2019 网民网络安全感满意度调查

数据统计报告

（从业人员版）

全国卷

指导单位：公安部网络安全保卫局

牵头组织：全国信息网络安全协会联盟

发起单位：全国 135 家网络安全社会组织

承办单位：广东新兴国家网络安全和信息化发展研究院

二〇一九年九月

本报告数据来源于 2019 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：

联系方式：办公室 020-83113010 / 林先生 13269828768
邮箱地址：cinsabj@163.com

目录

前 言

互联网已与国民经济社会发展深度融合，与人民群众日常生活密不可分。在提供各种生活便利和沟通便捷的同时，网络攻击、病毒传播、垃圾邮件等迅速增长；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，也正在严重危害青少年的身心健康。如何有效开展网络安全社会治理、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。

开展网络安全感满意度调查，旨在进一步贯彻习近平总书记关于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，提高综合治网的成效和水平。

2019 网民网络安全感满意度调查活动由公安部网络安全保卫局指导、全国 135 家网络社会组织共同发起（详见附录）。中央电视台《社会与法》频道、北京大学、《新华社经济参考报》、《信息安全与通信保密》、《中国信息安全》、《信息网络安全》、《信息安全研究》、《警察技术》、《经济》、《经济参考报》、《中国财经论坛》、《中青报》、《光明日报》、人民网、中国网、腾讯、百度、新浪、网易、今日头条、新浪、新浪微博、京东、爱奇艺、哔哩哔哩、花椒直播、斗鱼、快手、映客等各大媒体提供平台支持。参与活动各方齐心协力，各司其职，各尽其责，为调查活动的顺利开展做出了重大贡献。

调查问卷分为公众网民版和从业人员版。公众网民版从大众化的角度，设置七个专题二级问卷，在去年的个人信息保护、遏制网络违法犯罪行为、未成年人权益保护三个专题的基础上，增加了法制建设、网络购物安全、网络平台企业安全监督管理、数字政府安全服务四个专题。从业人员版从专业化、运营服务的角度，重点了解网络从业人员对当前网络安全状况的感知、评价、建议和期待，以及对有关问题的认知和态度，面向网络服务提供者、网络安全产品服务提供者、联网使用单位、政府网络安全监督管理部门、网络行业协会，设计分类问卷。

2019 年 8 月 13 日 9:00，调查活动启动线上样本采集，8 月 22 日 24:00 结束，历时十天。全国共收到样本 221266 份，其中公众网民答卷数量共计 189495 份，网络从业人员答卷数量共计 31771 份。样本来源覆盖全国 31 个省、直辖市、自治区和港澳台，样本数据总量大幅度超越去年。

与 2018 年相比，2019 网民网络安全感满意度调查活动取得多方面的进步和突破。一是规格和规模更上层次。公安部网络安全保卫局成为活动指导单位，对调查活动的宗旨、定位、组织等各方面工作进行全面指导；活动得到全国各省市网络社会组织积极响应，发起单位从 2018 年的 85 家增加至 135 家。二是调查范围更加广泛，依托分布在全国各地区、各领域数量众多的发起单位和支持单位，大幅度扩大调查范围。调查活动采取线上问卷调查和线下调研相结合的方式进行，主要通过“网络安全共建网”、活动发起单位和支持单位网站、网络平台、商业

门户网站、中央（地方）重点新闻网站等平台及其对应的移动端 App、公众号等媒体平台上发布调查公告和调查问卷的链接，通过持续置顶公告、持续悬浮窗公告、移动客户端热点推文、微博微信等公众号热点推文等形式，发动和鼓励社会公众网民和网络从业人员参与填写问卷。同时通过走访、座谈、培训、会议等方式开展线下调研，同步收集调查样本。三是更加注重倾听网民真实的声音，调查问卷增加重要议题，围绕与网民上网的安全感满意度相关的关键因素、关键行业、关键话题，从网络安全立法、应用、保护、执法司法、社会服务、产业发展等 6 个维度共 11 个议题，面向广大网民和网络从业人员来设计问卷题目。四是宣传形式更加灵活多样，以视频、小程序等方式广泛宣传网络安全法律法规及相关知识，利用活动平台，更好地提升网民的自我保护意识和能力。五是样本数据量更多，覆盖面更广。样本覆盖全国 31 个省、直辖市、自治区和港澳台，样本数据总量大幅度超越去年。

2019 网民网络安全感满意度调查数据统计报告

（从业人员版）

全国卷

一、概述

2019 网民网络安全感满意度调查从业人员版数据统计报告，是针对网络行业从业人员进行调查收回的有效问卷数据统计结果。网络行业从业人员指网络行业的工作人员，其工作单位或工作岗位和网络有关，包括互联网企业、网络安全产品与服务的提供者、网络安全协会、政府主管部门、企事业单位、网络安全的学校和科研机构、一般互联网用户等。网络行业从业人员本身对互联网的状态比较了解，是网络安全治理中主要的参与者、服务提供者和服务利用者。他们的意见体现了网络安全治理中各类利益群体和专业人士的观点。

从业人员版的调查问卷根据从业单位业务特点细分为 A 到 H 共 8 个问卷，分别如下。

A 问卷：面向网络服务提供者网络安全相关工作（以下简称 A 类）从业人员的问卷。

B 问卷：面向网络服务提供者非网络安全相关工作（以下简称 B 类）从业人员的问卷。

C 问卷：面向网络安全产品、服务提供者（以下简称 C 类）从业人员的问卷。

D 问卷：面向网络行业协会（以下简称 D 类）从业人员的问卷。

E 问卷：面向政府网络安全监督管理部门（以下简称 E 类）从业人员的问卷。

F 问卷：面向国有企事业单位（以下简称 F 类）从业人员的问卷。

G 问卷：面向科研机构、大学（以下简称 G 类）从业人员的问卷。

H 问卷：面向其他联网使用单位（以下简称 H 类）的从业人员的问卷。

本报告第一章为概述；第二章为总体分析，包括受调查从业人员的基本信息、从业人员整体网络安全感分析及主要发现；第三到第十章为从业人员版调查数据详细统计，包括 A 到 H 类从业人员调查问卷内容的详细统计结果。

二、总体分析

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 31771 份，数据清洗消除无效数据后，有 26513 份问卷数据纳入统计，数据样本有效性 83.45%。

参与调查的从业人员工作岗位，根据各个行业岗位方向的答卷数量，占比最高的前三位依次是：一般的联网使用单位人员（H 类）占 24.06% ， 网络服务提供者非网络安全相关工作的人员（B 类）占 17.52%，网络服务提供者的网络安全相关岗位工作（A 类）占 16.71%。第四到第八位的依次为网络安全产品、服务提供者（C 类）占 13.97%，国有企事业单位（F 类）占 11.21%，科研机构、大学（G 类）占 9.21%，政府网络安全监督管理部门（E 类）占 3.87%，网络行业协会（D 类）占 3.45%，如图 2-1 所示。

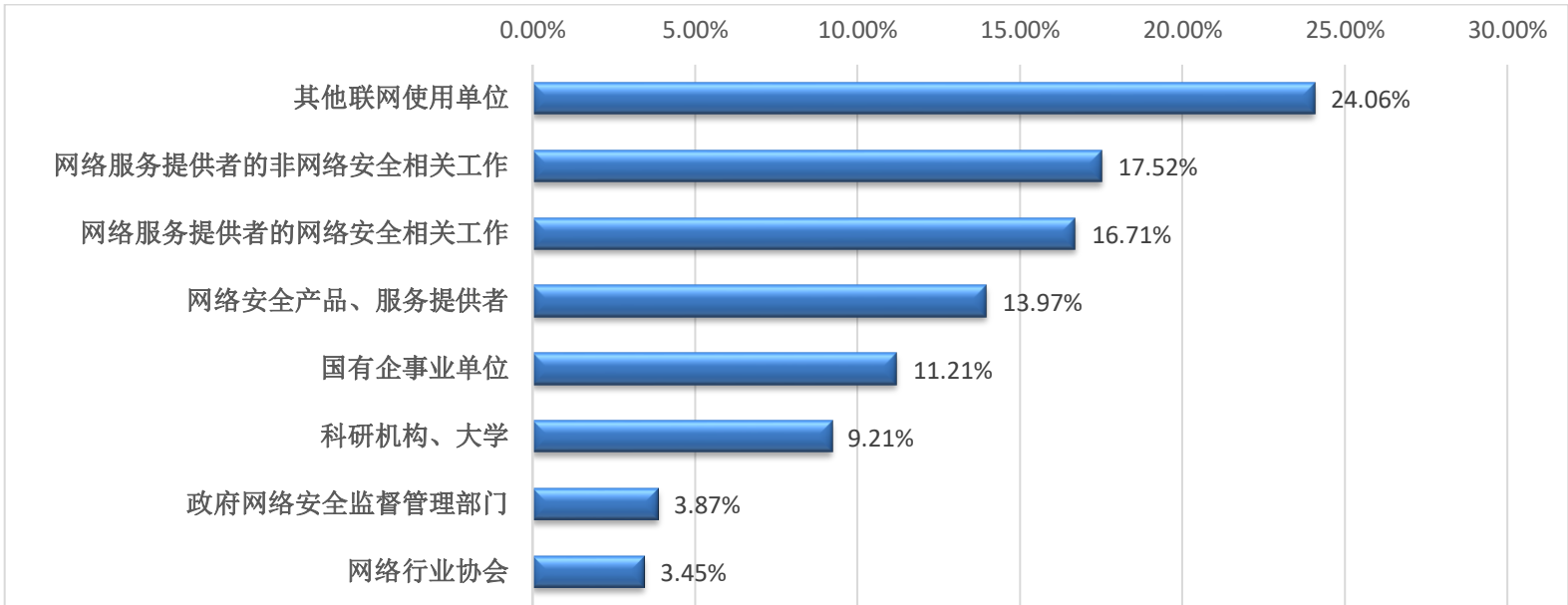


图2-1：岗位分布

1. 受调查从业人员基本信息

受调查从业人员的基本信息主要包括性别、年龄、从业时间、学历。

1.1、性别分布

受调查的从业人员男性占 70.21% ， 女性占 29.79 %。**相较于 2018 年数据男性占 64.95%，女性占 35.05%，有所变化（如图 2-2）。**

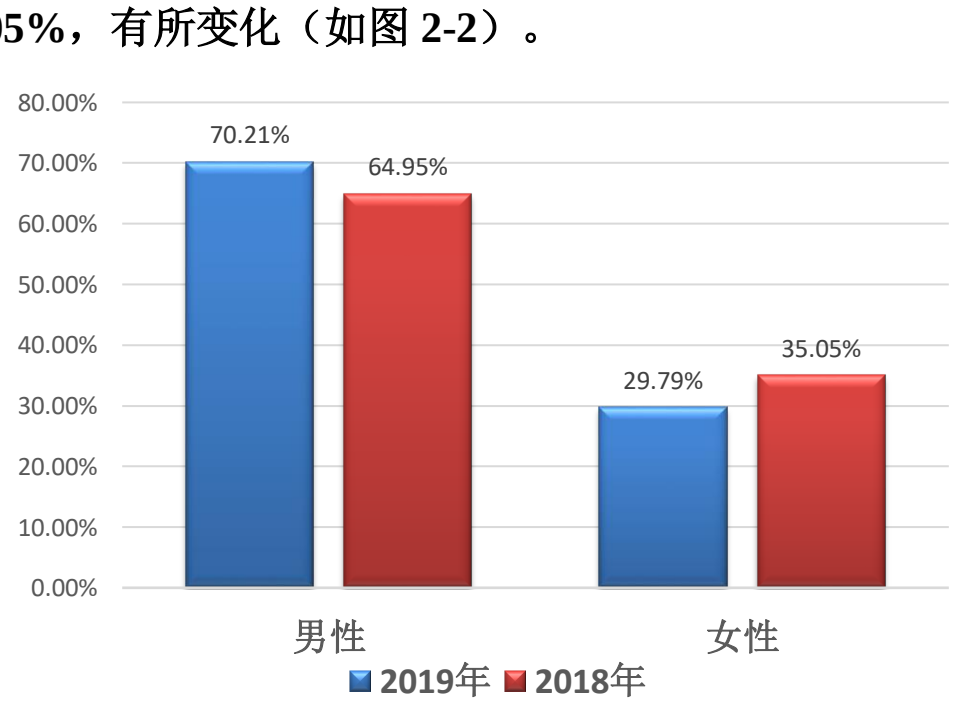


图2-2：性别比例

1.2、年龄分布

受调查的从业人员中 30 岁以下的占比 70.7%， 其中 12 到 18 岁占 4.84%，19 到 24 岁占 33.82%，25 到 30 岁占 32.04%。**相较于 2018 年数据， 30 岁以下占比 72.07%，略低了 1.37 个百分点（如图 2-3）。**

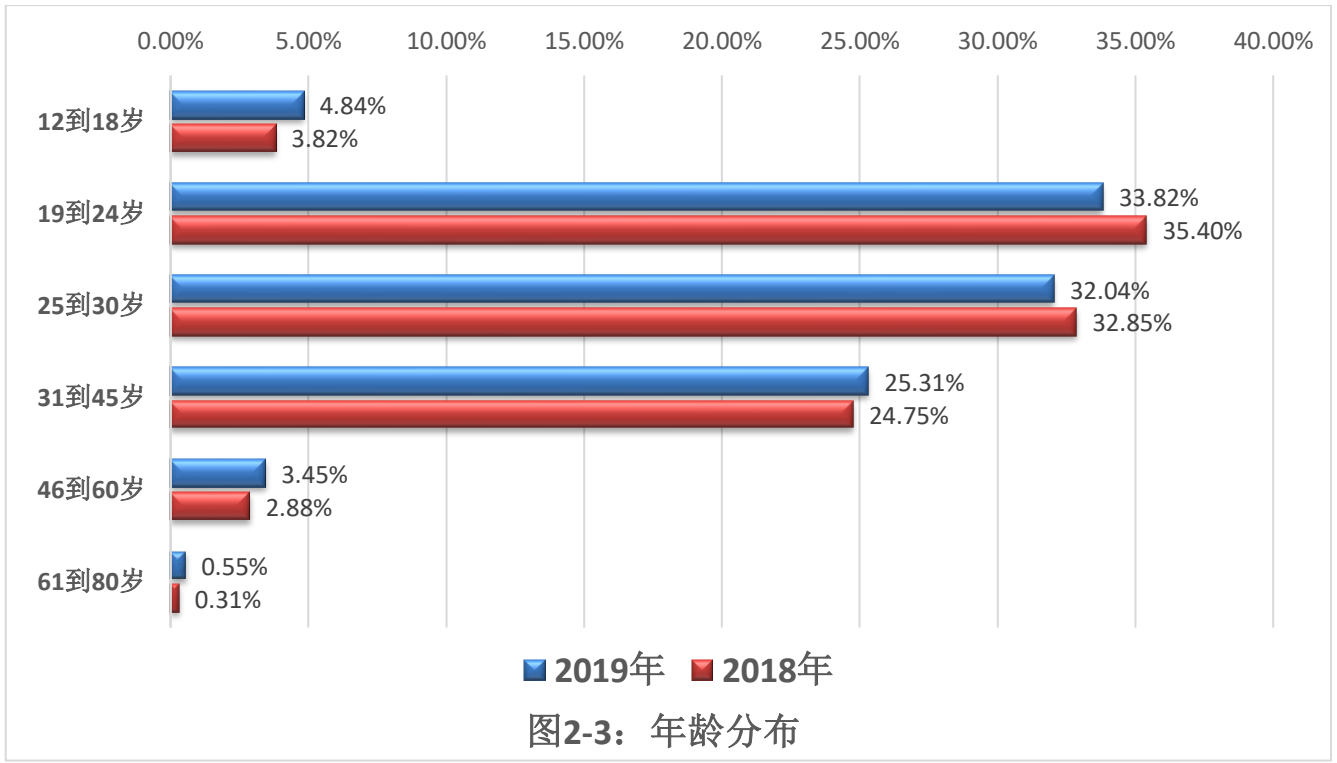


图2-3：年龄分布

1.3、从业时间

受调查从业人员的从业时间一般为 10 年以内。其中 4-10 年区间占 44.48%，1-3 年区间占 39.58%，两者合计 84.06%。**相较于 2018 年从业时间 10 年内的占比 85.16%，略低了 1.1 个百分点（如图 2-4）。**

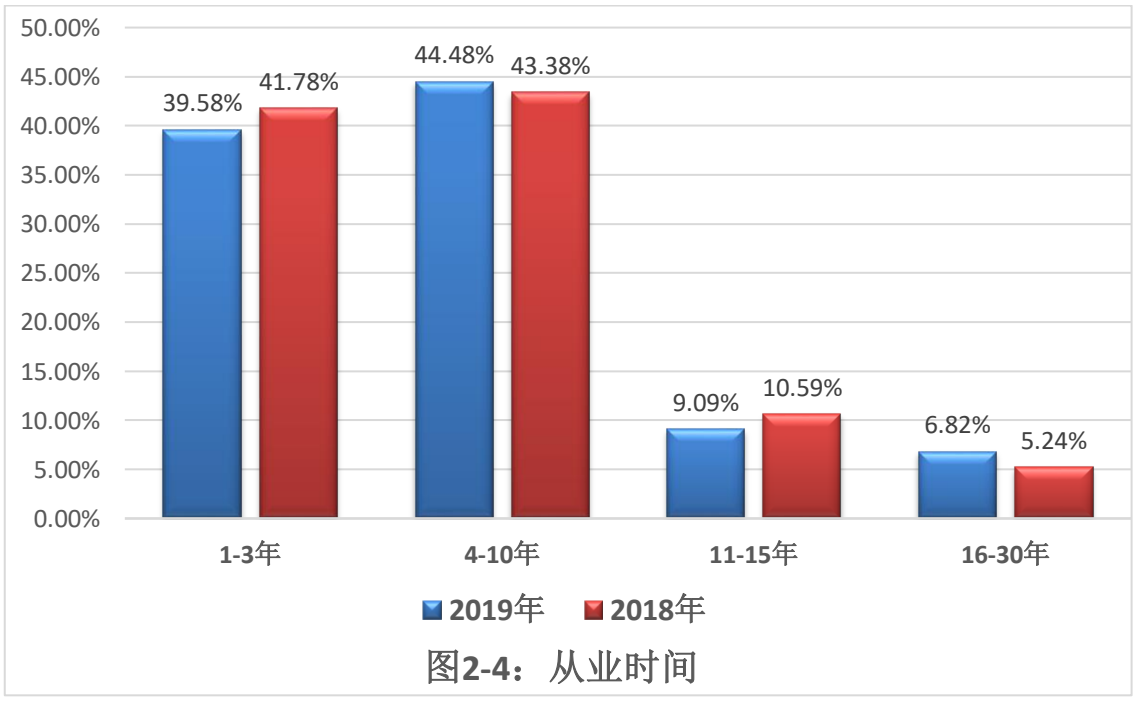


图2-4：从业时间

1.4、学历分布

受调查的从业人员学历以本科为主，占 50.08%，其次是大专占 24.24%。研究生及以上学历占 11.22%，大专及以上学历占比 85.54%，**相较于 2018 年数据 79.73%，高了 5.81 个百分点（如图 2-5）。**

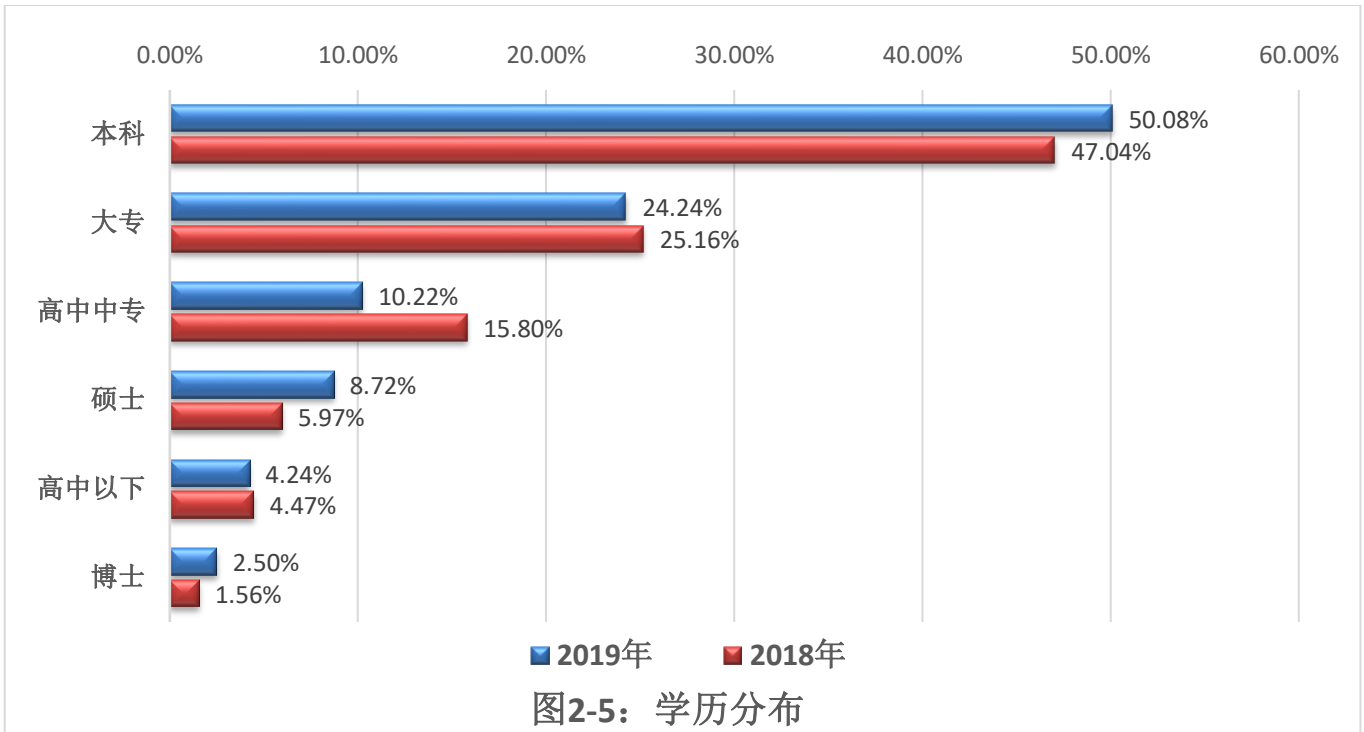
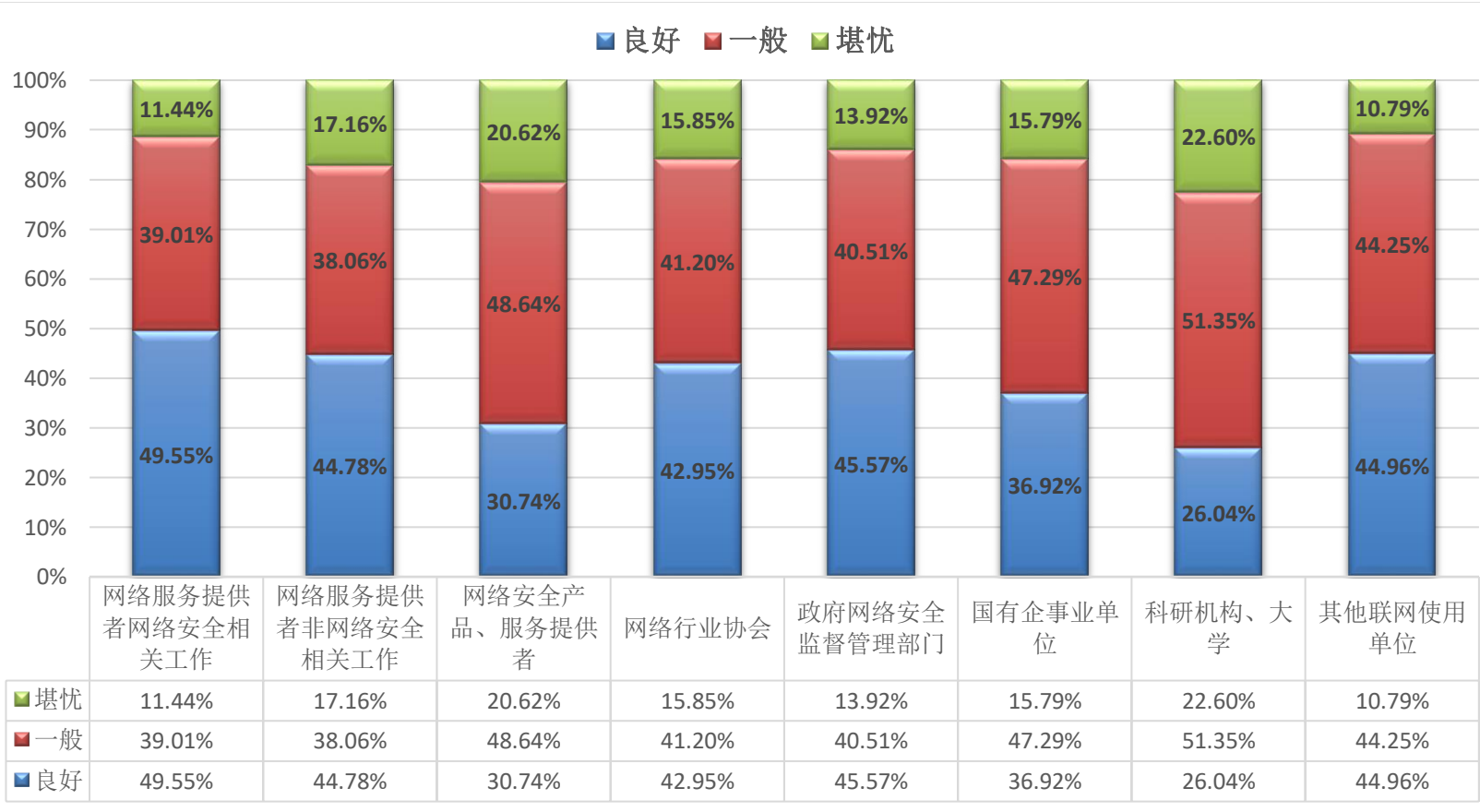


图2-5：学历分布

2.不同行业岗位的从业人员网络安全感分析

不同行业岗位的从业人员对当前网络安全状况的评价有所不同，评价最高的是网络服务提供者从事网络安全相关工作的从业人员，有 49.55%的人员认为良好，其次是政府网络安全监督管理部门的从业人员，有 45.57%的人员认为良好。对当前网络安全状况最担心的是科研机构、大学的从业人员，只有 26.04%的人员认为良好，而网络安全产品、服务提供者的从业人员有 30.74%的人员选择良好，也比较担心当前的网络安全状况。不同行业岗位的从业人员安全感评价对比如图 2-6 所示，其中良好包括非常安全/安全，堪忧包括不安全/非常不安全。

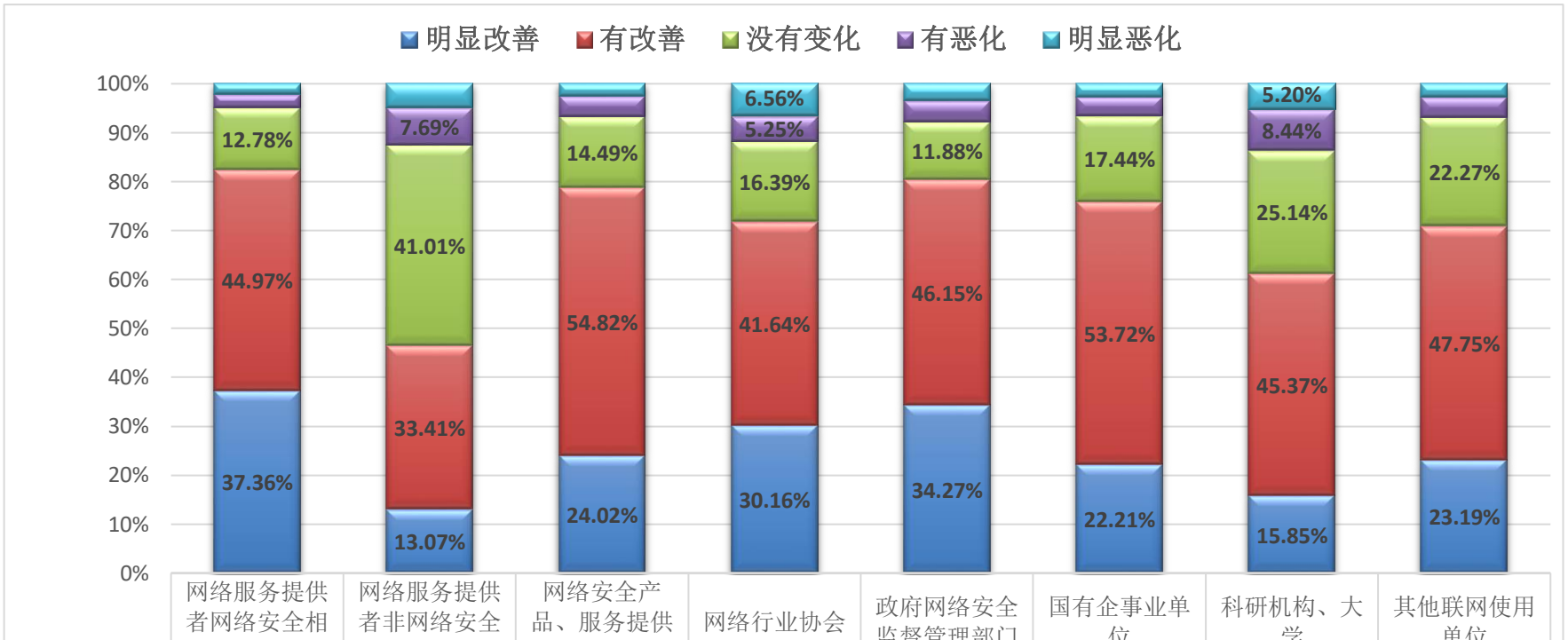


	网络服务提供者网络安全相关工作	网络服务提供者非网络安全相关工作	网络安全产品、服务提供者	网络行业协会	政府网络安全监督管理部门	国有企事业单位	科研机构、大学	其他联网使用单位
堪忧	11.44%	17.16%	20.62%	15.85%	13.92%	15.79%	22.60%	10.79%
一般	39.01%	38.06%	48.64%	41.20%	40.51%	47.29%	51.35%	44.25%
良好	49.55%	44.78%	30.74%	42.95%	45.57%	36.92%	26.04%	44.96%

图2-6：不同行业岗位从业人员网络安全感评价比较

不同行业岗位的从业人员对网络安全感变化的评价也有所不同，评价最高的是网络服务提供者从事网络安全相关工作的从业人员，共有 82.33%的人员认为网络安全状况改善，其次是政府网络安全监督管理部门的从业人员，共有 80.42%的人员认为网络安全状况改善。对网络安全感变化认为改善最少的是网络服务提供者从事非网络安全相关工作的从业人员，只有 46.48%的

人员认为改善了。不同行业岗位的从业人员网络安全感变化的评价对比如图 2-7 所示，其中明显改善包括明显提升、有改善包括有提升、有恶化包括有下降、明显恶化包括明显下降。



	网络服务提供者网络安全相关工作	网络服务提供者非网络安全相关工作	网络安全产品、服务提供者	网络行业协会	政府网络安全监督管理部门	国有企事业单位	科研机构、大学	其他联网使用单位
明显恶化	2.14%	4.82%	2.51%	6.56%	3.41%	2.63%	5.20%	2.74%
有恶化	2.75%	7.69%	4.16%	5.25%	4.28%	4.01%	8.44%	4.05%
没有变化	12.78%	41.01%	14.49%	16.39%	11.88%	17.44%	25.14%	22.27%
有改善	44.97%	33.41%	54.82%	41.64%	46.15%	53.72%	45.37%	47.75%
明显改善	37.36%	13.07%	24.02%	30.16%	34.27%	22.21%	15.85%	23.19%

图2-7：不同行业岗位从业人员对网络安全感变化的评价比较

3. 主要发现

主要发现是针对各类从业人员答卷中有代表性的共性内容进行综合分析的结论。

3.1、亟待加强的网络安全立法内容

公民个人信息保护是从业人员认为最迫切的网络安全立法内容，其次是网络平台责任，第三是数据安全保护。不同行业岗位从业人员网络安全立法需求综合分析如图 2-8 所示。从图中可以看出各类从业人员对需要加强的立法内容认识比较统一，顺序也基本一致。

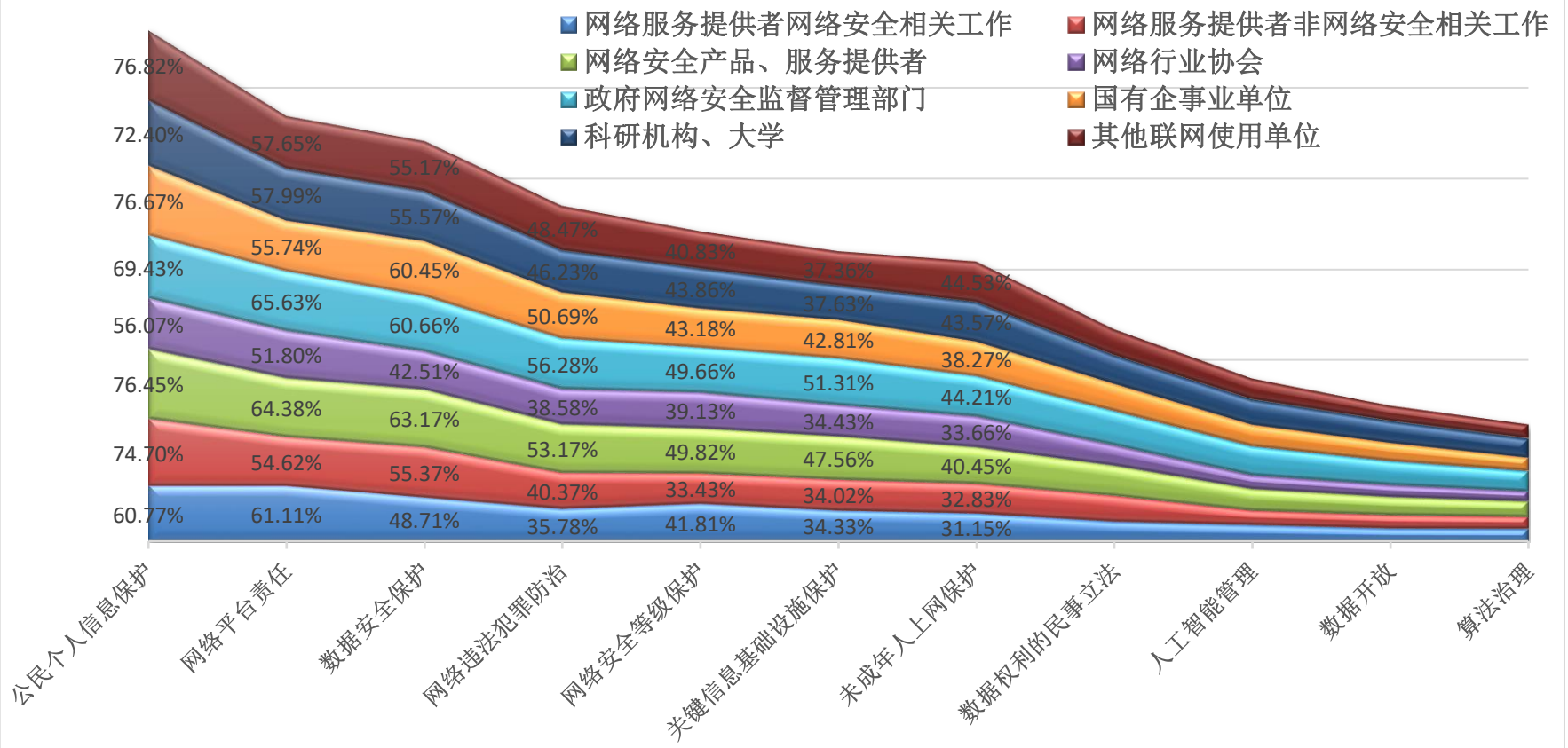


图2-8：不同行业岗位从业人员网络安全立法需求

3.2、网络安全最突出的问题

个人信息泄露是从业人员认为网络安全最突出的问题，其次是网络诈骗，第三是网络攻击。不同行业岗位从业人员网络安全突出问题认识的综合分析如图 2-9 所示。从图中可以明显看出，国有企事业单位和其他联网使用单位的从业人员除了对个人信息泄露外，对其他所有问题都没有太多的选择，认为网络安全突出问题较少。

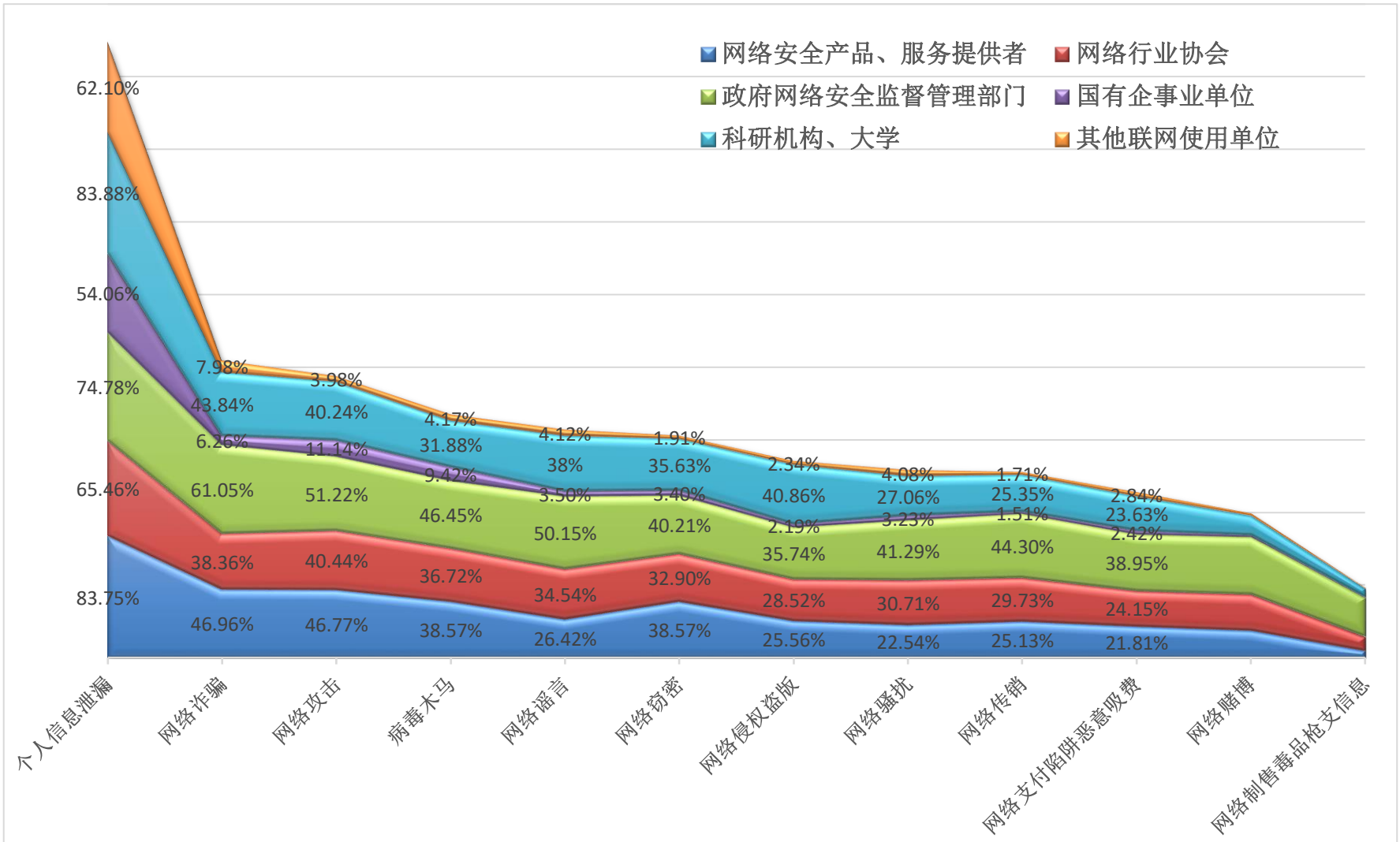


图2-9：不同行业岗位从业人员网络安全突出问题认识

3.3、对网络安全执法部门的认识

网信是从业人员首选的网络安全执法部门，其次是公安。不同行业岗位从业人员对执法部门的认识如图 2-10 所示，可以看出各类从业人员对执法部门认识较统一，顺序也基本一致。

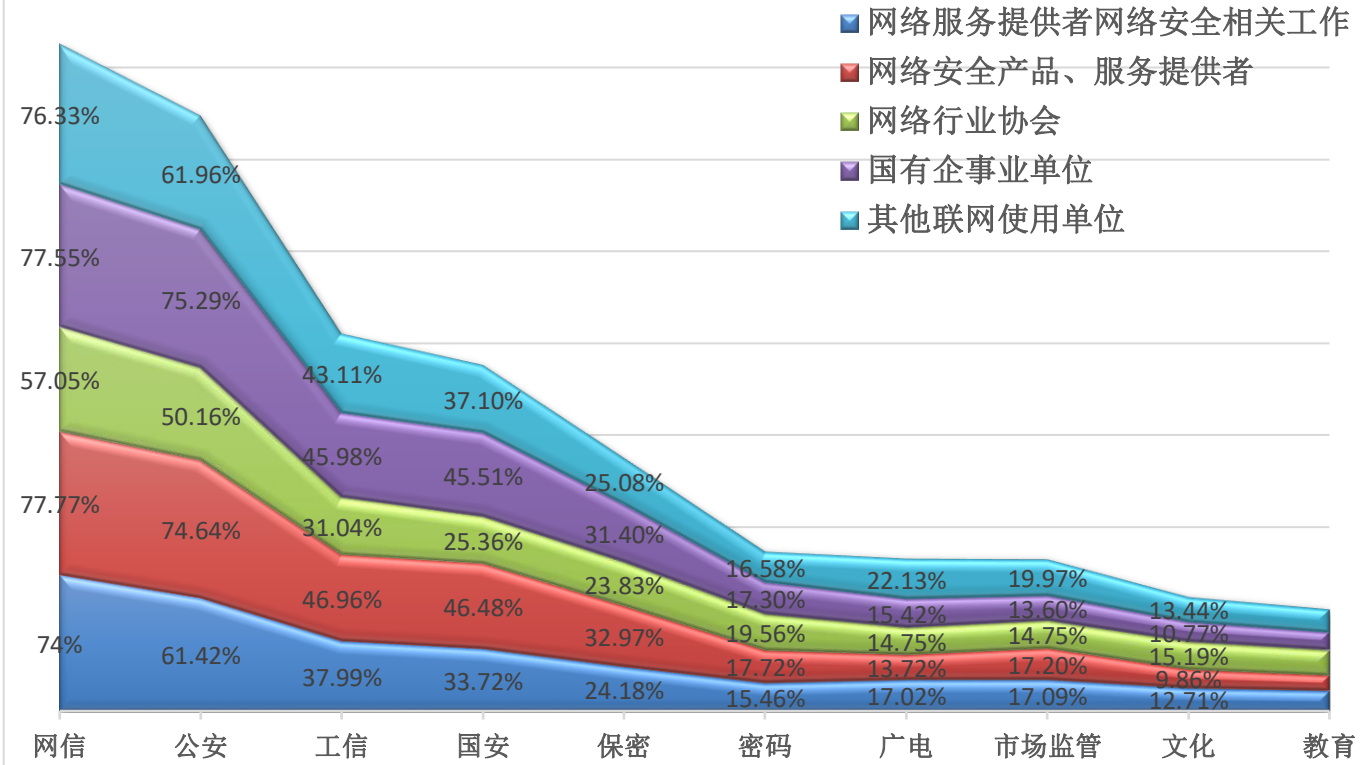


图2-10：不同行业岗位从业人员对网络安全执法部门的认识

3.4、对网络安全执法制约因素的认识

取证能力是从业人员认为网络安全执法的最大制约因素。不同行业岗位从业人员对执法制约因素的认识如图 2-11 所示，可以看出取证能力、检测能力、人员及法律素质这四项的选择比例非常接近，都是从业人员认为制约执法的重要因素。

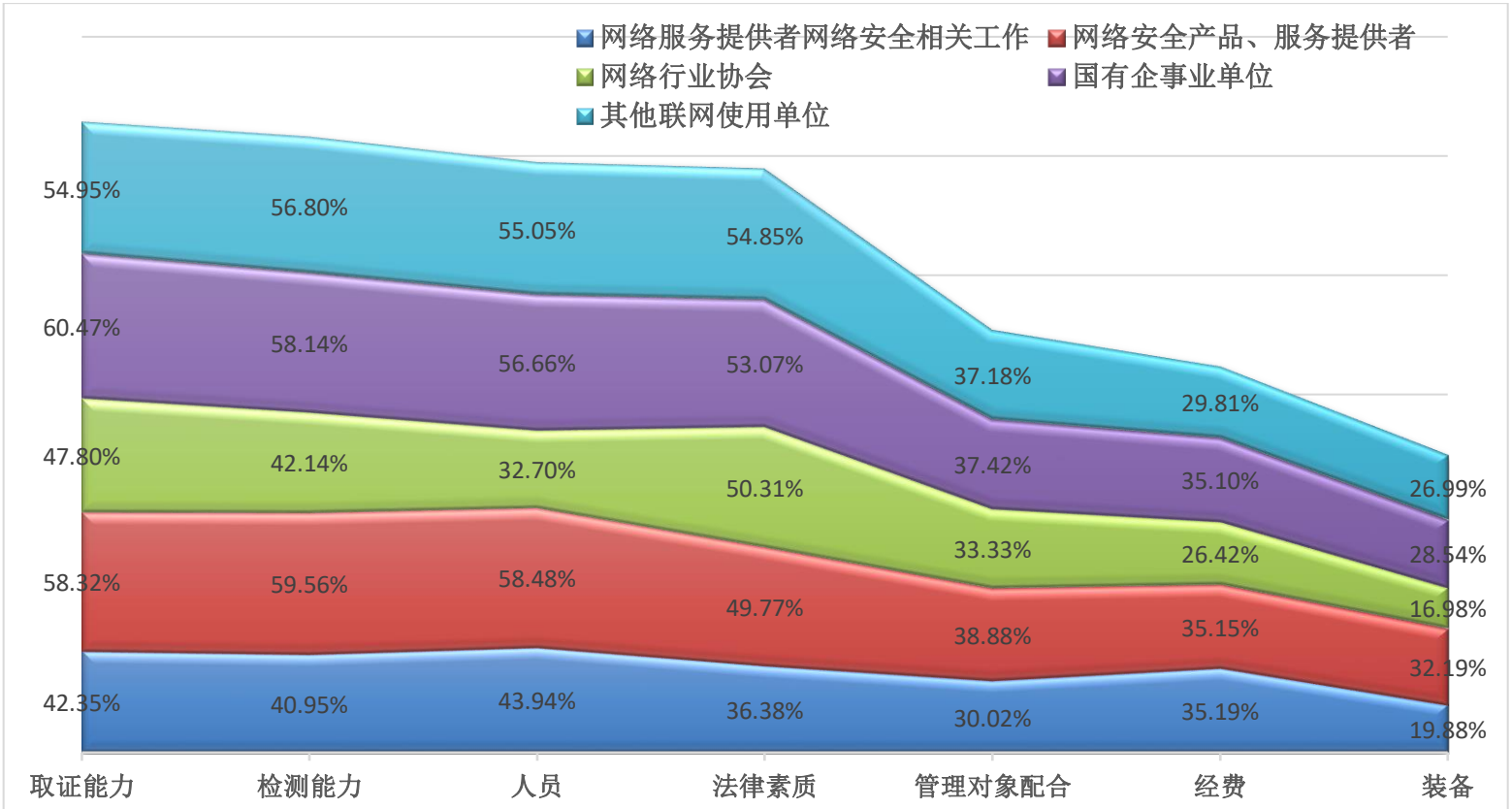
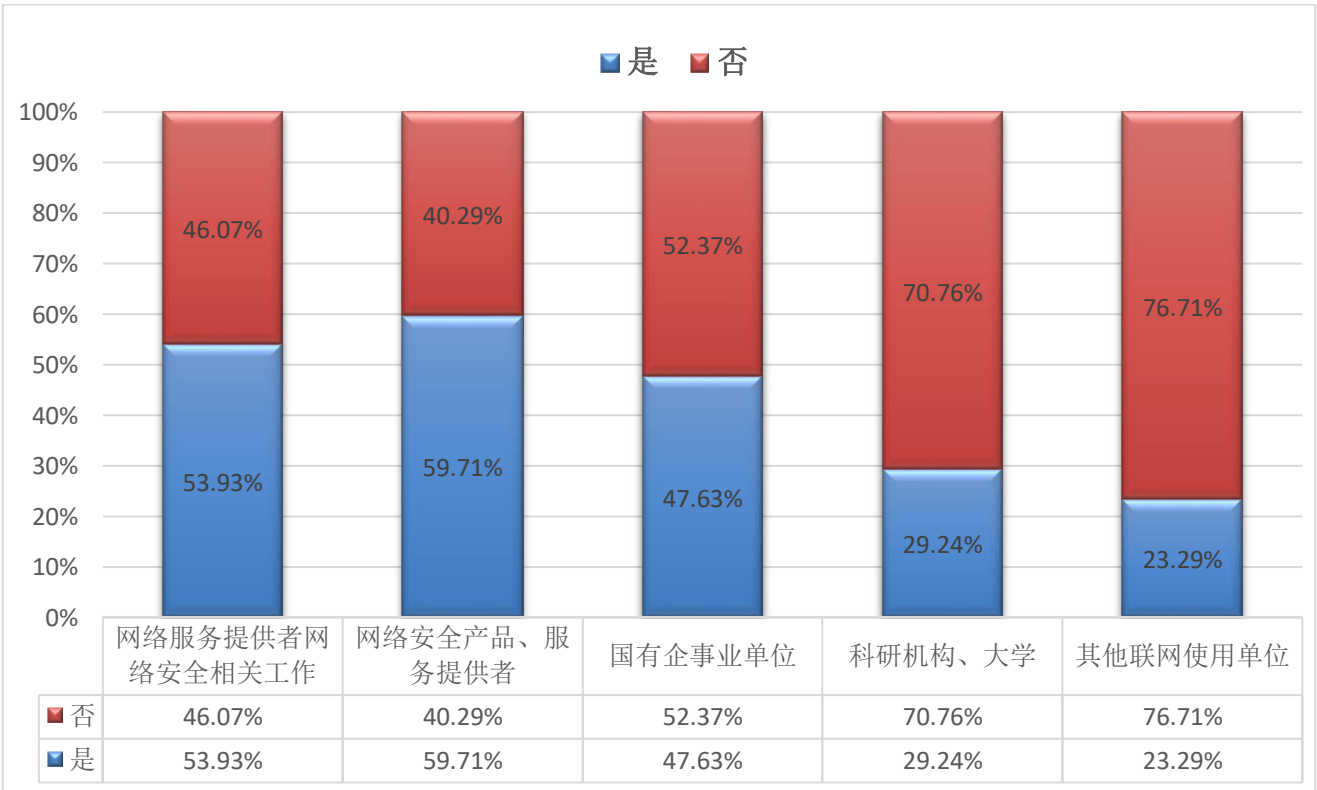


图2-11：不同行业岗位从业人员对执法制约因素的认识

3.5、对等级保护 2.0 国家标准的认识参差不齐

其他联网使用单位的从业人员对等级保护 2.0 国家标准的认识程度最低，仅有 23.29%的人员了解，科研机构、大学的从业人员也只有 29.24%的人了解，其他从业人员了解的较多。不同行业岗位从业人员对等保 2.0 的认识如图 2-12 所示，可以看出各类从业人员对等保 2.0 的认识参差不齐。

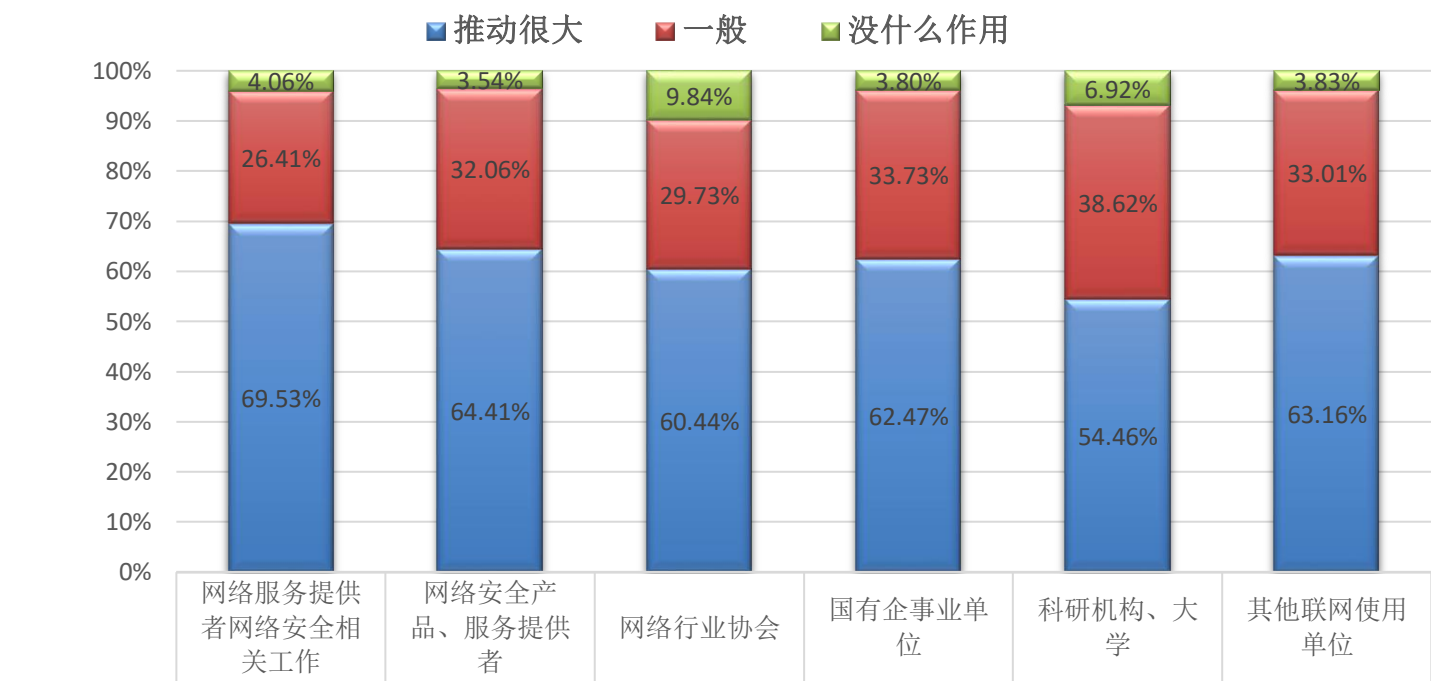


	网络服务提供者网络安全相关工作	网络安全产品、服务提供者	国有企事业单位	科研机构、大学	其他联网使用单位
否	46.07%	40.29%	52.37%	70.76%	76.71%
是	53.93%	59.71%	47.63%	29.24%	23.29%

图2-12：不同行业岗位从业人员对等保2.0的认识

3.6、对等级保护的积极作用的认可

等级保护的积极作用已经得到从业人员的广泛认可，不同行业岗位从业人员对等保作用的认可度如图 2-13 所示，可以看出各类从业人员认为等级保护作用很大的均已超过 50%，认为没有作用的都不超过 10%。

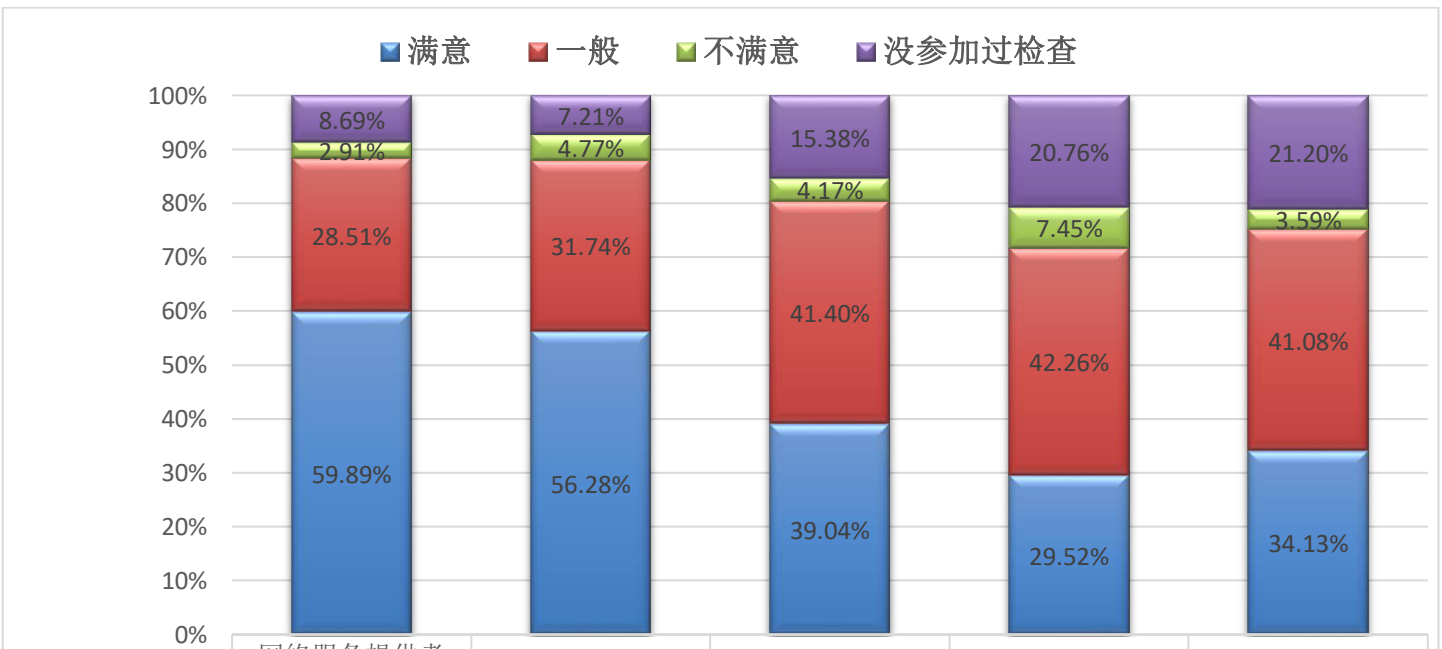


	网络服务提供者网络安全相关工作	网络安全产品、服务提供者	网络行业协会	国有企事业单位	科研机构、大学	其他联网使用单位
没什么作用	4.06%	3.54%	9.84%	3.80%	6.92%	3.83%
一般	26.41%	32.06%	29.73%	33.73%	38.62%	33.01%
推动很大	69.53%	64.41%	60.44%	62.47%	54.46%	63.16%

图2-13：不同行业岗位从业人员对等保作用的认可情况

3.7、对公安机关网络安全执法检查工作的评价

网络服务提供者网络安全相关工作及政府网络安全监督管理部门对公安机关执法工作的评价较高，而科研机构、大学对公安机关执法工作的评价较低，各类从业人员对公安机关网络安全执法工作的评价如图 2-14 所示，可以看出不同岗位从业人员的评价有所区别。

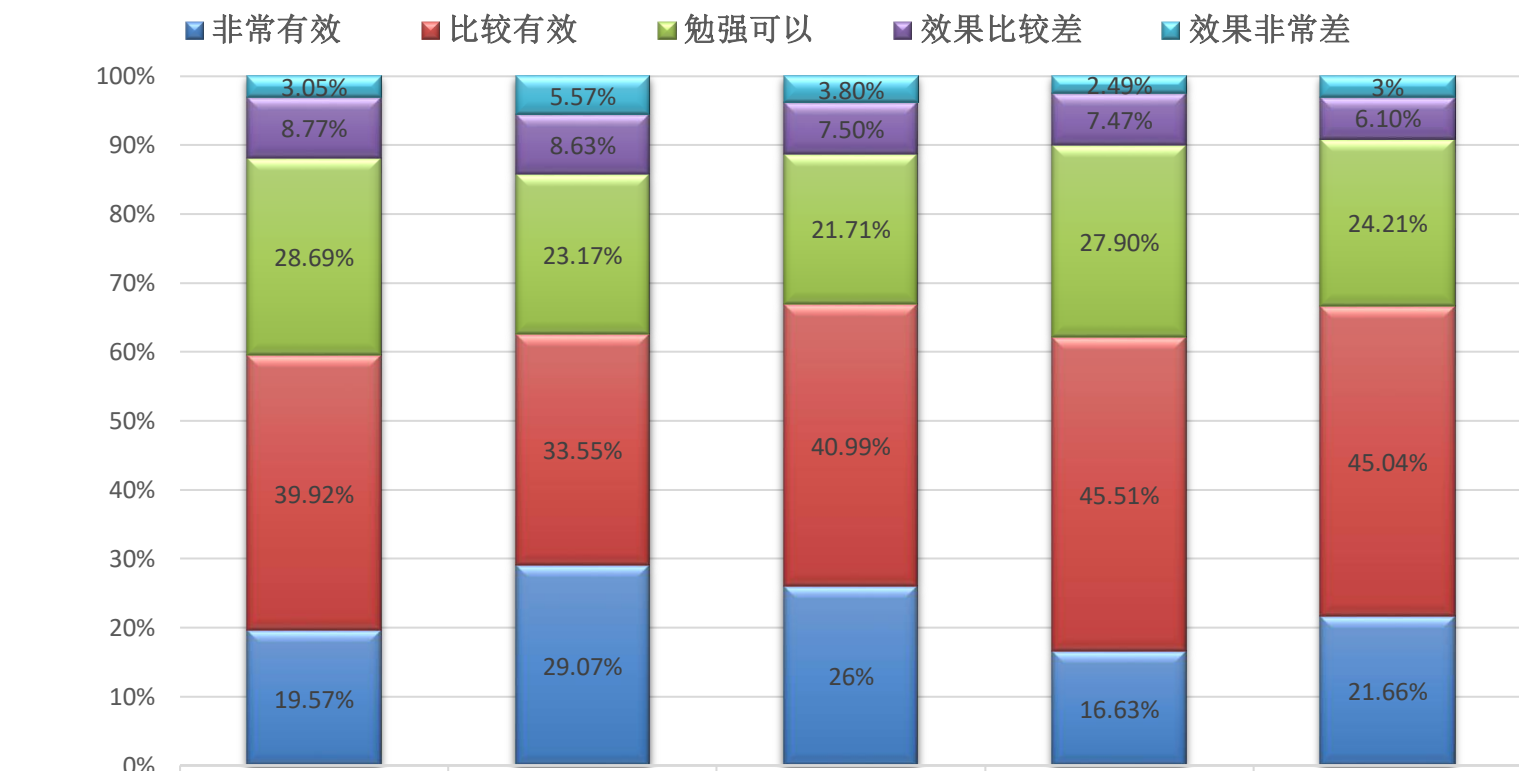


	网络服务提供者网络安全相关工作	政府网络安全监督管理部门	国有企事业单位	科研机构、大学	其他联网使用单位
没参加过检查	8.69%	7.21%	15.38%	20.76%	21.20%
不满意	2.91%	4.77%	4.17%	7.45%	3.59%
一般	28.51%	31.74%	41.40%	42.26%	41.08%
满意	59.89%	56.28%	39.04%	29.52%	34.13%

图2-14：不同行业岗位从业人员对公安机关执法工作的评价

3.8、网络服务提供者的管理措施对于保证网络安全是有效的

从业人员对网络服务提供者的管理措施对于保证网络安全的作用是肯定的，不同行业岗位的从业人员的认可情况如图 2-15 所示，可以看出各类从业人员选择比较有效和非常有效的基本都超过 60%，而选择比较差和非常差的都不超过 15%。



	网络安全产品、服务提供者	网络行业协会	政府网络安全监督管理部门	国有企事业单位	其他联网使用单位
效果非常差	3.05%	5.57%	3.80%	2.49%	3%
效果比较差	8.77%	8.63%	7.50%	7.47%	6.10%
勉强可以	28.69%	23.17%	21.71%	27.90%	24.21%
比较有效	39.92%	33.55%	40.99%	45.51%	45.04%
非常有效	19.57%	29.07%	26%	16.63%	21.66%

图2-15：不同行业岗位从业人员对网络服务提供者管理措施的认可情况

三、A 卷：网络服务提供者网络安全相关工作的从业人员

网络服务提供者网络安全相关工作（A 类）的从业人员对网络安全业务比较熟悉，对业界的安全状况的实际情况比较了解。

A 类问卷有效答卷数量 4430 份，以下是 A 类问卷各项数据的详细统计结果。

A3. 当前网络安全状况

受调查的 A 类从业人员中有 49.55%的评价是状况良好，几乎占到一半（如图 3-1）。

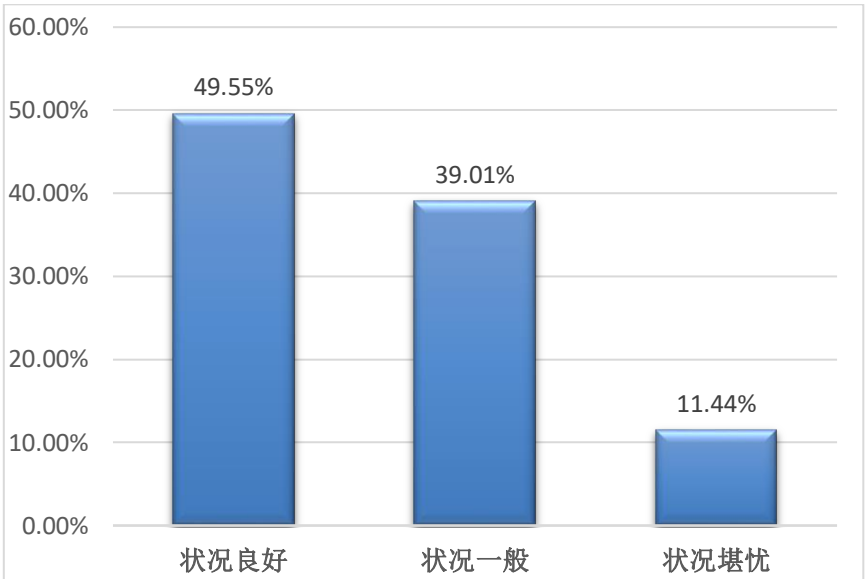


图3-1：安全状况评价

A3.1、与去年相比网络安全感的变化

绝大部分受调查的 A 类从业人员认为当前网络安全状况改善，37.36%的从业人员认为明显改善，44.97%认为有改善，两者合计共有 82.33%的 A 类从业人员认为网络安全状况改善了（如图 3-2）。

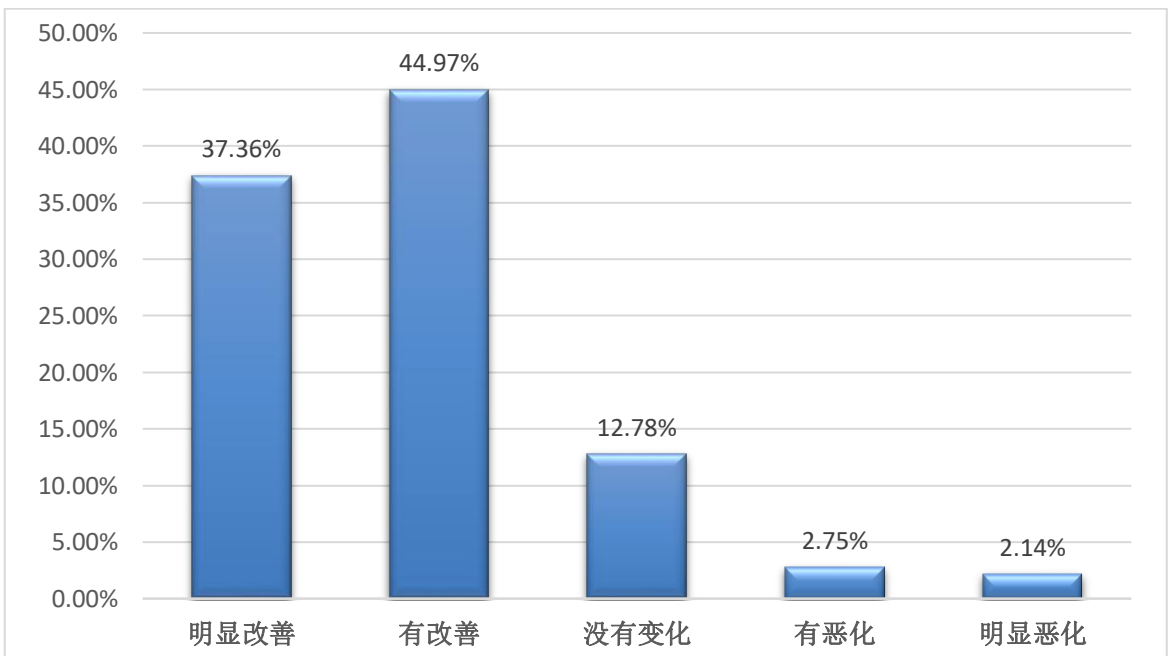


图3-2：网络安全感变化评价

A4. A 类从业人员所从事的网络服务类型

受调查的 A 类从业人员所在单位提供的服务覆盖面广，所有统计选项中的服务门类都有样本数据分布。提供的网络服务最多的依次是基础行业服务 20.99%、网络音视频 20.65%、网络新闻 19.71%、数据中心服务 18.35%，各类服务所占比例如图 3-3 所示。

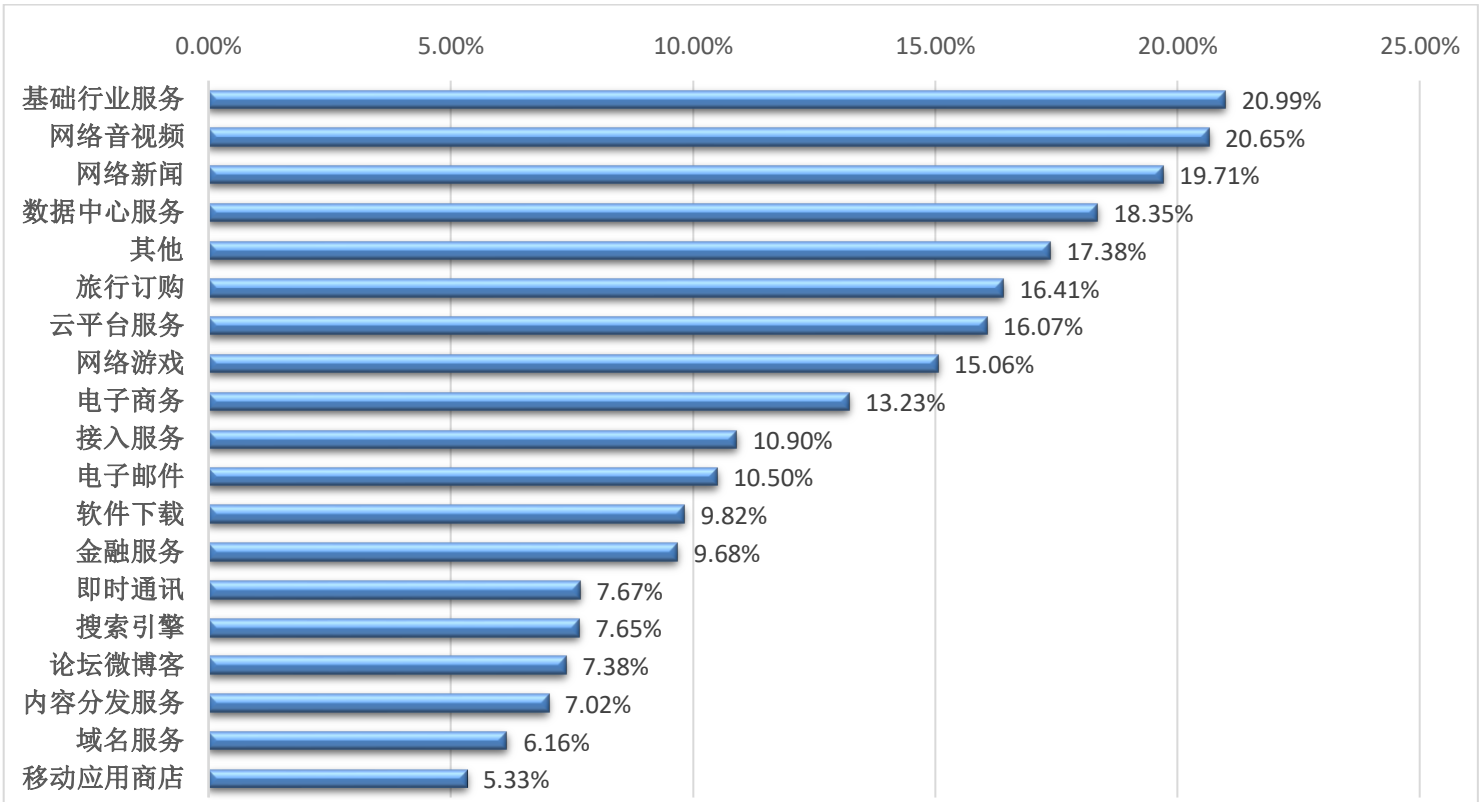


图3-3：网络服务类型

A5. 网络安全状况对网络服务提供者经营的影响

受调查的 A 类从业人员对网络安全的负面影响认识比较深刻，认为会造成直接经济损失（64.74%）、损害形象及声誉（50.86%）、会被处罚（38.19%）排前三位（如图 3-4）。

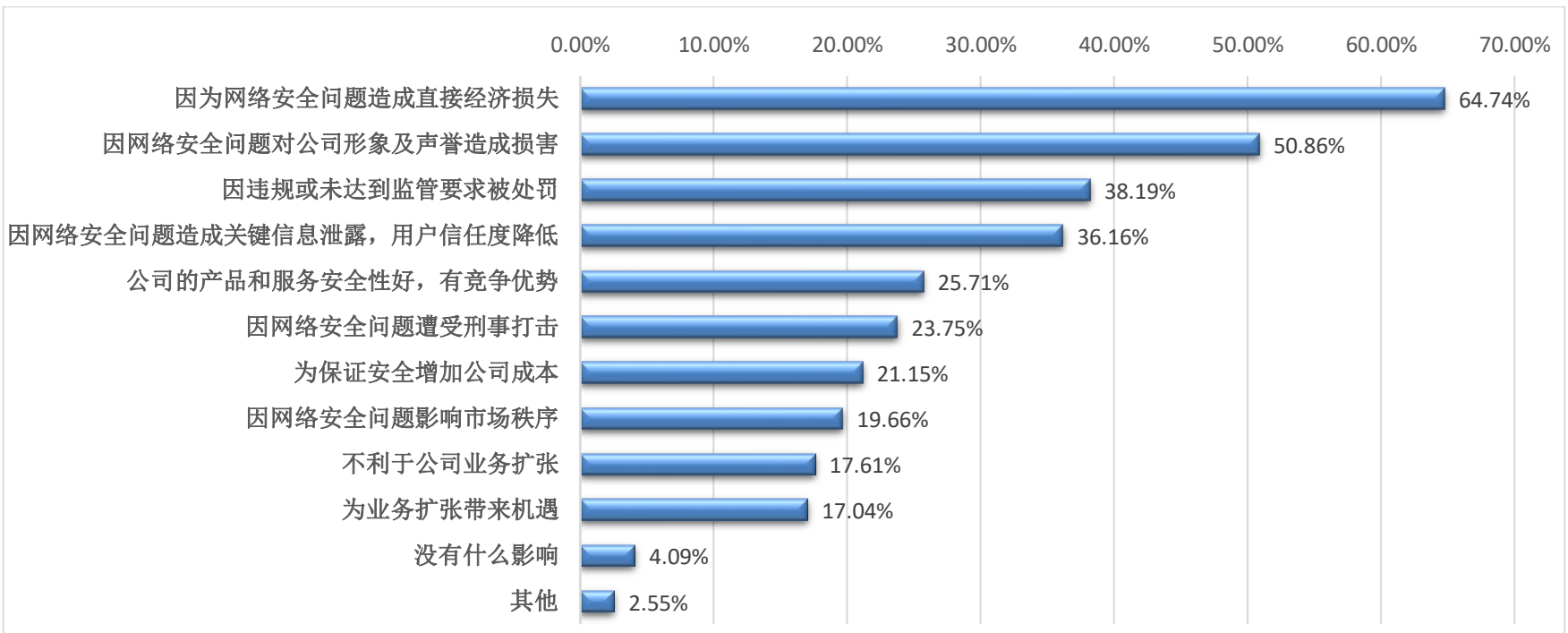


图3.4：网络安全状况对经营的影响

A6. 网络服务提供者经常遭遇的网络安全问题

受调查的 A 类从业人员认为，网络服务提供者遇到的网络安全问题最多依次是个人信息或单位信息泄露占 64.06%，网站被篡改占 59.46%，病毒木马 58.24%（如图 3-5）。

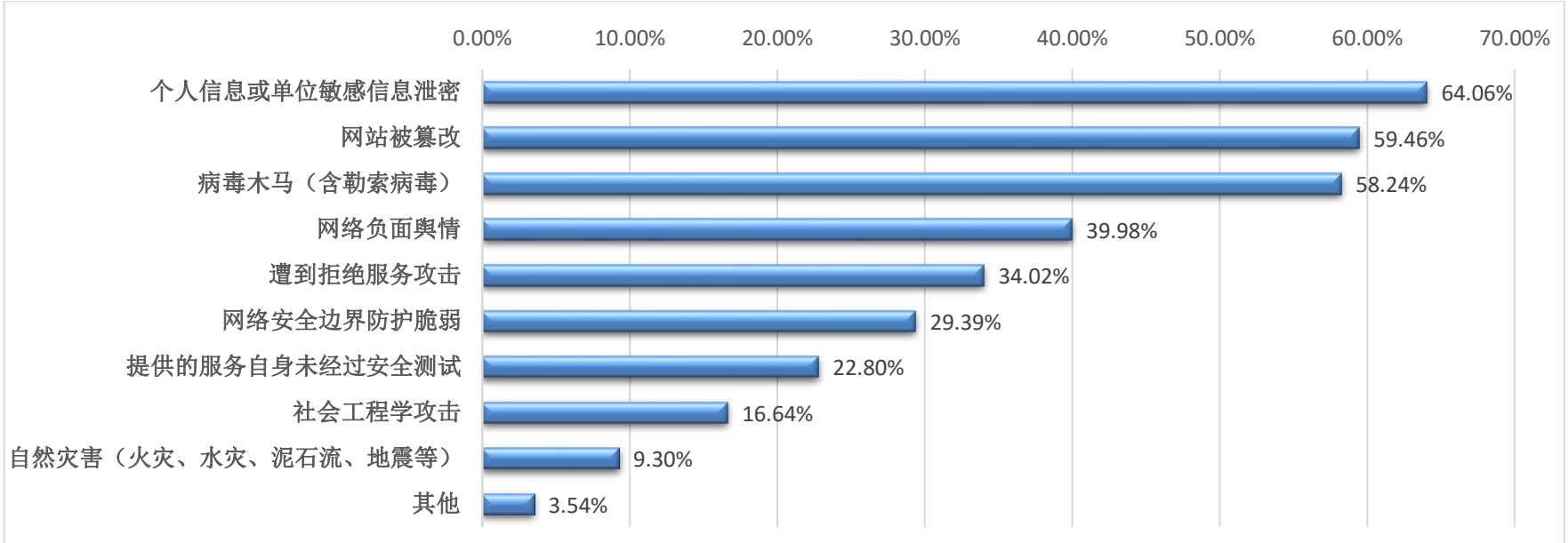


图3-5：常见的网络安全问题

A7. 互联网服务提供者处理网络安全问题时的困难

受调查的 A 类从业人员认为资金投入、领导支持、技术措施等是处理网络安全问题时面临的主要困难，46.03%的从业人员认为需要大量资金投入，45.94%的从业人员认为公司高层不够重视，44.94%的从业人员认为技术措施不够完善（如图 3-6）。

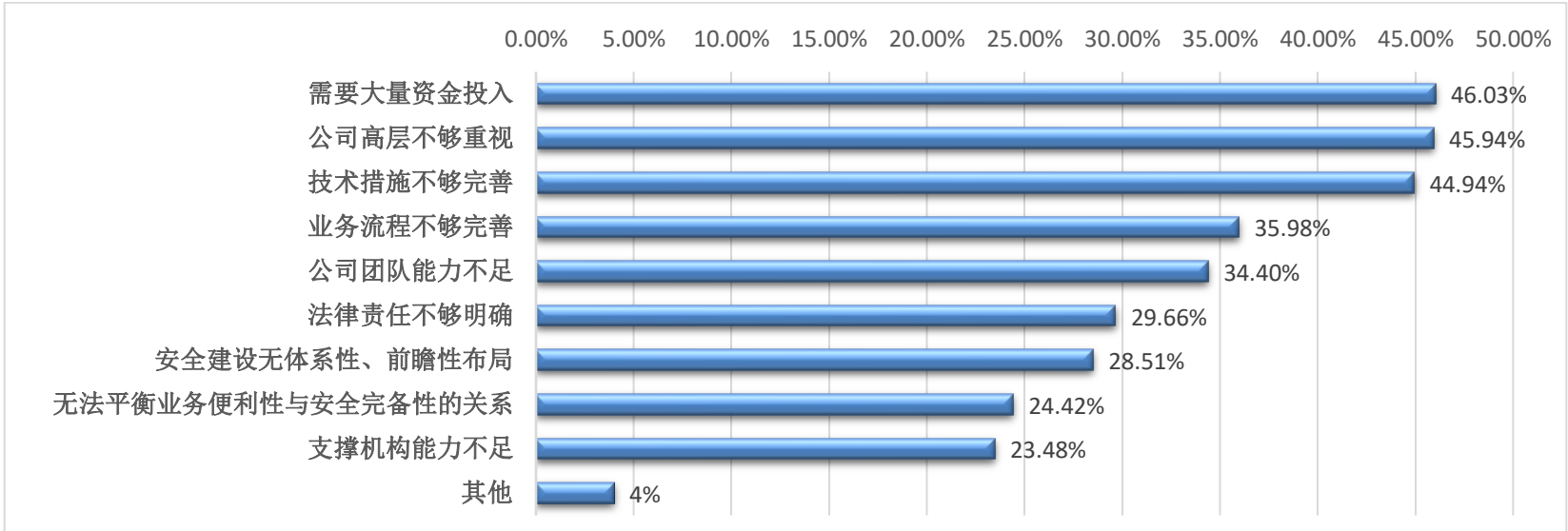


图3-6：处理网络安全问题常见困难

A8. 政府部门提供的网络安全服务形式

受调查的 A 类从业人员认为政府部门提供的网络安全服务主要是知识普及（67.95%）、教育培训（46.57%）、监督检查（45.89%），如图 3-7 所示。

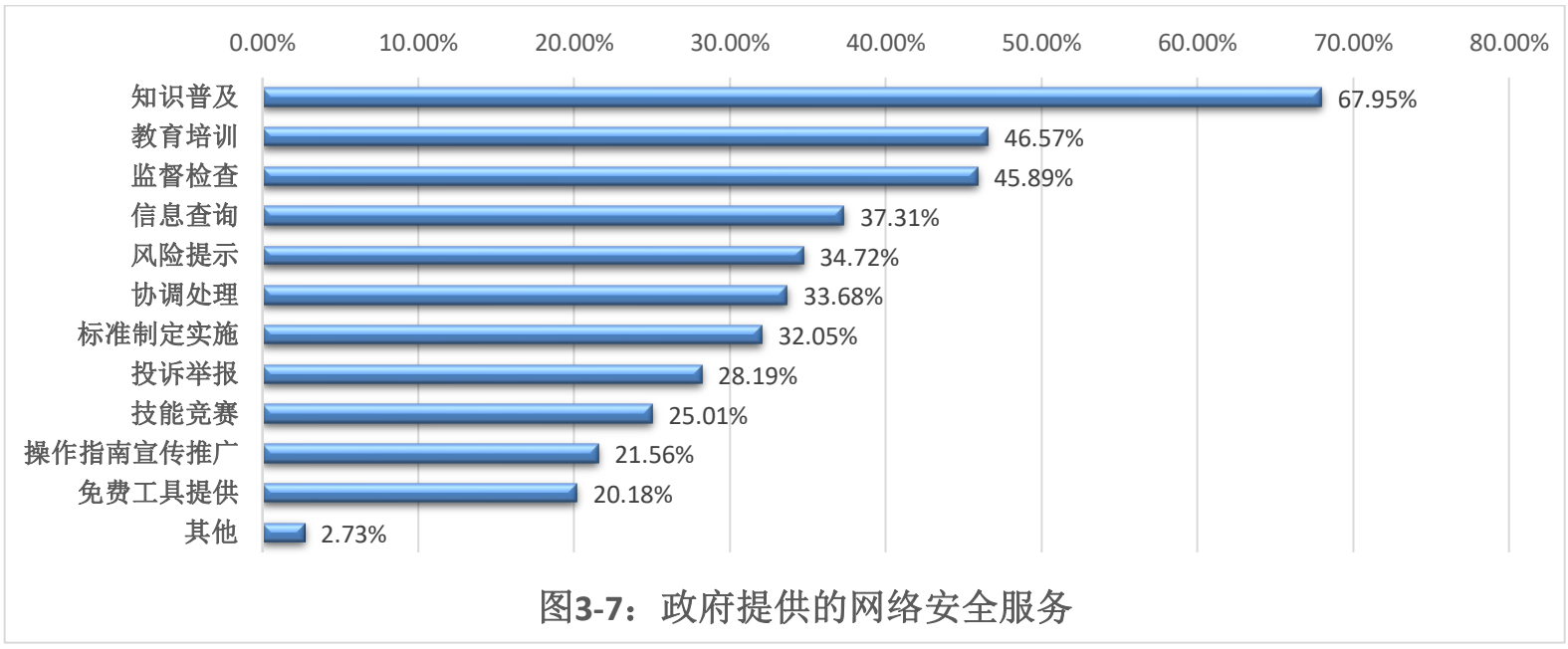


图3-7：政府提供的网络安全服务

A9. 国家网络安全管理对单位运营的作用

国家有关网络安全的管理对单位运营的作用，A 类从业人员有 76.79%认为是提高了网络安全意识，56.32%的人认为强化了网络安全措施，51.31%的人认为改进了网络安全制度，完善组织管理体系、降低网络安全风险、提高市场竞争力也都有较多选择（如图 3-8）。

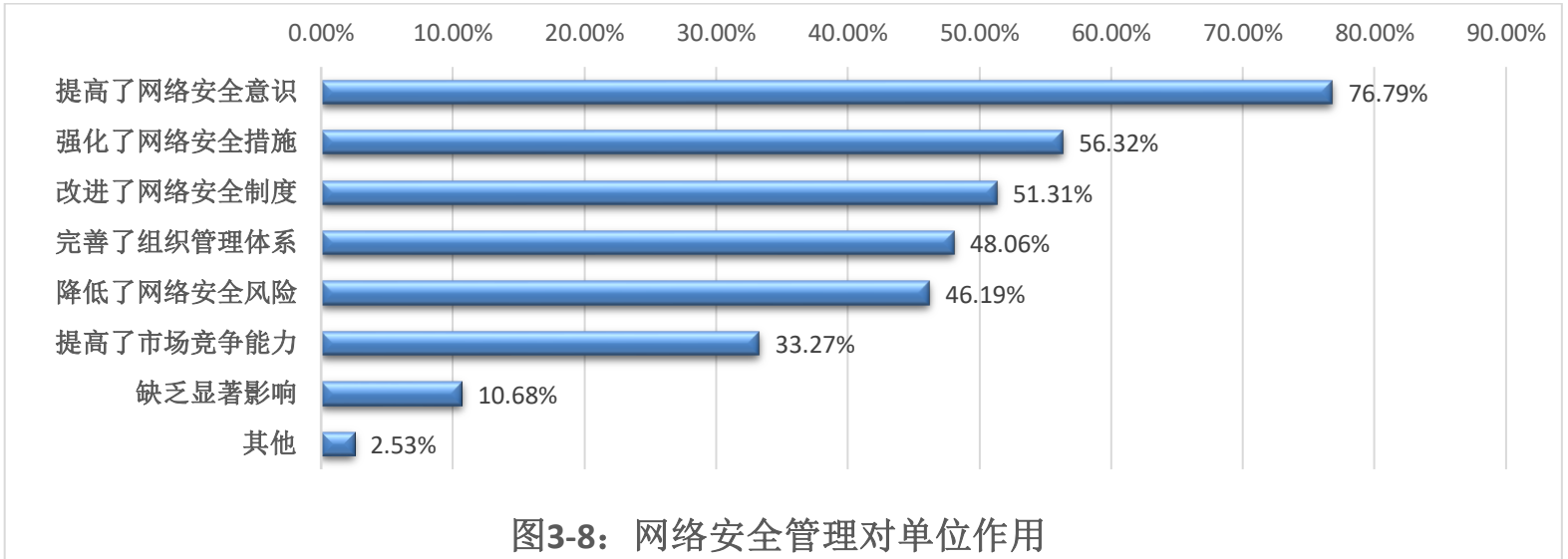


图3-8：网络安全管理对单位作用

A10. 网络安全维护措施

受调查的 A 类从业人员认为维护网络安全加强网络安全法制建设最为重要。有 71.94%的人选择了加强网络安全法制建设。排名第二和第三的分别是强化网络安全监管（59.75%）、提升网络安全问题的发现能力（51.31%），各项措施的选择比例如图 3-9 所示。

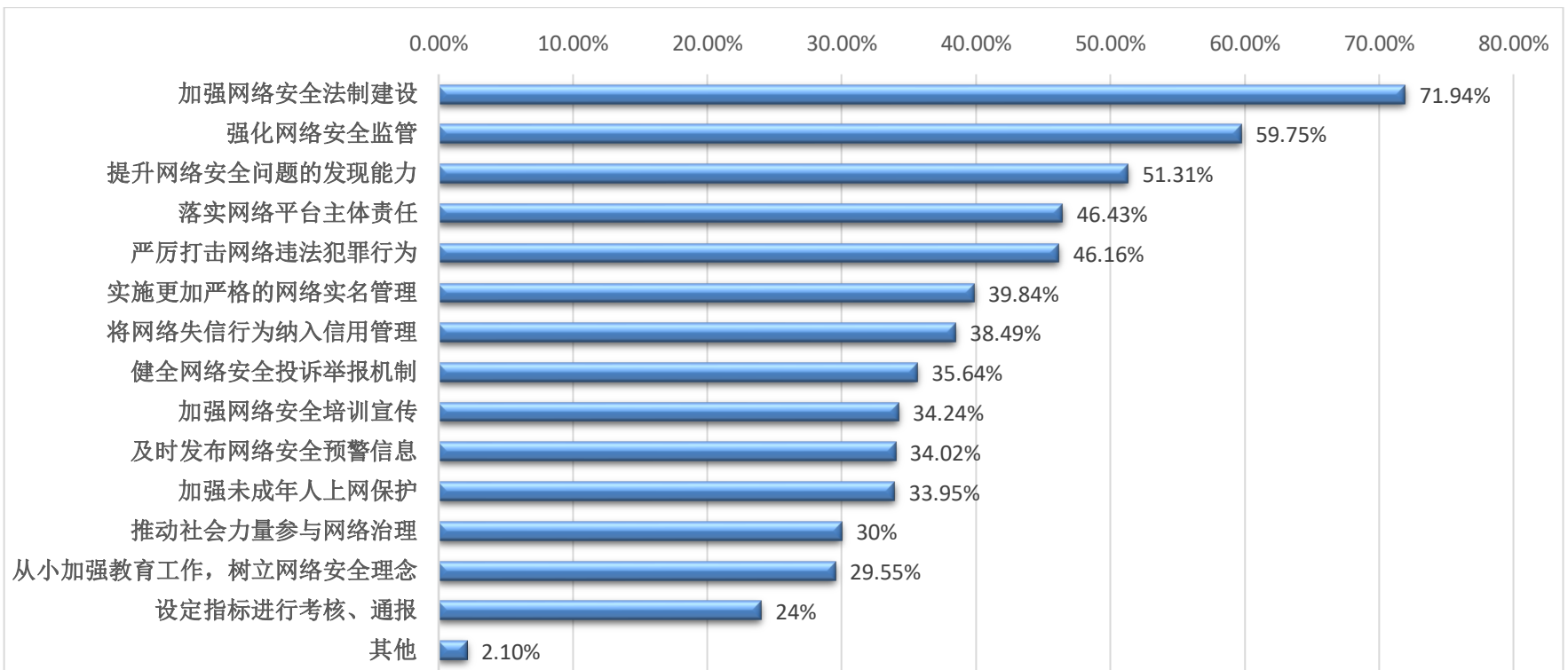


图3-9：网络安全维护措施

A11. 需要重点治理的网络安全问题

受调查的 A 类从业人员认为网络色情（52.62%）、网络赌博（49.19%）、网络诈骗（40.65%）、个人隐私信息泄露（40.29%）、网络敲诈勒索（40.16%）是需要重点治理安全问题的前五位，各类问题占比如图 3-10 所示。

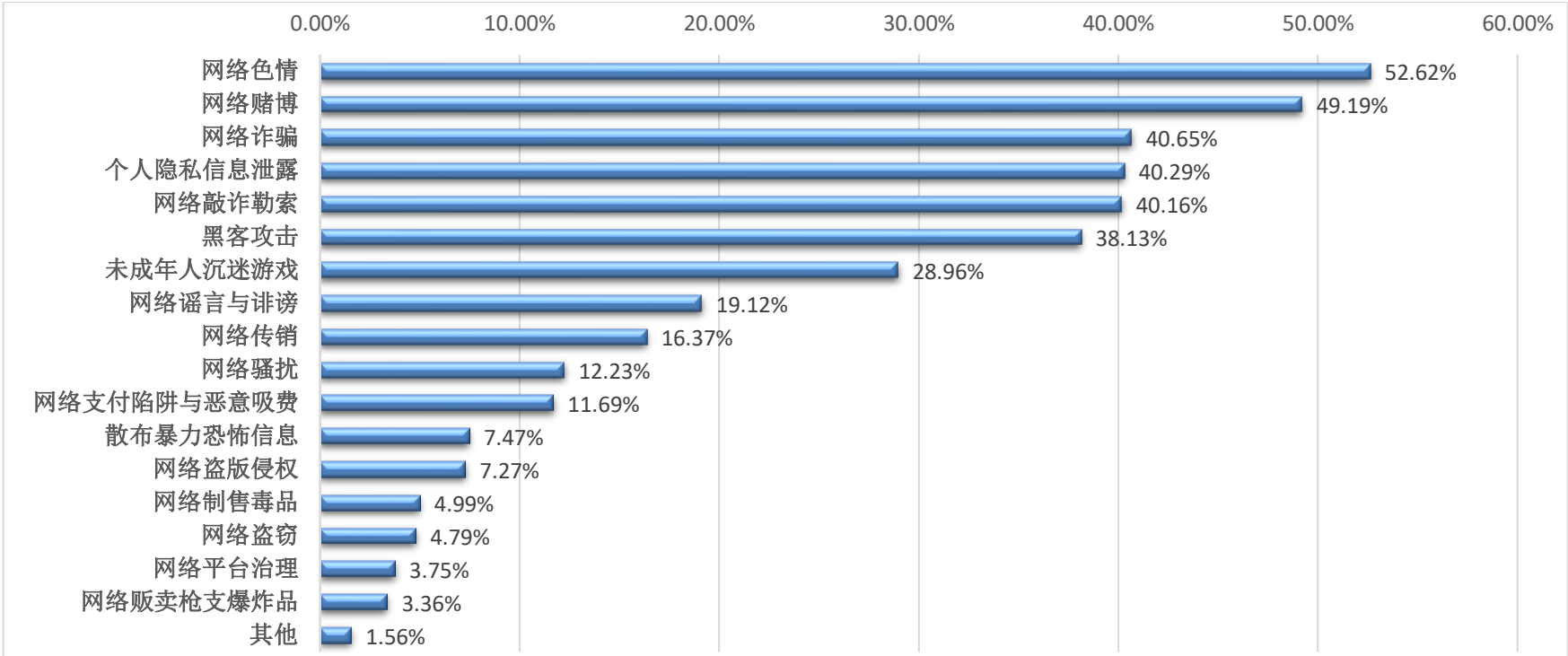


图3-10：需要治理的网络安全问题

A12. 对网络法规的认识

除了《中华人民共和国网络安全法》外，受调查的 A 类从业人员对安全方面的法律有一定的认识，知道比较多的法规分别是《中华人民共和国国家安全法》（69.57%）、《中华人民共和国保守国家秘密法》（39.35%）、《中华人民共和国消费者权益保护法》（35.91%）、《中华人民共和国计算机信息系统安全保护条例》（32.57%），如图 3-11 所示。

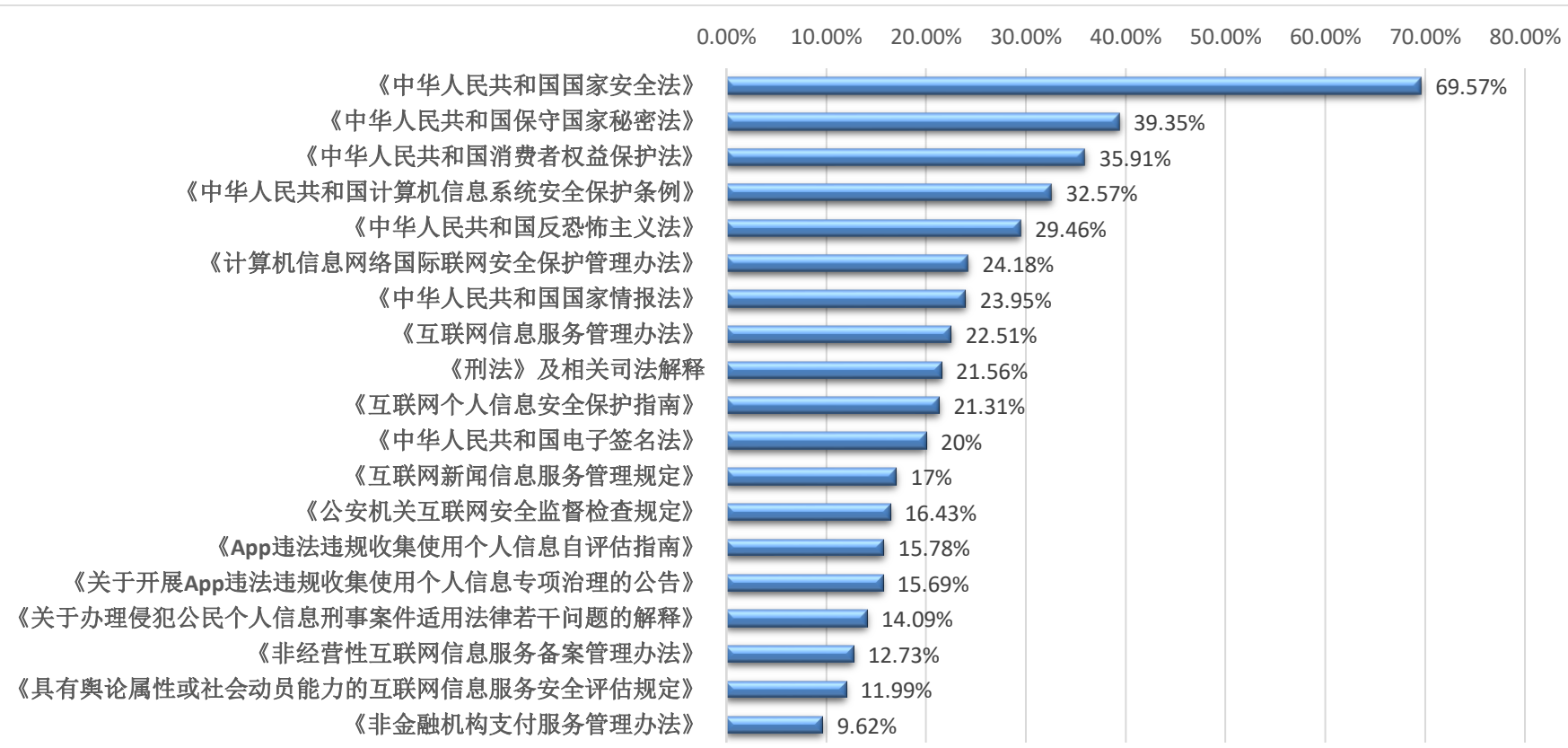


图3-11：对网络法规的认识

A13. 亟待加强的网络安全立法内容

受调查的 A 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：网络平台责任占 61.11%，公民个人信息保护占 60.77%，数据安全保护占 48.71%（如图 3-12）。

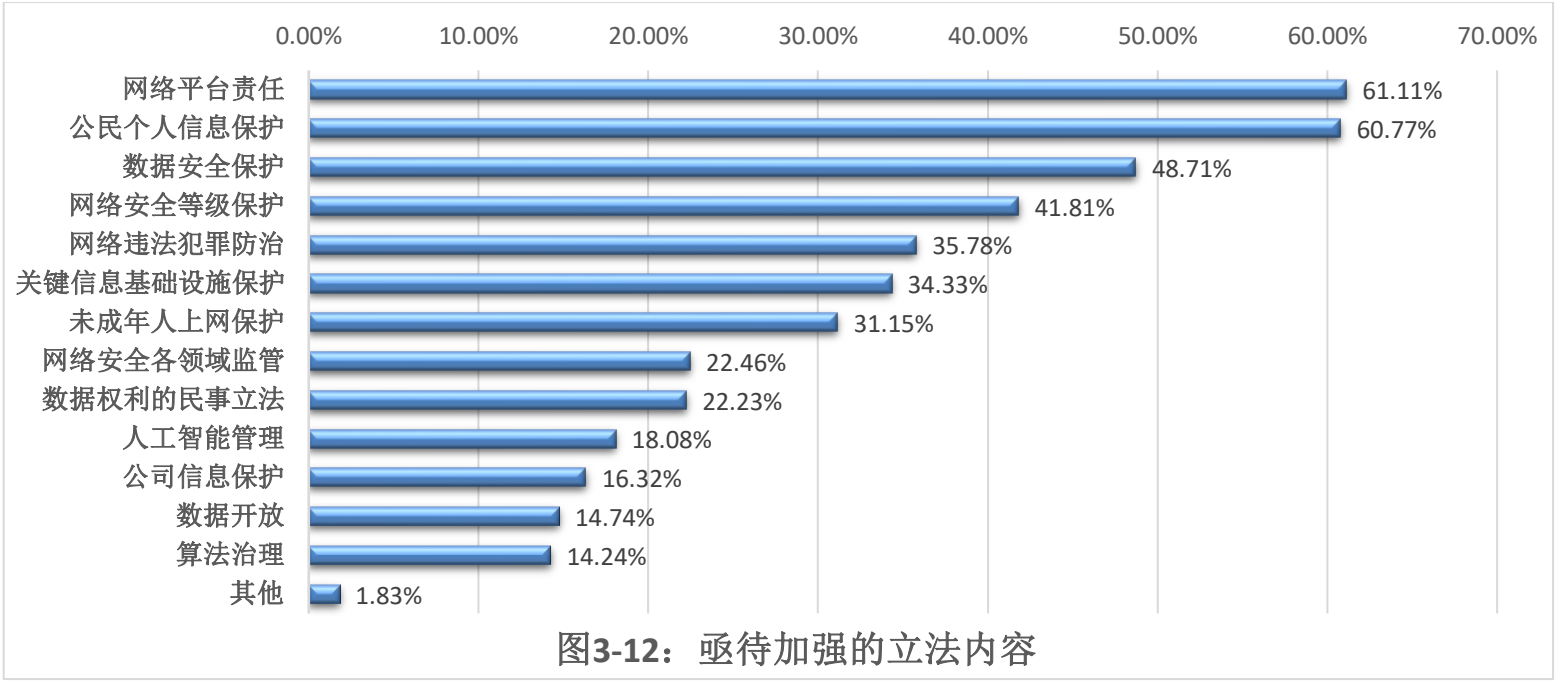


图3-12：亟待加强的立法内容

A14. 对网络安全行政执法部门的认识

受调查的 A 类从业人员认为政府最主要的网络安全执法部门前三位依次是网信（74%）、公安（61.42%）、工信（37.99%），如图 3-13 所示。

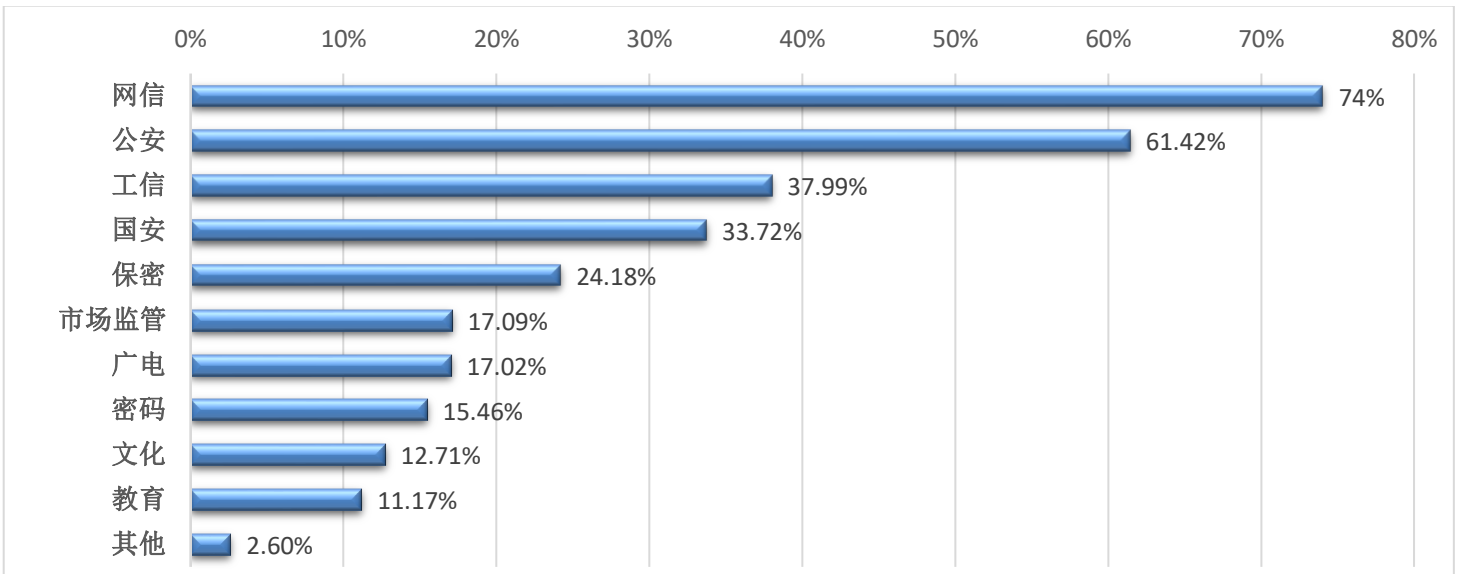


图3-13：政府网络安全执法部门

A14.1、政府部门在网络安全方面的执法力度评价

受调查的 A 类从业人员认为政府部门在网络安全方面的执法力度强的有 28.62%，认为比较强的有 32.3%，两者合计 60.92%；认为不足或严重不足的合计 11.35%（如图 3-14）。

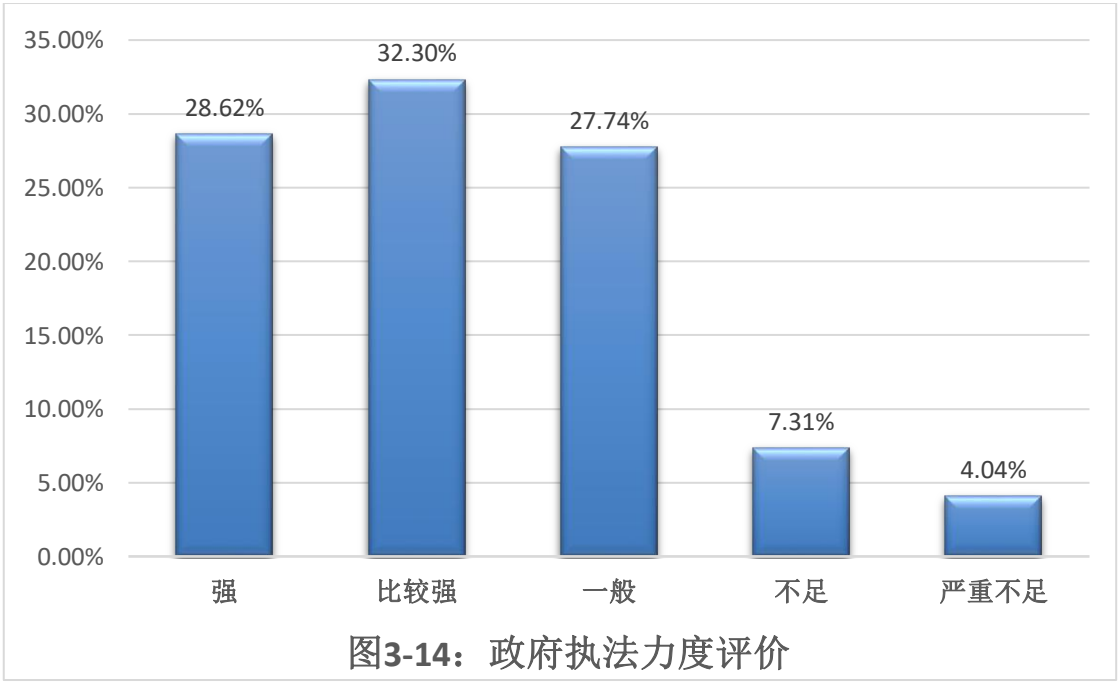


图3-14：政府执法力度评价

A14.2、网络安全执法的制约因素

受调查的 A 类从业人员认为影响网络安全执法的制约因素前三位的是：人员（43.94%）、取证能力（42.35% ）、检测能力（40.95%），各类制约因素占比如图 3-15 所示。

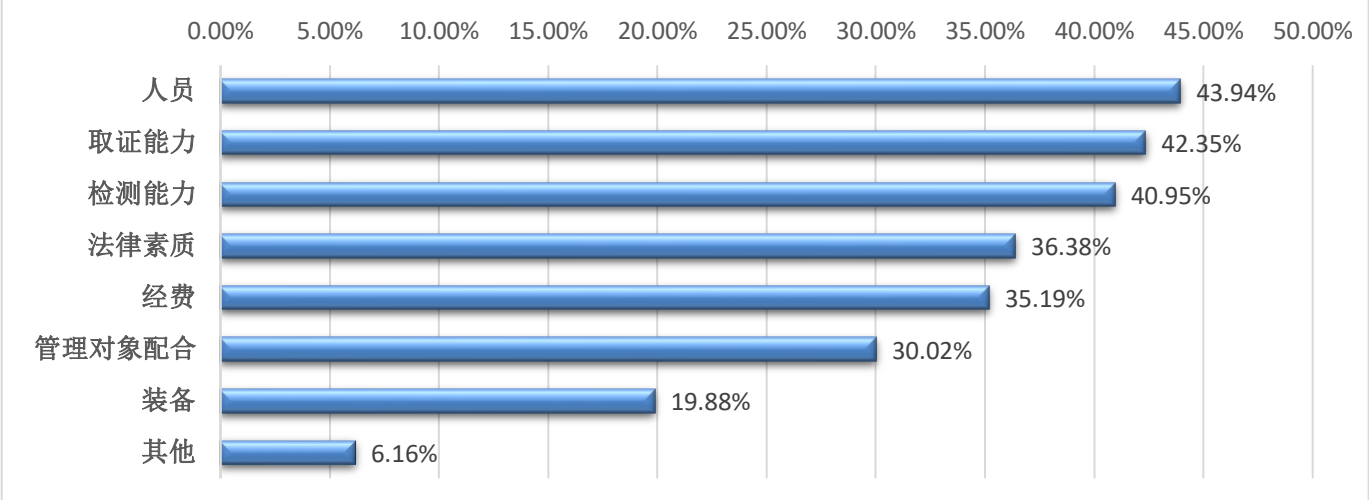


图3-15：网络安全执法的制约因素

A15. 近年来网络数据、账号违法交易等互联网黑灰产业的情况

受调查的 A 类从业人员认为黑灰产业活动大幅增加和有所增加的占比合计 55.85%，其中认为有所增加的有 30.23%，认为大幅增加的有 25.62%（如图 3-16）。

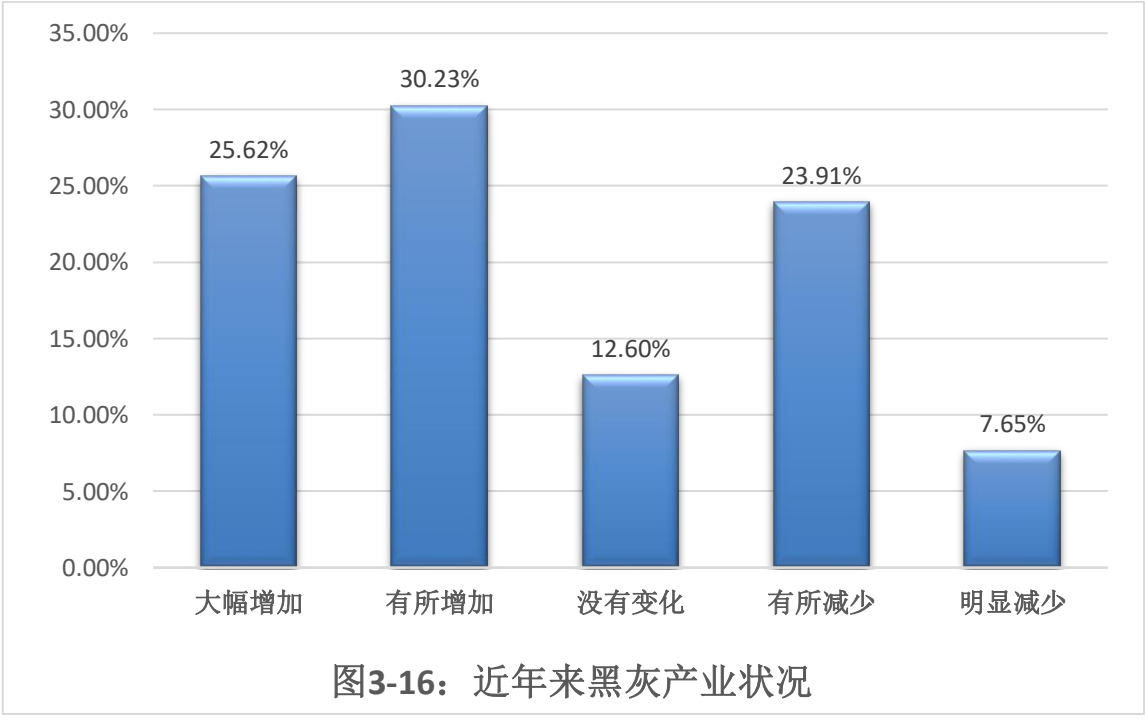


图3-16：近年来黑灰产业状况

A15.1、整治网络黑灰产业链条关键点

受调查的 A 类从业人员中有 40.74%认为治理网络黑灰产业链条最关键的是信息链条（如图 3-17）。

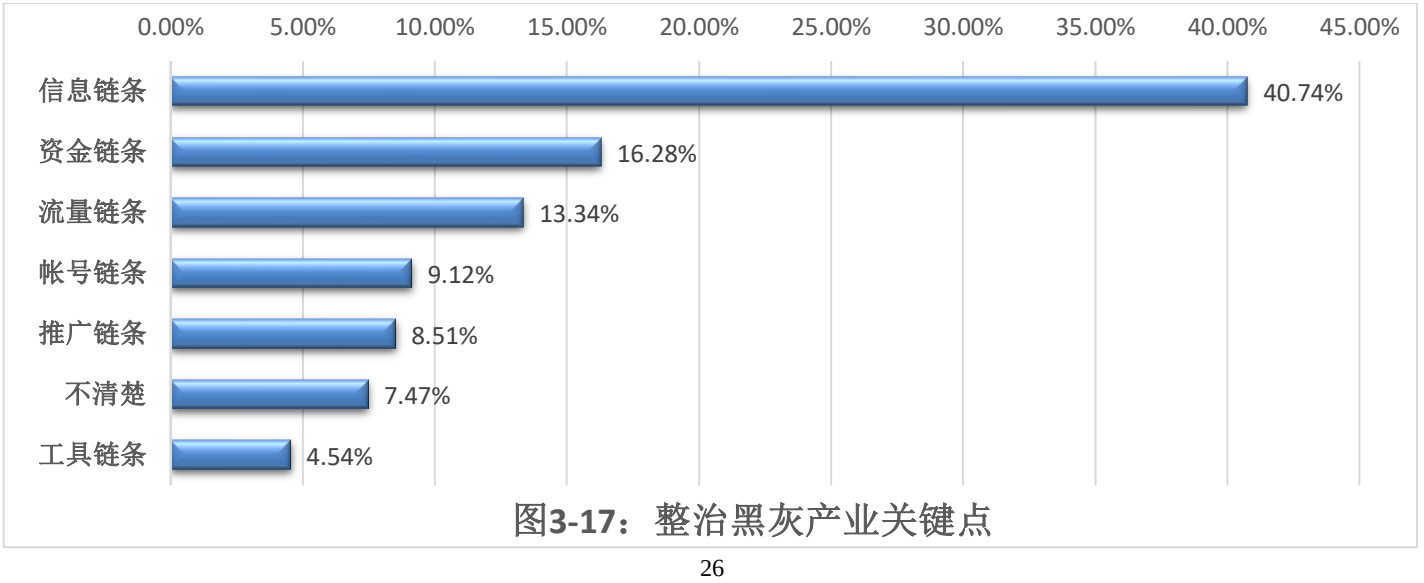


图3-17：整治黑灰产业关键点

A16. 黄色暴力等低俗不良信息现状

大多数受调查的 A 类从业人员认为黄色暴力等低俗不良信息的情况有一些好转，其中认为比过去少了一些的占 33.27%，比过去少了许多 17.63%，认为基本见不到 占 9.84%，三项合计共有 60.74%的 A 类从业人员认为低俗不良信息减少了（如图 3-18）。

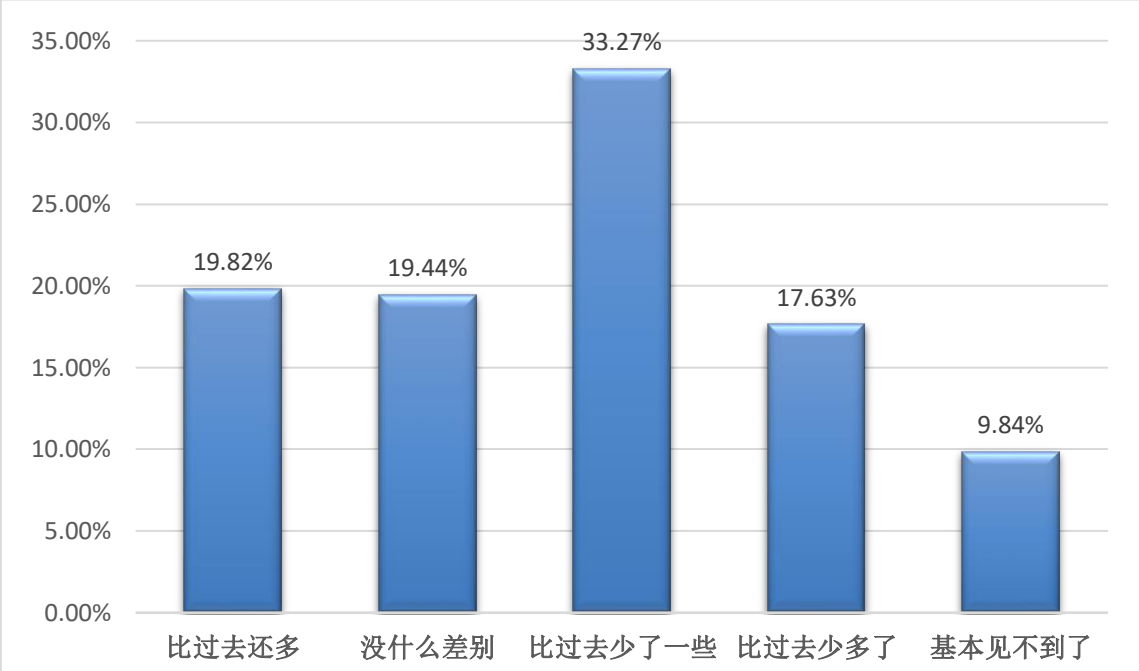


图3-18：不良信息现状

A17. 近一年来电信网络诈骗现状

大多数受调查的 A 类从业人员认为电信网络诈骗的情况有一些好转，其中认为比过去少了一些的占 33.61%，比过去少了许多的占 14%，认为基本见不到的占 6.05%，三项合计共有 53.66%的 A 类从业人员认为电信诈骗减少了（如图 3-19）。

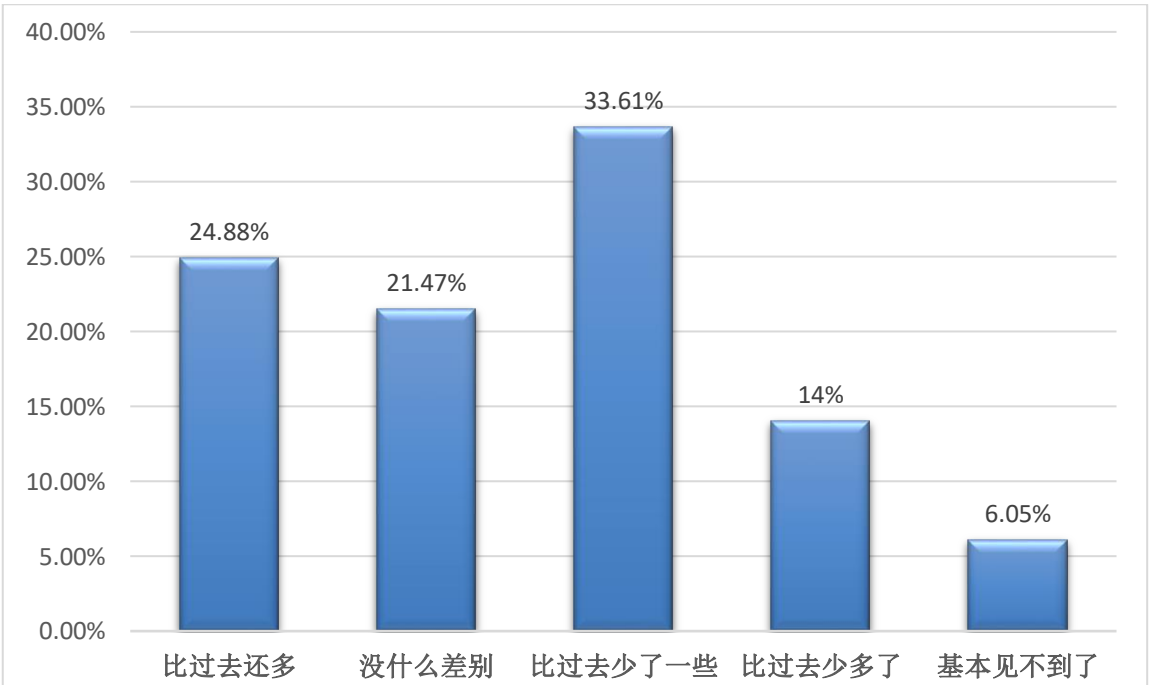


图3-19：电信网络诈骗现状

A18. 5G 网络应用的安全问题的关注

受调查的 A 类从业人员比较关注 5G 网络应用的安全问题，有 61.49%的人员关注过 5G 网络应用的安全问题（如图 3-20）。

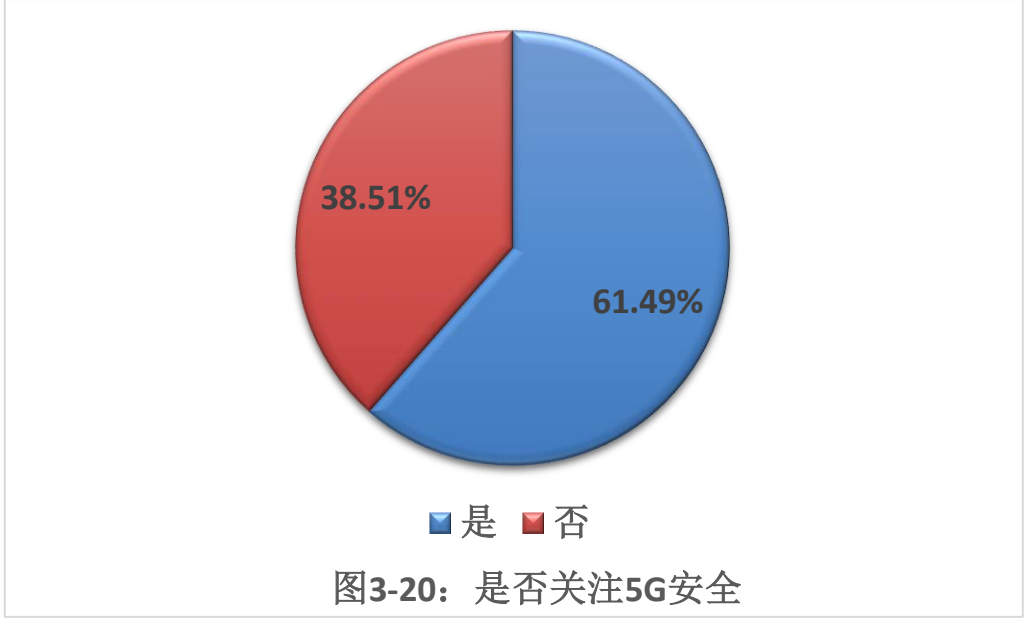


图3-20：是否关注5G安全

A18.1、5G 安全问题的关注重点

受调查的 A 类从业人员关注的重点在 5G 网络安全治理架构、安全产品、移动终端安全、技术标准制定，分别占 72.15%、53.98%、51.6%、50.57%（如图 3-21）。

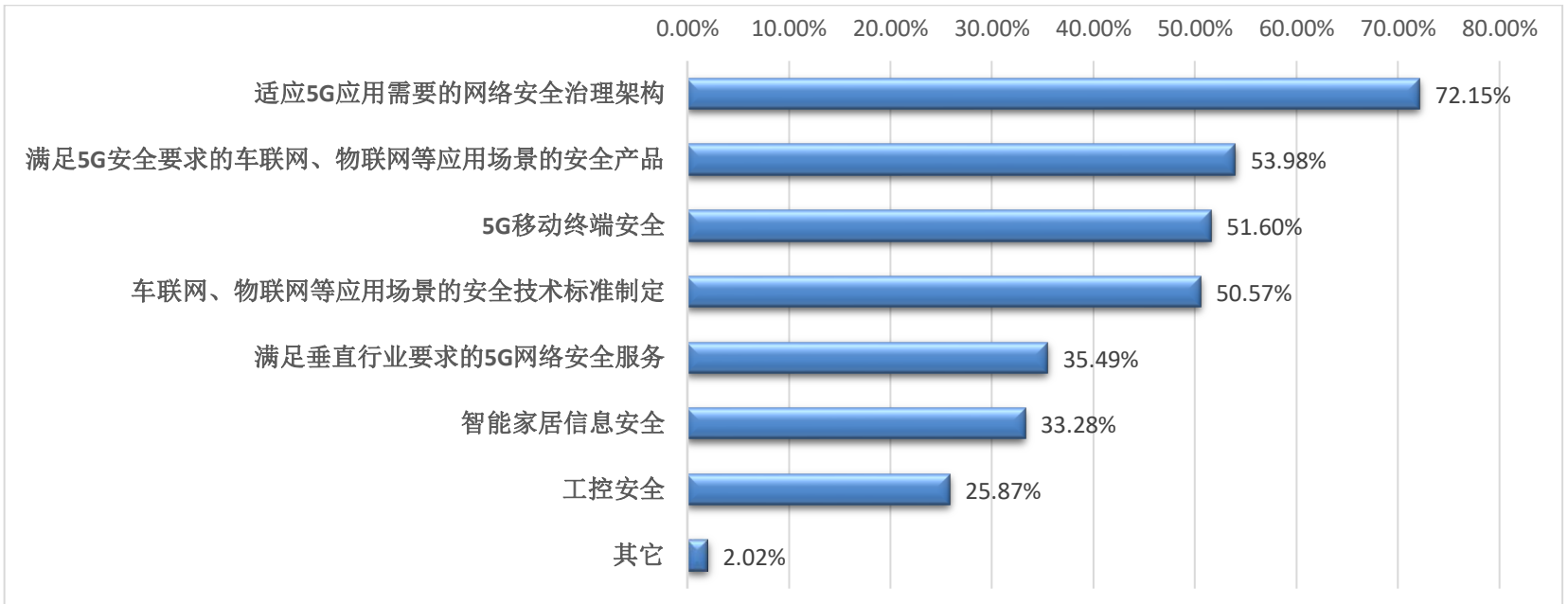


图3-21：5G安全关注重点

A19. 5G 时代应当重点加强安全管理措施

在安全管理措施方面，受调查的 A 类从业人员认为应重点加强 5G 网络安全技术标准体系建设（71.81%）、知识产权管理（60.07%）等措施（如图 3-22）。

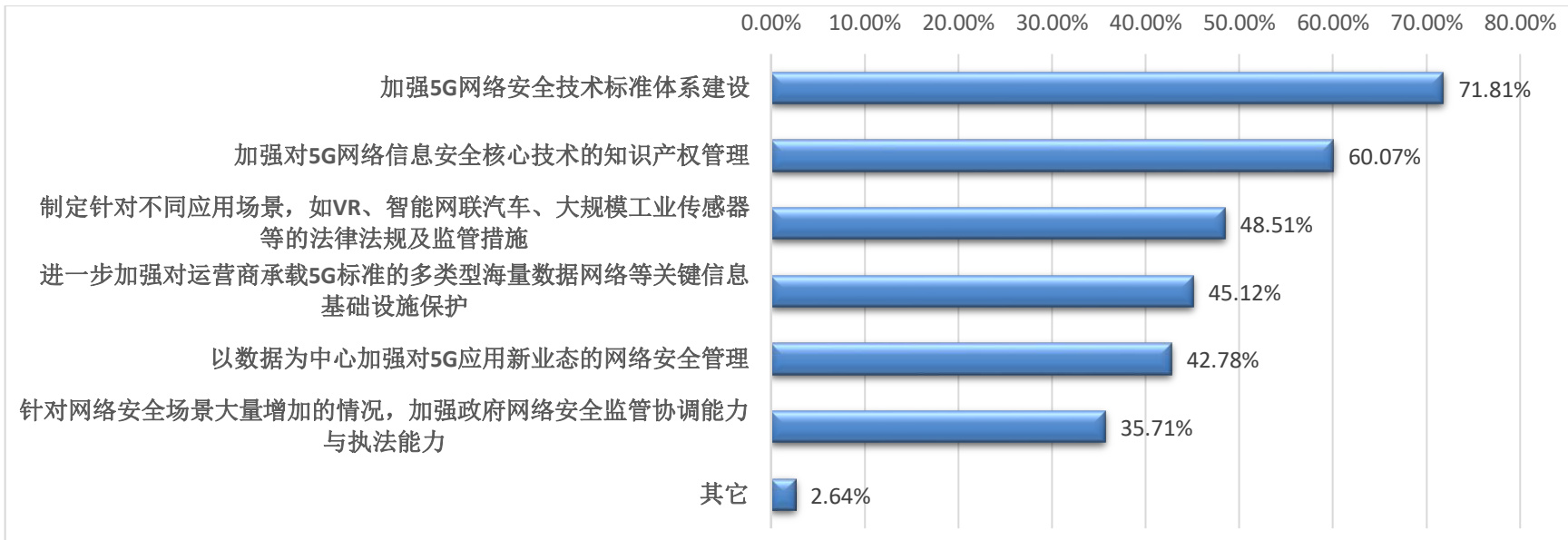


图3-22：重点加强的措施

A20. 网络安全培训状况

受调查的 A 类从业人员参加培训的情况良好。其中本单位组织过培训的占 53.48%，其次为政府部门组织的培训，占 34.38%（如图 3-23）。

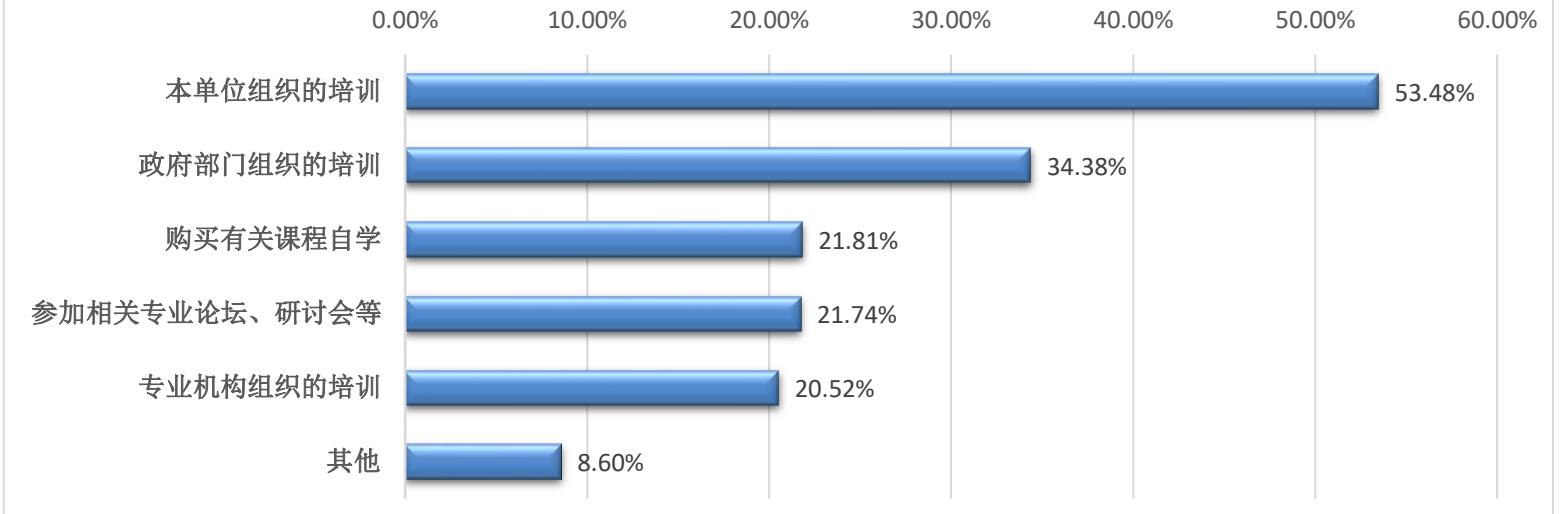


图3-23：网络安全培训状况

A21. 单位进行网络安全等级保护工作情况

单位参与等保工作的比例较高，受调查的 A 类从业人员单位中有 60.81%进行了信息系统定级备案，50.95%开展了网络安全自查（如图 3-24）。

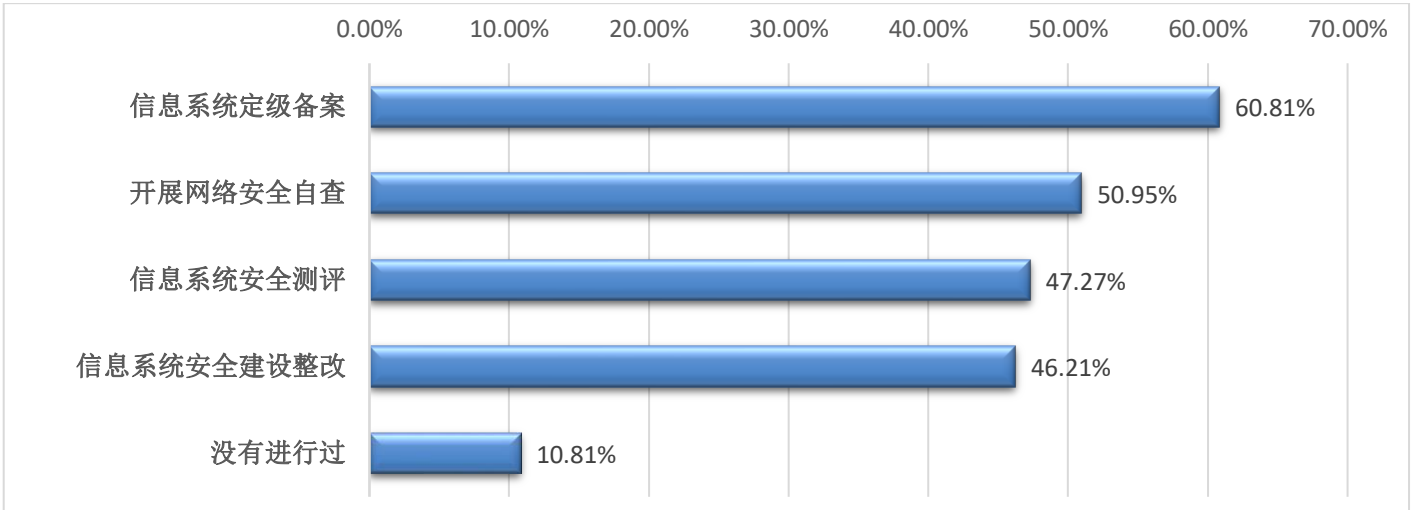


图3-24：单位进行过何种等级保护工作

A21.1、对测评机构进行测评工作的满意度现状

受调查的 A 类从业人员对测评工作评价较高，67.72%的人员对测评机构的工作表示满意（如图 3-25）。

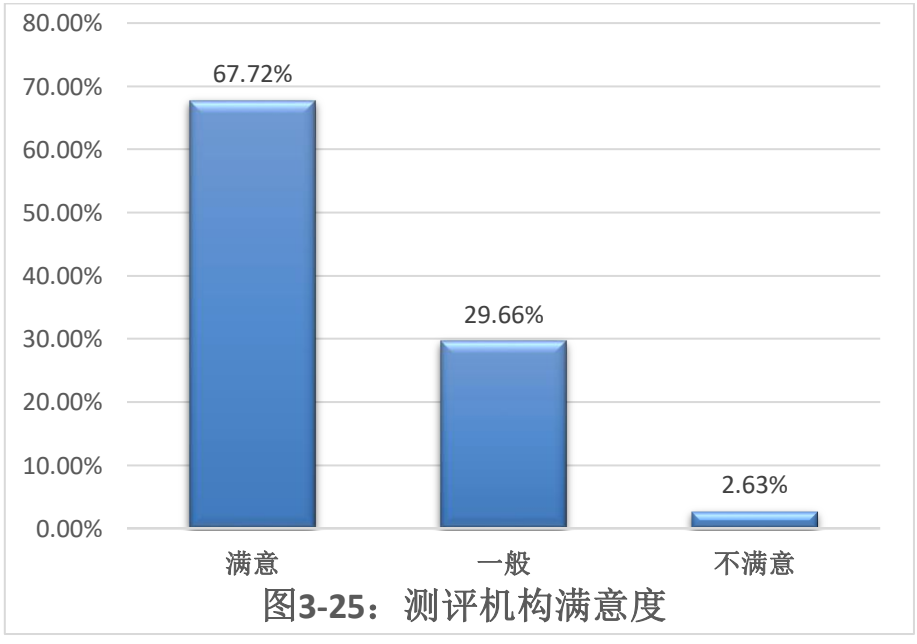


图3-25：测评机构满意度

A22. 网络安全等级保护制度重大意义的认识

受调查的 A 类从业人员对网络安全等级保护制度的意义认识比较务实，有 75.87%的人员认为是国家网络安全领域的基本政策和基本制度（如图 3-26）。

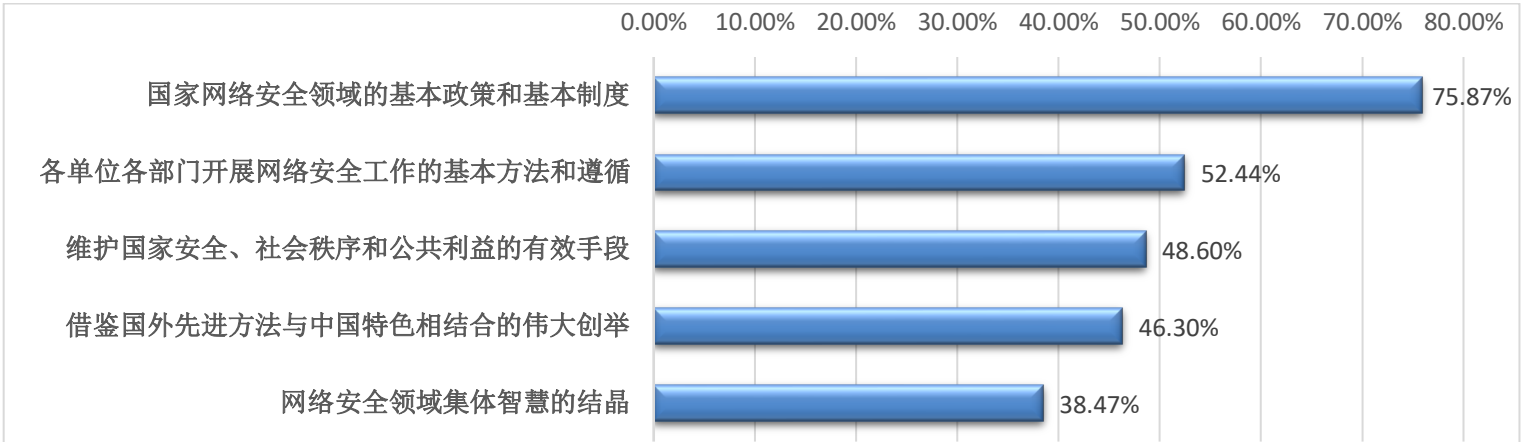


图3-26：等级保护重大意义

A23. 哪些单位应该开展网络安全等级保护工作

大部分受调查的 A 类从业人员对有等保义务单位范围的认识基本正确，但仍有 24.18%的人员选择了家庭和个人（如图 3-27）。

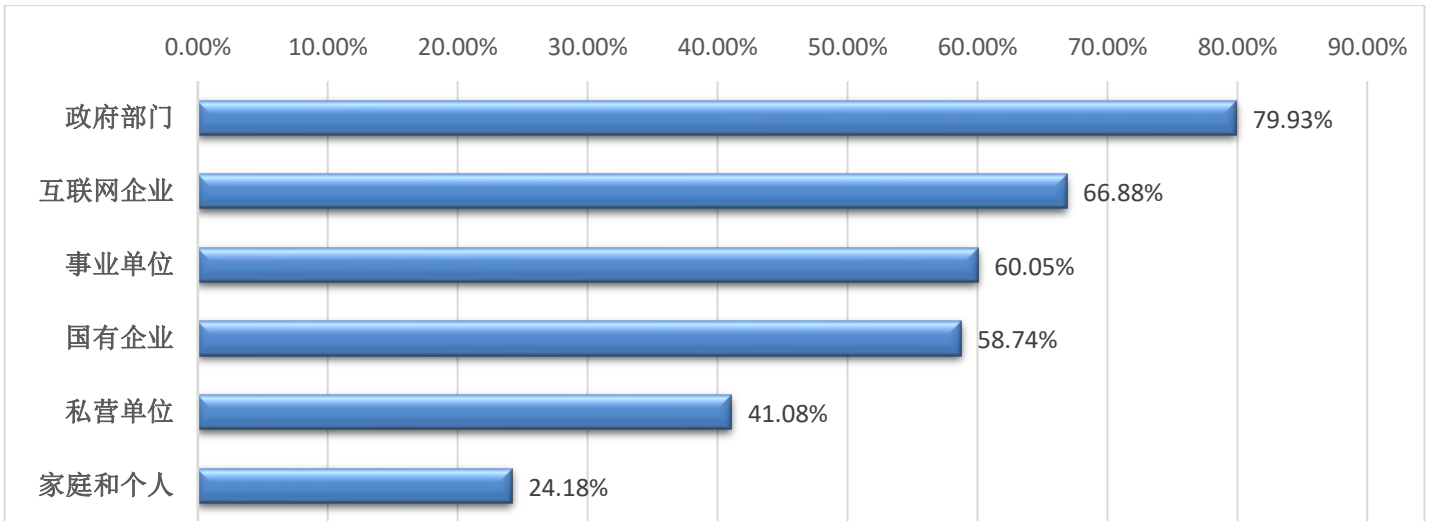


图3-27：应该开展等级保护工作的单位

A24. 哪些系统应该开展网络安全等级保护工作

受调查人的 A 类从业人员认为最该开展等级保护的系统前三位依次是关键信息基础设施占 70.43%，行业专网和业务信息系统占 58.65%，大数据系统占 57.81%（如图 3-28）。

图3-28：应该开展等级保护工作的系统

A25. 对网络安全等级保护制度 2.0 国家标准要求的了解

大部分受调查的 A 类从业人员了解网络安全等级保护制度 2.0 国家标准的要求，了解的比例占 53.93%（如图 3-29）。

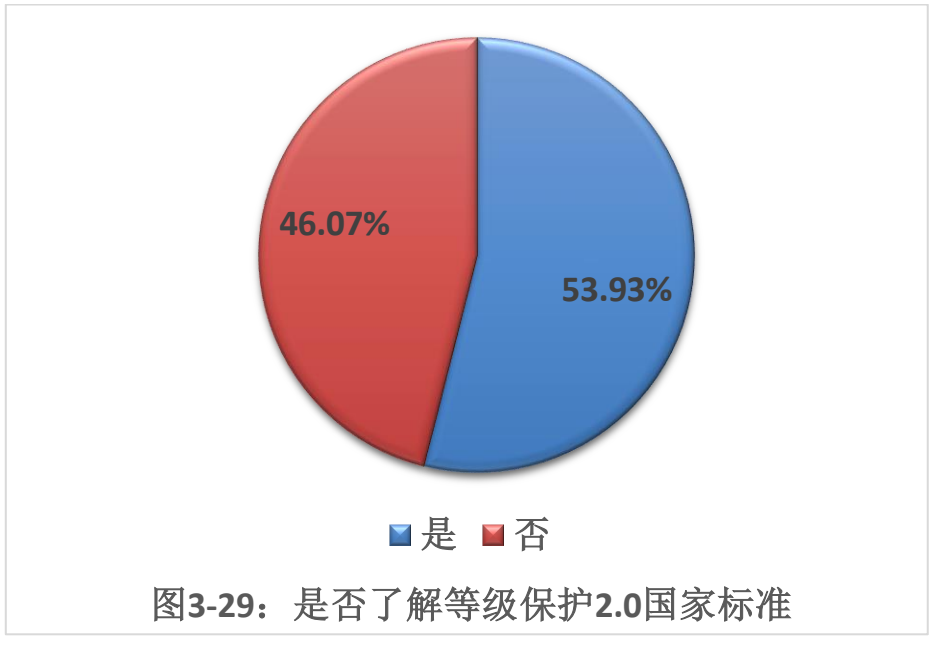


图3-29：是否了解等级保护2.0国家标准

A25.1、等保 2.0 的了解渠道

行业论坛是受调查的 A 类从业人员了解等保 2.0 标准的主要渠道，占比 56.74%，其次为单位或政府组织的培训（48.45%），如图 3-30 所示。

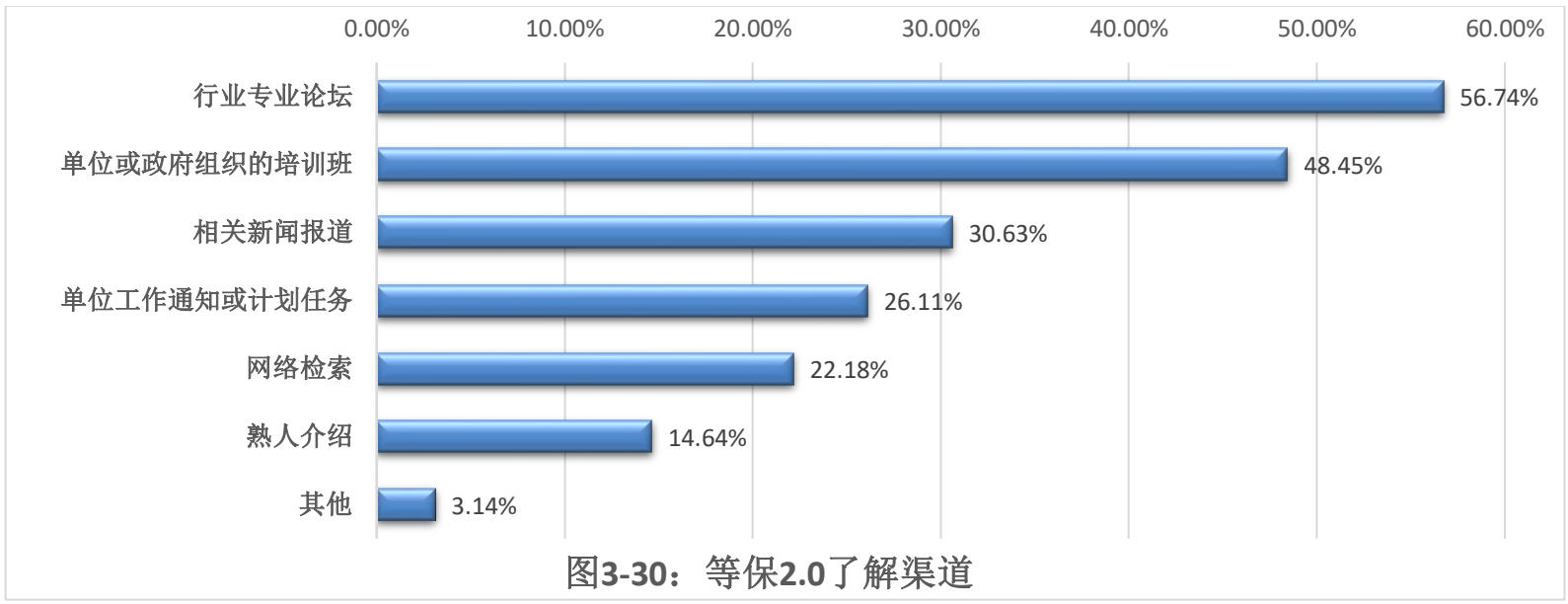


图3-30：等保2.0了解渠道

A26. 单位发生网络安全事件情况

单位没有发生过网络安全事件的受调查 A 类从业人员占比 51.51%（如图 3-31）。

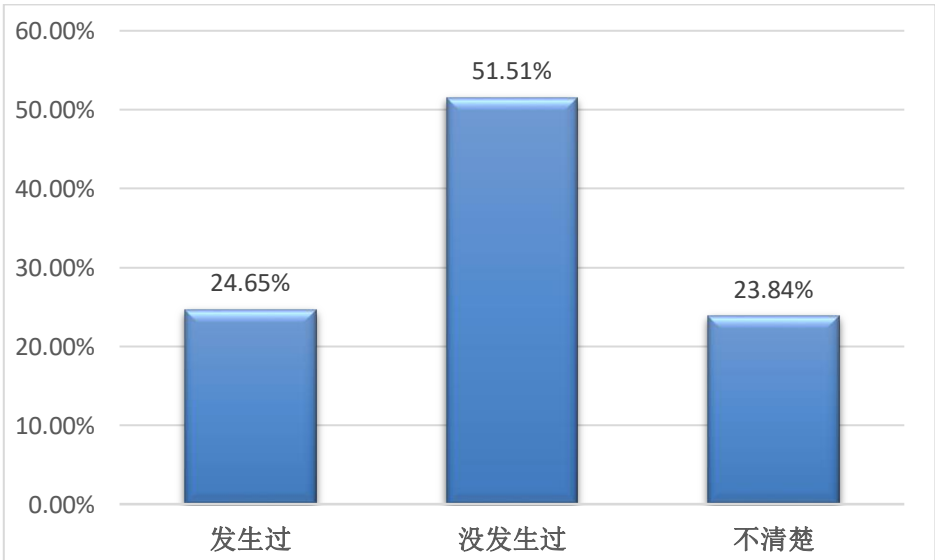


图3-31：单位网络安全事件发生情况

A26.1、安全事件的类型

受调查的 A 类从业人员单位发生最多的网络安全事件是网站被攻击篡改，占比 52.11%（如图 3-32）。

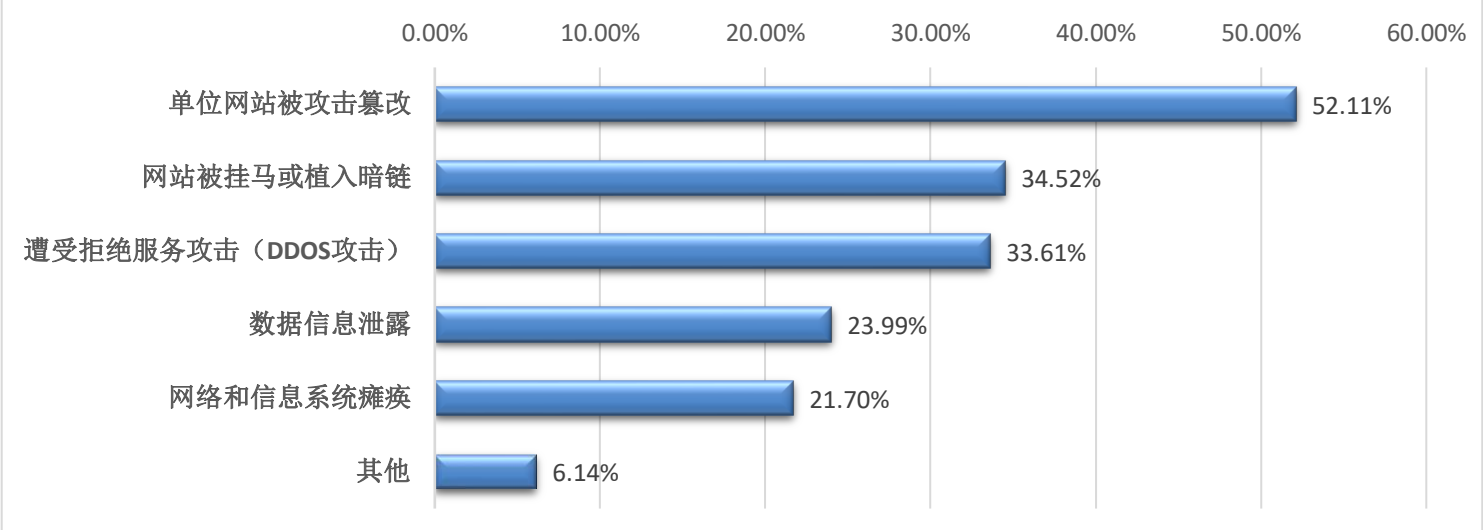


图3-32：单位安全事件类型

A26.2、单位针对发生的网络安全事件向公安机关报案情况

有 58.97%的受调查 A 类从业人员单位，在遇到网络安全事件时选择向公安机关报案（如图 3-33）。

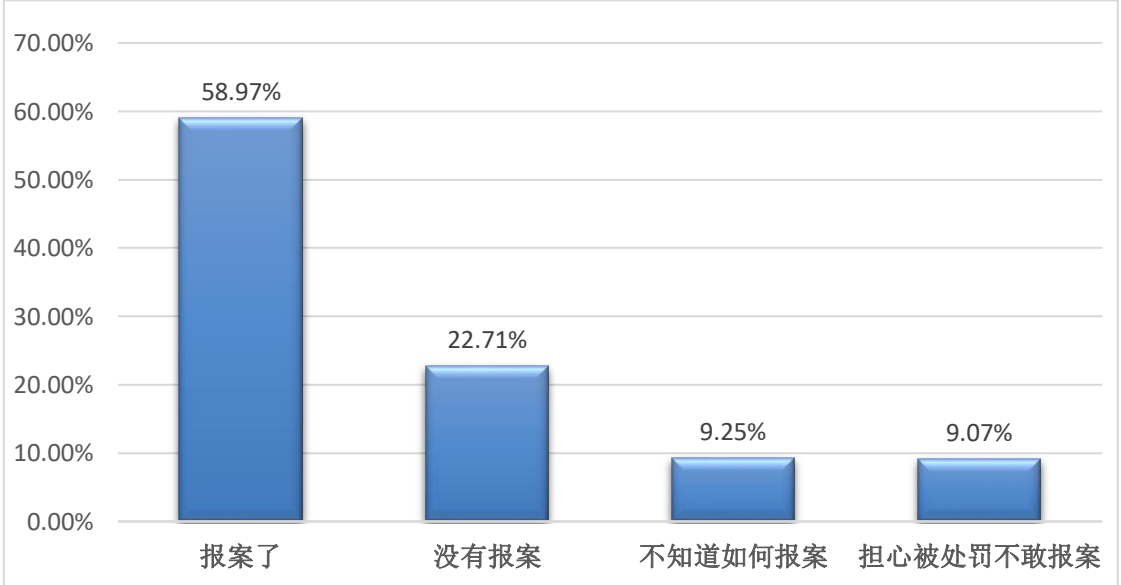


图3-33：单位网络安全事件报案情况

A26.3、对公安机关案件受理情况的满意度

受调查的 A 类从业人员对公安机关案件受理情况满意的占比 75.93%（如图 3-34）。

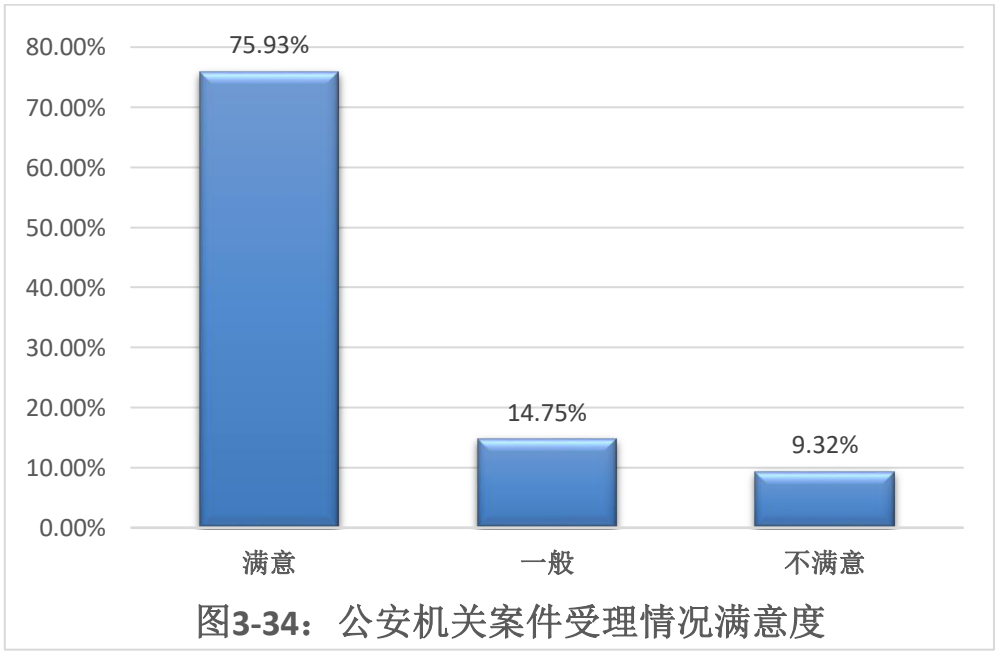


图3-34：公安机关案件受理情况满意度

A27. 网络安全等级保护对产业、企业发展的推动作用的认识

受调查的 A 类从业人员对网络安全等级保护的作用认识比较正面，有 69.53%的人员认为网络安全等级保护对产业、企业发展的推动很大（如图 3-35）。

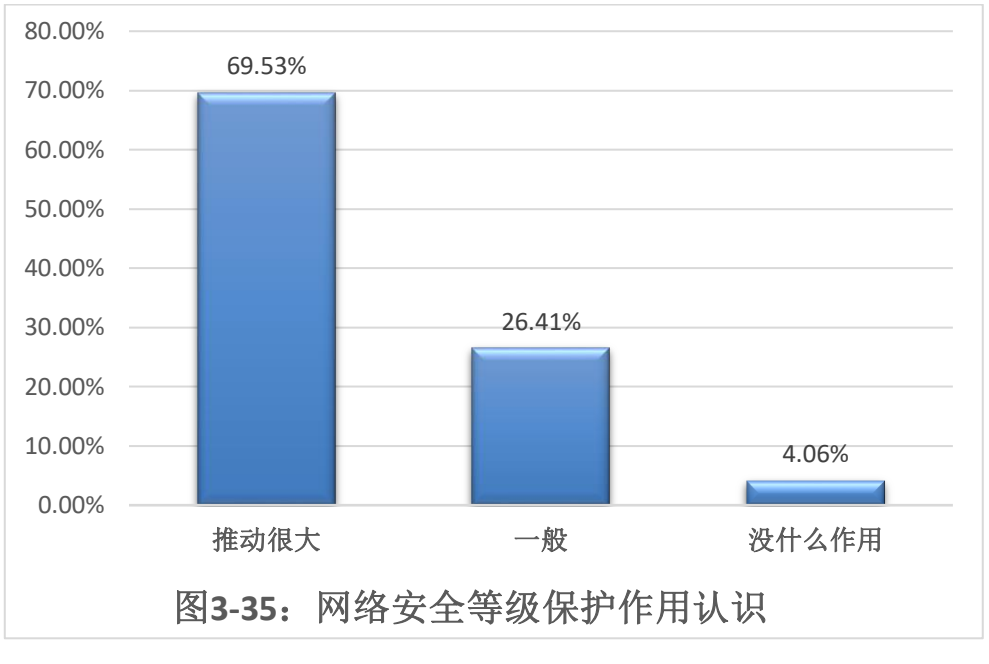


图3-35：网络安全等级保护作用认识

A28. 公安机关网络安全执法检查工作满意度

受调查的 A 类从业人员对公安机关网络安全执法检查工作满意度评价比较高，59.89%的人员评价为满意，排除没有参加过检查的 8.69%的样本，调整后满意的占比 65.59%（如图 3-36）。

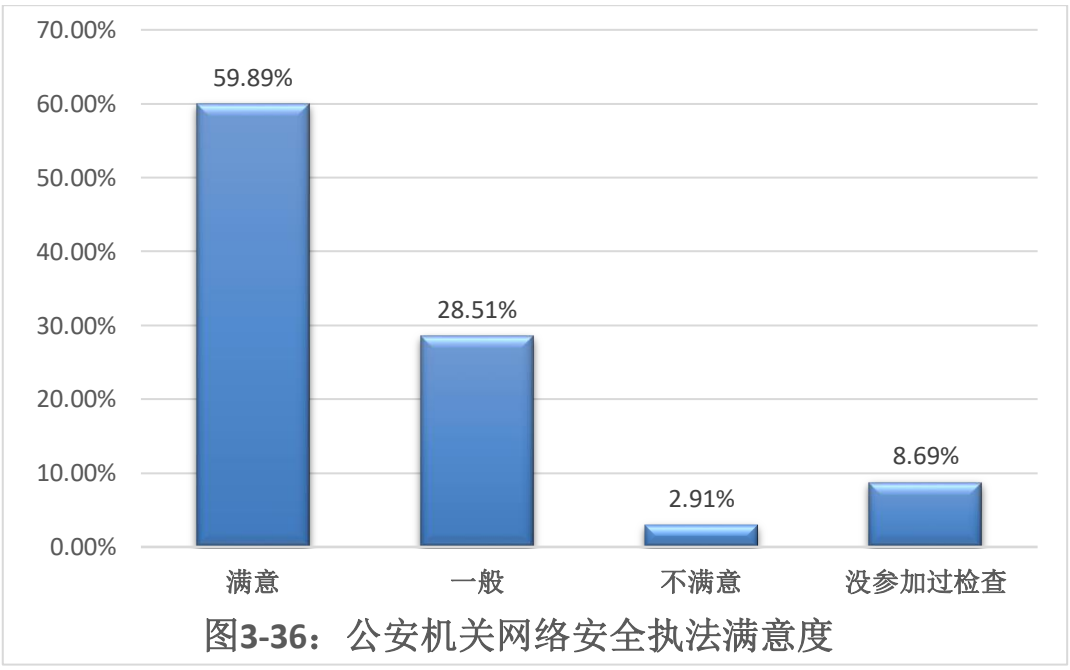


图3-36：公安机关网络安全执法满意度

四、B 卷：网络服务提供者非网络安全相关工作的从业人员

网络服务提供者非网络安全相关工作（B 类）的从业人员对网络行业的情况比较熟悉，但对专业的网络安全业务不一定了解。

B 类问卷有效答卷数量 4645 份，以下是 B 类问卷各项数据的详细统计结果。

B3. 当前网络安全状况

受调查的 B 类从业人员网络安全感为安全的占比较高，11.24%认为非常安全，33.54%认为安全，两者合计有 44.78%的人员感觉安全和非常安全（如图 4-1）。

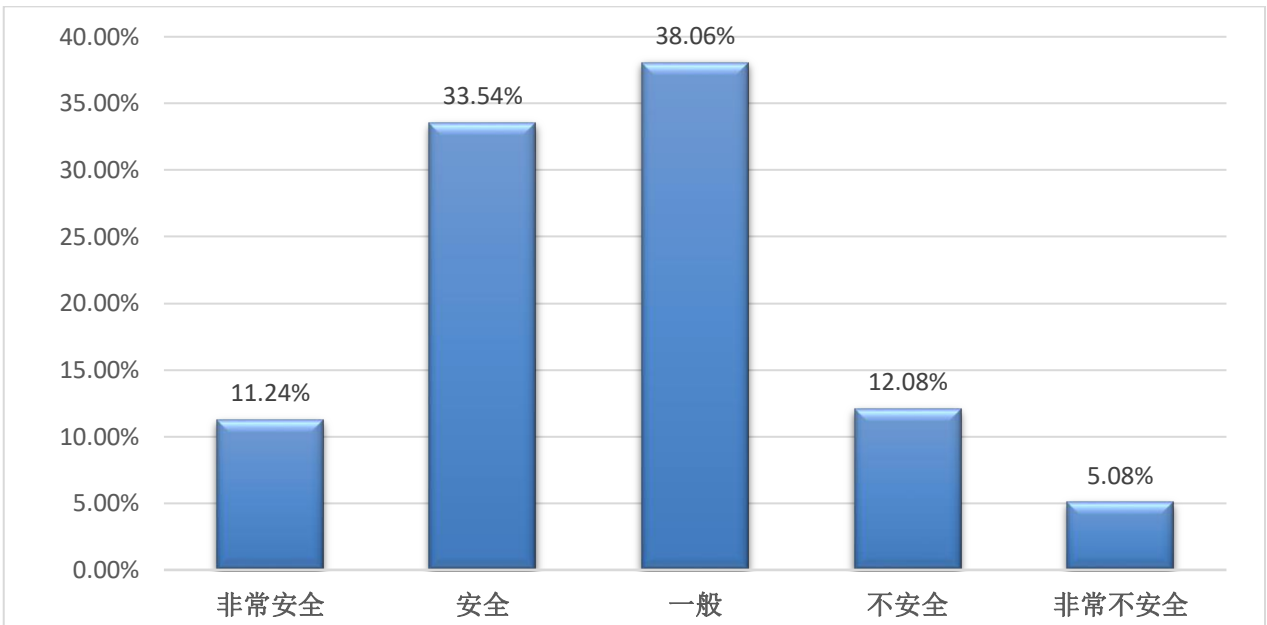


图4-1：安全状况评价

B3.1、与去年相比网络安全感的变化

接近一半受调查的 B 类从业人员认为当前网络安全感提升，13.07%从业人员认为明显提升，33.41% 人员认为有提升，两者合计 46.48%的人员认为提升或明显提升（如图 4-2）。

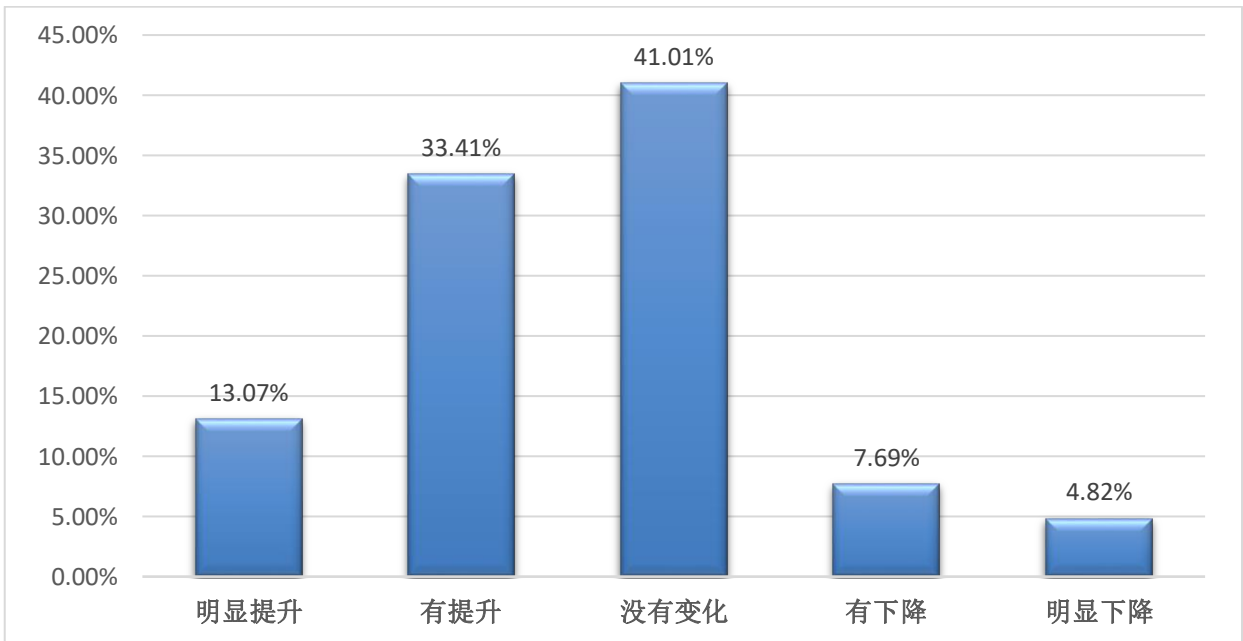


图4-2：网络安全感变化评价

B4. 网络安全培训状况

受调查的 B 类从业人员参加网络安全培训最主要为本单位组织，占 50.85%（如图 4-3）。

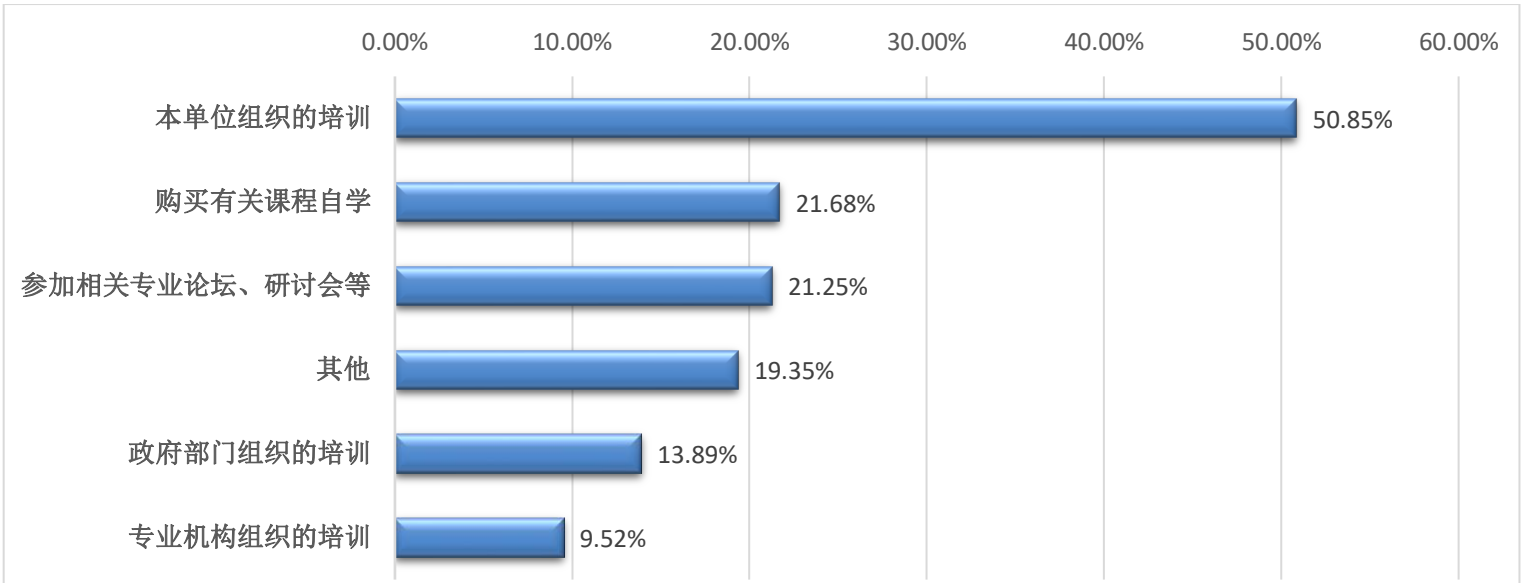


图4-3：网络安全培训状况

B5. 遇到的网络个人信息泄露状况

受调查的 B 类从业人员认为遇到的或身边的人遇到的网络个人信息泄露非常多的占 25.86%，比较多的占 24.33%，两者合计 50.19%（如图 4-4）。

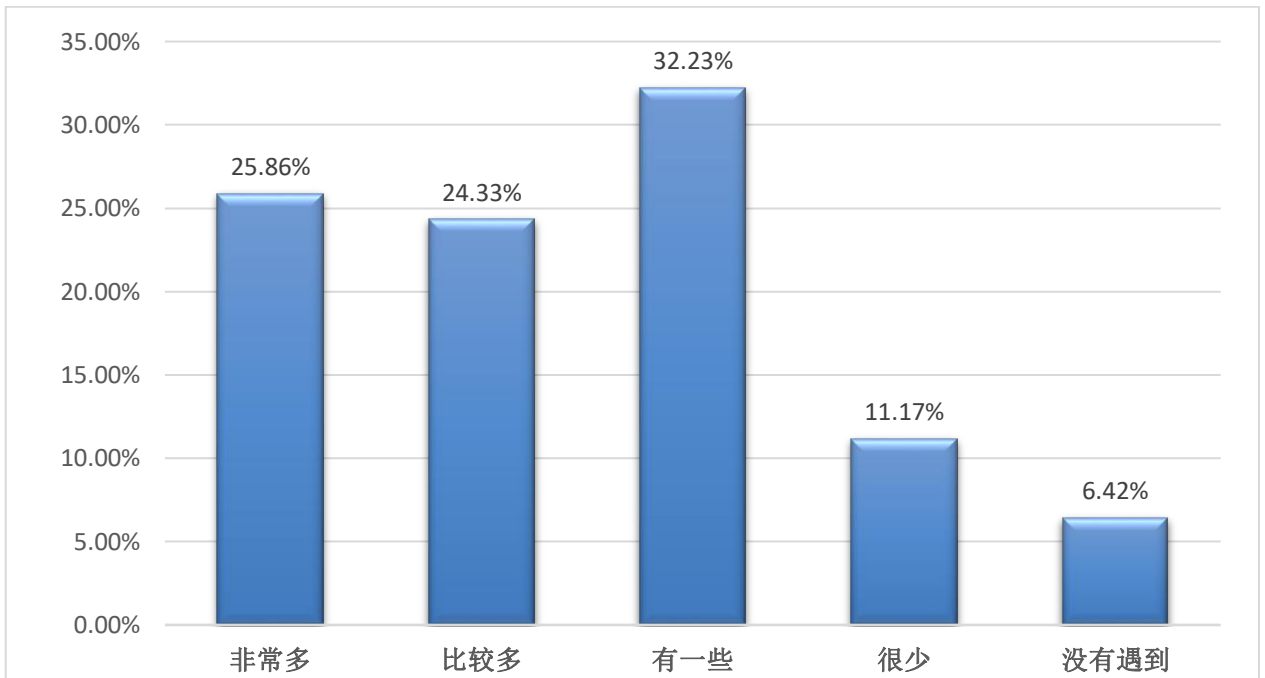


图4-4：网络个人信息泄露状况

B6. 安全问题较多网络应用或服务

受调查的 B 类从业人员认为安全问题最多的网络应用或服务前五位依次是：社交应用（38.75%），网络购物（35.78%），互联网理财（29.19%），网上支付（28.65%），网络游戏（27.49%），如图 4-5 所示。

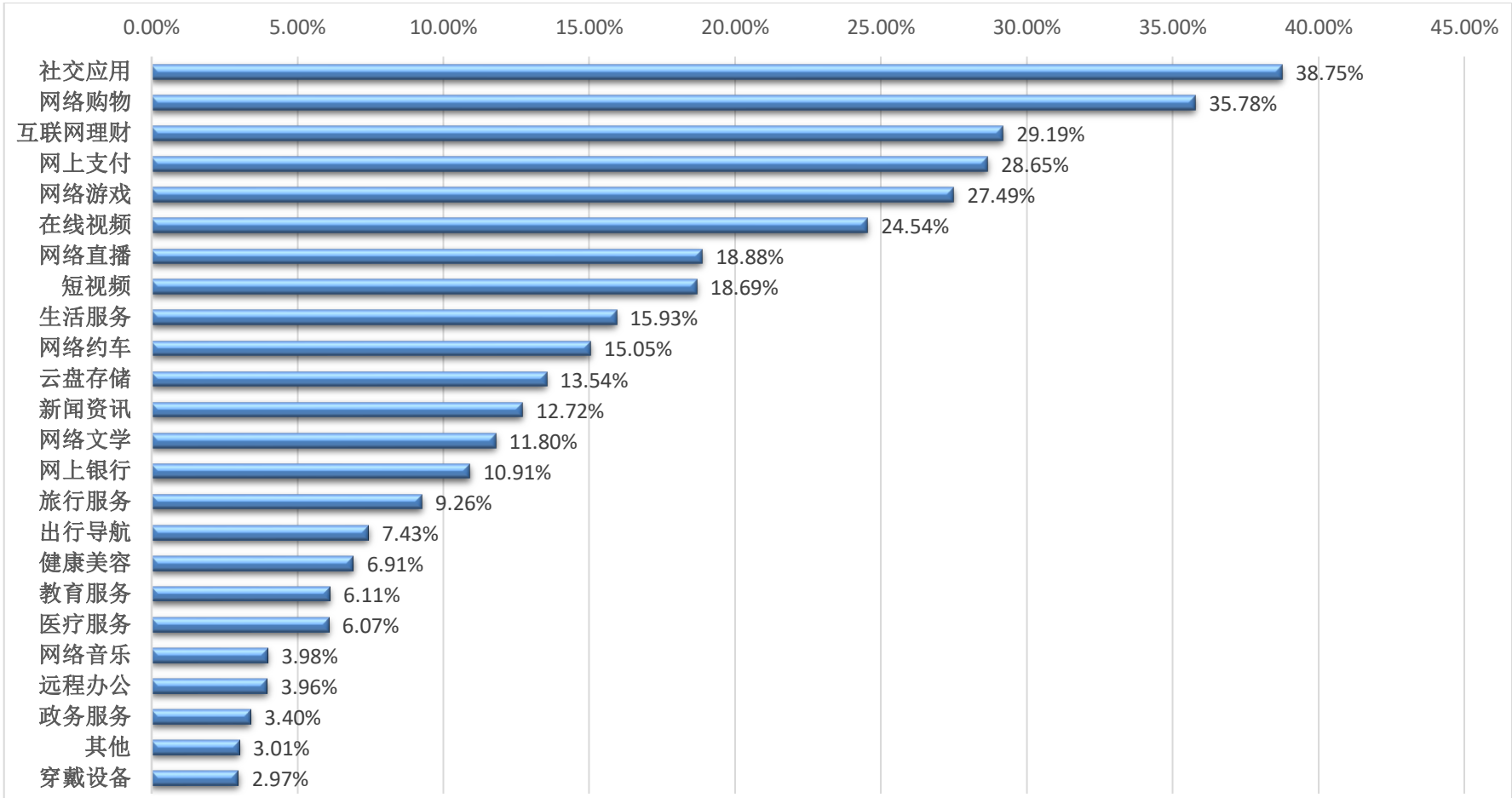


图4-5：安全问题多的网络应用或服务

B7. 近年来网络数据、账号违法交易等互联网黑灰产业的情况

受调查的 B 类从业人员认为黑灰产业活动大幅增加和有所增加的占比合计 48.07%，其中认为有所增加的有 33.52%，认为大幅增加的有 14.55%（如图 3-16）。

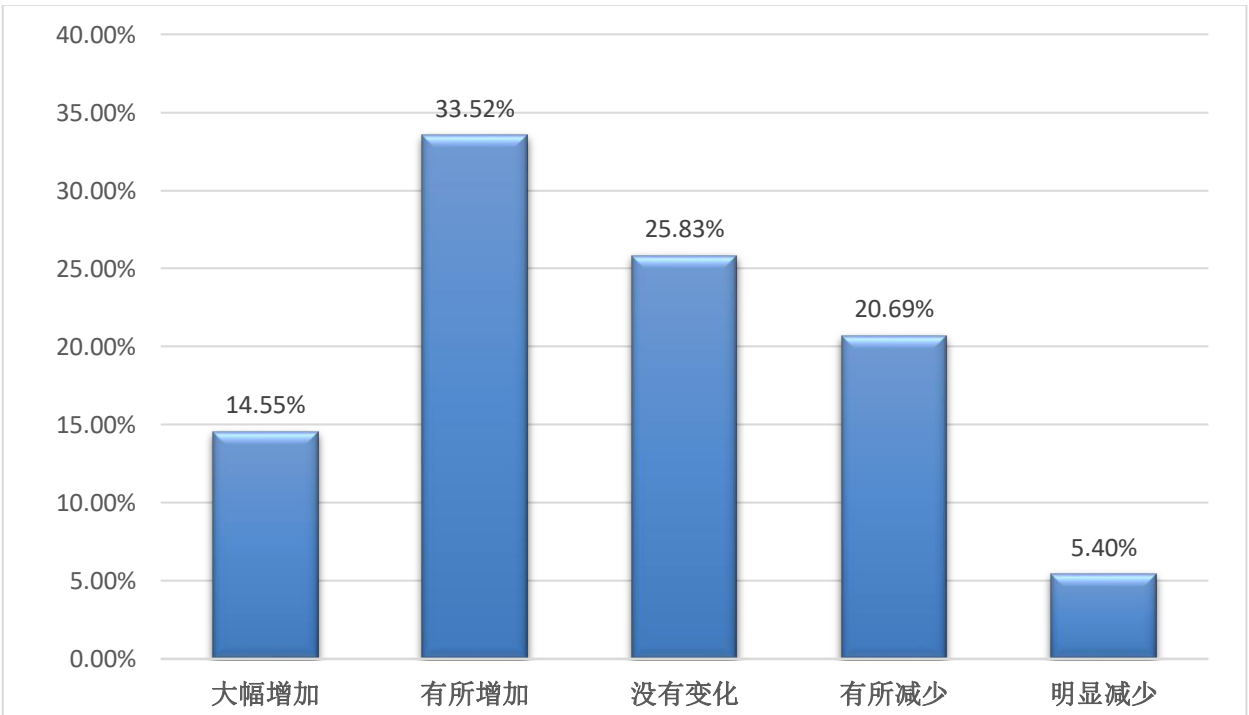


图4-6：近年来黑灰产业状况

B7.1、整治网络黑灰产业链条关键点

受调查的 B 类从业人员中有 37.87%认为治理网络黑灰产业链条最关键的是信息链条（如图 4-7）。

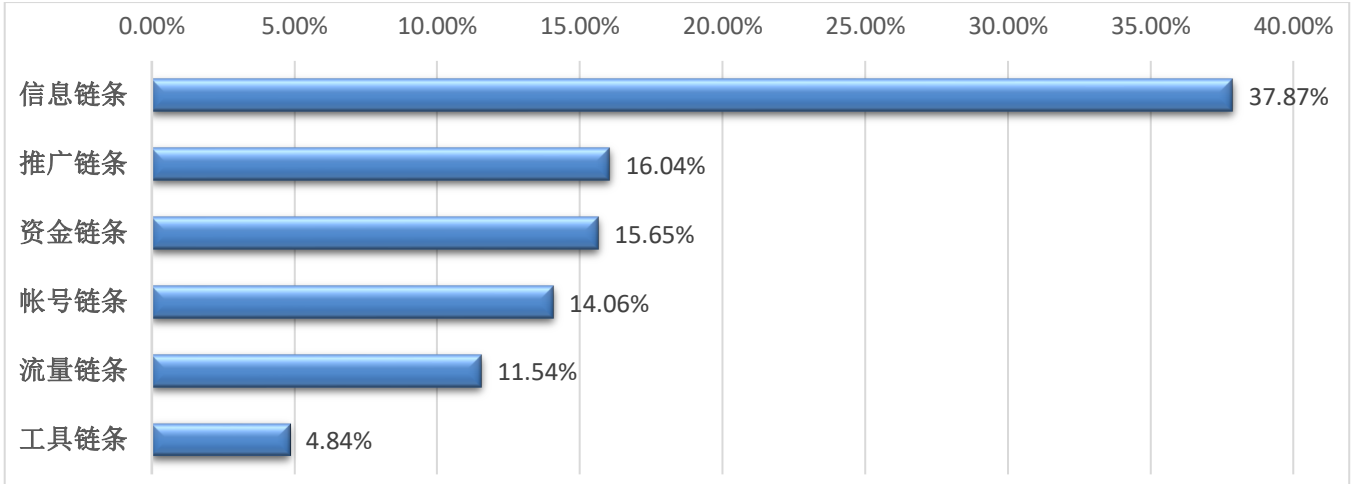


图4-7：整治黑灰产业关键点

B8. 近一年来电信网络诈骗现状

部分受调查的 B 类从业人员认为电信网络诈骗的情况有一些好转，其中认为比过去少了一些的占 32.66%，比过去少了许多了占 9.84%，认为基本见不到的占 4.76%，三项合计共有 47.26%的 B 类从业人员认为电信诈骗减少了（如图 4-8）。

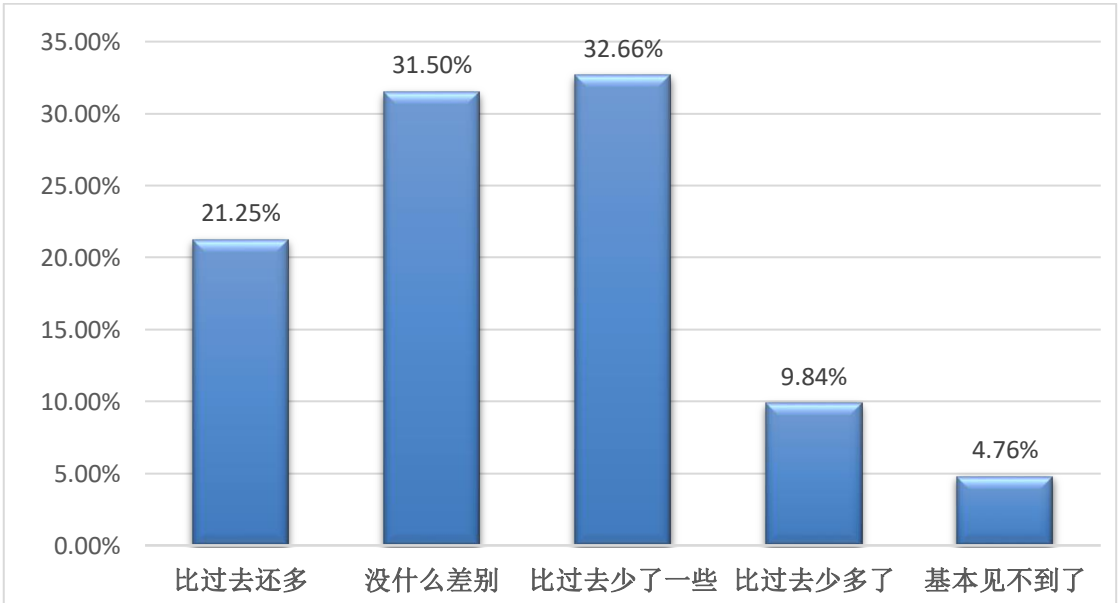


图4-8：电信网络诈骗现状

B9. 黄色暴力等低俗不良信息现状

大多数受调查的 B 类从业人员认为黄色暴力等低俗不良信息的情况有一些好转，其中认为比过去少了一些的占 30.94%，比过去少多了的占 14.17%，认为基本见不到的占 9.97%，三项合计共有 55.08%的 B 类从业人员认为低俗不良信息减少了（如图 4-9）。

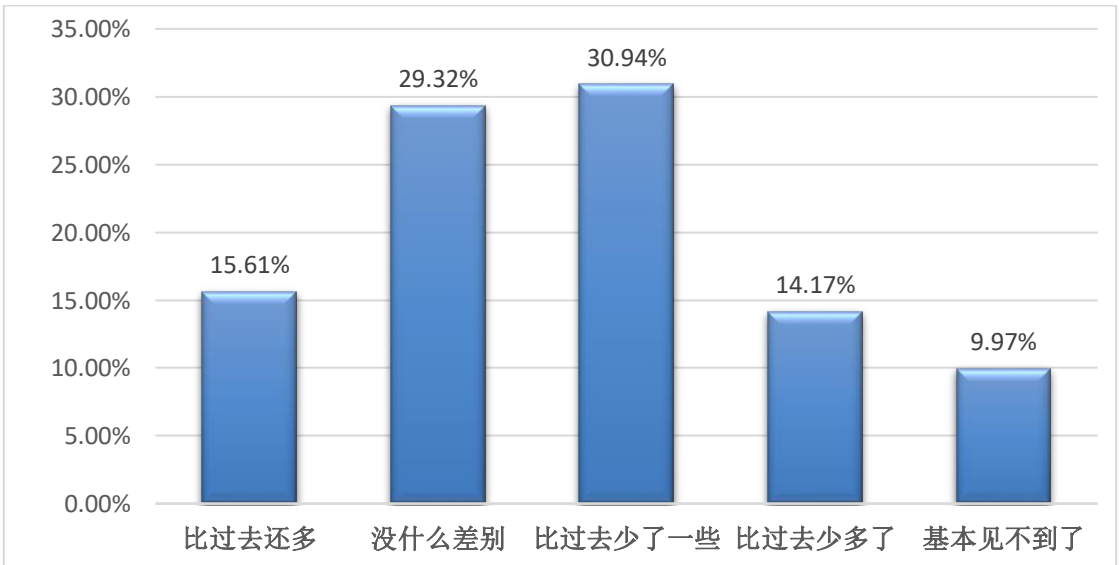


图4-9：不良信息现状

B10. 需要重点治理的网络安全问题

受调查的 B 类从业人员认为个人隐私信息泄露（67.75%）、网络诈骗（54.68%）、网络赌博（53.56%）、网络谣言与诽谤（45.96%）、网络色情（42.95%）是需要重点治理安全问题的前五位，各类问题占比如图 4-10 所示。

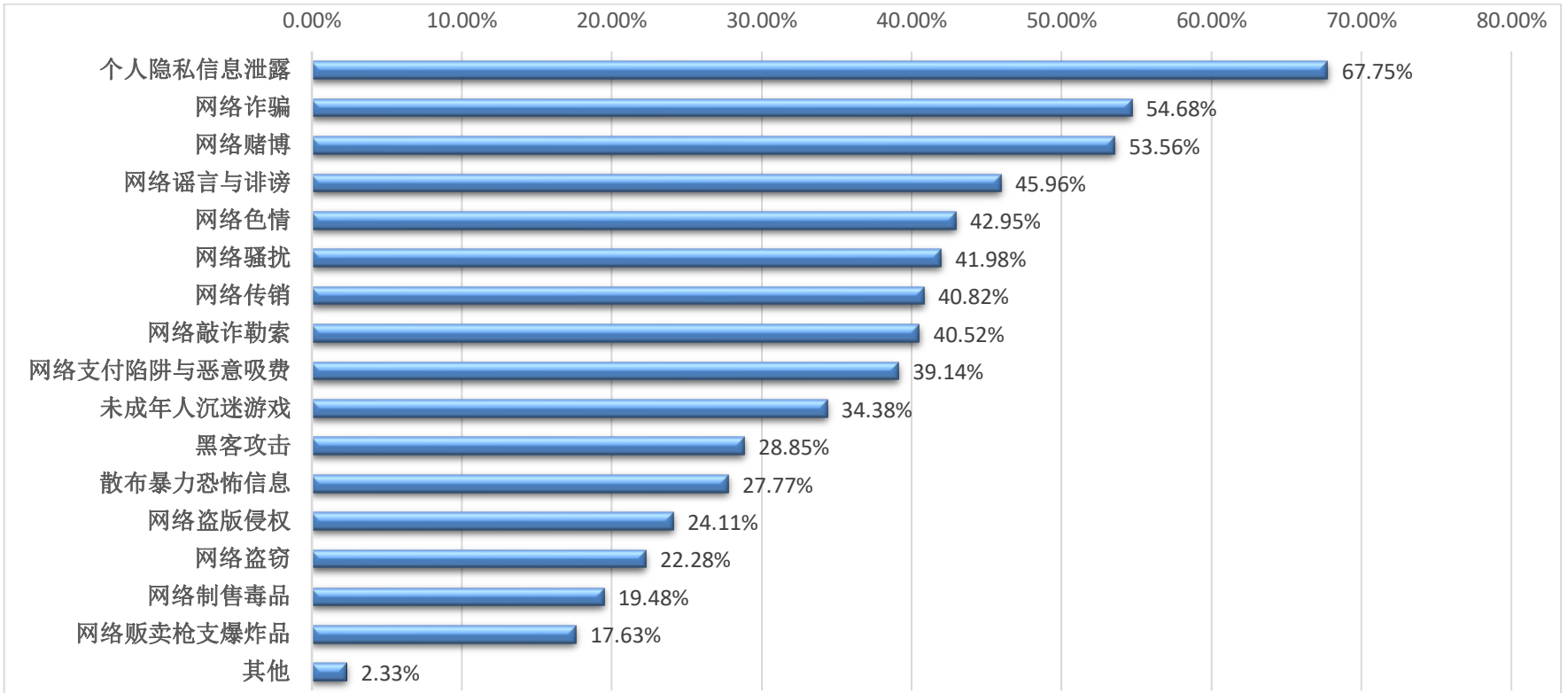


图4-10：需要治理的网络安全问题

B11. 亟待加强的网络安全立法内容

受调查的 B 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 74.7%，数据安全保护占 55.37%，网络平台责任占 54.62%（如图 4-11）。

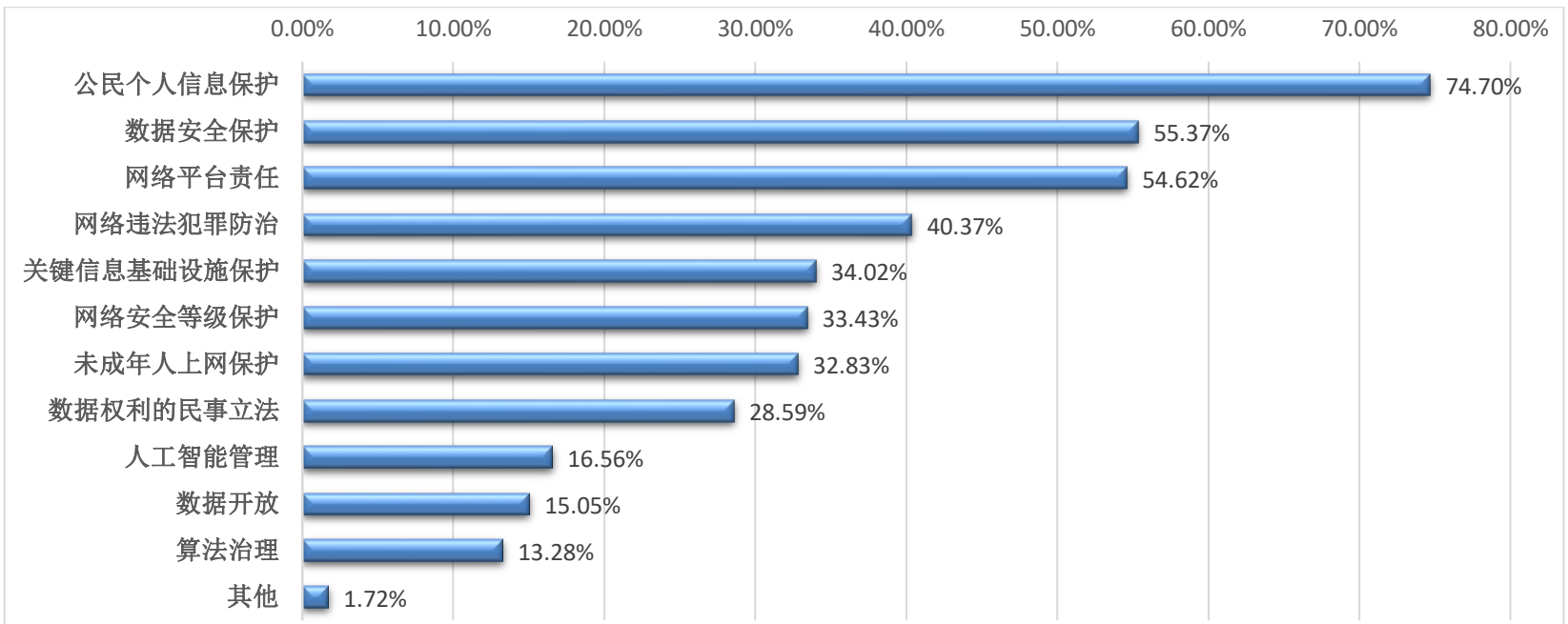


图4-11：亟待加强的立法内容

B12. 对网络法规的认识

除了《中华人民共和国网络安全法》外，受调查的 B 类从业人员对安全方面的法律有一定的认识，知道比较多的法规分别是《中华人民共和国国家安全法》（57.63%）、《中华人民共和国消费者权益保护法》（42.39%）、《中华人民共和国保守国家秘密法》（28.05%）、《中华人民共和国反恐怖主义法》（25.94%），如图 4-12 所示。

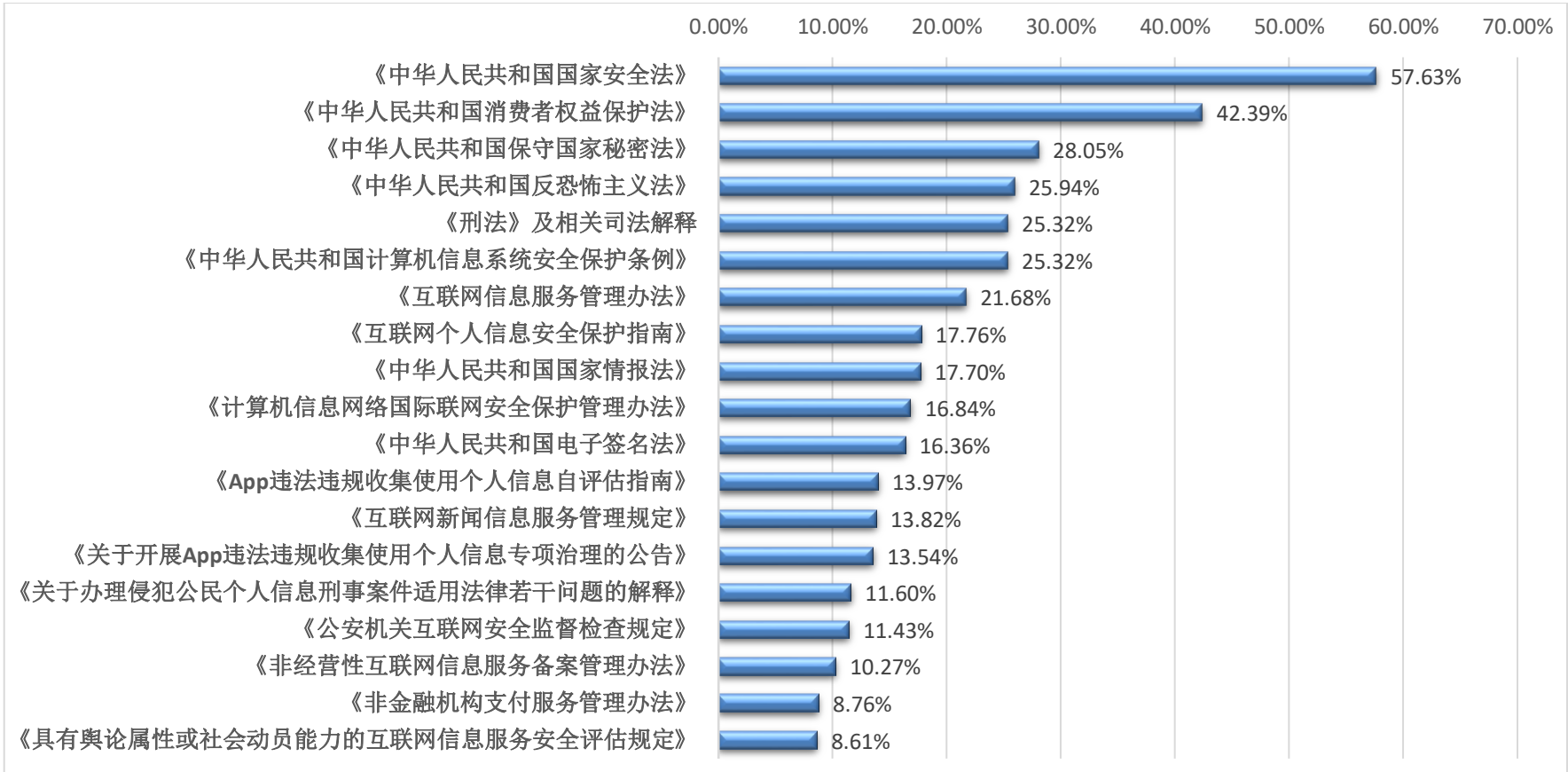


图4-12：对网络法规的认识

五、C 卷：网络安全产品、服务提供者的从业人员

网络安全产品、服务提供者（C 类）的从业人员熟悉安全技术和产业发展状况，对安全问题的认识比较深刻，评价一般较为保守。

C 类问卷有效问卷数量 3705 份，以下是 C 类问卷各项数据的详细统计结果。

C3. 当前网络安全状况

受调查的 C 类从业人员认为网络安全状况一般的最多，有 48.64% 的人员选择，认为状况良好的占 30.74%，认为状况堪忧的占 20.62%（如图 5-1）。

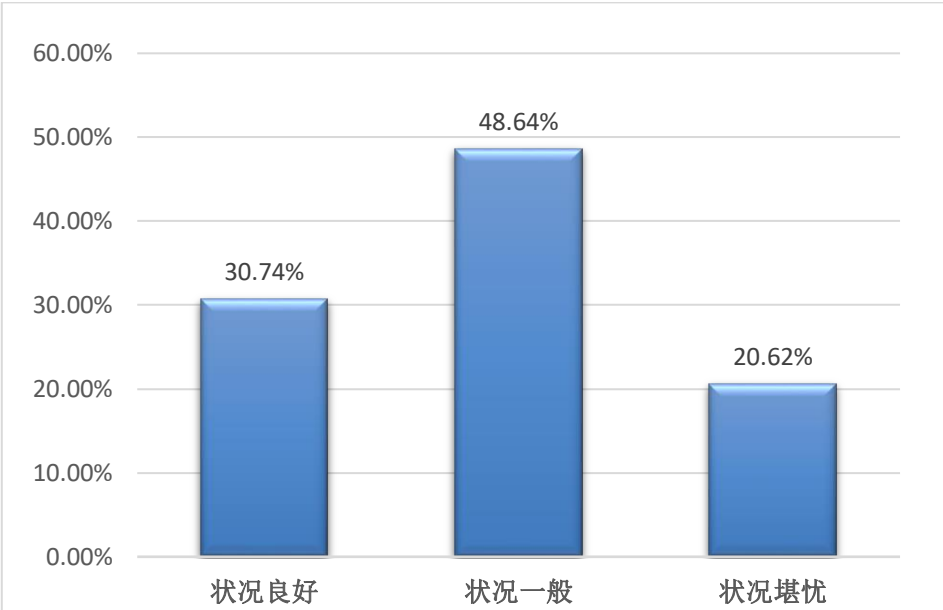


图5-1：安全状况评价

C3.1、与去年相比网络安全感的变化

绝大部分受调查的 C 类从业人员认为当前网络安全状况改善，有 24.02%的人员认为明显改善，有 54.82% 的人员认为有改善，两者合计有 78.84%的人员认为网络安全状况改善或明显改善（如图 5-2）。

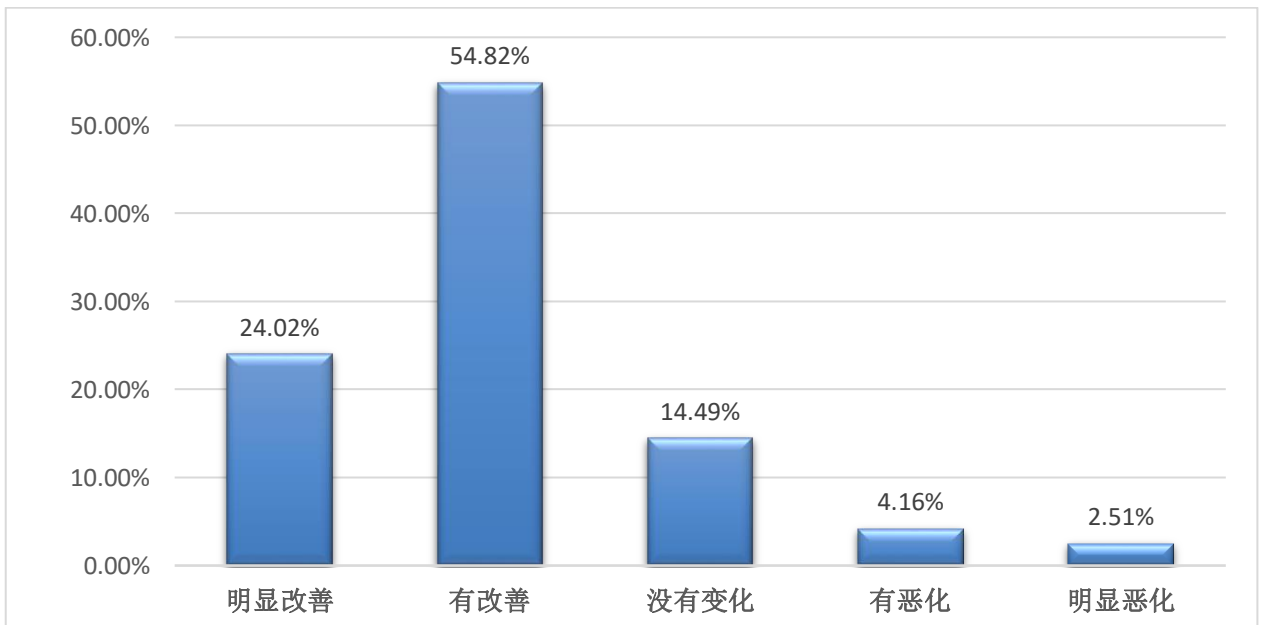


图5-2：网络安全感变化评价

C4. 网络服务提供者的管理措施对于保证网络安全水平的有效程度

受调查的 C 类从业人员有 19.57%认为非常有效，有 39.92%认为比较有效，两者合计共有 59.49%的人员认为非常有效和比较有效（如图 5-3）。

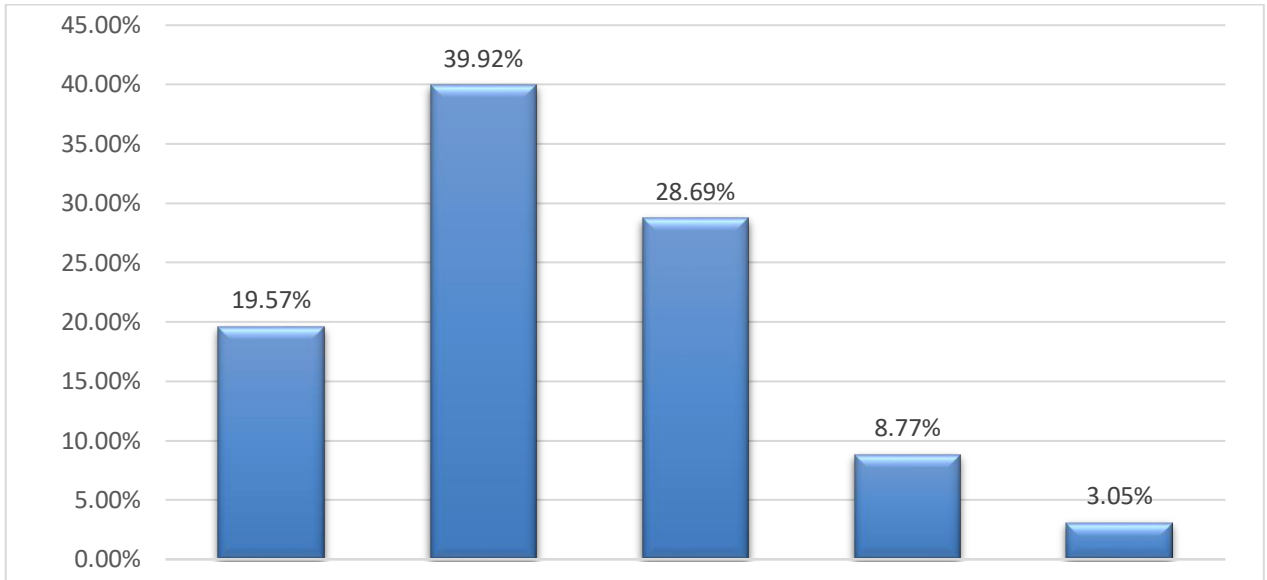


图5-3：管理措施有效程度

C5. 当前发展网络安全产品服务的政策环境状况

受调查的 C 类从业人员有 22.46%认为非常好，有 40.62%认为好，两者合计共有 63.08%的人员认为非常好和好（如图 5-4）。

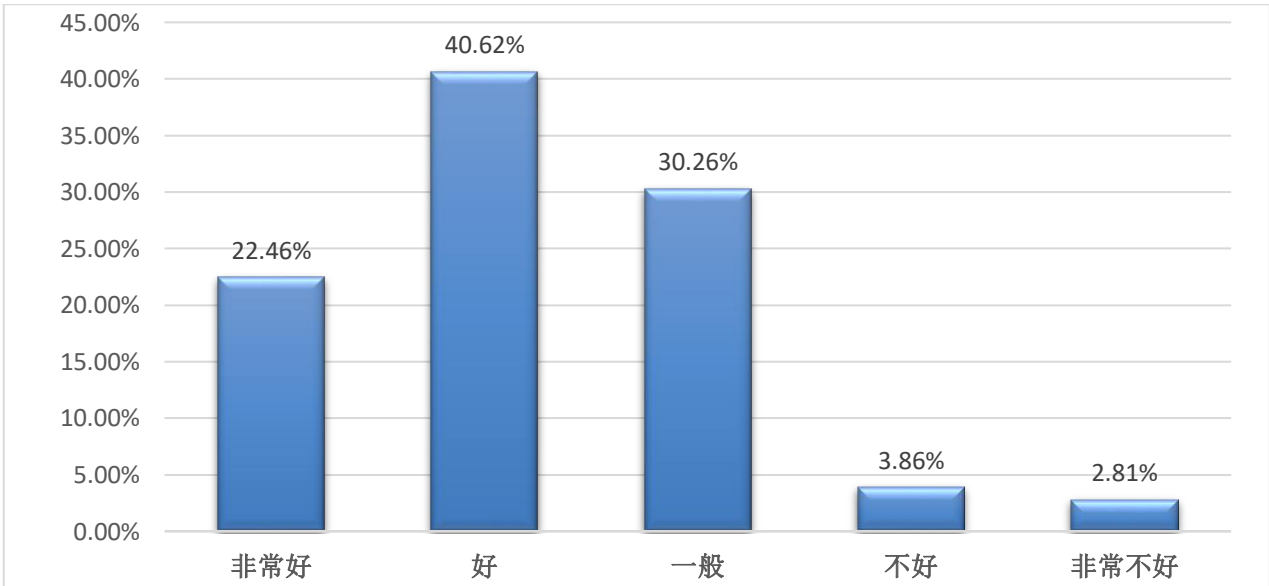


图5-4：政策环境状况

C6. 当前网络安全产品服务的需求变化状况

大部分受调查的 C 类从业人员认为网络安全产品服务需求上涨，占 81.86%（如图 5-5）。

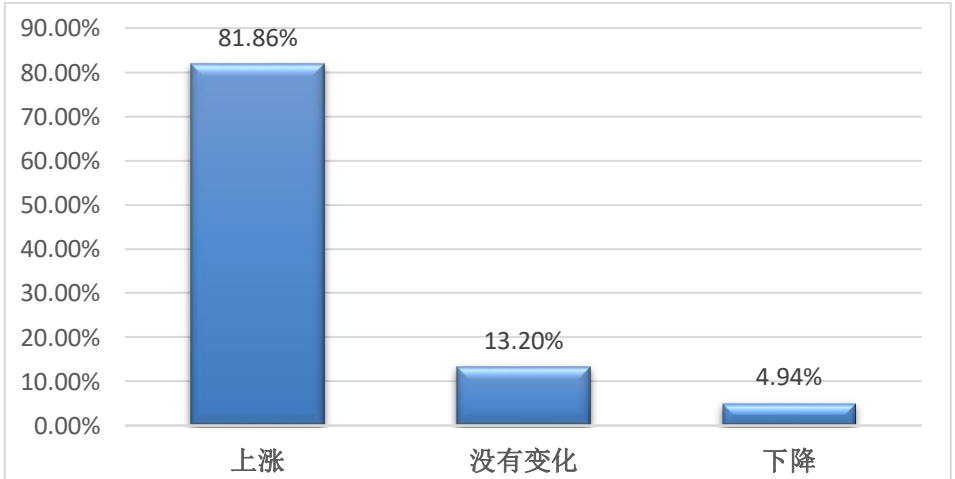


图5-5：网络安全服务产品需求

C7. 当前国内网络安全产品服务的门类是否齐全

有 55.47%的受调查 C 类从业人员认为国内网络安全产品服务门类齐全（如图 5-6）。

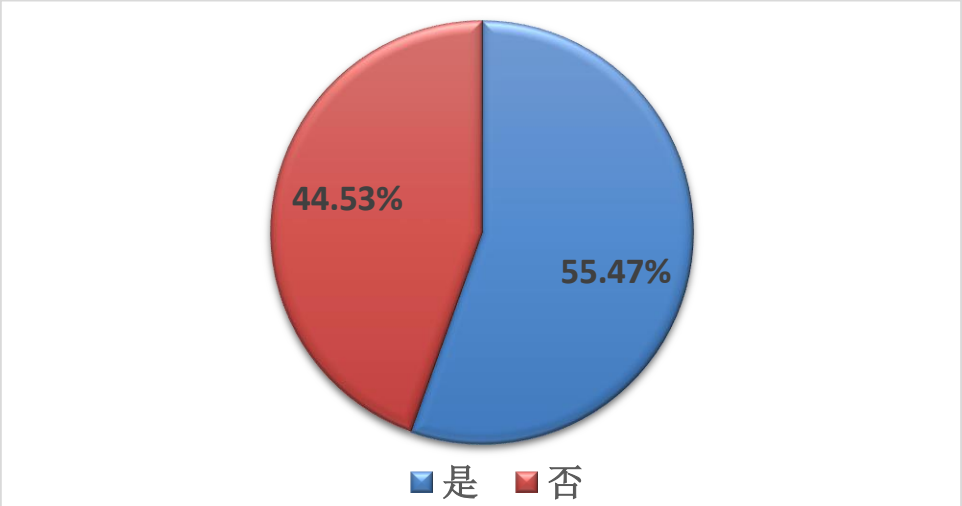


图5-6：网络安全产品服务门类是否齐全

C9. 当前网络安全产品服务是否应当划分等级

行业内对网络安全产品服务的分级管理普遍表示支持，有 90.07%的 C 类从业人员认为网络安全产品服务应该划分等级（如图 5-7）。

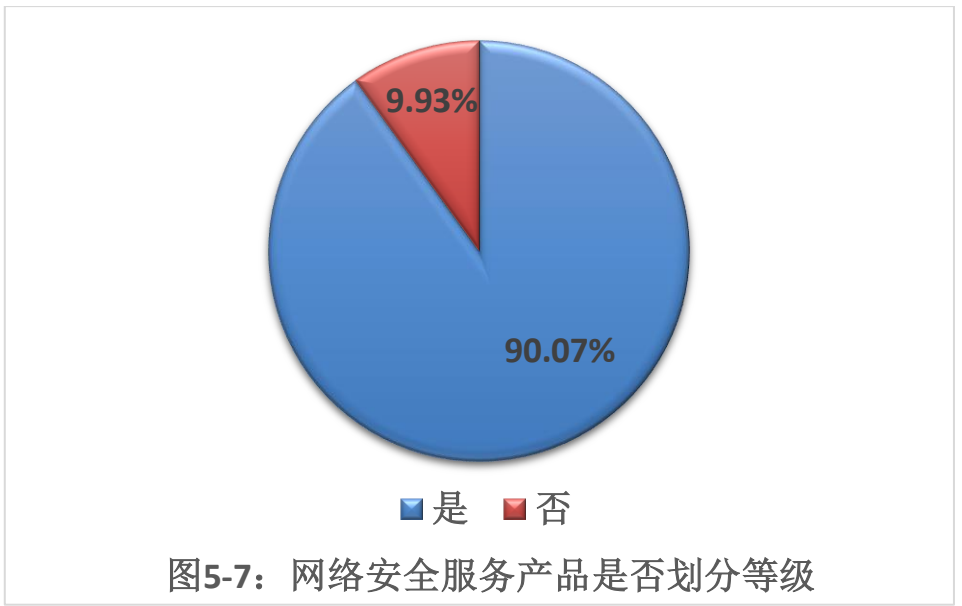


图5-7：网络安全服务产品是否划分等级

C10. 当前网络安全产品服务加强规范的方式

受调查的 C 类从业人员认为当前网络安全产品服务加强规范的主要方式是技术，有 76.79%的人员选择，其次是人才占 72.63%（如图 5-8）。

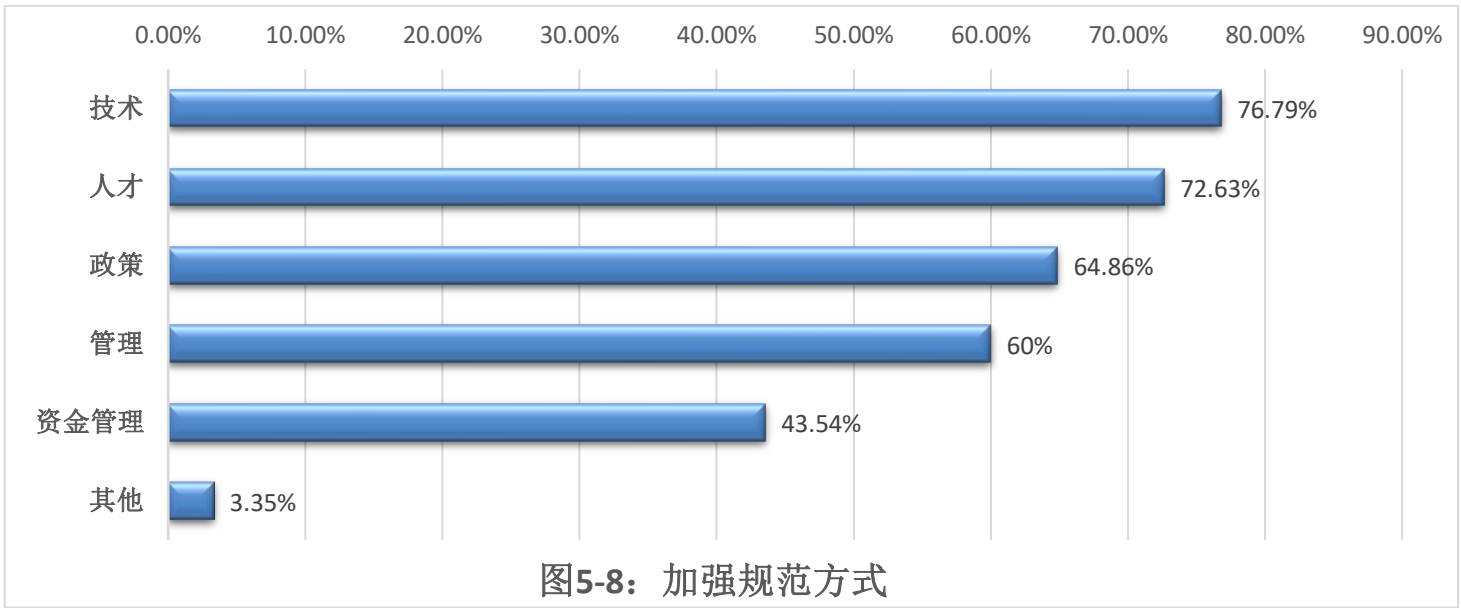


图5-8：加强规范方式

C11. 当前网络安全技术人才供应程度

受调查的 C 类从业人员认为网络安全技术人才供应充足的占 14.71%，认为一般的占 37.03%，认为有些缺乏（32.98%）和严重不足（15.28%）的合计 48.26%（如图 5-9）。

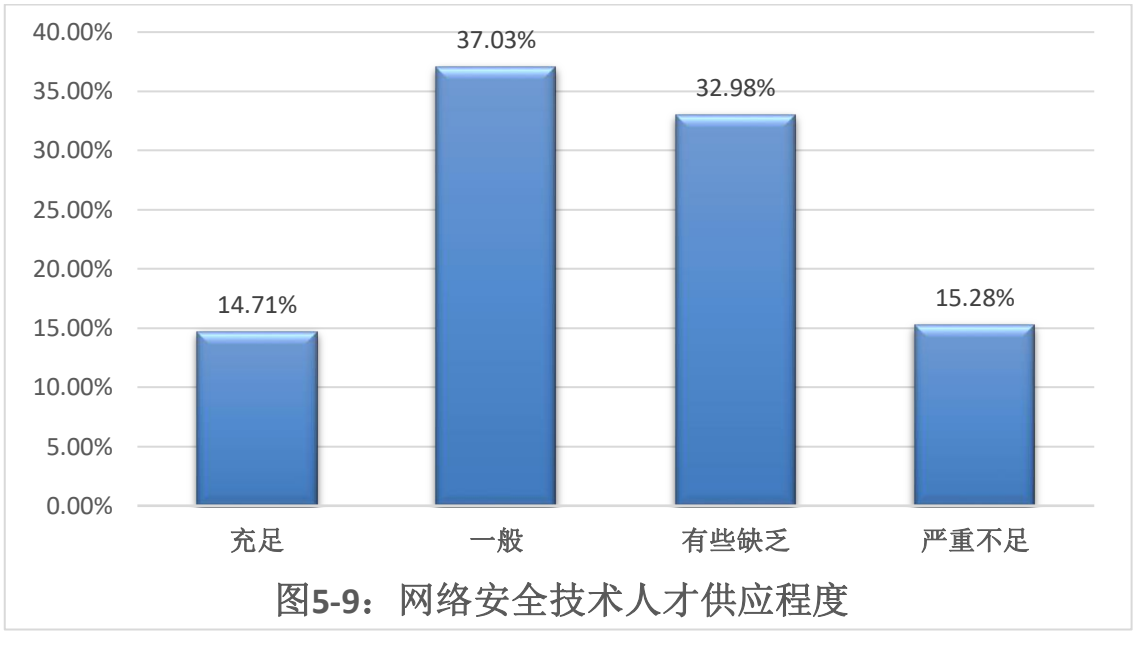


图5-9：网络安全技术人才供应程度

C12. 当前网络安全最突出的问题

受调查的 C 类从业人员认为最突出的网络安全问题是个人信息泄露，有 83.75%的人员选择，排名第二和第三的分别是网络诈骗（46.96%）、网络攻击（46.77%），各类网络安全问题占比如图 5-10 所示。

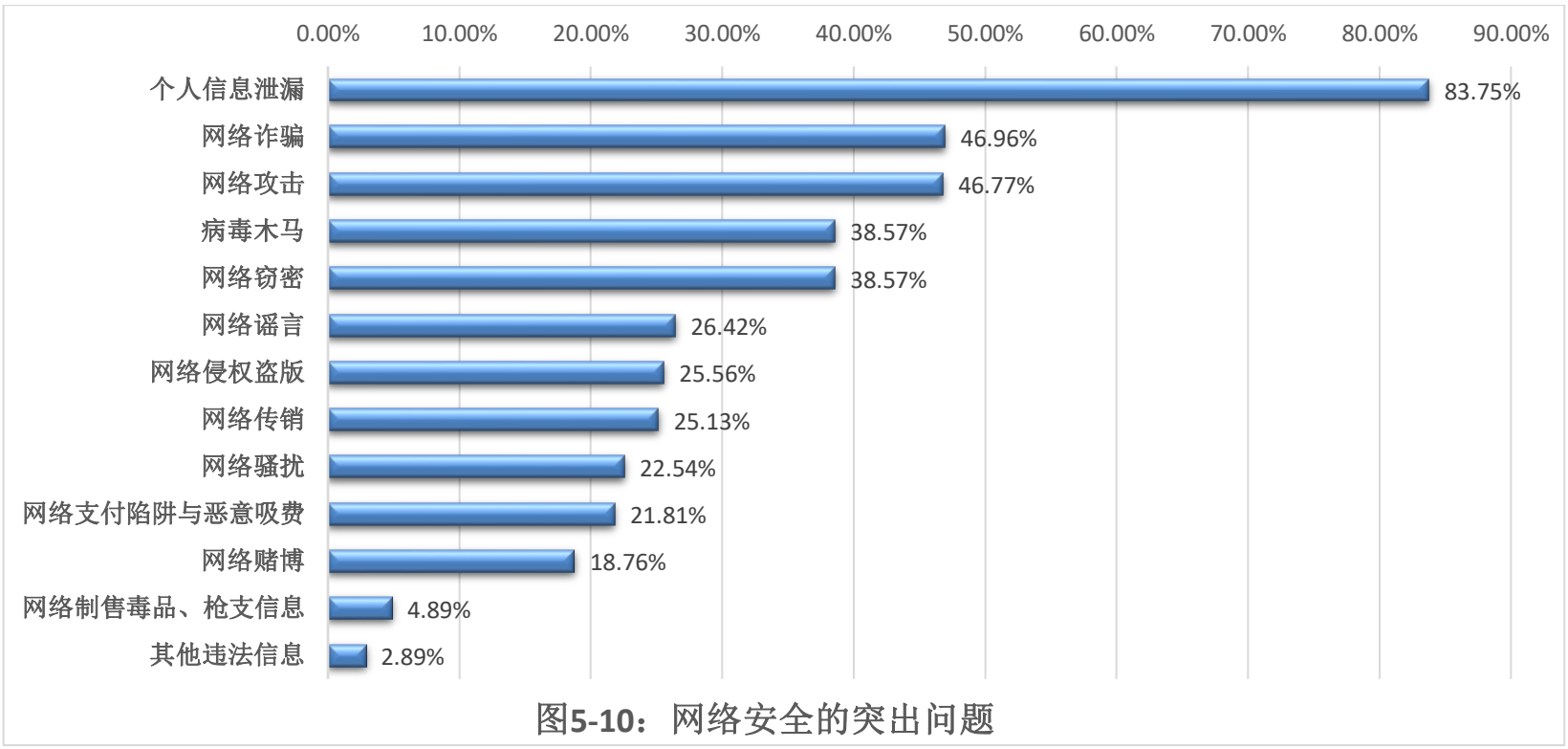


图5-10：网络安全的突出问题

C13. 对移动应用可以采取的治理方式

受调查的 C 类从业人员对移动应用认为最应该采取的治理方式前三位依次是：开发者委托第三方测试（58.27%），政府部门抽查检测（57.62%），加强网络犯罪打击（57.52%），各种治理方式的选择比例如图 5-11 所示。

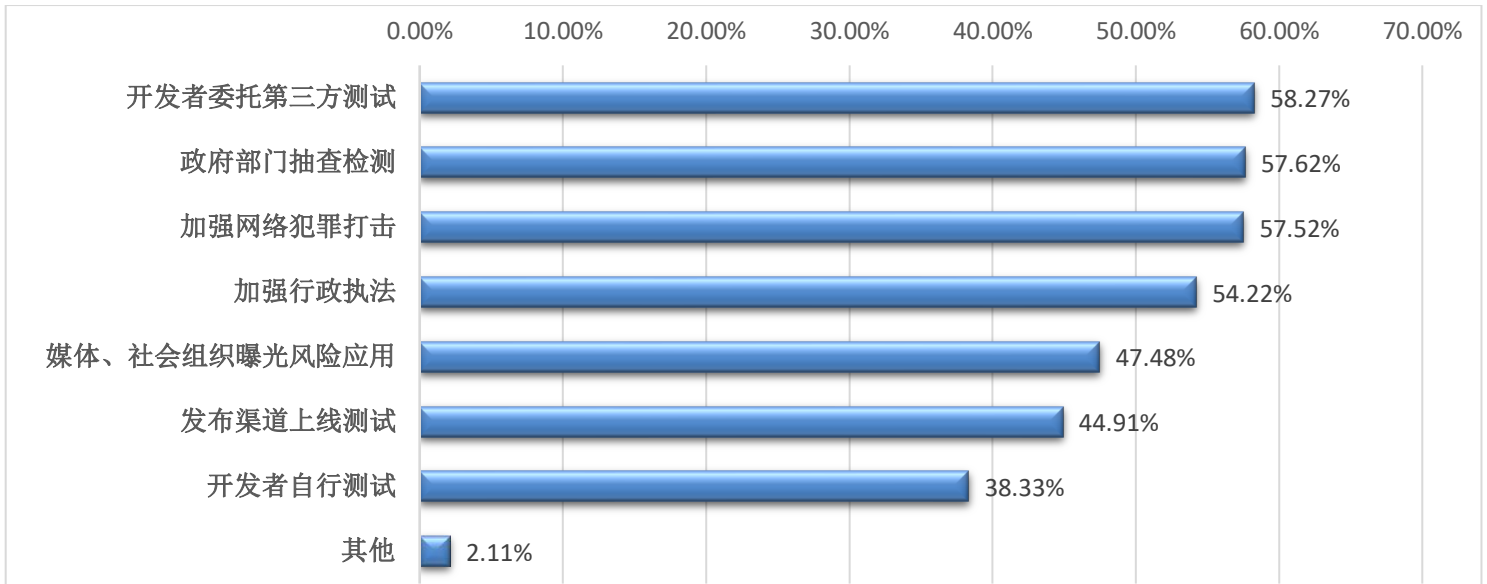


图5-11：移动应用的治理方式

C14. 移动应用不合理采集的用户信息

受调查的 C 类从业人员认为移动应用最不合理采集的用户信息是身份证号，有 68.69%的人员选择，排名第二到第五的依次是住址（60.3%）、聊天记录（59.76%）、通讯录（58.52%）、通信记录（57.89%），各类不合理采集的用户信息占比如图 5-12 所示。从整体上看，受调查网民的选择比较分散，认为不合理的用户信息采集涉及面广泛。

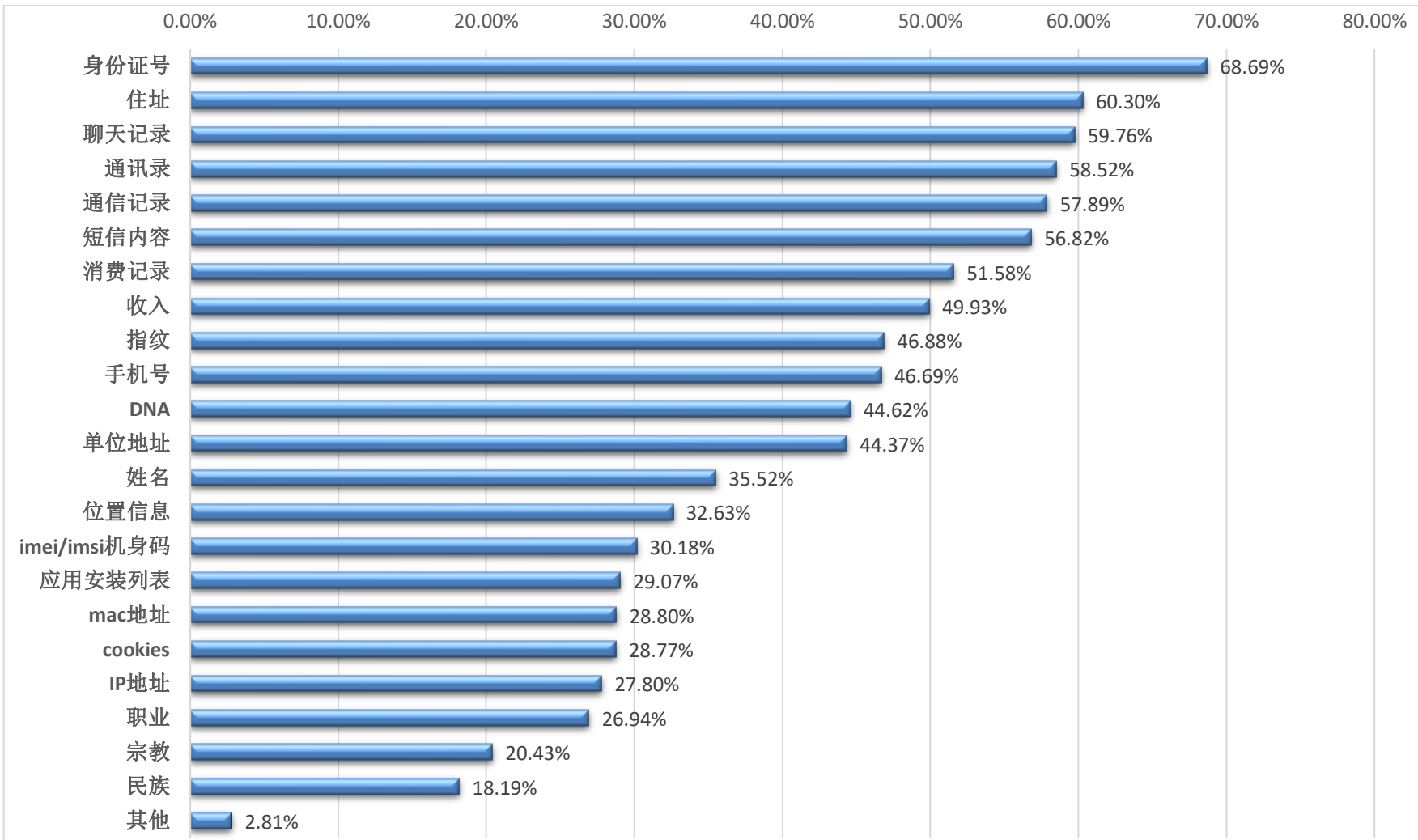


图5-12：不合理采集的用户信息

C15. 对网络安全行政执法部门的认识

受调查的 C 类从业人员认为政府最主要的网络安全执法部门前三位依次是网信（77.77%）、公安（74.64%）、工信（46.96%），如图 5-13 所示。

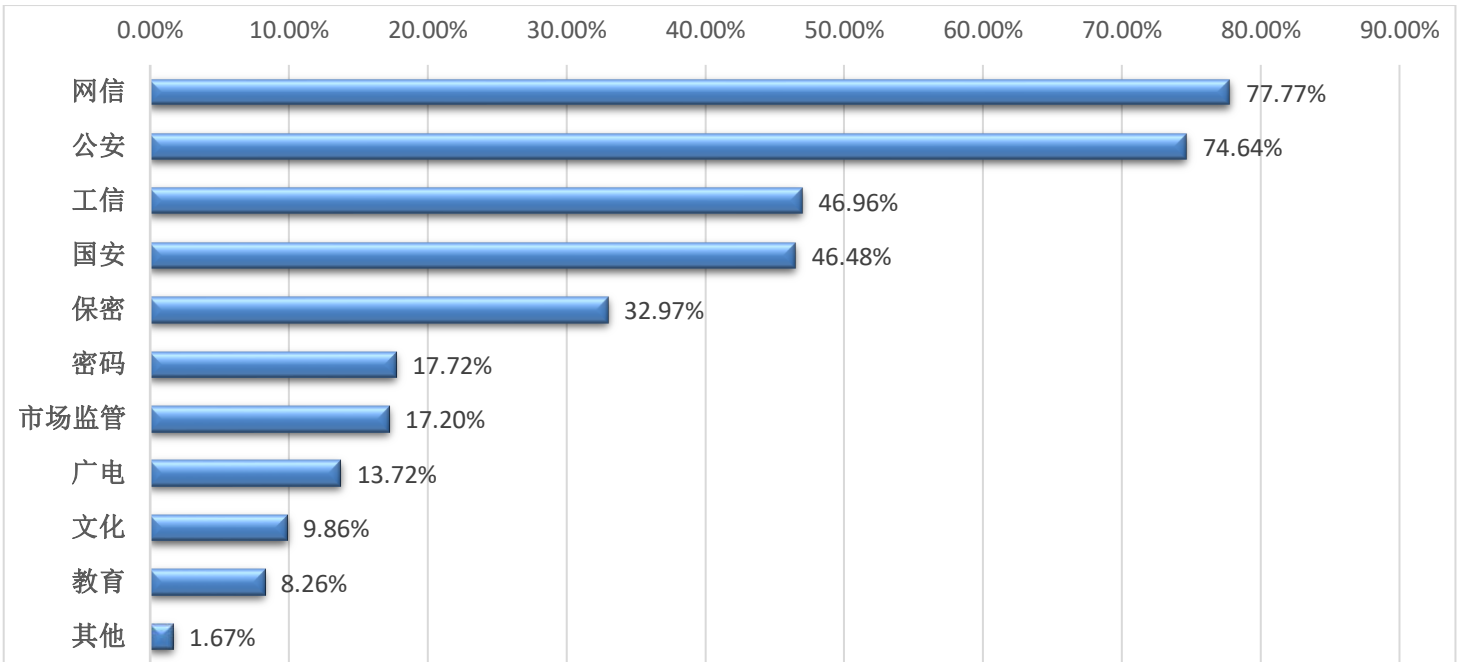


图5-13：政府网络安全执法部门

C15.1、政府部门在网络安全方面的执法力度评价

受调查的 C 类从业人员认为政府部门在网络安全方面的执法力度强的有 15.86%，认为比较强的有 30.69%，两者合计 46.55%；认为不足或严重不足的合计 17.44%（如图 5-14）。

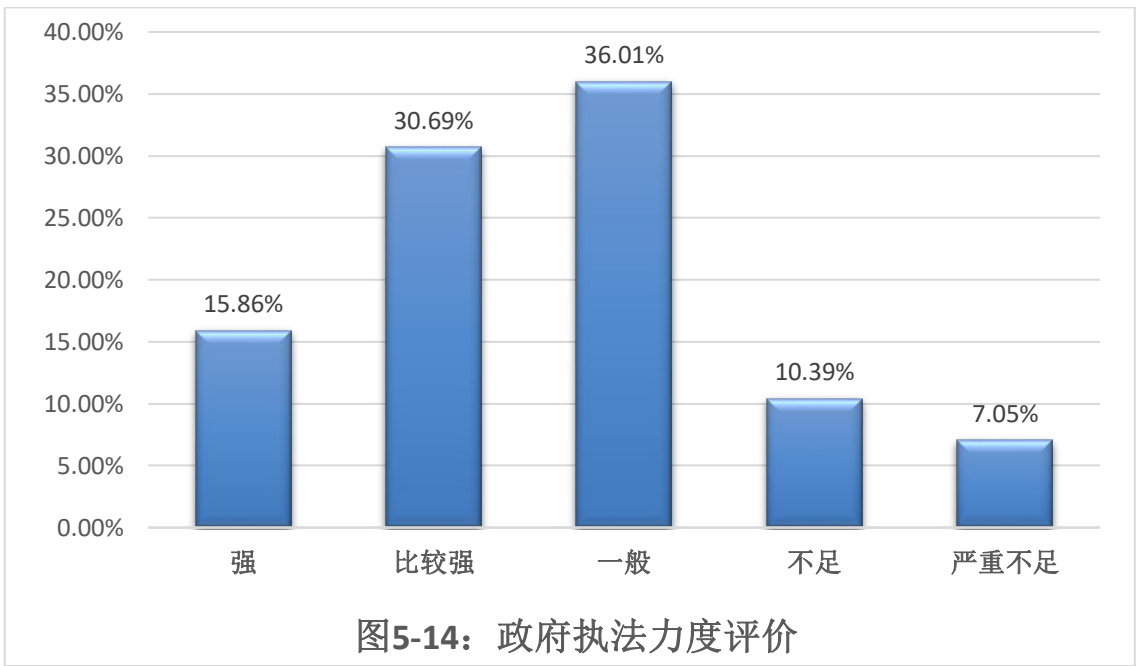


图5-14：政府执法力度评价

C15.2、网络安全执法的制约因素

受调查的 C 类从业人员认为影响网络安全执法的制约因素前三位的是：检测能力（59.56%）、人员（58.48%）、取证能力（58.32% ），各类制约因素占比如图 5-15 所示。

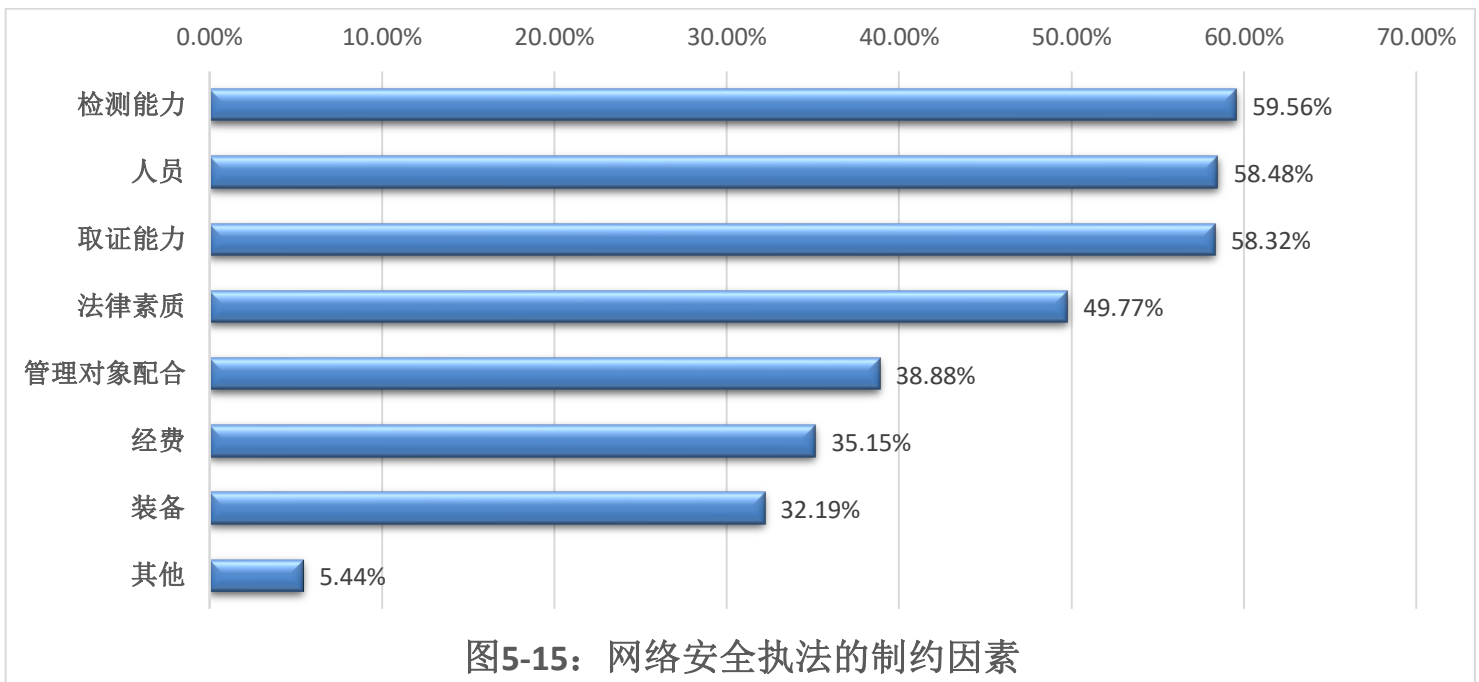


图5-15：网络安全执法的制约因素

C16. 亟待加强的网络安全立法内容

受调查的 C 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 76.45%，网络平台责任占 64.38%，数据安全保护占 63.17%（如图 5-16）。

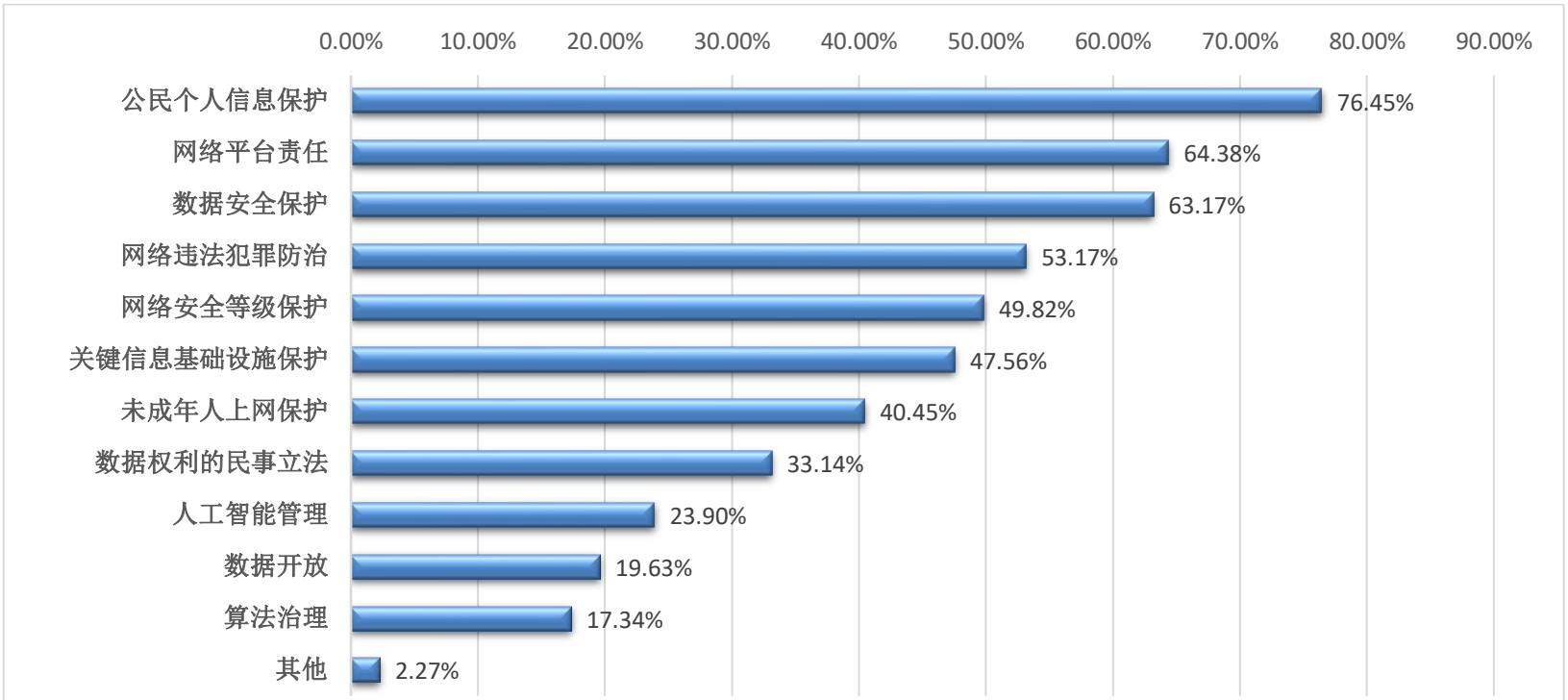


图5-16：亟待加强的立法内容

C17. 对网络安全等级保护制度 2.0 国家标准要求的了解

大部分受调查的 C 类从业人员了解网络安全等级保护制度 2.0 国家标准的要求，了解的比例占 59.71%（如图 5-17）。

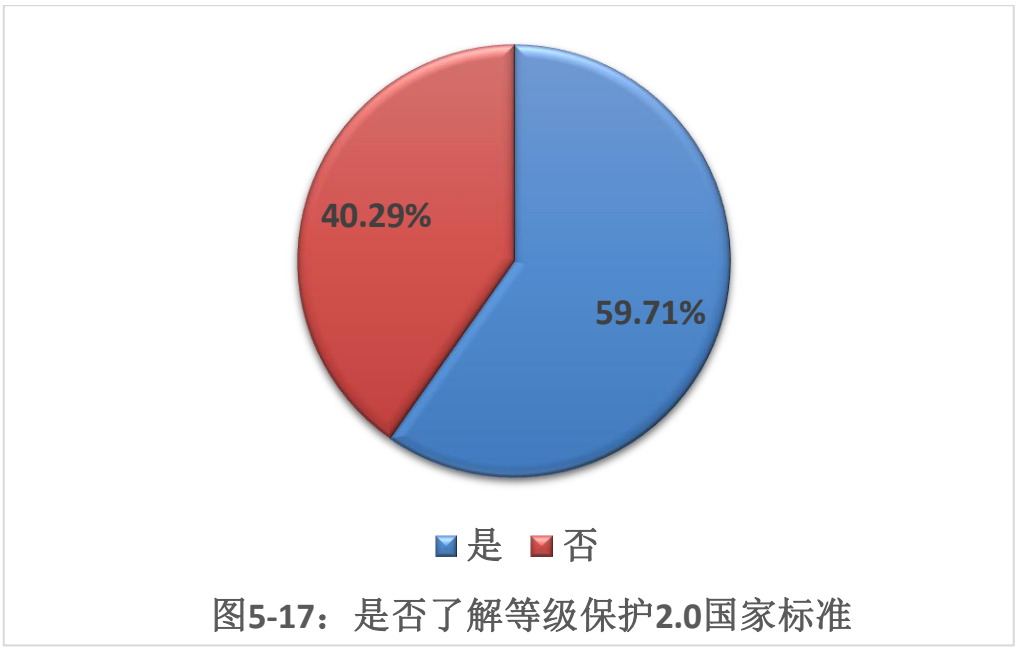


图5-17：是否了解等级保护2.0国家标准

C17.1、等保 2.0 的了解渠道

行业论坛是受调查的 C 类从业人员了解等保 2.0 标准的主要渠道，占比 60.08%，其次为单位或政府组织的培训（52.35%），如图 5-18 所示。

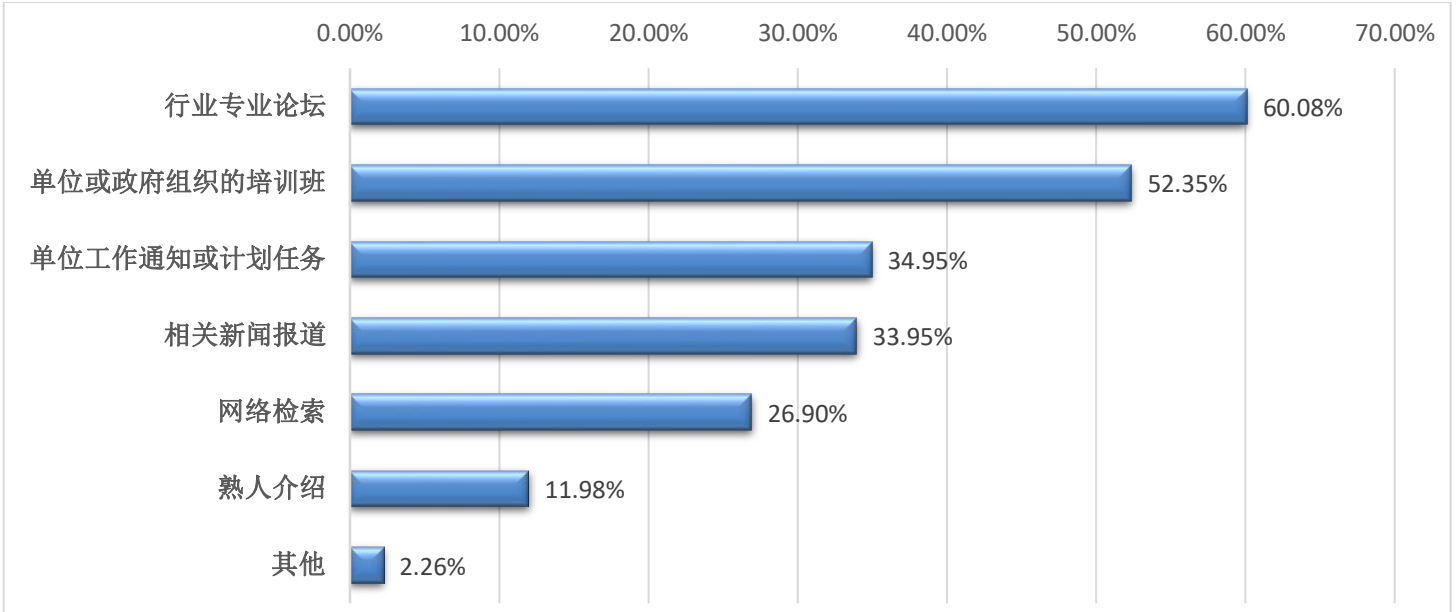


图5-18：等保2.0了解渠道

C18. 网络安全等级保护对产业、企业发展的推动作用的认识

受调查的 C 类从业人员对网络安全等级保护的作用认识比较正面，有 64.41%的人员认为网络安全等级保护对产业、企业发展的推动很大（如图 5-19）。

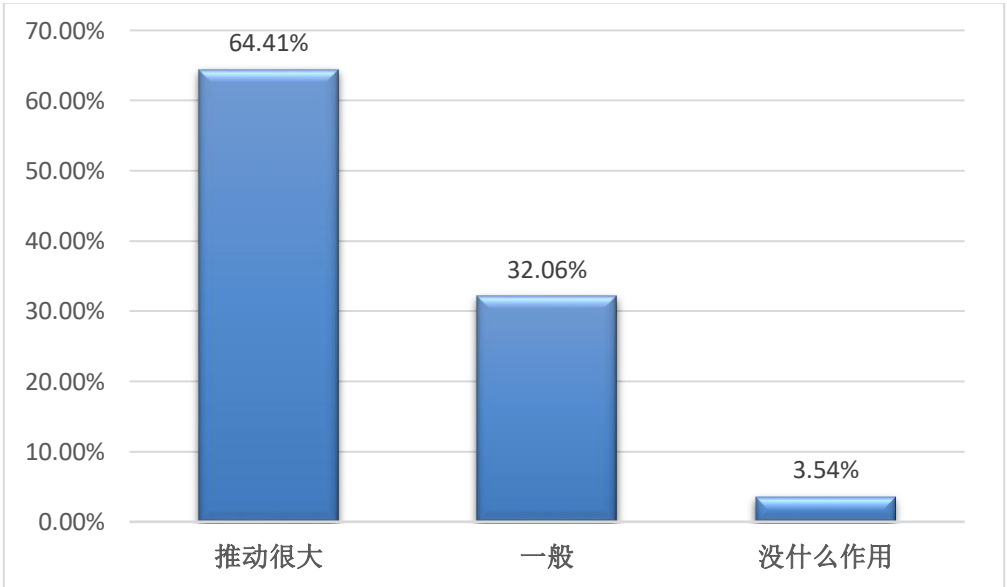


图5-19：网络安全等级保护作用认识

六、D 卷：网络行业协会的从业人员

网络行业协会（D 类）的从业人员对网络行业情况比较熟悉，态度比较平和。

D 类问卷有效问卷的数量为 915 份，以下是 D 类问卷各项数据的详细统计结果。

D3. 当前网络安全状况

受调查的 D 类从业人员认为网络安全状况良好的最多，有 42.95% 的人员选择，认为状况一般的占 41.2%，认为状况堪忧的占 15.85%（如图 6-1）。

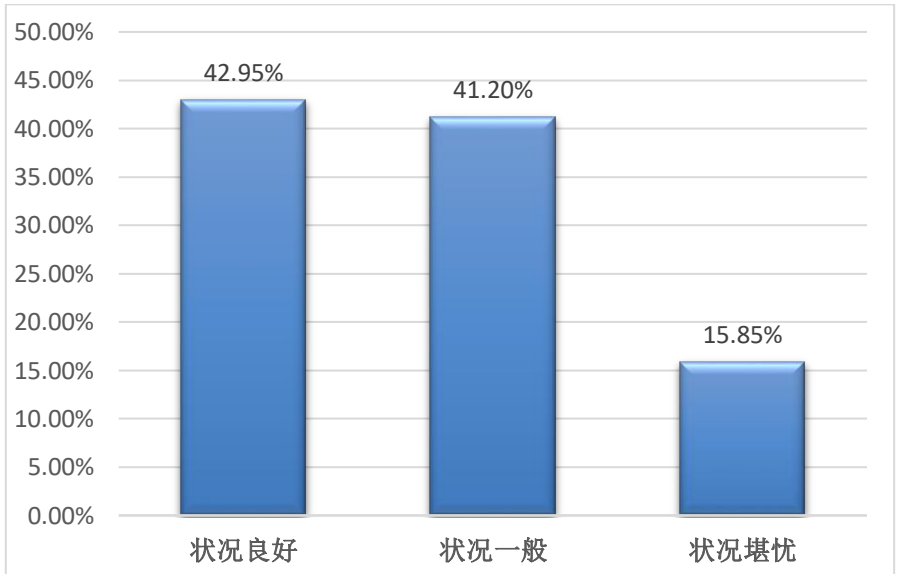


图6-1：安全状况评价

D3.1、与去年相比网络安全感的变化

绝大部分受调查的 D 类从业人员认为当前网络安全状况改善，有 30.16%的人员认为明显改善，有 41.64% 的人员认为有改善，两者合计有 71.8%的人员认为网络安全状况改善或明显改善（如图 6-2）。

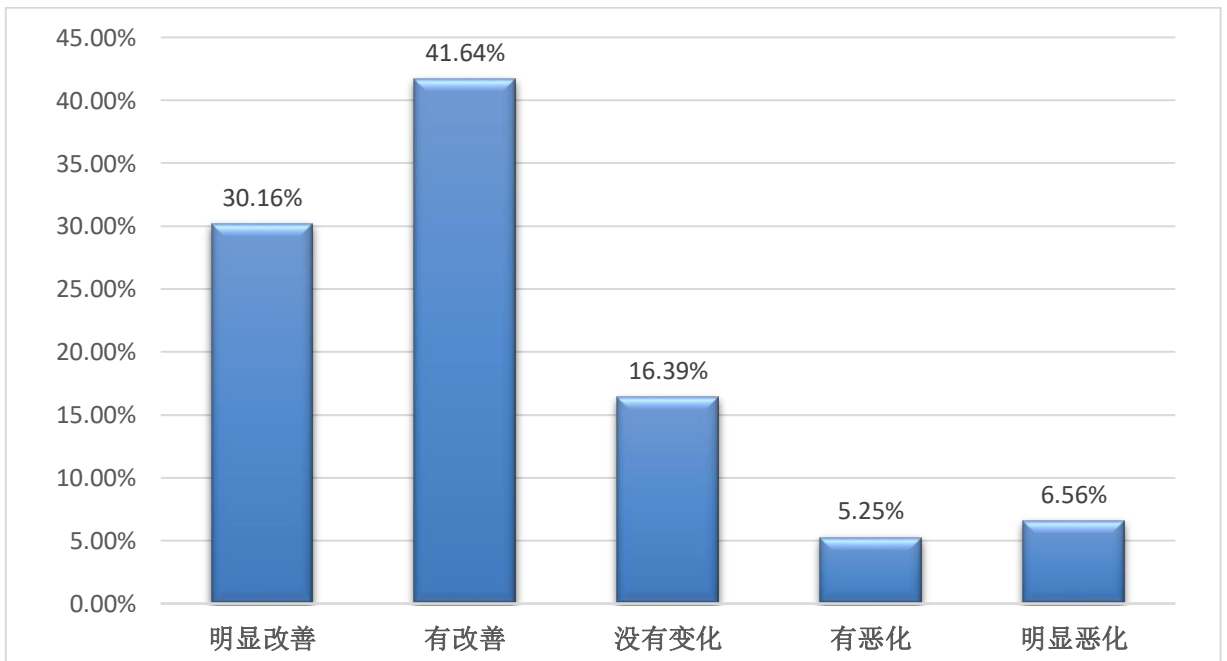


图6-2：网络安全感变化评价

D4. 网络服务提供者的管理措施对于保证网络安全水平的有效程度

受调查的 D 类从业人员有 29.07%认为非常有效，有 33.55%认为比较有效，两者合计共有 62.62%的人员认为非常有效和比较有效（如图 6-3）。

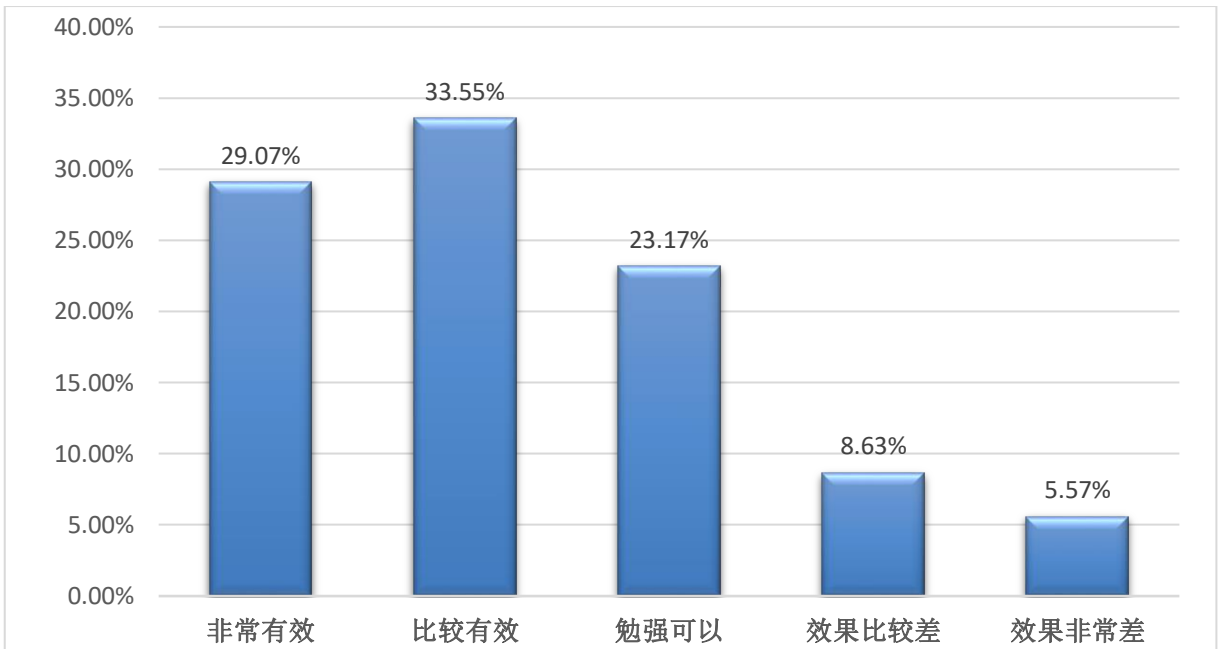


图6-3：管理措施有效程度

D5.政府网络安全管理政策措施对网络服务提供者和联网使用单位的影响

受调查的 D 类从业人员认为政府网络安全管理措施，对网络服务提供者和联网使用单位影响最大的前三位依次是提高了意识（62.3%）、建立了组织体系（41.31%）、提高了风险防控水平（40.44%），各类影响占比如图 6-4 所示。

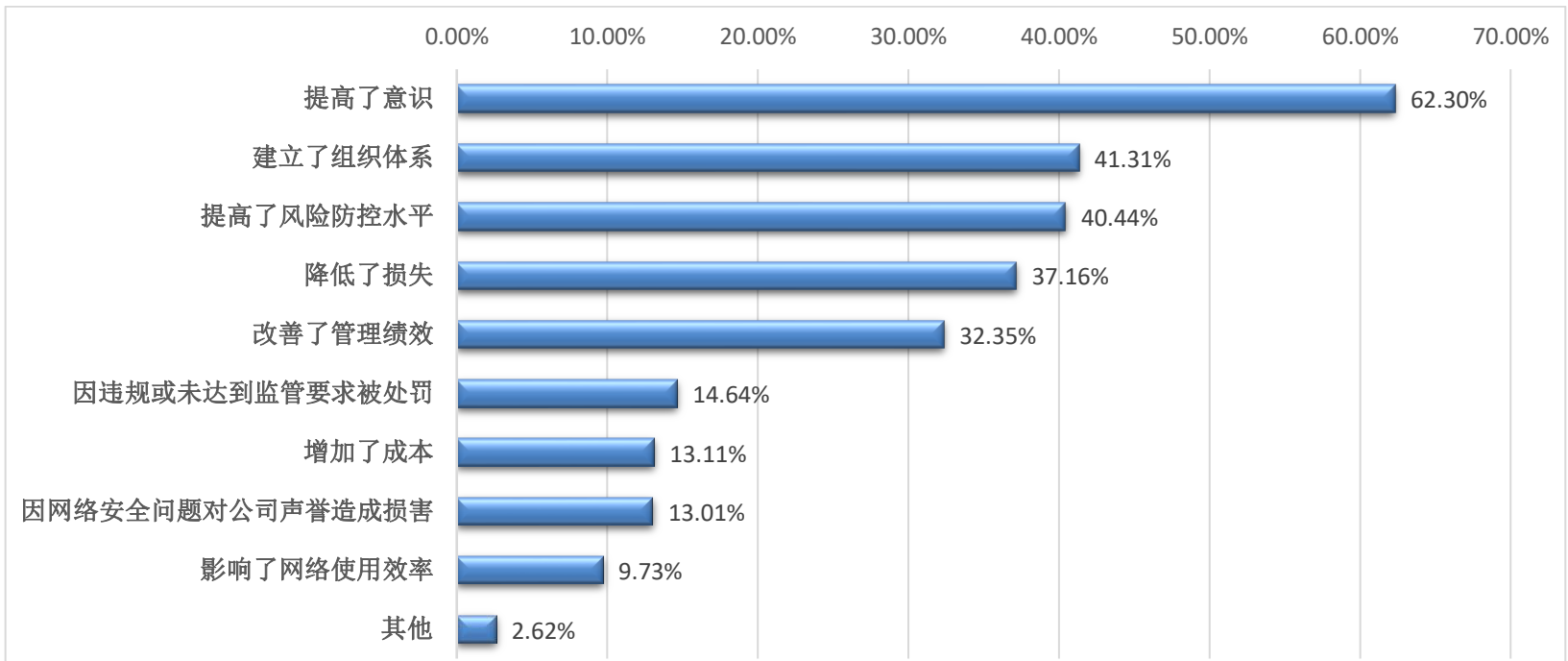


图6-4：政府政策措施对单位的影响

D6.当前网络安全最突出的问题

受调查的 D 类从业人员认为最突出的网络安全问题是个人信息泄露，有 65.46%的人员选择，排名第二和第三的分别是网络攻击（40.44%）、网络诈骗（38.36%），各类网络安全问题占比如图 6-5 所示。

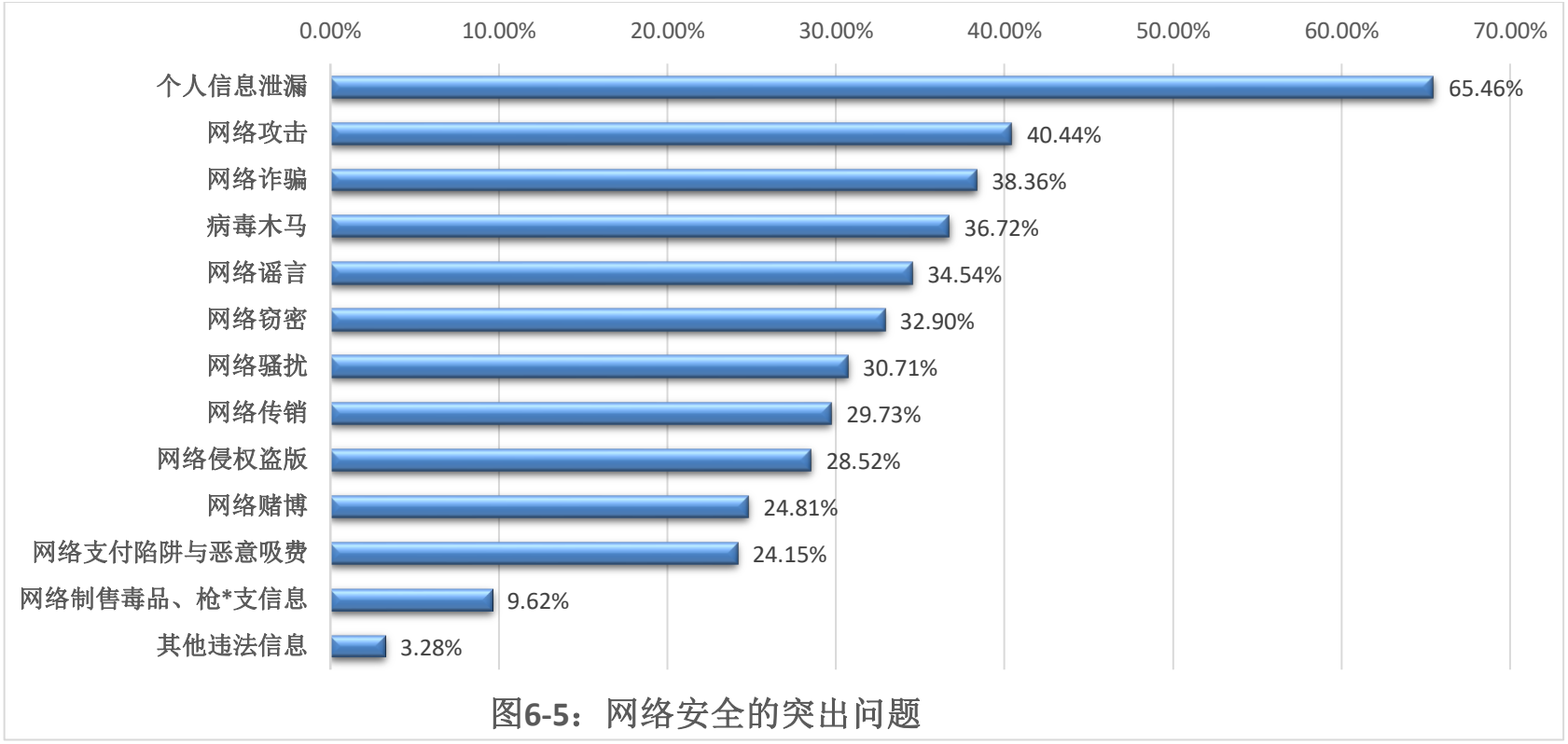


图6-5：网络安全的突出问题

D7. 安全问题较多网络应用或服务

受调查的 D 类从业人员认为安全问题最多的网络应用或服务前五位依次是：在线视频（37.92%），网络游戏（29.95%），网络直播（28.96%），短视频（27.43%），网络购物（23.61%），如图 6-6 所示。

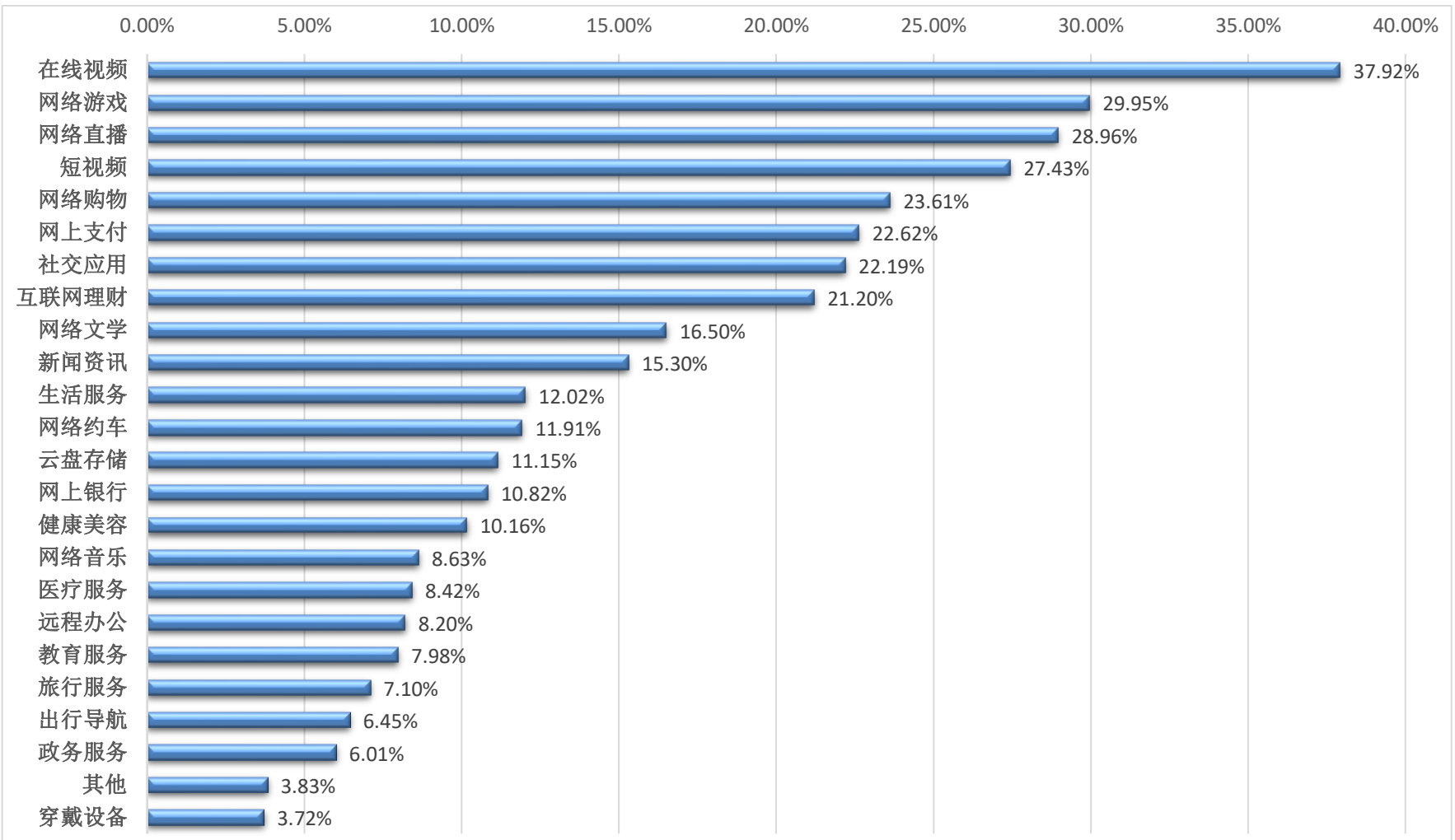


图6-6：安全问题多的网络应用或服务

D8. 当前我国个人信息保护状况

受调查的 D 类从业人员认为当前我国个人信息保护状况非常好的占 22.08%，比较好的占 22.19%，两者合计 44.27%（如图 6-7）。

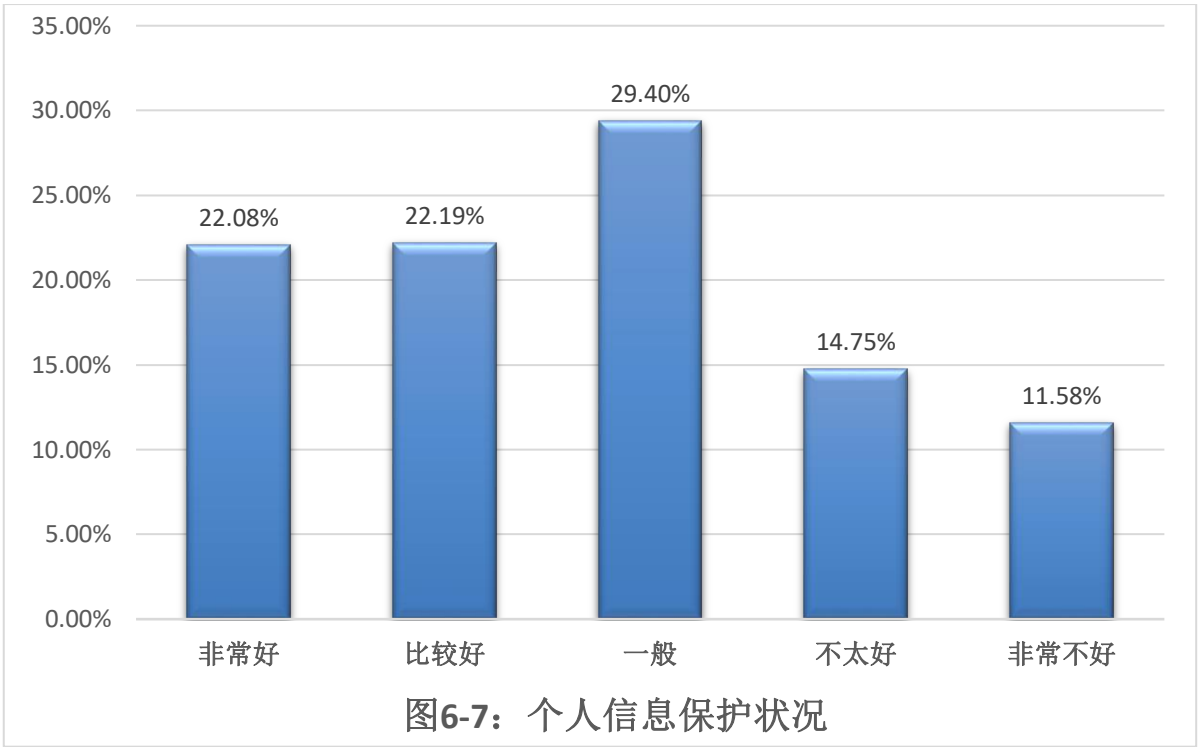


图6-7：个人信息保护状况

D8.1、个人信息保护可以在哪些方面加强

受调查的 D 类从业人员认为个人信息保护最应该加强的方面是犯罪打击，有 60.17%的人员选择，其次有 52.28%的人员选择行政执法（如图 6-8）。

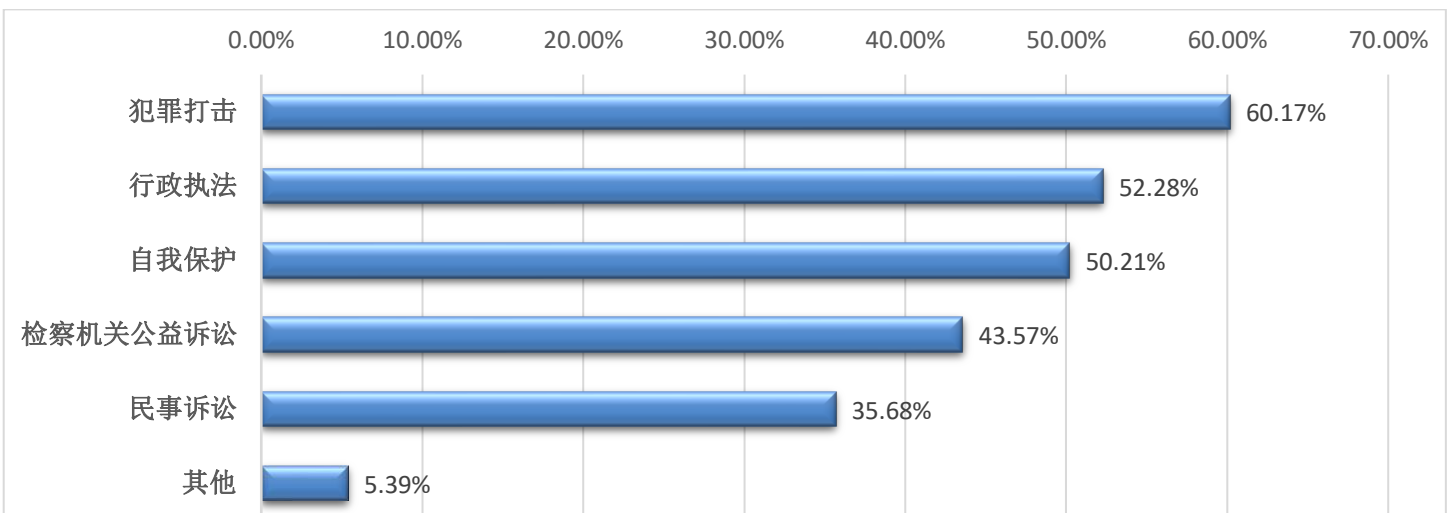


图6-8：个人信息保护应在哪些方面加强

D9. 整治网络黑灰产业链条关键点

受调查的 D 类从业人员中有 56.17%认为治理网络黑灰产业链条最关键的是信息链条（如图 6-9）。

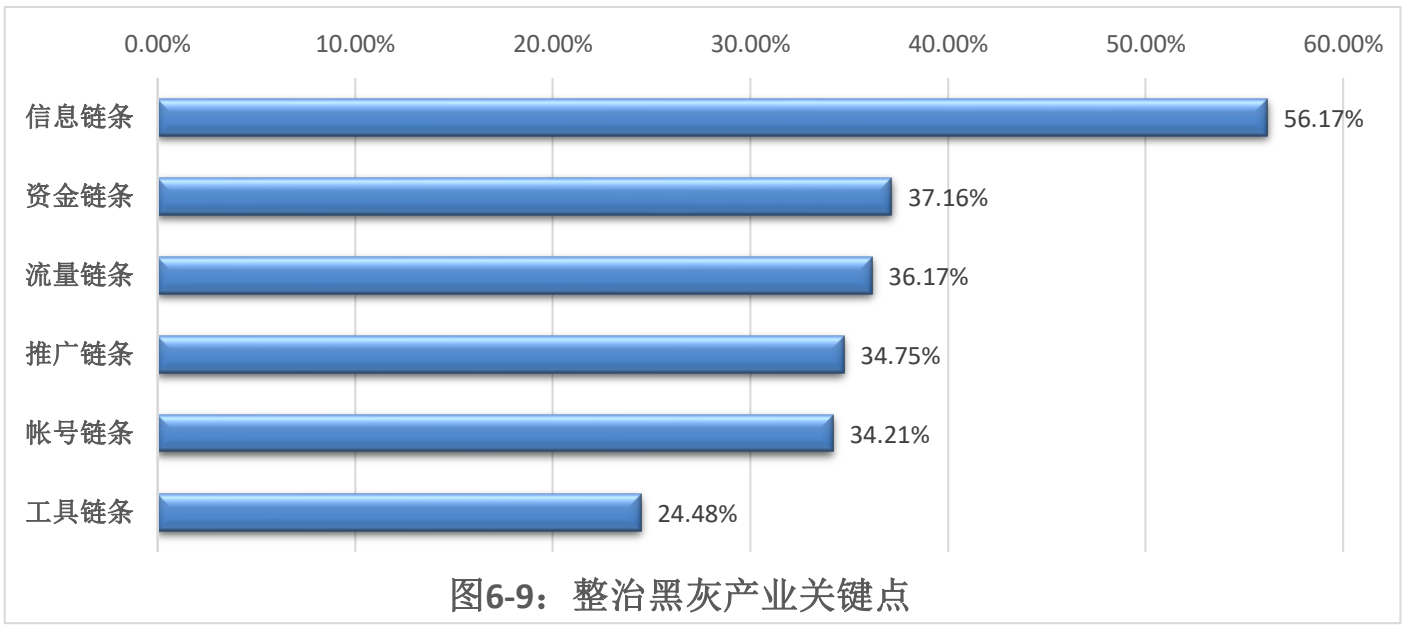


图6-9：整治黑灰产业关键点

D10. 对网络安全行政执法部门的认识

受调查的 D 类从业人员认为政府最主要的网络安全执法部门前三位依次是网信（57.05%）、公安（50.16%）、工信（31.04%），如图 6-10 所示。

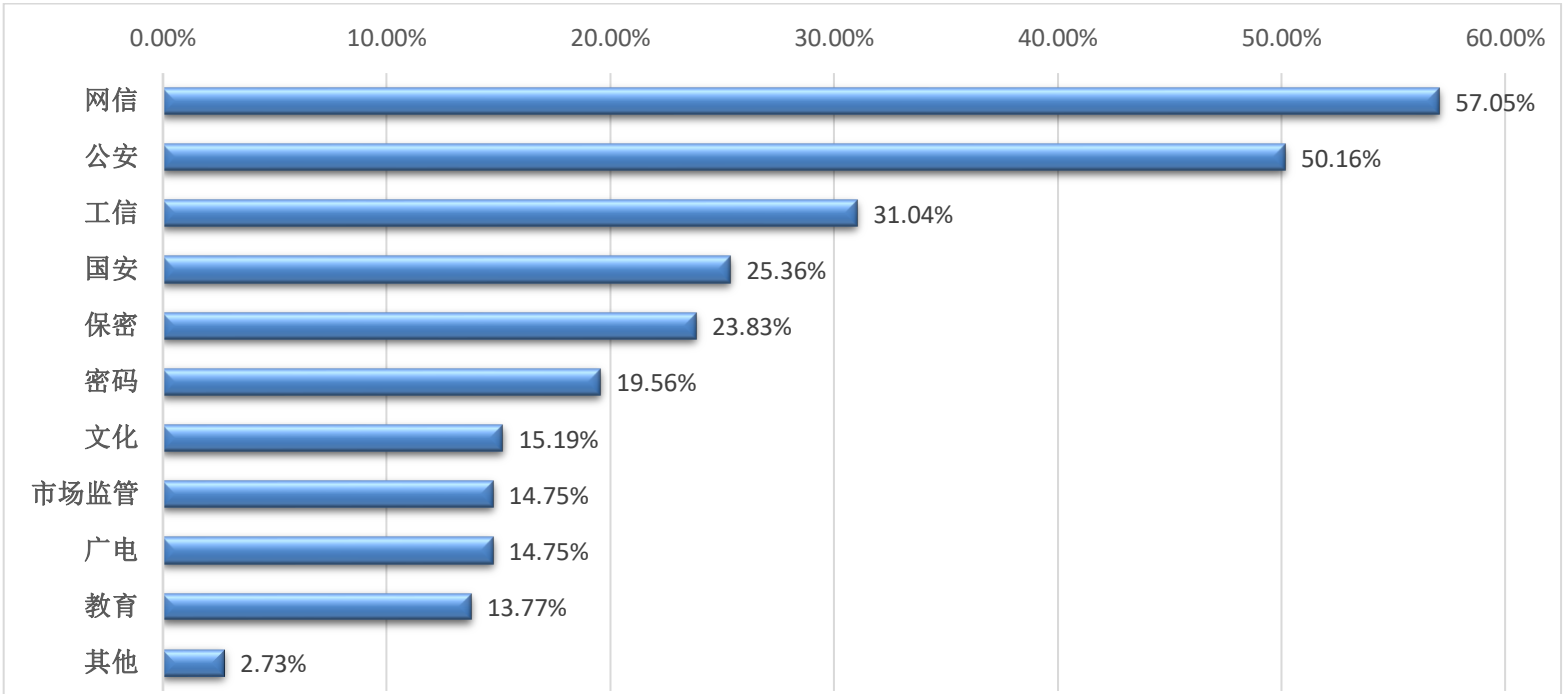


图6-10：政府网络安全执法部门

D10.1、政府部门在网络安全方面的执法力度评价

受调查的 D 类从业人员认为政府部门在网络安全方面的执法力度强的有 21.72%，认为比较强的有 29.26%，两者合计 50.98%；认为不足或严重不足的合计 17.36%（如图 6-11）。

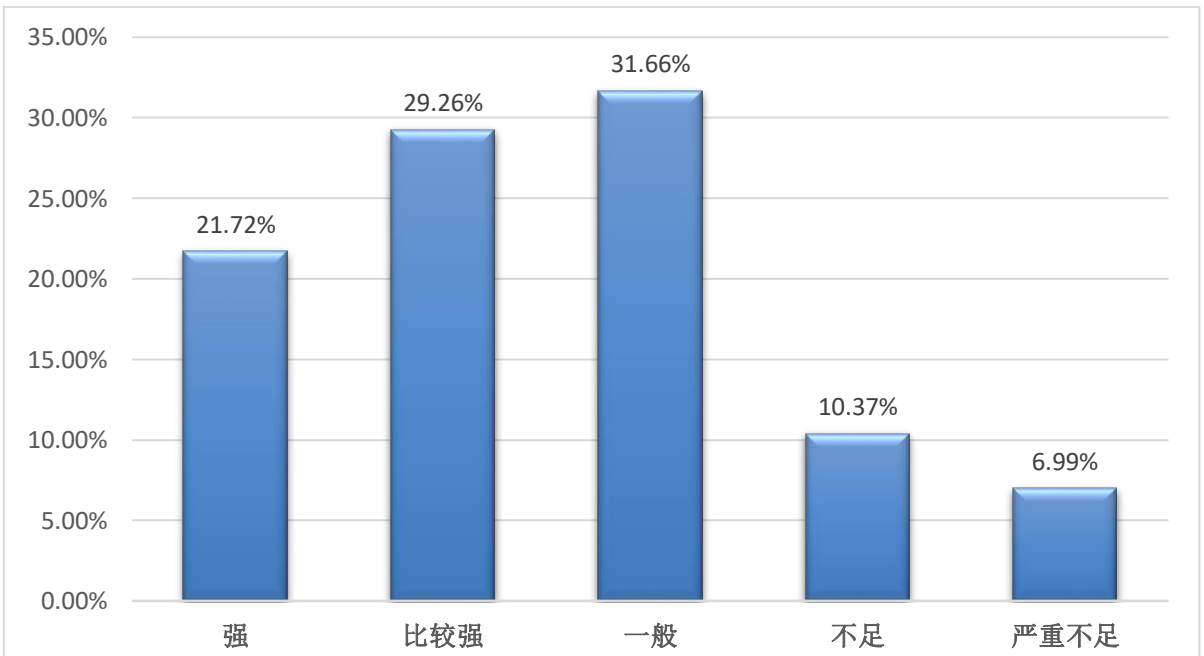


图6-11：政府执法力度评价

D10.2、网络安全执法制约因素

受调查的 D 类从业人员认为影响网络安全执法的制约因素前三位的是：法律素质（50.31%）、取证能力（47.8% ）、检测能力（42.14%），各类制约因素占比如图 6-12 所示。

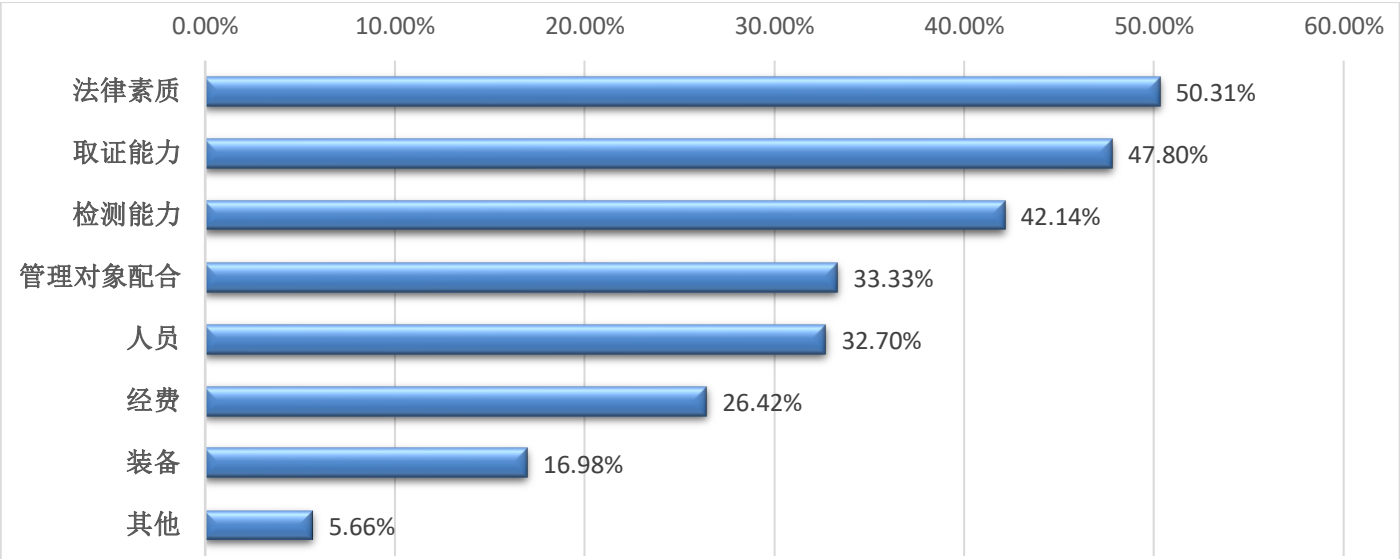


图6-12：网络安全执法的制约因素

D11. 亟待加强的网络安全立法内容

受调查的 D 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 56.07%，网络平台责任占 51.8%，数据安全保护占 42.51%（如图 6-12）。

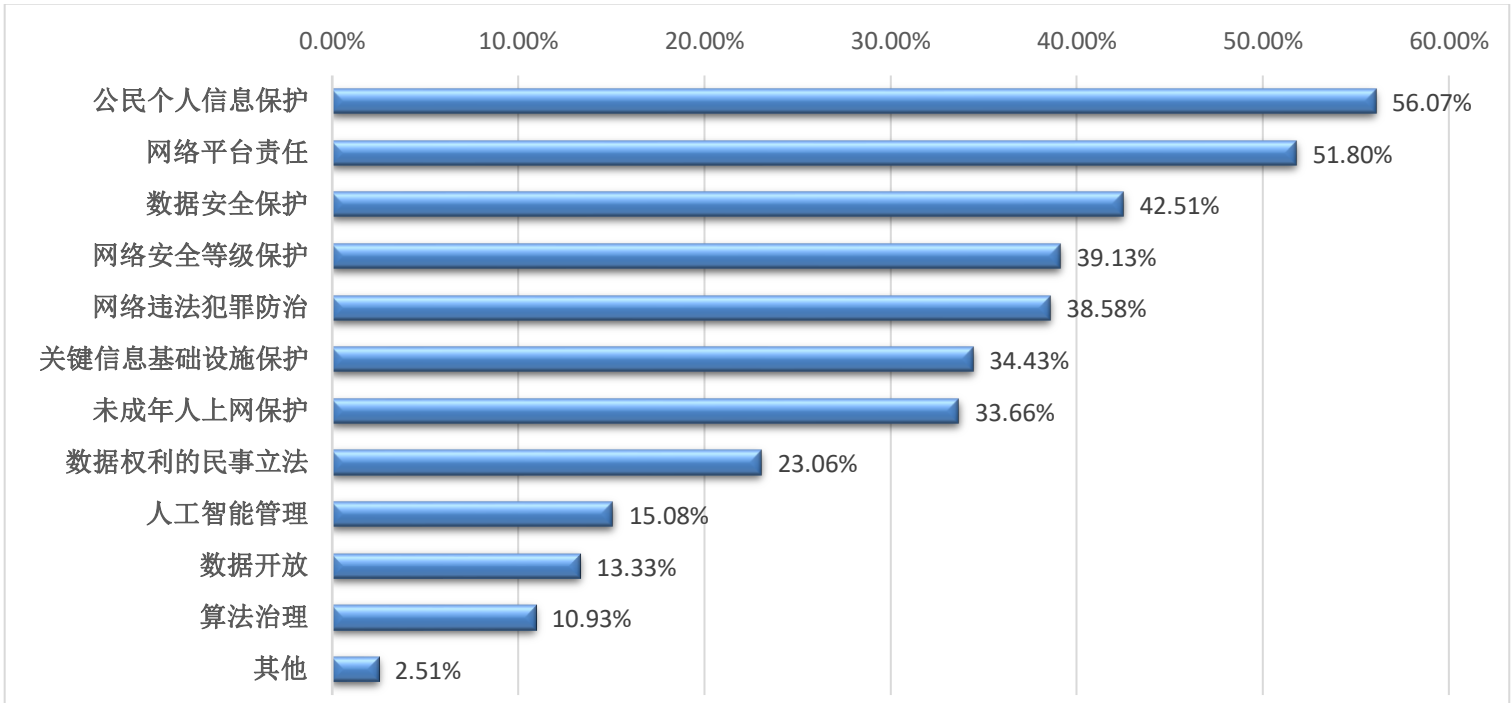


图6-13：亟待加强的立法内容

D12. 您网络安全等级保护对提升我国网络安全保护水平的作用

受调查的 D 类从业人员对网络安全等级保护的作用认识比较正面，有 60.44%认为对提升我国网络安全保护水平很有促进（如图 6-14）。

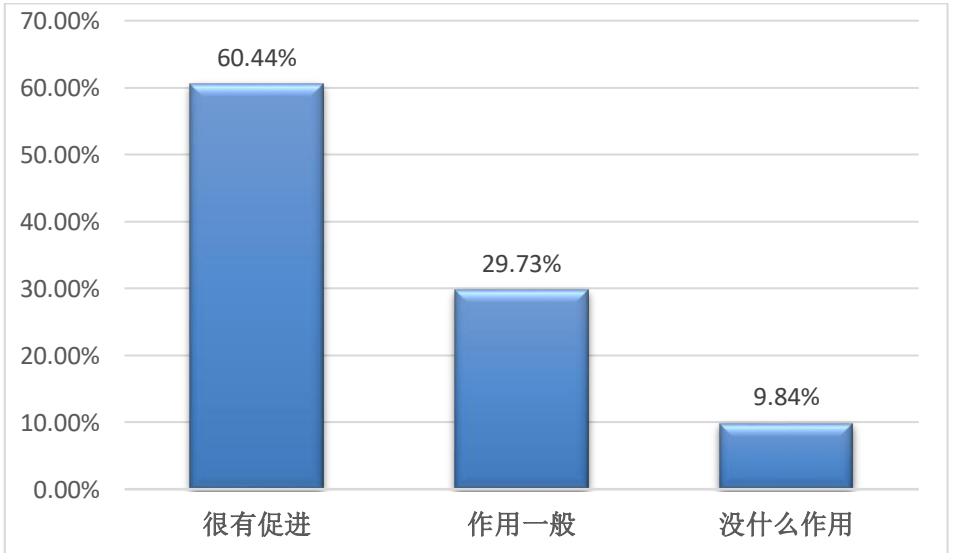


图6-14：网络安全等级保护作用认识

七、E 卷：政府网络安全监督管理部门的从业人员

政府网络安全监督管理部门（E 类）的从业人员对政府政策要求比较熟悉。

E 问卷有效问卷数量 1027 份，以下是 E 类问卷各项数据的详细统计结果。

E3. 当前网络安全状况

受调查的 E 类从业人员认为网络安全状况良好的最多，有 45.57% 的人员选择，认为状况一般的占 40.51%，认为状况堪忧的占 13.92%（如图 7-1）。

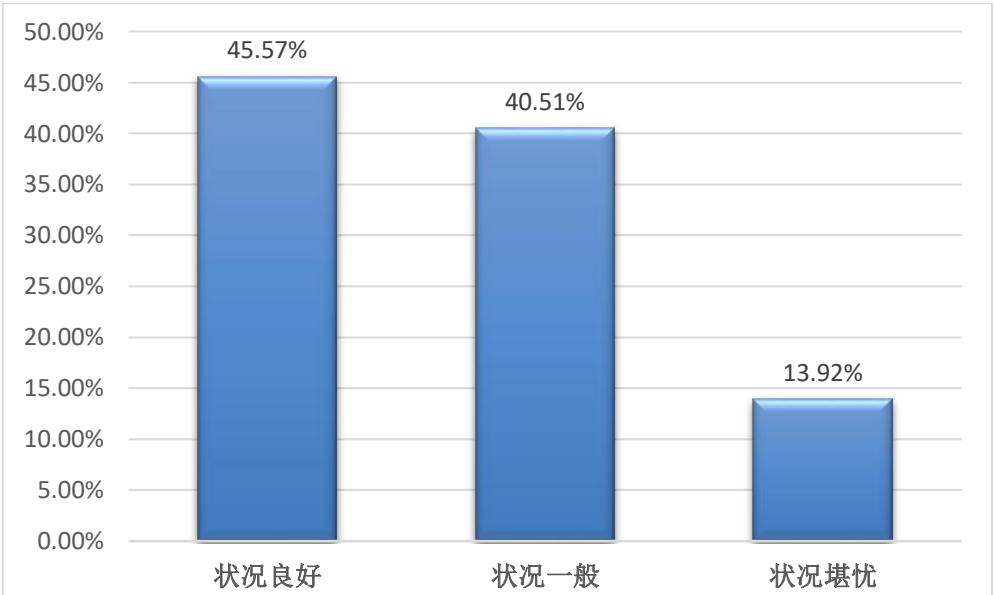


图7-1：安全状况评价

E3.1、与去年相比网络安全感的变化

绝大部分受调查的 E 类从业人员认为当前网络安全状况改善，有 34.27%的人员认为明显改善，有 46.15% 的人员认为有改善，两者合计有 80.42%的人员认为网络安全状况改善或明显改善（如图 7-2）。

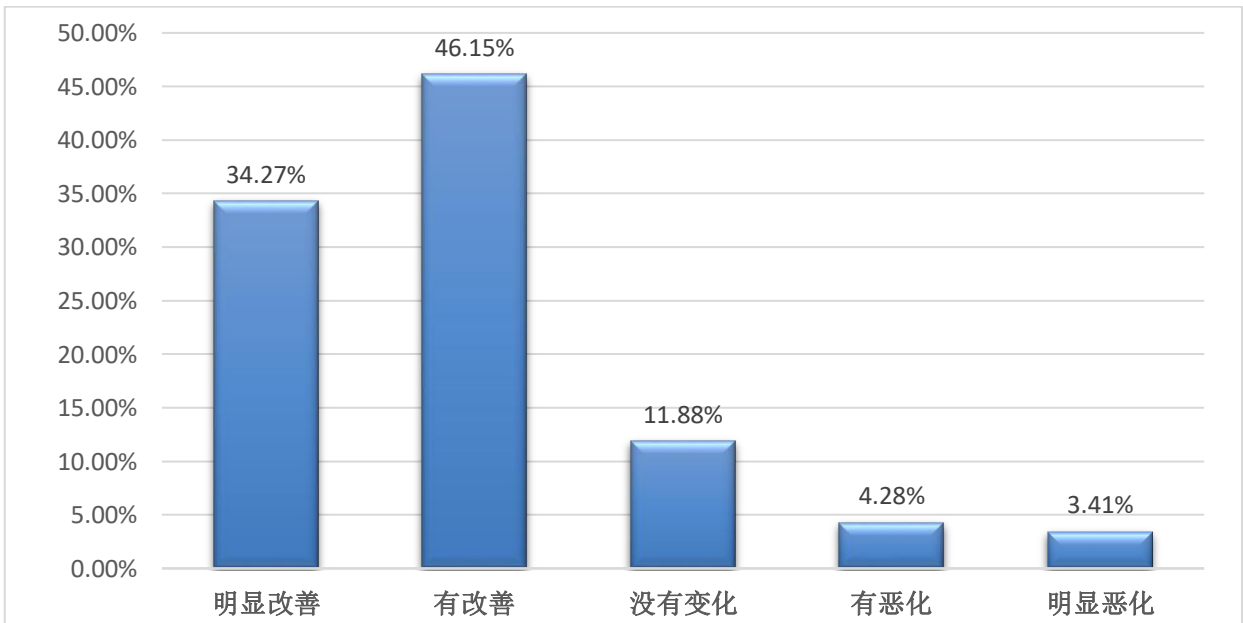


图7-2：网络安全感变化评价

E4. 网络服务提供者的管理措施对于保证网络安全水平的有效程度

受调查的 E 类从业人员有 26%认为非常有效，有 40.99%认为比较有效，两者合计共有 66.99%的人员认为非常有效和比较有效（如图 7-3）。

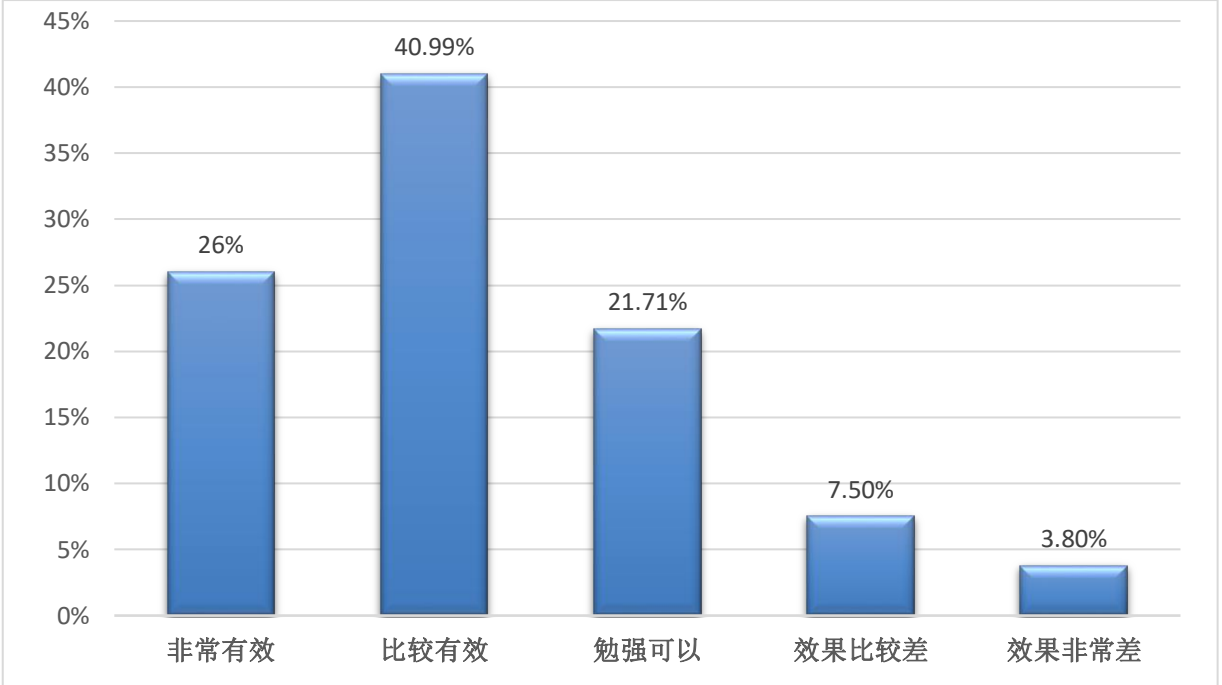


图7-3：管理措施有效程度

E5. 当前的执法依据是否充足

有 62.12%的受调查 E 类从业人员认为当前的执法依据充足（如图 7-4）。

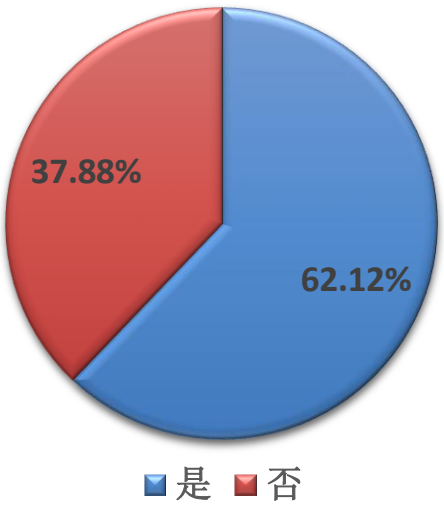


图7-4：执法依据是否充足

E6. 政府部门在网络安全方面的执法力度评价

受调查的 E 类从业人员认为政府部门在网络安全方面的执法力度强的有 35.83%，认为还需加强的有 56.57%，认为力度不足的有 7.59%（如图 7-5）。

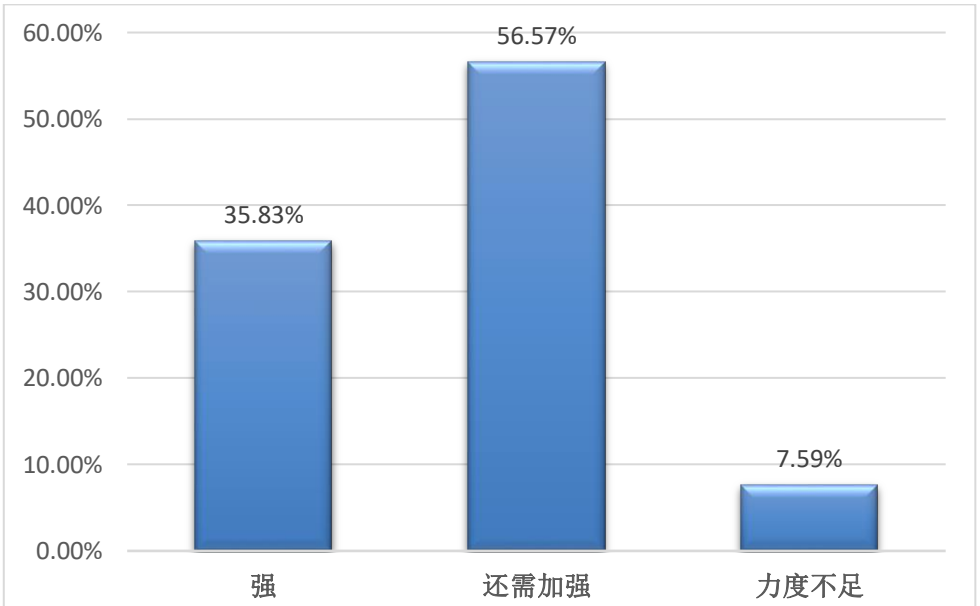


图7-5：政府执法力度评价

E6.1、网络安全执法制约因素

受调查的 E 类从业人员认为影响网络安全执法的制约因素前三位的是：人员（64.65%）、经费（50.54%）、装备（50.44%），各类制约因素占比如图 7-6 所示。

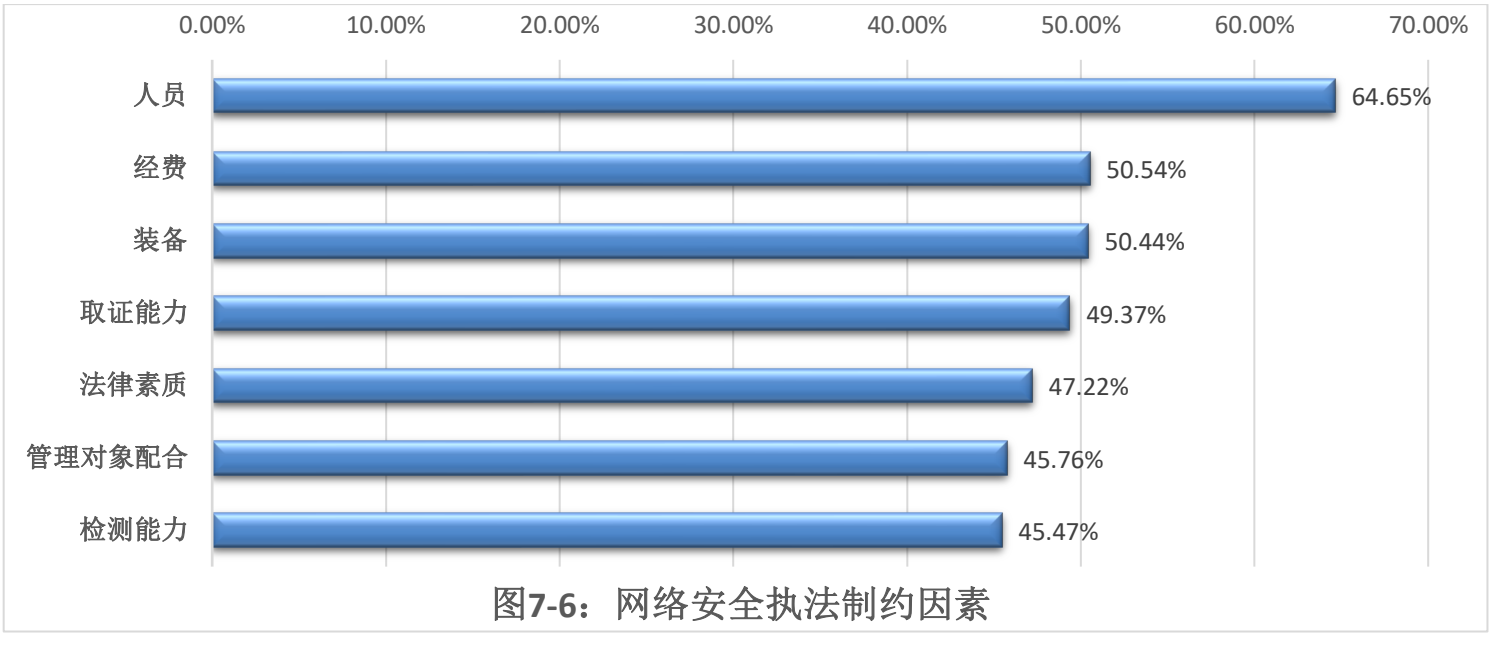


图7-6：网络安全执法制约因素

E6.2、应当加强的装备

受调查的 E 类从业人员认为最应当加强的装备是检测工具，有 71.37%的人员选择，其次是检查工具，有 70.01%的人员选择（如图 7-7）。

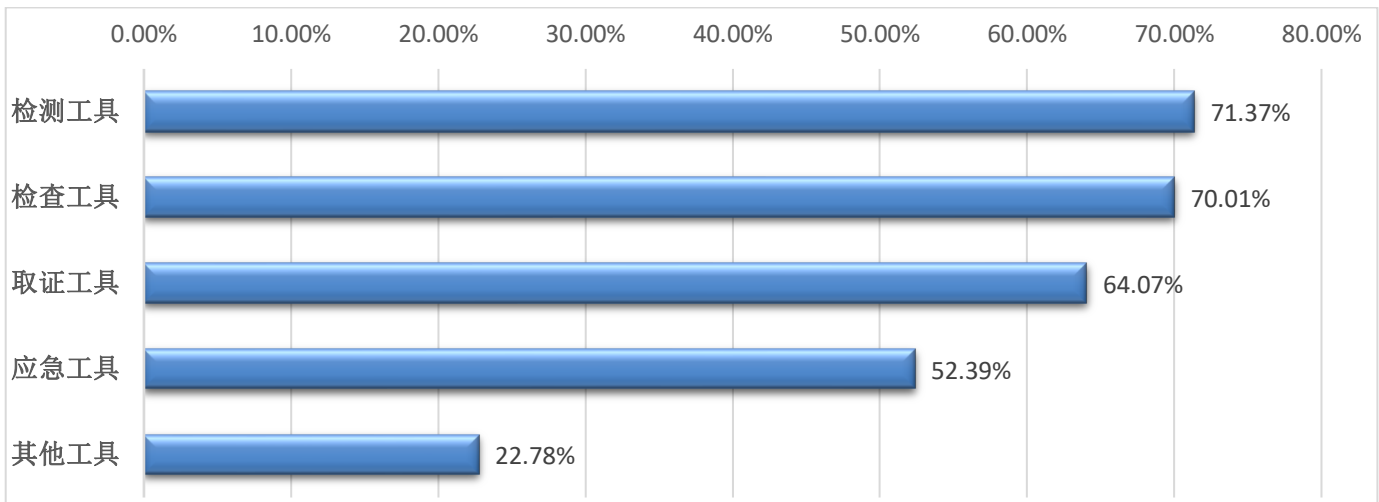


图7-7：应当加强的装备

E6.3、单位开展网络安全执法培训频率

受调查的 E 类从业人员单位每季度开展网络安全执法培训的有 32.91%，从来没有开展过网络安全执法培训的有 11.98%（如图 7-8）。

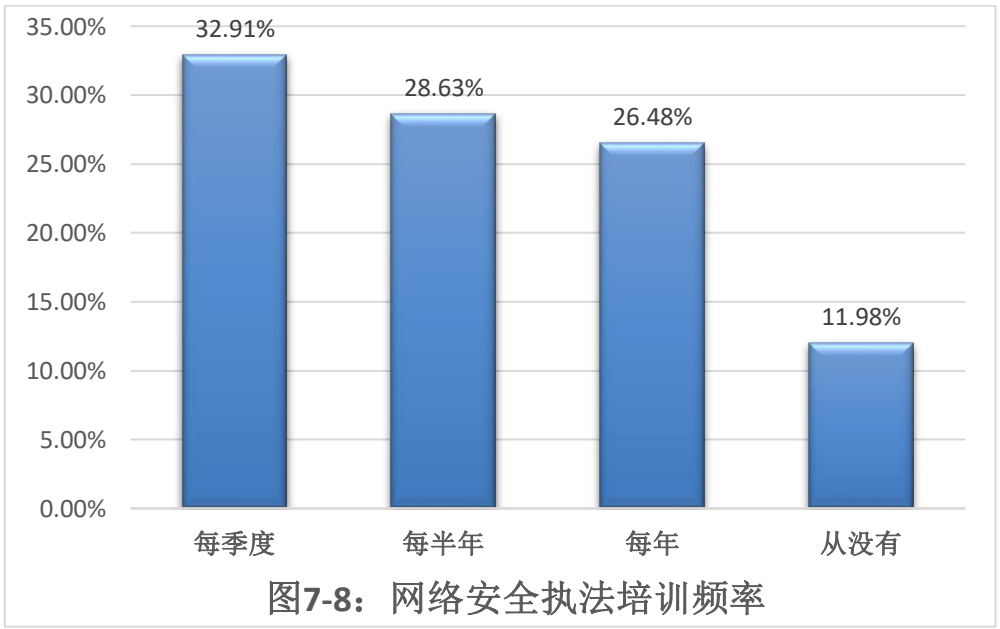


图7-8：网络安全执法培训频率

E7. 亟待加强的网络安全立法内容

受调查的 E 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 69.43%，网络平台责任占 65.63%，数据安全保护占 60.66%（如图 7-9）。

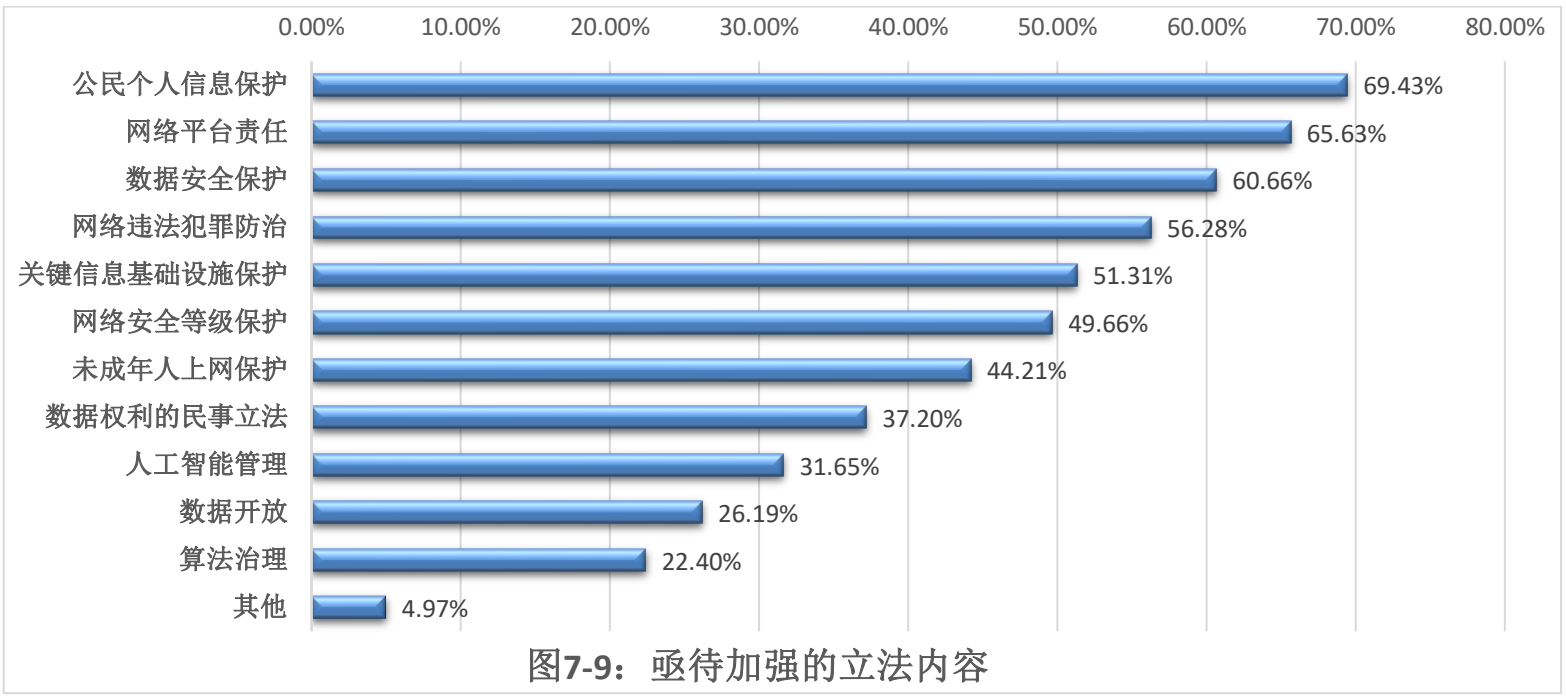


图7-9：亟待加强的立法内容

E8. 否需要建立指标体系跟踪网络安全监管的绩效

受调查的 E 类从业人员中有 85.39%的人员认为有必要家里一套指标体系，以跟踪网络安全监管的绩效（如图 7-10）。

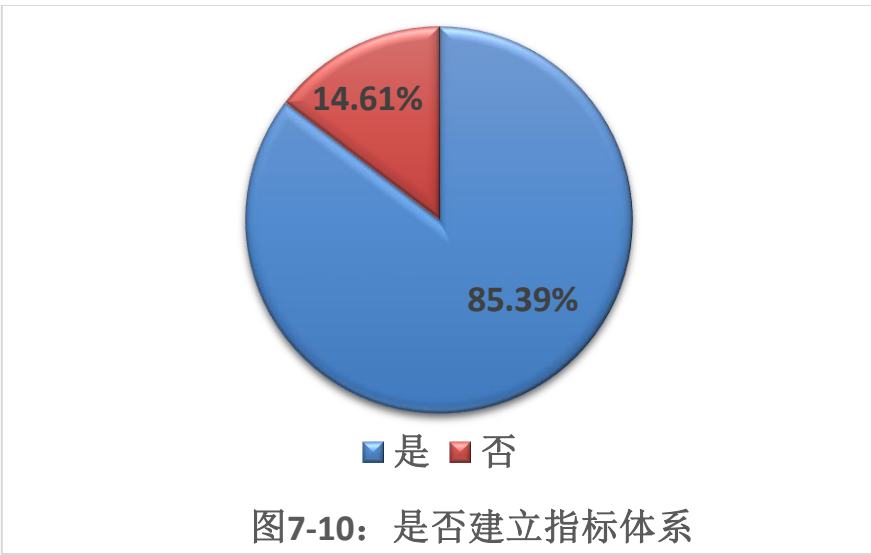


图7-10：是否建立指标体系

E9. 当前部门协作是否紧密

受调查的 E 类从业人员认为当前部门协作紧密的占 28.53%，认为比较紧密的占 47.61%，不紧密的占 23.86%（如图 7-11）。

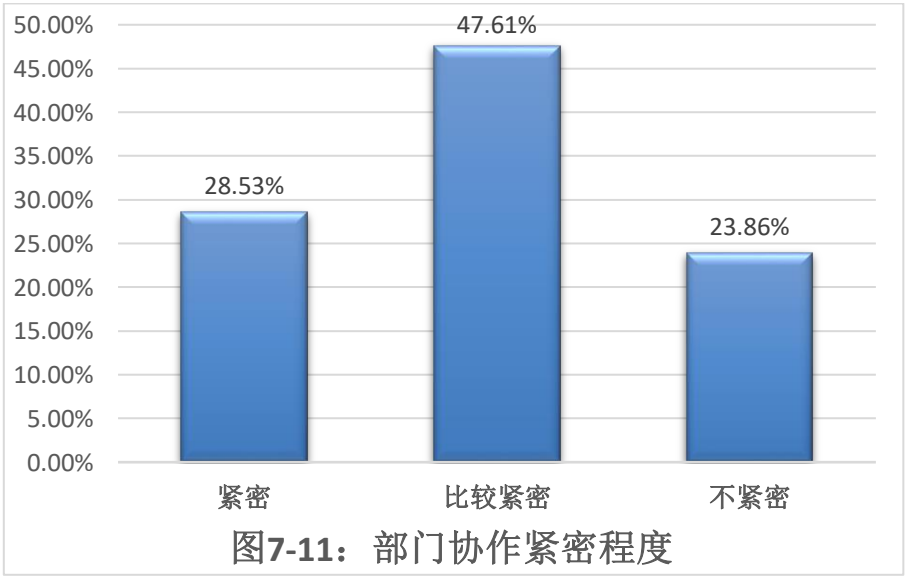


图7-11：部门协作紧密程度

E9.1、需要加强合作的部门

受调查的 E 类从业人员认为需要加强合作部门的前三位依次是网信（74.59%）、公安（64.46%）、工信（56.38%），各部门占比如图 7-12 所示。

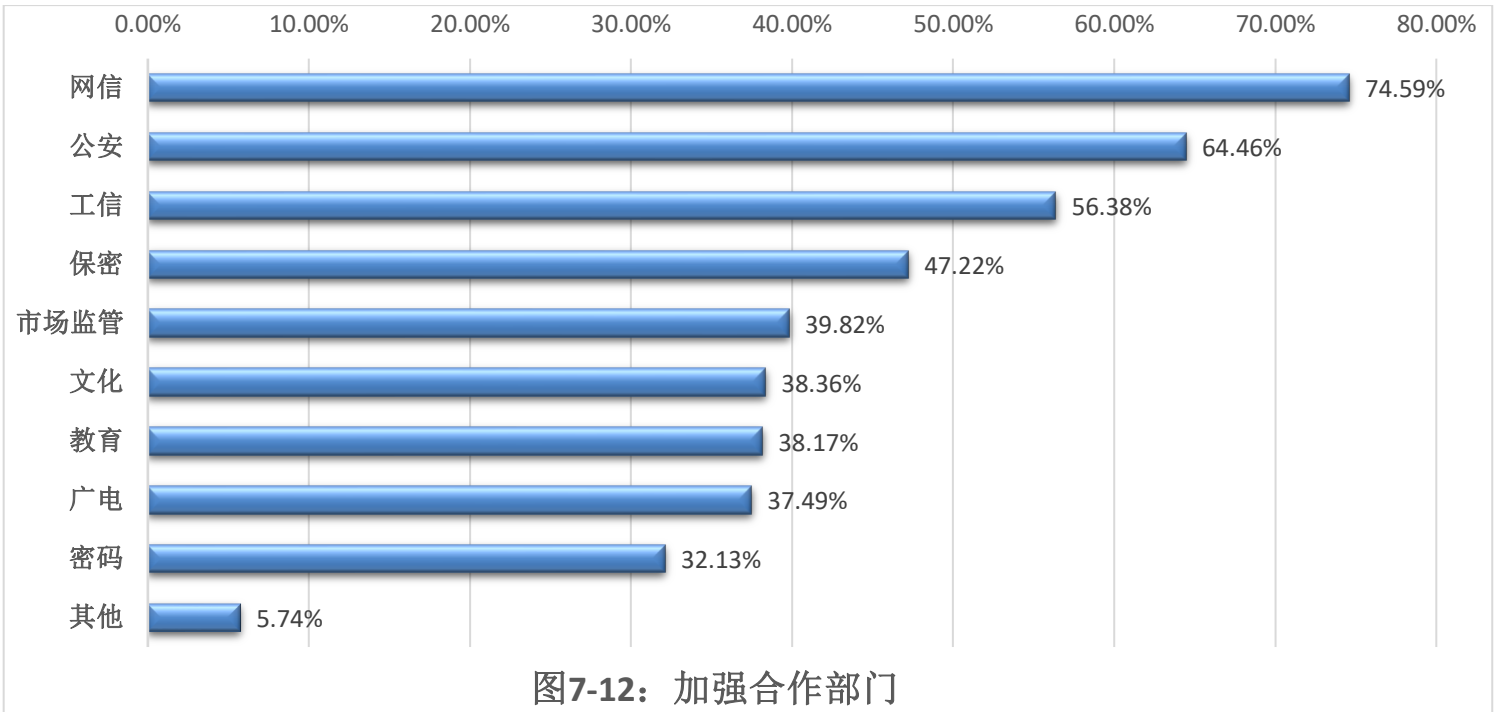


图7-12：加强合作部门

E10. 单位开展网络安全宣传频率

受调查的 E 类从业人员单位每周开展网络安全宣传的有 15.19%，每月开展的有 18.89%，每季度开展的有 25.32%，三项合计每季度至少开展一次的单位有 59.4%，从来没有开展过网络安全宣传的单位有 7.01%（如图 7-13）。

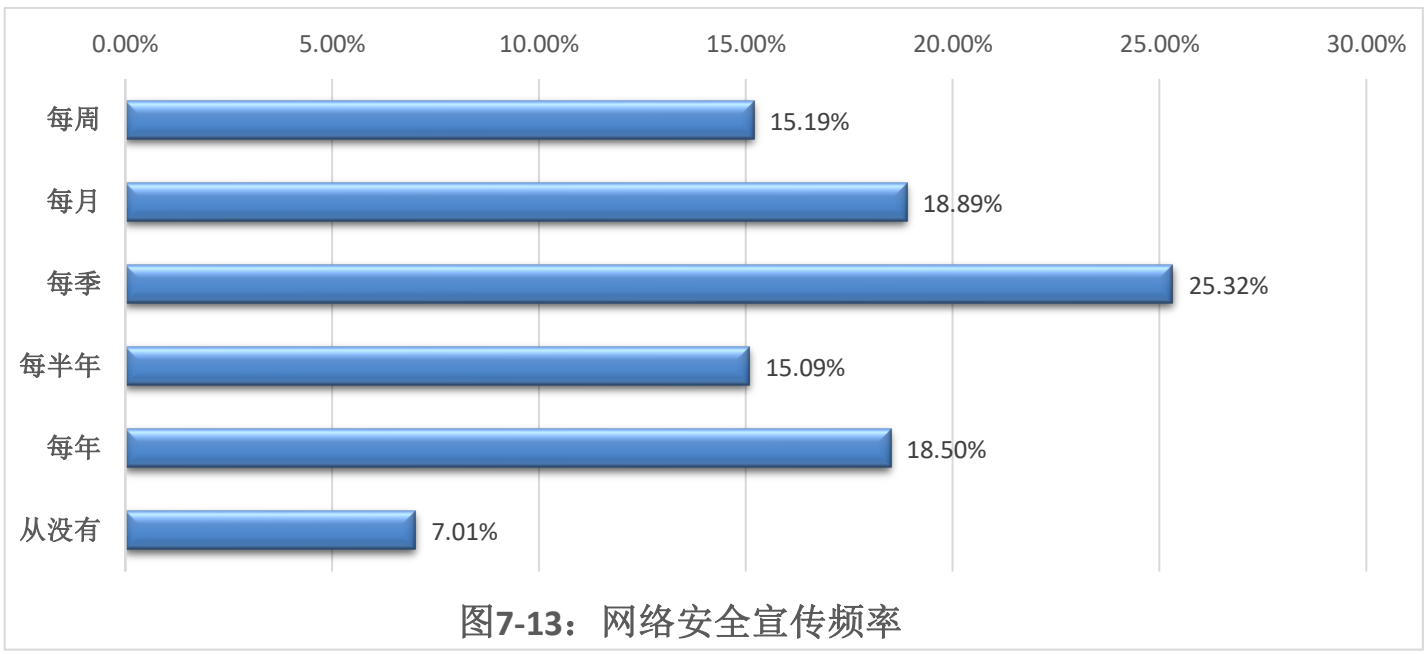


图7-13：网络安全宣传频率

E11. 当前网络安全最突出的问题

受调查的 E 类从业人员认为最突出的网络安全问题是个人信息泄露，有 74.78%的人员选择，排名第二和第三的分别是网络诈骗（61.05%）、网络攻击（51.22%），各类网络安全问题占比如图 7-14 所示。

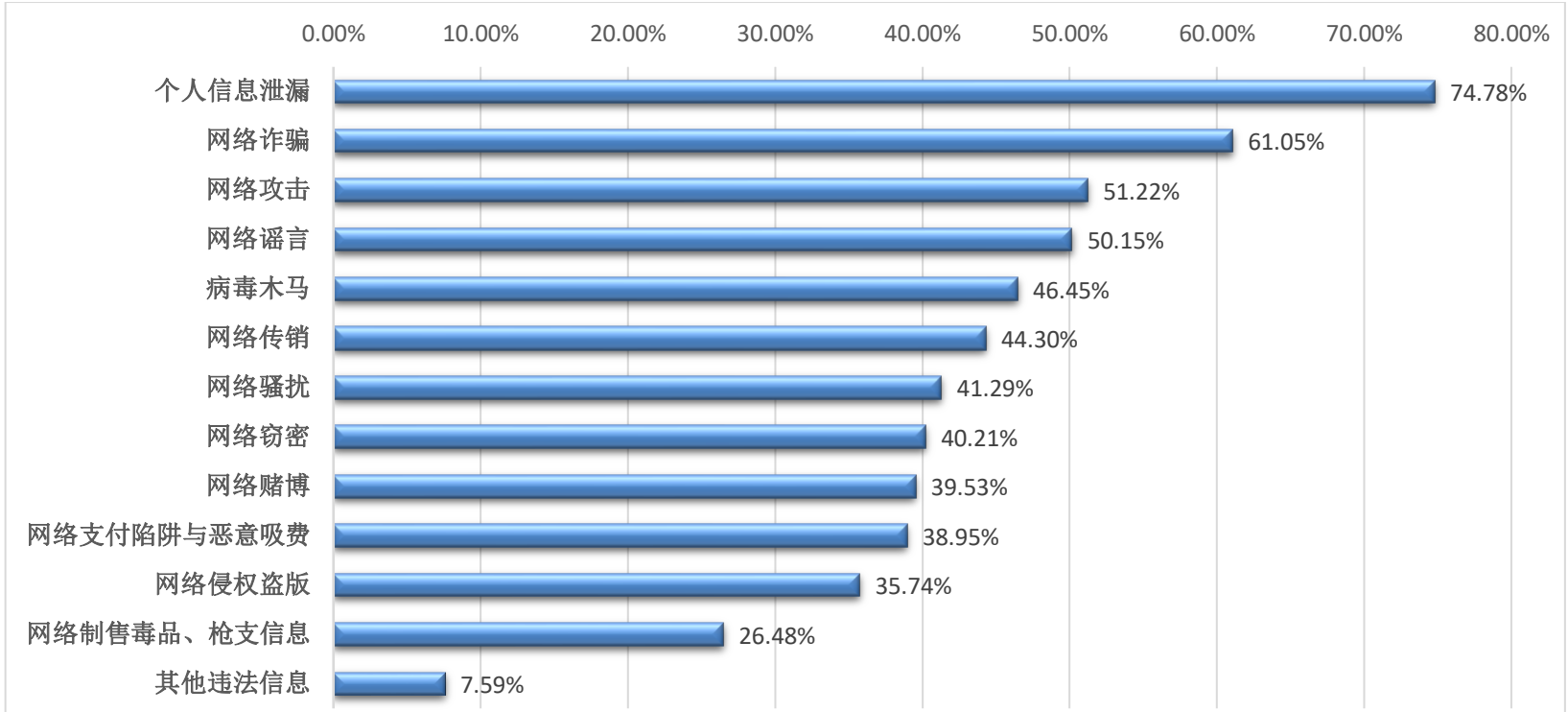


图7-14：网络安全的突出问题

E12. 安全问题较多网络应用或服务

受调查的 E 类从业人员认为安全问题最多的网络应用或服务前五位依次是：在线视频（41.77%），网络直播（40.12%），网络游戏（38.95%），短视频（33.79%），网上支付（31.16%），如图 7-15 所示。

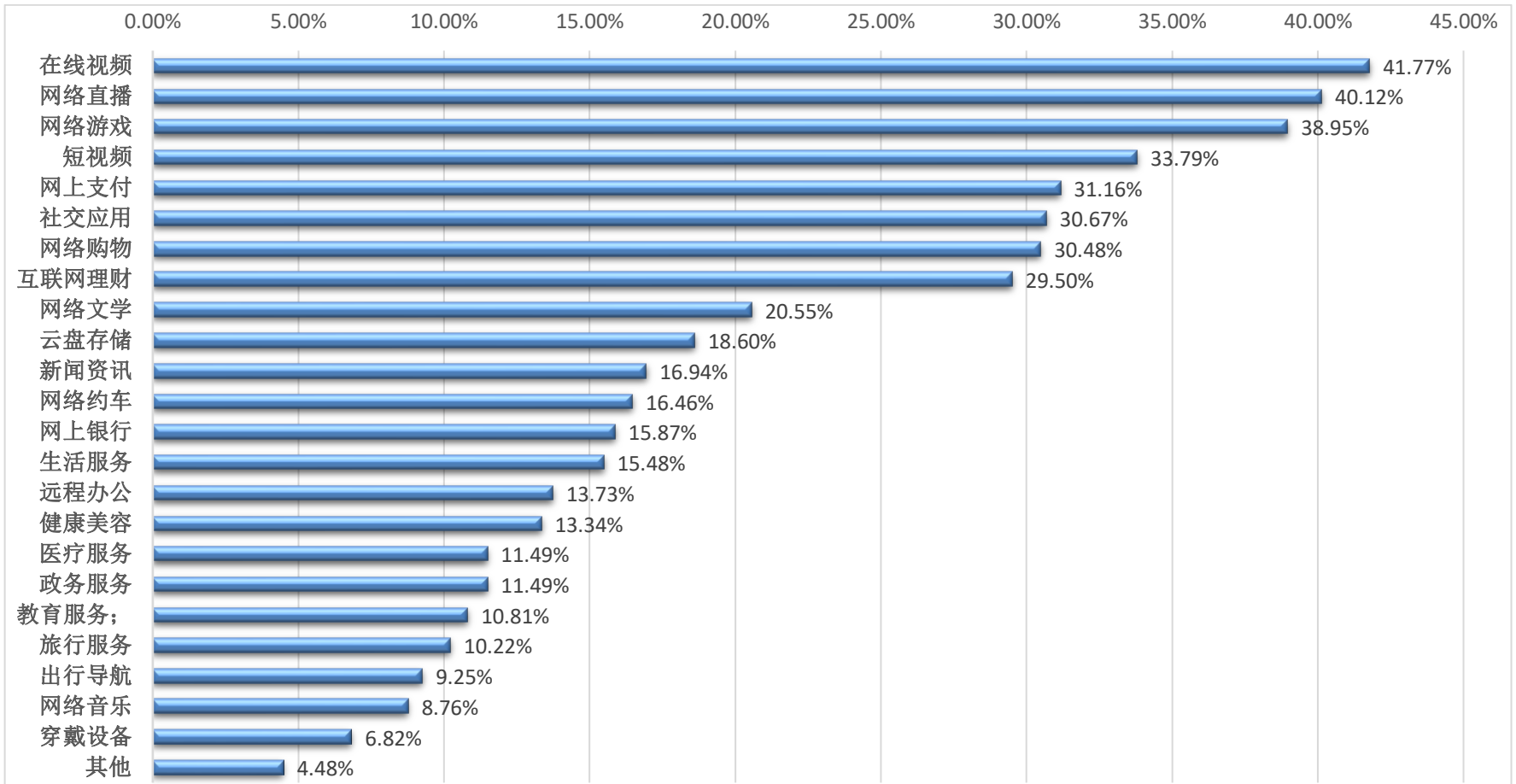


图7-15：安全问题多的网络应用或服务

E13. 当前我国个人信息保护状况

受调查的 E 类从业人员认为当前我国个人信息保护状况非常好的占 16.36%，比较好的占 25.71%，两者合计 42.07%（如图 7-16）。

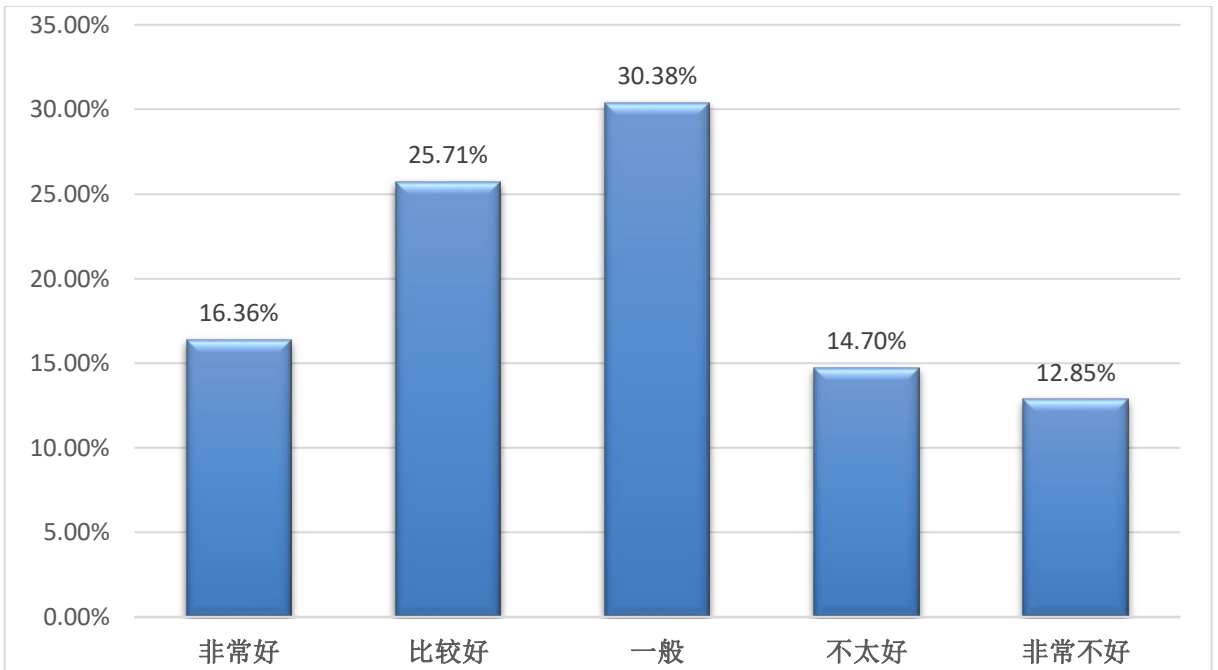


图7-16：个人信息保护状况

E13.1、个人信息保护可以在哪些方面加强

受调查的 E 类从业人员认为个人信息保护最应该加强的方面是犯罪打击，有 75.97%的人员选择，其次有 68.9%的人员选择行政执法（如图 7-17）。

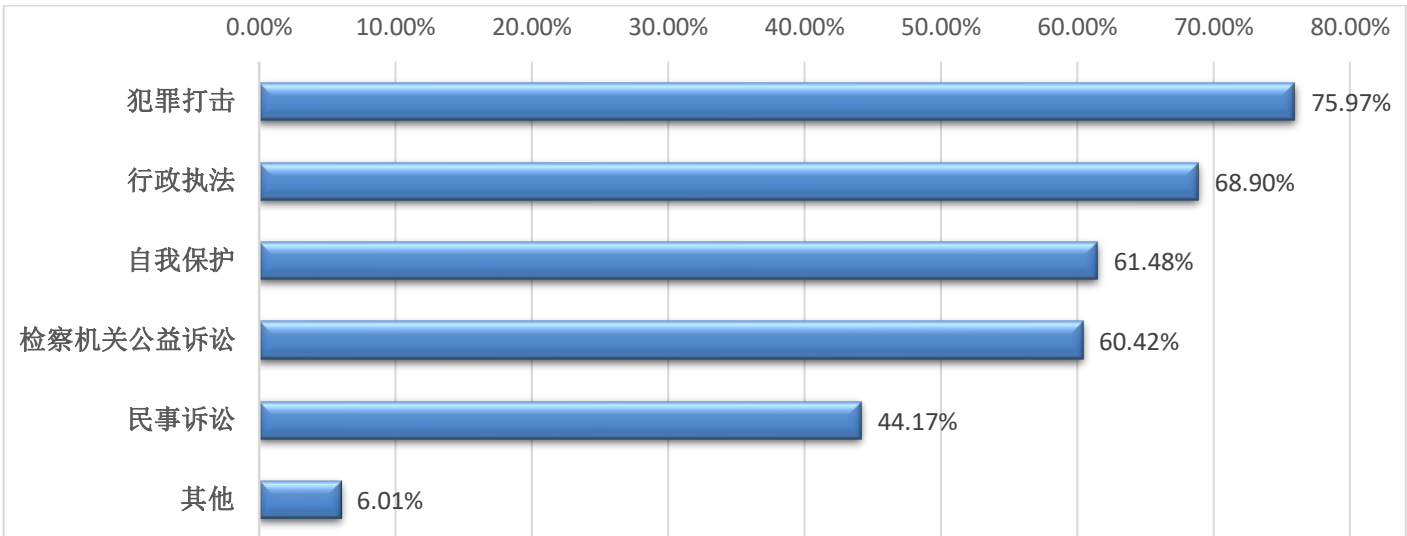


图7-17：个人信息保护应在哪些方面加强

E14. 整治网络黑灰产业链条关键点

受调查的 E 类从业人员中有 68.65%认为治理网络黑灰产业链条最关键的是信息链条（如图 7-18）。

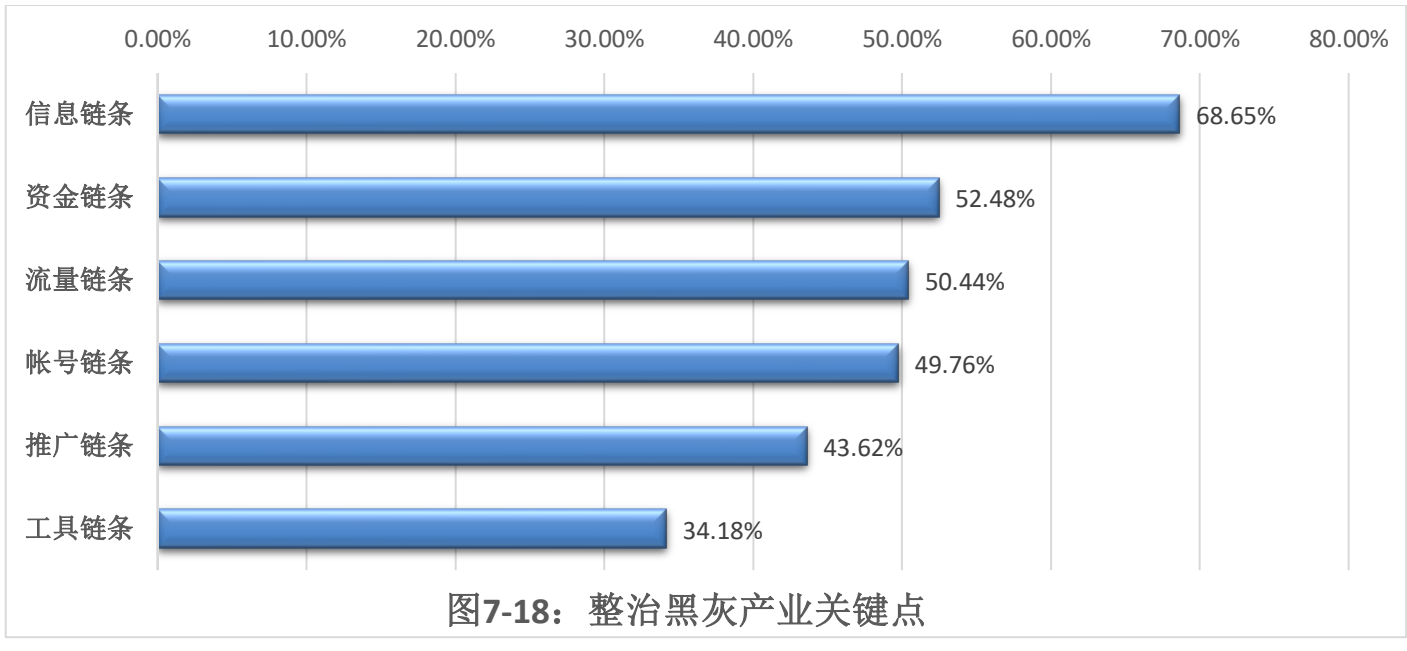


图7-18：整治黑灰产业关键点

E15. 对移动应用可以采取的治理方式

受调查的 E 类从业人员对移动应用认为最应该采取的治理方式前三位依次是：政府部门抽查检测（59.01%），开发者委托第三方测试（54.92%），加强行政执法（52.39%），各种治理方式的选择比例如图 7-19 所示。

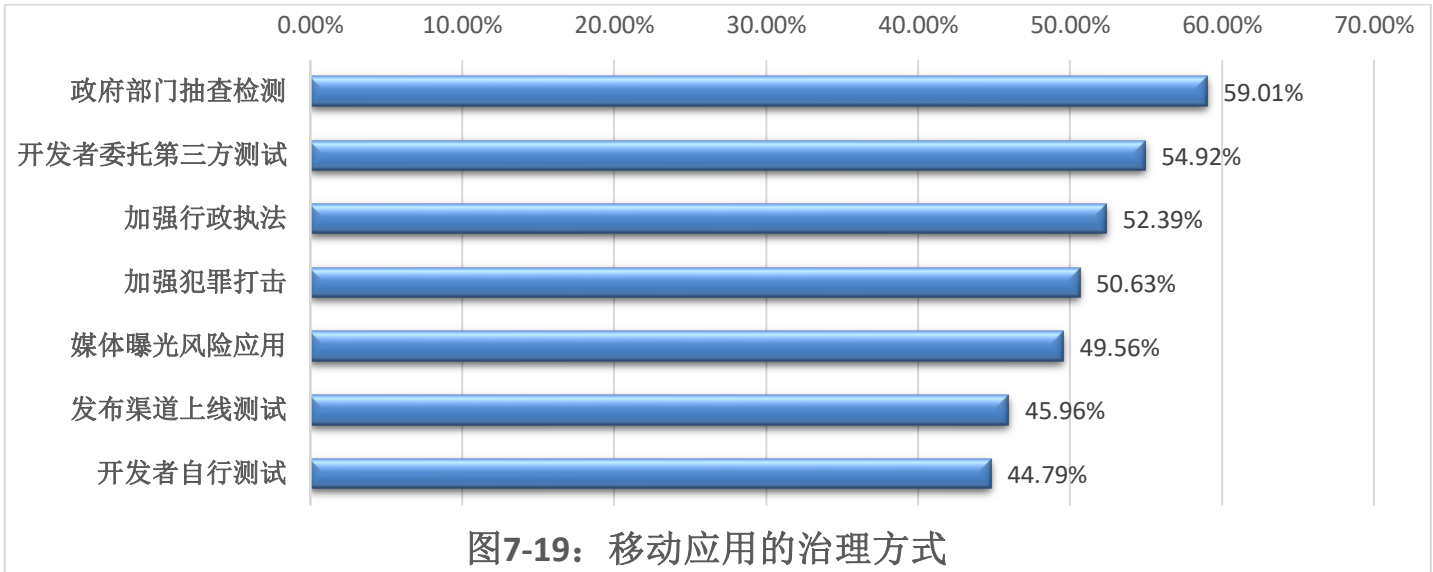


图7-19：移动应用的治理方式

E16. 移动应用不合理采集的用户信息

受调查的 E 类从业人员认为移动应用最不合理采集的用户信息是身份证号，有 62.12%的人员选择，排名第二到第五的依次是聊天记录（52.97%）、短信内容（52.78%）、住址（50.44%）、通信记录（50.44%），各类不合理采集的用户信息占比如图 7-20 所示。从整体上看，受调查网民的选择比较分散，认为不合理的用户信息采集涉及面广泛。

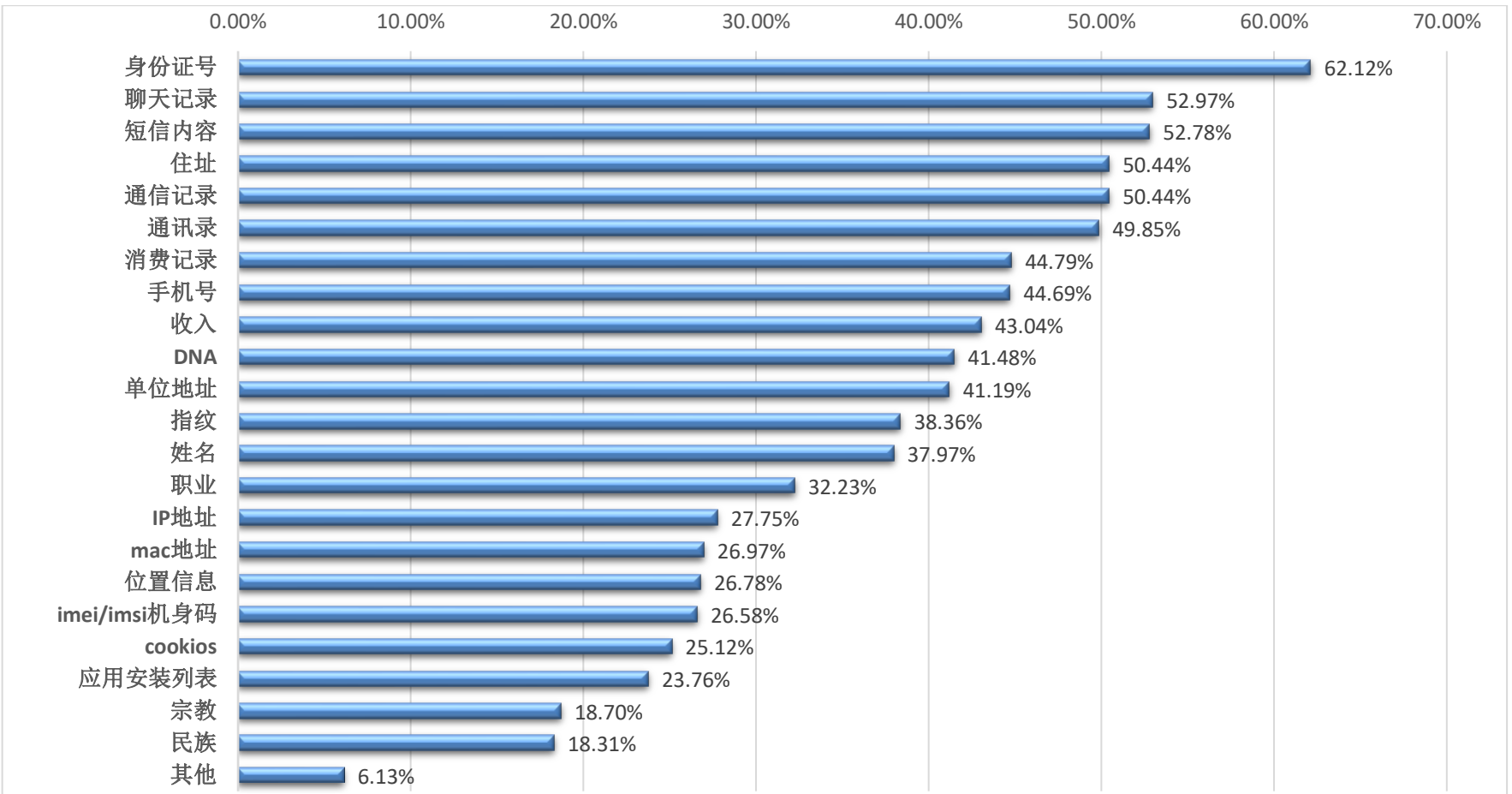


图7-20：不合理采集的用户信息

E17. 落实网络安全等级保护制度的情况

受调查的 E 类从业人员有 64.85%认为本行业落实网络安全等级保护制度的进展良好（如图 7-21）。

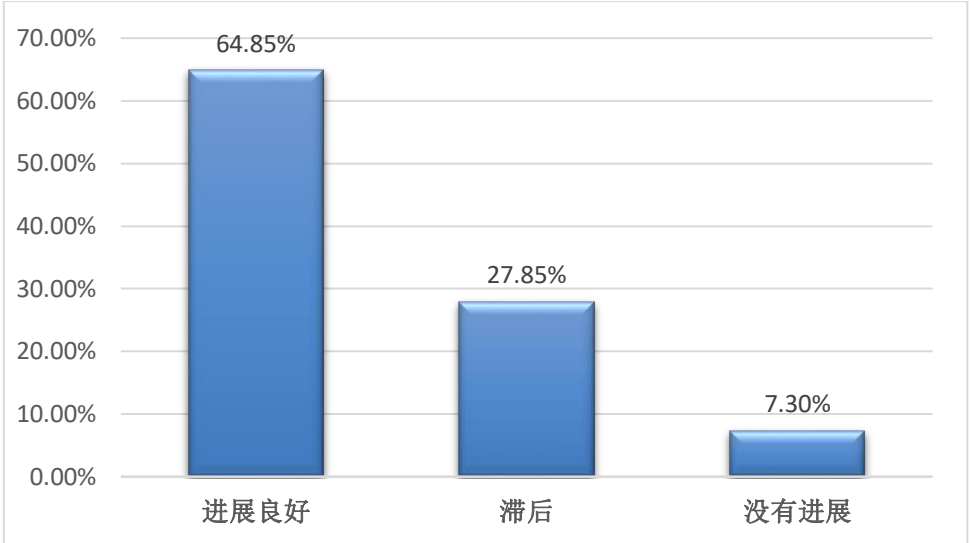


图7-21：等保制度落实情况

E18. 网络安全等级保护开展了哪些工作

受调查的 E 类从业人员认为本行业网络安全等级保护开展的工作最多的是定级备案，有63.68%的人员选择，其次是安全评测（58.71%），各项工作占比如图 7-22 所示。

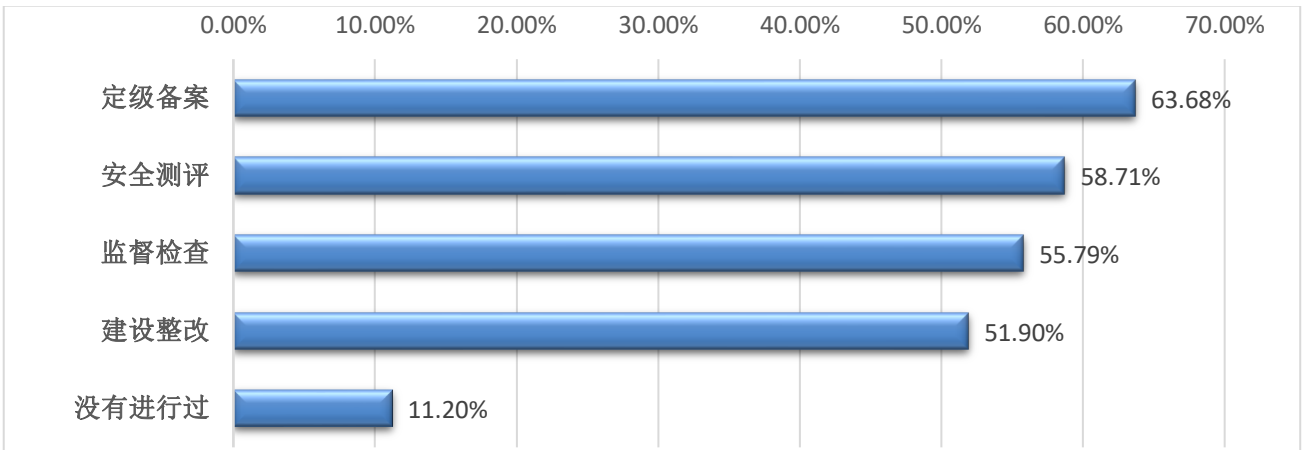


图7-22：开展的网络安全等级保护工作

E19. 公安机关网络安全执法检查工作满意度

受调查的 E 类从业人员对公安机关网络安全执法检查工作满意度评价比较高，56.28%的人员评价为满意，排除没有参加过检查的 7.21%的样本，调整后满意的占比 60.65%（如图 7-23）。

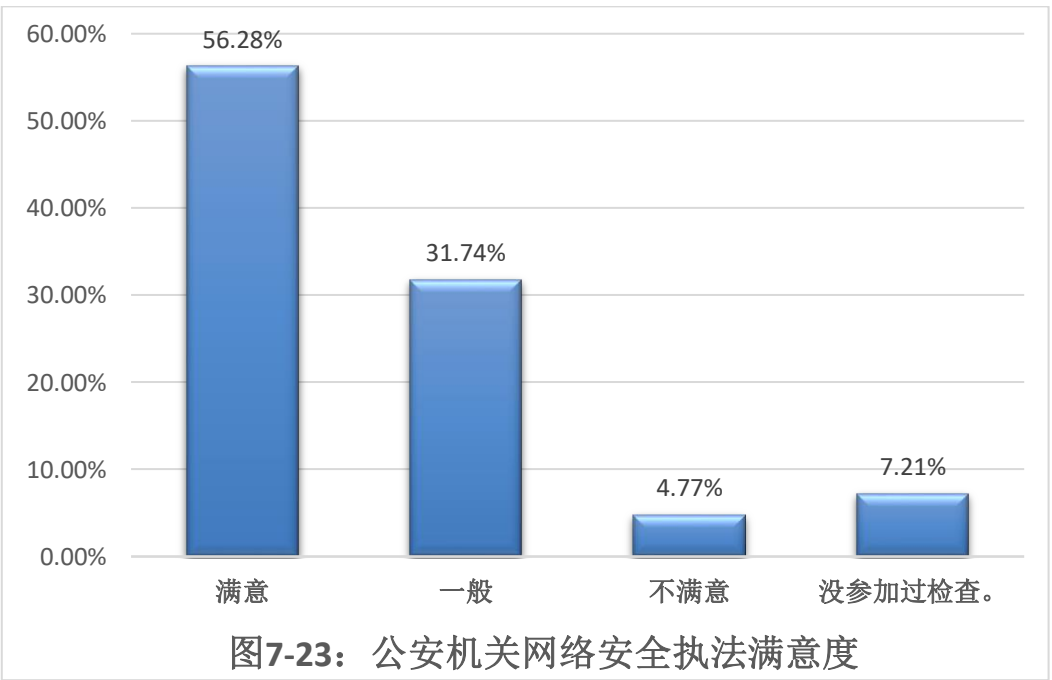


图7-23：公安机关网络安全执法满意度

E20. 当前政府机关和事业单位网络安全管理不足之处

受调查的 E 类从业人员认为当前政府机关和事业单位网络安全管理最不足的是专业技术人才，有 74.59%的人员选择，其次是工作经费不足，有 55.89%的人员选择（如图 7-24）。

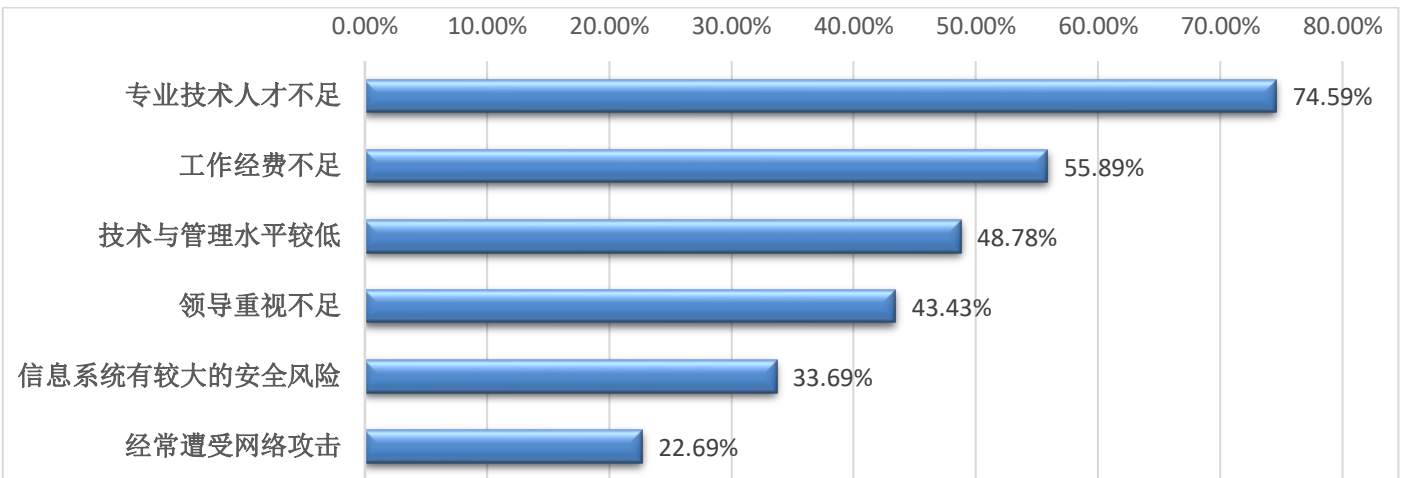


图7-24：网络安全管理的不足

E21. 数字政府的风险

受调查的 E 类从业人员认为数字政府存在的风险前三位的依次是数据集中（51.51%）、个人信息泄露（44.6%）、运维管理（43.04%），各项风险占比如图 7-25 所示。

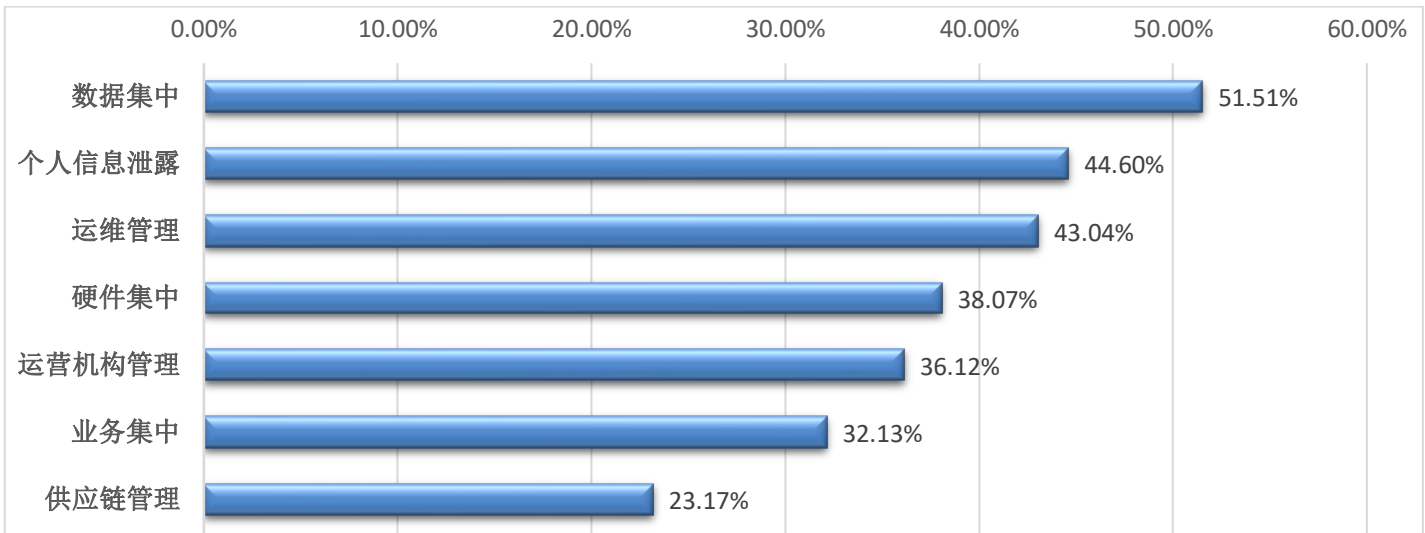


图7-25：数字政府的风险

E21.1、风险大的服务

受调查的 E 类从业人员认为数字政府风险大的服务前三位依次是住房（70.15%）、医疗（53.81%）、社保（52.72%），各项服务占比如图 7-26 所示。

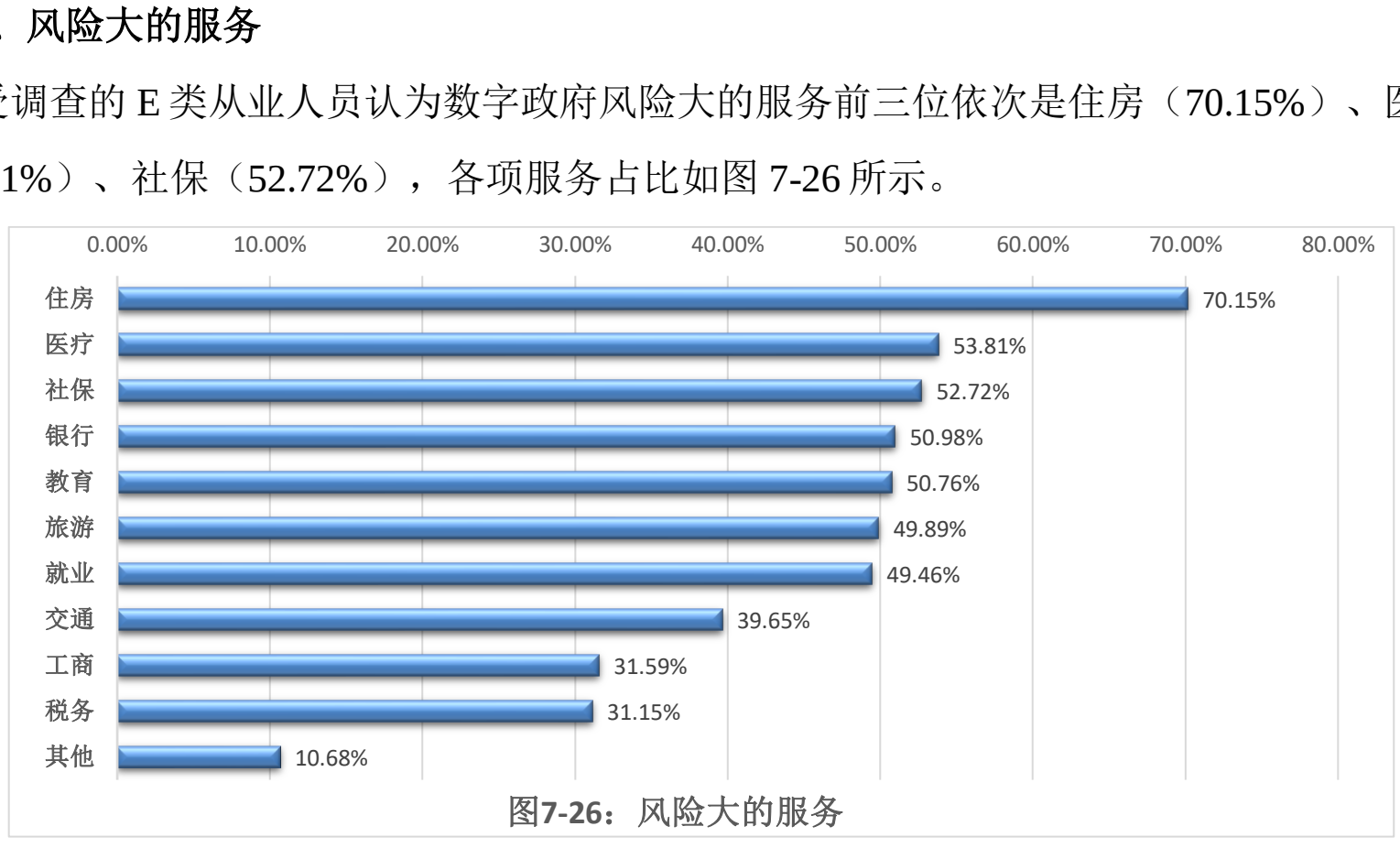


图7-26：风险大的服务

八、F 卷：国有企事业单位的从业人员

国有企事业单位（F 类）的从业人员主要是网络用户的身份，单位业务管理比较规范。

F 问卷有效问卷数 2971 份，以下是 F 类问卷各项数据的详细统计结果。

F3. 当前网络安全状况

受调查的 F 类从业人员认为网络安全状况良好有 36.92%，认为状况一般的占 47.29%，认为状况堪忧的占 15.79%（如图 8-1）。

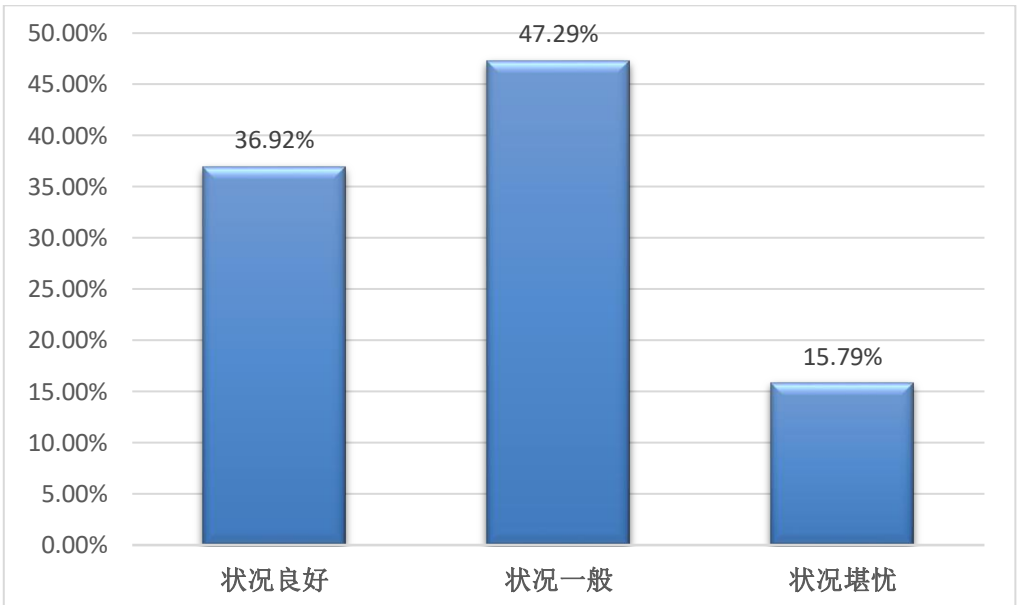


图8-1：安全状况评价

F4. 与去年相比网络安全感的变化

大部分受调查的 F 类从业人员认为当前网络安全状况改善，有 22.21%的人员认为明显改善，有 53.72% 的人员认为有改善，两者合计有 75.93%的人员认为网络安全状况改善或明显改善（如图 8-2）。

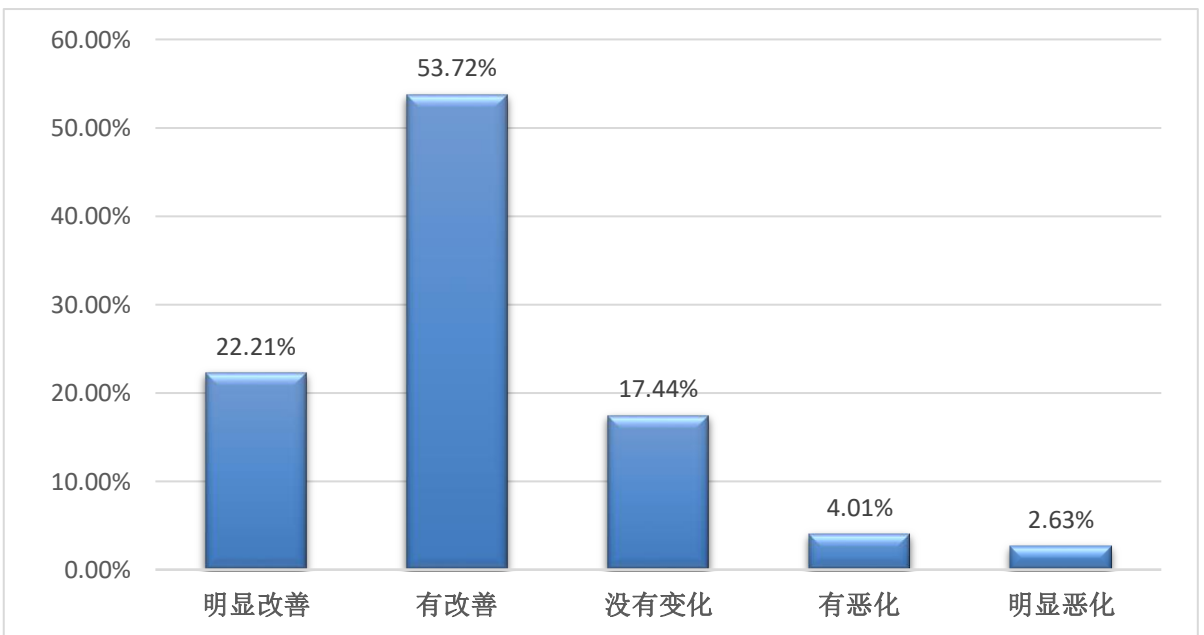


图8-2：网络安全感变化评价

F5. 网络服务提供者的管理措施对于保证网络安全水平的有效程度

受调查的 F 类从业人员有 16.63%认为非常有效，有 45.51%认为比较有效，两者合计共有 62.14%的人员认为非常有效和比较有效（如图 8-3）。

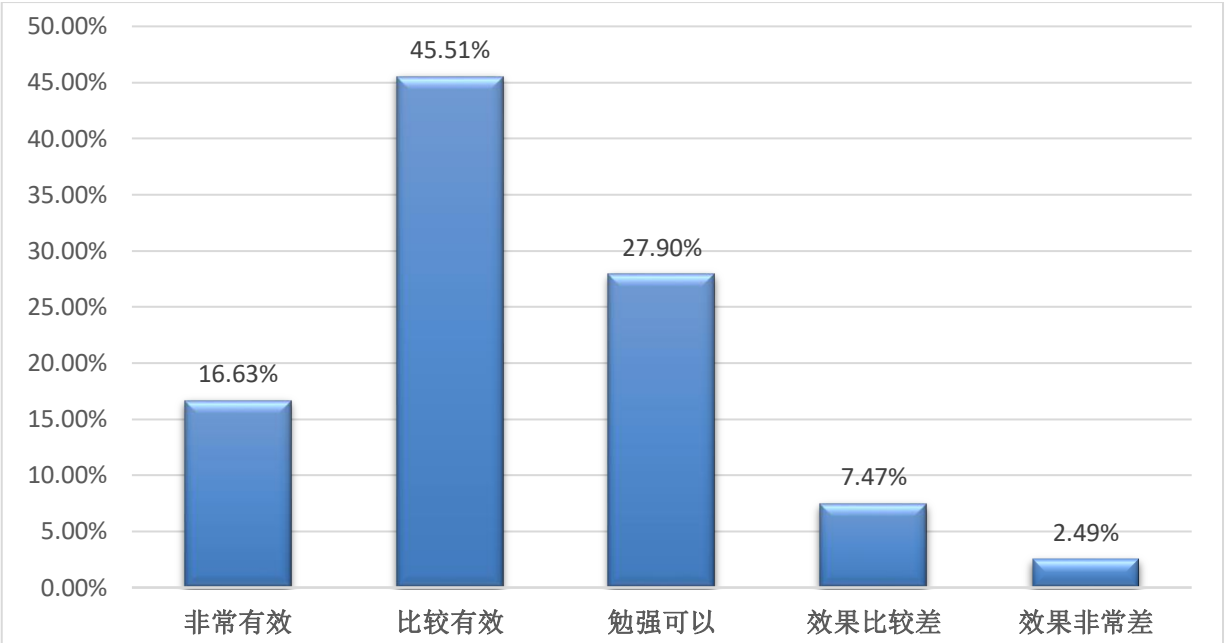


图8-3：管理措施有效程度

F6. 当前网络安全产品服务的资费水平

受调查的 F 类从业人员认为当前网络安全产品服务的资费水平高的占 40.12%，认为适中的占 52.47%，认为低的占 7.4%（如图 8-4）。

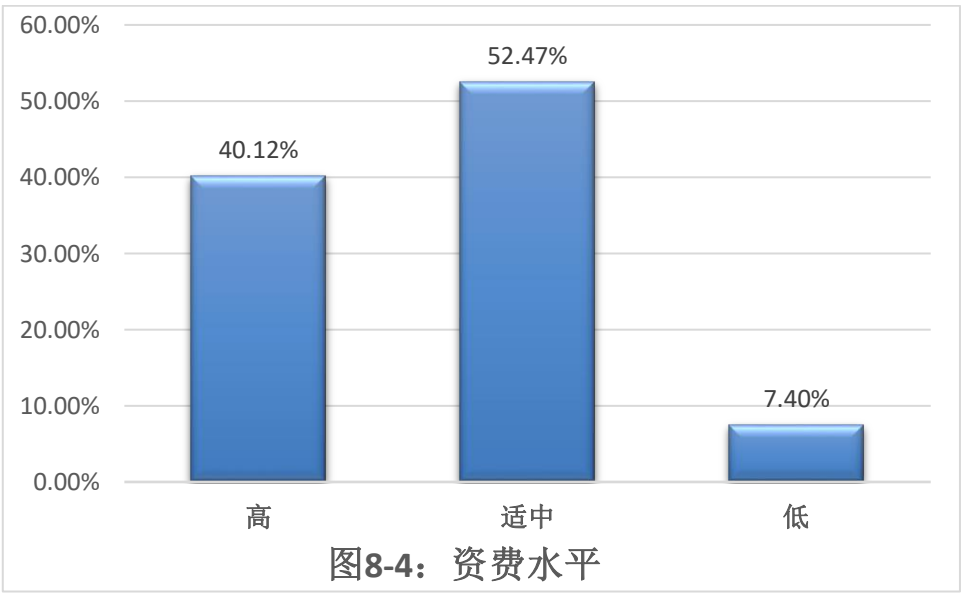


图8-4：资费水平

F7. 单位网络安全方面经费预算

受调查的 F 类从业人员单位在网络安全方面经费预算充裕的占 14.27%，较充裕的占 27.26%，两者合计共有 41.53%的人员认为经费充裕（如图 8-5）。

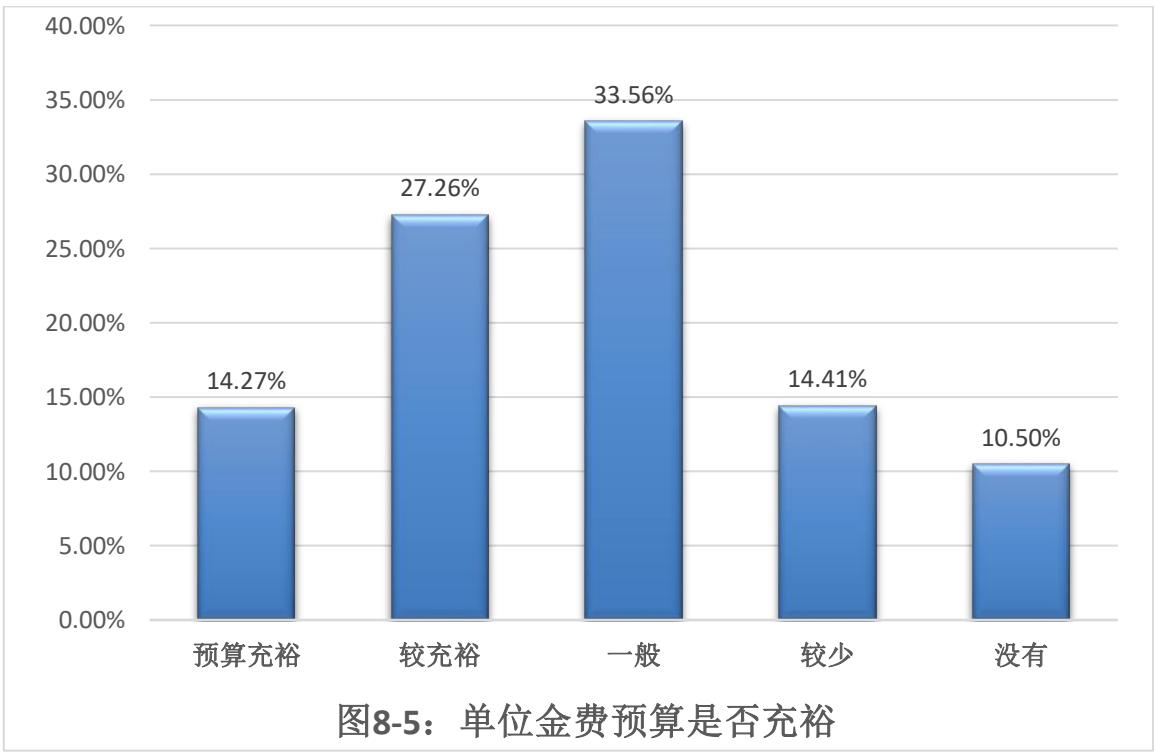


图8-5：单位金费预算是否充裕

F8、单位的网络安全技术保障状况满意程度

受调查的 F 类从业人员认为单位的网络安全技术保障状况满意的占 25.21%，认为较满意的占 33.32%，两者合计共有 58.53%的人员认为满意或较满意（如图 8-6）。

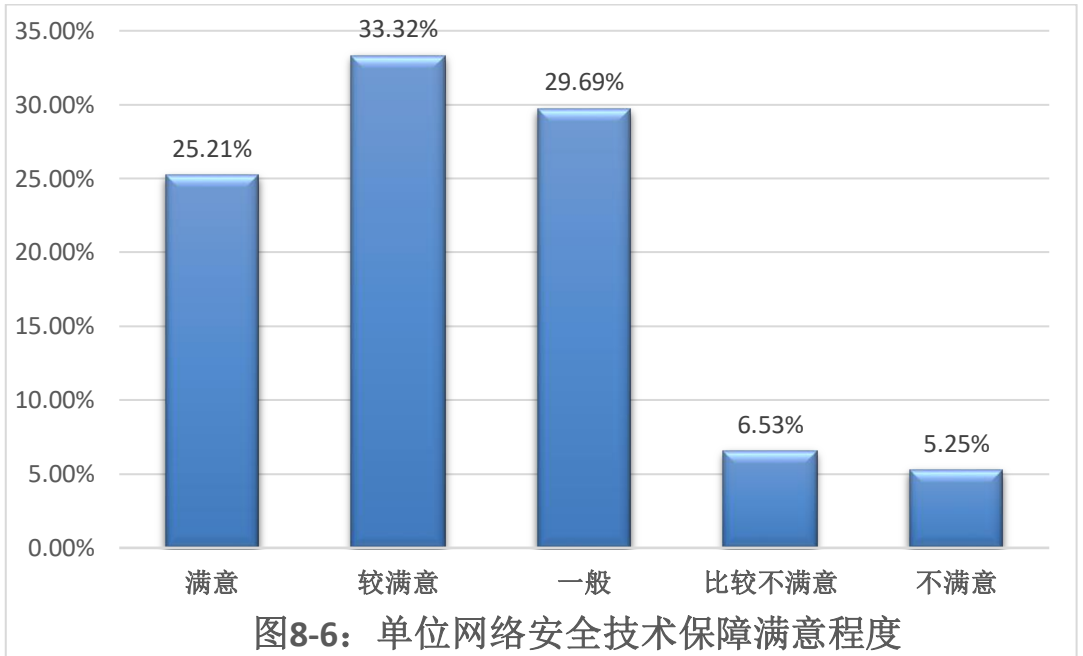


图8-6：单位网络安全技术保障满意程度

F9. 单位的网络安全管理状况满意程度

受调查的 F 类从业人员认为单位的网络安全管理状况满意的占 26.83%，认为较满意的占 33.79%，两者合计共有 60.62%的人员认为满意或较满意（如图 8-7）。

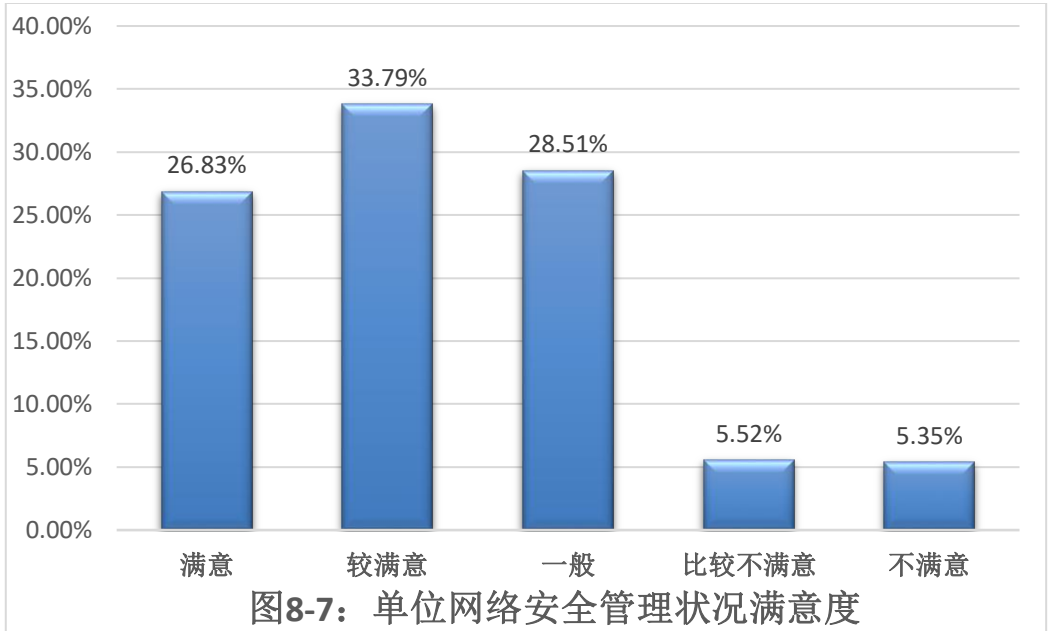


图8-7：单位网络安全管理状况满意度

F9.1、单位的网络安全管理哪些方面应改善

受调查的 F 类从业人员认为单位的网络安全管理最应该在人才队伍方面改善，有 75.85%的人员选择，其次是网络安全管理的贯彻落实，有 60.06%的人员选择（如图 8-8）。

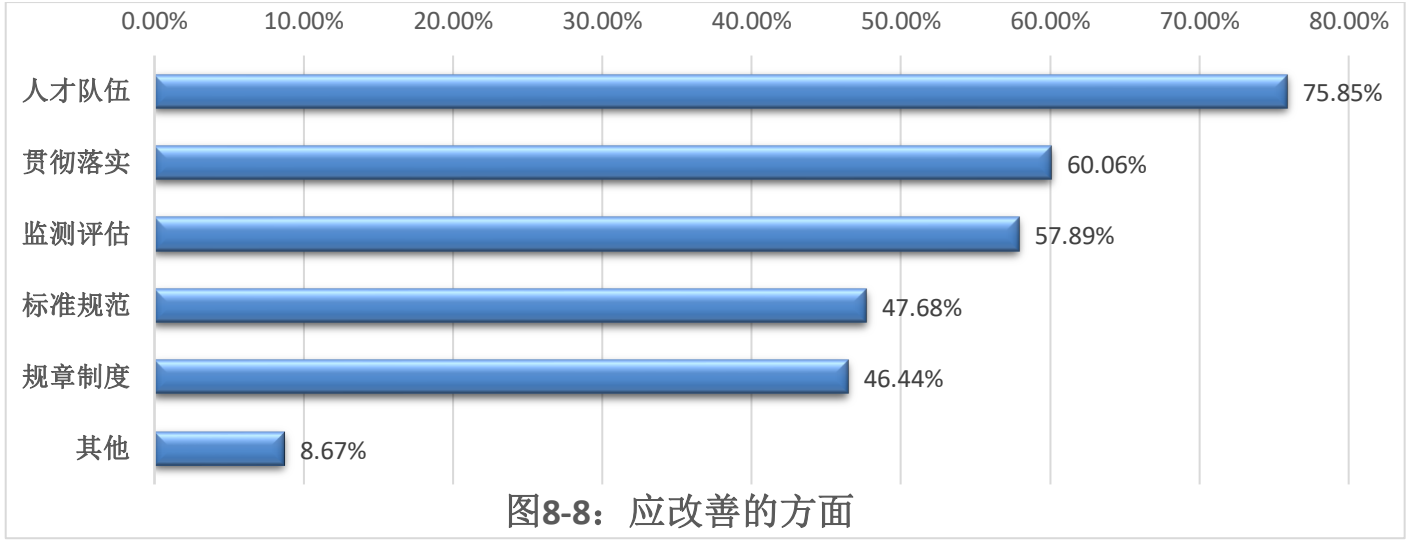


图8-8：应改善的方面

F10、单位的网络安全教育培训满意程度

受调查的 F 类从业人员认为单位的网络安全教育培训满意的占 25.04%，认为较满意的占 30.09%，两者合计共有 55.13%的人员认为满意或较满意（如图 8-9）。

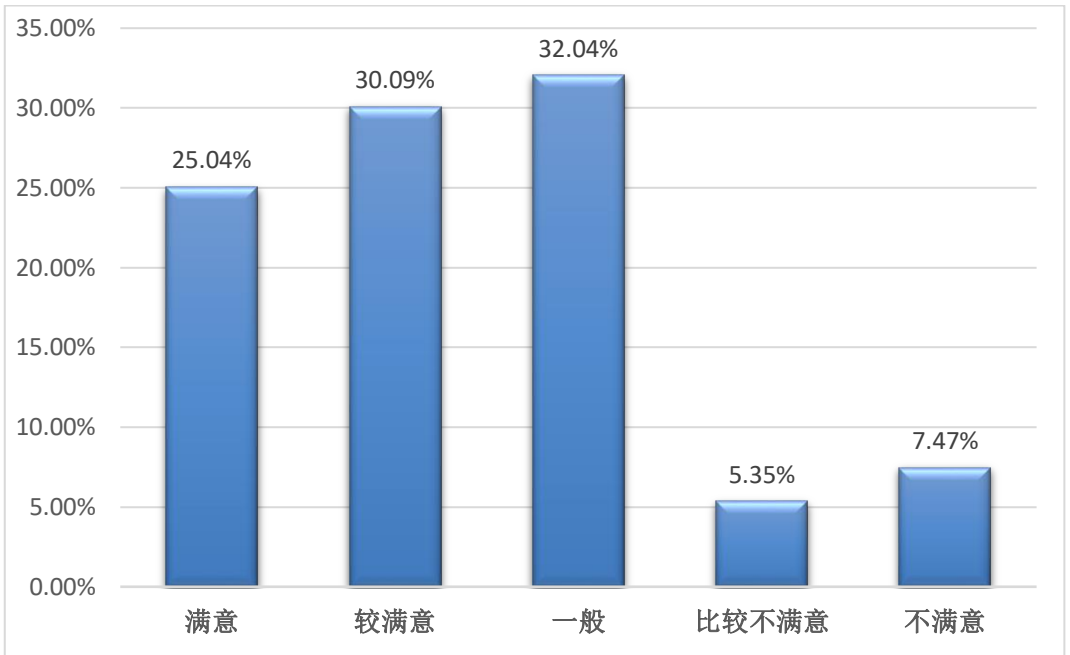


图8-9：单位网络安全教育培训满意程度

F10.1、哪些方面不满意

受调查的 F 类从业人员认为单位网络安全教育培训最不满意的是用处不大，有 45.93%的人员选择，其次是形式单调，有 44.88%的人员选择（如图 8-10）。

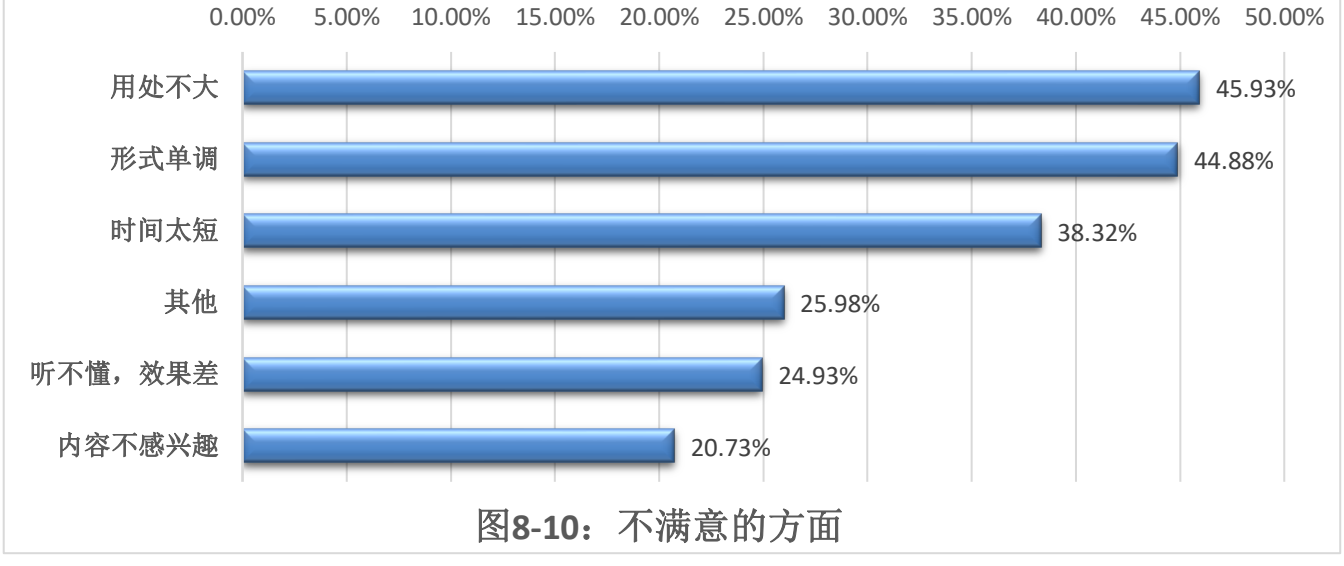


图8-10：不满意的方面

F11. 当前网络安全最突出的问题

受调查的 F 类从业人员认为最突出的网络安全问题是个人信息泄露，有 54.06%的人员选择，排名第二和第三的分别是网络攻击（11.14%）、病毒木马（9.42%），各类网络安全问题占比如图 8-11 所示。

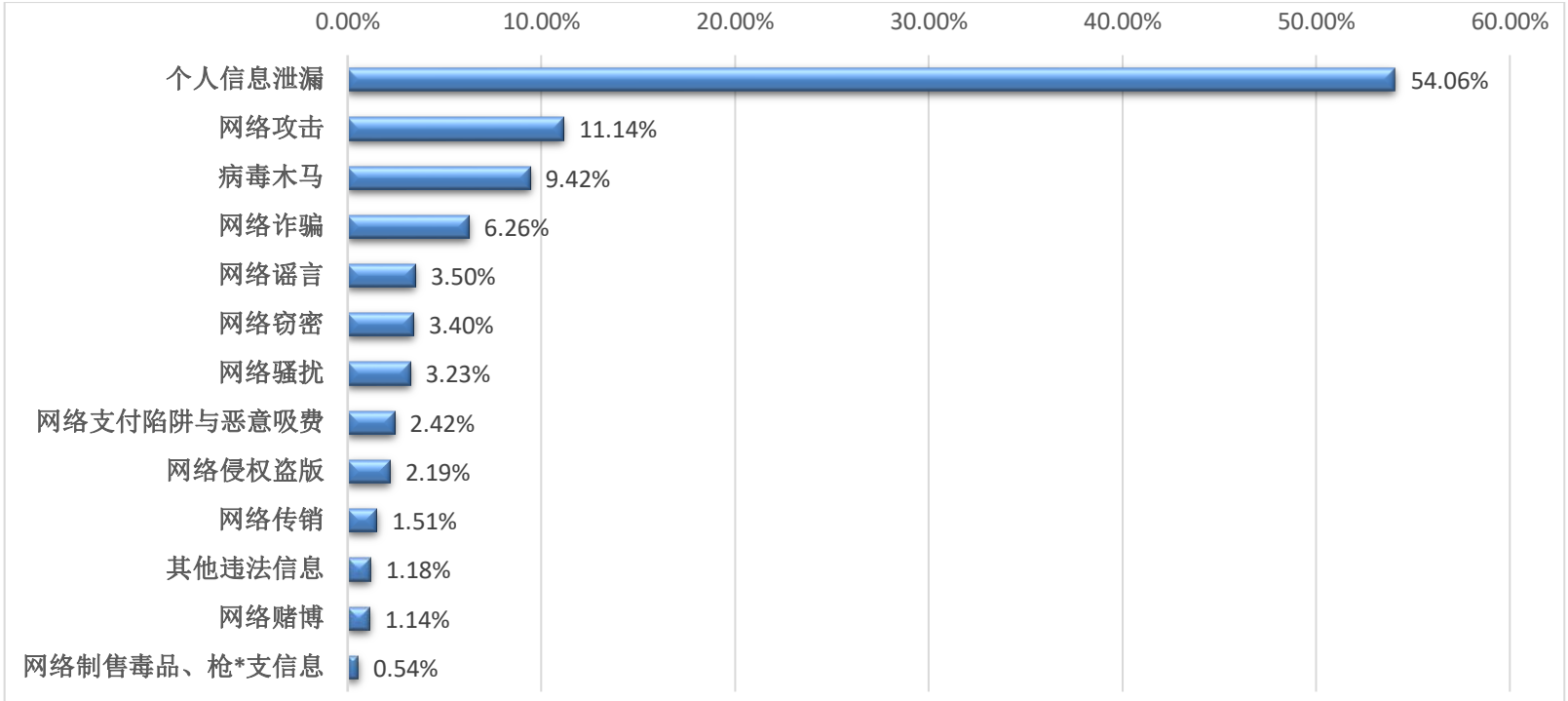


图8-11：网络安全的突出问题

F12. 当前我国个人信息保护状况

受调查的 F 类从业人员认为当前我国个人信息保护状况非常好的占 7.2%，比较好的占 17.2%，两者合计有 24.4%的人员认为好，认为不太好（24.47%）和非常不好（21.37%）的合计 45.84%（如图 8-12）。

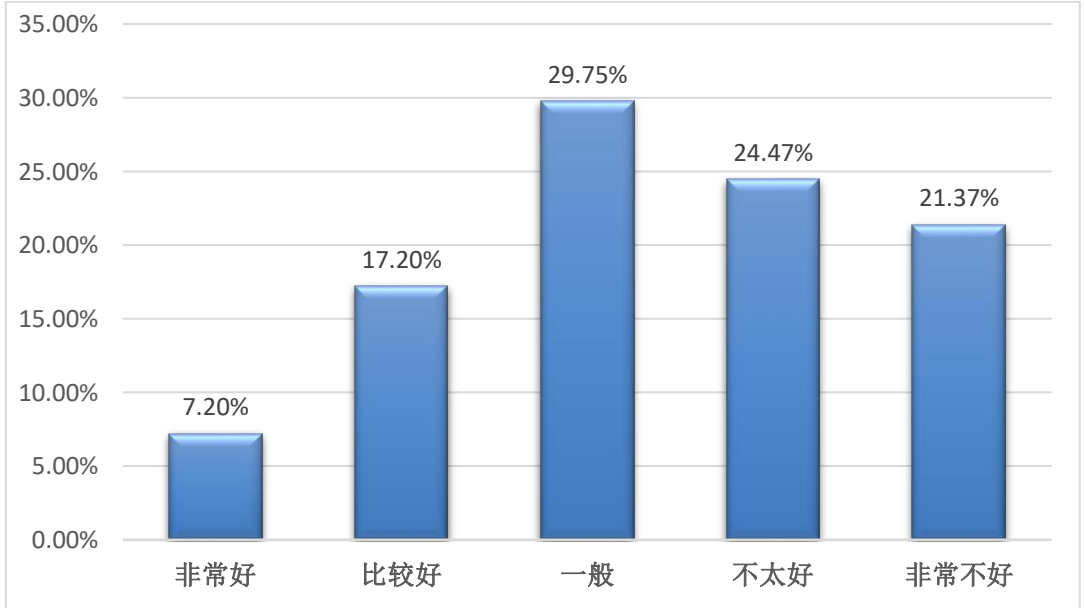


图8-12：个人信息保护状况

F12.1、个人信息保护可以在哪些方面加强

受调查的 F 类从业人员认为个人信息保护最应该加强的方面是犯罪打击，有 81.35%的人员选择，其次有 73.42%的人员选择行政执法（如图 8-13）。

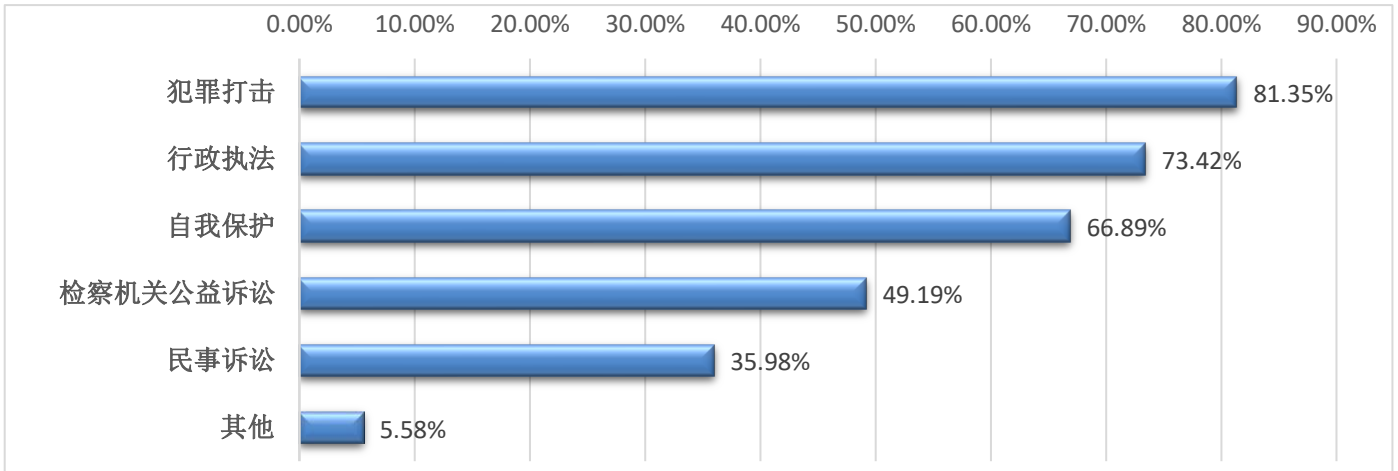


图8-13：个人信息保护应在哪些方面加强

F13. 政府网络安全管理政策措施对单位的影响

受调查的 F 类从业人员认为政府网络安全管理措施对单位影响最大的前三位依次是提高了意识（72.97%）、提高了风险防控水平（55.33%）、建立了组织体系（46.58%），各类影响占比如图 8-14 所示。

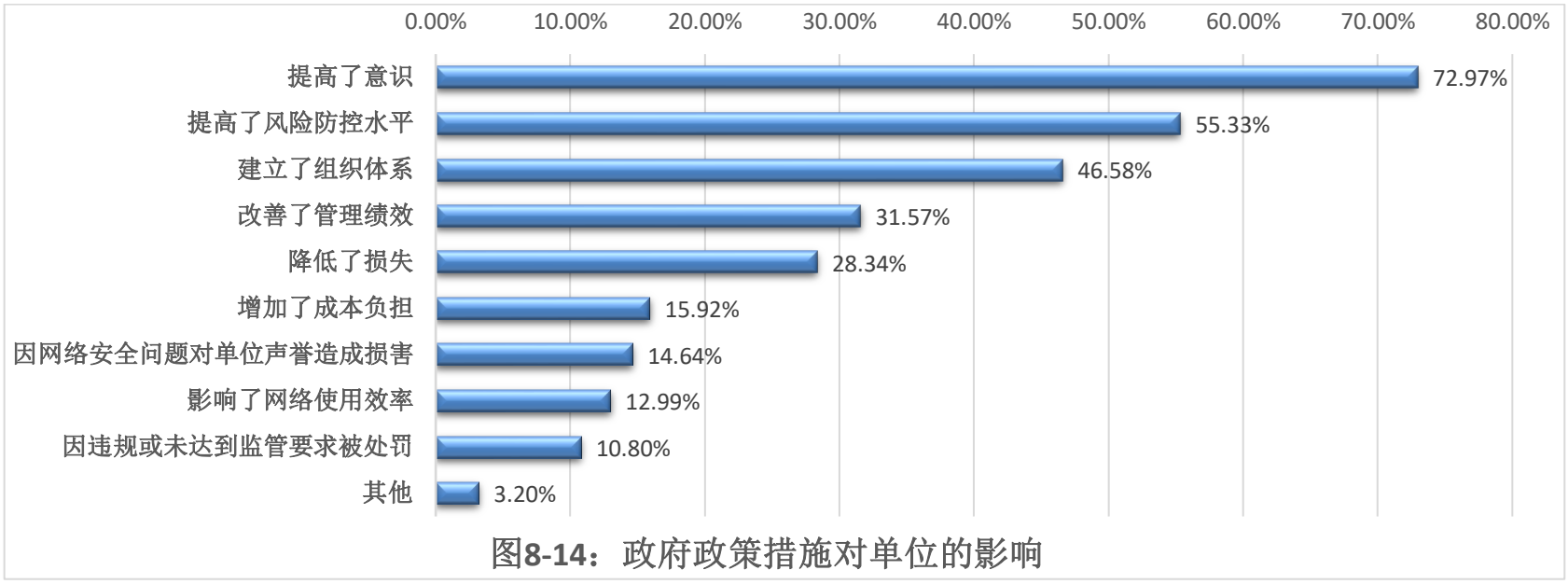


图8-14：政府政策措施对单位的影响

F14. 当前政府机关和事业单位网络安全管理的不足

受调查的 F 类从业人员认为当前政府机关和事业单位网络安全管理最不足的是专业技术人才，有 71.76%的人员选择，其次有 47.12%的人员选择技术与管理水平较低（如图 8-15）。

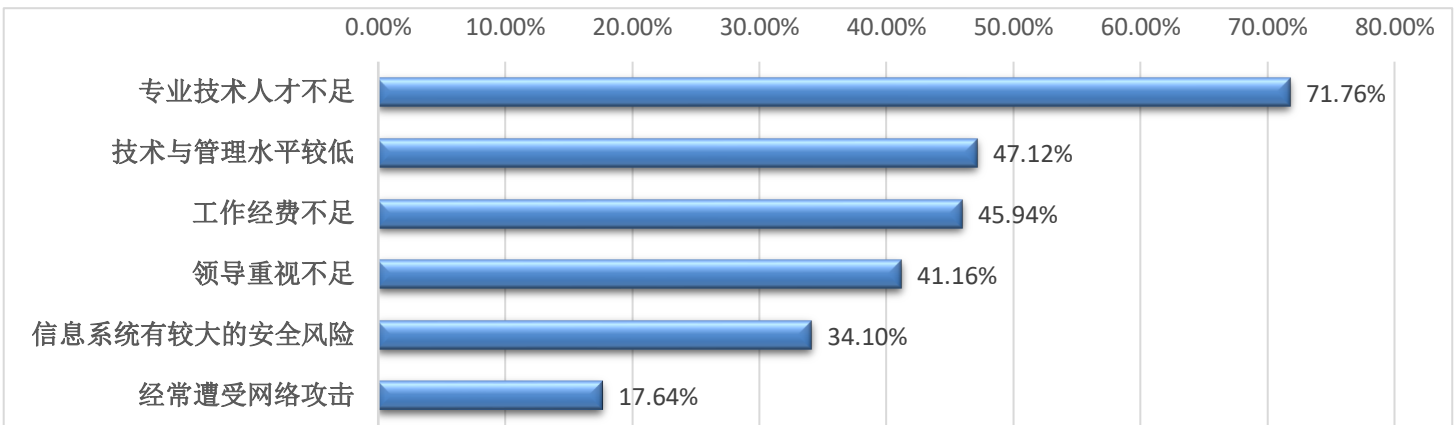


图8-15：网络安全管理的不足

F15. 亟待加强的网络安全立法内容

受调查的 F 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 76.67%，数据安全保护占 60.45%，网络平台责任占 55.74%（如图 8-16）。

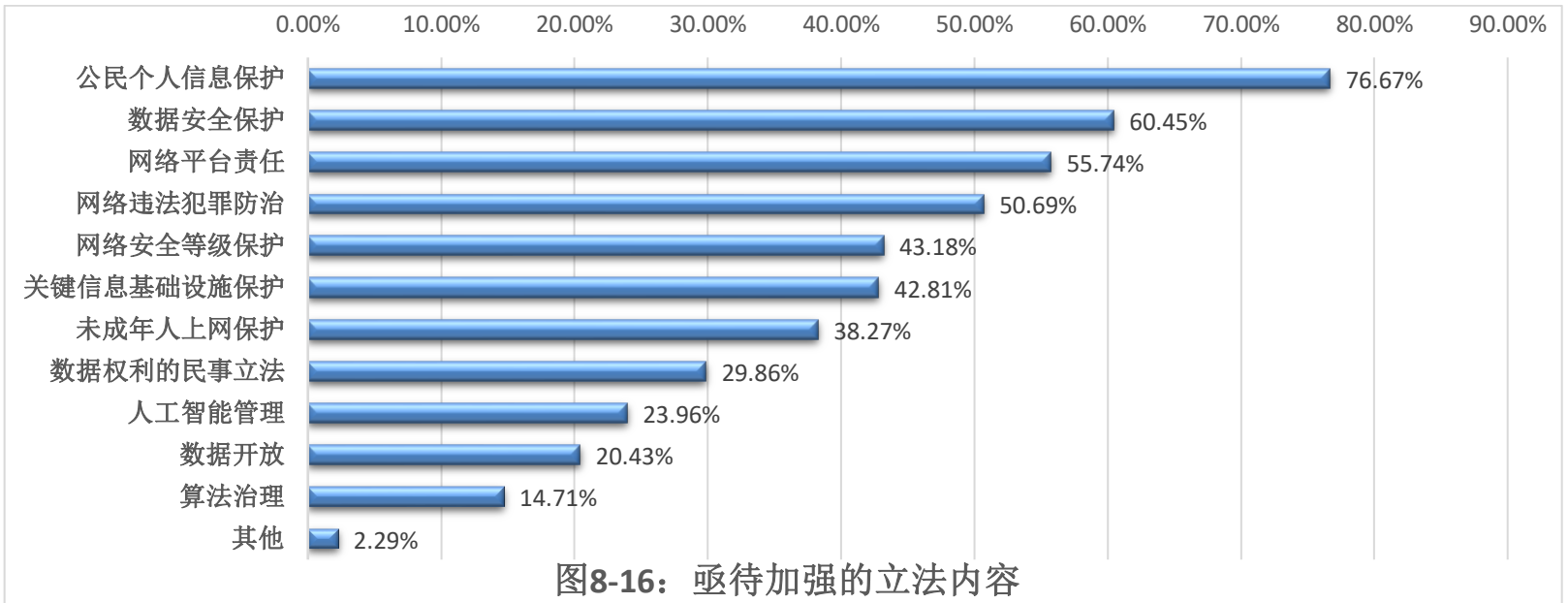


图8-16：亟待加强的立法内容

F16. 对网络安全行政执法部门的认识

受调查的 F 类从业人员认为政府最主要的网络安全执法部门前三位依次是网信（77.55%）、公安（75.29%）、工信（45.98%），如图 8-17 所示。

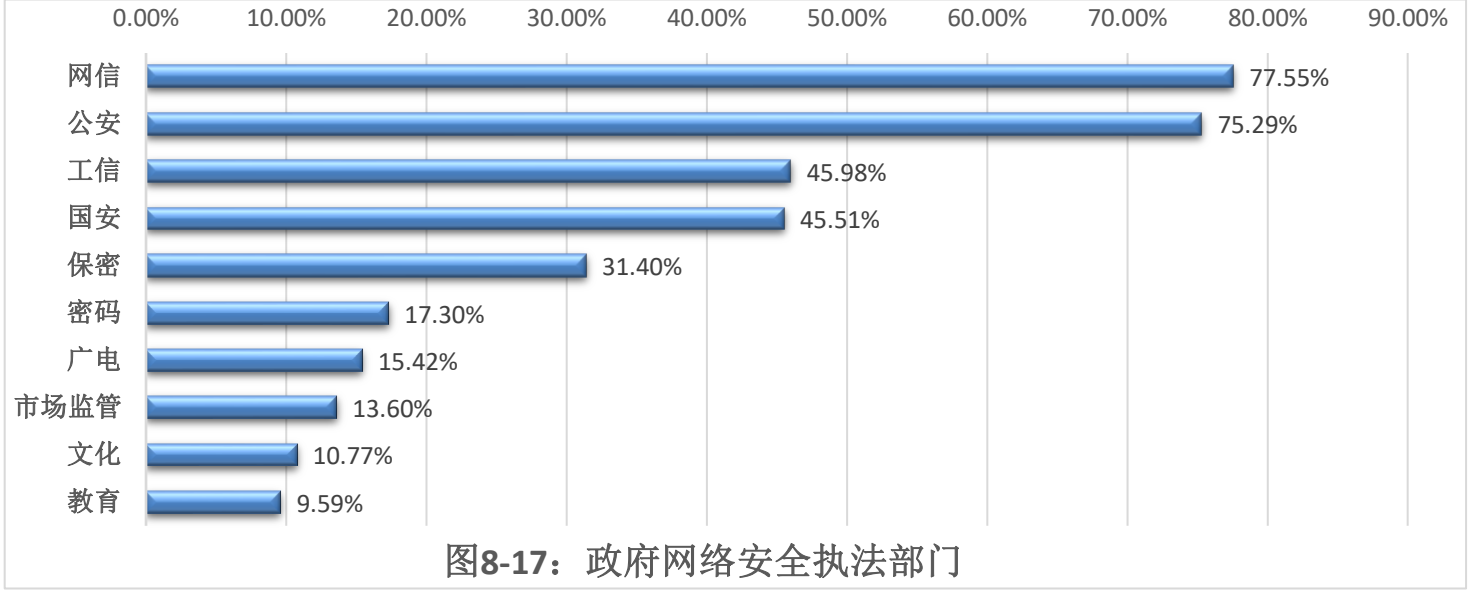


图8-17：政府网络安全执法部门

F16.1、政府部门在网络安全方面的执法力度评价

受调查的 F 类从业人员认为政府部门在网络安全方面的执法力度强的有 13.46%，认为比较强的有 33.96%，两者合计 47.42%；认为不足或严重不足的合计 15.92%（如图 8-18）。

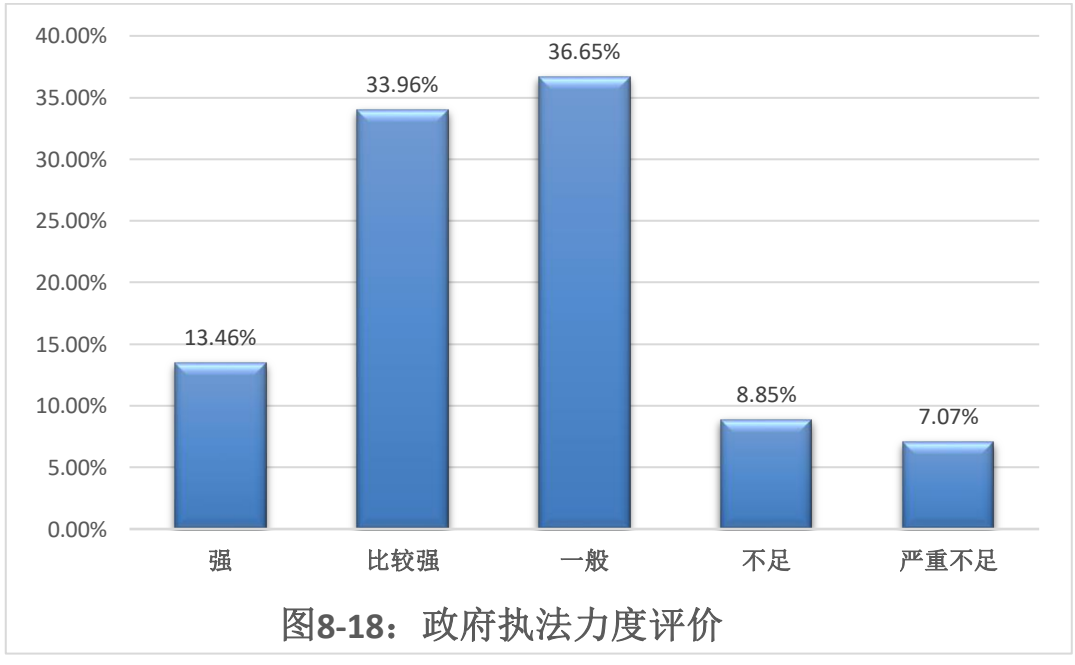


图8-18：政府执法力度评价

F16.2、网络安全执法制约因素

受调查的 F 类从业人员认为影响网络安全执法的制约因素前三位的是：取证能力（60.47% ）、检测能力（58.14%）、人员（56.66%），各类制约因素占比如图 8-19 所示。

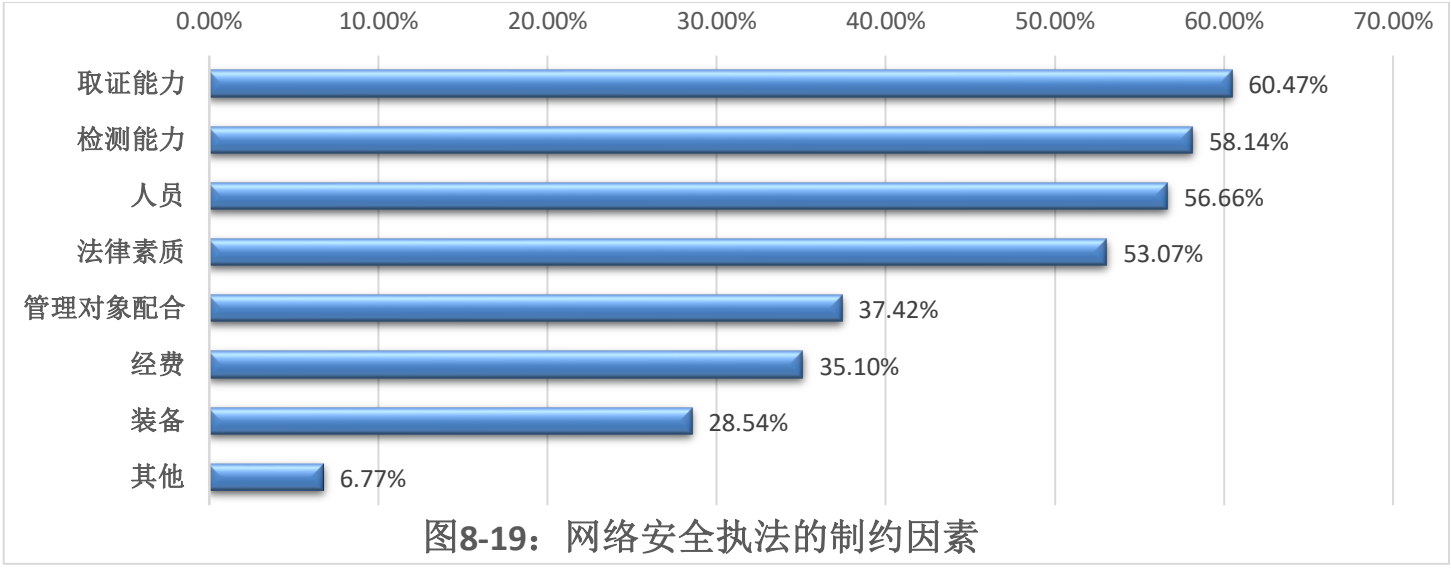


图8-19：网络安全执法的制约因素

F17. 单位进行网络安全等级保护工作情况

单位参与等保工作的比例较高，受调查的 F 类从业人员单位中有 58.94%开展了网络安全自查，58.36%进行了信息系统定级备案（如图 8-20）。

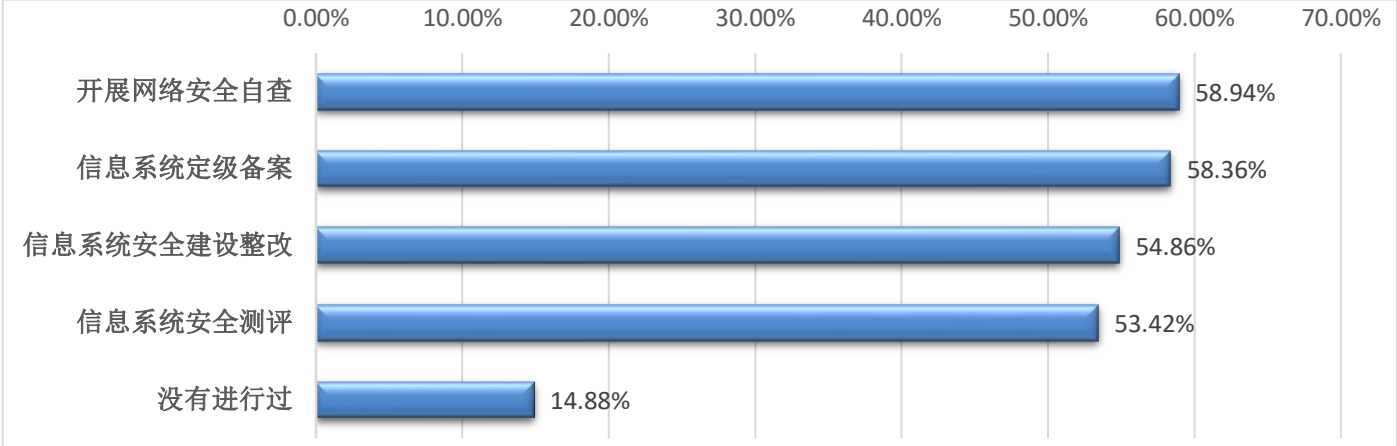


图8-20：单位进行过何种等级保护工作

F17.1、对测评机构进行测评工作的满意度现状

受调查的 F 类从业人员对测评工作评价较高，51.23%的人员对测评机构的工作表示满意（如图 8-21）。

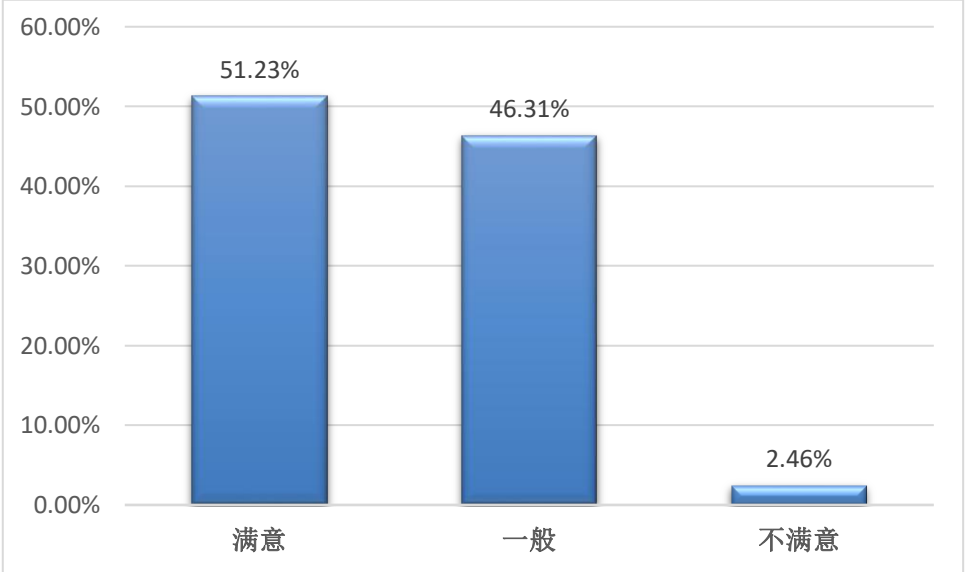


图8-21：测评机构满意度

F18. 网络安全等级保护制度重大意义的认识

受调查的 F 类从业人员对网络安全等级保制度的意义认识比较务实，有 79.8%的人员认为是国家网络安全领域的基本政策和基本制度（如图 8-22）。

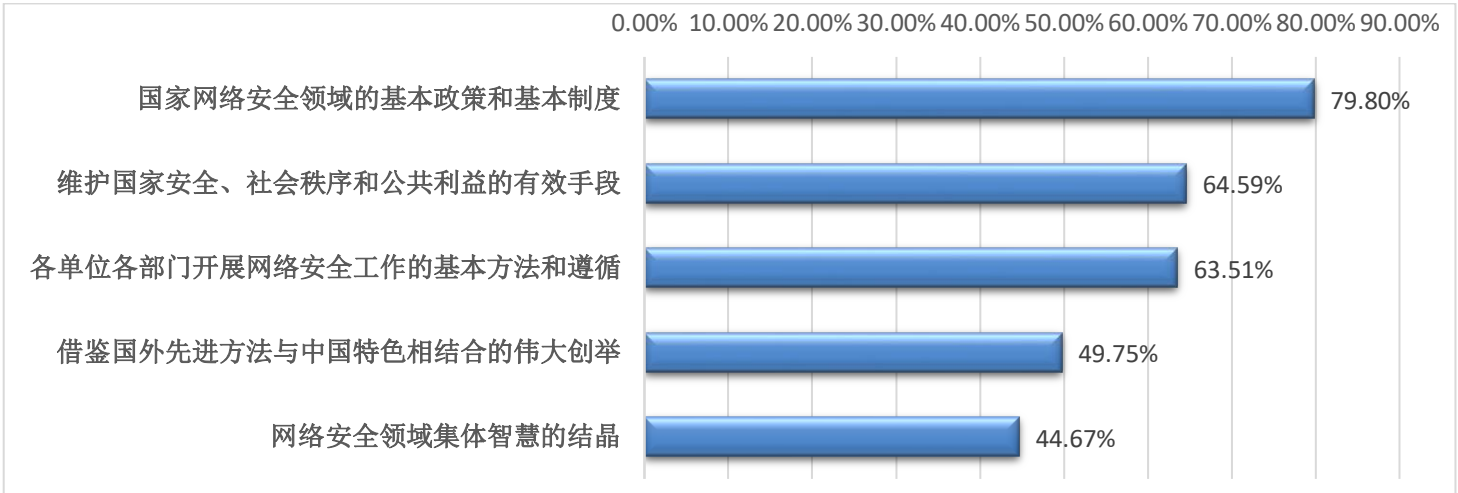


图8-22：等级保护重大意义

F19. 哪些单位应该开展网络安全等级保护工作

大部分受调查的 F 类从业人员对有等保义务单位范围的认识基本正确，但仍有 35.71%的人员选择了家庭和个人（如图 8-23）。

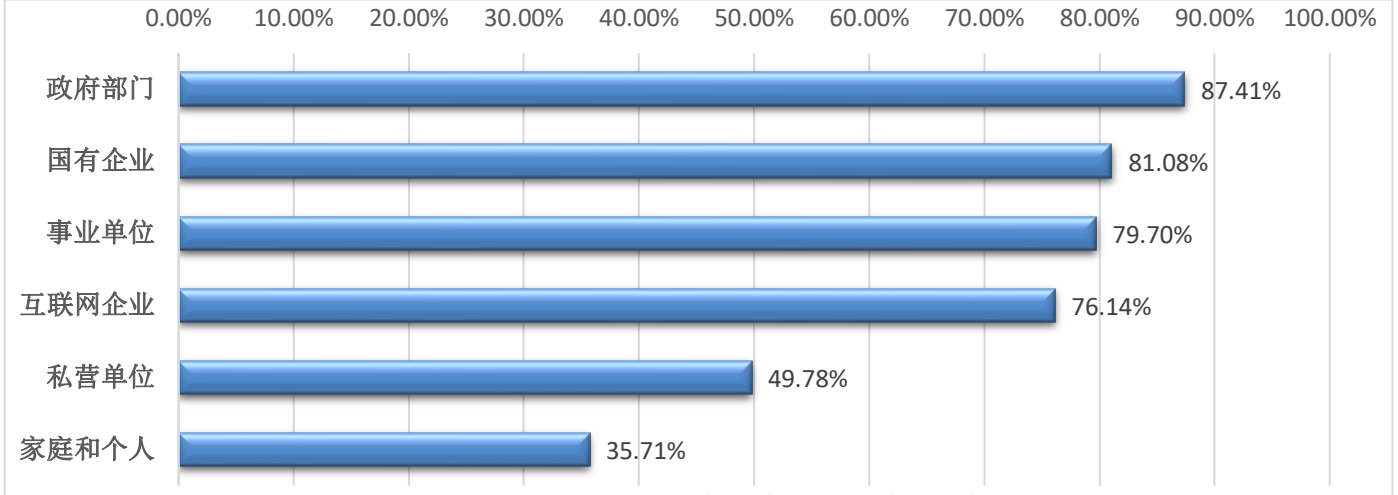


图8-23：应该开展等级保护工作的单位

F20. 哪些系统应该开展网络安全等级保护工作

受调查人的 F 类从业人员认为最该开展等级保护的系统前三位依次是关键信息基础设施占 80.07%，大数据系统占 74.08%，行业专网和业务信息系统占 73.75%（如图 8-24）。

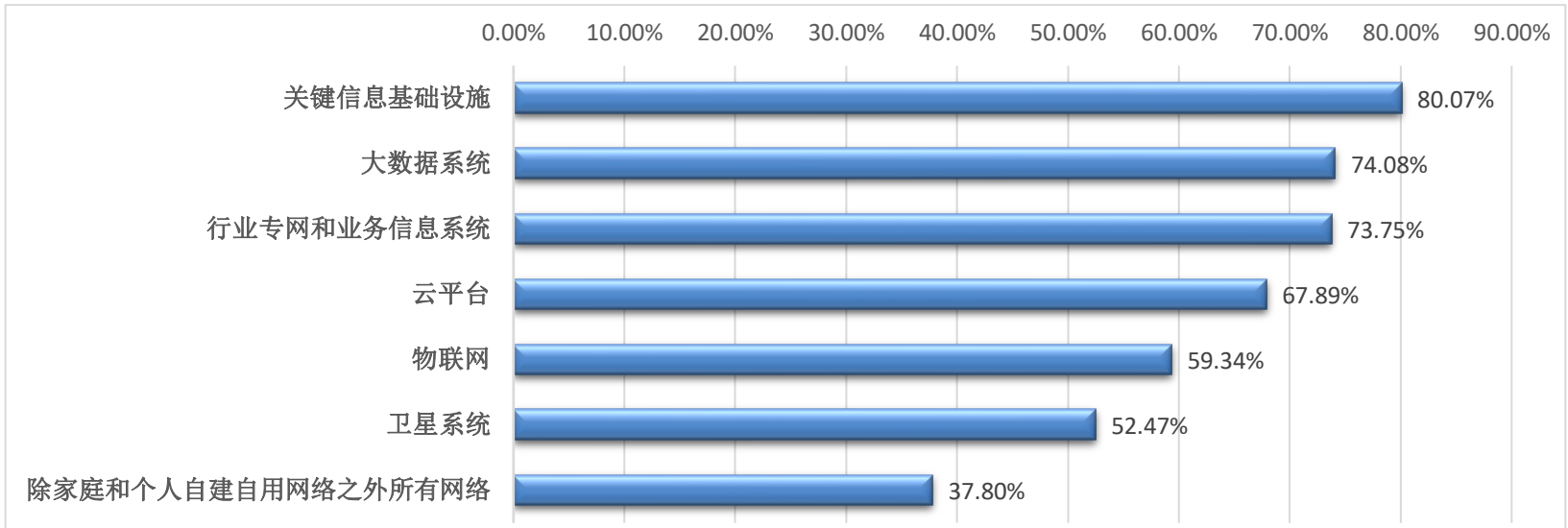


图8-24：应该开展等级保护工作的系统

F21. 对网络安全等级保护制度 2.0 国家标准要求的了解

受调查的 F 类从业人员了解网络安全等级保护制度 2.0 国家标准要求的占 47.63%，不了解的占 52.37%（如图 8-25）。

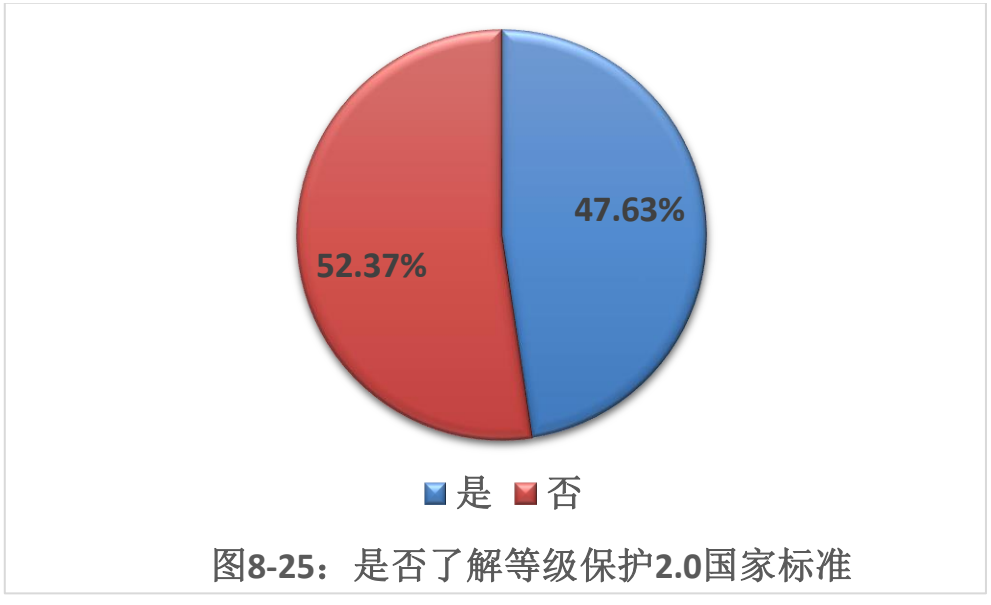


图8-25：是否了解等级保护2.0国家标准

F21.1、等保 2.0 的了解渠道

单位或政府组织的培训是受调查的 F 类从业人员了解等保 2.0 标准的主要渠道，占比 57.39%，其次为行业论坛（51.31%），如图 8-26 所示。

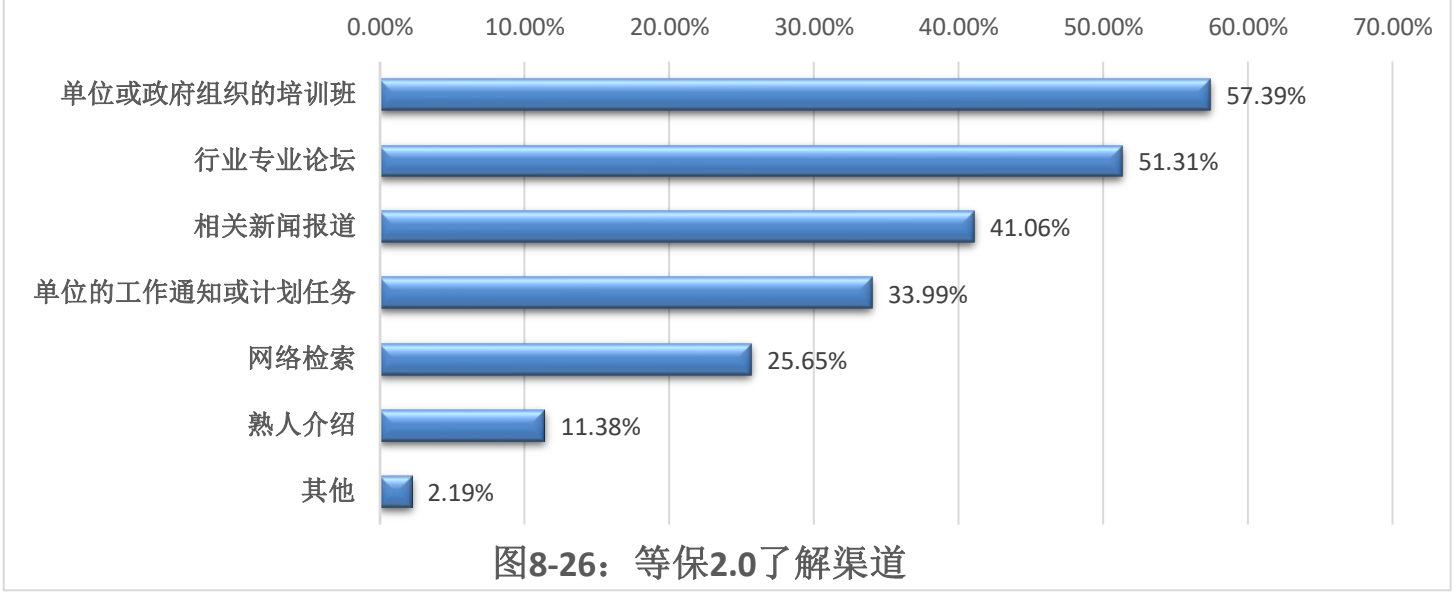


图8-26：等保2.0了解渠道

F22. 单位发生网络安全事件情况

单位没有发生过网络安全事件的受调查 F 类从业人员占比 56.41%（如图 8-27）。

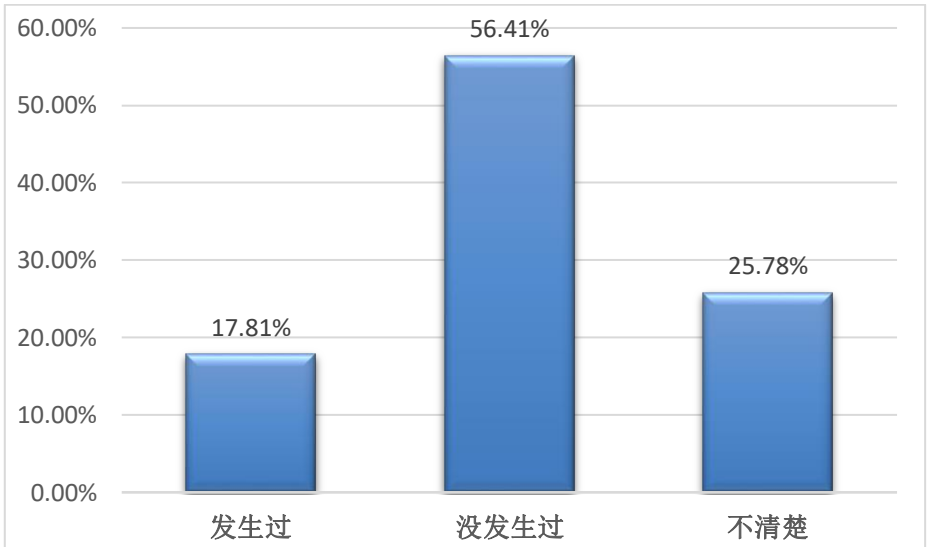


图8-27：单位网络安全事件发生情况

F22.1、安全事件的类型

受调查的 F 类从业人员单位发生最多的网络安全事件是网站被攻击篡改，占比 37.05%（如图 8-28）。

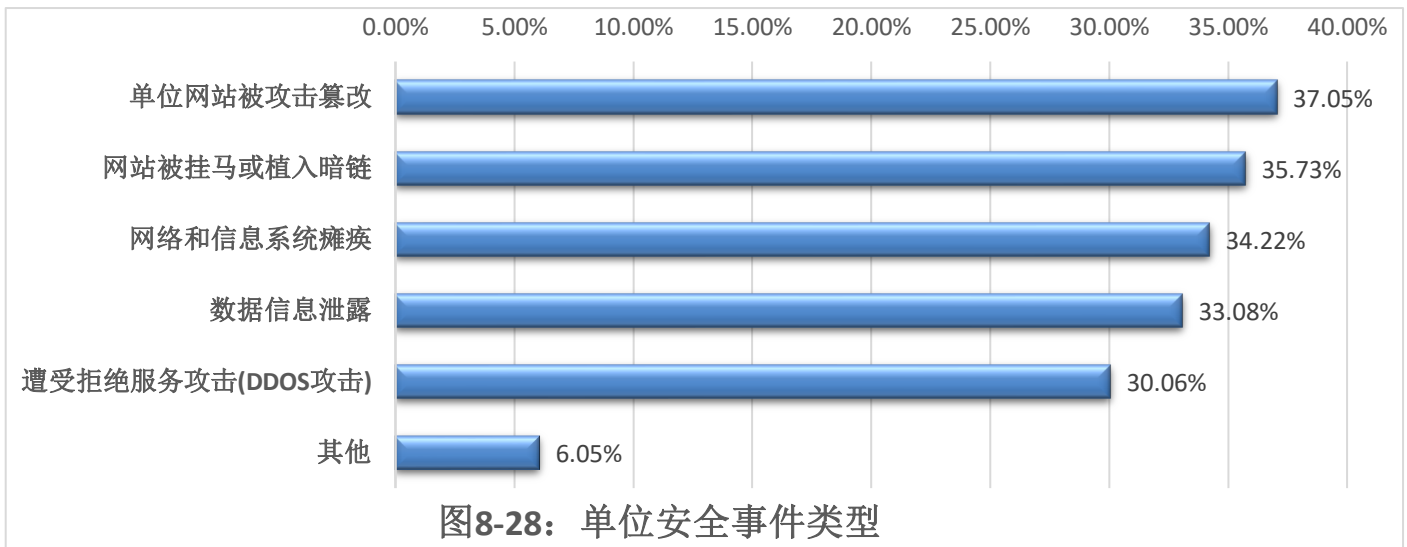


图8-28：单位安全事件类型

F22.2、单位针对发生的网络安全事件向公安机关报案情况

有 45.56%的受调查 F 类从业人员单位，在遇到网络安全事件时选择向公安机关报案（如图 8-29）。

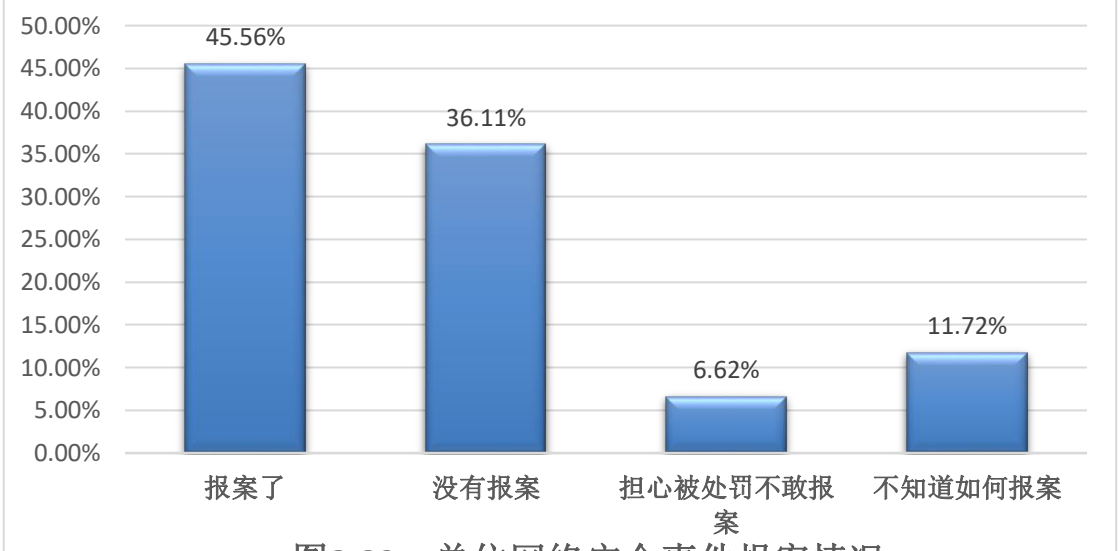


图8-29：单位网络安全事件报案情况

F22.3、对公安机关案件受理情况的满意度

受调查的 F 类从业人员对公安机关案件受理情况满意的占比 63.49%（如图 8-30）。

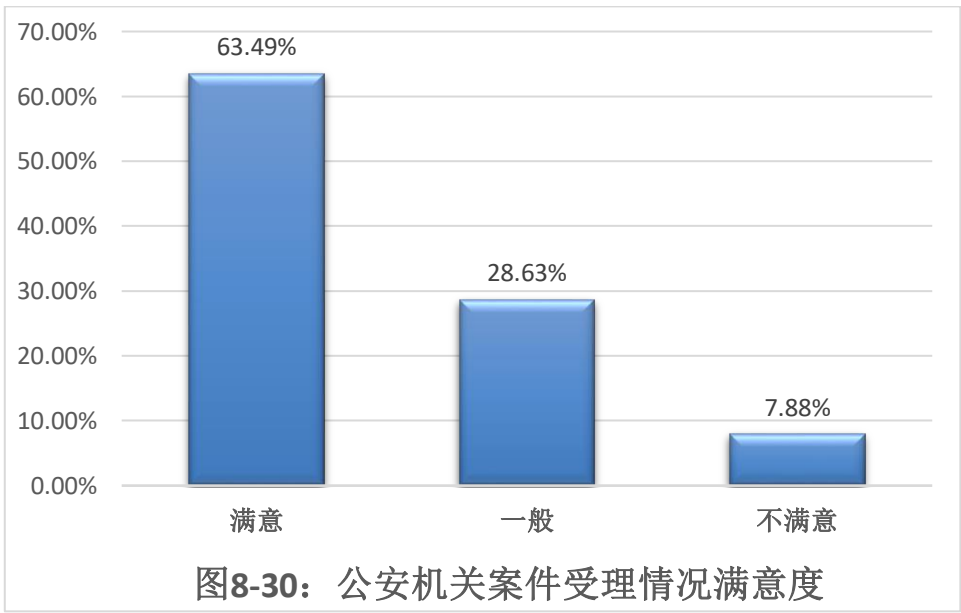


图8-30：公安机关案件受理情况满意度

F23. 公安机关网络安全执法检查工作满意度

受调查的 F 类从业人员对公安机关网络安全执法检查工作评价满意的占 39.04%，排除没有参加过检查的 15.38%的样本，调整后满意的占比 46.14%（如图 8-31）。

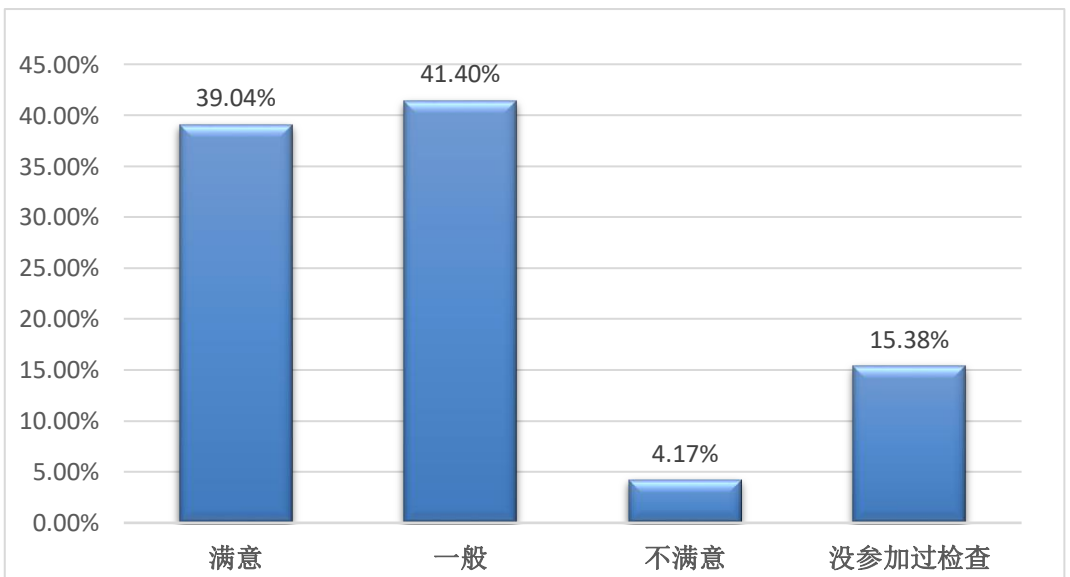


图8-31：公安机关网络安全执法满意度

F24. 网络安全等级保护对产业、企业发展的推动作用的认识

受调查的 F 类从业人员对网络安全等级保护的作用认识比较正面，有 62.47%的人员认为网络安全等级保护对产业、企业发展的推动很大（如图 8-32）。

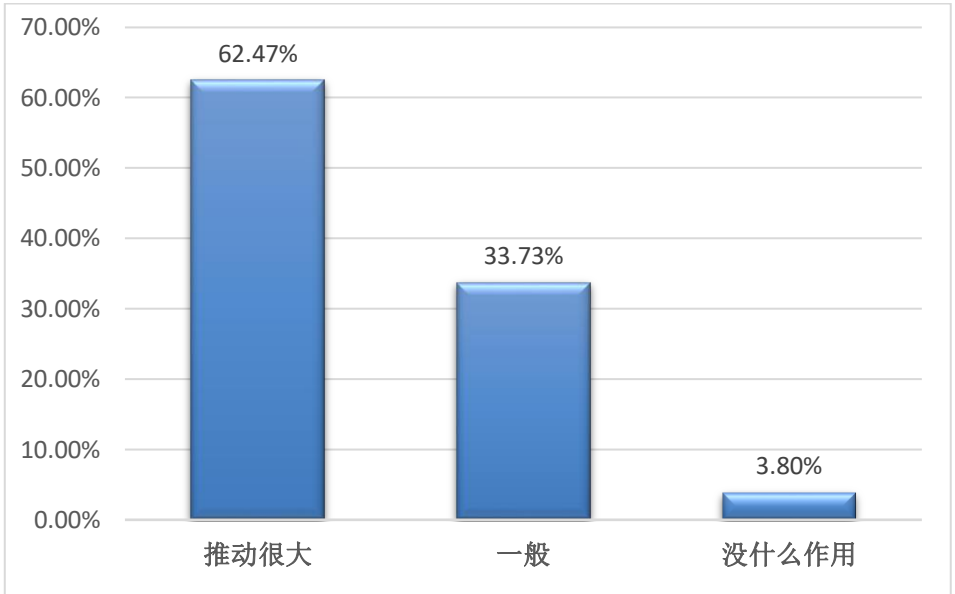


图8-32：网络安全等级保护作用认识

九、G 卷：科研机构、大学从业人员

科研机构、大学（G 类）从业人员熟悉安全技术发展状况，态度比较中立。

G 问卷有效答卷数量 2442 份，以下是 G 类问卷各项数据的详细统计结果。

G3. 当前网络安全状况

受调查的 G 类从业人员认为网络安全状况良好有 26.04%，认为状况一般的占 51.35%，认为状况堪忧的占 22.6%（如图 9-1）。

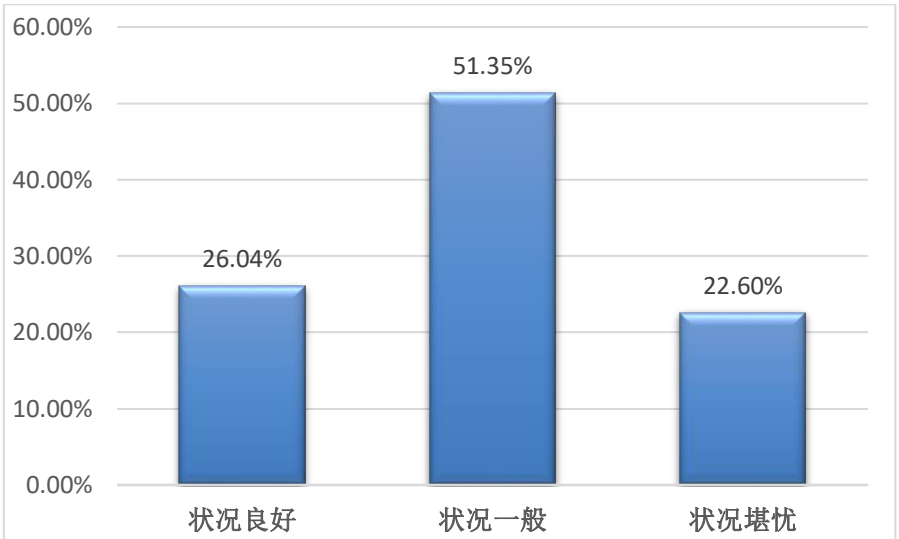


图9-1：安全状况评价

G3.1、与去年相比网络安全感的变化

受调查的 G 类从业人员有 15.85%认为有明显改善，有 45.37% 的人员认为有改善，两者合计有 61.22%的人员认为网络安全状况改善或明显改善（如图 9-2）。

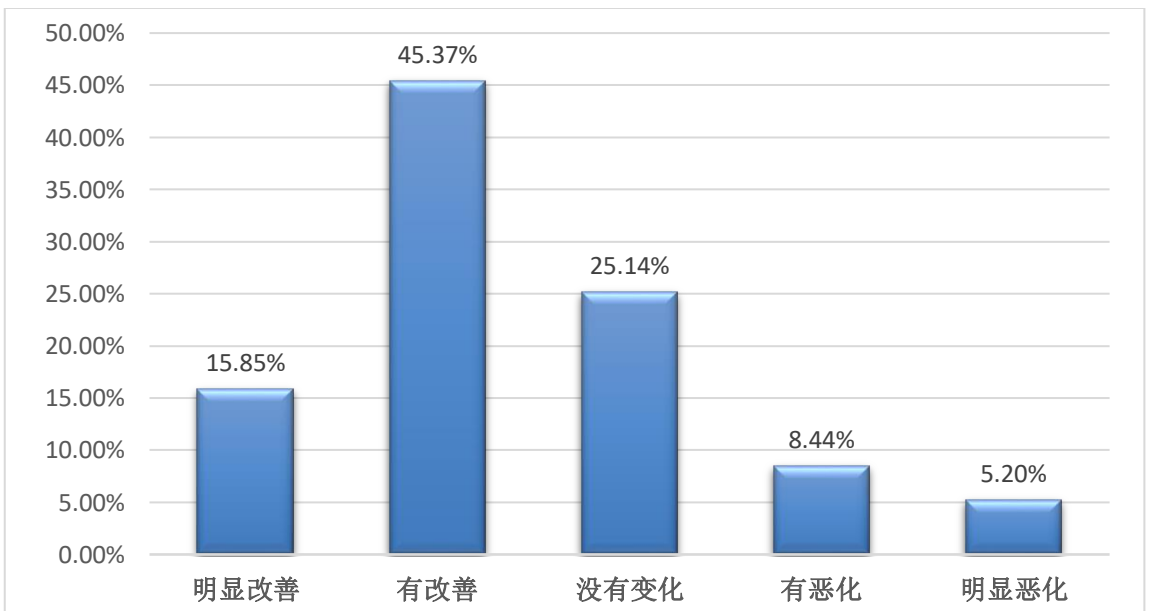


图9-2：网络安全感变化评价

G4. 单位网络安全方面的科研经费预算

受调查的 G 类从业人员认为单位在网络安全方面经费预算充裕的占 12.04%，较充裕的占 17.65%，两者合计共有 29.69%的人员认为经费充裕，认为较少（18.3%）和没有（18.76%）的合计共有 37.06%（如图 9-3）。

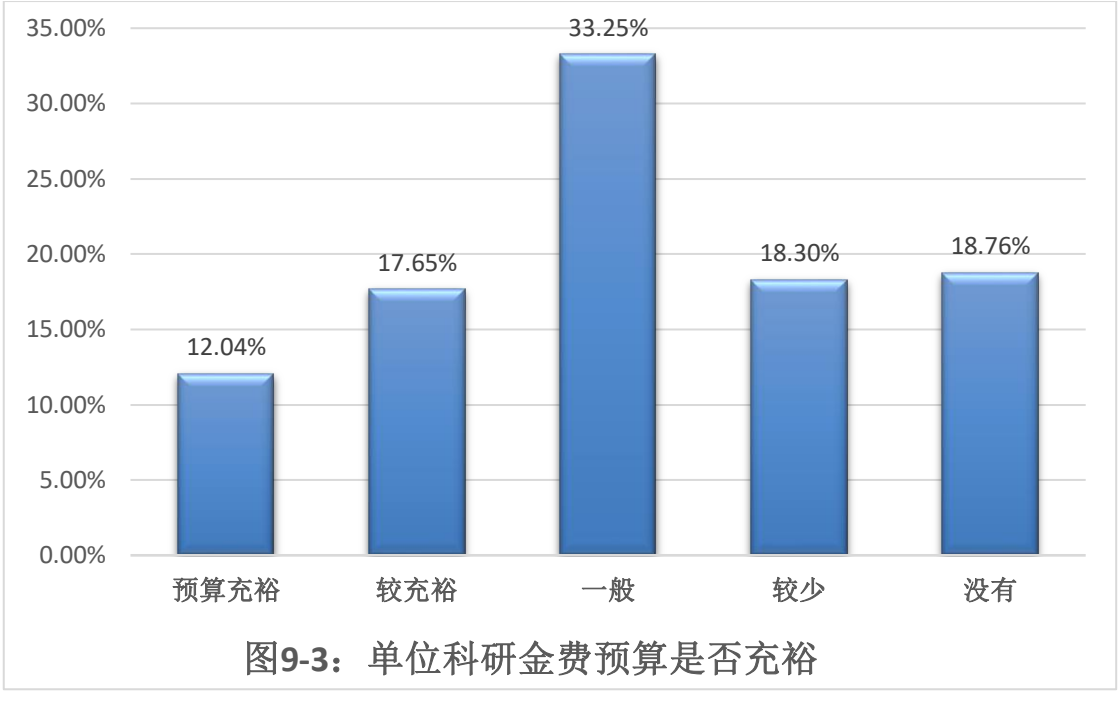


图9-3：单位科研金费预算是否充裕

G5.网络安全科研课题立项和管理状况满意度

受调查的 G 类从业人员对网络安全科研课题立项和管理状况满意的占 17.04%，较满意的占 23.83%，两者合计有 40.87%的人员认为满意或较满意（如图 9-4）。

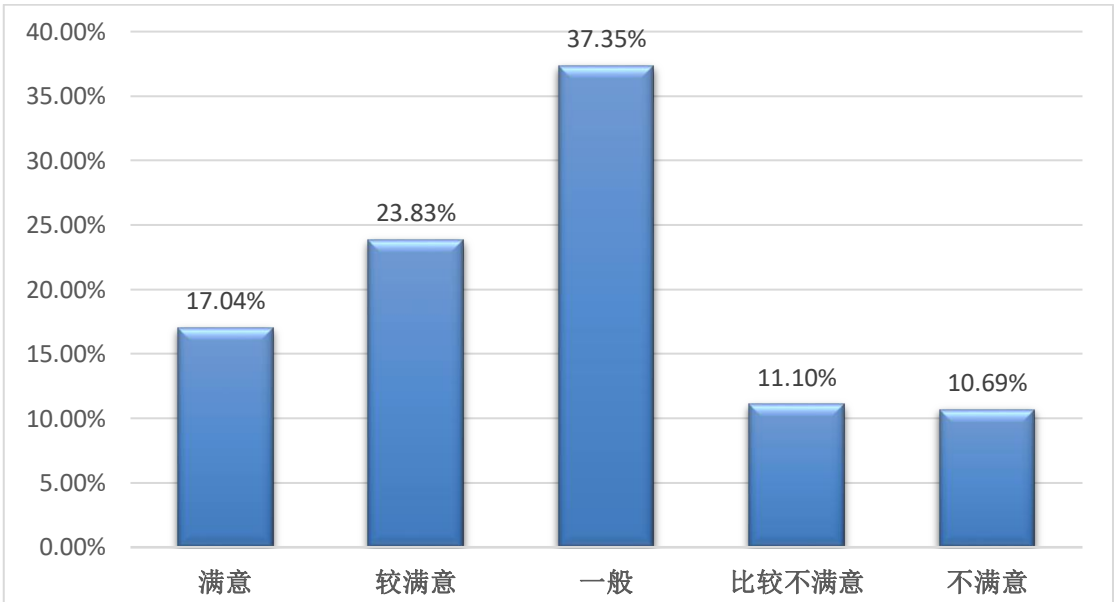


图9-4：课题立项和管理状况满意度

G6.网络安全科研工作开展改善需求

受调查的 G 类从业人员认为网络安全科研工作最需要改善的是课题规划，有 57.29%的人员选择，从整体上看 G 类从业人员对所列内容都有较多的改善需求（如图 9-5）。

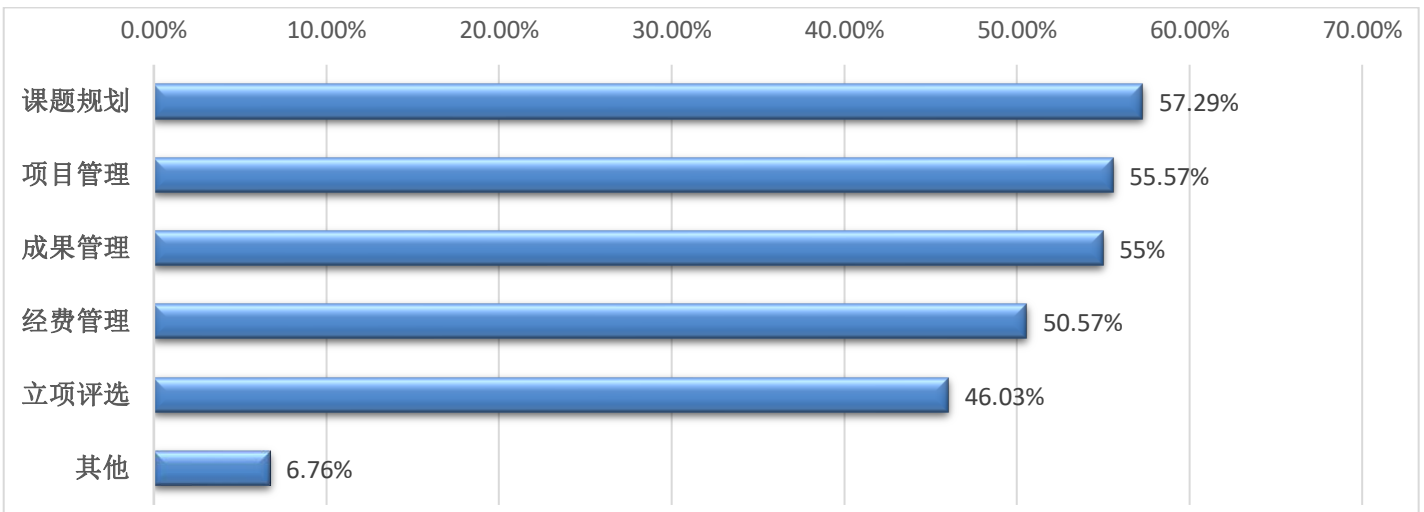


图9-5：科研工作开展需求

G7. 网络安全方面科研成果转化状况满意度

受调查的 G 类从业人员对网络安全科研成果转化状况满意的占 16.3%，较满意的占 26.95%，两者合计有 43.25%的人员认为满意或较满意（如图 9-6）。

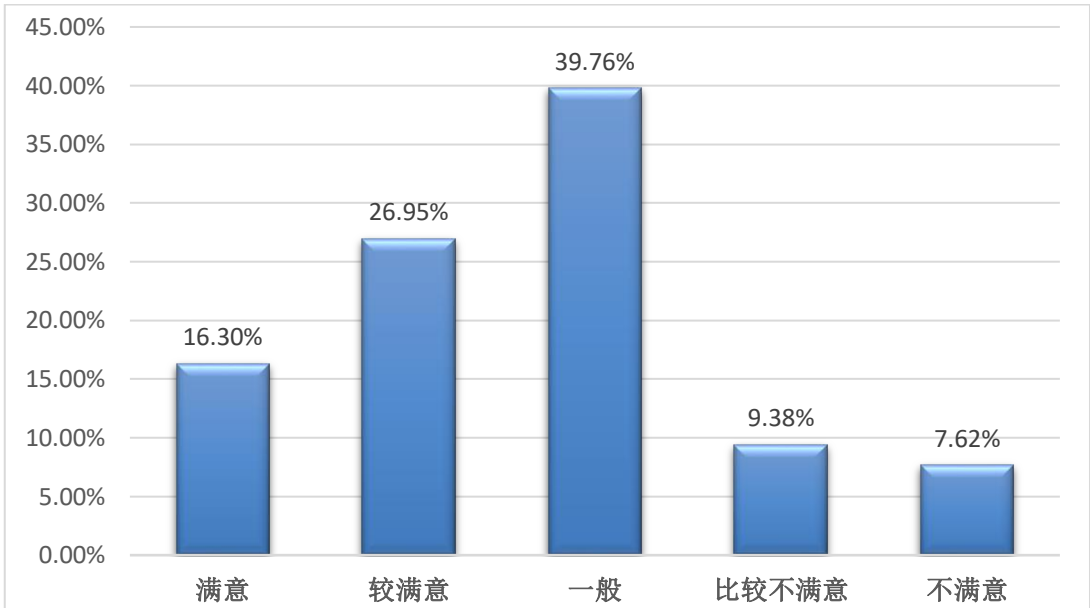


图9-6：网络安全科研成果转化状况满意度

G7.1、哪些方面感到不满意

受调查的 G 类从业人员对科研成果转化最不满意的是管理机制，有 62.17%的人员选择，从整体上看 G 类从业人员对所列内容都有较多的选择（如图 9-7）。

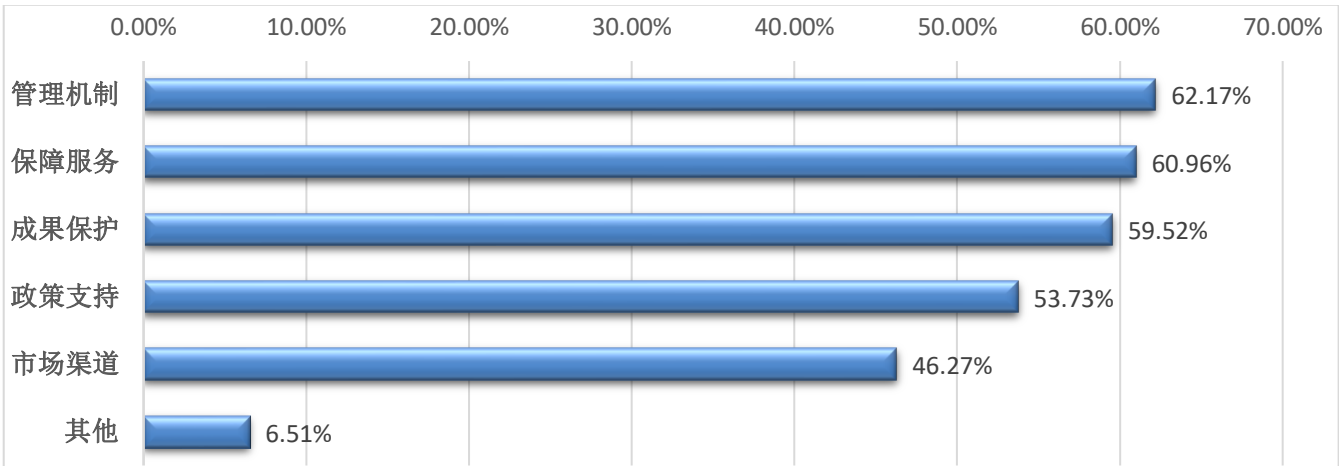


图9-7：哪些方面不满意

G8. 网络安全方面的学科建设状况满意度

受调查的 G 类从业人员对网络安全方面的学科建设状况满意的占 17.98%，较满意的占 28.17%，两者合计有 46.15%的人员认为满意或较满意（如图 9-8）。

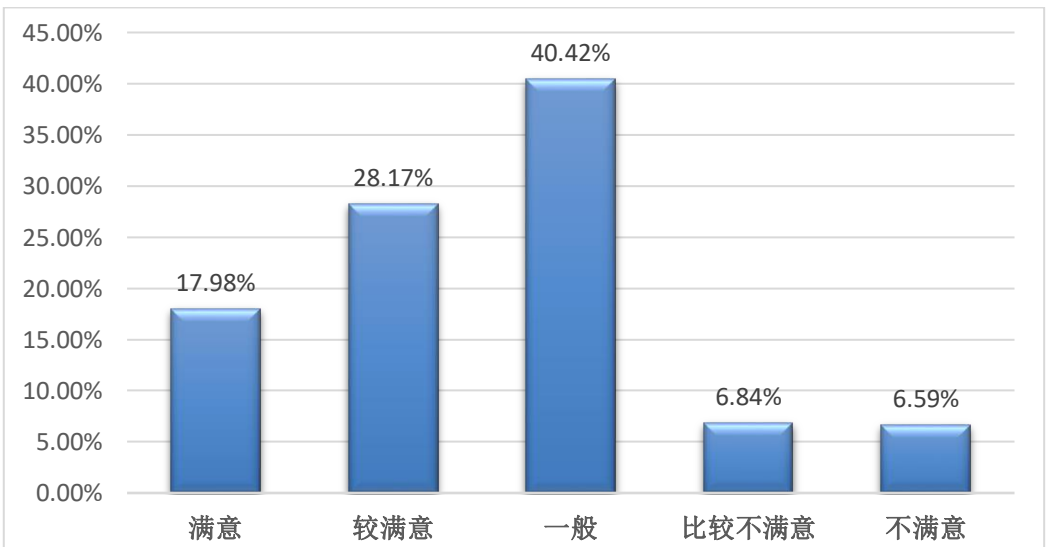


图9-8：学科建设状况满意度

G9. 单位开设网络安全课程情况

受调查的 G 类从业人员单位有 26.74% 将网络安全课程作为专业课在信息类学院/研究室开设， 23.55%作为通识选修课， 21.17%作为通识必修课， 16.75%没有开设（如图 9-9）。

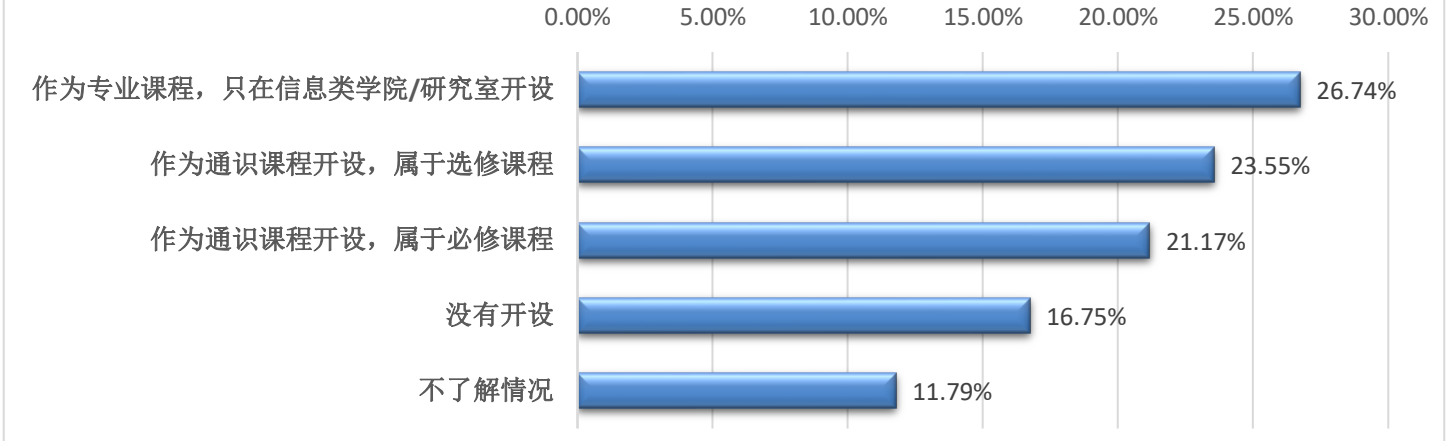


图9-9：开设网络安全课程情况

G10. 单位开展对学生关于网络安全的培训情况

受调查的 G 类从业人员单位对学生开展网络安全培训最多的是对新生进行培训，有 35.68%的人员选择，其次是开展专题讲座占 32.81%（如图 9-10）。

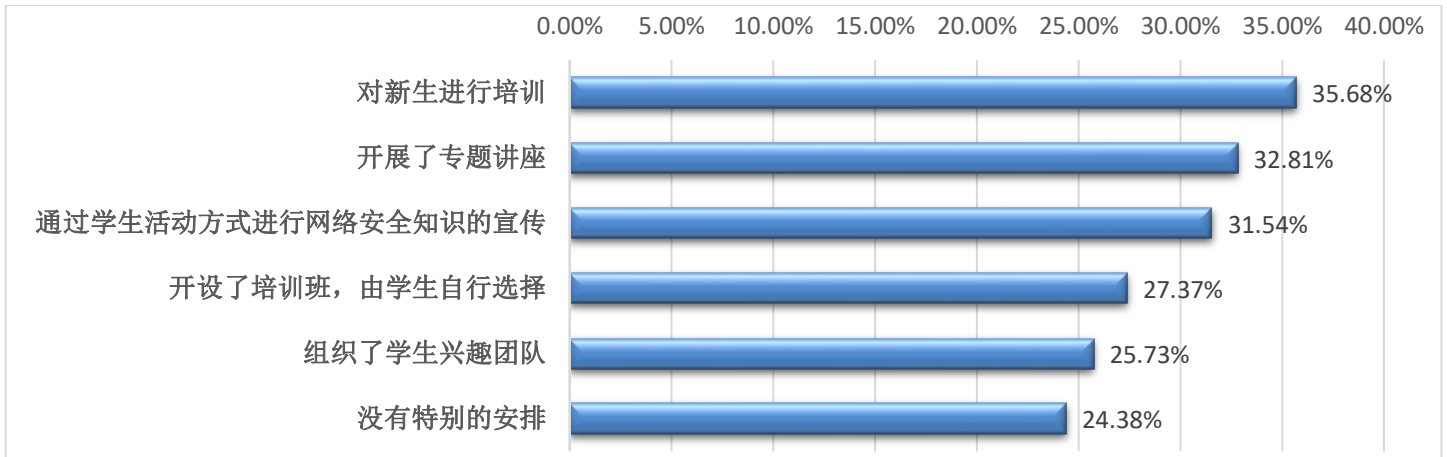


图9-10：开展网络安全培训情况

G11. 单位对网络安全责任人和技术人员开展关于网络安全的培训情况

受调查的 G 类从业人员单位对网络安全责任人和技术人员每年都开展（1 次及以上）网络安全培训的共计有 71.13%，有 28.87 %的单位没有开展过培训（如图 9-11）。

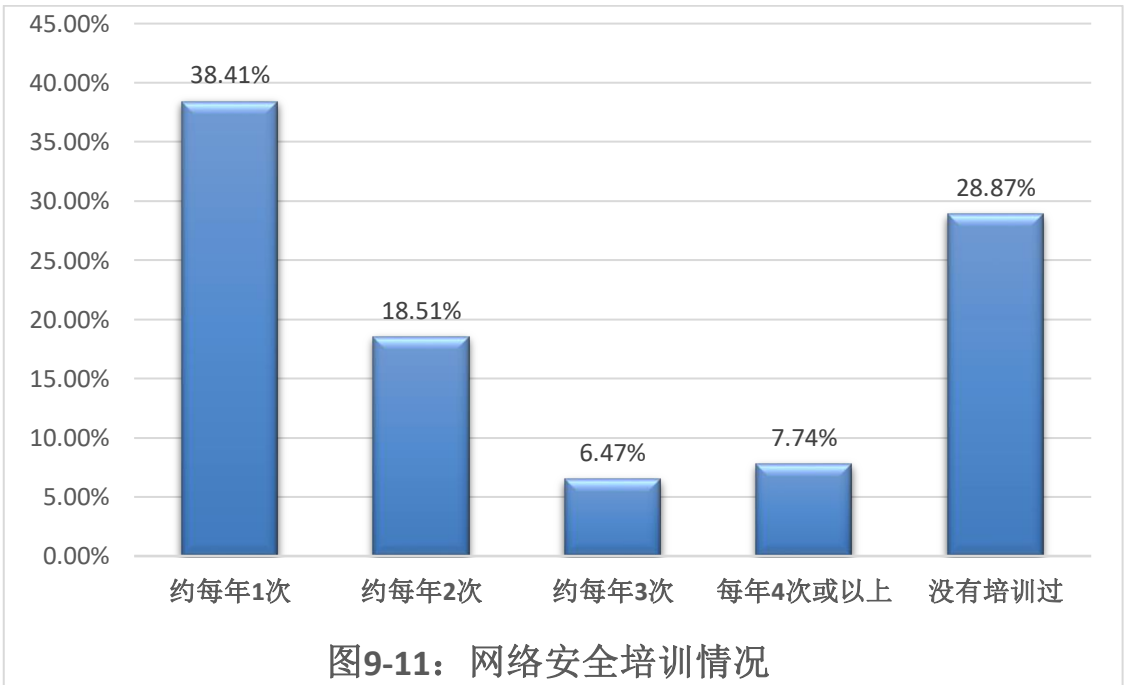


图9-11：网络安全培训情况

G11.1、单位对全体人员开展关于网络安全的培训情况

受调查的 G 类从业人员单位对全体人员每年都开展（1 次及以上）网络安全培训的共计有 61.59%，有 38.41%的单位没有开展过培训（如图 9-12）。

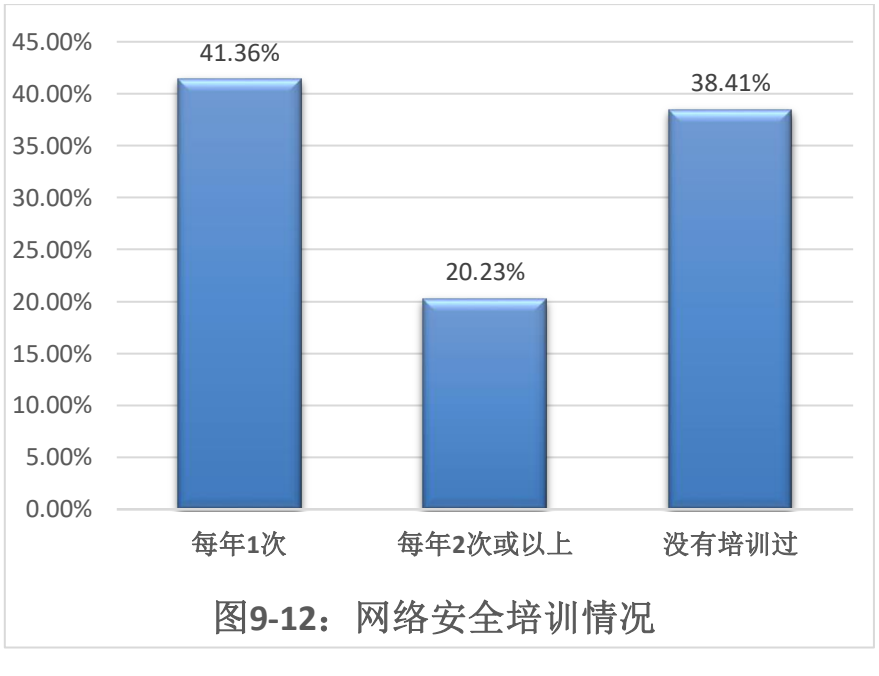


图9-12：网络安全培训情况

G12. 单位网络安全责任落实情况

对于单位网络安全责任落实情况，受调查的 G 类从业人员有 34.48%不了解情况，有 32.92%认为每个部门都确定安全责任人并落实了安全责任，有 17.08%认为安全责任没有落实到每个部门，有 15.52%认为每个部门都确定安全责任人但没有明确安全责任（如图 9-13）。

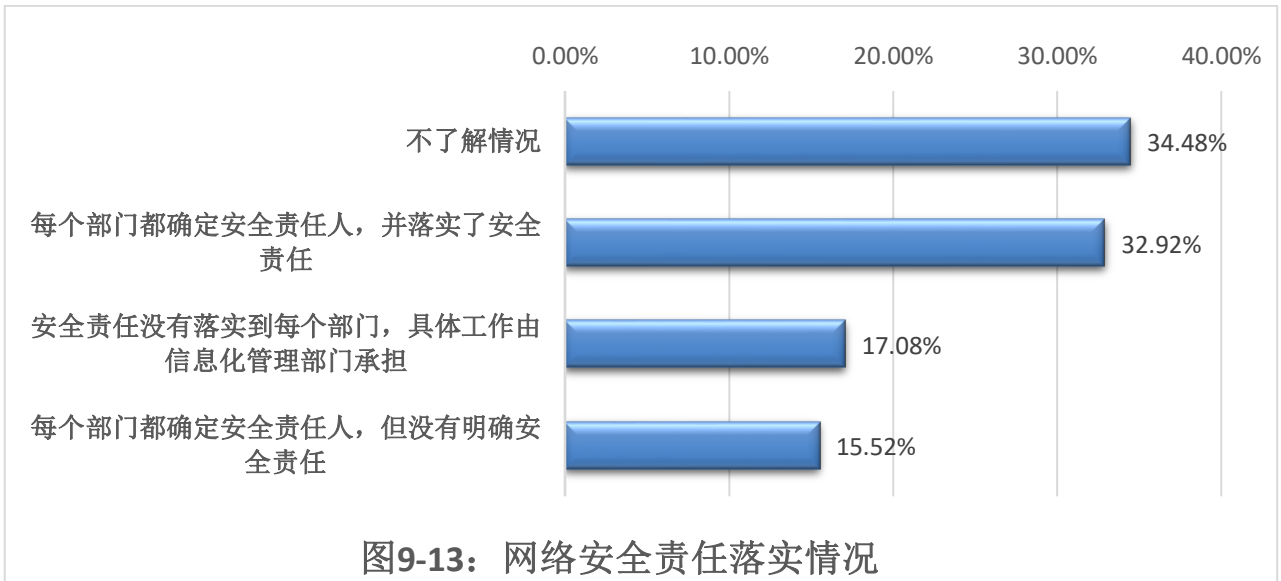


图9-13：网络安全责任落实情况

G13. 当前网络安全最突出的问题

受调查的 G 类从业人员认为最突出的网络安全问题是个人信息泄露，有 83.88%的人员选择，排名第二和第三的分别是网络诈骗（43.84%）、网络侵权盗版（40.86%），各类网络安全问题占比如图 9-14 所示。

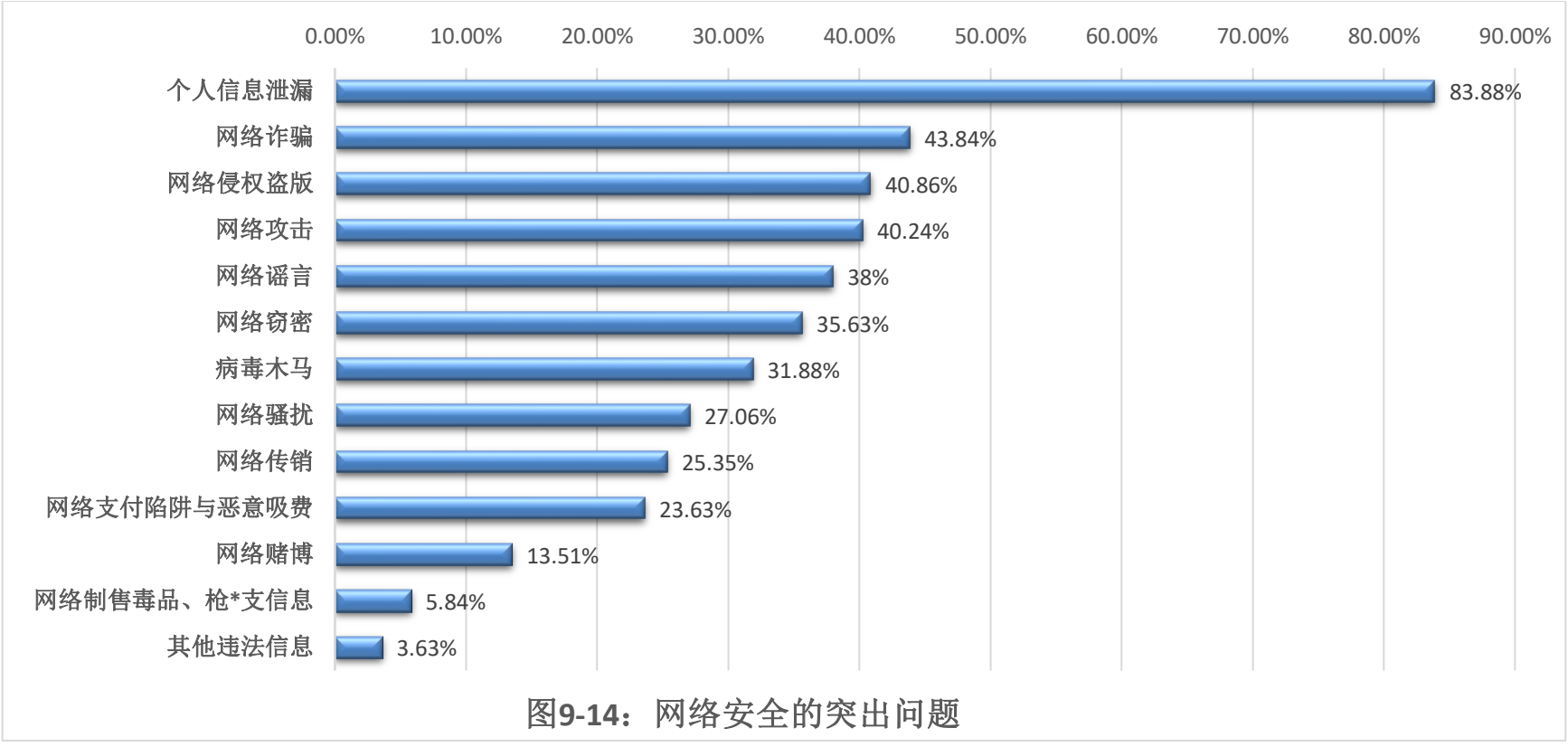


图9-14：网络安全的突出问题

G14. 政府网络安全管理政策措施对单位的影响

受调查的 G 类从业人员认为政府网络安全管理措施对单位影响最大的前三位依次是提高了意识（66.22%）、提高了风险防控水平（41.07%）、建立了组织体系（33.37%），各类影响占比如图 9-15 所示。

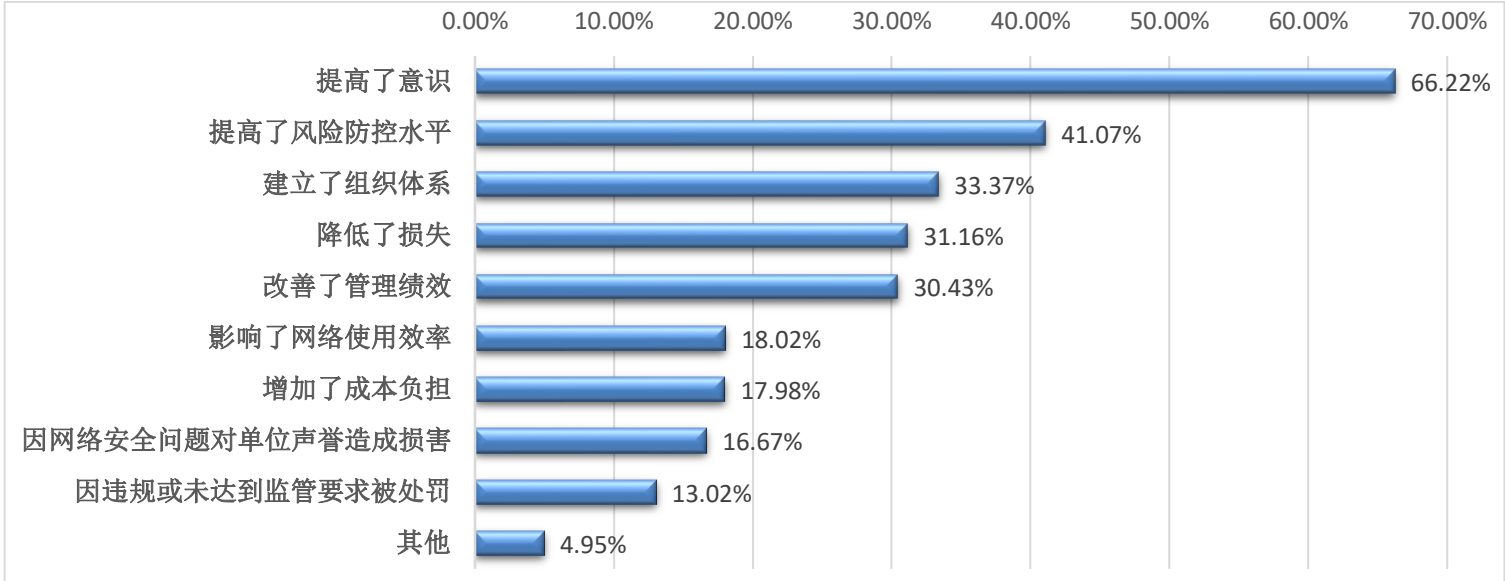


图9-15：政府政策措施对单位的影响

G15. 当前政府机关和事业单位网络安全管理的不足

受调查的 G 类从业人员认为当前政府机关和事业单位网络安全管理最不足的是专业技术人才，有 60.11%的人员选择，其次有 50.82%的人员选择技术与管理水平较低（如图 9-16）。

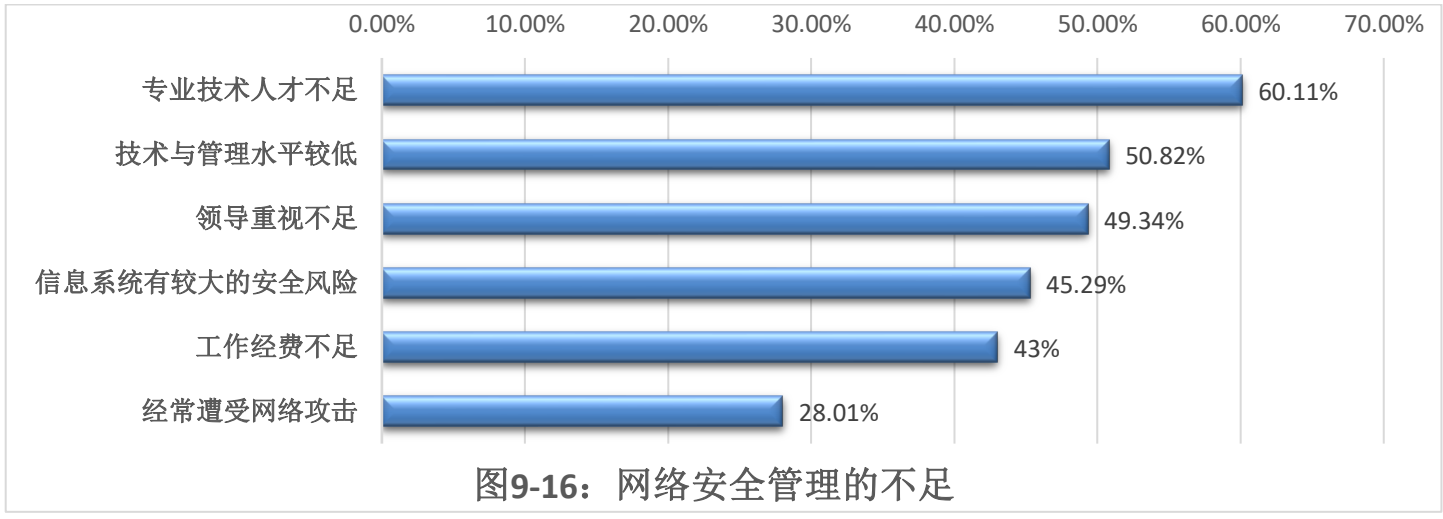


图9-16：网络安全管理的不足

G16. 亟待加强的网络安全立法内容

受调查的 G 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 72.4%，网络平台责任占 57.99%，数据安全保护占 55.57%（如图 9-17）。

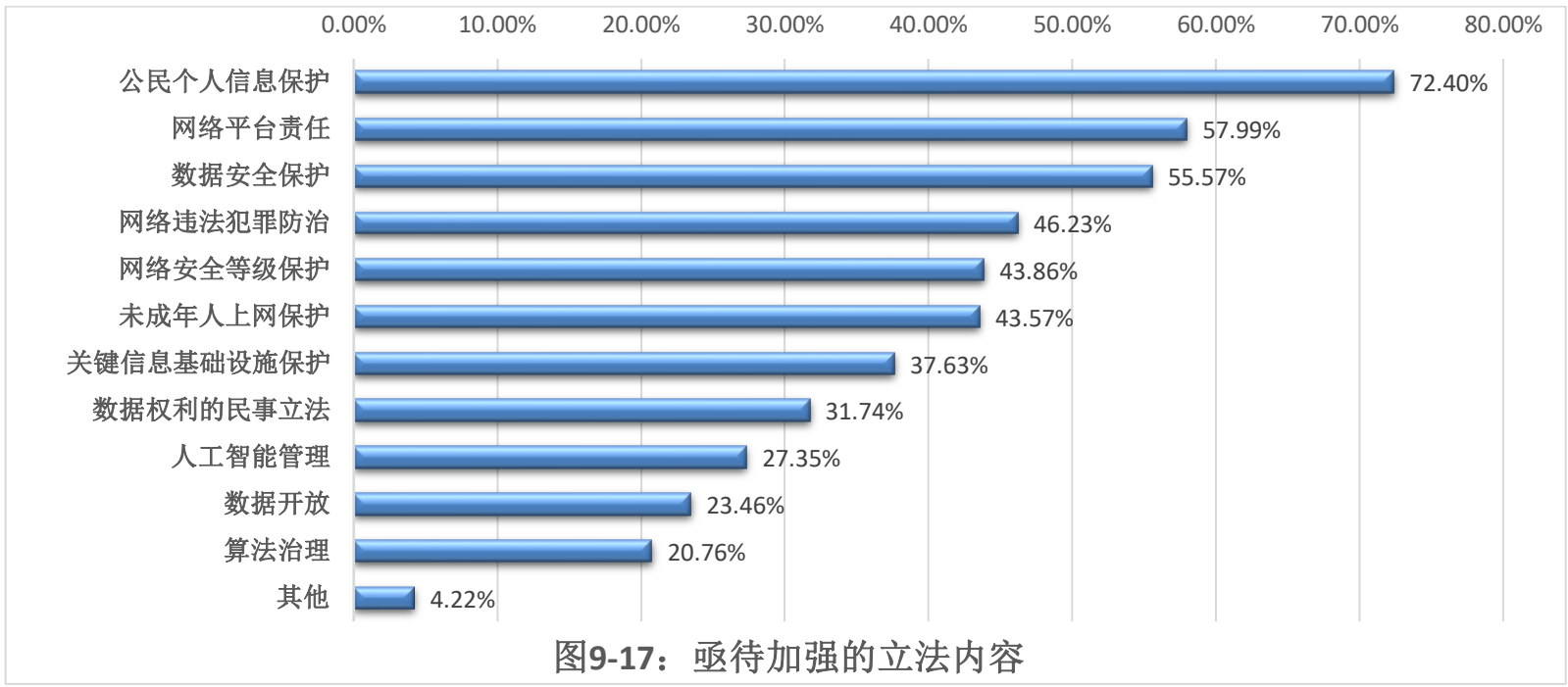


图9-17：亟待加强的立法内容

G17. 5G 网络应用的安全问题的关注

受调查的 G 类从业人员比较关注 5G 网络应用的安全问题，有 62.9%的人员关注过 5G 网络应用的安全问题（如图 9-18）。

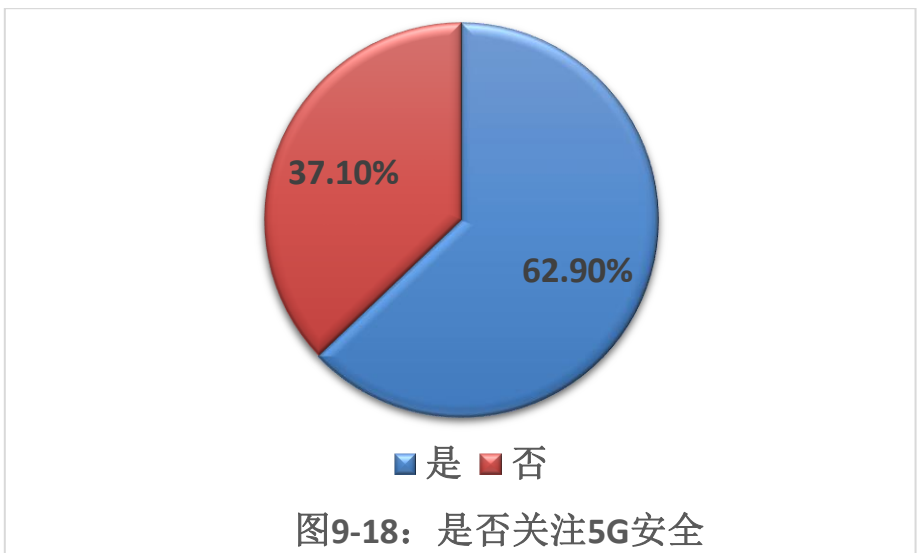


图9-18：是否关注5G安全

G17.1、5G 安全问题的关注重点

受调查的 G 类从业人员关注的重点在 5G 网络安全治理架构、移动终端安全、安全产品，分别占 65.71%、62.39%、55.95%（如图 9-19）。

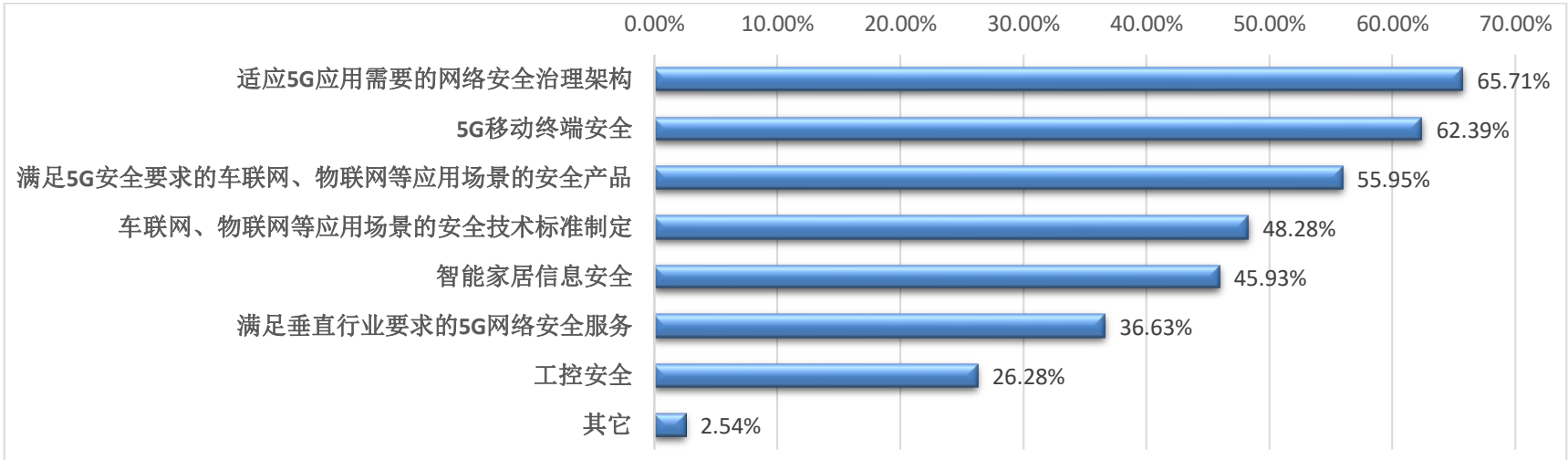


图9-19：5G安全关注重点

G18. 5G 时代应当重点加强安全管理措施

在安全管理措施方面，受调查的 G 类从业人员认为应重点加强 5G 网络安全技术标准体系建设（66.13%）、知识产权管理（57.86%）等措施（如图 9-20）。

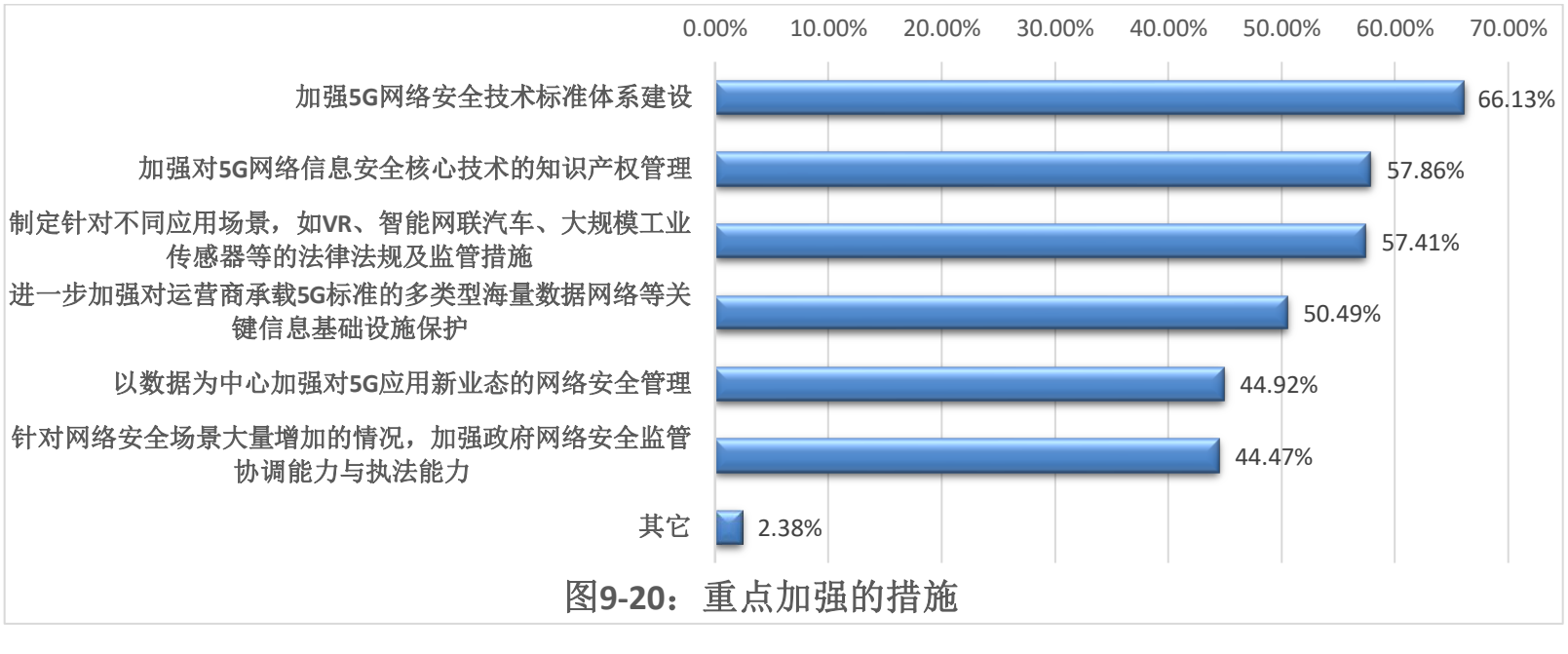


图9-20：重点加强的措施

G19. 单位网站和应用系统内部登记备案情况

受调查的 G 类从业人员单位对每个网站和应用系统都做了登记的占 35.26%，其他情况如图 9-21 所示。

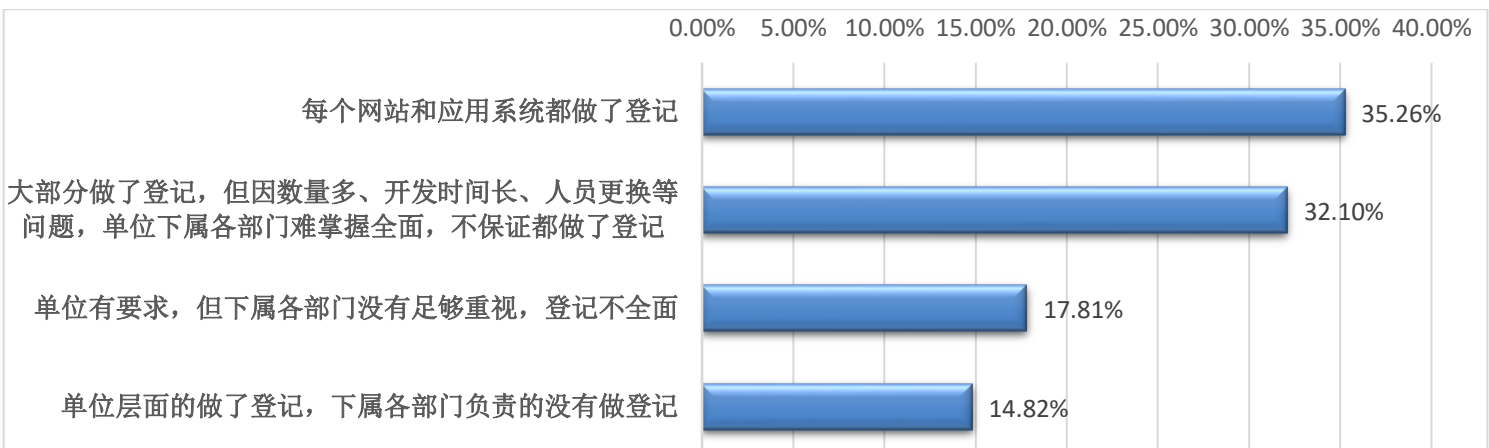


图9-21：网站和应用系统内部登记备案情况

G20. 单位进行网络安全等级保护工作情况

受调查的 G 类从业人员单位中有 41.48%进行了信息系统定级备案，其他开展的网络安全等级保护工作占比如图 9-22 所示。

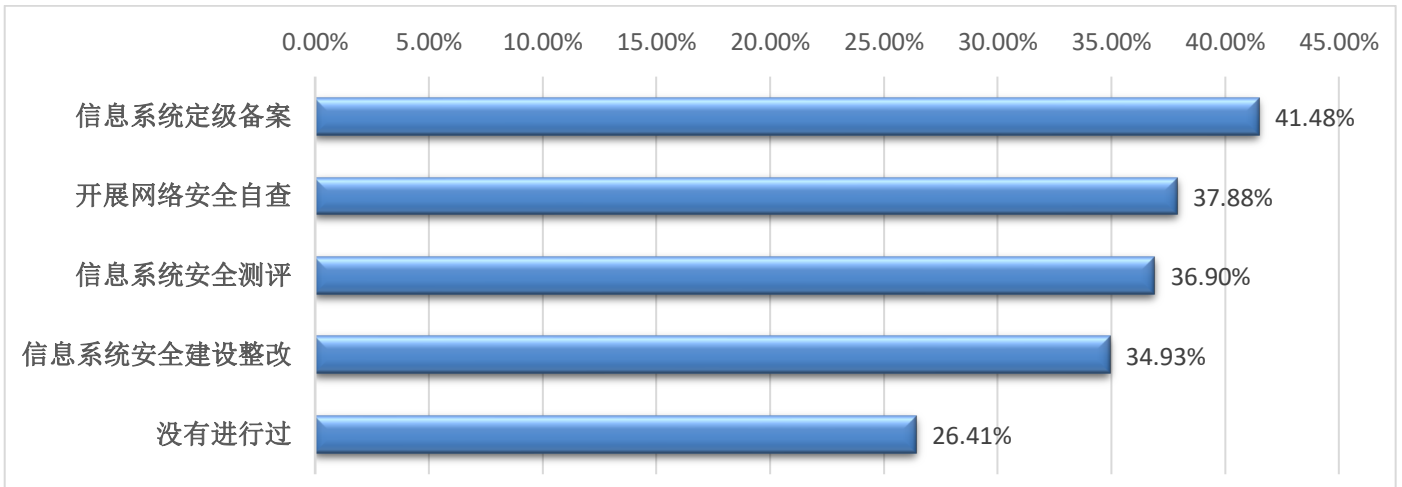


图9-22：单位进行过何种等级保护工作

G20.1、对测评机构进行测评工作的满意度现状

受调查的 G 类从业人员对测评机构进行测评工作评价满意的占 41.13%（如图 9-23）。

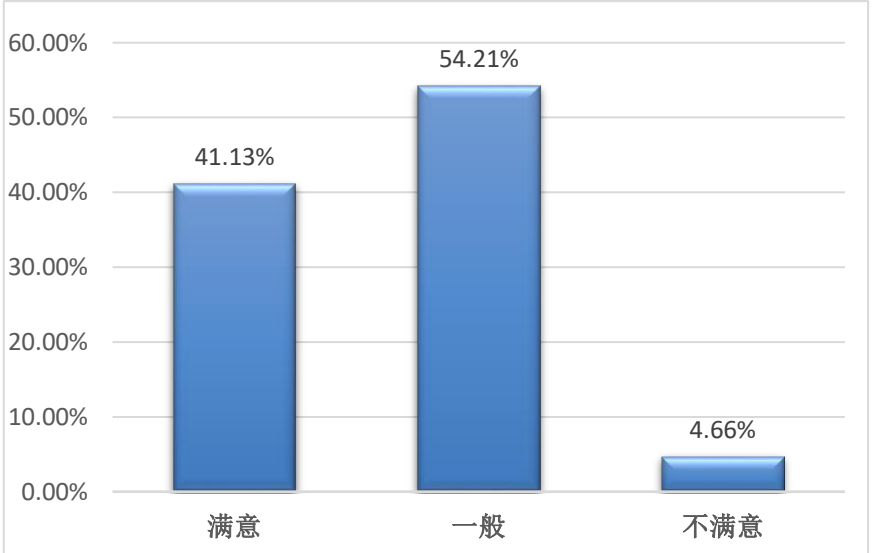


图9-23：测评机构满意度

G21. 网络安全等级保护制度重大意义的认识

受调查的 G 类从业人员对网络安全等级保制度的意义认识比较务实，有 68.88%的人员认为是国家网络安全领域的基本政策和基本制度（如图 9-24）。

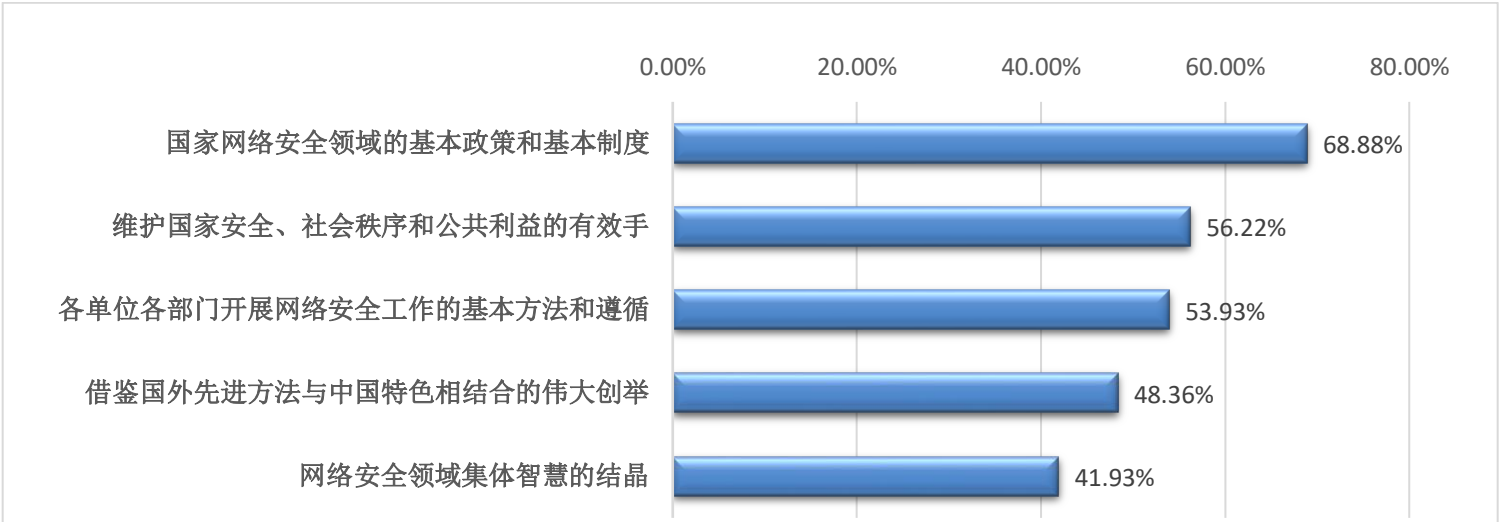


图9-24：等级保护重大意义

G22. 哪些单位应该开展网络安全等级保护工作

大部分受调查的 G 类从业人员对有等保义务单位范围的认识基本正确，但仍有 52.66%的人员选择了家庭和个人（如图 9-25）。

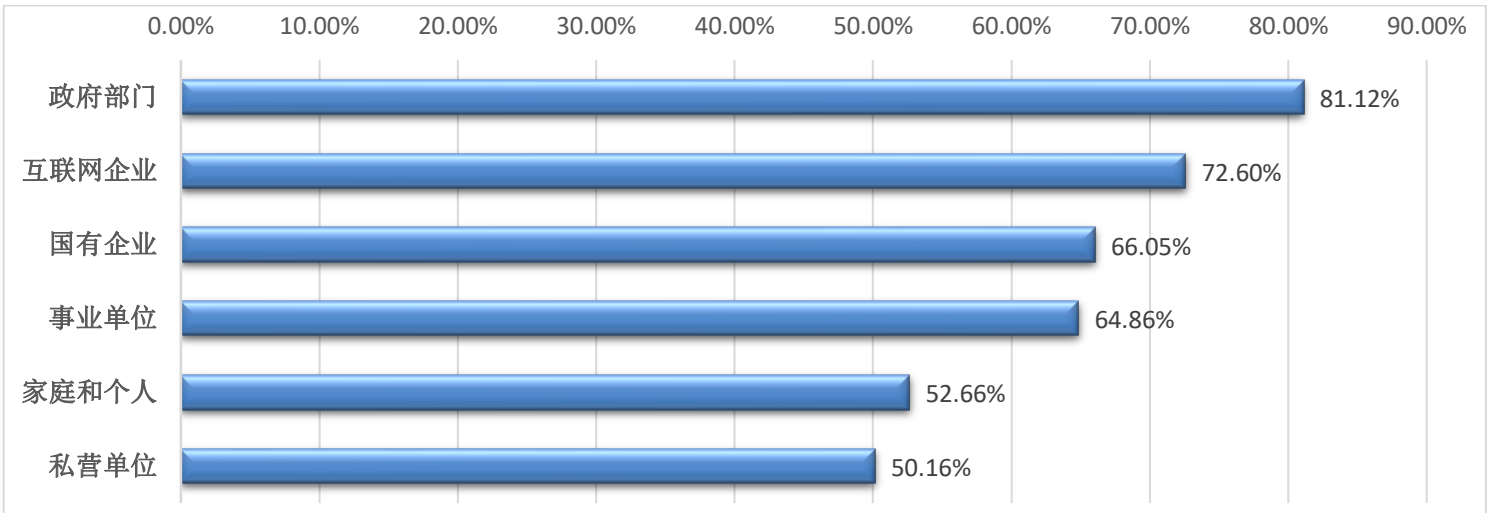


图9-25：应该开展等级保护工作的单位

G23. 哪些系统应该开展网络安全等级保护工作

受调查人的 G 类从业人员认为最该开展等级保护的系统前三位依次是校园网系统占 74.65%，校园卡系统占 62.53%，财务系统占 57.82%（如图 9-26）。

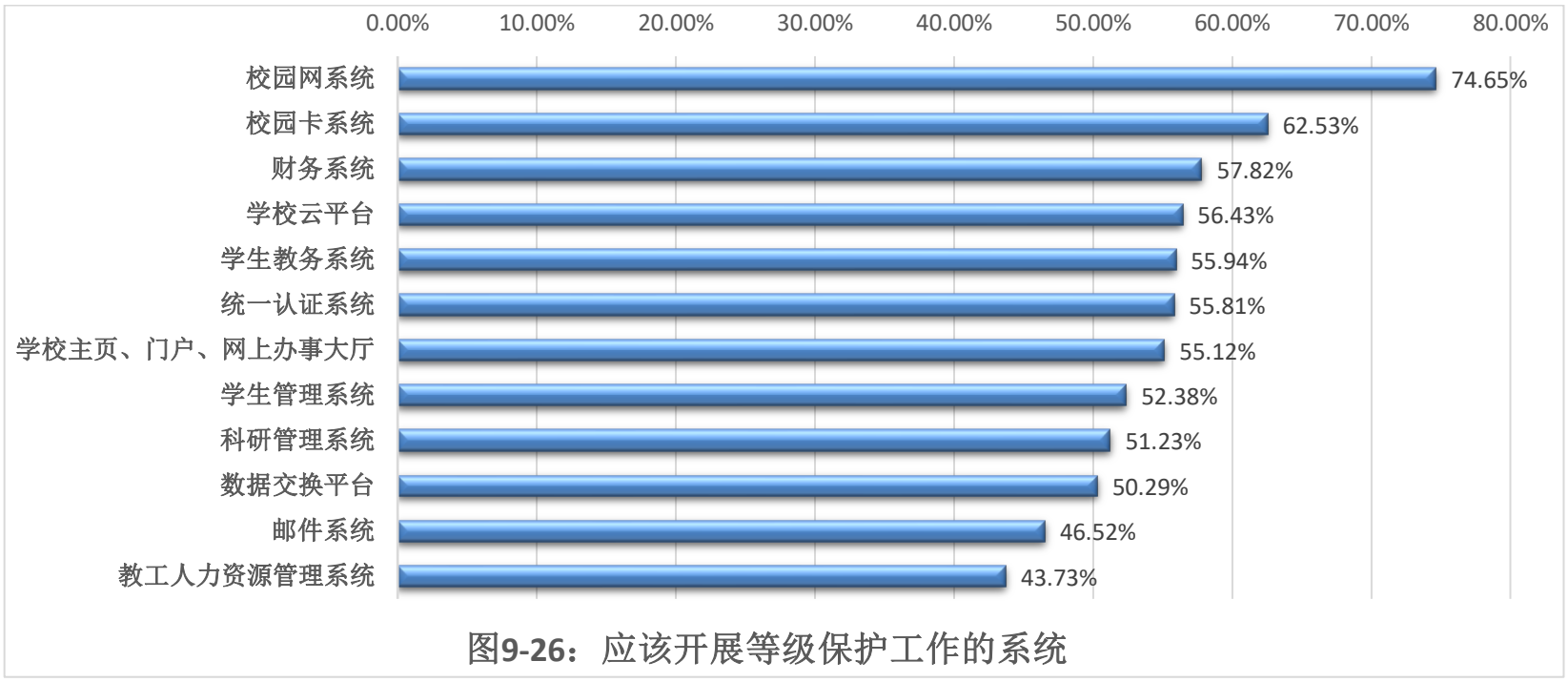


图9-26：应该开展等级保护工作的系统

G24. 对网络安全等级保护制度 2.0 国家标准要求的了解

受调查的 G 类从业人员了解网络安全等级保护制度 2.0 国家标准要求的占 29.24%，不了解的占 70.76%（如图 9-27）。

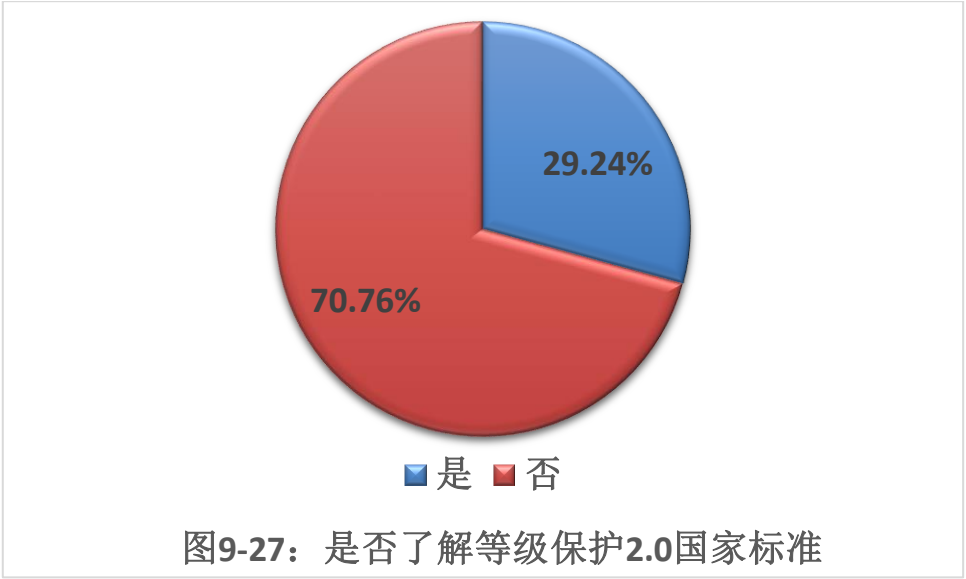


图9-27：是否了解等级保护2.0国家标准

G24.1、等保 2.0 的了解渠道

行业专业论坛是受调查 G 类从业人员了解等保 2.0 主要渠道，占比 62.18%（如图 9-28）。

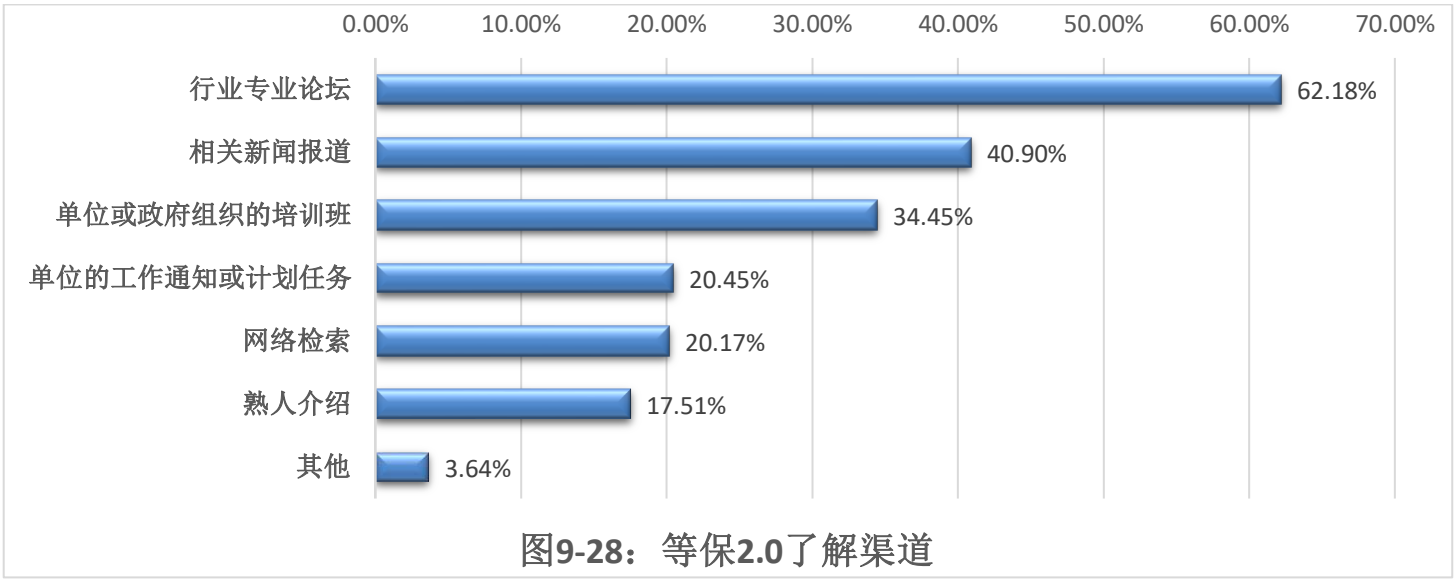


图9-28：等保2.0了解渠道

G25.单位发生网络安全事件情况

受调查 G 类从业人员单位发生过网络安全事件的占比 27.4%，没有发生过的占比 33.46%（如图 9-29）。

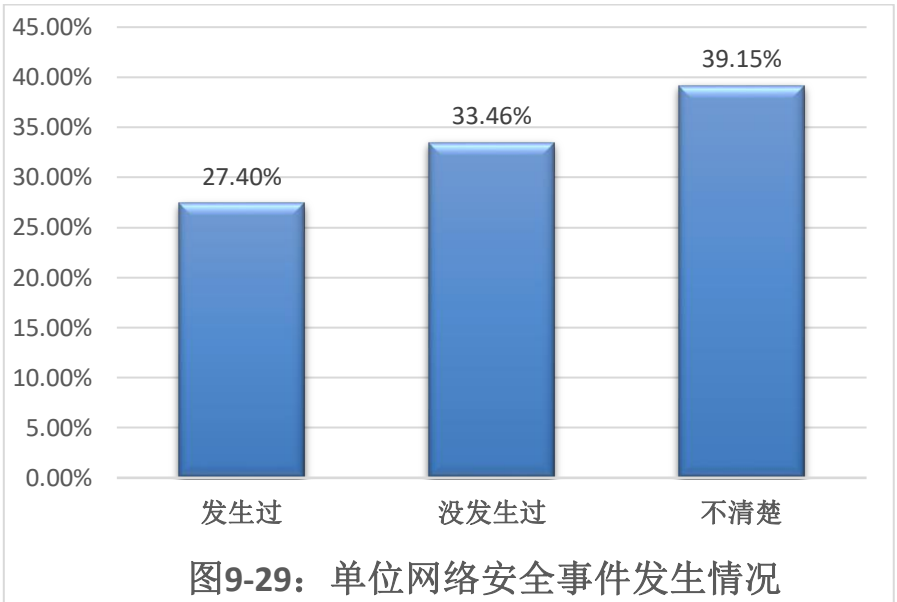


图9-29：单位网络安全事件发生情况

G25.1、安全事件的类型

受调查的 G 类从业人员单位发生最多的网络安全事件是数据信息泄露，占比 48.58%（如图 9-30）。

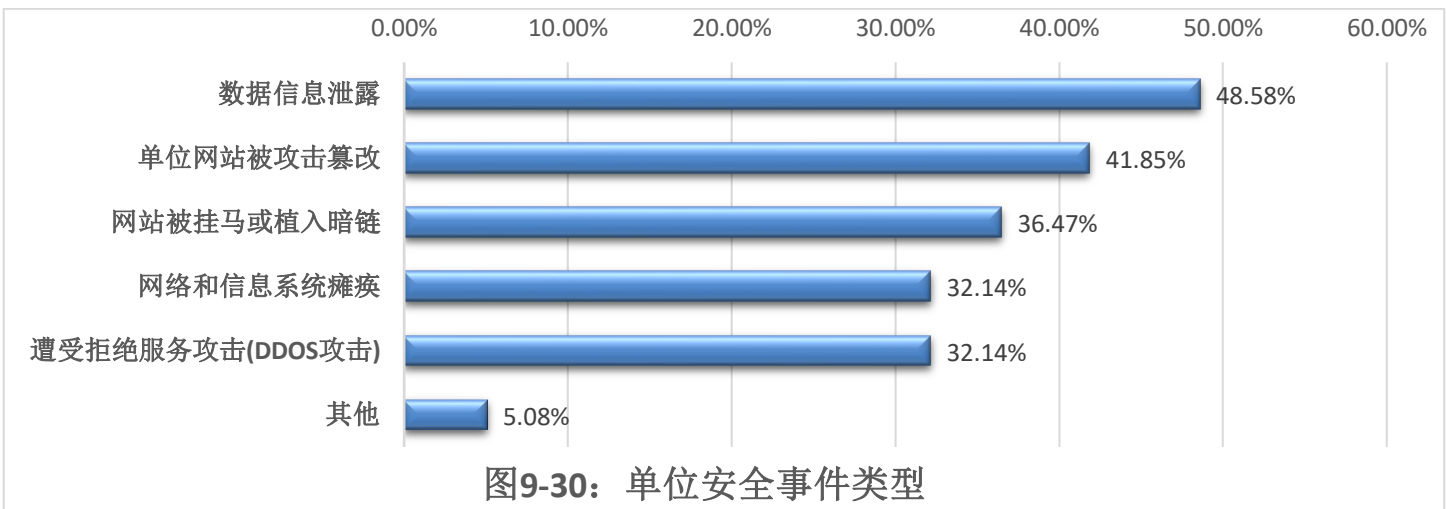


图9-30：单位安全事件类型

G25.2、单位针对发生的网络安全事件向公安机关报案情况

有 41.55%的受调查 G 类从业人员单位，在遇到网络安全事件时选择向公安机关报案（如图 9-31）。

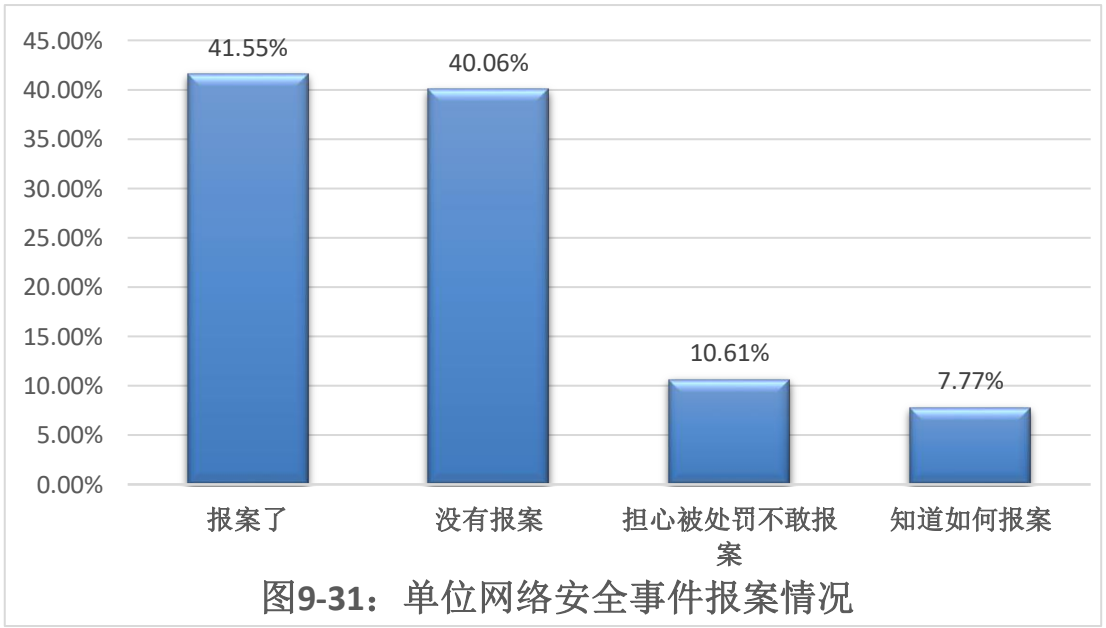


图9-31：单位网络安全事件报案情况

G25.3、对公安机关案件受理情况的满意度

受调查的 G 类从业人员对公安机关案件受理情况满意的占比 53.96%（如图 9-32）。

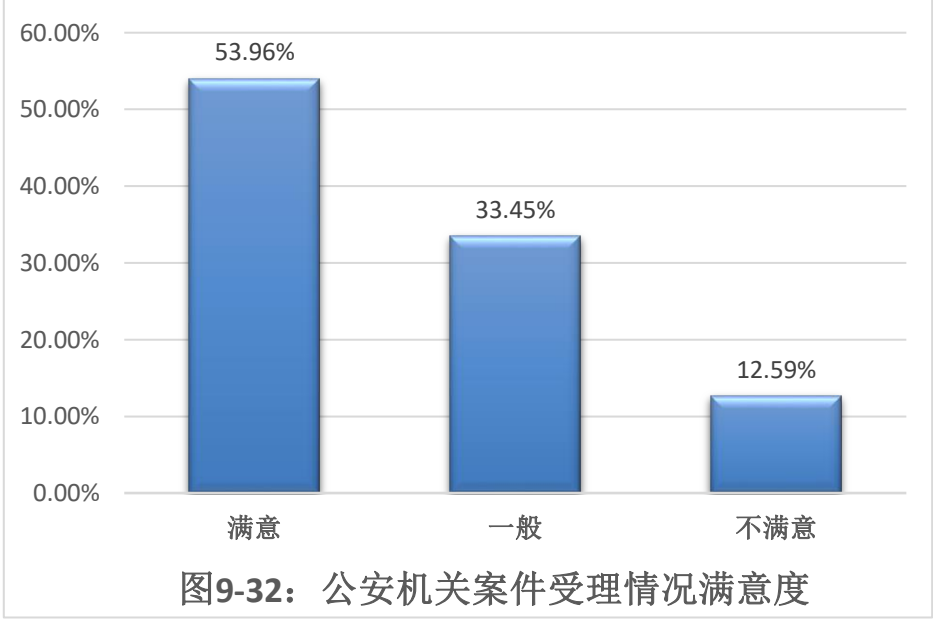


图9-32：公安机关案件受理情况满意度

G26. 公安机关网络安全执法检查工作满意度

受调查的 G 类从业人员对公安机关网络安全执法检查工作评价满意的占 29.52%，排除没有参加过检查的 20.76%的样本，调整后满意的占比 37.26%（如图 9-33）。

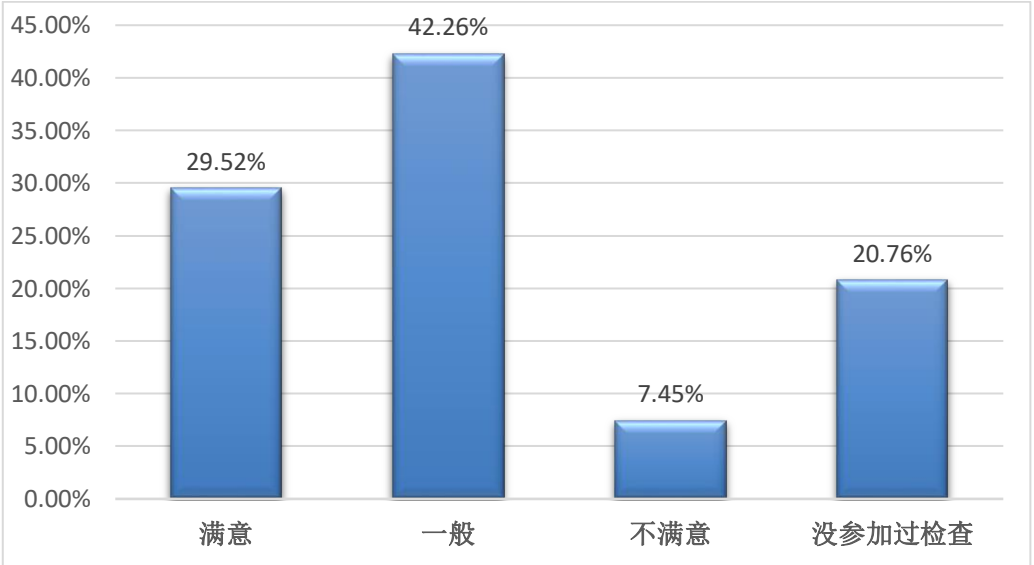


图9-33：公安机关网络安全执法满意度

G27. 网络安全等级保护对产业、企业发展的推动作用的认识

受调查的 G 类从业人员对网络安全等级保护的作用认识比较正面，有 54.46%的人员认为网络安全等级保护对产业、企业发展的推动很大（如图 9-34）。

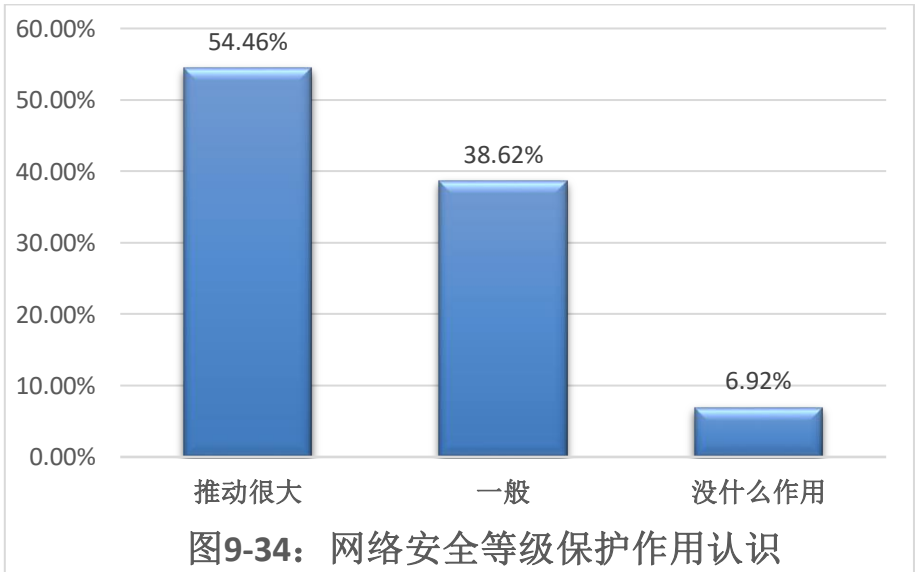


图9-34：网络安全等级保护作用认识

十、H 卷：其他联网使用单位从业人员

其他联网使用单位（H 类）从业人员主要是网络用户身份，态度比较中立。

H 问卷有效问卷数量 6378 份，以下是 H 类问卷各项数据的详细统计结果。

H3. 当前网络安全状况

受调查的 H 类从业人员认为网络安全状况良好有 44.96%，认为状况一般的占 44.25%，认为状况堪忧的占 10.79%（如图 10-1）。

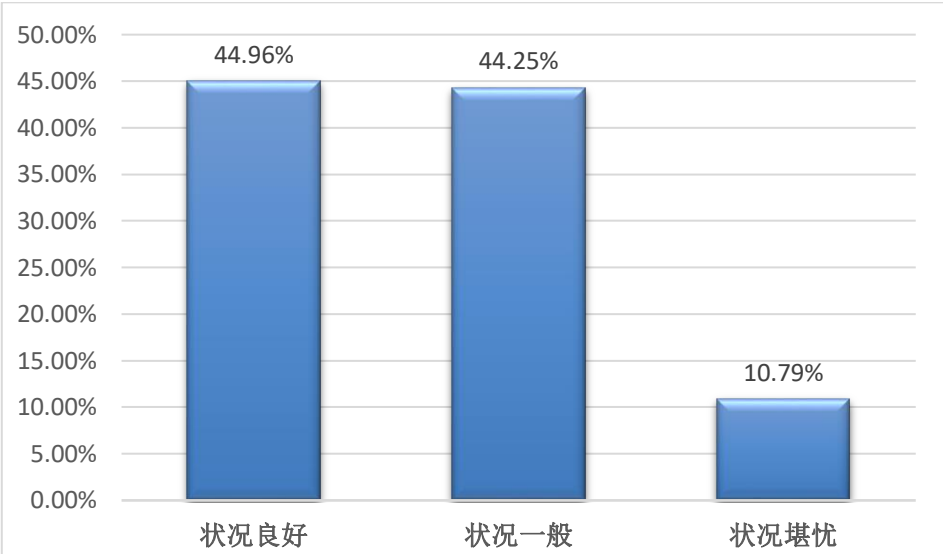


图10-1：安全状况评价

H4. 与去年相比网络安全感的变化

受调查的 H 类从业人员有 23.19%认为有明显改善，有 47.75% 的人员认为有改善，两者合计有 70.94%的人员认为网络安全状况改善或明显改善（如图 10-2）。

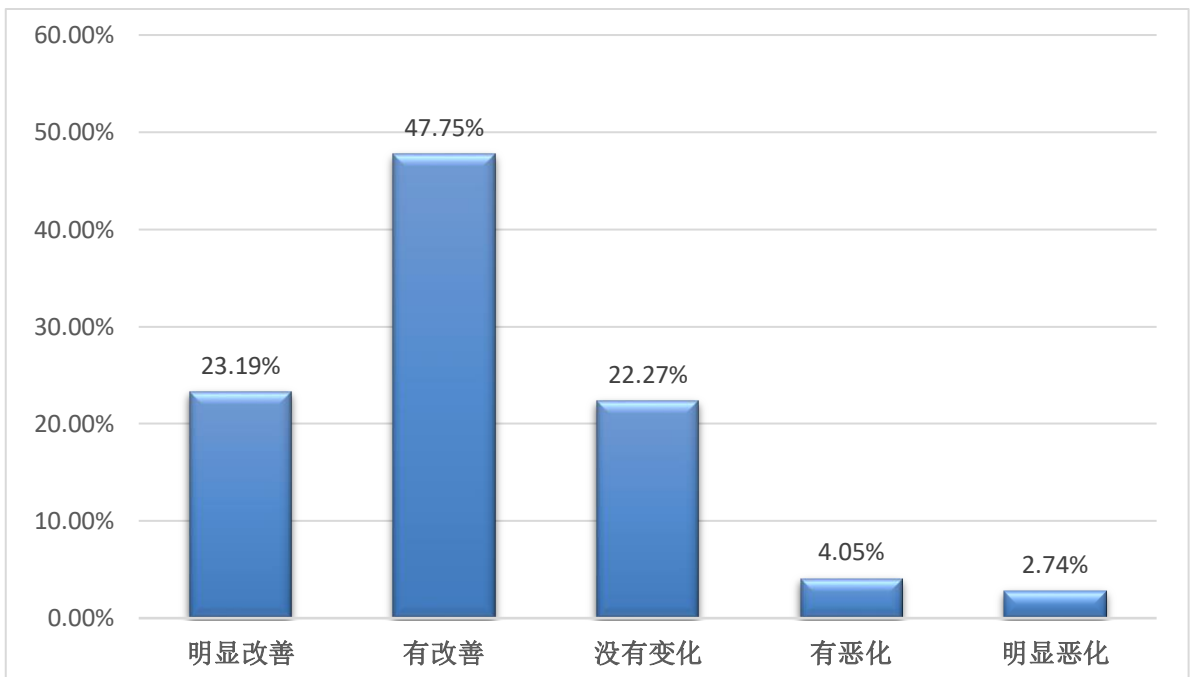


图10-2：网络安全感变化评价

H5. 网络服务提供者的管理措施对于保证网络安全水平的有效程度

受调查的 H 类从业人员有 21.66%认为非常有效，有 45.04%认为比较有效，两者合计共有 66.7%的人员认为非常有效和比较有效（如图 10-3）。

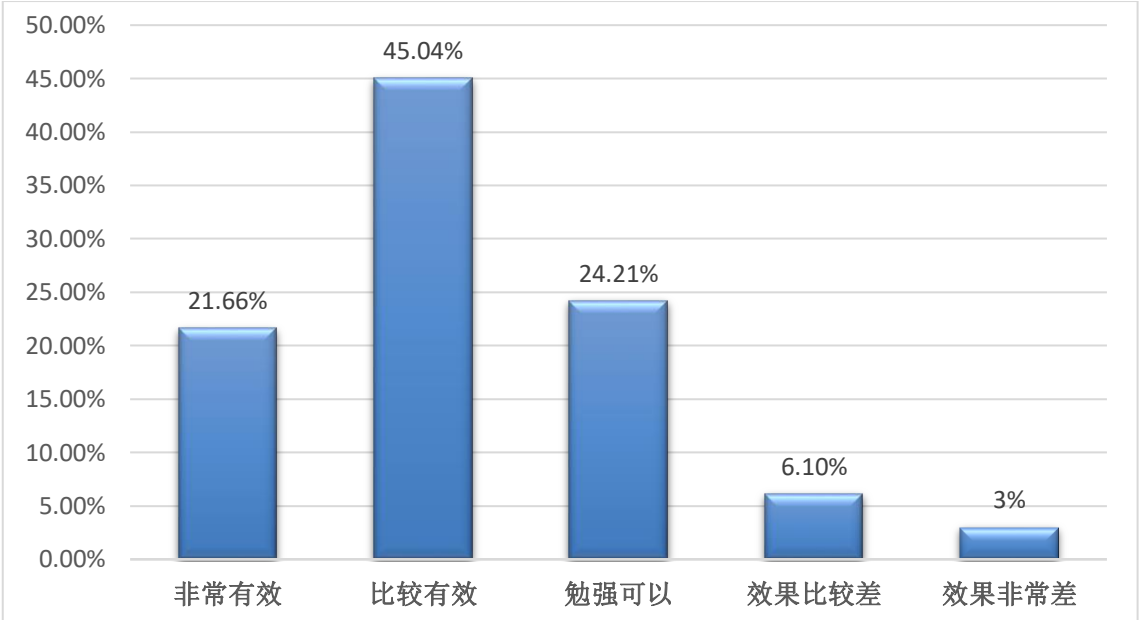


图10-3：管理措施有效程度

H6. 当前网络安全产品服务的资费水平

受调查的 H 类从业人员认为当前网络安全产品服务的资费水平高的占 35.02%，认为适中的占 59.6%，认为低的占 5.38%（如图 10-4）。

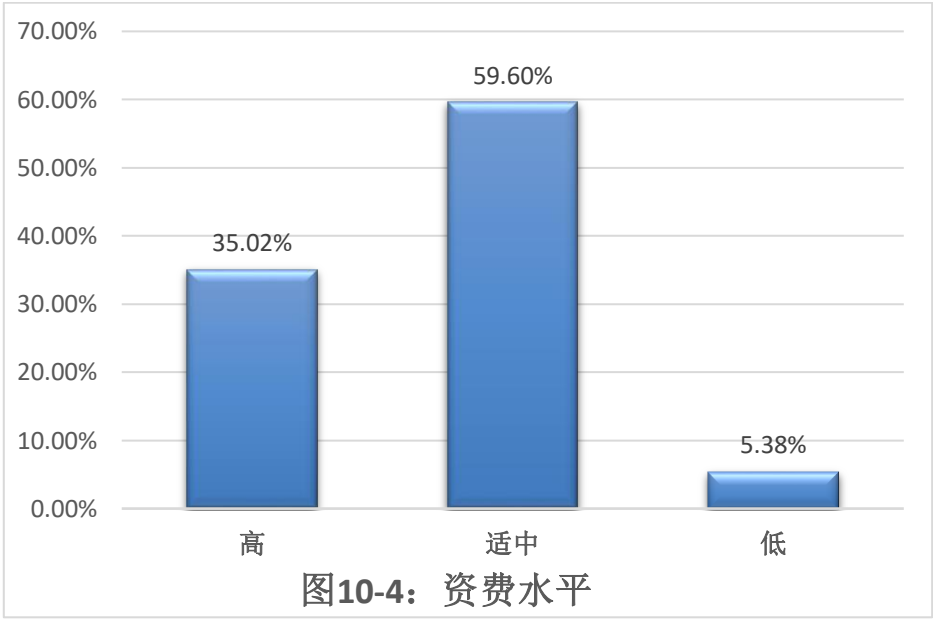


图10-4：资费水平

H7. 当前网络安全最突出的问题

受调查的 H 类从业人员认为最突出的网络安全问题是个人信息泄露，有 62.1%的人员选择，其它问题选择的人员较少，各类网络安全问题占比如图 10-5 所示。

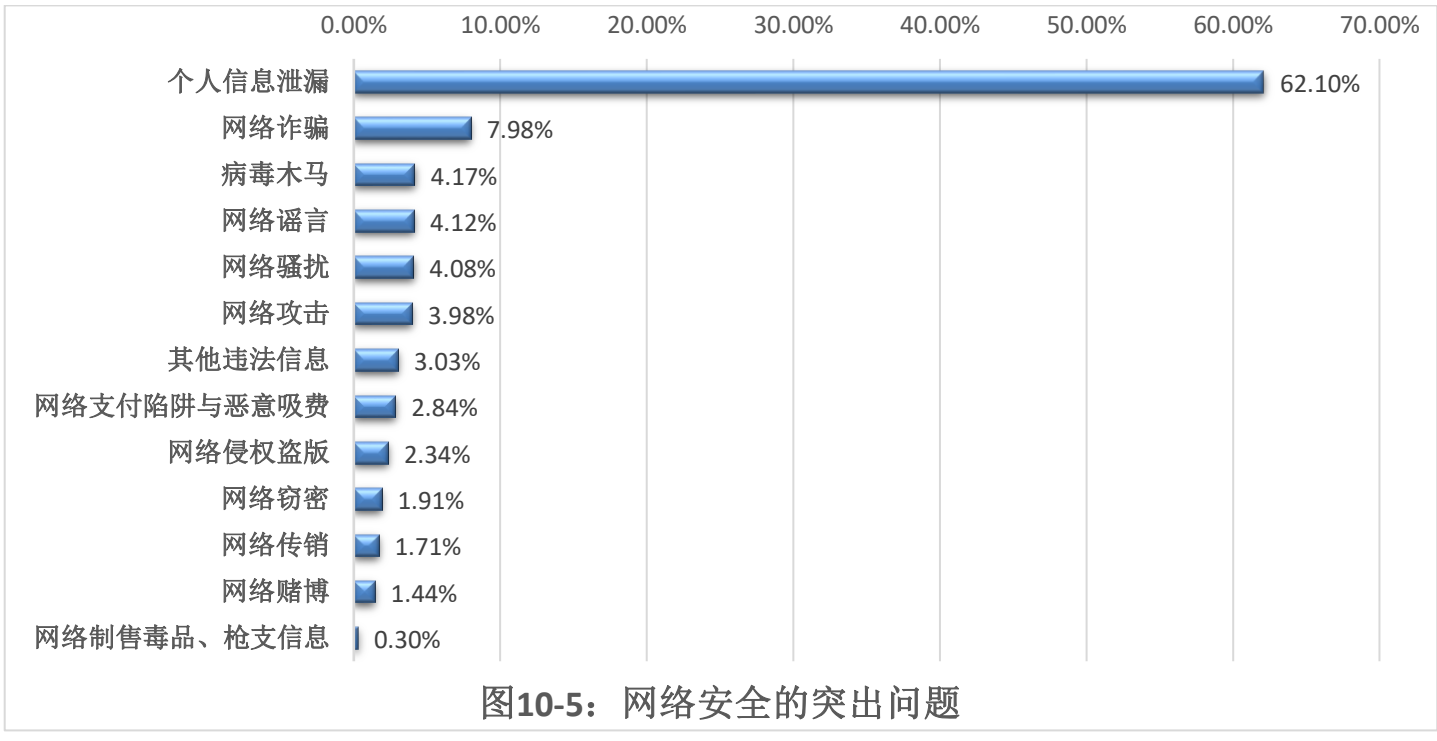


图10-5：网络安全的突出问题

H8. 当前我国个人信息保护状况

受调查的 H 类从业人员认为当前我国个人信息保护状况非常好的占 10%，比较好的占 20.21%，两者合计有 30.21%的人员认为好，认为不太好（20.45%）和非常不好（18.13%）的合计 38.58%（如图 10-6）。

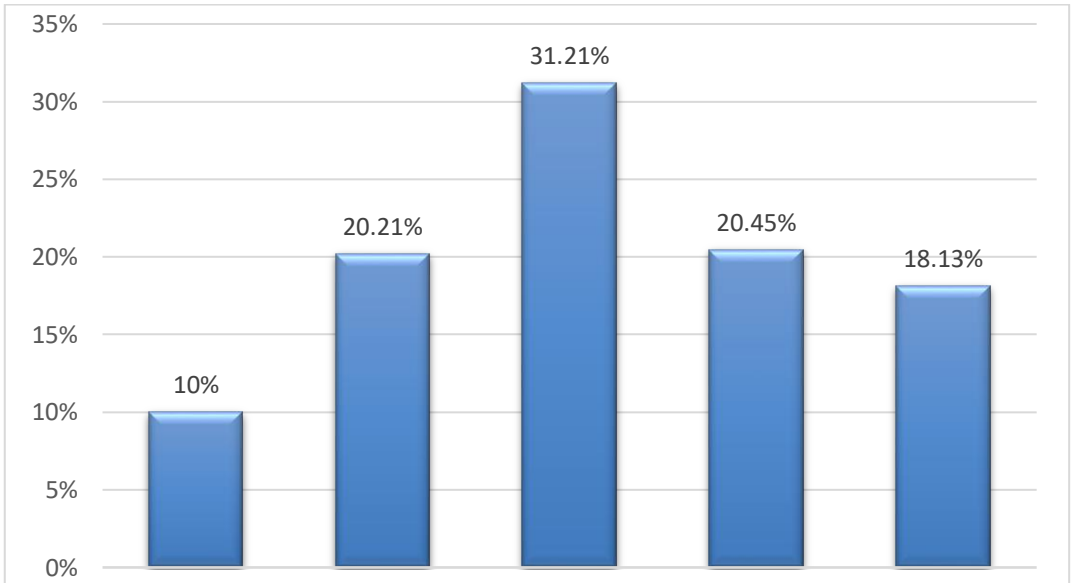


图10-6：个人信息保护状况

H8.1、个人信息保护可以在哪些方面加强

受调查的 H 类从业人员认为个人信息保护最应该加强的方面是犯罪打击，有 73.67%的人员选择，其次有 66.96%的人员选择行政执法（如图 10-7）。

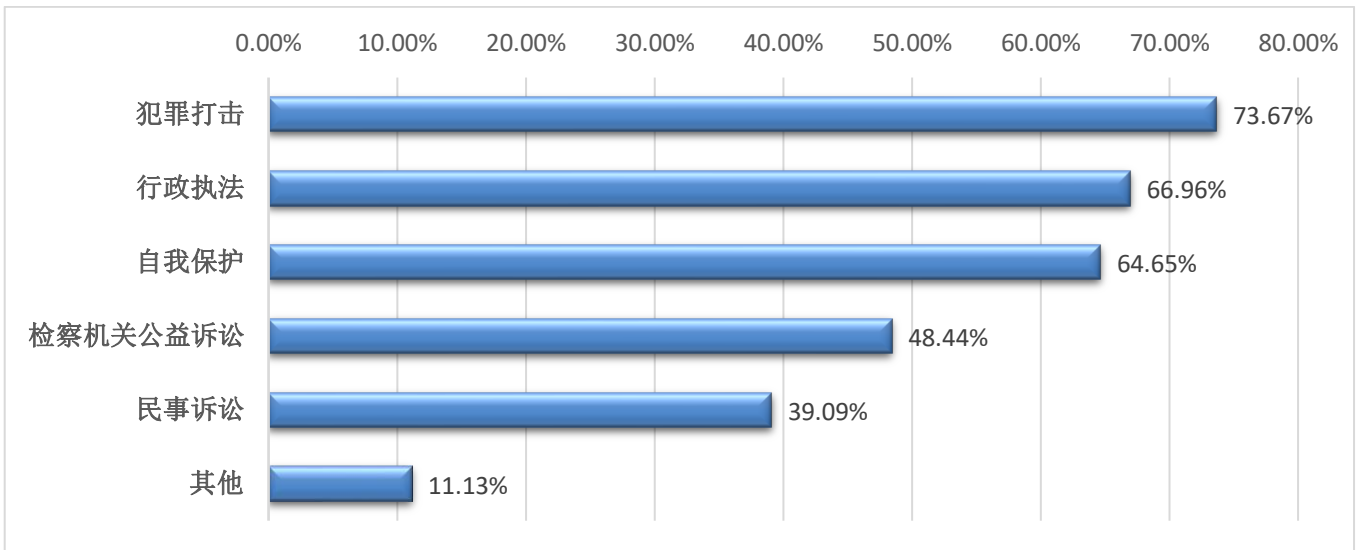


图10-7：个人信息保护应在哪些方面加强

H9. 政府网络安全管理政策措施对单位的影响

受调查的 H 类从业人员认为政府网络安全管理措施对单位影响最大的前三位依次是提高了意识（71.6%）、建立了组织体系（43.32%）、提高了风险防控水平（40.37%），各类影响占比如图 10-8 所示。

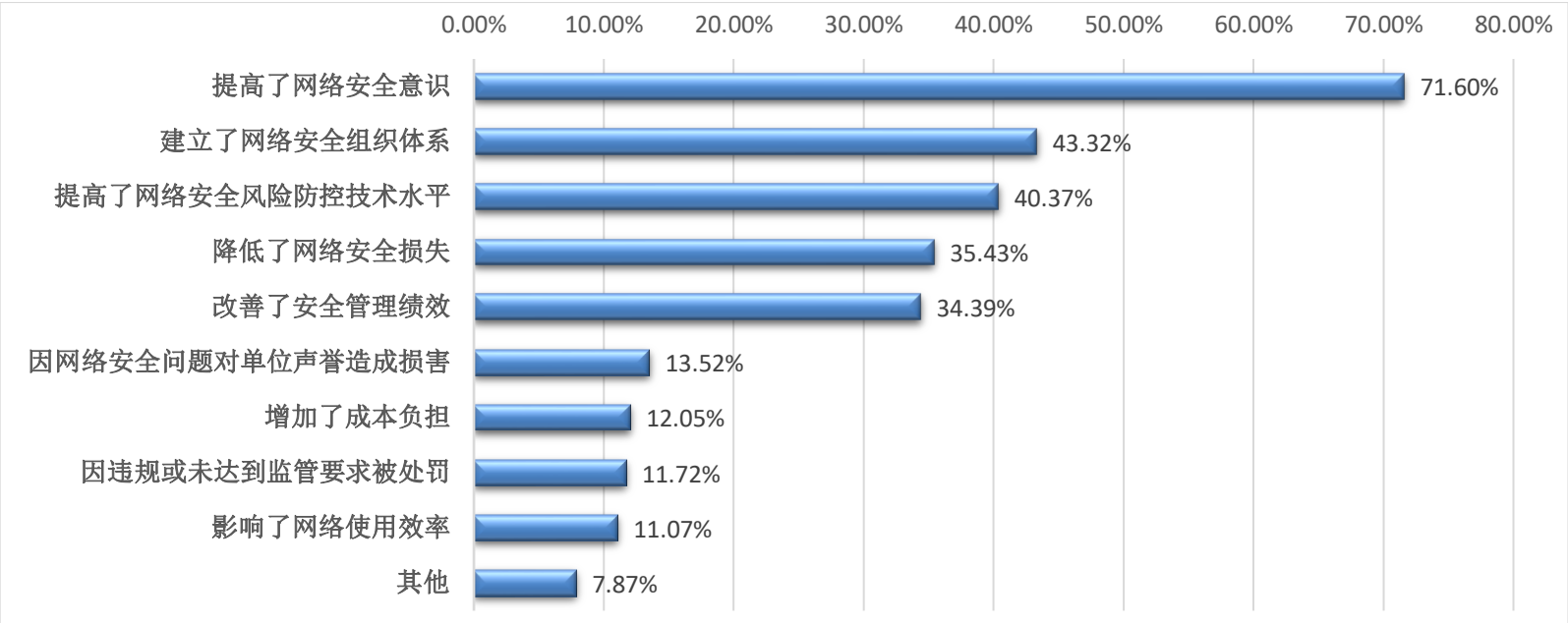


图10-8：政府政策措施对单位的影响

H10. 当前政府机关和事业单位网络安全管理的不足

受调查的 H 类从业人员认为当前政府机关和事业单位网络安全管理最不足的是专业技术人才，有 55.61%的人员选择，其次有 42.47%的人员选择信息系统安全风险较大（如图 10-9）。

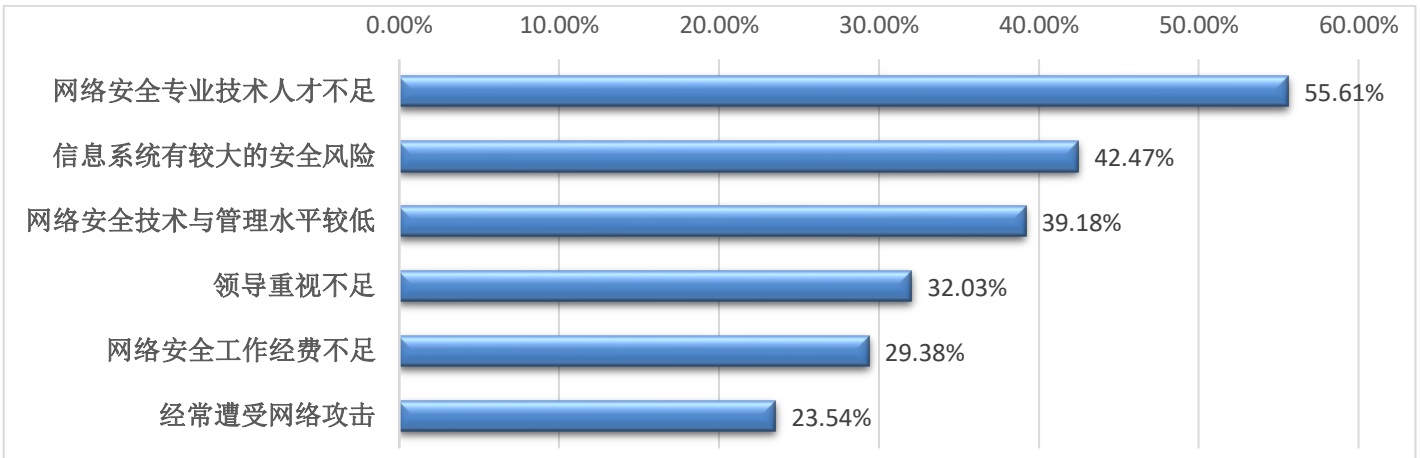


图10-9：网络安全管理的不足

H11. 亟待加强的网络安全立法内容

受调查的 H 类从业人员认为亟待加强的网络安全立法内容排名前三位的是：公民个人信息保护占 76.82%，网络平台责任占 57.65%，数据安全保护占 55.17%（如图 10-10）。

图10-10：亟待加强的立法内容

H12. 对网络安全行政执法部门的认识

受调查的 H 类从业人员认为政府最主要的网络安全执法部门前三位依次是网信（76.33%）、公安（61.96%）、工信（43.11%），如图 10-11 所示。

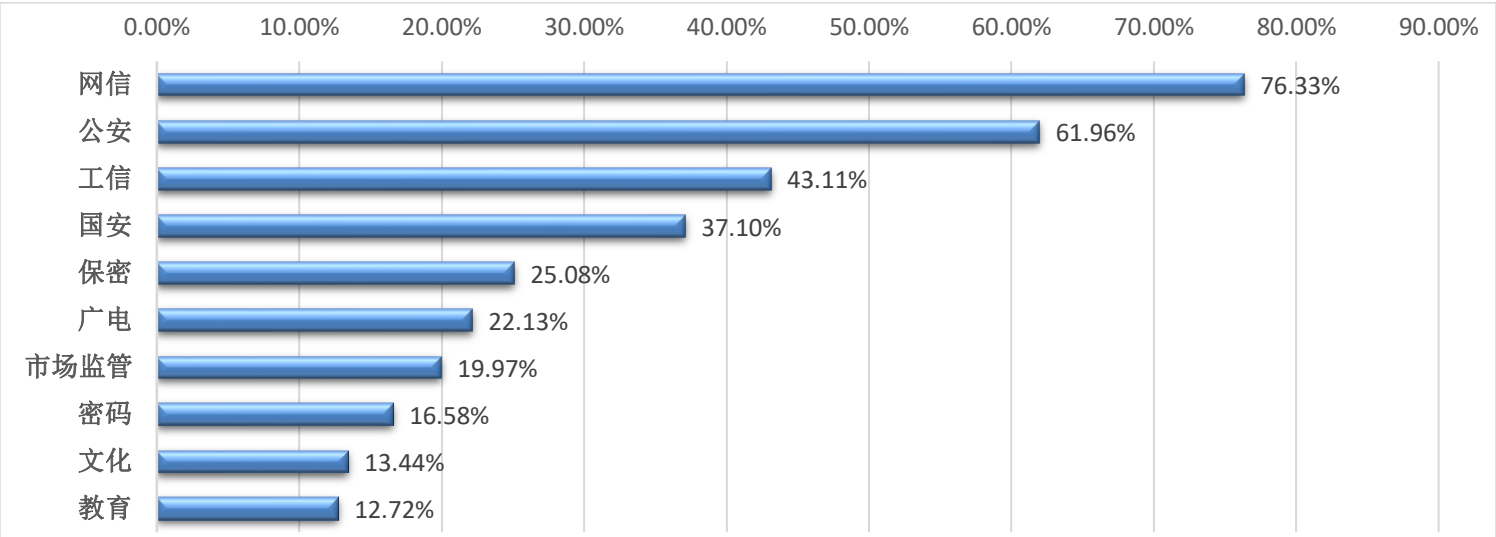


图10-11：政府网络安全执法部门

H12.1、政府部门在网络安全方面的执法力度评价

受调查的 H 类从业人员认为政府部门在网络安全方面的执法力度强的有 15.03%，认为比较强的有 30.51%，两者合计 45.54%；认为不足或严重不足的合计 16.15%（如图 10-12）。

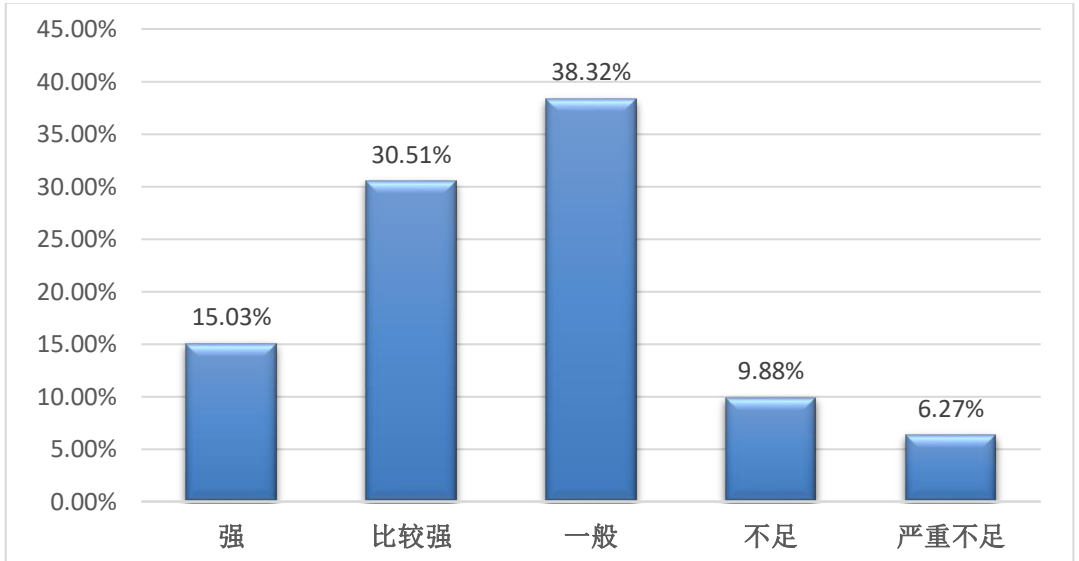


图10-12：政府执法力度评价

H12.2 、您认为当前影响网络安全执法的制约因素是什么？

受调查的 H 类从业人员认为影响网络安全执法的制约因素前三位的是：检测能力（56.8%）、人员（55.05%）、取证能力（54.95% ），各类制约因素占比如图 10-13 所示。

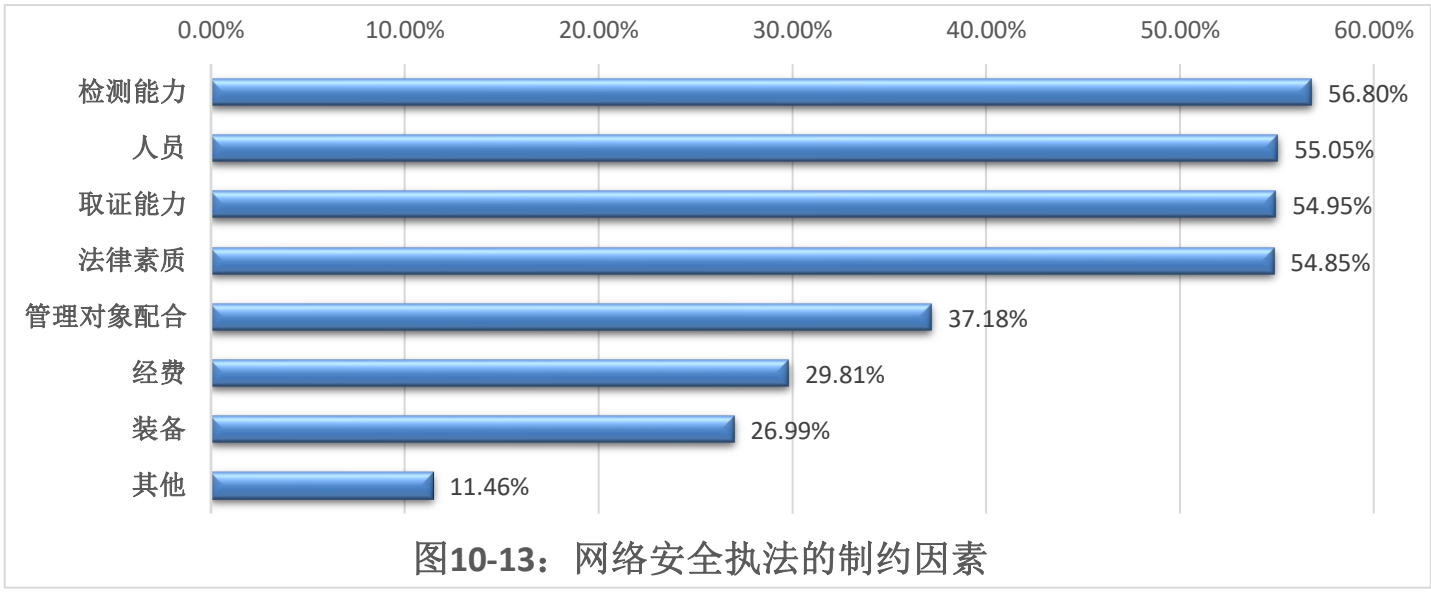


图10-13：网络安全执法的制约因素

H13. 单位进行网络安全等级保护工作情况

受调查的 H 类从业人员单位中有 46.16%进行了信息系统定级备案，其他开展的网络安全等级保护工作占比如图 10-14 所示。

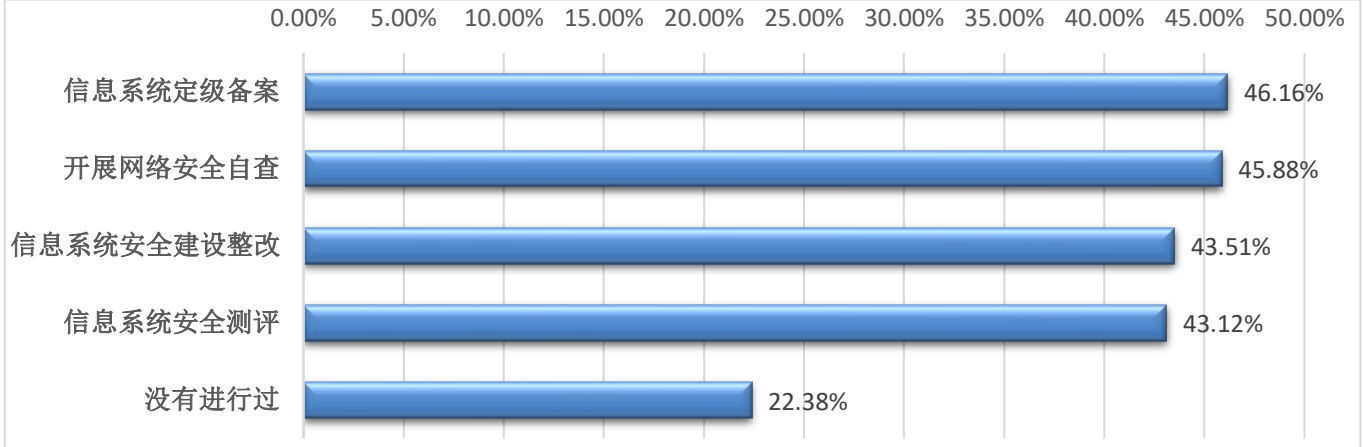


图10-14：单位进行过何种等级保护工作

H13.1、对测评机构进行测评工作的满意度现状

受调查的 H 类从业人员对测评机构进行测评工作评价满意的占 45.82%（如图 10-15）。

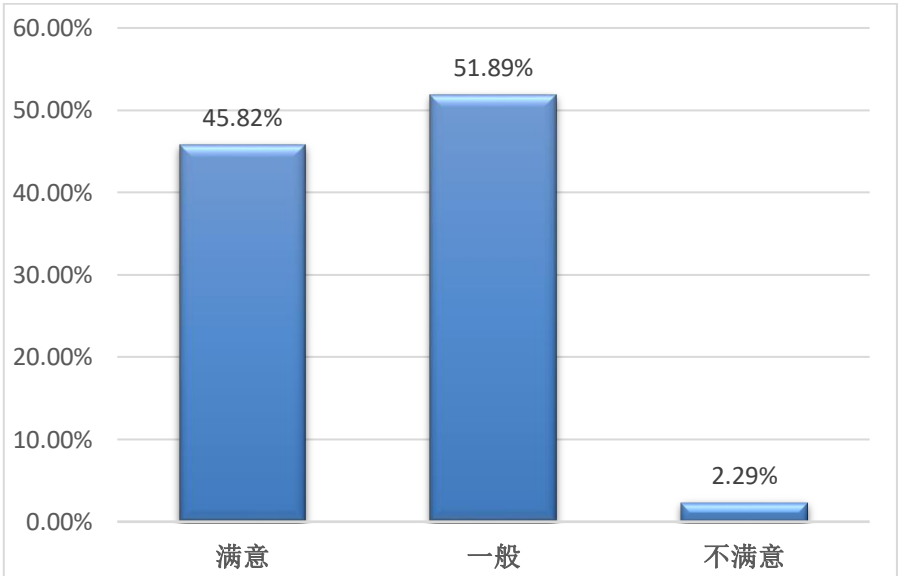


图10-15：测评机构满意度

H14. 网络安全等级保护制度重大意义的认识

受调查的 H 类从业人员对网络安全等级保制度的意义认识比较务实，有 74.8%的人员认为是国家网络安全领域的基本政策和基本制度（如图 10-16）。

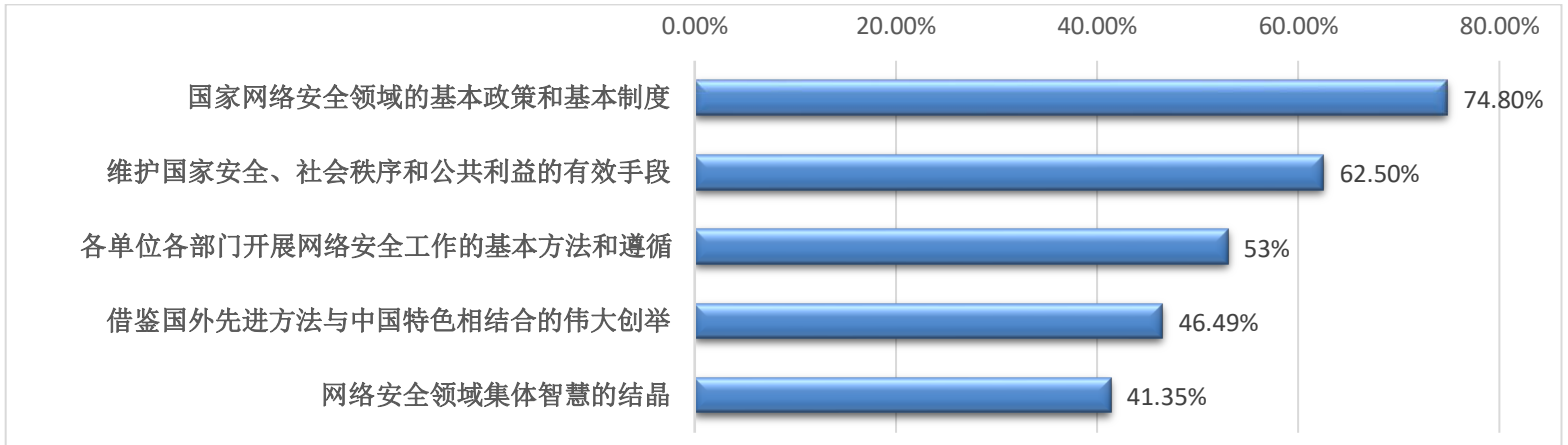


图10-16：等级保护重大意义

H15. 哪些单位应该开展网络安全等级保护工作

大部分受调查的 H 类从业人员对有等保义务单位范围的认识基本正确，但仍有 51.11%的人员选择了家庭和个人（如图 10-17）。

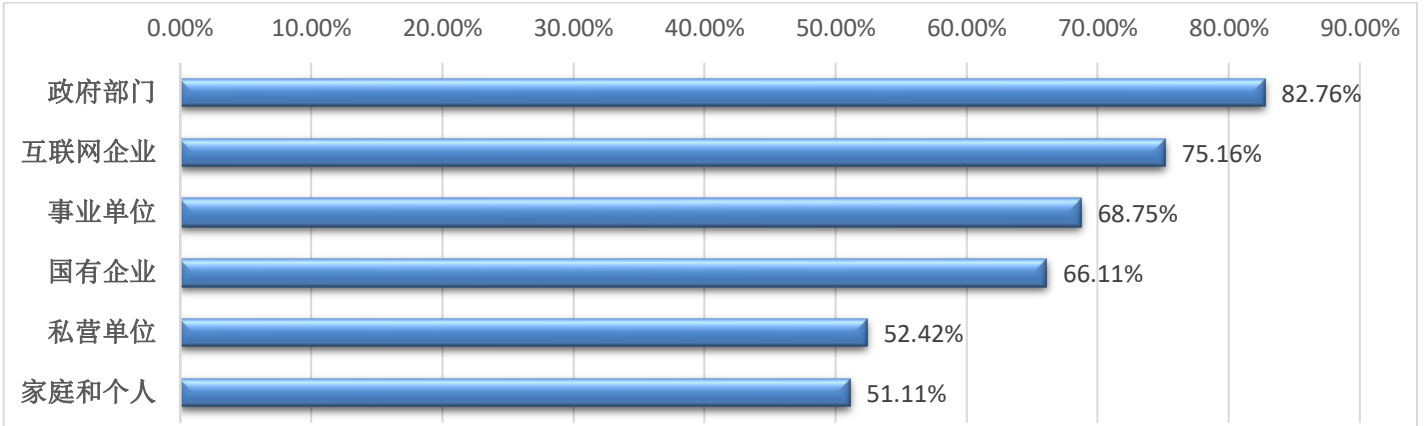


图10-17：应该开展等级保护工作的单位

H16. 哪些系统应该开展网络安全等级保护工作

受调查人的 H 类从业人员认为最该开展等级保护的系统前三位依次是关键信息基础设施占 75.11%，大数据系统占 67.64%，行业专网和业务信息系统占 65.42%（如图 10-18）。

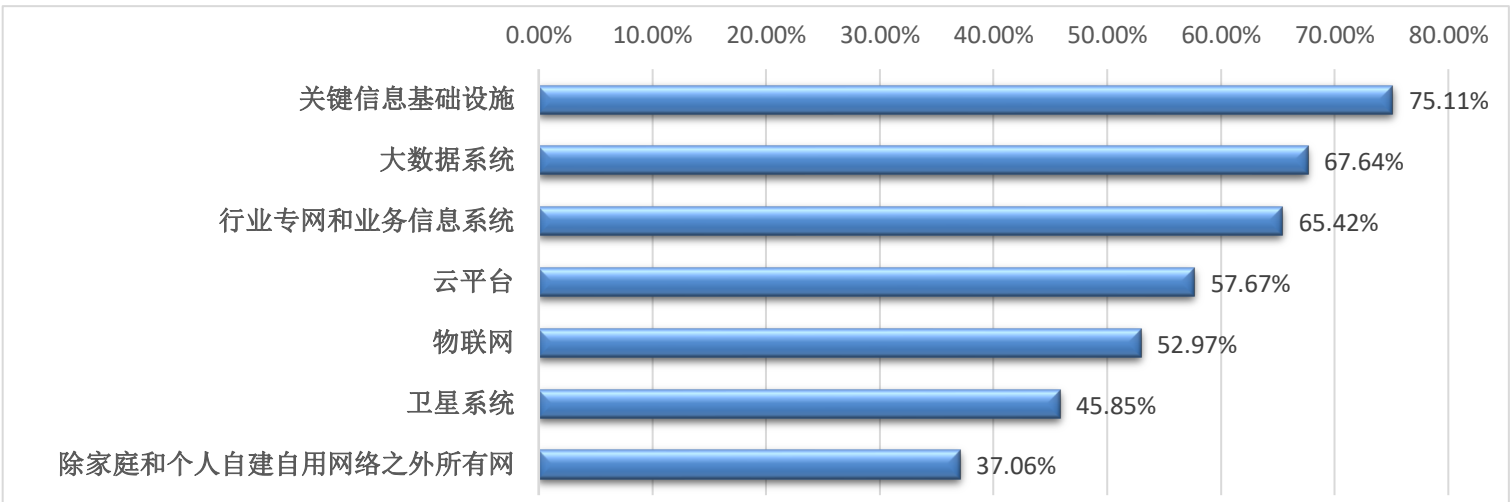


图10-18：应该开展等级保护工作的系统

H17. 对网络安全等级保护制度 2.0 国家标准要求的了解

受调查的 H 类从业人员了解网络安全等级保护制度 2.0 国家标准要求的占 23.29%，不了解的占 76.71%（如图 10-19）。

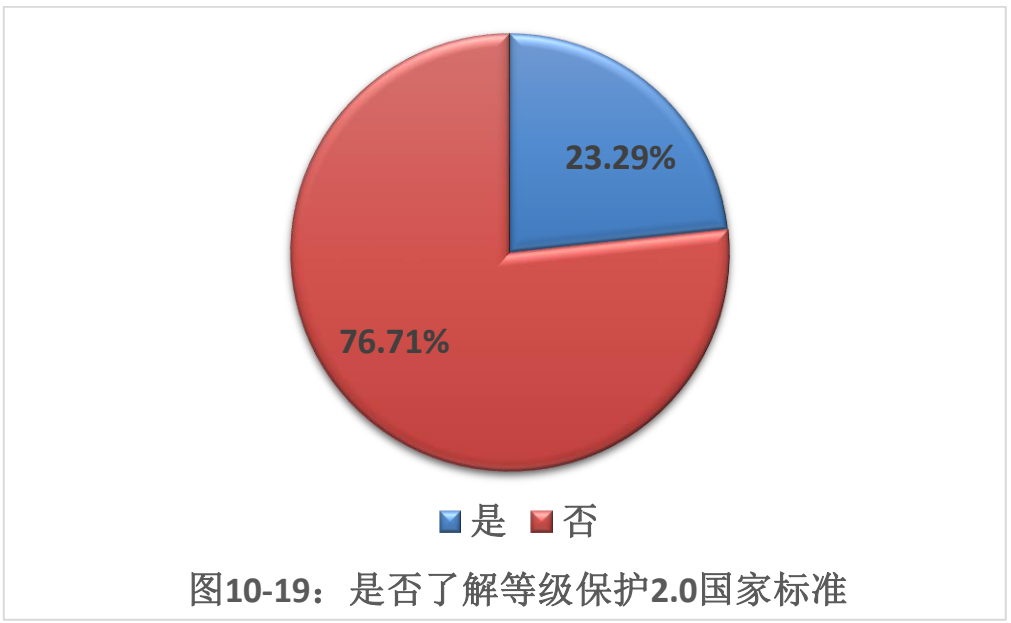


图10-19：是否了解等级保护2.0国家标准

H17.1、等保 2.0 的了解渠道

行业专业论坛是受调查 H 类从业人员了解等保 2.0 主要渠道，占比 46.9%（如图 10-20）。

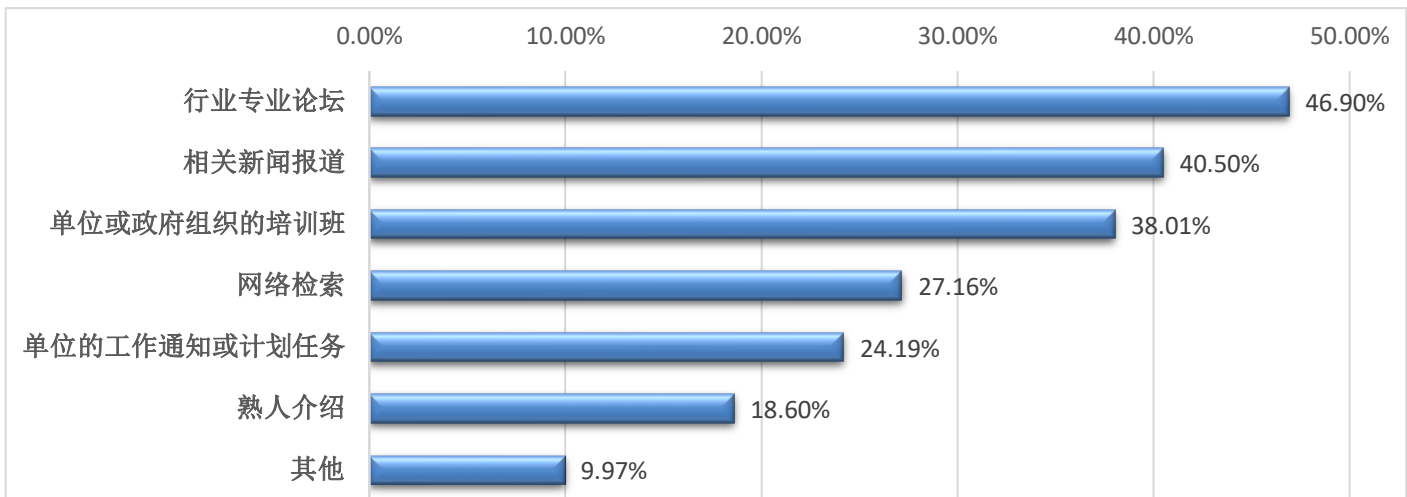


图10-20：等保2.0了解渠道

H18. 单位发生网络安全事件情况

受调查 H 类从业人员单位发生过网络安全事件的占比 15.25%，没有发生过的占比 43.76%（如图 10-21）。

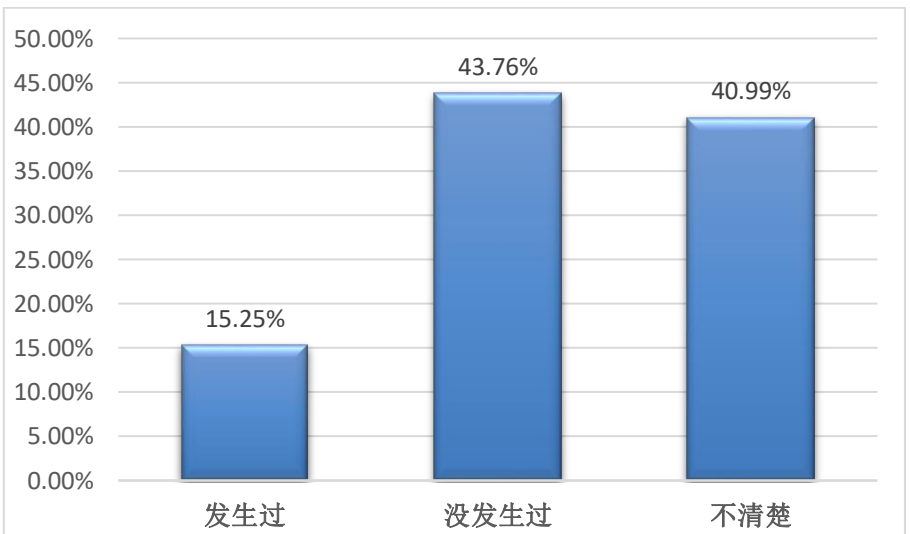


图10-21：单位网络安全事件发生情况

H18.1、安全事件的类型

受调查的 H 类从业人员单位发生最多的网络安全事件是数据信息泄露，占比 45.43%（如图 10-22）。

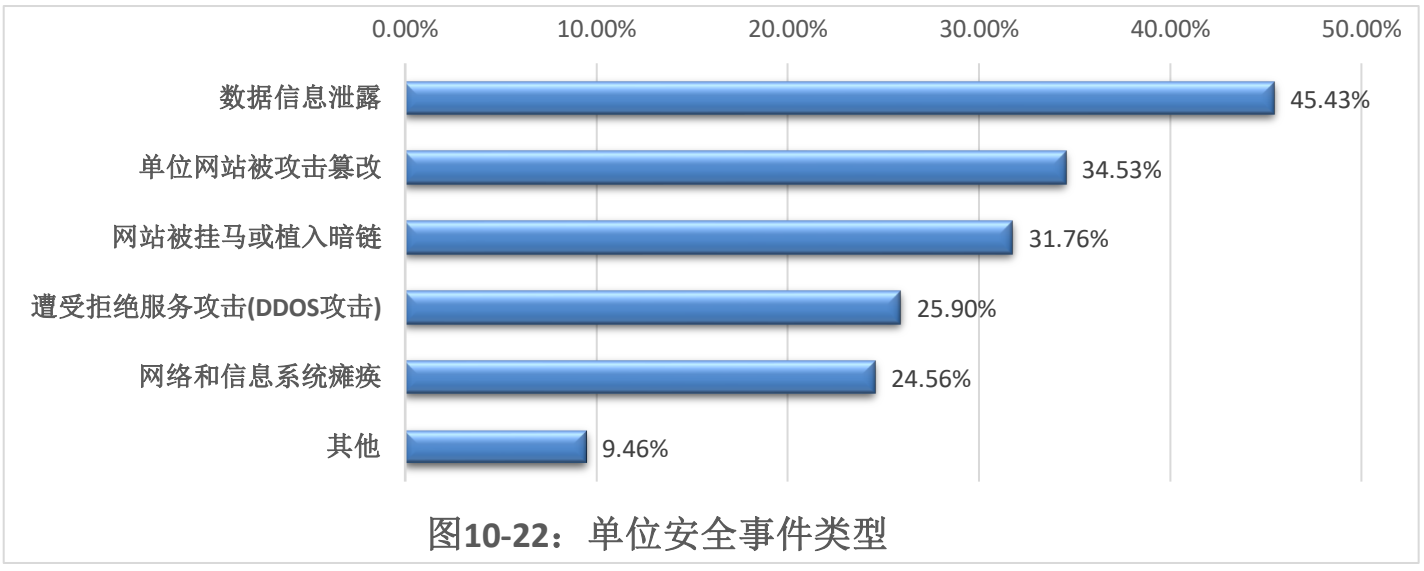


图10-22：单位安全事件类型

H18.2、单位针对发生的网络安全事件向公安机关报案情况

有 40.7%的受调查 H 类从业人员单位，在遇到网络安全事件时选择向公安机关报案（如图 10-23）。

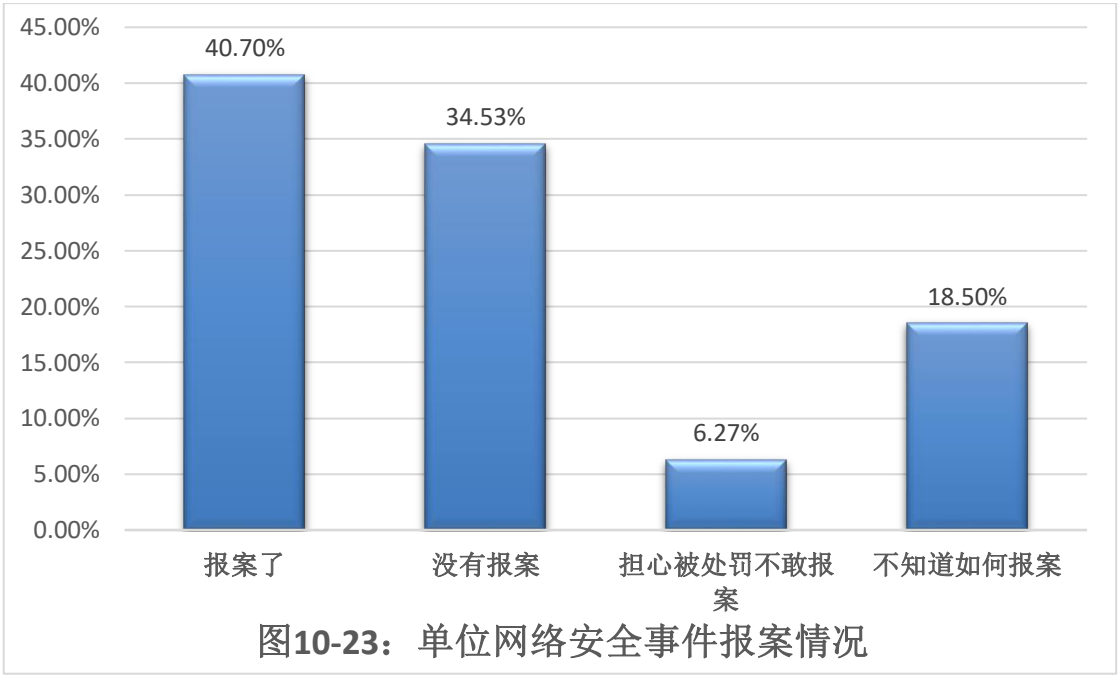


图10-23：单位网络安全事件报案情况

H18.3、对公安机关案件受理情况的满意度

受调查的 H 类从业人员对公安机关案件受理情况满意的占比 56.06%（如图 10-24）。

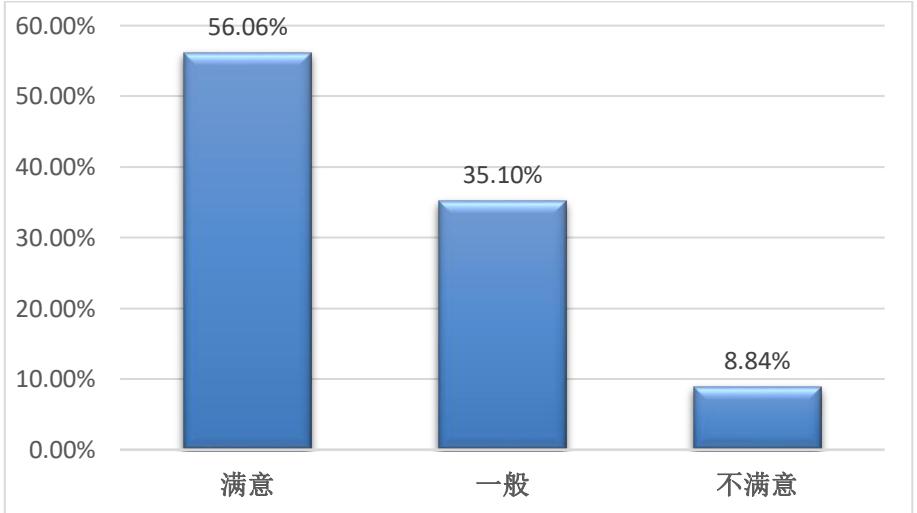


图10-24：公安机关案件受理情况满意度

H19. 公安机关网络安全执法检查工作满意度

受调查的 H 类从业人员对公安机关网络安全执法检查工作评价满意的占 34.13%，排除没有参加过检查的 21.2%的样本，调整后满意的占比 43.3%（如图 10-25）。

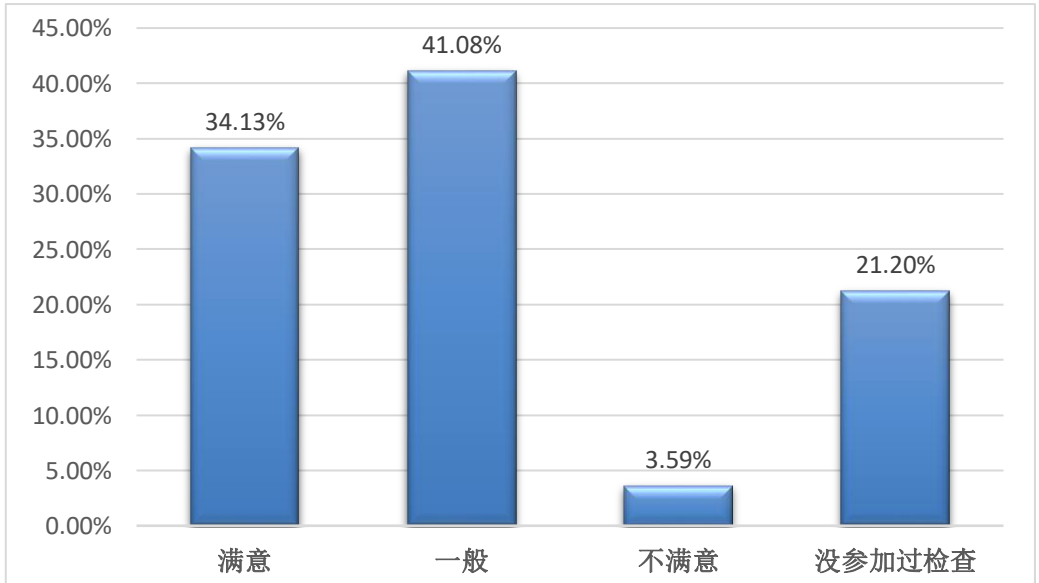


图10-25：公安机关网络安全执法满意度

H20. 网络安全等级保护对产业、企业发展的推动作用的认识

受调查的 H 类从业人员对网络安全等级保护的作用认识比较正面，有 63.16%的人员认为网络安全等级保护对产业、企业发展的推动很大（如图 10-26）。

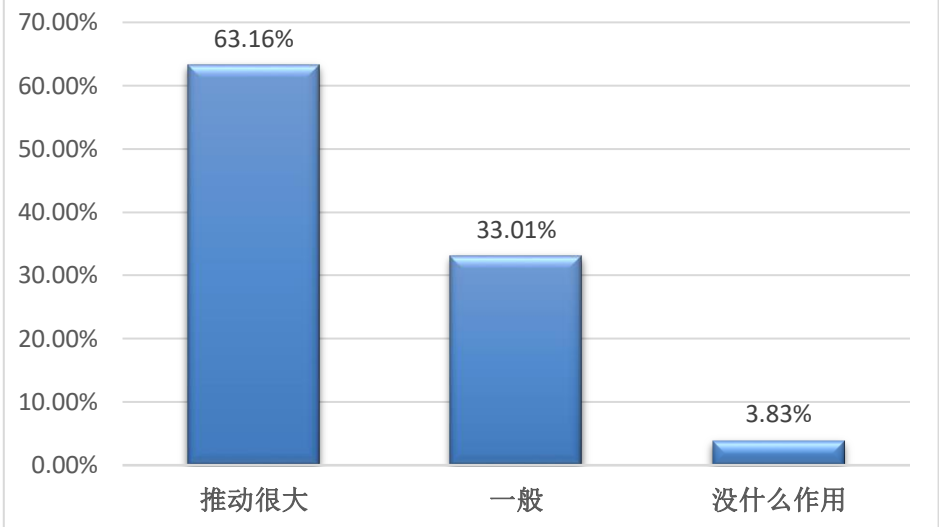


图10-26：网络安全等级保护作用认识

附件一：调查活动发起单位及支持单位名单（排名不分先后）

发 起 单 位

（1）北京网络行业协会
（2）北京网络空间安全协会
（3）中关村信息安全测评联盟
（4）中关村可信计算产业联盟
（5）中关村网络安全与信息化产业联盟
（6）关键信息基础设施保护技术创新联盟
（7）北京关键信息基础设施安全保护中心
（8）上海市信息网络安全管理协会
（9）上海市信息安全行业协会
（10）天津市网络文化行业协会
（11）天津市青少年网络协会
（12）天津市软件行业协会
（13）天津市互联网协会
（14）天津市大数据协会
（15）重庆市信息安全协会
（16）重庆计算机安全学会
（17）重庆信息安全产业技术创新联盟
（18）河北省网络空间安全学会
（19）山西省信息网络安全协会
（20）山西省互联网协会
（21）吉林省信息网络安全协会
（22）吉林省信息技术应用协会
（23）吉林省电子信息行业联合会
（24）吉林省计算机行业商会
（25）辽宁省信息网络安全协会
（26）黑龙江省网络安全协会
（27）黑龙江省旅游产业发展促进会
（28）黑龙江省虚拟现实科技学会
（29）陕西省信息网络安全协会
（30）山东省信息网络安全协会
（31）福建省互联网创业促进会
（32 福建省互联网经济促进会
（33）浙江省计算机系统安全协会
（34）河南省网络营销协会
（35）湖北省信息网络安全协会
（36）湖南省网络空间安全协会
（37）江西省网络空间安全协会
（38）江苏省信息网络安全协会
（39）安徽省计算机网络与信息安全协会
（40）广东省计算机信息网络安全协会
（41）广东省网络空间安全协会
（42）广东关键信息基础设施保护中心
（43）广东省电子政务协会
（44）广东软件行业协会
（45）广东省首席信息官协会
（46）广东省版权保护联合会
（47）广东省互联网协会
（48）广东省信息消费协会
（49）广东省医药合规促进会
（50）广东省图书文化信息协会
（51）海南省计算机学会
（52）海南省网络安全协会
（53）四川省计算机信息安全行业协会
（54）贵州省软件开发行业协会
（55）云南省信息安全协会
（56）内蒙古自治区网络行业协会
（57）新疆维吾尔自治区信息网络安全协会
（58）宁夏网络与信息安全行业协会
（59）广西网络安全协会
（60）石家庄市信息网络安全协会
（61）秦皇岛市信息网络安全协会
（62）长春市计算机信息网络安全协会
（63）沈阳市信息网络安全协会
（64）大连市信息网络安全协会
（65）辽阳市网络安全协会
（66）西安市信息网络安全协会

（67）宝鸡市信息网络安全协会
（68）渭南市互联网协会
（69）济宁市信息网络安全协会
（70）青岛市计算机学会
（71）潍坊市网络空间安全协会
（72）曲阜市信息网络安全协会
（73）聊城市东昌府区信息网络安全协会
（74）郑州市网络安全协会
（75）杭州市网络安全协会
（76）宁波市计算机信息网络安全协会
（77）金华市信息安全协会
（78）金华市信息产业协会
（79）金华市网商协会
（80）湖州市计算机系统安全协会
（81）丽水市信息网络安全协会
（82）温州市软件行业协会
（83）焦作市信息网络安全协会
（84）新乡市信息网络安全协会
（85）三门峡信息网络安全协会
（86）洛阳市信息网络安全协会
（87）南昌市网络信息安全协会
（88）扬州市信息网络安全协会
（89）连云港市计算机信息网络安全协会
（90）南通市信息网络安全协会
（91）泰州市信息网络安全协会
（92）苏州市互联网协会
（93）郴州市信息网络安全协会
（94）湘潭市计算机学会
（95）广州市信息网络安全协会
（96）广州市信息基础协会
（97）广州华南信息安全测评中心
（98）深圳市计算机网络公共安全协会
（99）深圳市网络与信息安全行业协会
（100）佛山市信息协会
（101）揭阳市计算机学会
（102）揭阳网络空间安全协会
（103）揭阳市信息技术和软件协会
（104）珠海市信息网络安全协会
（105）清远市网络安全协会
（106）茂名市计算机信息网络安全协会
（107）茂名市网络文化协会
（108）河源市计算机信息网络安全协会
（109）惠州市计算机信息网络安全协会
（110）成都信息网络安全协会
（111）成都安全可靠信息技术联合会
（112）成都市大数据协会
（113）成都物联网产业发展联盟
（114）贵阳市信息网络安全协会
（115）贵阳市大数据产业协会
（116）曲靖市计算机信息网络安全协会
（117）玉溪市网络安全协会
（118）包头市计算机公共网络安全协会
（119）呼和浩特市计算机信息网络安全协会
（120）巴彦淖尔市计算公共信息网络安全协会
（121）呼伦贝尔市网络行业协会
（122）乌海市计算机公共安全网络协会
（123）锡林格尔盟信息网络安全协会
（124）通辽市信息网络安全协会
（125）南宁市信息网络安全协会
（126）北京融智企业社会责任研究院
（127）重庆信息安全产业研究院
（128）甘肃烽侦网络安全研究院
（129）广东新兴国家网络安全和信息化发展研究院
（130）广东省现代社会评价科学研究院
（131）广东中证声像资料司法鉴定所
（132）四川大学信息安全研究所
（133）中国计算机学会计算机安全专委会
（134）中国联合国采购促进会网信分会
（135）中国文化管理协会网络文化工作委员会

联合发起单位

北京大学

中国电子技术标准化研究院

国家计算机病毒应急处理中心

中国互联网协会

技术支撑单位

中关村信息安全测评联盟

长沙冉星信息科技有限公司（问卷星）

北京天融信网络安全技术有限公司

广州华南信息安全测评中心

部分新闻媒体

人民网

中国网

央视《社会与法》频道

《经济参考报》

《中国信息安全》

《信息安全与通信保密》

《信息网络安全》

《信息安全研究》

中国消费者报

南方都市报

凤凰网

南方网

金羊网

大洋网

企业家日报网

腾讯新闻

百 度

新 浪

搜 狐

深圳新闻网

佛山新闻网

奥一网

21CN

东莞阳光网

广众网

大河网

大名网

湖南频道

广西新闻

苏州新闻网

平安时报

南国早报

平安常州

浙中在线

茂名日报

金华新闻网

莆田新闻网

其他新闻媒体

部分支持企业

腾 讯	UC 网站
百 度	益安在线
网 易	爱加密
新 浪	西部数据
斗 鱼	酷 六
虎 牙	优贝在线
优 酷	第一视频
爱奇艺	安全牛
今日头条	维沃移动通
哔哩哔哩	唯品会
搜狐视频	广东太平洋
酷狗音乐	房多多
奇虎 360	顺 丰
YY	滴 滴
TT 语音	摩 拜
映 客	金 山
美 团	58 到家
魅 族	成都联通
vivo	成都安洵
贝壳找房	荔枝微课
珍爱网	足力健
4399 网站	其它支持单位

特别鸣谢

公安部第一研究所

公安部信息安全等级保护评估中心

中关村信息安全测评联盟

全国各级公安网安部门

全国各级网信部门

全国各网络安全等级保护测评机构

附件二：系列调查报告清单

系列调查报告

“2019 网民网络安全感满意度调查活动数据统计报告”共分为三大类，62 个报告，分别为：

一、 全国报告（共 3 个）

1、总报告

2、公众网民版报告

3、从业人员版报告

二、 地方公众网民版调查报告（共 41 个）

其中，31 个省份、直辖市、自治区报告：

1、北 京	2、天 津	3、河 北	4、山 西
5、内蒙古	6、辽 宁	7、吉 林	8、黑龙江
9、上 海	10、江 苏	11、浙 江	12、安 徽
13、福 建	14、江 西	15、山 东	16、河 南
17、湖 北	18、湖 南	19、广 东	20、广 西
21、海 南	22、重 庆	23、四 川	24、贵 州
25、云 南	26、西 藏	27、陕 西	28、甘 肃
29、青 海	30、宁 夏	31、新 疆	

10 个地市报告：

1、广 州	2、深 圳	3、杭 州	4、苏 州
5、成 都	6、武 汉	7、贵 阳	8、郑 州
9、南 宁	10、金 华		

三、 地方从业人员版调查报告（共 9 个）

1、北 京	4、天 津	3、江 苏	4、浙 江
5、安 徽	6、福 建	7、广 东	8、广 西
9、四 川			

四、　　专题报告汇编（共 9 个专题报告）

报告名称	承担单位	撰写人	职务/职称
1、2019 网络安全法制建设报告	公安部第三研究所 网络安全法律研究中心	黄道丽	主任、副研究员
2、2019 遏制网络违法犯罪行为报告	中国政法大学 网络法学研究院	李怀胜	副教授、刑法学博士
3、2019 年网络犯罪防治网民基础报告	北京师范大学 网络法治国际中心	吴沈括	执行主任、法学教授
4、2019 互联网企业网络安全社会责任感调查报告	赛迪区块链研究院	黄忠义	院长助理、方案策划部主任
5、2019 个人信息保护调查报告	中国政法大学 网络法学研究院	王立梅	副院长、教授
6、2019 未成年人网络权益保护调查报告	南都大数据研究院	冯群星	高级研究员
7、2019 网络购物安全调查报告	阿里巴巴法务部	顾 伟	法律应用研究中心副主任
8、数字政府服务安全调查报告	工信部赛迪智库 网络安全研究所	刘 权	所长
9、网络安全产业发展调查报告	中关村网络安全 与信息化产业联盟	王 克	联盟企业移动计算工作组（EMCG）组长