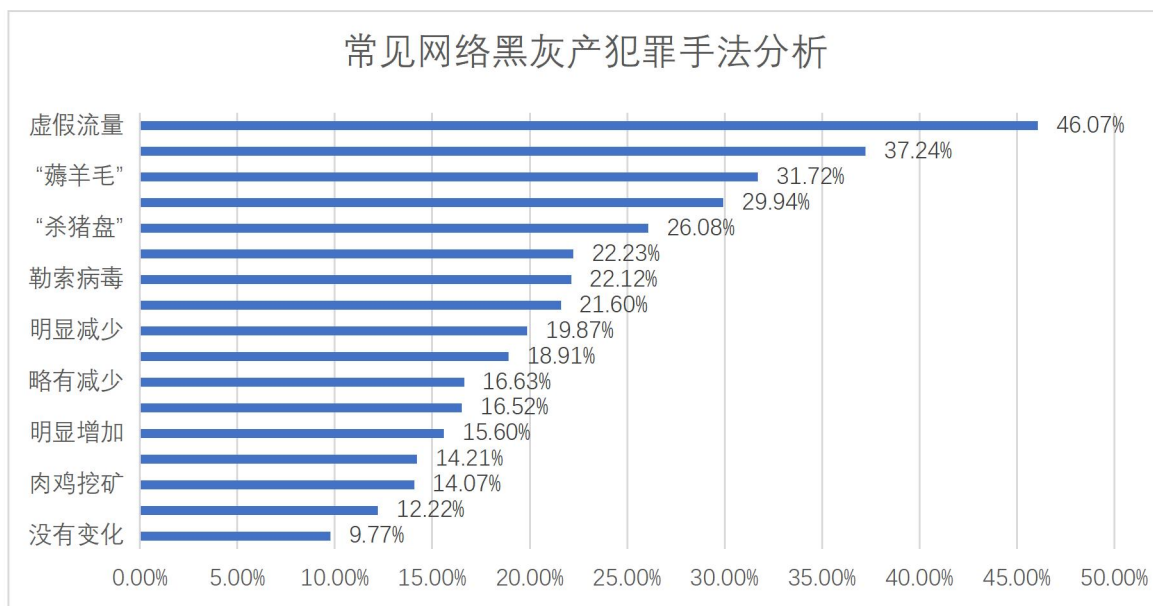


图表 4.2-1：网络黑产发展情况分析

（图表数据来源：从业人员版主问卷第 11 题：您认为近年来网络数据违法交易，网络色情等互联网黑灰产业的情况有何变化？）

（2）常见网络黑灰产犯罪手法分析

从业人员认为最常见的网络黑灰产犯罪手法排名前 5 的是：虚假流量（46.07%）、暗扣话费（37.24%）、“薅羊毛”（31.72%）、手机应用分发（29.94%）、“杀猪盘”（26.08%）。

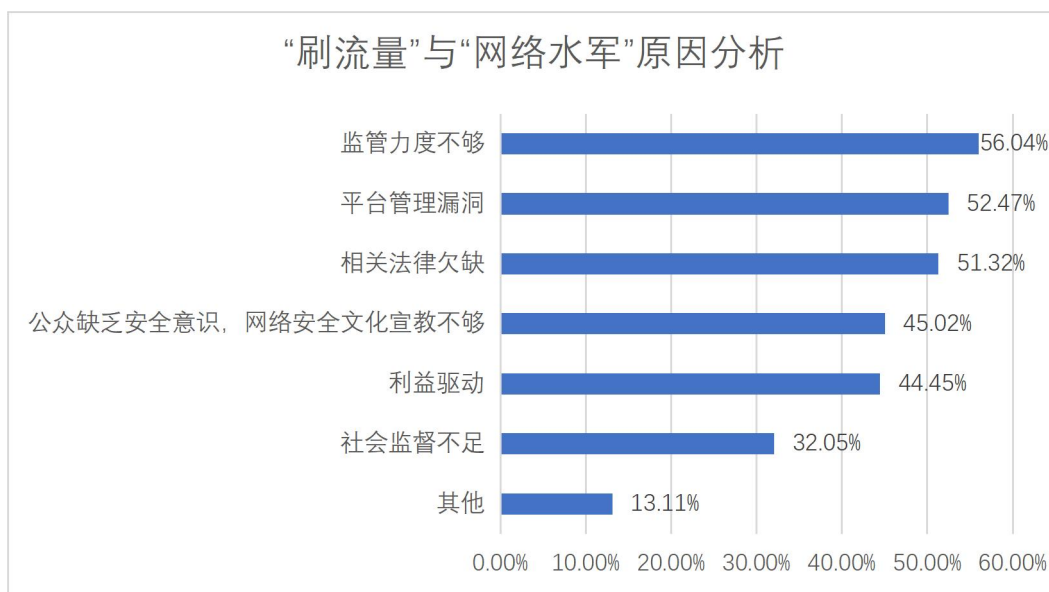


图表 4.2-2：常见网络黑灰产犯罪手法分析

（图表数据来源：从业人员版主问卷第 12 题：哪些网络黑灰产犯罪手法是您近一年常见的？）

（3）“刷流量”与“网络水军”原因分析

参与调查的从业人员认为“刷流量”与“网络水军”屡禁不止的原因中，最主要的三大原因分别是：监管力度不够（56.04%）、平台管理漏洞（52.47%）、相关法律欠缺（51.32%）。



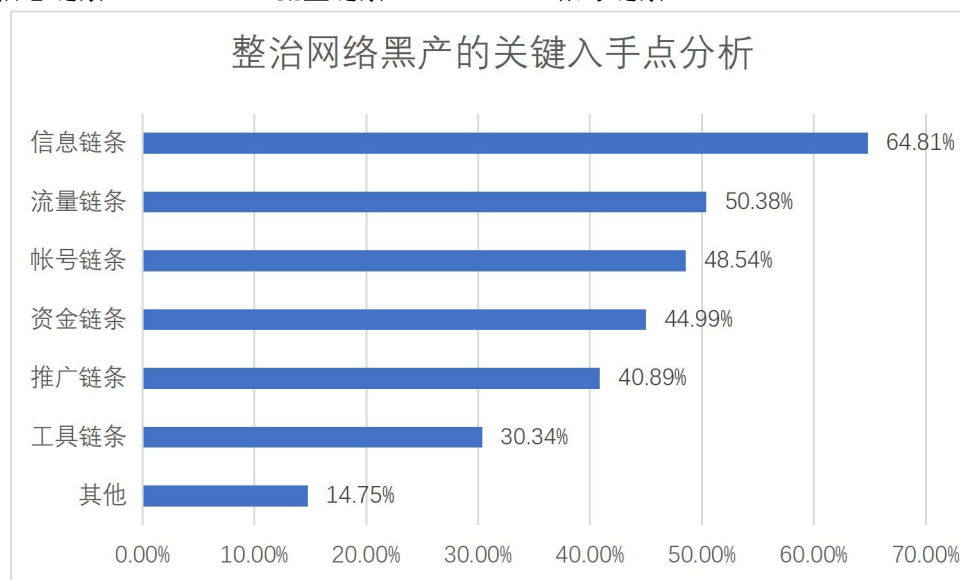
图表 4.2-3：“刷流量”与“网络水军”原因分析

（图表数据来源：从业人员版主问卷第 13 题：您认为“刷流量”、“网络水军”的现象为何屡禁不绝？）

（4）整治网络黑产的关键入手点分析

参与调查的从业人员认为整治网络黑产的关键入手点中，最主要的三大链条分别是：

信息链条（64.81%）、流量链条（50.38%）、帐号链条（48.54%）。



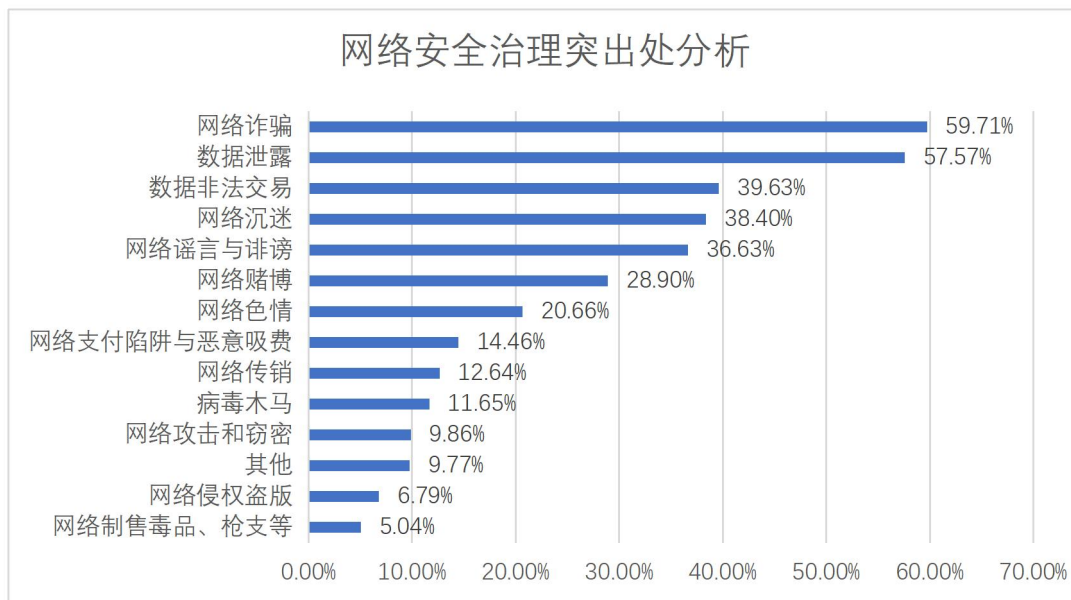
图表 4.2-4：整治网络黑产的关键入手点分析

（图表数据来源：从业人员版主问卷第 14 题：您认为整治网络黑灰产业，从哪些链条入手最关键？）

4.3 网络安全治理

（1）网络安全治理突出处分析

从业人员认为网络安全最突出或亟待治理的问题排名前 5 的是：网络诈骗(59.71%)、数据泄露(57.57%)、数据非法交易(39.63%)、网络沉迷(38.40%)和网络谣言与诽谤(36.63%)。

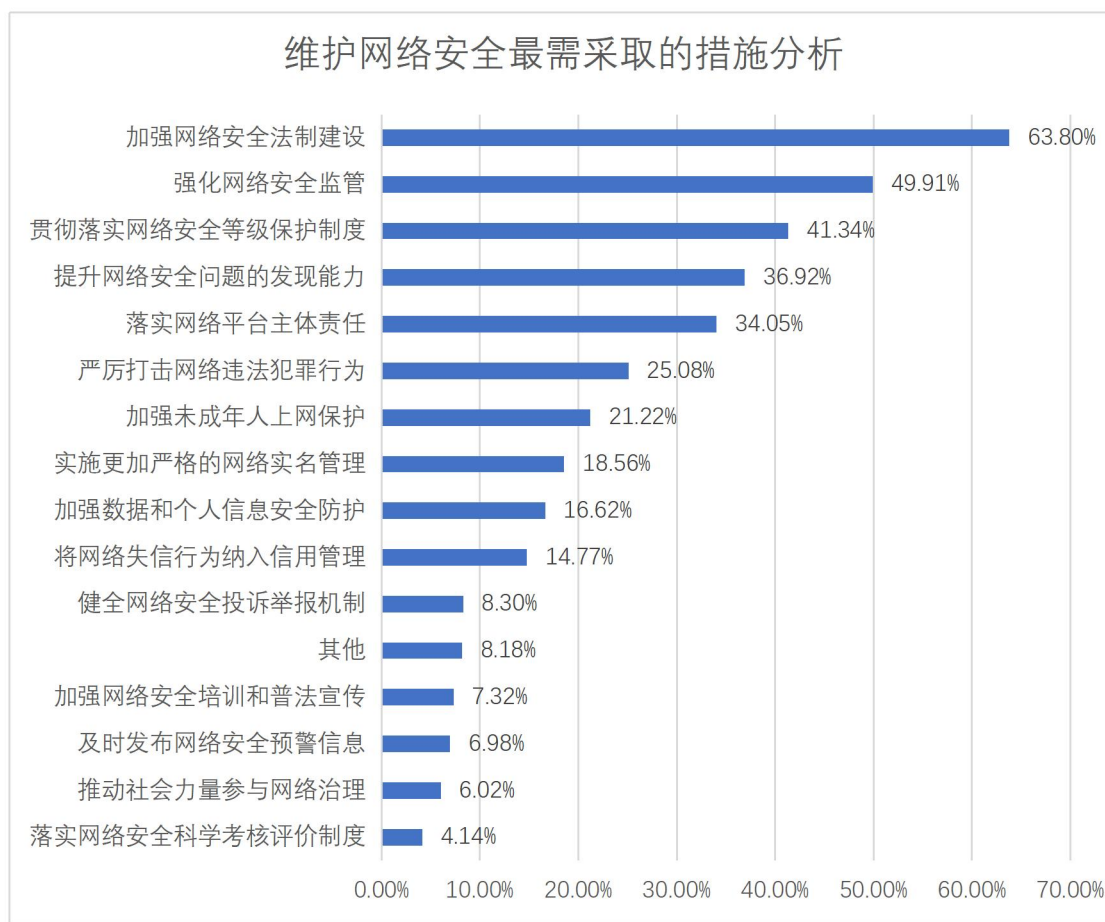


图表 4.3-1：网络安全治理突出处分析

（图表数据来源：从业人员版主问卷第 15 题：您认为当前网络安全最突出或亟待治理的问题有哪些？）

（2）维护网络安全最需采取的措施分析

从业人员认为维护网络安全最需采取的措施排名前 5 的是：加强网络安全法制建设(63.80%)、强化网络安全监管(49.91%)、贯彻落实网络安全等级保护制度(41.34%)、提升网络安全问题的发现能力(36.92%)和落实网络平台主体责任(34.05%)。

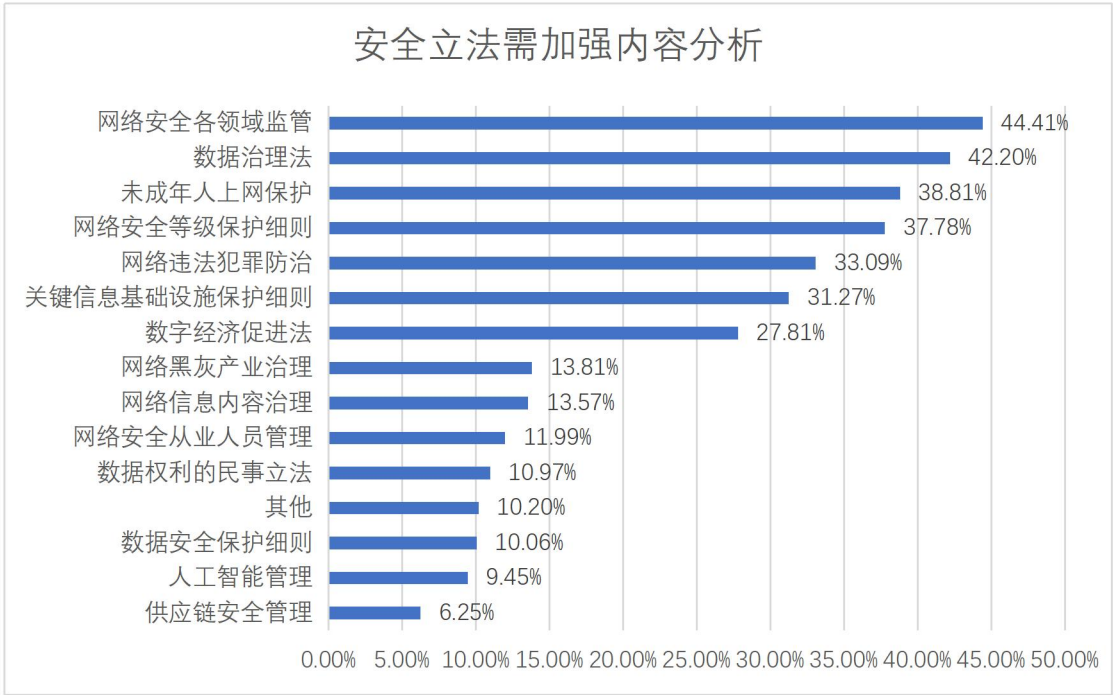


图表 4.3-2：维护网络安全最需采取的措施分析

（图表数据来源：从业人员版主问卷第 16 题：您认为维护网络安全最需要采取哪些措施？）

（3）安全立法需加强内容分析

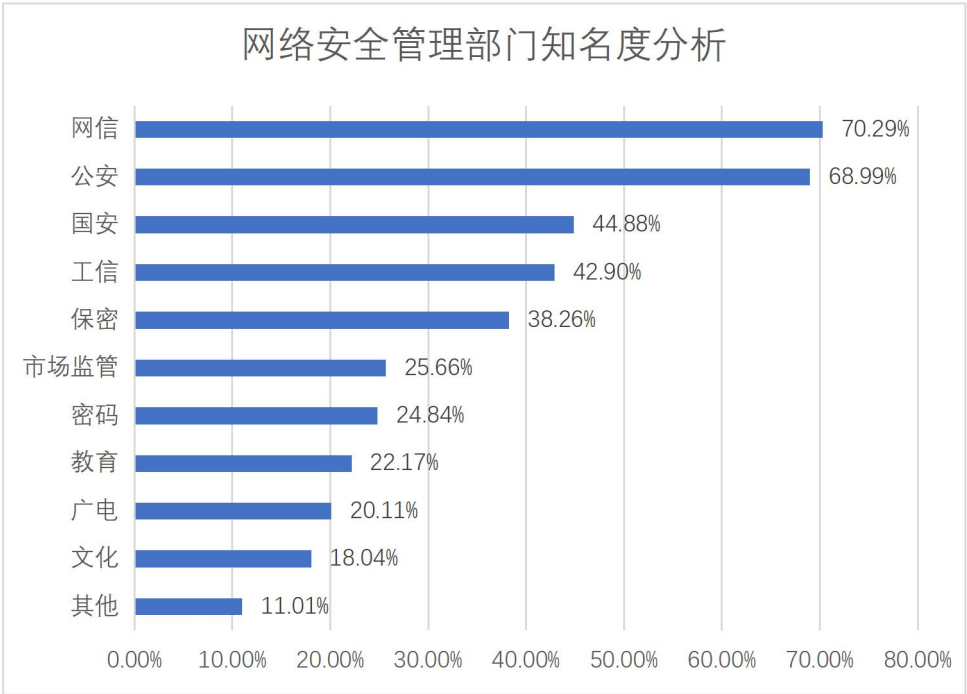
从业人员认为安全立法需加强的内容排名前 5 的是：网络安全各领域监管（44.41%）、数据治理法（42.20%）、未成年人上网保护（38.81%）、网络安全等级保护细则（37.78%）和网络违法犯罪防治（33.09%）。



图表 4.3-3：从业人员常遇见的网络安全问题
(图表数据来源：从业人员版主问卷第 17 题：您认为亟待加强的网络安全立法内容有哪些？)

(4) 网络安全管理部门知名度分析

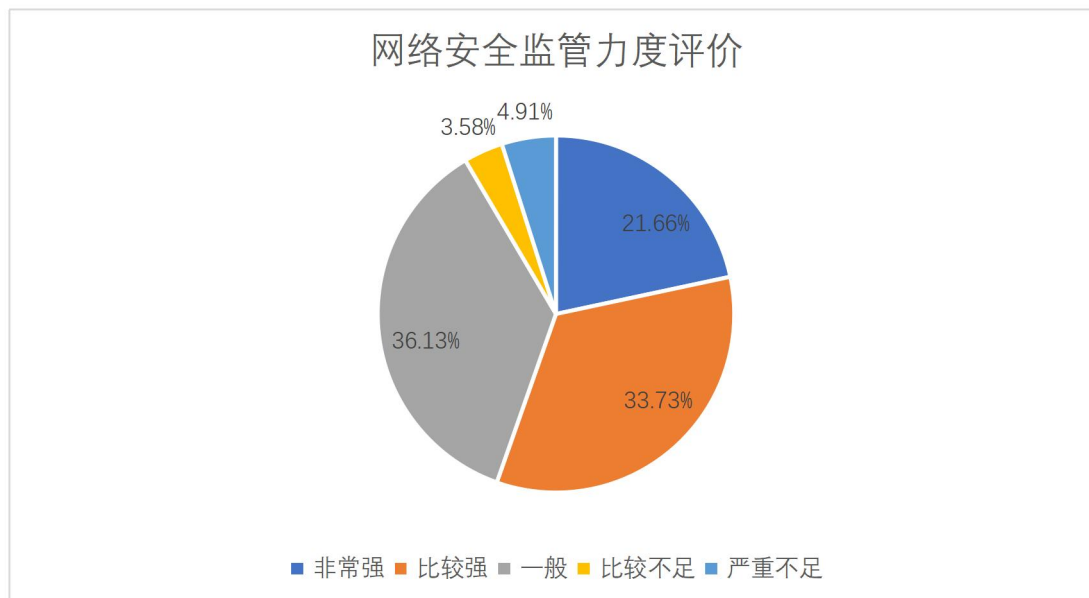
在从业人员对于网络安全管理部门知名度的了解，排名前 5 的是：网信（70.29%）、安全（68.99%）、国安（44.88%）、工信（42.90%）和保密（38.26%）。



图表 4.3-4：网络安全管理部门知名度分析
(图表数据来源：从业人员版主问卷第 18 题：据您了解，以下哪些部门是网络安全的相关管理部门？)

（5）网络安全监管力度评价

从业人员对网络安全监管力度的评价中，非常强的占 21.66%，比较强的最多，占 33.73%，认为一般的占 36.13%，认为强的超过一半（55.39%），总体上目前从业人员对于网络安全监管力度的感知是强的。



图表 4.3-5：网络安全监管力度评价

（图表数据来源：从业人员版主问卷第 19 题：您认为政府相关部门在网络安全方面的监管力度如何？）

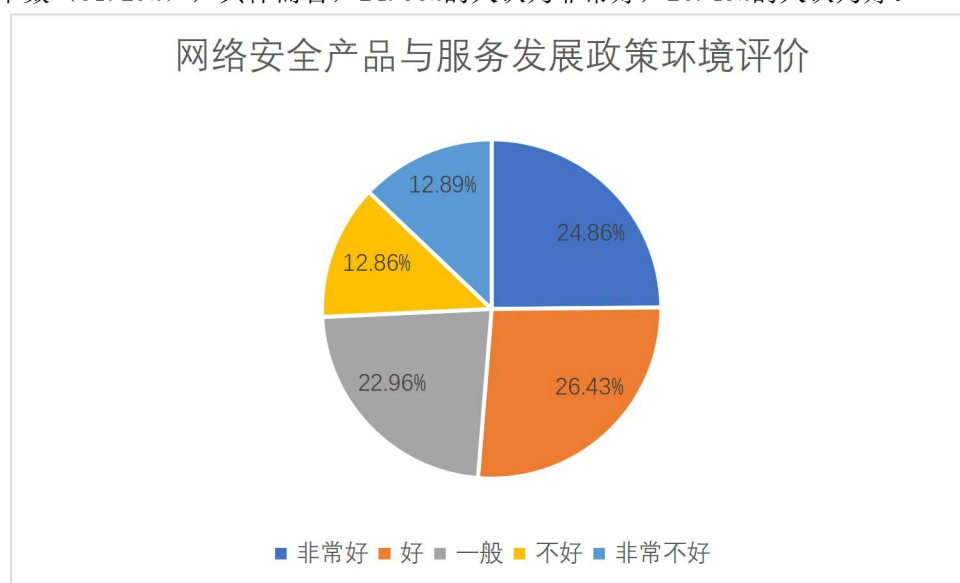
五、 专题分析

5.1 行业发展与生态建设

参加本专题调查的从业人员数量一共 80025 人。

（1）网络安全产品与服务发展政策环境评价

参与调查的从业人员对网络安全产品与服务发展政策环境评价持正向态度的超过半数（51.29%），具体而言，24.86%的人认为非常好，26.43%的人认为好。

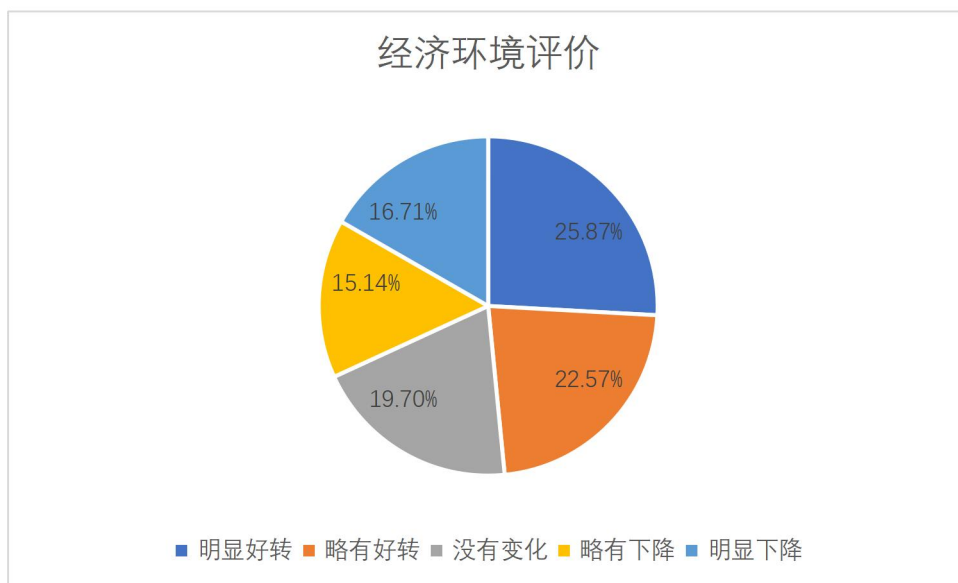


图表 5.1-1：网络安全产品与服务发展政策环境评价

（图表数据来源：从业人员版行业发展与生态建设专题第 B1 题：您认为当前促进网络安全产品与服务发展的政策环境如何？）

（2）经济环境评价

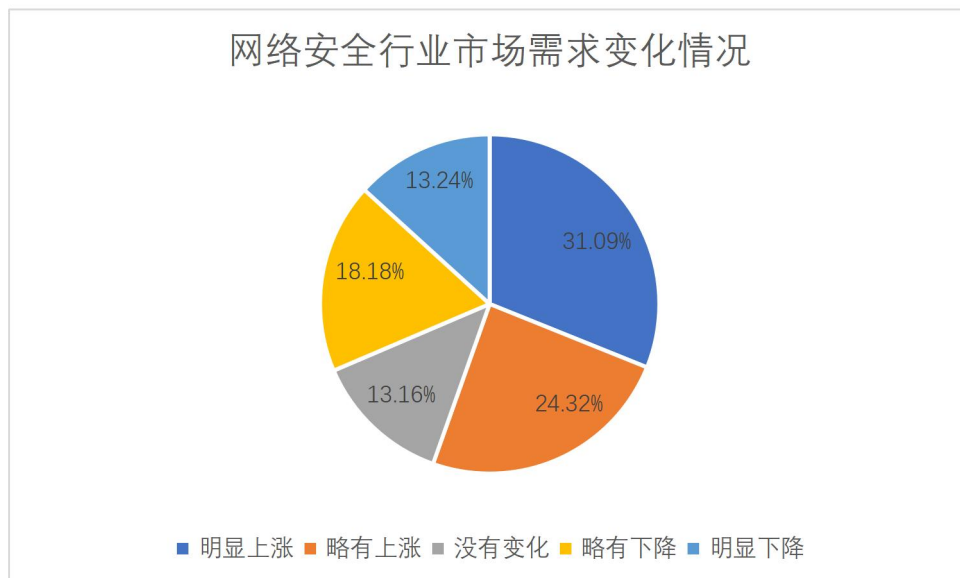
参与调查的从业人员对经济环境评价持正向态度的未达半数（48.44%），具体而言，19.7%的人认为经济环境一般，15.14%的人认为经济环境略有下降，16.71%的人认为经济环境出现明显下降的情况。



图表 5.1-2: 经济环境评价

(图表数据来源: 从业人员版行业发展与生态建设专题第 B2 题: 您认为当前经济环境总体状况如何?)

在对从业人员感受到的网络安全行业市场需求变化情况进一步调查时发现,网络安全全行业市场呈现增长的趋势,超过一半的从业者认为网络安全需求出现增长的迹象,其中 31.08% 的人认为明显上涨, 24.32% 的人认为略有上涨。



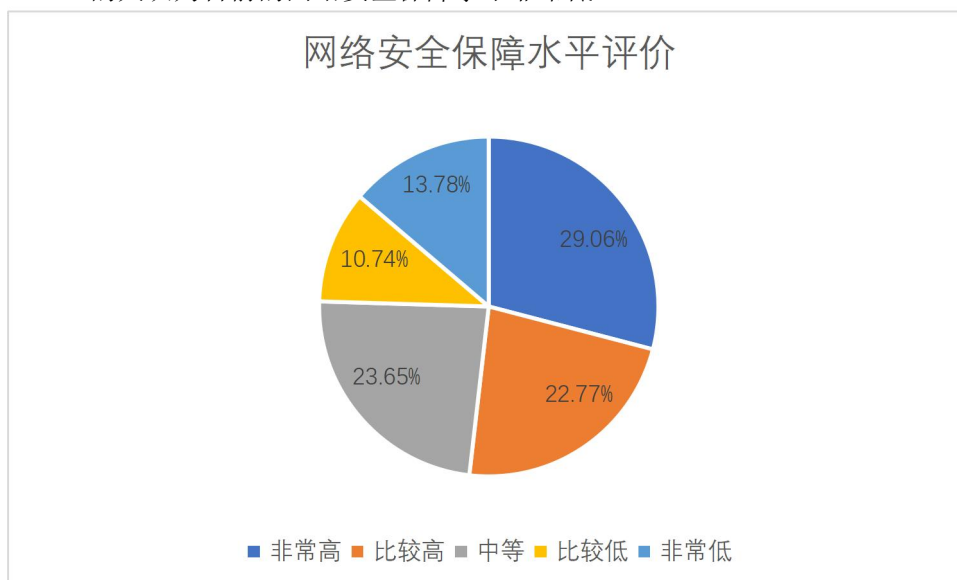
图表 5.1-2.1: 网络安全行业市场需求变化情况

(图表数据来源: 从业人员版行业发展与生态建设专题第 B2.1 题: 相比以往您认为当前网络安全行业市场的需求变化如何?)

(3) 网络安全保障水平评价

在调查从业人员对于目前网络安全行业能够提供的网络安全保障水平时发现, 13.77% 的人几乎每天都使用, 24.48% 的人经常使用, 超过一半的从业人员给出积极评价 (51.83%), 其中有 29.06% 的人认为目前的网络安全保障水平非常高。但同时, 也有

13.78%的人认为目前的网络安全保障水平非常低。

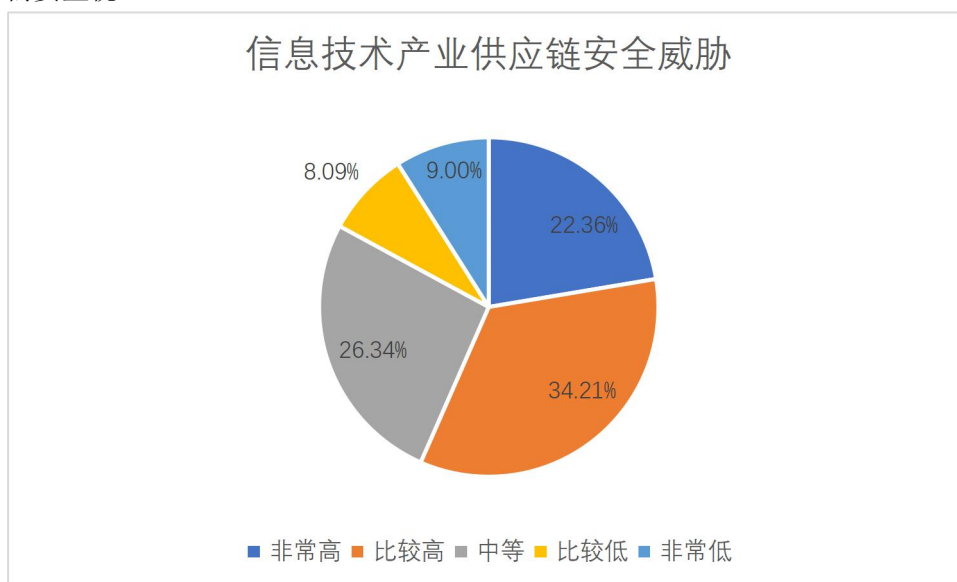


图表 5.1-3：网络安全保障水平评价

（图表数据来源：从业人员版行业发展与生态建设专题第 B3 题：据您了解目前网络安全行业提供的网络安全保障水平如何？）

（4）信息技术产业供应链安全威胁

在调查从业人员察觉到的信息技术产业供应链安全问题的威胁时发现，22.36%的人认为安全威胁非常高；认为安全威胁比较高的人占比最多，达 34.21%，两者相加超过半数（56.57%）。数据显示，目前信息技术产业供应链受到安全问题的威胁是相对高的，需要重视。

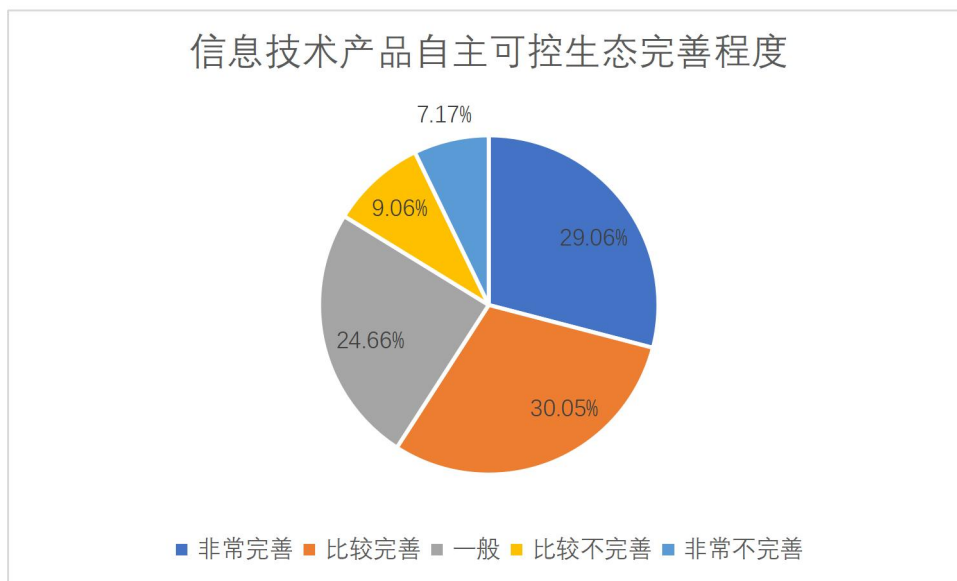


图表 5.1-4：信息技术产业供应链安全威胁

（图表数据来源：从业人员版行业发展与生态建设专题第 B4 题：您认为当前信息技术产业供应链安全问题的威胁如何？）

（5）信息技术产品自主可控生态完善程度

参与调查的从业人员对于目前信息技术产品自主可控生态完善程度评价较为积极，有超过半数（59.11%）的人给予正向评价，其中 29.06% 的人认为非常完善，30.05% 的人认为比较完善。

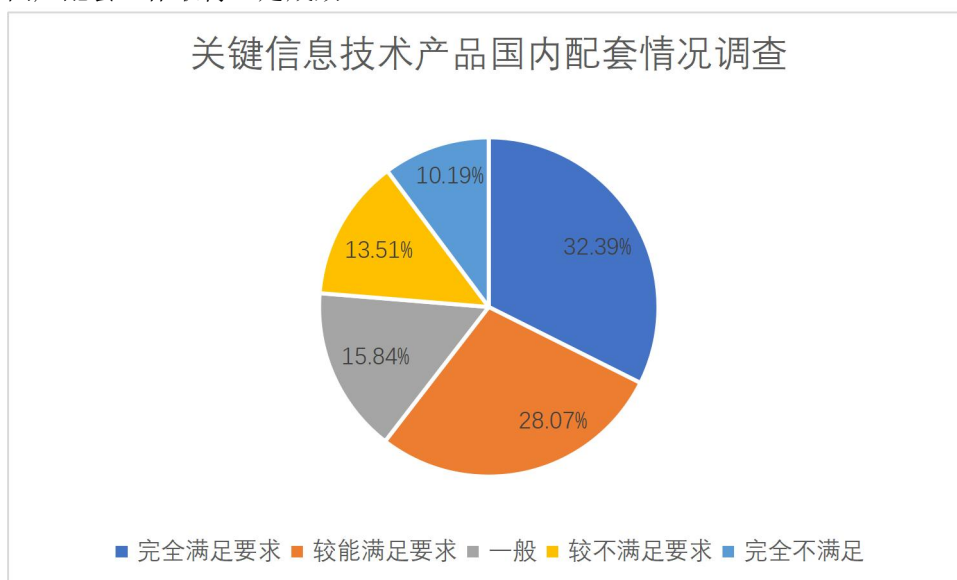


图表 5.1-5：信息技术产品自主可控生态完善程度

（图表数据来源：从业人员版行业发展与生态建设专题第 B5 题：您认为当前信息技术产品自主可控生态是否已完善？）

（6）关键信息技术产品国内配套情况调查

参与调查的从业人员评价其工作单位的关键信息技术产品国内配套情况时，超过 60% 的人都给予积极评价（60.46%），其中有 32.39% 的人认为完全满足要求，占比最多，另外有 28.07% 的人认为较能满足要求。数据显示，目前关键信息技术产品的国产化、国产配套工作取得一定成效。

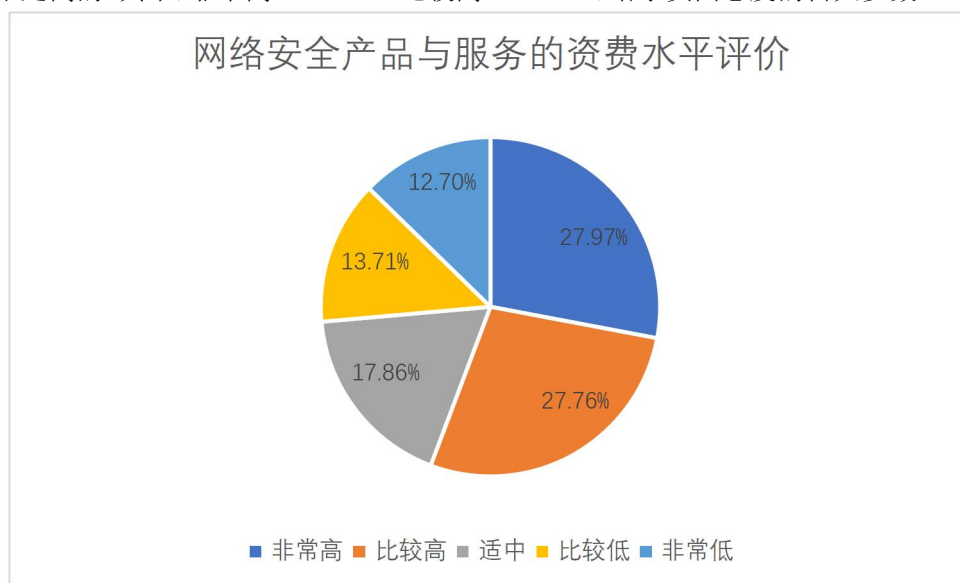


图表 5.1-6：关键信息技术产品国内配套情况调查

（图表数据来源：从业人员版行业发展与生态建设专题第 B6 题：您所在单位所需的关键信息技术产品国内配套状况如何）

（7）网络安全产品与服务的资费水平评价

从业人员对于当前网络安全产品与服务的资费水平评价,总体上认为当前的资费水平是高的。其中,非常高(27.97%)、比较高(27.76%),给予负面态度的占大多数(55.73%)。

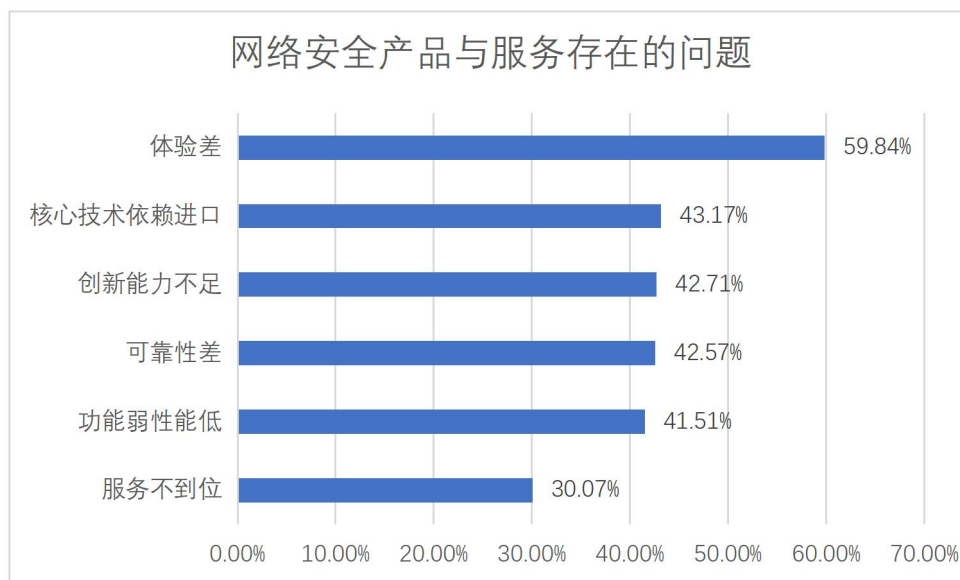


图表 5.1-7：网络安全产品与服务的资费水平评价

（图表数据来源：从业人员版行业发展与生态建设专题第 B7 题：您认为当前网络安全产品与服务的资费水平如何？）

（8）网络安全产品与服务存在的问题

从业人员对于目前网络安全产品与服务存在的问题的评价中,有 5 项问题较为突出：体验差（59.84）、核心技术依赖进口（43.17%）、创新能力不足（42.71%）、可靠性差（42.57%）、功能弱性能低（41.51%）。

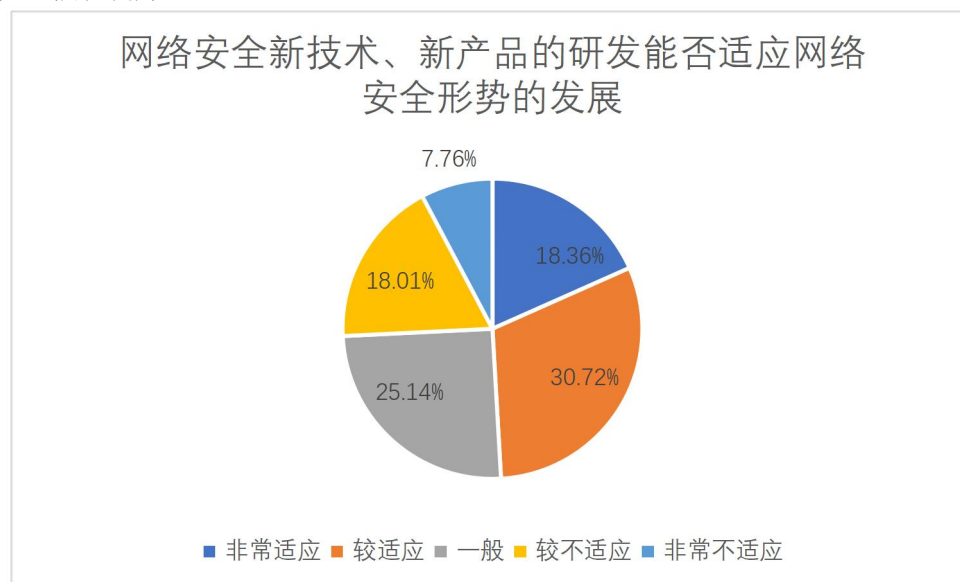


图表 5.1-8：网络安全产品与服务存在的问题

（图表数据来源：从业人员版行业发展与生态建设专题第 B8 题：您认为当前网络安全产品与服务存在的不足之处是？）

（9）网络安全新技术、新产品的研发能否适应网络安全形势的发展

对于调查从业人员对于网络安全新技术、新产品的研发能否适应网络安全形势的发展的评价时，18.36%的人认为非常适应，30.72%的人认为较适应，持有积极态度的不足半数（49.08%），数据显示，网络安全行业的新技术和新产品研发创新工作还需要进一步加强和提升。

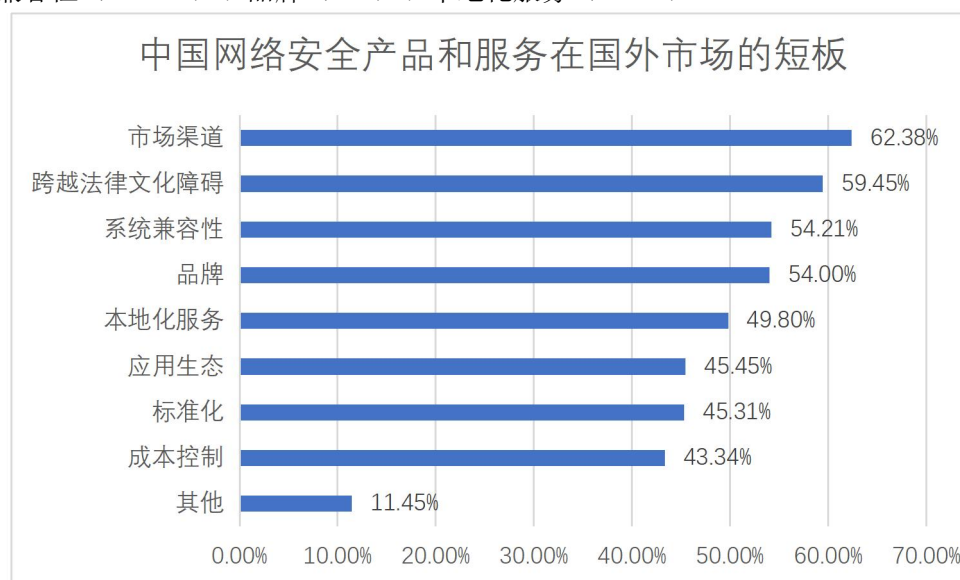


图表 5.1-9：网络安全新技术、新产品的研发能否适应网络安全形势的发展

（图表数据来源：从业人员版行业发展与生态建设专题第 B9 题：您认为行业内网络安全新技术、新产品的研发是否能适应现在的网路安全形势？）

（10）中国网络安全产品和服务在国外市场的短板

从业人员认为，对于中国品牌的网络安全产品和服务走出国门时还需要加强补足的地方，排名前 5 的分别是：市场渠道（62.38%）、跨越法律文化障碍（59.45%）、系统兼容性（54.21%）、品牌（54.00%）、本地化服务（49.80%）。

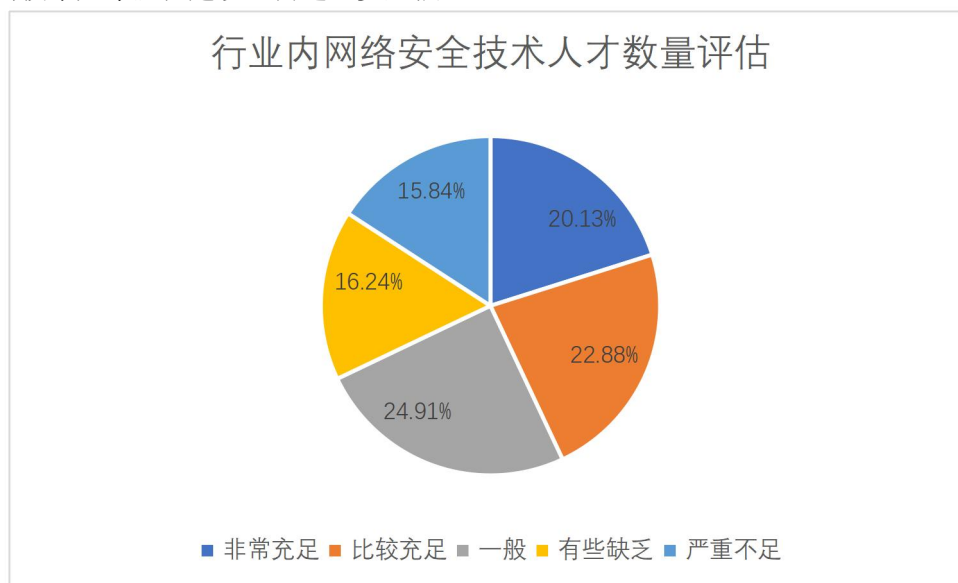


图表 5.1-10：中国网络安全产品和服务在国外市场的短板

（图表数据来源：从业人员版行业发展与生态建设专题第 B10 题：您认为中国品牌的网络安全产品和服务走出国门还欠缺什么？）

（11）行业内网络安全技术人才数量评估

对于行业内网络安全技术人才数量的评估，持有积极评价的不足半数（43.01%），其中 20.13% 的人认为非常充足，22.88% 的人认为比较充足，数据显示，网络安全行业的技术人才队伍建设还需进一步加强。

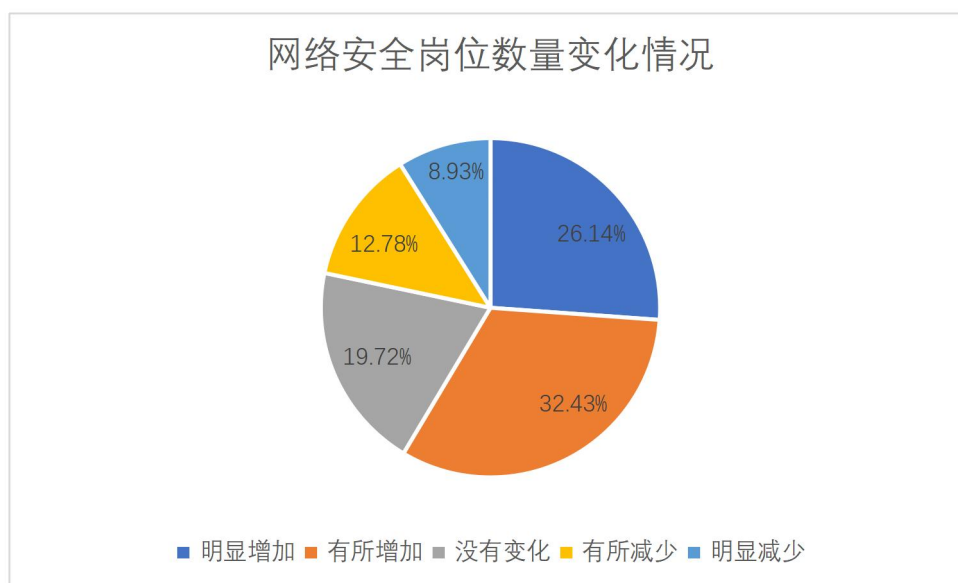


图表 5.1-11：行业内网络安全技术人才数量评估

（图表数据来源：从业人员版行业发展与生态建设专题第 B11 题：您认为当前行业内网络安全技术人才数量如何？）

（12）网络安全岗位数量变化情况

在调查从业人员所在单位的网络安全岗位数量变化情况时，有 26.14% 的人表示明显增加，有 32.43% 的人表示有所增加，数据显示，网络安全岗位数量是有所上升的（58.57%）。

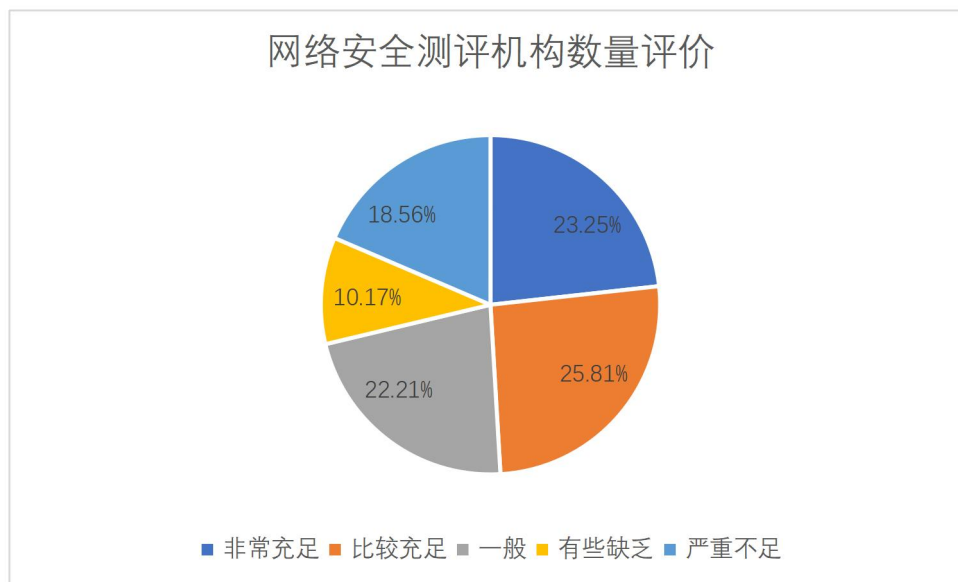


图表 5.1-12：网络安全岗位数量变化情况

（图表数据来源：从业人员版行业发展与生态建设专题第 B12 题：您所在单位网络安全岗位数量变化情况？）

（13）网络安全测评机构数量评价

在调查从业人员对于网络安全测评机构数量的评价时，只有不到一半的人表示目前的数量是充足的（49.06%），数据显示，当前网络安全测评机构数量还有进一步增加的空间。

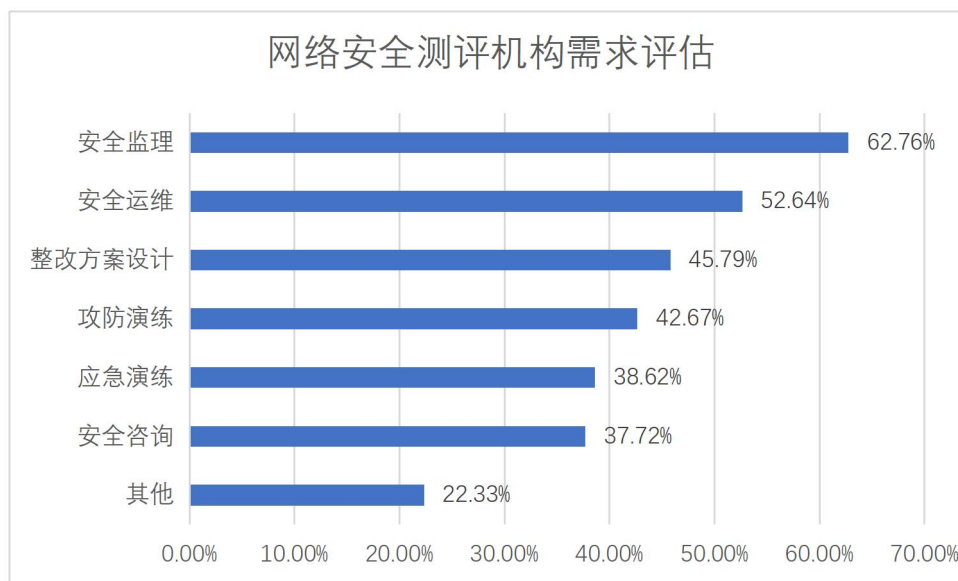


图表 5.1-13：网络安全测评机构数量评价

（图表数据来源：从业人员版行业发展与生态建设专题第 B13 题：您认为当前网络安全测评机构数量如何？）

（14）网络安全测评机构需求评估

参与调查的从业人员认为所在单位还需要测评机构提供哪些服务时，排名前 3 的是：安全监理（62.76%）、安全运维（52.64%）和整改方案设计（45.79%）。

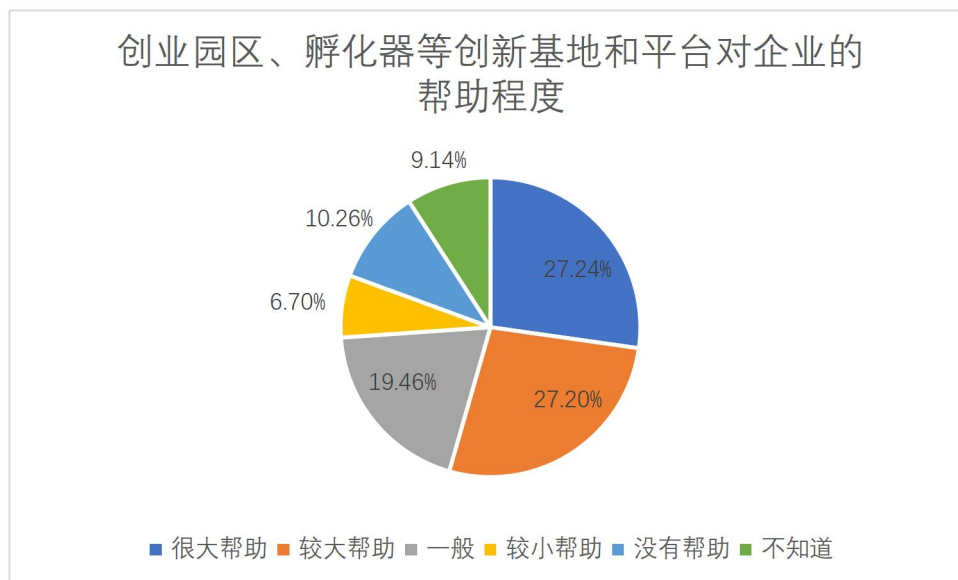


图表 5.1-14：网络安全测评机构需求评估

（图表数据来源：从业人员版行业发展与生态建设专题第 B14 题：您所在单位还需要测评机构提供哪些服务？）

（15）创业园区、孵化器创新基地和平台对企业的帮助程度

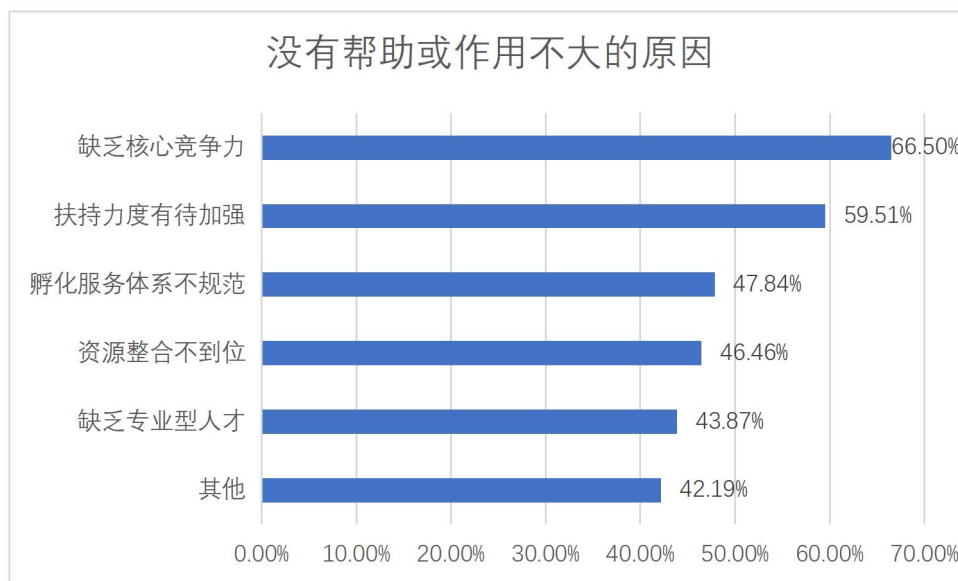
在调查创业园区、孵化器创新基地和平台对企业的帮助程度时，超过半数（54.44%）的从业人数给予积极评价，其中表示有很大帮助的占 27.24%，表示有较大帮助的占 27.2%。



图表 5.1-15：创业园区、孵化器创新基地和平台对企业的帮助程度

（图表数据来源：从业人员版行业发展与生态建设专题第 B15 题：您认为创业园区、孵化器创新基地和平台对企业是否有帮助？）

在进一步调查从业人员认为创业园区、孵化器创新基地和平台对于企业帮助不大的可能原因时，缺乏核心竞争力（66.5%）和扶持力度有待加强（59.51%）是两个超过 50%的选项。

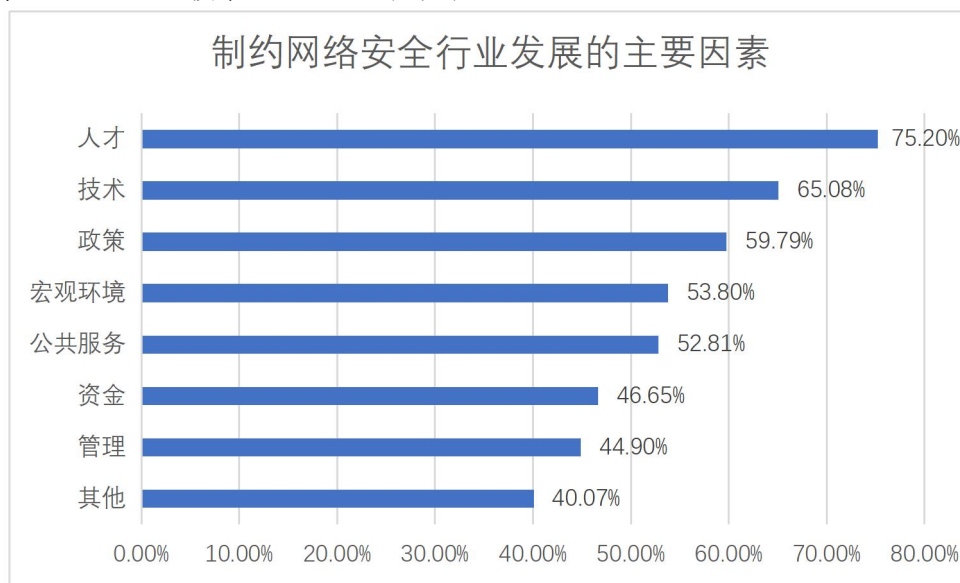


图表 5.1-15.1：没有帮助或作用不大的原因

（图表数据来源：从业人员版行业发展与生态建设专题第 B15.1 题：您认为没有帮助或作用不大的原因是？）

（16）制约网络安全行业发展的主要因素

参与调查的从业人员认为制约网络安全行业发展的主要因素中，排名前 3 的是：人才（75.20%）、技术（65.08%）和政策（59.79%）。

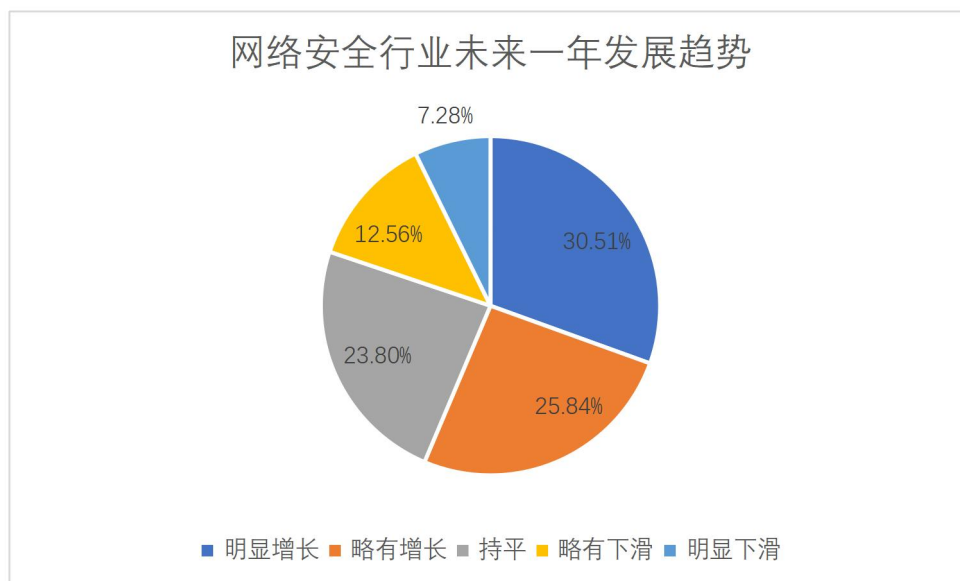


图表 5.1-16：制约网络安全行业发展的主要因素

（图表数据来源：从业人员版行业发展与生态建设专题第 B16 题：您认为制约网络安全行业发展的主要因素是什么？）

（17）网络安全行业未来一年发展趋势

参与调查的从业人员对网络安全行业未来一年发展趋势的评价，给予正向态度的超过半数（56.35%），有 30.51%的人表示未来一年会有明显增长，25.84%的人认为会略有增长。

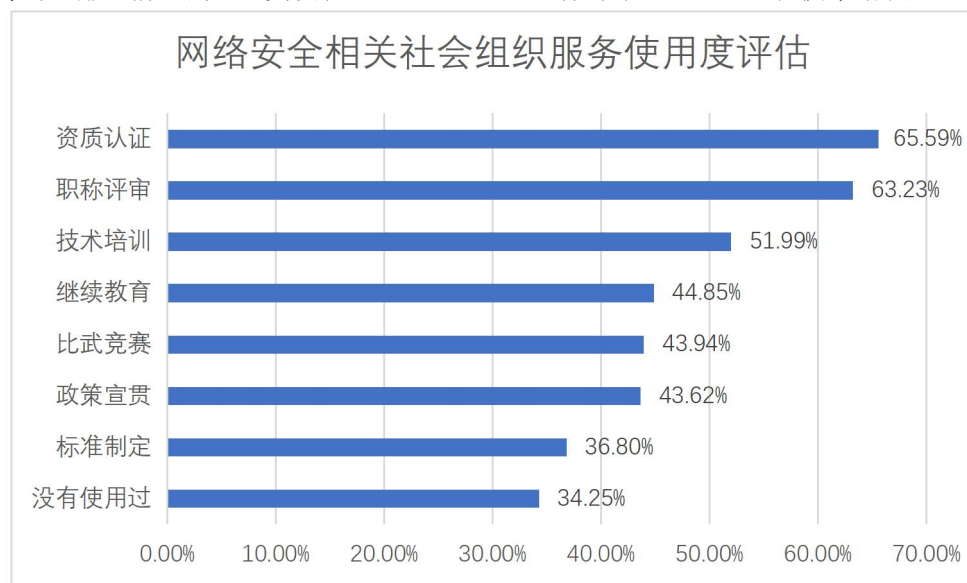


图表 5.1-17：网络安全行业未来一年发展趋势

（图表数据来源：从业人员版行业发展与生态建设专题第 B17 题：您认为网络安全行业未来一年发展的趋势如何？）

（18）网络安全相关社会组织服务使用度评估

调查从业人员使用过哪些由网络安全相关行业协会、技术联盟等社会组织提供的服务时，排名前 3 的是：资质认证（65.59%）、职称评审（63.23%）和技术培训（51.99%）。



图表 5.1-18：网络安全相关社会组织服务使用度评估

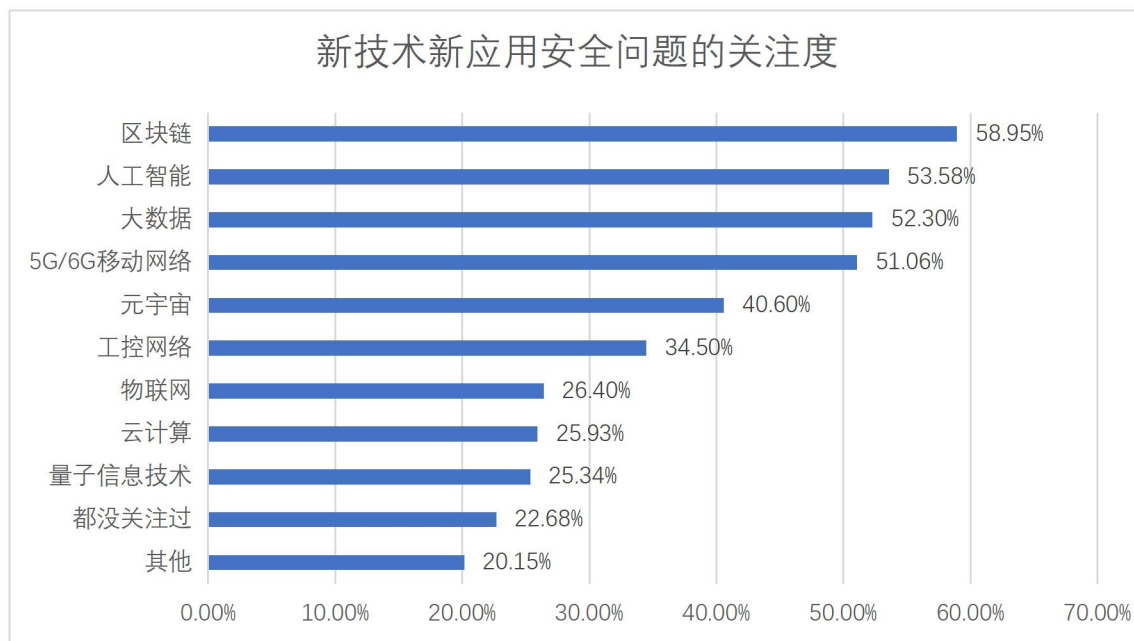
（图表数据来源：从业人员版行业发展与生态建设专题第 B18 题：您使用过哪些由网络安全相关行业协会、技术联盟等社会组织提供的服务？）

5.2 新技术新应用与网络安全

参加本专题调查的从业人员数量一共 79651 人。

（1）新技术新应用安全问题的关注度

在调查的从业人员对新技术新应用的网络安全问题的关注度时，关注程度最高的 5 项分别是：区块链（58.95%）、人工智能（53.58%）、大数据（52.3%）、5G/6G 移动网络（51.06%）、元宇宙（40.6%）。

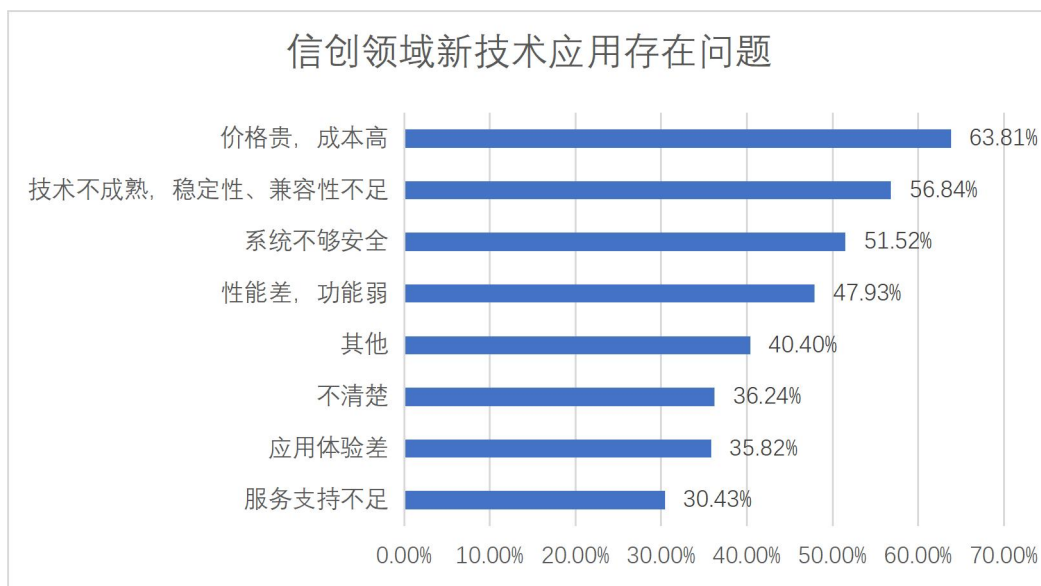


图表 5.1-1：新技术新应用安全问题的关注度

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C1 题：您关注过以下哪项新技术新应用的网络安全问题？）

（2）信创领域新技术应用存在问题

在调查的从业人员认为信创领域存在的新技术应用问题时，排名最高的 3 项分别是：价格贵，成本高（63.81%）、技术不成熟，稳定性、兼容性不足（56.84%）、系统不够安全（51.52%）。

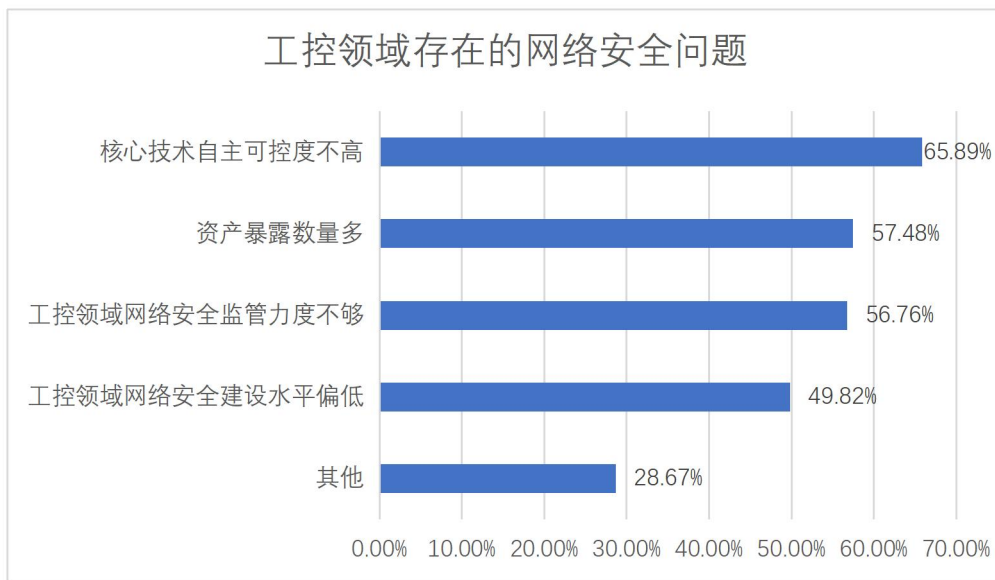


图表 5.1-2：信创领域新技术应用存在问题

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C2 题：您对信创领域新技术应用存在哪些问题？）

（3）工控领域存在的网络安全问题

在调查的从业人员认为工控领域存在的网络安全问题时，排名最高的 3 项分别是：核心技术自主可控度不高（65.89%）、资产暴露数量多（57.48%）、工控领域网络安全监管力度不够（56.76%）。



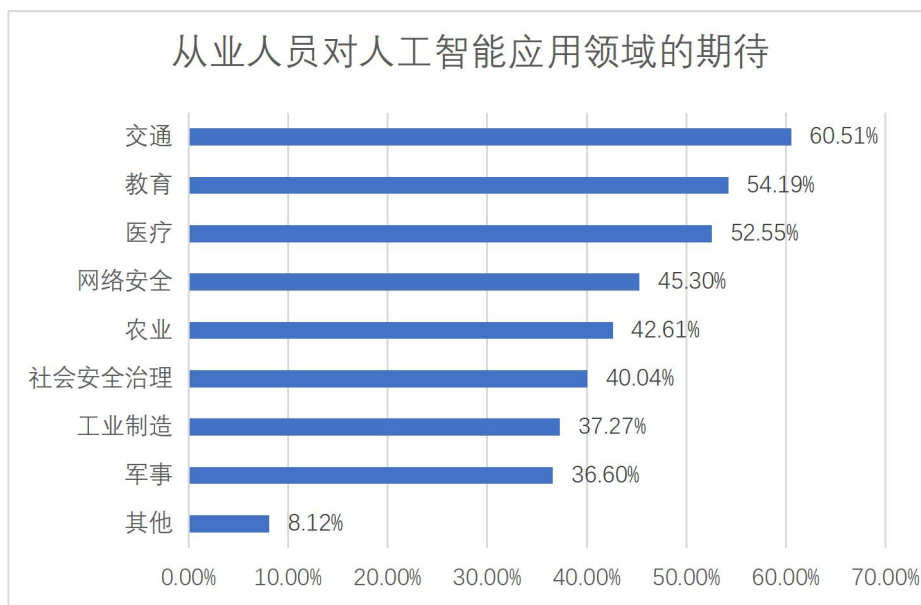
图表 5.1-3：工控领域存在的网络安全问题

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C3 题：您认为工控领域网络安全存在哪些问题？）

（4）从业人员对人工智能应用领域的期待

在调查的从业人员最期待人工智能 (AI) 在哪些领域发挥优势时，排名最高的 3 项分

别是：交通（60.51%）、教育（54.19%）、医疗（52.55%）。

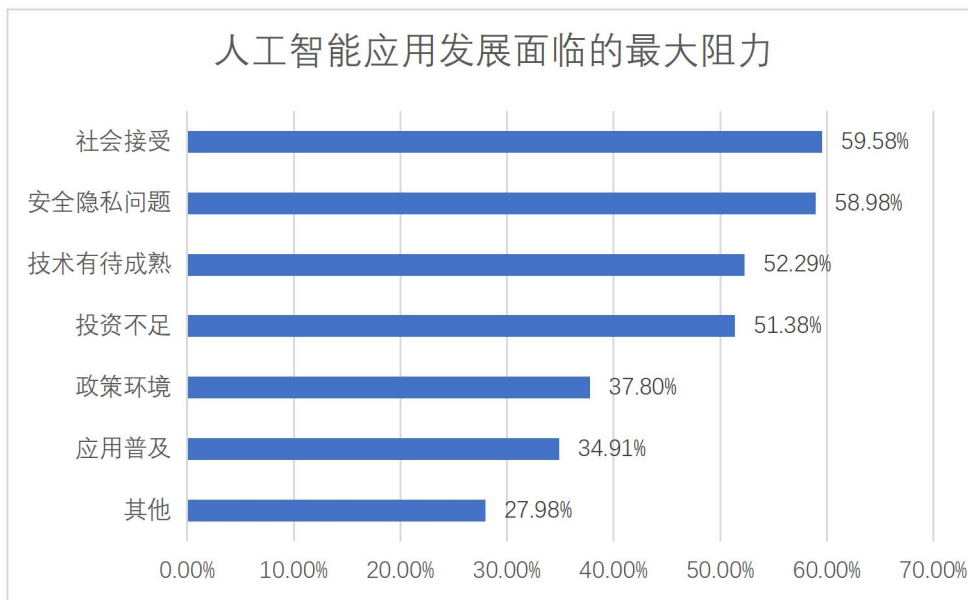


图表 5.1-4：从业人员对人工智能应用领域的期待

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C4 题：您最期待人工智能(AI)在哪些领域发挥优势？）

（5）人工智能应用发展面临的最大阻力

在调查的从业人员认为人工智能应用发展面临的最大阻力时，排名最高的 3 项分别是：社会接受（59.58%）、安全隐私问题（58.98%）、技术有待成熟（52.29%）。

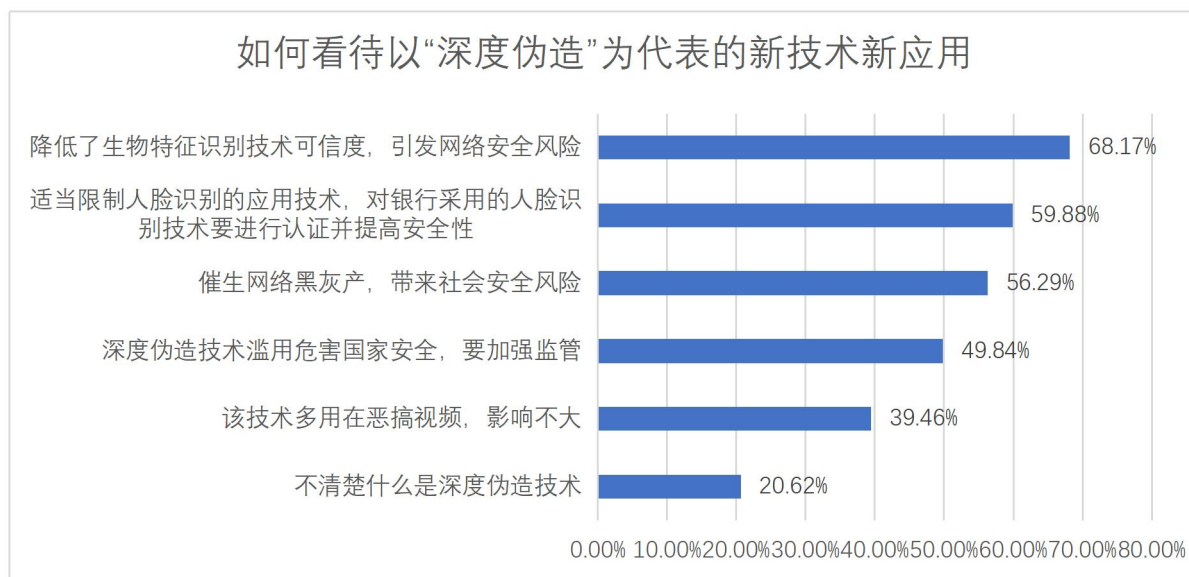


图表 5.1-5：人工智能应用发展面临的最大阻力

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C5 题：您认为目前人工智能应用的发展面临的最大阻力是？）

（6）如何看待以“深度伪造”为代表的新技术新应用

在调查的从业人员如何看待以“深度伪造”为代表的新技术新应用时，排名最高的3项分别是：降低了生物特征识别技术可信度，引发网络安全风险（68.17%）、适当限制人脸识别的应用技术，对银行采用的人脸识别技术要进行认证并提高安全性（59.88%）、催生网络黑灰产，带来社会安全风险（56.29%）。

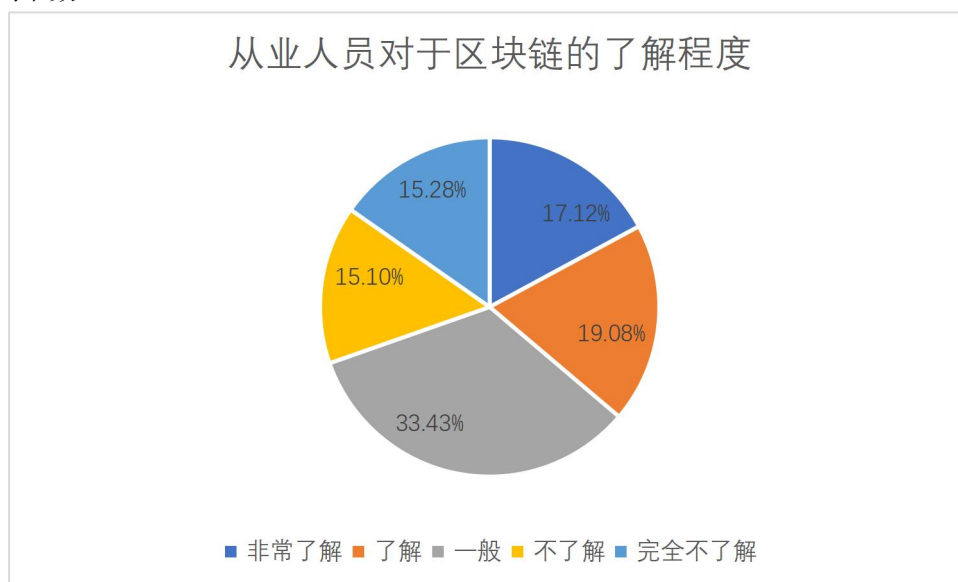


图表 5.1-6：如何看待以“深度伪造”为代表的新技术新应用

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C6 题：近两年出现了“AI 换脸”应用，您怎么看这种以“深度伪造”为代表的新技术新应用？）

（7）从业人员对于区块链的了解程度

在调查从业人员对于区块链的了解程度时，总体上从业人员对于区块链的了解程度是非常欠佳的。其中，非常了解（17.12%）、了解（19.08%），给予积极态度的占比不到半数（36.2%）。



图表 5.1-7：从业人员对于区块链的了解程度

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C7 题：对区块链，您了解多少？）

（8）区块链存在的问题

在调查的从业人员认为当前区块链存在的问题时，排名最高的 3 项分别是：区块链业务和技术标准规范有待完善（55.41%）、技术有待成熟，安全性需要加强（50.49%）、应用场景开发有待深入，缺乏具颠覆性的行业应用（44.81%）、应用

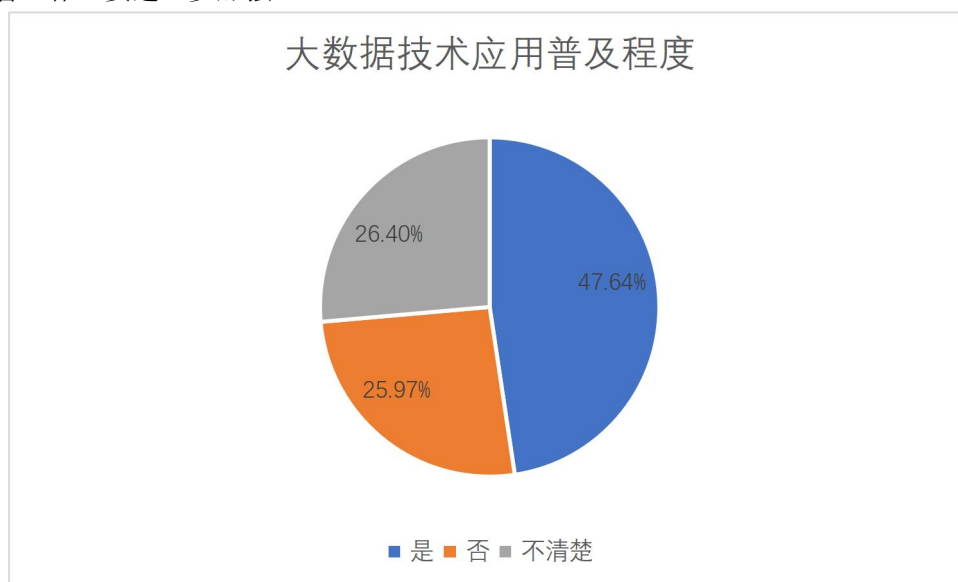


图表 5.1-8：区块链存在的问题

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C8 题：觉得目前区块链应用存在什么问题？）

（9）大数据技术应用普及程度

在调查从业人员所在单位是否应用了大数据技术时，有 47.64%表示已经应用，有 25.97%的人表示没有应用，26.4%的人表示不清楚。数据显示，大数据技术的应用和科普工作还要进一步加强。

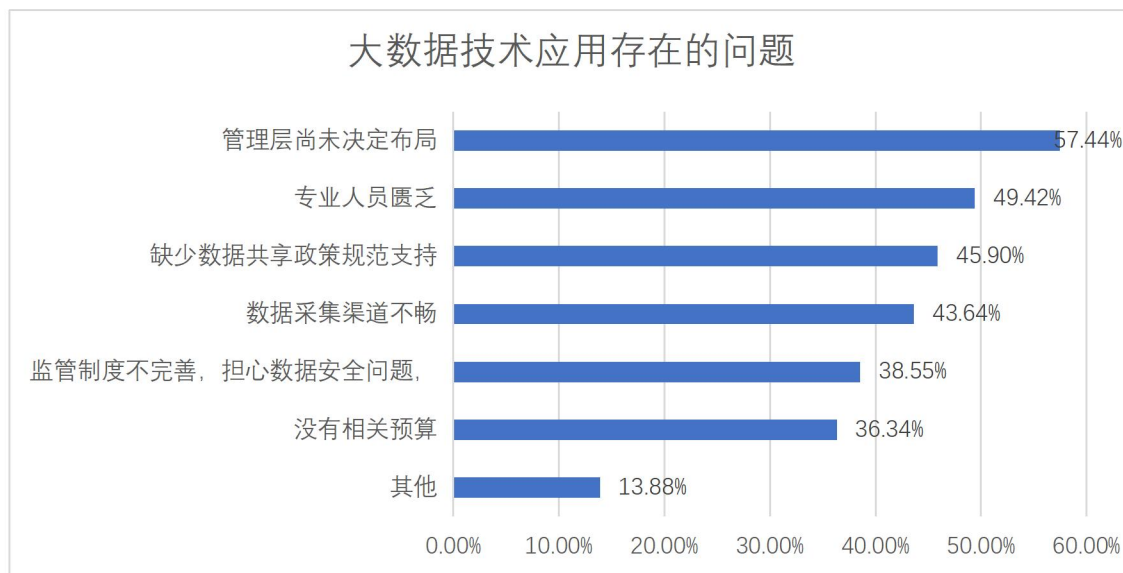


图表 5.1-9：大数据技术应用普及程度

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C9 题：您现所在单位是否应用了大数据技术？）

(10) 大数据技术应用存在的问题

在调查的从业人员认为当前大数据技术应用存在的问题时,排名最高的3项分别是:管理层尚未决定布局(57.44%)、专业人员匮乏(49.42%)、缺少数据共享政策规范支持(45.90%)。

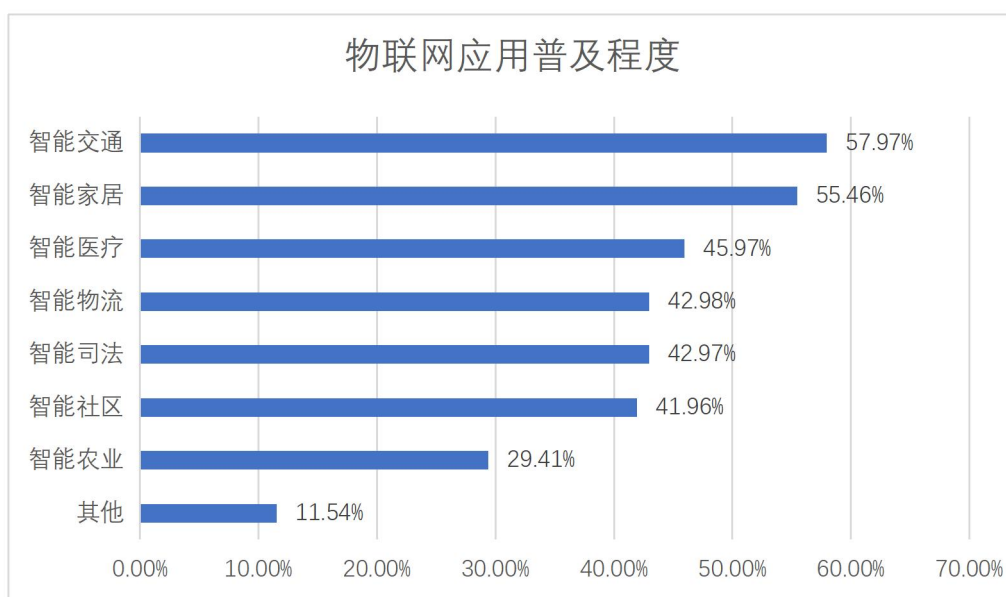


图表 5.1-10: 大数据技术应用存在的问题

(图表数据来源: 从业人员版新技术新应用与网络安全专题第 C10 题: 您认为目前大数据技术应用上存在哪些问题?)

(11) 物联网应用普及程度

在调查的从业人员体验过哪些领域的物联网应用时,排名最高的3项分别是:智能交通(57.97%)、智能家居(55.46%)、智能医疗(45.97%)。



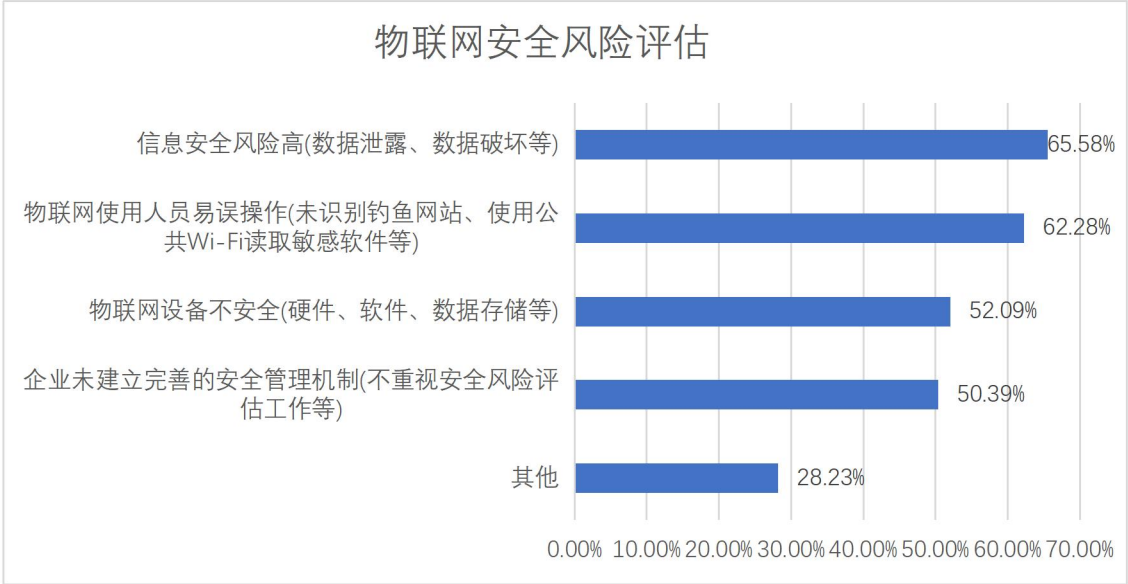
图表 5.1-11: 物联网应用普及程度

(图表数据来源: 从业人员版新技术新应用与网络安全专题第 C11 题: 您在哪些领域体

验过物联网的应用？）

（12）物联网安全风险评估

在调查从业人员认为当下的物联网安全风险主要存在哪些方面时，排名最高的 3 项分别是：信息安全风险高（65.58%）、物联网使用人员易误操作（62.28%）、物联网设备不安全（52.09%）。

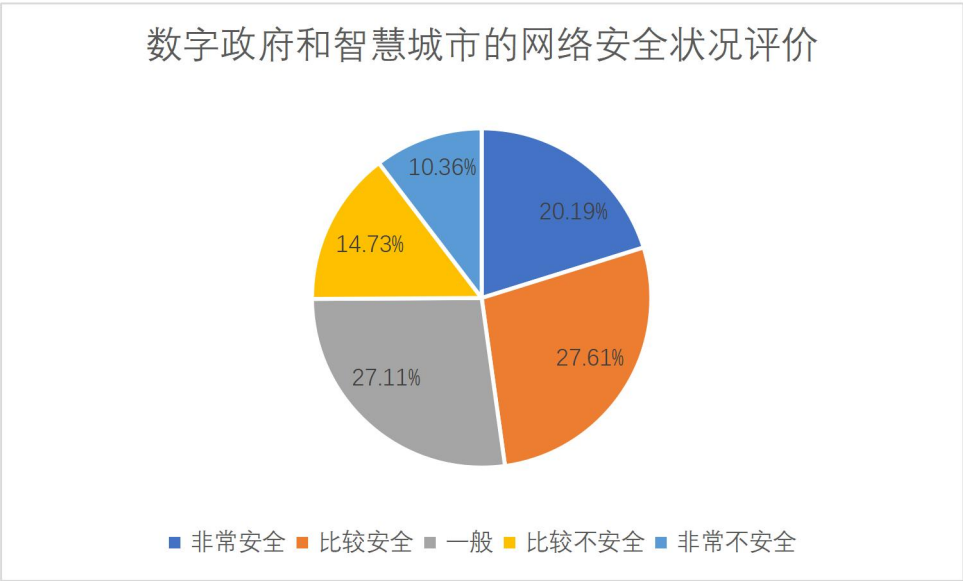


图表 5.1-12：物联网安全风险评估

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C12 题：您认为当下的物联网安全风险主要存在哪些方面？）

（13）数字政府和智慧城市的网络安全状况评价

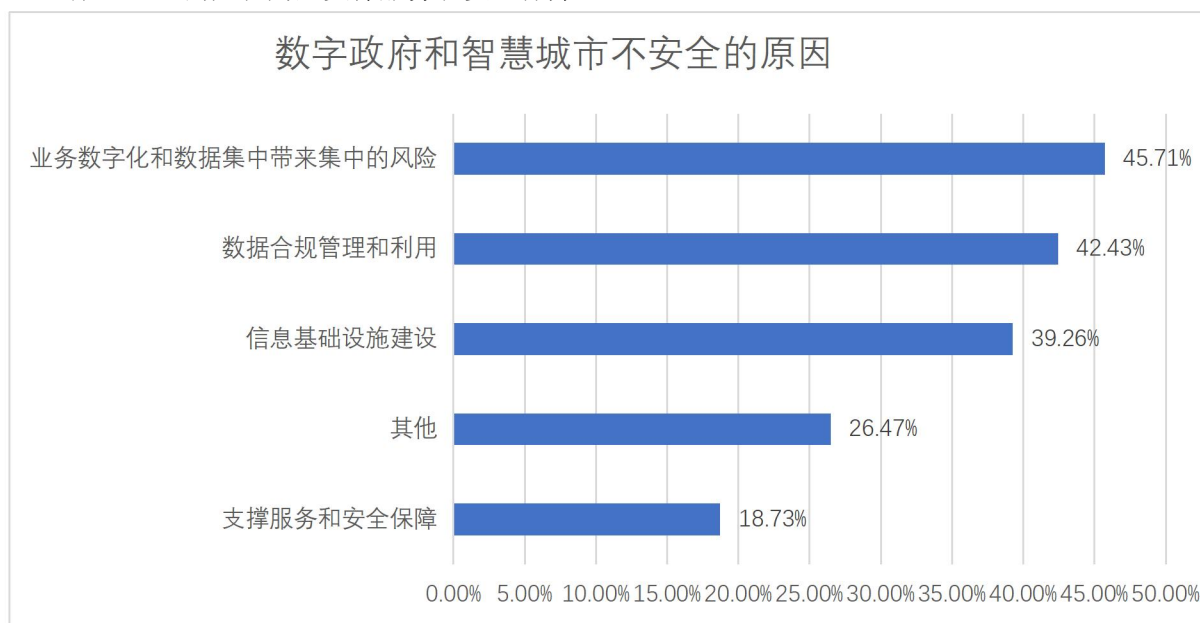
在调查从业人员对于数字政府和智慧城市的网络安全状况评价时，只有不到一半的人表示积极的态度（47.8%），数据显示，数字政府和智慧城市的网络安全状况还需要提升。



图表 5.1-13：数字政府和智慧城市的网络安全状况评价

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C13 题：您对数字政府和智慧城市的网络安全状况评价？）

在进一步调查从业人员认为数字政府和智慧城市不安全的地方主要是什么时，有 45.71%的人认为是业务数字化和数据集中带来集中的风险；42.43%的人认为是数据合规管理和利用；39.26%的人认为是信息基础设施建设；26.47%的人认为是其他原因；以及有 18.73%的人认为是支撑服务和安全保障。



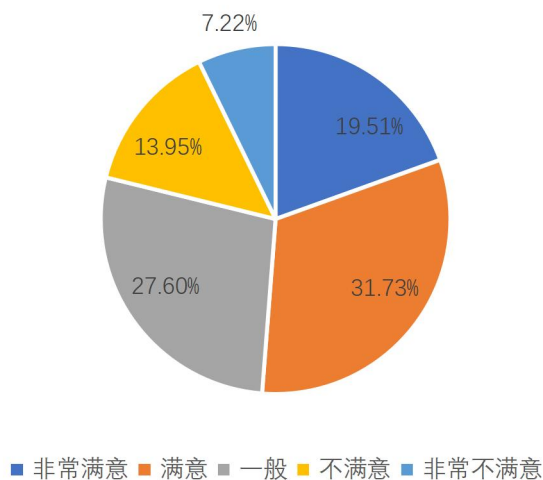
图表 5.1-13.1：数字政府和智慧城市不安全的原因

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C13.1 题：你认为数字政府和智慧城市不安全的地方主要是什么？）

（14）数字政府和智慧城市中新技术的应用效果评价

参与调查的从业人员对于数字政府和智慧城市中新技术的应用效果评价时，超过半数的人给予积极态度（51.24%），其中认为非常满意的有 19.51%，认为满意的最多，占比 31.73%。

数字政府和智慧城市中新技术的应用效果评价

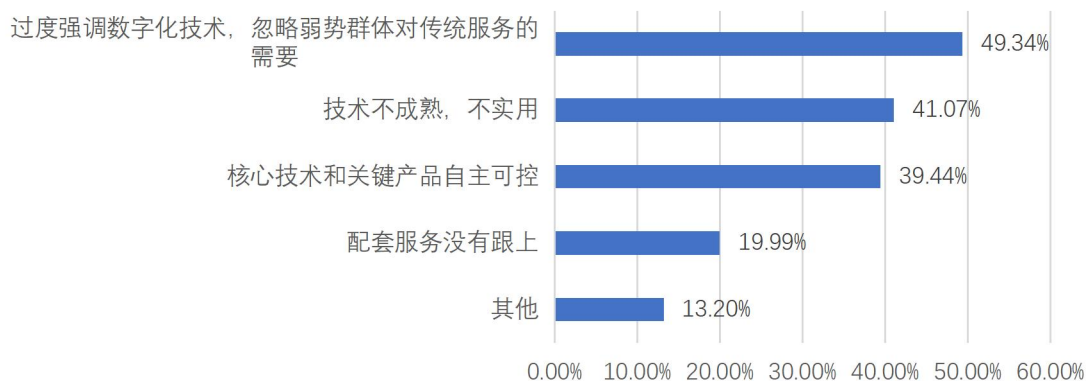


图表 5.1-14：数字政府和智慧城市中新技术的应用效果评价

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C14 题：您对数字政府和智慧城市中新技术的应用效果评价？）

在进一步调查从业人员认为数字政府和智慧城市新技术应用存在问题的主要原因时，排名前 3 的是：过度强调数字化技术，忽略弱势群体对传统服务的需要（49.34%）、技术不成熟，不实用（41.07%）、核心技术和关键产品自主可控（39.44%）。

数字政府和智慧城市新技术应用存在的问题



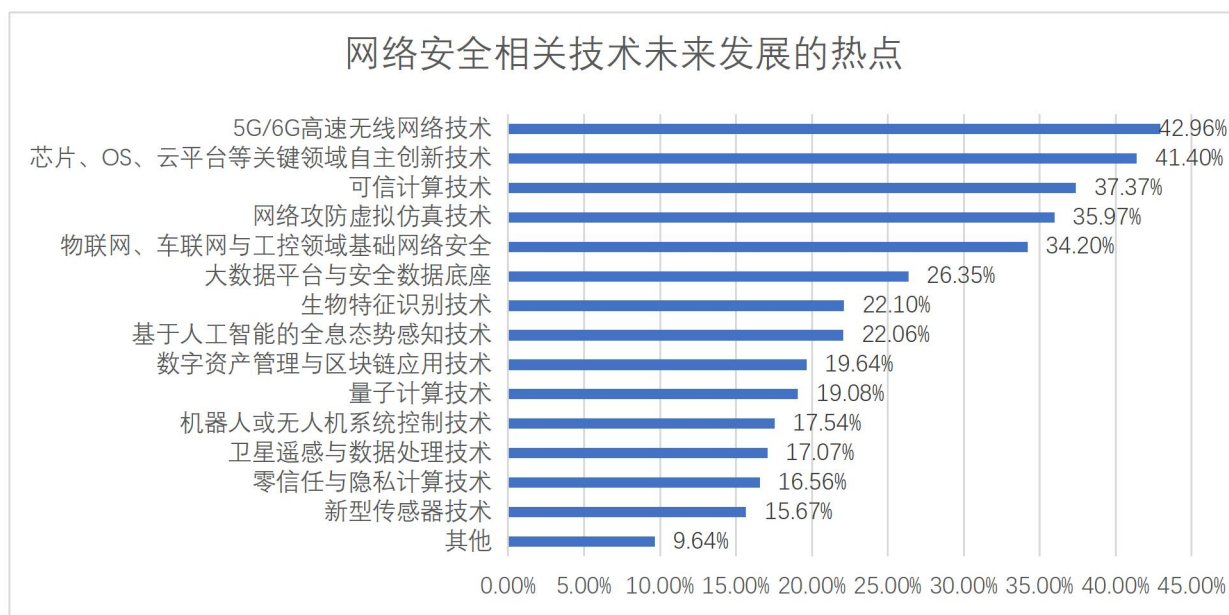
图表 5.1-14.1：数字政府和智慧城市新技术应用存在的问题

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C14.1 题：你认为数字政府和智慧城市新技术应用存在的问题主要是什么？）

（15）网络安全相关技术未来发展的热点

在调查从业人员认为网络安全相关技术未来发展的热点时，排名前 5 的是：5G/6G 高速无线网络技术（42.96%）；芯片、OS、云平台等关键领域自主创新技术（41.40%）；可信计算技术（37.37%）；网络攻防虚拟仿真技术（35.97%）；物联网、车联网与工控

领域基础网络安全（34.20%）。

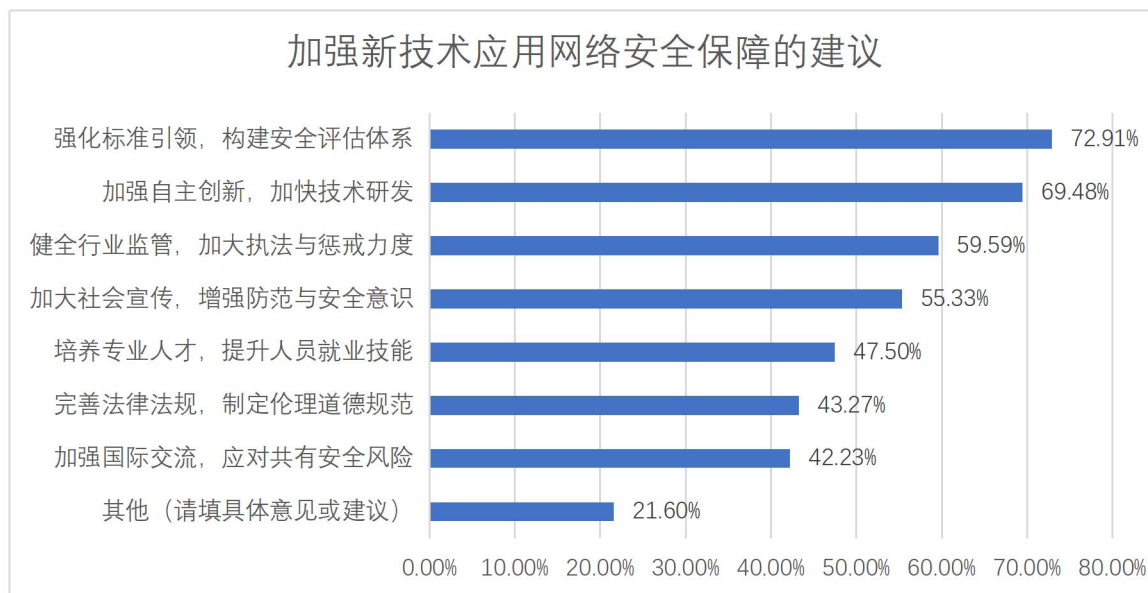


图表 5.1-15：网络安全相关技术未来发展的热点

（图表数据来源：从业人员版新技术新应用与网络安全专题第 C15 题：您认为哪些网络安全相关技术是未来发展的热点？）

（16）加强新技术应用网络安全保障的建议

在调查从业人员对加强新技术应用网络安全保障的建议时，排名前 5 的是：强化标准引领，构建安全评估体系（72.91%）；加强自主创新，加快技术研发（69.48%）；健全行业监管，加大执法与惩戒力度（59.59%）；加大社会宣传，增强防范与安全意识（55.33%）；培养专业人才，提升人员就业技能（47.50%）。



图表 5.1-16：加强新技术应用网络安全保障的建议

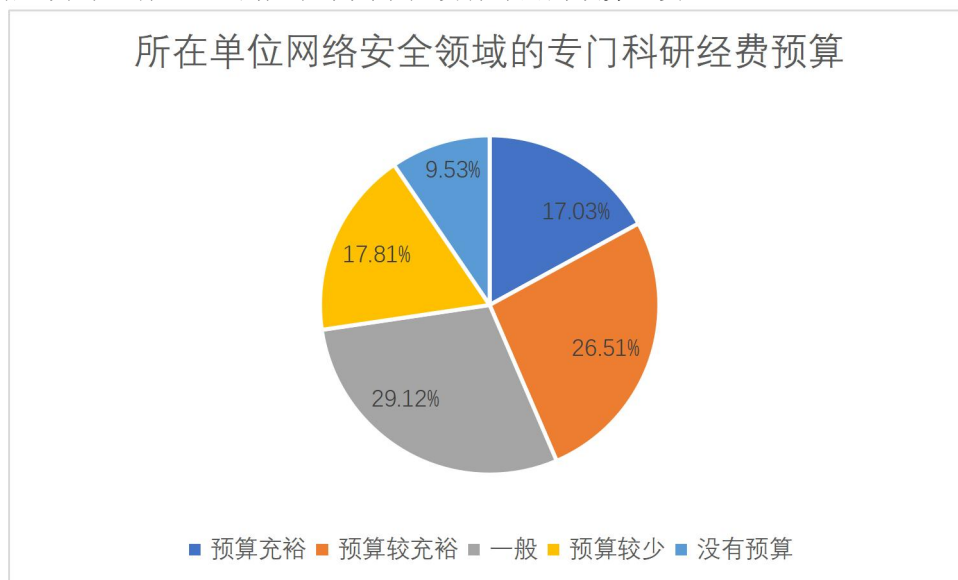
（图表数据来源：从业人员版新技术新应用与网络安全专题第 C16 题：您对加强新技术应用的网络安全保障有哪些建议？）

5.3 科技创新与人才培养

参加本专题调查的从业人员数量一共 72530 人。

（1）所在单位网络安全领域的专门科研经费预算

在调查从业人员所在单位网络安全领域的专门科研经费预算时，评价持正向态度的不足半数（43.54%），具体而言，17.03%的人认为预算充裕，26.51%的人认为预算较充裕。另外，有 9.53%的人表示其单位没有专门的预算经费。



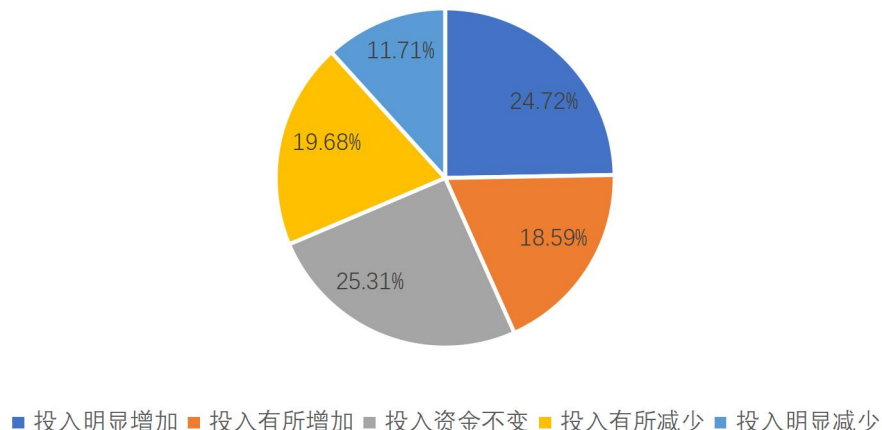
图表 5.3-1：所在单位网络安全领域的专门科研经费预算

（图表数据来源：从业人员版科技创新与人才培养专题第 D1 题：您所在单位在网络安全方面有没有专门的科研经费预算？）

（2）宏观经济环境对网络安全方面资金投入的影响

在调查从业人员所在单位的网络安全方面的资金投入受到宏观经济环境影响时，24.72%的人表示投入明显增加、18.59%的人表示投入有所增加、11.71%的人表示投入明显减少、19.68%的人表示投入有所减少。数据显示，即便受到 2022 年不良的宏观经济环境影响，网络安全方面投入有增加的单位数量比投入有减少的单位要多。

宏观经济环境对网络安全方面资金投入的影响



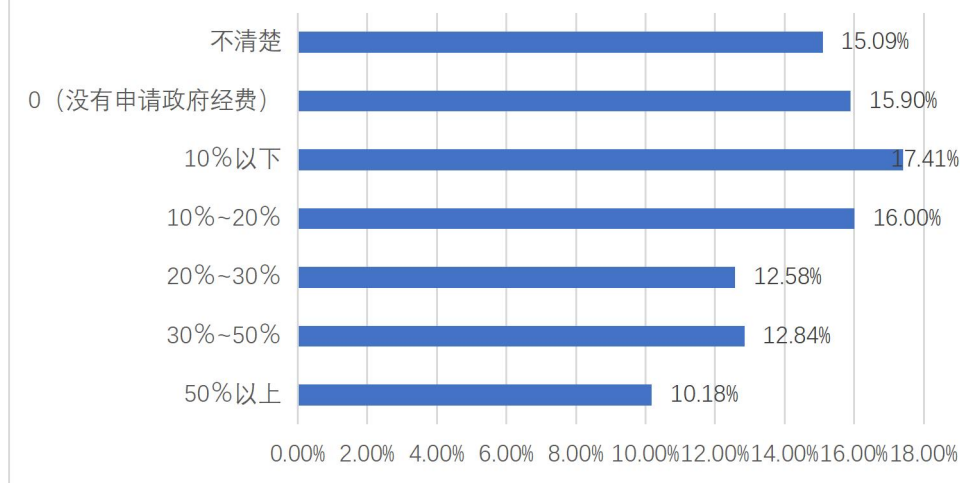
图表 5.3-2：宏观经济环境对网络安全方面资金投入的影响

（图表数据来源：从业人员版科技创新与人才培养专题第 D2 题：今年宏观经济环境状况对本单位网络安全方面的资金投入有什么变化？）

（3）网络安全科研经费中政府支持经费的比例

在调查从业人员所在单位的网络安全科研经费中来自政府方面经费支持的比例时发现，10.18%的单位政府支持经费占比超过 50%、12.84%的单位占比在 30%~50%之间、28.58%的单位占比在 10%~30%之间。

网络安全科研经费中政府支持经费的比例



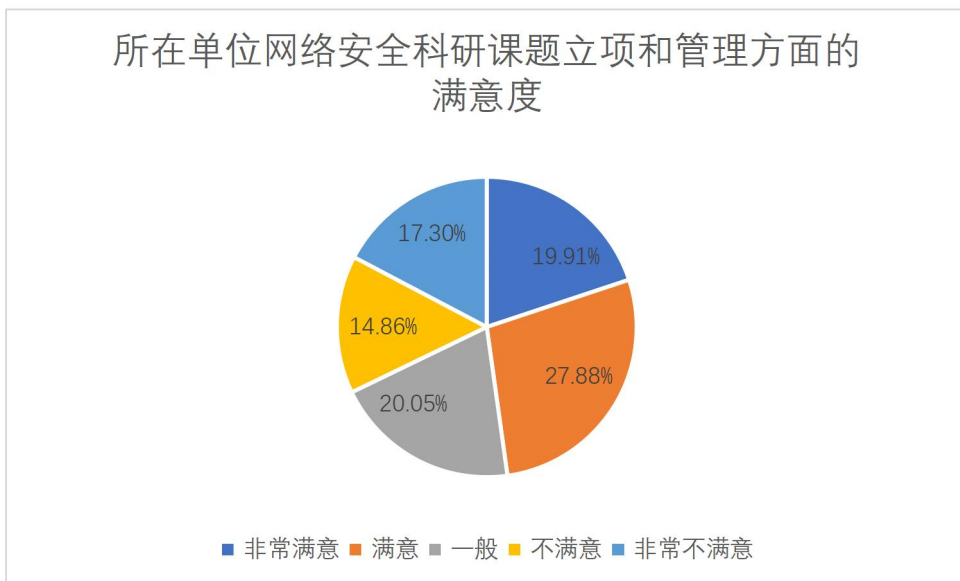
图表 5.3-3：网络安全科研经费中政府支持经费的比例

（图表数据来源：从业人员版科技创新与人才培养专题第 D3 题：您所在单位的网络安全科研经费中来自政府方面经费支持的比例是多少？）

（4）所在单位网络安全科研课题立项和管理方面的满意度

在调查从业人员所在单位网络安全科研课题立项和管理方面的满意度时，持有积极态度的不足半数（47.79%），另外持有负面态度的占比 32.16%。数据显示，从业人员

对于所在单位网络安全科研课题立项和管理方面的满意度不高。

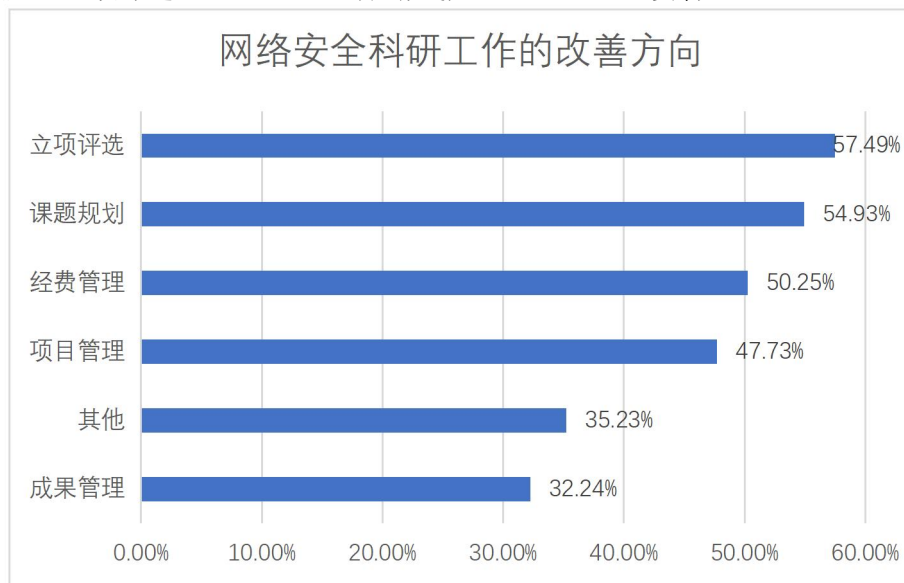


图表 5.3-4：所在单位网络安全科研课题立项和管理方面的满意度

（图表数据来源：从业人员版科技创新与人才培养专题第 D4 题：您对单位在网络安全科研课题立项和管理方面的状况是否满意？）

（5）网络安全科研工作的改善方向

在调查从业人员认为网络安全科研工作开展在哪些方面需要改善时，排名前 3 的选项是：立项评选（57.49%）、课题规划（54.93%）、经费管理（50.25%）。



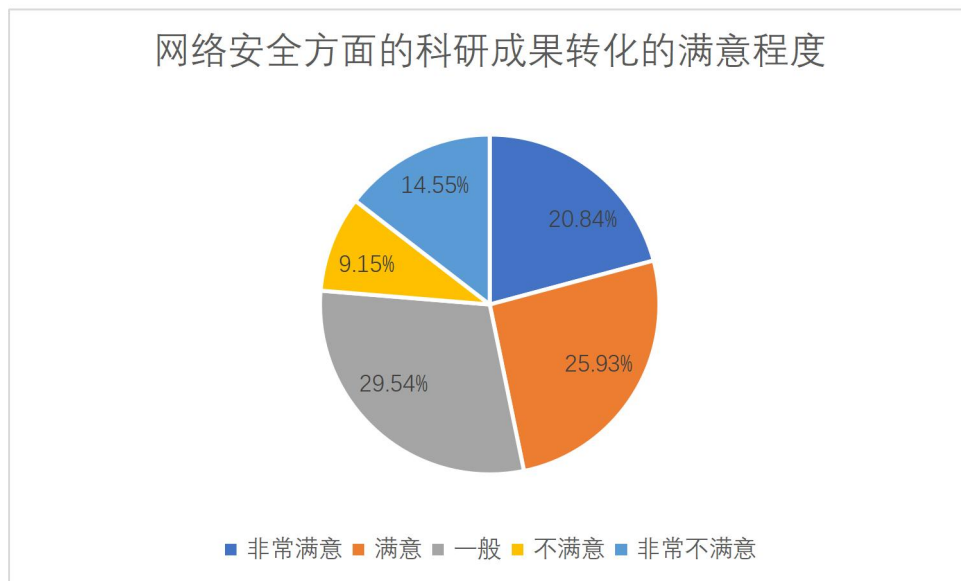
图表 5.3-5：网络安全科研工作的改善方向

（图表数据来源：从业人员版科技创新与人才培养专题第 D5 题：您认为网络安全科研工作开展在哪些方面需要改善？）

（6）网络安全方面的科研成果转化的满意程度

在调查从业人员对于网络安全方面的科研成果转化的满意程度时，持有积极态度的不足半数（46.77%），另外持有负面态度的占比 23.7%。数据显示，从业人员对于网络

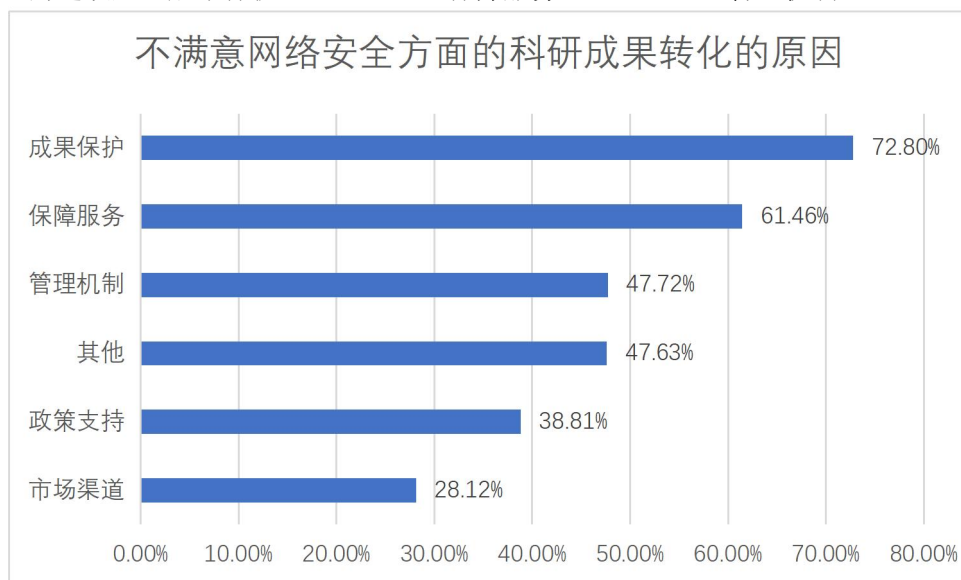
安全方面的科研成果转化的满意度不高。



图表 5.3-6：网络安全方面的科研成果转化的满意程度

（图表数据来源：从业人员版科技创新与人才培养专题第 D6 题：您对网络安全方面的科研成果转化状况是否满意？）

在进一步调查从业人员对于网络安全方面的科研成果转化不满意的原因时，排名前 3 的选项是：成果保护（72.80%）、保障服务（61.46%）、管理机制（47.72%）。



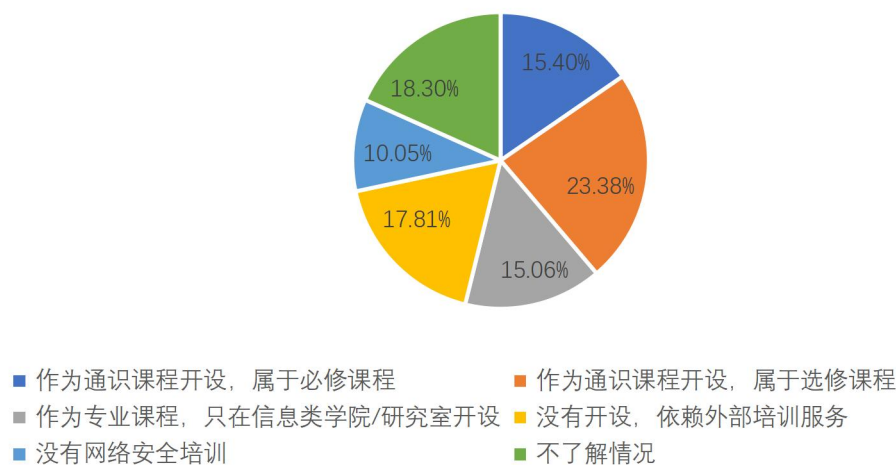
图表 5.3-6.1：不满意网络安全方面的科研成果转化的原因

（图表数据来源：从业人员版科技创新与人才培养专题第 D6.1 题：您对以下哪些方面感到不满意？）

（7）网络安全课程普及程度

在调查从业人员所在单位开设的网络安全课程的情况时，15.4%的人表示作为通识课程开设，属于必修课程；23.38%表示作为通识课程开设，属于选修课程，占比最多；另外有 15.06%的人表示作为专业课程，只在信息类学院/研究室开设。

网络安全课程普及程度



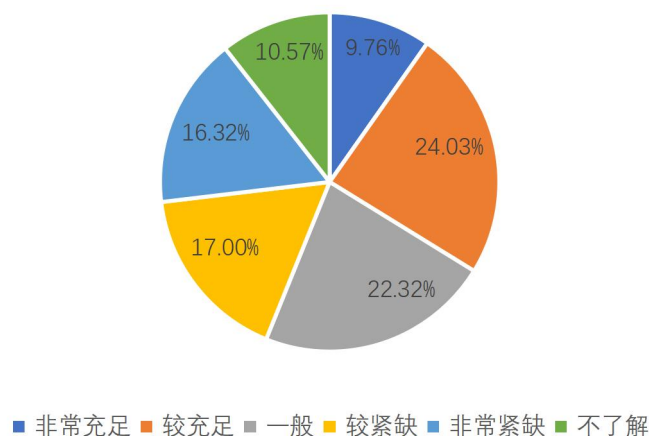
图表 5.3-7：网络安全课程普及程度

（图表数据来源：从业人员版科技创新与人才培养专题第 D7 题：您所在单位开设了关于网络安全的课程吗？）

（8）网络安全领域继续教育培训服务供给评价

在调查从业人员对于网络安全领域继续教育培训服务供给评价时，持有积极态度的不足半数（33.79%），另外持有负面态度的占比 33.32%。数据显示，网络安全领域继续教育培训服务供给市场还有较大的深耕提升空间。

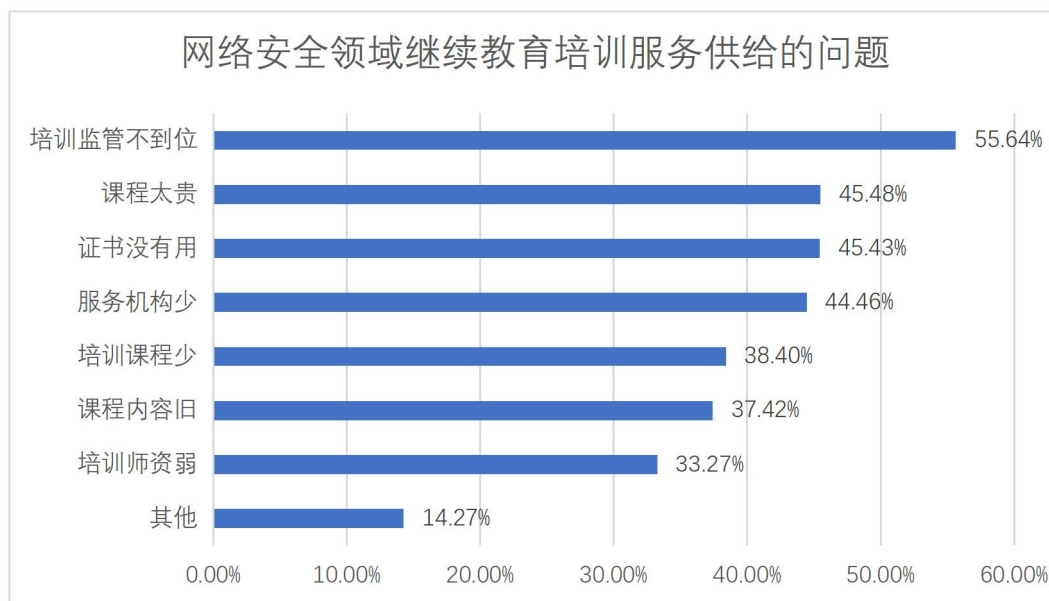
网络安全领域继续教育培训服务供给评价



图表 5.3-8：网络安全领域继续教育培训服务供给评价

（图表数据来源：从业人员版科技创新与人才培养专题第 D8 题：您认为网络安全领域继续教育培训服务供给如何评价？）

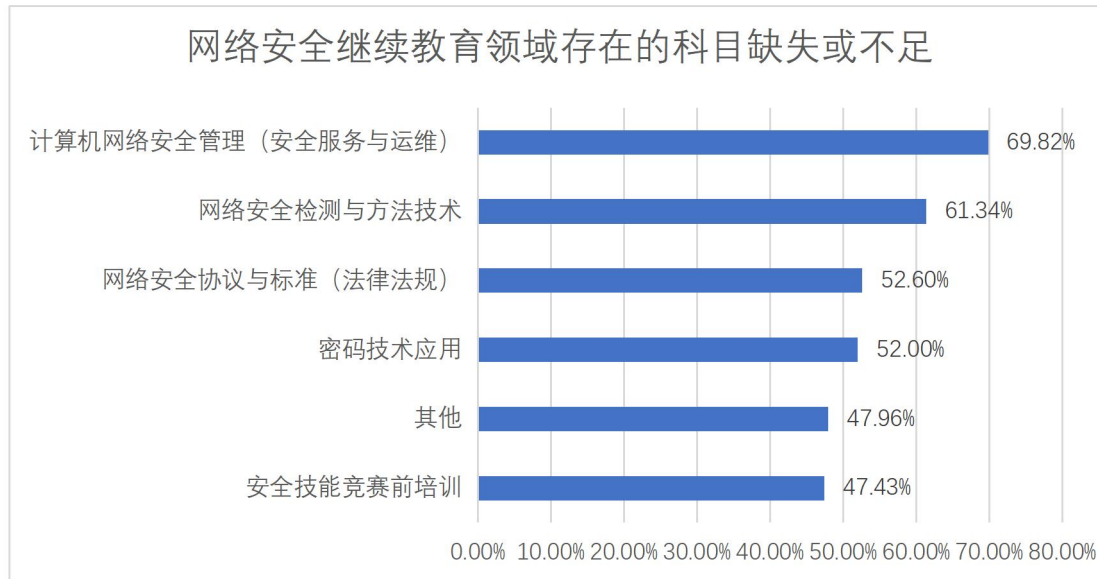
在进一步调查从业人员认为网络安全领域继续教育培训服务供给有什么问题时，排名前 3 的选项是：培训监管不到位（55.64%）、课程太贵（45.48%）、证书没有用（45.43%）。



图表 5.3-8.1：网络安全领域继续教育培训服务供给存在的问题

（图表数据来源：从业人员版科技创新与人才培养专题第 D8.1 题：您认为网络安全领域继续教育培训服务供给有什么问题？）

在进一步调查从业人员认为网络安全继续教育领域存在的科目缺失或不足时，排名前 3 的选项是：计算机网络安全管理（69.82%）、网络安全检测与方法技术（61.34%）、网络安全协议与标准（52.60%）。

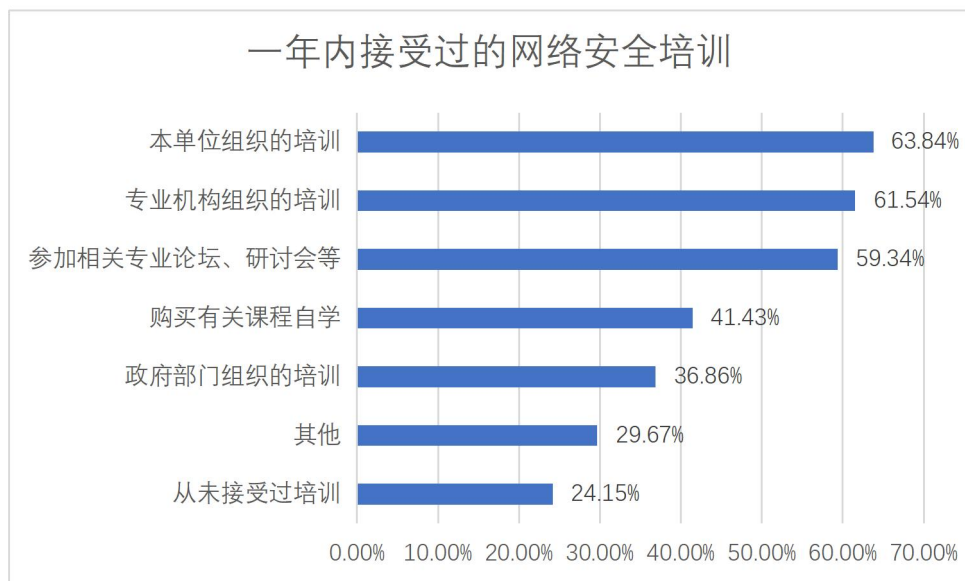


图表 5.3-8.2：网络安全继续教育领域存在的科目缺失或不足

（图表数据来源：从业人员版科技创新与人才培养专题第 D8.2 题：您认为网络安全继续教育领域哪些科目存在缺失或不足？）

（9）一年内接受过的网络安全培训

在调查从业人员在过去的一年接受过的网络安全培训时，排名前3的是：本单位组织的培训（63.84%）、专业机构组织的培训（61.54%）、参加相关专业论坛、研讨会等（59.34%）。

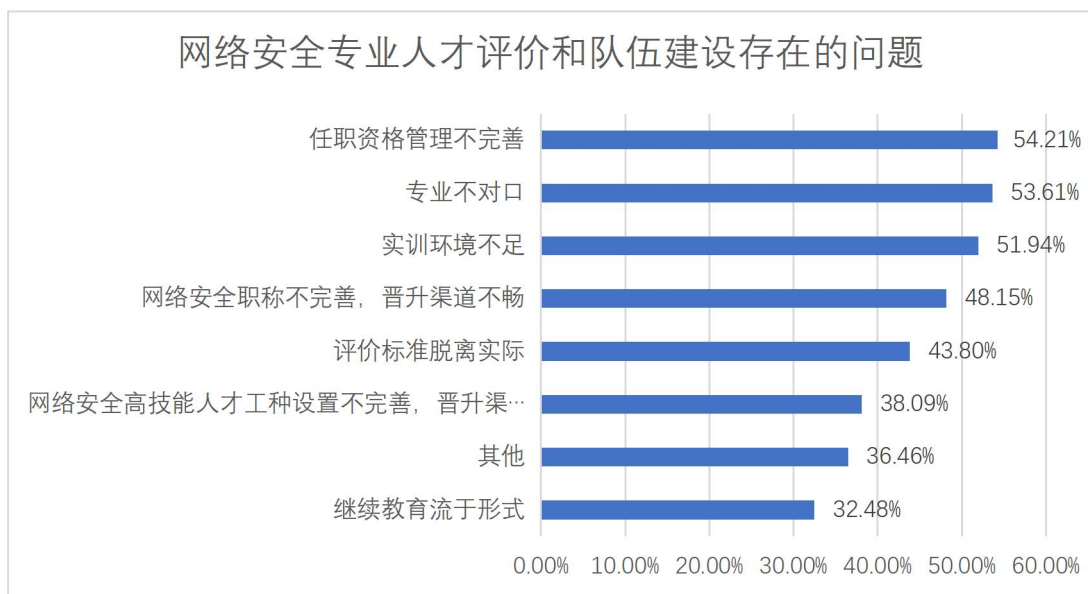


图表 5.3-9：一年内接受过的网络安全培训

（图表数据来源：从业人员版科技创新与人才培养专题第 D9 题：在过去的一年里，您接受过哪些网络安全培训？）

（10）网络安全专业人才评价和队伍建设存在的问题

从业人员认为网络安全专业人才评价和队伍建设方面存在的问题，排名前3的分别是：任职资格管理不完善（54.21%）、专业不对口（53.61%）、实训环境不足（51.94%）。

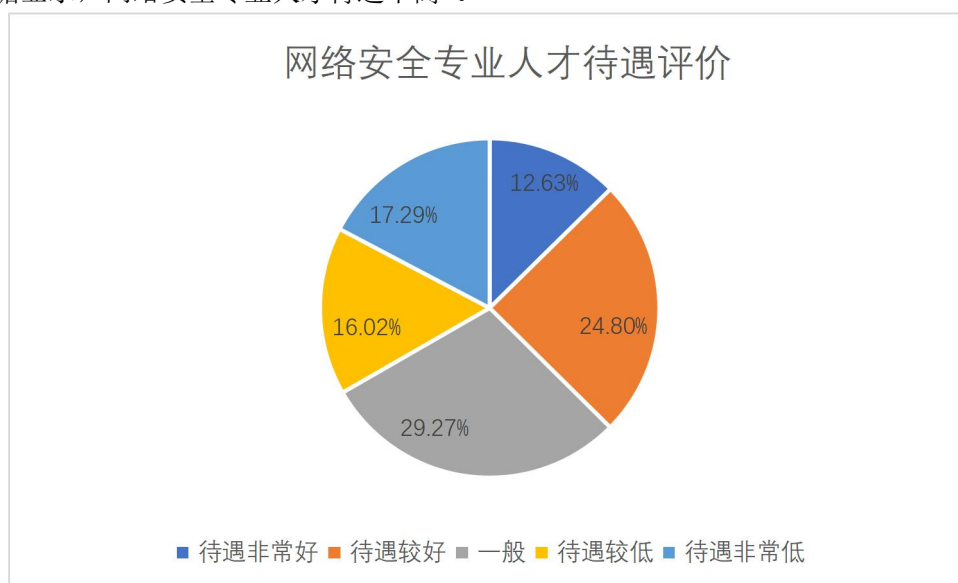


图表 5.3-10：网络安全专业人才评价和队伍建设存在的问题

（图表数据来源：从业人员版科技创新与人才培养专题第 D10 题：您认为网络安全专业人才评价和队伍建设方面存在哪些问题？）

（11）网络安全专业人才待遇评价

在调查从业人员单位内部网络安全专业人才待遇时发现,持有积极评价的不足半数(37.43%), 另外有 33.31%的人认为其单位内部网络安全专业人才待遇是偏低的。数据显示,网络安全专业人才待遇不高。



图表 5.3-11: 网络安全专业人才待遇评价

(图表数据来源: 从业人员版科技创新与人才培养专题第 D11 题: 您认为单位内部网络安全专业人才待遇如何?)

六、 结论

本次网民网络安全感满意度调查是在总结去年满意度调查成功经验的基础上进行的,在许多方面包括问卷设计、组织发动、活动支持、数据服务等都有新的突破。在公安等有关主管部门大力支持下,在各组织单位共同努力下,调查活动取得良好效果,活动收回的问卷数量比去年有跨越式的增长,说明网络安全感满意度调查活动受到了网民极大的关注。从统计结果来看,本次问卷调查数据提供了丰富的信息,反映了广大网民对当前网络安全状况和治理效果的满意程度的评价,包括网民对热点问题的关注、对整体网络安全态势的感受、以及对政府监管、企业自律、行业发展、数字政府服务等方面的评价。另外,网民还提出了许多意见和建议,这些意见对政府有关部门加强网络空间治理,打造一个安全、清朗的网络空间有增添的调查的成果是丰富的。

总体来说,本次调查成果有以下主要结论:

(1) 网络安全状况总体评价较高, 相较 2021 年有所提升

绝大多数参与调查的从业人员对当前网络安全总体状况表示肯定,超过半数的网民认为网络状况相比较 2021 年有一定的提升。在网络安全监管力度、网络安全产品与服务发展政策环境、信息技术产品自主可控生态、网络安全未来发展趋势、数字政府与智慧城市新技术应用等方面获得从业人员的积极评价。

在过去一年里,各级政府部门在党中央的统一部署下,围绕网络安全的各种问题,突出重点,积极谋划,精准施策,先后推出一系列有针对性的法律、规范、措施和行动,从多个层面和领域出发,打出了一套套组合拳,取得了显著的成果,给人民交出了一份漂亮的答卷。其行动之迅速,力度之大,成果之丰富,令人印象深刻,体现出我国政府成熟、自信、眼光和气魄,更标志着我国政府在网络空间治理能力方面有了长足的进步。

随着数据安全保护法、个人信息保护法、关键信息基础设施保护条例等重要法律的推出和实施,网络安全治理的“四梁八柱”框架建设取得重要成果,加上一系列的配套措施的落实,打开了网络安全治理的新局面,也标志着我国网络安全治理上了一个新台阶。调查结果也显示过去一年里我国网络安全治理在多个方面的工作取得了显著成效,网民的评价的大幅提升也充分证明了这一点。

(2) 助力数字经济发展, 网络安全治理作用凸显

多数网民在使用网络时总体感觉是安全的。相对于去年,在网络骚扰行为、违法有害信息和侵犯个人信息等几个比较常见的网络安全问题上,数据显示出现的比例有一定的程度下降,表明网络安全治理取得一定成效。

今年以来抗击疫情的斗争进入常态化阶段,在党、政府和人民的共同努力下,我国国民经济加快恢复和发展。疫情的发生和发展,给人们工作和生活方式带来了很大的变化。隔离、封锁等变化一方面给人们生活造成不便,但另一方面也给数字经济的发展提供了一个特殊的契机。远程办公、网络协同、线上服务等需求的爆发,极大地推动了各行各业向业务数字化转型。有了网络和信息技术的加持,传统经济迎来了升级换代加速发展的新阶段。在应对变局的过程中,出现了许多基于网络信息技术的新技术、新应用,也让人看到了数字经济的巨大活力和发展潜力。碳中和、绿色经济等新发展目标和理念的提出引领各个行业进入新一轮转型、升级和发展阶段。数字化是未来发展的方向,数字技术和网络技术已经成为关键技术,网络和信息化基础设施成为不可或缺的基础条件,网络安全将起重要的保障作用。习近平总书记对网络安全的重要性作出了重要论断:“没有网络安全就没有国家安全,没有信息化就没有现代化”。

习总书记还深刻阐述了网络安全和信息化发展的辩证关系,指出“网络安全和信息化是



网安联微信公众号

网安联秘书处

官网：www.iscn.org.cn

电话：020-8380 3843/13911345288

邮箱：cinsabj@163.com