网络安全产业人才发展报告

（2021年版）

工业和信息化部人才交流中心

工业和信息化部网络安全产业发展中心

2021 年 10 月

编委会名单

指导委员会（按姓氏笔画排序）

付京波　色云峰　李学林　李新社　张盛兵　杨　超

陈　新　苗春雨　段平霞　高　明

工作委员会（按姓氏笔画排序）

于孟琪　王欢欢　李天佑　李吉音　李利利　李君晟

刘志强　杜　妍　张俊伟　杨嘉丽　张　磊　苗　雨

郑思洵　金碧霞　柏　雪　唐　林　程　宇　谭　念

目 录

序　言 5
执行摘要 7
前　言 9
第一章 网络安全产业人才的发展概况 11
第一节 欧美发达国家网络安全人才培养情况简介 11
一、全民网络安全意识普及和宣贯 11
二、院校学历教育 12
三、网络安全知识体系和评价标准 13
四、网络安全认证认可和培训 13
第二节 我国网络安全人才发展概况 14
一、院校教育 15
二、网络安全从业人员培训 16
三、认证认可 17
第二章 网络安全产业人才的市场特征 19
第一节 网络安全人才的定义及特征 19
一、网络安全人才的定义 19
二、网络安全人才的特征 19
第二节 网络安全人才市场分析 25
一、网络安全人才的供需变化趋势 25
二、网络安全人才的供需地域差异 26
第三章 网络安全产业人才的需求分析 29
第一节 不同行业网络安全人才需求分布 29
第二节 不同规模用人单位网络安全人才需求分布 29
第三节 网络安全产业的岗位分析 31
一、网络安全产业的人才短缺岗位 31
二、网络安全相关岗位的能力要求 32
第四节 网络安全人才能力提升需求分析 33
第四章 网络安全产业人才的在校供给分析 38
第一节 院校网络安全及相关专业人才基本情况 38
一、在校生对专业的认知情况 38

二、在校生选择专业的影响因素 38
第二节 院校网络安全及相关专业建设情况 39
一、所在专业培养满意度 39
二、专业课程设置满意度 40
三、教学设施及条件满意度 41
第三节 在校生从业规划分析 41
一、在校生从业期望基本特征 41
二、在校生对网络安全行业从业期望分析 45
三、在校生就业需求分析 48
四、在校生网络安全相关证书考取情况 51
第五章 网络安全产业人才的在岗供给分析 53
第一节 网络安全从业人员择业分析 53
一、职业规划 53
二、网络安全从业人员择业的首要因素 54
三、网络安全从业人员择业渠道 55
第二节 网络安全从业人员工作现状 55
一、网络安全从业人员工作压力及满意度 55
二、管理制度建立及实施效果 56
第三节 网络安全人才流动分析 57
第六章 网络安全产业人才的发展建议 59

序　言

信息时代，网络空间已成为陆、海、空、天之外人类活动的“第五空间”。维护好网络空间这一非传统领域的安全，最关键的要素在于人。习总书记明确指出，人才是第一资源；网络空间的竞争，归根结底是人才的竞争。近年来，我国网络安全人才的问题得到了空前的重视，2016年12月《国家网络空间安全战略》正式发布，提出实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境。2017年6月，《中华人民共和国网络安全法》正式实施，提出国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。2020年，工业和信息化部发布促进网络安全产业发展的指导性文件把“网络安全职业人才队伍日益壮大”作为发展目标之一，并提出“推动高校设立网络空间安全学院或网络安全相关专业”“加强网络安全职业教育和技能培训”“推动校企对接”等一系列保障措施。2021年7月，《网络安全产业高质量发展三年行动计划（2021—2023年）（征求意见稿）》把“人才队伍建设行动”列为五大重点任务之一，指出要加强多层次人才支撑保障，促进创新链、产业链、价值链协同发展，培育健康有序的产业生态，为制造强国、网络强国建设奠定坚实基础，并明确了“创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高”的发展目标。

随着网络安全人才培养战略被推上前所未有的高度，各项人才措施全面推进，得到了全社会的热烈响应。学历教育方面，网络空间安全学科建设方兴未艾，已建立起本科、硕士和博士等不同层次的人才教育培养体系；在职培训方面，工业和信息化部人才交流中心积极贯彻网络强国战略，牵头组织揭榜了“工业和信息化重点领域人才能力评价机构”，与诸多高校、研究所及企业等主体明确能力评价合作关系，以安恒为例，成功申报了“工业互联网安全认证”“网络和信息安全认证”及“大数据安全认证”，旨在通过专业系统的岗位能力评价，提升网络安全人才的专业能力和综合素养，为国家党政军和关键信息基础设施运营单位的安全防护持续输送急需骨干人才。

尽管如此，我们需清楚看到我国网络安全人才队伍整体上还存在着人才供需失衡、教育培训缺乏、人才管理和激励机制有限等不足之处，远不能满足信息化快速发展的需要。长期以来网络安全人才市场一直处于供不应求的状态下，预估目前我国网络安全专业人才累计缺口在140万以上，而每年网络安全相关专业的高校毕业生规模仅2万余人，由此可见，我国网络安全人才供给存在“青黄不接”的情况，人才成长和培养速度显著落后于技术与社会变革的整体速度。但随着院校办学规模的扩大和办学模式的成熟，网络安全及相关专业的在校生数量及质量均处于稳步提升的状态，结合不断出台的各项利好政策，必将促进网络安全人才供给侧改革，推动网络安全人才培养进入良性发展阶段。

在工业和信息化部网络安全管理局的指导下，工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）共同牵头编写的《网络安全产业人才发展报告》（2021版）从促进产业人才供需对接的角度出发，全面分析梳理了网络安全产业人才队伍建设和发展情况，提出相关网络安全产业人才工作建议。报告中存在不当之处，还请指正！

执行摘要

《网络安全产业人才发展报告》（2021版）从多个维度对网络安全产业人才培养和发展现状的整体市场形势进行全面的分析，为院校、企事业单位的网络安全人才队伍的培养和建设提供借鉴。

本年度《网络安全产业人才发展报告》（2021版）的数据主要来源是，2019年6月至2021年6月猎聘网求职招聘平台大数据，以及由安恒信息设计、发放并回收的来自党政机关、企事业单位及院校的线上调研问卷，所形成安恒信息大数据。报告基于数据从网络安全产业人才市场的供需现状出发，对网络安全产业人才需求和人才供给进行了详细的分析和总结，得到以下结论：

（1）后疫情时代经济快速回温，网络安全产业人才需求高速增长，2021年上半年人才需求总量较去年增长高达39.87%，网络人才队伍在不断扩大；网络安全人才的质量和薪资也在稳步提高，自2019年以来超九成网络安全人才的最高学历为本科及研究生以上，2021年网络安全领域的平均招聘薪酬达到22387元/月，较去年同期提高了4.85%，这主要是因为用人单位通过社会招聘网站招募的大多数为中高端人才，薪资待遇会显著高于行业整体的平均工资水平。

（2）网络安全从业者呈现逐渐年轻化态势，80%以上的网络安全从业人员的年龄段集中于25-40岁之间，同时网络安全人才具有显著的性别特征，男性在网络安全行业仍然占据着主体的地位，占比超70%，这主要是由行业性质和网络安全及相关专业报考学生的性别差异所决定的。

（3）网络安全人才供需严重失衡，不仅体现在数量，更体现在不同类型人才供给和需求之间的错位。现阶段由于行业发展特点，人才队伍呈现底部过大，顶部过小的结构，即从事运营与维护、技术支持、管理、风险评估与测试的人员相对较多，从事战略规划、架构设计的人员相对较少，尤其缺乏既懂业务、又懂技术的高端综合人才，“重产品、轻服务、重技术、轻管理”的现象仍很普遍，导致人才的供需矛盾不断加深。

（4）网络安全在各行业的渗透率全面提高，同时网络安全人才分布呈现一定的集中效应，从行业来说，IT信息技术行业和互联网成为网络安全人才的需求大户；从用人单位规模和性质来说，千人以上规模的大（中）型、民营企业

抢占了大部分网络安全人才市场。

（5）参加社会类的网络安全培训已经成为网络安全从业者的提升技能的主流选择之一，对于培训方向的选择上，从业人员偏向于基础攻防技术、安全管理、安全运营和安全运维及应急响应等方向。

（6）信息安全专业认证已经逐步成为各行各业的对信息安全人才认定的方式，信息安全人员持证上岗已经成为大势所趋，网络安全人才多从认可度及权威性考虑考证类型，由国家测评中心、工业和信息化部、人力资源和社会保障部以及中国网络安全审查技术与认证中心（CCRC）发布的证书受到从业者的广泛认可；注册信息安全专业人员（CISP）、信息系统安全专业认证（CISSP）、中国信息安全保障人员认证（CISAW）等成为考证的热门选择，除此之外，随着产业数字化转型，细分岗位垂直化专业化愈发显著，由工业和信息化部人才交流中心推出的工业和信息化人才岗位能力评价证书在从业者当中的认可度不断提升。

（7）对于网络安全及相关专业，受访学生对专业了解程度总体较高。从专业建设情况来看，多数学生对包括课程设置、教学设施等专业培养相关内容较为满意，但仍存在亟待改进之处。从就业规划角度而言，呈现出学生对行业兴趣浓厚，就业热情高涨的态势，选择城市依旧以一线沿海地区为主。

（8）调查显示出行业招聘与学生求职过程中存在信息不对称的现象，使得部分人才在求职过程中因信息渠道受限，而出现就业难的问题。企业对于就业学生的帮助可在多提供实习机会、加强与院校合作及提供培训等方面进行。

前　言

伴随数字化的快速发展、信息技术的更广泛应用，数字经济已成为国民经济繁荣发展的重要战略。新的发展机遇带来新的风险与挑战，网络安全作为数字经济和智能化发展的基石，关乎国家利益、人民福祉。为打造更高水平的网络安全阵地，国家对网络安全产业发展给予了不同维度的政策支持。

从国家发展的宏观战略背景来看，2021年国务院发布《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》（以下简称十四五规划）正式发布，全文共十九篇、六十五章，“数字经济”被单独列为一篇，并提出2025年数字经济核心产业增加值占GDP比重提升至10%。作为数字经济发展的重要保障，网络安全、数据安全文共被提及18次，贯穿整个十四五规划，涉及国家、经济、网络、数据、生态、公共等各个领域。“安全”成为继“发展”之后，又一重要关键词，已成为国民经济和社会发展的重要风向标，也是“十四五”期间中国发展建设的工作重点之一。同时，为尽快实现网络安全产业的发展预期，2021年7月12日，工业和信息化部公开征求对《网络安全产业高质量发展三年行动计划（2021—2023年）（征求意见稿）》的意见。文中提出，到2023年，网络安全产业规模超过2500亿元，年复合增长率超过15%。一批网络安全关键核心技术实现突破，达到先进水平。

产业的发展都离不开人才培养，自2015年6月，“网络空间安全”一级学科正式获批后，2016年7月，在《关于加强网络安全学科建设和人才培养的意见》中提出要求建立党政机关、事业单位和国有企业网络安全工作人员培训制度，提升网络安全从业人员安全意识和专业技能。2016年《网络安全法》正式通过，其中提出“各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。大众传播媒介应当有针对性地面向社会进行网络安全宣传教育；国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流”。在教育部发布的《2021年度普通高等学校本科专业申报材料公示》中，拟新增的455个本科专业中，共有30所高校新增“网络空间安全”专业，此外还有8所高校新增了“信息安全”专业，2所高校

新增了“保密技术”专业，6所高校新增了“密码科学与技术”专业，不难看出，网络安全相关专业已成为高校新兴专业建设的重点方向。

“网络空间的竞争，归根结底是人才的竞争”，但人才培养具有滞后性，加之网络安全本身也具有后伴生性的特点，导致网络安全从业人员的职业技能也需要与时俱进，随着5G基础设施等新基建的推进，智慧城市数字化进程逐步完善，网络安全人才的数量和质量需求均进一步增加，提升当前从业人员的网络安全素养和为网络安全人才队伍建设不断输入新鲜血液刻不容缓。

为了深入探究网络安全产业人才发展的现状，促进网络安全人才的培养与发展，为进一步提升网络安全人才的数量与质量，本次报告基于国内外网络安全人才培养过程中的知识体系建设，从网络安全产业人才的市场特征、人才需求、院校供给、社会供给及网络安全产业人才的发展建议等五个维度进行展开，深挖网络安全人才的发展特点，从而更有针对性地反映网络安全产业这一垂直领域的人才供需现状，希望能够为网络安全人才培养相关的多方主体提供启发和借鉴。

本次报告总计分为六章，第一章主要从全民网络安全意识普及、院校学历教育、网络安全知识体系和评价标准、网络安全认证认可和培训等几个方面分别对欧美发达国家和我国网络安全人才培养状况进行了总结和对比；第二章阐述了网络安全产业人才的定义、基本特征及市场供需情况，反映了当下网络安全人才的市场特征；第三章详细分析了当下市场对于网络安全人才的需求，从行业、用人单位、短缺岗位及能力提升方式等方面展开讨论；第四章基于不同的维度深入剖析了网络安全产业人才的在校供给情况，内容涵盖了网络安全及相关专业的学生的基本情况、专业建设情况、以及相关专业在校生的从业规划；第五章是网络安全从业人员的择业情况、工作现状及网络安全人才流动情况构成的网络安全产业人才在岗供给分析；第六章是基于前述的人才培养现状并综合考虑了发达国家的培养模式，提出相应的建议。

目前，网络安全人才事业已迎来最好的发展机遇，人才队伍建设工作多点发力，成效初现。在当前网络安全人才发展的关键历史时期，需要继续投身网络安全人才发展实践和探索工作中，共同为我国网络安全人才培养和队伍建设努力。

第一章 网络安全产业人才的发展概况

作为计算机、网络等新兴IT技术起源地，欧美国家在网络空间安全技术创新和人才培养方面较早的建立了体系，凝练出成果，特别是美国，早在2003年发布了国家网络空间安全战略后，次年即开启了网络安全意识月活动，旨在提高全民网络安全认知、理念和常识，并先后开展了K12网络安全教育、网络安全人才能力评估标准开发等工作。可以说，发达国家在网络安全文化宣传、人才梯队建设、学历教育和从业人员培养方面均开展了体系化的推进工作。

第一节 欧美发达国家网络安全人才培养情况简介

一、全民网络安全意识普及和宣贯

美国自2002年开始每年10月，以周为单位，设置特定主题开展网络安全意识月活动（National Cybersecurity Awareness Month），旨在提高美国公众（家庭、社区、组织机构）对网络空间安全的风险意识以及网络使用的责任心，同时吸引更多的年轻人学习和从事网络安全职业。并于2010年开始举办美国国家网络安全意识挑战赛（National Cybersecurity Awareness Campaign Challenge），通过参与一起虚拟的网络安全事件的活动，强化民众特别是青少年的网络安全意识提升和网络威胁的应对能力。相对来说，欧盟的相关工作启动较晚，2013年首次开展了网络安全月活动。

另一方面，在普适性网络安全教育方面，美国制定了大众数字文化培训的标准和战略方案，主要目的包括：1.使公众能够使用工具和技术来减少网络环境中的风险，增强公众策略；2.提供相关资源，方便院校教师对非计算机和网络安全相关专业的学生提供关于网络空间安全知识，这种网络安全教育已经覆盖从K12教育到高校非专业学生；3.通过各种途径，包括宣传普及运动、公共服务公告，提升小型企业和组织从业人员对于网络安全基础知识的素养。

可见美国的网络安全人才培养策略已经深入群众，惠及面广，通过宣传和特定活动强化民众对于网络安全的了解和认知，为网络安全人才队伍建设培养了良好的氛围和民众基础。

二、院校学历教育

早期，欧美国家的网络空间安全院校教育主要以“计算机科学与技术”专业方向的研究生培养为主，当各国纷纷发布了网络空间安全相关的战略后，部分高校开设网络安全相关专业，体系化的培养网络安全专业人才。值得注意的是，欧美国家的网络安全人才学历教育的主管单位一般均为国家安全部门或安全中心，而不是教类主管机构。美国计算机学会（ACM）、电子电器工程师协会计算机学会（IEEE-CS）、信息系统协会安全专业工作组（As SIGSEC）、国际信息处理联合会信息安全教育技术委员会（FPWG）于2017年底联合发布了《2017年网络安全高等教育课程指南（CSEC2017）》，定义了全面的院校教育网络安全课程知识体系，结合下文的NICE框架，为学历教育网络安全人才培养提供了依托和指导。CSEC将网络安全领域知识分为八大知识领域：a.数据安全、b.软件安全、c.组件安全、d.连接安全、e.系统安全、f.人员安全、g.组织安全、h.社会安全，共44个知识模块，并通过交叉概念为学生建立安全领域之间的内在联系，最后再以学科知识体系构建为导向，将上述八类知识和方法论紧密结合。

另外，美国也广泛开展高校非专业学生的第二专业学习，以此来广泛挖掘网络空间安全领域的专业交叉型复合人才，美国国家安全局（NSA）和国土安全部（DHS）“网络安全卓越学术计划（CAE）”联合制定了网络安全的知识体系和教学标准，2004年开始对美国高校和学术科研单位进行认定或认证。全美已有48个州、超过300所高校、科研院所及培训机构通过了CAE认定。同时，由美国国土安全部（DHS）、人事管理办公室（OPM）和国家科学基金会（NSF）推出的“网络兵团服役奖学金”（SFS）计划，旨在通过减免助学贷款或提供补贴等政策，鼓励有能力的学生在规定的时间到政府部门实习或工作，目前已有大约93%的学生通过SFS计划进入多个联邦政府部门从事全职或实习工作。欧盟也于2014年起将网络与信息安全培训引入高校，针对专业为计算机科学的学生进行网络与信息安全、安全软件开发以及个人数据保护等学科知识的培训。可见，为解决网络安全人才短缺的问题，欧美各国已经将专业人才培养扩展至更广泛的高校相关专业人才培养与选拔。

三、网络安全知识体系和评价标准

美国国家标准与技术研究院（NIST）于2017年发布了《国家网络安全教育计划(NICE)网络安全劳动力框架》指南，从网络安全行业的岗位角色维度，定义了相应角色的人员应该具备哪类知识、技术和能力，旨在为各组织对于网络安全职位的定义和类别提供参考，促进政府、学术界和企业之间在网络空间安全人才培养方面能够达成一致的理解，保障在网络安全行业的教育工作者、认证者、培训师、雇主和雇员之间能够针对人才培养和认证进行清晰的沟通，2020年NIST更新了这份指南，去掉了能力维度，增加了NICE框架的开放性和可操作性，这份指南对美国网络安全从业人员的在职业培训和认证提供了一个很完备的参考依据。同期，也出台了《联邦网络安全人员基线评估法案》《联邦网络安全人力评估法案》等一系列推动网络安全人才能力评估的法案和标准。英国学术界则从完整知识体系的角度出发，于2017年启动了网络安全知识体系研究计划，于2019年发布了第一版报告：*The Cyber Security Body of Knowledge*，将网络安全知识按照基础设施安全、系统安全、软件和平台安全、攻防技术体系和管理体系五大维度将网络安全的相关知识分为19个类别，并对每一类知识所覆盖的范围和内涵进行了详细介绍。

四、网络安全认证认可和培训

人员认证和认可是行业人才队伍建设的重要形式之一，能够为从业人员提供能力或资格的证明和证据，纵观全球网络安全行业，欧美发达国家的网络安全人员认证开展较早，比如由(ISC)（International Information Systems Security Certification Consortium, 国际信息系统安全认证联盟）组织与管理的CISSP（Certification for Information System Security Professional）认证，于上世纪90年代开始推广，成为了全球知名的信息安全行业人员认证，其它认证机构、协会也推出了若干普适性或细分领域的网络安全人员认证，美国的知名机构和协会，包括美国SANS（System Administration, Networking, and Security）、计算机行业协会（Computing Technology Industry Association, CompTIA）以及EC-CONSUL（International Council of E-Commerce Consultants, 电子商务顾问局）均为在职人员提供各类网络安

全培训和认证，且因其知识体系的完备性和教学资源与形式的先进性在业界形成了良好的口碑与知名度。以SANS的培训认证为例，覆盖网络防御、渗透测试、事件响应和取证、管理、审计、法律、安全开发、工业控制系统8大类，且每一大类下又细分若干小类，比如网络防御类培训包含从基础、纵深防御到入侵检测等10个小类的培训，且几乎每类培训均配备了相关的案例和练习平台，可以说SANS的网络安全从业人员培训和认证已成为体系最完备、影响力最大的国际网络安全从业人员培训和认证序列。其它一些行业协会和企业，也在运营特色鲜明的网络安全相关人员认证，如CSA（Cloud Security Alliance，云安全联盟）、ISACA（Information Systems Audit and Control Association，信息系统审计与控制协会）等组织。除了网络安全认证体系建设方面的工作，美国早在2010年发布的DoD8507号令中明确要求从事网络和信息系统相关岗位工作的现役军人、文职雇员及项目承担企业的人员必须获得相应的网络安全从业资质认证。每类信息安全保障人员均须通过相关要求规定的背景调查，经考试获得相应信息安全资质持证上岗；在岗期间还需采用持续学习教育等方式，维持资质的有效性，可见，美国政府希望通过登记注册和继续学习等手段，确保网络安全从业人才队伍具备技术能力和可信性。

欧美发达国家在网络和信息安全方面的人员认证品类与完整度上有着明显优势，但也存在发证主体多和自成体系的问题，即使如SANS这样的机构也在不断调整认证种类，同时将认证培训和夏令营、技能培训等业务进行打通，力求发挥教育教学资源的增值效应。

第二节 我国网络安全人才发展概况

我国于2001年由武汉大学设立了第一个信息安全专业，如信息工程大学等其它军事院校也已经在培养信息对抗等相关专业人才，但直到2015年国家才设立网络空间安全一级学科，2016年中央网络安全和信息化领导小组办公室发布《关于加强网络安全学科建设和人才培养的意见》，加速了网络空间安全人才培养的步伐，各类网络空间安全相关的法律法规中均涵盖了人才培养的条款和内容。可以说，无论是学科和专业建设，还是从业人员的能力提升，均得到了空前的重视，“网络空间的竞争归根结底是人的竞争”这个重要论断逐步得到

全行业的重视并作为构建网络安全保障体系的关键指引。在多方主体的共同努力下，近年来，网络安全行业和产业的人才匮乏状况得到明显的改善，但由于数字化转型的迅速开展、历史遗留缺口较大，加之前文提到的人才培养路径和复杂度问题，目前网络安全人才仍呈现供不应求态势，另一方面，由于网络安全贴近实战、不产生直接价值等诸多客观因素和特性，导致网络安全人才的供给两侧错配、人才发展受限的情况依然存在。

一、院校教育

从宏观来讲，网络安全人才包括安全产品研发、市场营销等网络安全产业链前后端工作角色，但本文只讨论网络空间安全、信息安全应用技术直接相关的院校教育。在这一范畴内，自2016年起，有将近100所本科院校设立或申请设置网络空间安全专业，近200所高职类院校开设信息安全应用技术或相关专业，因此，我们将高校和科研院所培养的网络安全人才粗粒度地分为基础研究型人才和高水平应用型人才两大类，总体来说，这两类人才均无法满足企事业单位的用人需求。

基础研究型人才的理论研究内容与实际应用场景偏离较大，除某些密码学领域研究无需太多考虑应用场景外（其实密码学基础研究，有时也需要考虑场景，如：物联网应用场景需要轻量级加密和认证方法），大量的基础性研究最后仍需要落地于具体的应用场景和实际生产环境，脱离实际的纯方法论研究导致短时间内无法走出实验室，而网络安全产业国内外竞争激烈，讲究实战，导致此类基础研究型人才的能力无法在企业得到快速转化，价值降低，往往需要1-2年的转化期，对掌握的方法论重新梳理和整合，才能胜任企业研发工作。

高水平应用型人才在各高校的实践能力养成方面存在较大差距，加之在校期间主动参与企业实践的能动性不同，导致部分应届毕业生（约20%）能够快速融入真实业务，达到企业人才需求，另一部分（约40%），需要1-2个月的实践培训和演练，能够胜任企业实践能力要求，另外的部分则根本没有掌握行业相关实战技能，也就没有能力进入行业工作。引发上述供给侧错配的根本原因是院校培养资源匮乏，主要表现在师资队伍、实践教学环境、实践教材和实践能力养成体系等几个方面：

1.师资严重不足的问题在应用型人才培养院校表现尤为突出。

2.在实践教学环境建设方面投入不足，或在有限的投入中希望纳入实践教学和竞赛指导等外包服务，导致本身的建设费用降低，无法构建真正贴近实际生产环境的实践平台。

3.实践教学体系由实验、实训和实习三大主要阶段构成，而由于网络安全相关专业的学科交叉特性，导致需要大量的课外和校外学习与实践，而在这方面的体系化设计、计划和执行方面均存在不足。

4.考核机制问题导致大量年轻教师进入院校后，在真正的应用型人才培养方面无法投入过多精力。

5.由于相应制度和保障措施的不完备或不到位，导致产学研合作往往是两张皮，价值不能统一，无法形成真正的产教融合。

二、网络安全从业人员培训

（一）从业人员面临的挑战呈上升趋势

在信息技术与各行各业不断融合的大背景下，国家导向和合规性方面均对网络安全从业人员提出能力提升要求；而结合大量国内外企业信息安全相关风险和解决方案的调研数据，人员已经成为网络安全保障工作的最重要因素，人员的安全素养和技术能力已成为网络安全体系建设中不可忽略的要素，因此，在合规性需求和业务需求双轮驱动的态势下，从业人员面临的安全挑战呈上升趋势，无论是从组织视角还是个人视角，能力提升的需要也水涨船高。

（二）从业人员能力提升渠道有限

当前，大部分网络安全从业人员除了在工作中经验的自我积累和沉淀，能力提升的主要渠道包括自主报名认证培训、学习社区或平台进行自学，只有少数网络安全队伍建设比较完备的行业会组织内部分享、邀请专家或购买服务的方式为网络安全从业人员提供学习机会，但总体来说，网络安全人员的能力提升仍然是依靠自学为主。

（三）从业人员学习内容缺少体系化设计

无论是自学为主，还是单位组织的网络安全培训，均呈现培训内容零散，缺少体系化设计，而部分强制培训的网络安全人员认证，由于其课程体系是基于学员已有基础和培训目标而设计，具有一定的体系化特性，但其培训时长固定，无法满足定制化需求；虽然讲座形式能够起到提升理念，开拓视野的作用，但对于系统化的提升从业人员能力也是收效甚微。

（四）从业人员培训成果与业务关联度有待提高

虽然部分行业进行了有组织的人员培训，但从培训导向和实施过程来看，培训内容与实际业务的关联度有待提升。一方面，有些培训是因为各行业通过组织技能竞赛来实现“以赛促学、以赛促建”的目标，但网络安全行业的特殊性，导致竞赛内容无法与真实业务高度关联，因此配套的培训也受限于竞赛内容和形式；另一方面，以不同视角组织的技术培训虽然突破了竞赛模式的限制，但由于网络安全的伴生性和对场景的高度依赖，也无法做到有的放矢，导致培训无法产生闭环效果，无法切实提升受训人员的业务能力。

三、认证认可

对技术技能型密集的行业来说，建立完善的职业培训和认证体系，为从业人员提供持续性学习和知识更新渠道，是填补新兴领域人才缺口的有效解决途径，对于网络安全行业更是如此。而构建符合行业发展需求、体系完备的网络安全从业人员培训和认证标准是实施行业从业人员培养和评估的重要指导和保障。目前，我国多家网络安全主管机构均已构建和运营系列网络安全人员认证认可证书，其中以中国信息安全测评中心的CISP系列认证、中国网络安全审查技术与认证中心的CISAW系列认证最具代表性，这两大认证体系均设置了若干子领域，CISP系列认证以技术领域划分为主，CISAW以工作岗位划分为主。此外，国家互联网应急中心（CNCERT）的CCSC（Certification for Cyber Security Competence，网络安全能力认证）、公安部的网络安全等级保护测评师认证、工业和信息化部的信息安全工程师，都具有较强的权威性。其中，工业和信息化部有关单位一直基于《工业和信息化人才岗位能力评价通则》所规定的评价

框架积极开展产业人才能力评价工作，该评价框架从专业知识、技术技能、工程实践和综合能力四个维度对评估对象进行考核与评价，并按照产业发展需求及岗位进阶的客观规律，将产业人才岗位能力等级分为3级，共9等，即能力1-3等为初级、能力4-6等为中级、能力7-9等为高级。例如工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）牵头正在编制网络信息安全产业人才岗位能力要求标准，涉及安全体系架构师等38个岗位。另外，人力资源和社会保障部发布的网络与信息安全管理人员、信息安全测试人员等职业技能等级认定证书，也切实为行业技能人才培养提供了指导和评价作用。

以专业应用型人才培养为定位的高校学生近几年则以“1+X”培训和认证作为职业技能提升和评价依据，但众多厂商推出的“1+X”认证重复性较高，能力评价标准规范性和操作性均有待提高。

第二章 网络安全产业人才的市场特征

第一节 网络安全人才的定义及特征

一、网络安全人才的定义

广义的网络安全人才包含了信息安全环境的建设者、攻击者、保护者和管理者，而狭义的网络安全人才则通常指的是网络安全的保护者，本次报告将网络安全人才界定为在网络安全行业从事保护计算机硬件、软件、数据不因偶然和恶意的原因而遭到破坏、更改和泄露的人员，包括了攻防类人才、工程类人才、开发类人才、治理类人才、管理运维类人才等多类型的网络安全人才。

二、网络安全人才的特征

（一）网络安全人才的基本特征

1.网络安全人才的性别特征

对近三年的网络安全从业人员的性别分布情况进行分析，我们发现，男性在网络安全行业仍然占据着主体的地位，占比超70%，同时女性占比的增长趋势愈发明显，2020年同比增长不足0.3个百分点，2021年增幅已接近2个百分点，男女比例首次低于3:1，但结合高校网络安全及相关专业接近4:1的男女比例来看，网络安全行业女性占比未来提升空间比较有限，这表明不仅需要提高网络安全专业对高校女生的吸引力，同时也要提高在职女性对网络安全行业的好感度。

以上特点主要是受网络安全行业的工作特点和人才供给特征所影响，大多数传统的网络安全岗位需求专业多为理工科专业，如计算机、电子信息工程、软件工程和网络工程等，而此类专业都是男性居多，但随着数字经济时代的到来，网络安全的形态正在发生变化，网络安全岗位需求逐渐呈现多元化，为女性提供了更多的合适岗位，如安全咨询、安全教学、安全管理体系构建等岗位。

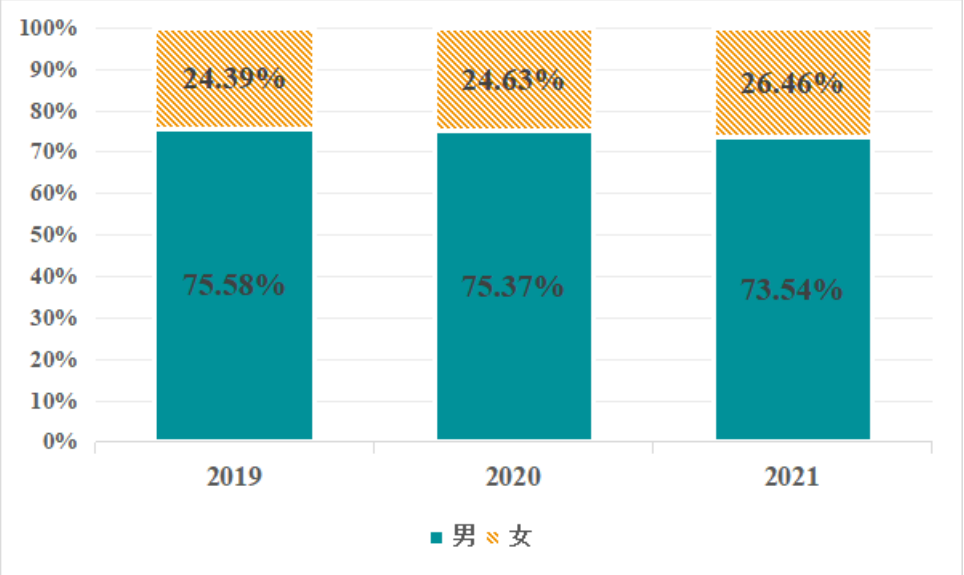
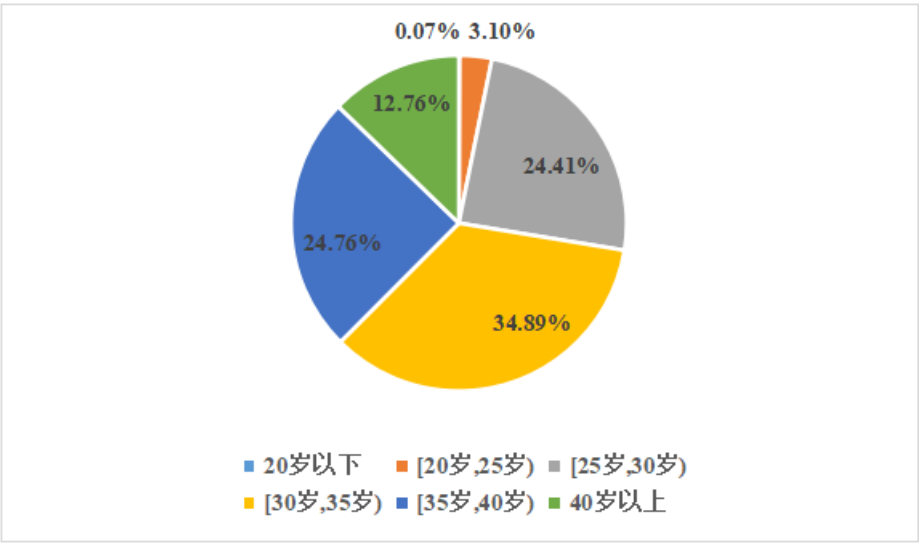


图2-1 2019-2021年网络安全人才性别分布[1]

2.网络安全人才的年龄及工作年限

从网络安全人才的年龄来看，网络安全从业者年轻化程度高。近两年来，八成以上的网络安全从业人员的年龄段集中于25-40岁之间，过半都是35岁以下的青年，30-35岁之间占比最高，约为35%，与去年同期基本持平。结合工作年限来看，从业5-10年的人数最多，为34.58%，10-15年和不到5年的从业人数占比次之，分别为27.16%和18.50%，反映了网络安全领域从业人群的年轻化现象，这说明网络安全领域对青年人才存在较高的吸引力，但资深人才储备不足，以及新人培养和育留难度大，将成为企业普遍面临的挑战。



[1] 注：来自于猎聘大数据、工业和信息化部人才交流中心人才大数据中心

图2-2 2021年网络安全人才年龄分布

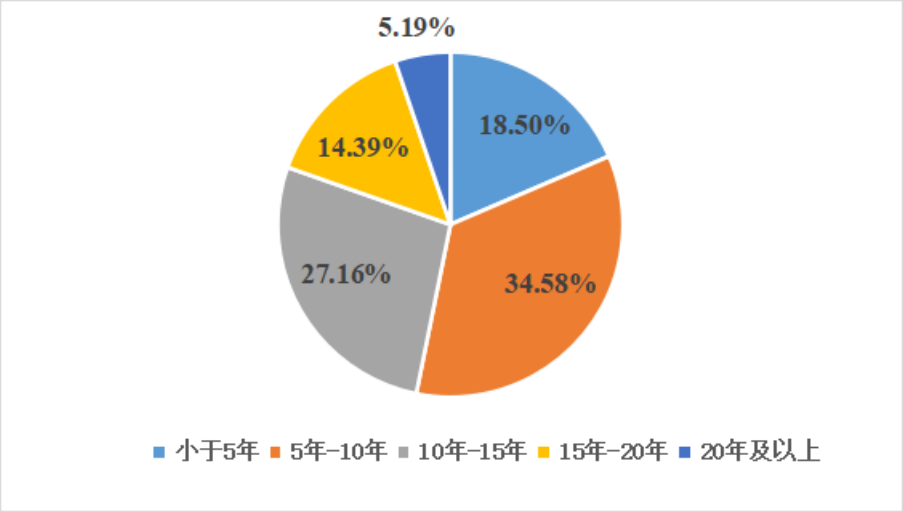


图2-3 2021年网络安全人才工作年限分布[2]

3.网络安全人才的薪资

人才竞争态势也体现在薪酬水平的变化上。数据显示，网络安全领域的薪酬近年来稳步增长，2021年上半年，网络安全领域的平均招聘薪酬达到22387元/月，较去年同期提高了4.85%，相较于全行业的平均工资偏高的主要原因是大部分公司通过社会招聘网站希望招募的人才都是经验足、技术强的人才，对应的薪酬也比较高，对于基础的薪酬比较低的岗位，大部分公司都偏向于选择内推而非社会招聘。

从不同岗位的平均薪资比较来看，技术岗和产品岗由于其各方面岗位能力要求较高，相应的工资水平也显著高于其他岗位，其中市场需求量最高的研发技术岗成为含金量最高的岗位，2021年上半年平均月薪24887元/月，这主要是因为在当前网络安全人才紧缺的大环境下，企业想招到合适的人，必须在薪酬福利上体现出竞争优势。

表2-1 2019-2021年网络安全行业不同岗位平均薪资（元/月）

年份	2019年		2020年		2021年	
岗位	平均薪资	需求占比	平均薪资	需求占比	平均薪资	需求占比
研发岗	22623	60.41%	23691	61.93%	24887	64.32%
销售岗	10652	10.22%	11024	12.14%	12569	13.24%

[2] 注：来自猎聘大数据、工业和信息化部人才交流中心人才大数据中心

运营岗	12103	5.25%	12892	5.96%	13854	6.02%
职能岗	7099	4.97%	7252	4.89%	7800	4.92%
产品岗	20679	4.54%	21398	4.81%	21965	4.83%

注：来自猎聘大数据

（二）网络安全人才的专业背景

1.网络安全人才的最高学历

国内网络安全人才培养的主要途径是大学教育，主要培养本科及以上专业人才。从近三年的网络安全人才的学历情况统计结果来看，网络安全人才的最高学历分布呈现橄榄型特点，即本科学历占比最高，随着学历的提高和降低，网络安全人才占比都有相应的降低，2021年本科占比63.89%，与2020年相比稳中有升，大专及以下和硕士占比较为接近，均在17.51%左右，较2020年波动不大，反映了在2019年网络安全行业迎来第一批“网络空间安全”专业毕业人才后，网络安全行业人才综合素质水平有显著的提升。

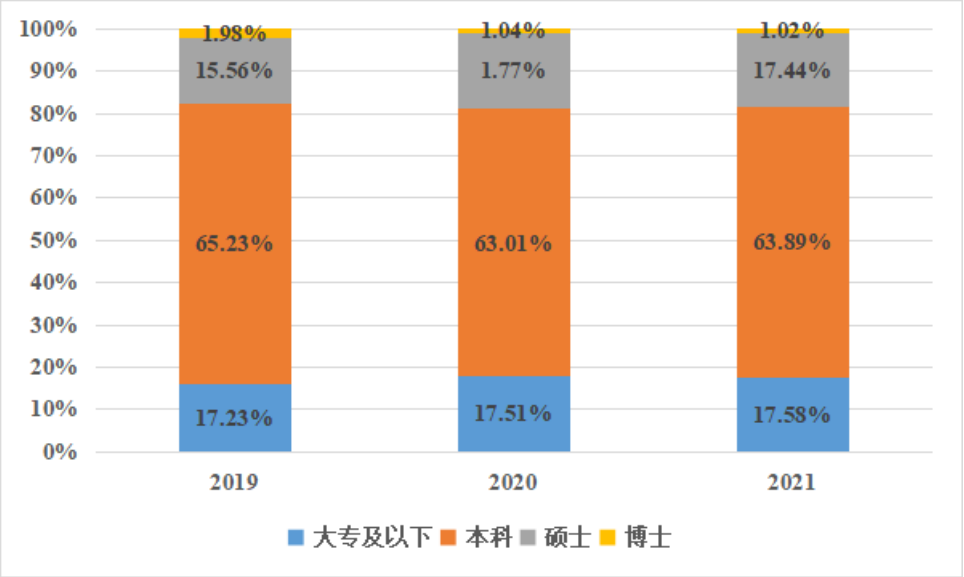


图2-4 2019-2021年网络安全人才最高学历分布[3]

2.网络安全人才的毕业院校

根据猎聘网提供的数据来看，华中科技大学、电子科技大学、西安电子科技大学、哈尔滨工业大学、武汉大学等名校为网络安全行业输送了大量的人才。下表所示为猎聘平台上，投递网络安全岗位的求职者毕业的前15所国内学

[3] **注：来自猎聘大数据、工业和信息化部人才交流中心人才大数据中心**

校，其中，前15名中大学所属城市前三名：武汉（3所）高校、西安（2所）、成都（2所）。

值得注意的是，在2019-2021年期间，前五名的学校仅在顺序上发生了内部的变化，表明了这5个高校在网络安全行业内人才输送的稳定度。毕业院校是学生就业的一个敲门砖，网络安全人才综合素质的体现更取决于自身的学习能力及发展空间，如何培养出高质量的网络安全人才是我们需要继续努力的方向。

表2-2 网络安全人才毕业学校占比TOP15

学校名称	2019年	2020年	2021年
华中科技大学	1.84%	1.73%	1.81%
电子科技大学	1.91%	1.83%	1.69%
西安电子科技大学	1.73%	1.76%	1.60%
哈尔滨工业大学	1.35%	1.22%	1.32%
武汉大学	1.12%	1.13%	1.07%
武汉理工大学	1.06%	1.09%	1.03%
重庆邮电大学	1.04%	1.03%	1.01%
吉林大学	1.08%	1.04%	1.01%
南京邮电大学	1.08%	1.08%	0.95%
中南大学	0.94%	0.87%	0.86%
四川大学	0.88%	0.84%	0.82%
北京邮电大学	0.86%	0.86%	0.81%
东北大学	0.87%	0.86%	0.78%
西安交通大学	0.80%	0.83%	0.77%
浙江大学	0.76%	0.69%	0.71%

注：来自猎聘大数据

3.网络安全人才的专业及知识技能来源渠道

从网络安全人才的学科专业背景来看，近三年来，绝大多数的网络安全行业求职者来自于计算机、通信工程、电子信息工程及软件工程等相关专业，拥有网络安全或信息安全的学科教育背景的人数较少，表明虽然越来越多的院校设立了网络安全专业，但对于网络安全行业巨大的人才缺口来说还是供不应

求，需要进一步加大对高校网络安全及相关专业的建设，提升网络安全人才的数量和质量。

表2-3 网络安全行业求职者所学专业TOP10

专业	2019年	2020年	2021年
计算机科学与技术	8.66%	8.22%	7.15%
通信工程	4.92%	4.75%	4.65%
电子信息工程	4.84%	4.81%	4.43%
工商管理	2.32%	2.33%	2.39%
软件工程	2.46%	2.37%	2.10%
市场营销	1.81%	1.93%	2.05%
自动化	2.06%	1.95%	1.83%
电子信息科学与技术	1.26%	1.28%	1.25%
计算机应用	1.35%	1.28%	0.96%
网络工程	0.87%	0.96%	0.92%

注：来自猎聘大数据

根据问卷调查显示，学科背景为网络安全相关专业的从业人员中，五成左右的人认为他们现在的就业领域与专业对口率在60%以上，从中可以反映出网络安全专业的学生毕业之后多倾向于从事与之专业相对口的工作。

与之相对应的是，当前网络安全相关专业的教学内容并不能满足学生的就业需求。从知识技能来源相关调查数据观察可得，62.82%的网络安全从业者在实际工作中应用的知识技能大多来自于工作后的项目积累，校内课堂学习仅占技能来源渠道的6.82%，不到校内课后自学占比的一半，直观地反映出，高校的人才培养与企业实际需求之间也存在一定的供需错配，还需进一步加强对网络安全相关专业的建设与改革，增加实践课程的教学内容，加深校企合作，缩小学校教育与企业用工需求之间的差距。

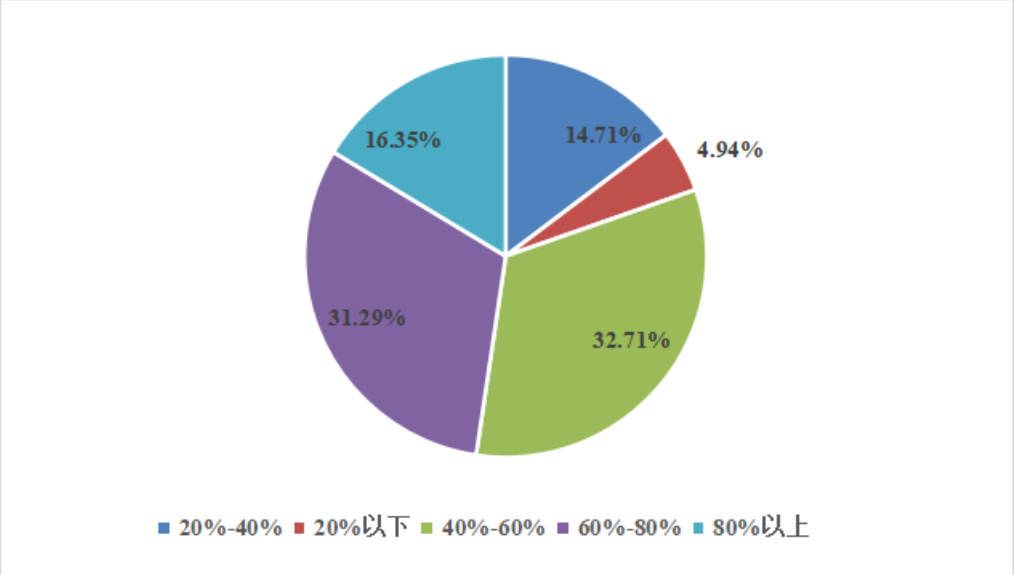


图2-5 网络安全及相关专业就业对口率[4]

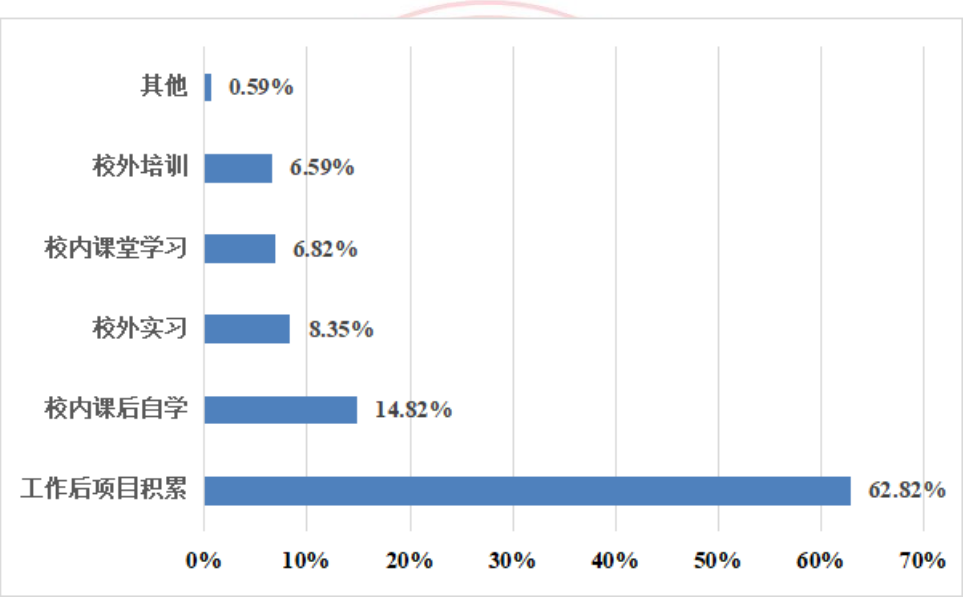


图2-6网络安全人才知识技能来源[5]

第二节 网络安全人才市场分析

一、网络安全人才的供需变化趋势

从2019-2021年上半年网络安全行业人才总体的供需变化中可以看出，由于疫情的严重影响，2020年网络安全行业的人才需求和供给明显下降，除此之

[4] 注：来自安恒大数据、工业和信息化部人才交流中心人才大数据中心
[5] 注：来自安恒大数据、工业和信息化部人才交流中心人才大数据中心

外，2019年和2021年网络安全行业的人才需求，较前一年同期相比，增幅显著，尤其是复工复产的后疫情时代，伴随着国内经济高速回温，企业对网络安全人才的需求也随之升温，2021年上半年增幅高达39.87%，反映了网络安全在各行业的渗透率全面提高，在人才需求结构中的重要性显著上升。

在网络安全人才需求持续升温的人才市场状态下，网络安全人才供给虽每年在稳步递增，但仍处于供小于求的人才市场局面，人才缺口不容乐观。愈发增加的招聘岗位数，愈发精确的网络安全岗位人才需求，亟需学校输送更多更高质量的人才进入到行业中。

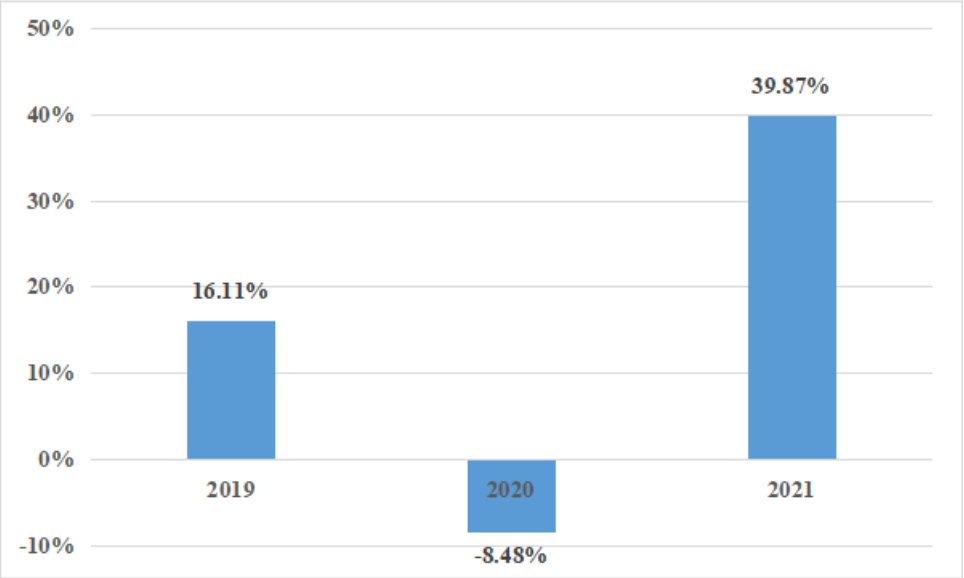


图2-7 2019-2021年网络安全行业人才需求同比增长[6]

二、网络安全人才的供需地域差异

网络安全行业是一个新兴的高新技术产业，从地域上来看，网络安全行业的龙头企业和国内高校多集中于北京、上海、深圳等一线城市，故不论是供给还是需求，上述城市在网络安全人才市场中都占据了极大的比例，从而网络安全人才的供需两端都存在着区域差异巨大的现象。

猎聘大数据显示，2021年网络安全人才需求排名前五的城市分别是北京、深圳、杭州、上海及成都，占了市场总需求的61.17%，与去年同期相比，提高了1.2个百分点，其中需求量排名前两位的北京和深圳远远领先于其他城市，占比超40%，表明龙头企业对于网络安全人才的需求在不断扩大；从网络安全人才

[6] 注：来自猎聘大数据、工业和信息化部人才交流中心人才大数据中心

供给侧来看，网络安全人才供给排名前五的城市分别是北京、深圳、上海、南京及成都，除北京基本不变外，其他城市占比都出现了不同程度的下降，这表明网络安全岗位人才的供给正在逐步下沉，越来越多非一线城市加大了对网络安全人才的培养力度。

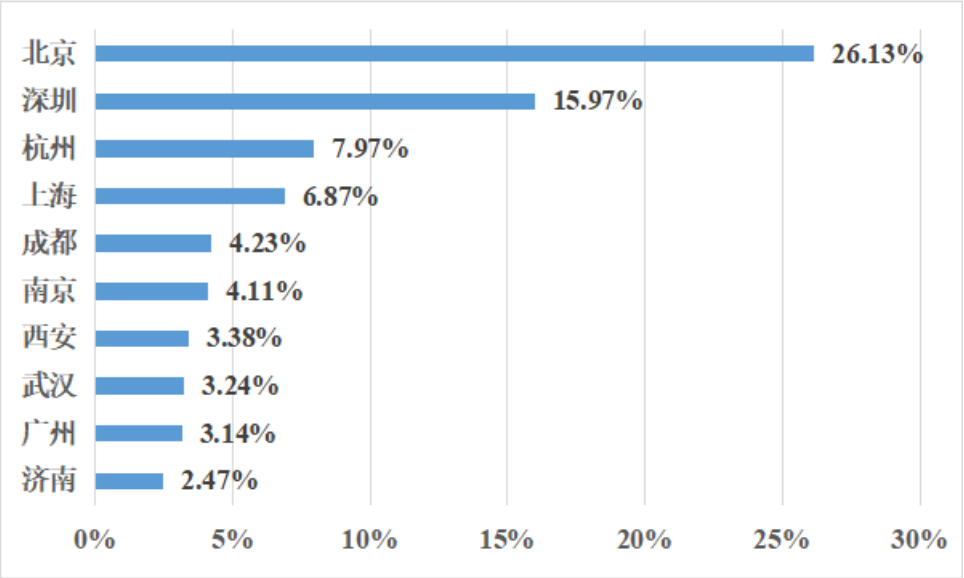


图2-8 2021年网络安全人才招聘需求城市排行[7]

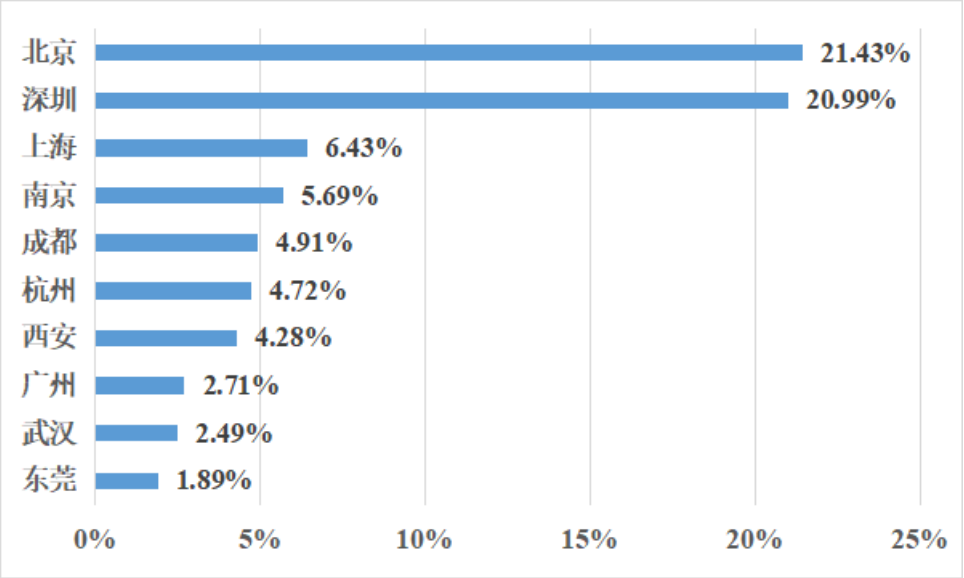


图2-9 2021年网络安全人才供给城市排行[8]

从区域的网络安全人才供需情况来看，以历年企业网络安全岗位数量和每年院校毕业的网络安全专业的学生总数为基础，网络安全人才市场每年的平均

[7] 注：来自猎聘大数据、工业和信息化部人才交流中心人才大数据中心
[8] 注：来自猎聘大数据、工业和信息化部人才交流中心人才大数据中心

需求与供给之比约为2:1。本报告以此作为市场供需的平均水平，并将各区域的数据进行处理，将“需求占比”指标除以“供给占比”指标得到供需系数，若供需系数大于1，则表明该地区的网络安全人才供需失衡高于市场平均水平；若供需系数小于1，则表明该地区的网络安全人才供需失衡低于市场平均水平。从表中可以看出，北京、杭州、上海、武汉、广州和济南对于网络安全人才供需失衡情况较为严重，需求量远高于供给量；而深圳、成都、南京和西安的供需情况，相较于市场平均水平而言，更加平衡。

表2-4 不同城市的供需系数表

城市	需求占比	供给占比	供需系数
北京	26.13%	21.43%	1.22
深圳	15.97%	20.99%	0.76
杭州	7.97%	4.72%	1.69
上海	6.87%	6.43%	1.07
成都	4.23%	4.91%	0.86
南京	4.11%	5.69%	0.72
西安	3.38%	4.28%	0.79
武汉	3.24%	2.49%	1.30
广州	3.14%	2.71%	1.16
济南	2.47%	1.41%	1.76

注：来自猎聘大数据

第三章 网络安全产业人才的需求分析

第一节 不同行业网络安全人才需求分布

从各行业对网络安全人才的需求分布来看，需求量最大的是IT信息技术行业和互联网，网络安全人才招聘需求占比总和超七成，其中IT信息技术行业对于网络安全人才的渴求显著高于其他行业，该行业发布的网络安全人才招聘数量占网络安全人才招聘总人数的45.24%，这主要是由其行业性质所决定的，IT信息技术行业是一门带有高科技性质的服务性产业，它运用信息手段和技术，收集、整理、储存、传递信息情报，提供信息服务，因此对于信息安全的保护有高度的需求。

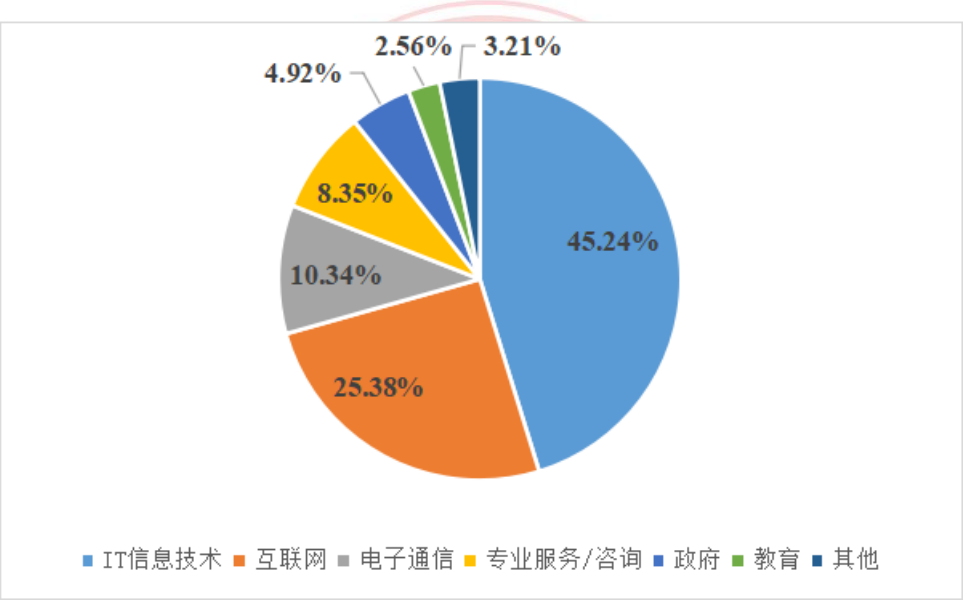


图3-1 不同行业对网络安全人才的需求量分布[9]

第二节 不同规模用人单位网络安全人才需求分布

从用人单位的规模和经营性质来看，网络安全行业存在一定的人才集聚效应，千人以上规模的大（中）型、民营企业成为网络安全人才市场需求的主力军，近三年民营企业的比例均在50%左右，这与前几年所呈现的市场局面有所不

[9] 注：来自猎聘大数据和安恒大数据、工业和信息化部人才交流中心人才大数据中心

同，央企、大型科研院所、机关直属单位不再是网络安全人才需求大户。

从用人单位规模维度出发，具体而言，万人规模以上的大型企业对于网络安全类的人才需求最高，为35.70%。面对外部冲击，大型企业的抗压性和稳定性较好，为网络安全产业的平稳发展提供了良好的结构性基础。值得注意的是，近三年来，百人规模以上的中型企业和中小型企业，对于网络安全人才的需求，以每年接近3个百分点的增幅在不断提高，表明自2019年网络安全等级保护制度2.0标准正式发布，提高了对中小型机构的安全等级要求，中小企业、民营企业——经济社会中数量最多的企业主体的安全需求正在逐步提升。

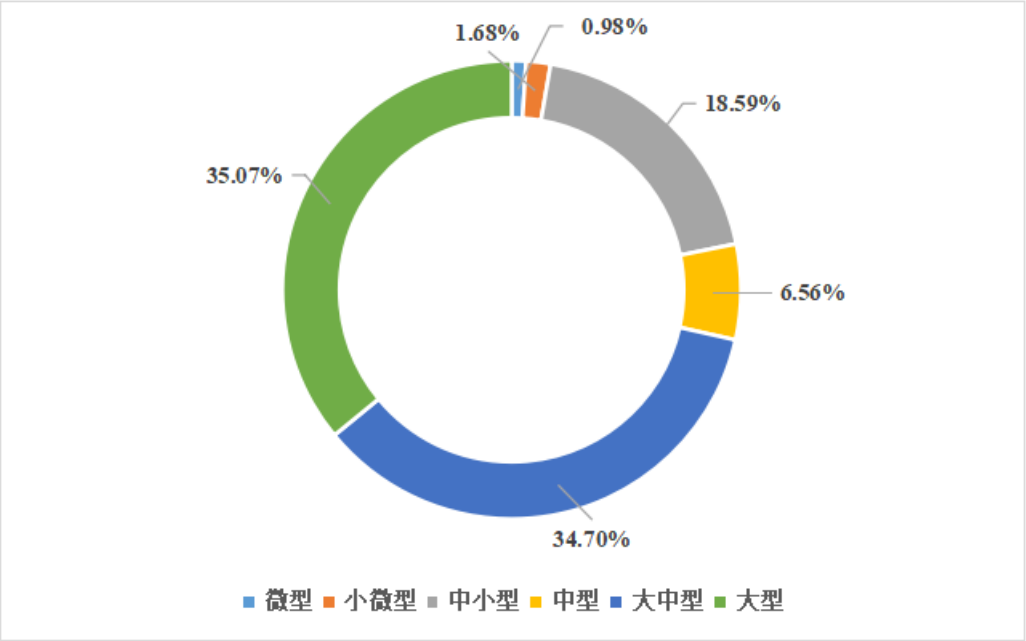


图3-2 不同规模用人单位对网络安全人才的需求量分布[10]

表3-1 企业规模表

企业规模	对应人数
微型	20人以下
小微型	20-99人
中小型	100-499人
中型	500-999人
大中型	1000-9999人
大型	10000人以上

[10] 注：来自安恒大数据、工业和信息化部人才交流中心人才大数据中心

第三节 网络安全产业的岗位分析

一、网络安全产业的人才短缺岗位

网络安全领域目前整体面临人才短缺情况，根据问卷调查显示，53.88%的网络安全行业从业者认为当前公司的网络信息安全人员队伍规模并不能满足当前工作需求，其中10.82%的从业人员认为公司处于人才非常短缺的状态。从业者认为人才短缺情况突出表现在，熟悉各种网络、系统及应用的安全攻击和防御技术研究的安全研究岗位、具有丰富实战攻防经验的核心技术研发岗位以及具有行业和政策视野的安全管理岗位上。具体而言，认为安全研究岗位人才短缺的占调查总人数的42.96%，是近半数的网络安全从业者公认的人才短缺岗位，其次是审计与评估、应急响应、安全态势分析、内容安全等技术岗位，均有超30%的从业者认为符合岗位职能的人才仍有所欠缺。值得注意的是，由于近年来，网络安全教学及培训业务兴起，该类型的岗位人才也存在较大的缺口。亟待由学校、企业培训和公共机构多个层面联合，出台更加完备、实战型和业务性更强的体系化训练机制。

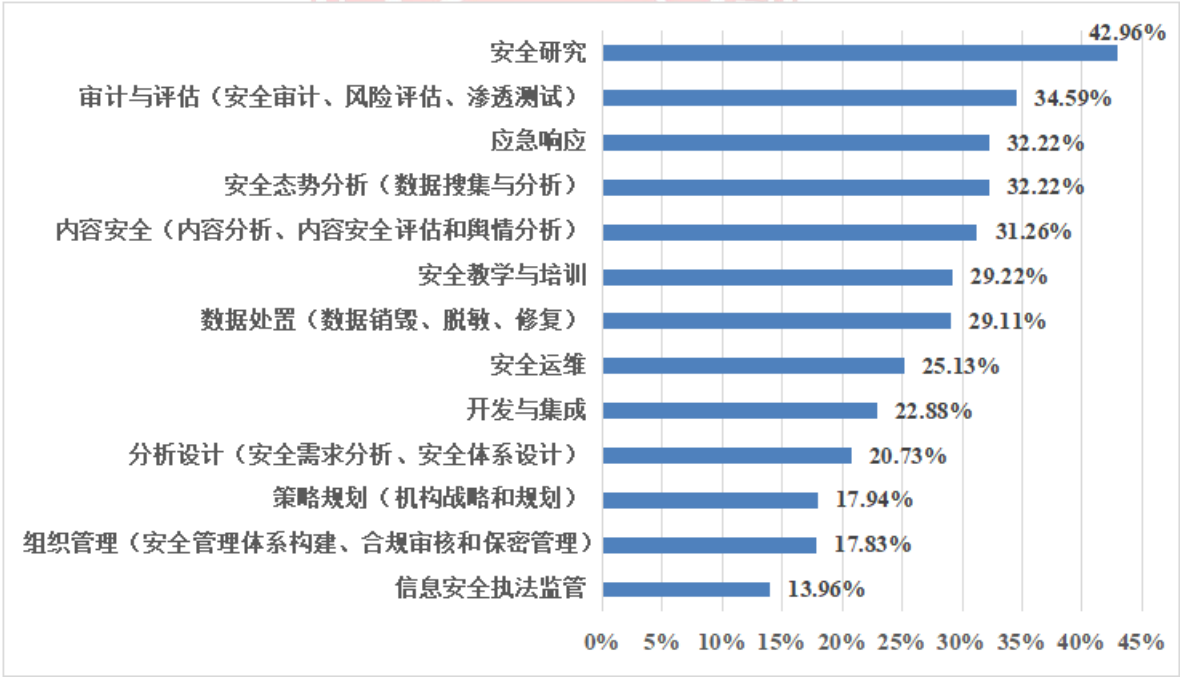


图3-3 2021年网络安全人才短缺岗位分布[11]

[11] 注：来自安恒大数据、工业和信息化部人才交流中心人才大数据中心

二、网络安全相关岗位的能力要求

随着网络安全挑战复杂程度和演变速度不断提高，用人单位对于网络安全人才的能力要求也在不断的提高。根据调查样本数据显示，网络安全从业人员认为用人单位在招聘时倾向于寻找工作经验丰富、技术基础扎实、实战能力和沟通交流能力强，同时具备一定的抗压能力的网络安全人才，学历文凭和竞赛经验相对而言，并非是用人单位特别注重的能力特质。对学历文凭相关数据进一步分析，48.35%的网络安全从业者认为从事网络信息安全岗位的平均学历水平应在本科及以上，同时也有35.82%的从业者认为平均学历水平应该视具体岗位而定，这主要是由行业特性所决定的。网络安全专业人才缺口巨大、实战能力要求高、技术针对性强等特性让网络安全行业对于学历的要求的并非如此严格，技术突出、综合素质高的大专毕业生同样也能找到一份好工作。基于此，既不可忽视学历的短板所在，同时也要进一步优化对网络安全及相关专业的人才培养方式，增加校内实践实验课程及校外的校企合作，全面提升网络安全人才的综合素质。

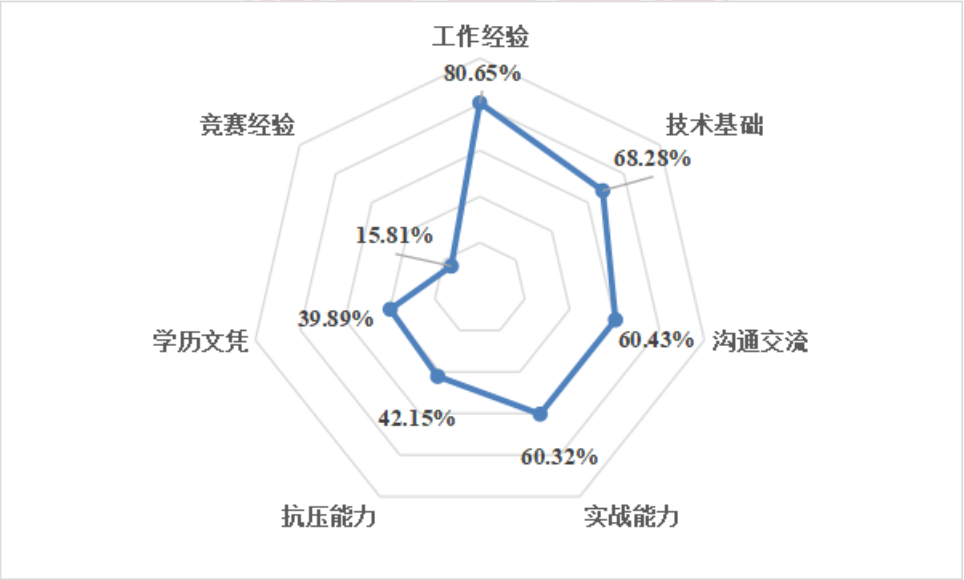


图3-4 用人单位能力要求[12]

进一步分析可知，由于岗位性质的不同，不同的信息安全岗位需要具备不同的专业技术和职业能力，但对于人格和行为特质而言，所有岗位的要求都是统一的，积极主动、认真负责、热爱学习都是每个从业者必备的特性，同时还

[12] 注：来自安恒大数据、工业和信息化部人才交流中心人才大数据中心

需具备一定的执行与管控能力、沟通与协作能力以及问题解决能力。从专业技术维度而言，研发技术岗的要求最高，对于计算机专业知识、网络安全、网络工程等相关技术与原理都需要达到熟悉及精通以上，产品岗位和销售岗位次之，其他岗位相较而言入门水平即可。

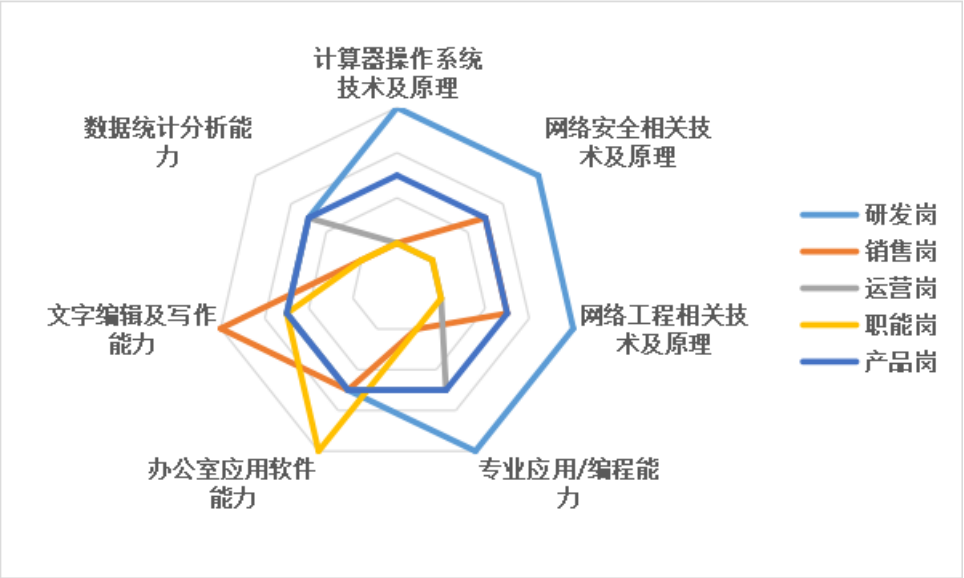


图3-5 不同岗位专业能力分布图[13]

第四节 网络安全人才能力提升需求分析

一、网络安全人才提升方式

从能力提升方式来看，60%左右的网络安全从业者都是通过积极承接并跟进项目，并不断地主动学习研究，同时工作之余参加各类考证社会培训等三种方式来提升自身的技能水平和综合素质。此外，还有部分从业者会通过参加网络安全竞赛及进校学习的方式来充实自己。

[13] 注：来自安恒大数据、工业和信息化部人才交流中心人才大数据中心

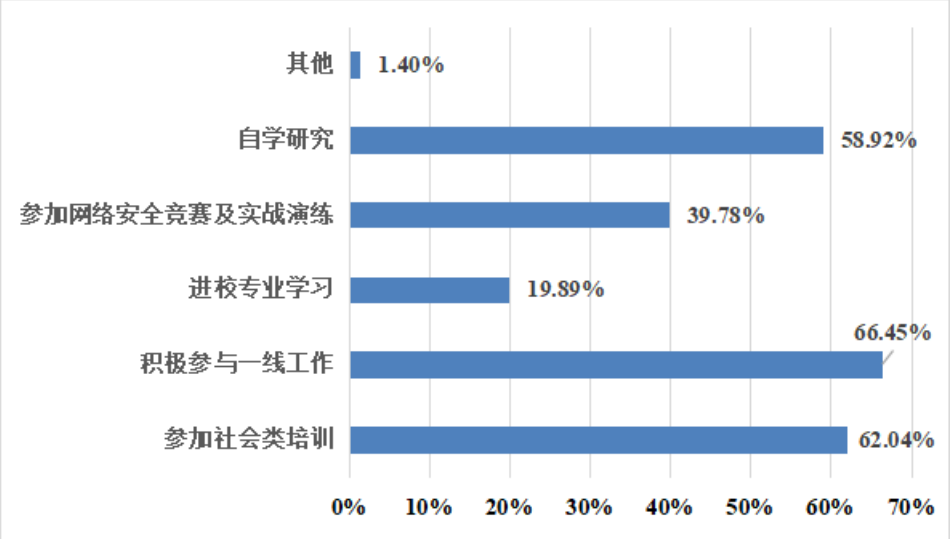


图3-6 网络安全人才能力提升方式

二、网络安全培训

从上述的数据可以看出，参加社会类的网络安全培训已经成为网络安全从业者的提升技能的主流选择之一。对于培训方向的选择上，59.25%的从业人员偏向于基础攻防技术，其次超过40%的从业者对于安全管理、安全运营和安全运维及应急响应也有较高的需求，此外实战演练、安全意识以及云大物智等新兴技术领域的安全也有一定程度的进修需求，相较而言，竞赛培训类的并非是热门选项。根据从业者对于网络安全培训（脱产）周期的可接受情况来看，近五成的人可以接受7-10天的脱产网络安全培训。基于此，企业可以定期开展不同方向的网络安全培训，满足员工能力提升需求的同时增强自身人才队伍建设。

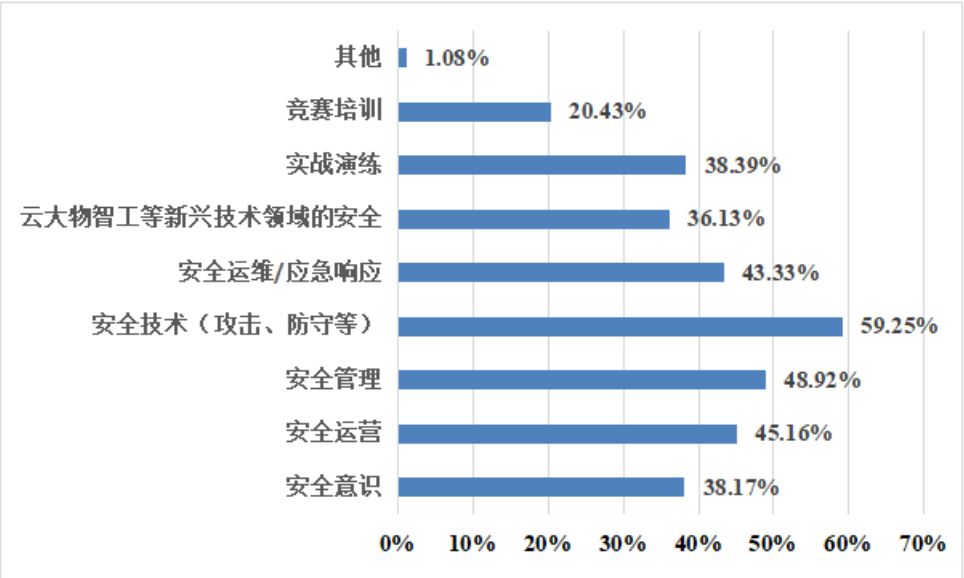


图3-7 网络安全培训方向

三、信息安全资质证书

随着网络安全领域的快速发展，信息安全专业认证已经逐步成为各行各业的对信息安全人才认定的方式，信息安全人员持证上岗已经成为大势所趋。数据调查显示，73.06%的网络安全从业者认为考取信息安全资质证书有助于提高就业率和专业能力，这主要是因为考取证书的过程就是全面学习掌握特定安全领域前沿知识和技术的过程，这就有助于提升个人在特定安全领域的竞争能力，使个人职业生涯稳步提升。

从网络安全从业者已考取的信息安全资质证书类型来看，成功考取人数最多是的证书是注册信息安全专业人员（CISP），持证人数占调查样本总数的39.57%，其次是注册信息系统安全专家（CISSP）和信息安全保障从业人员认证（CISAW），占比均超过10%，相较而言，其他几类证书考考取人数较少，这主要是受资质证书的权威性、认可程度及受众范围等因素的影响。

值得一提的是，近年来，，新一代信息技术引领的新一轮科技革命和产业变革加速兴起，制造业数字化转型加速迈进产业链的分工协作和工作岗位的设置向着细分化、垂直化、专业化发展，但社会已有的岗位证书并不能满足社会和企业需求。基于此，工业和信息化部人才交流中心2020年开始建设各行业领域的岗位人才评价体系，并推出了“工业和信息化人才岗位能力评价证书”，以此来培养适应市场需求、推动产业转型升级的创新型人才。

对于资质证书的认可度而言，认可度最高的是由国家测评中心所发布的资质证书，认可度高达75.27%，其次是由工业和信息化部、人力资源和社会保障部及中国网络安全审查技术与认证中心所发布的资质证书，认可度均在50%左右，相较而言，由厂商认证和社会职业培训机构发布的资质证书，在网络安全从业者中认可度不高。

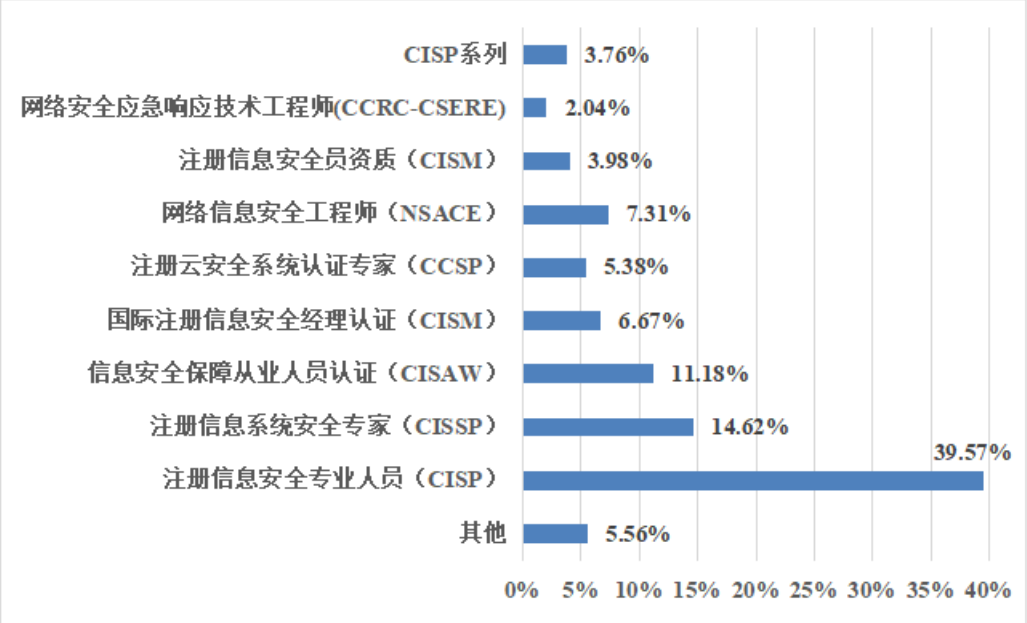


图3-8 网络安全从业者已考取安全资质证书类型[14]

随着数字化时代2.0的到来，面对日趋复杂的网络环境和威胁态势，信息与网络安全面临着更大的挑战。因此，网络安全从业者在未来更倾向于考取包含云、大、物、工的新技术领域的相关证书，借助新技术能够更加智能地洞悉信息与网络安全的态势，更加主动、弹性地应对无所不在的信息安全威胁和未知多变的风险。

[14] 注：CISP系列包括工业控制系统安全工程师（CISP-ICSSE）、大数据安全分析师（CISP-BDSA）、云安全工程师（CISP-CSE）、注册信息安全专业人员渗透测试工程师（CISP-PTE）

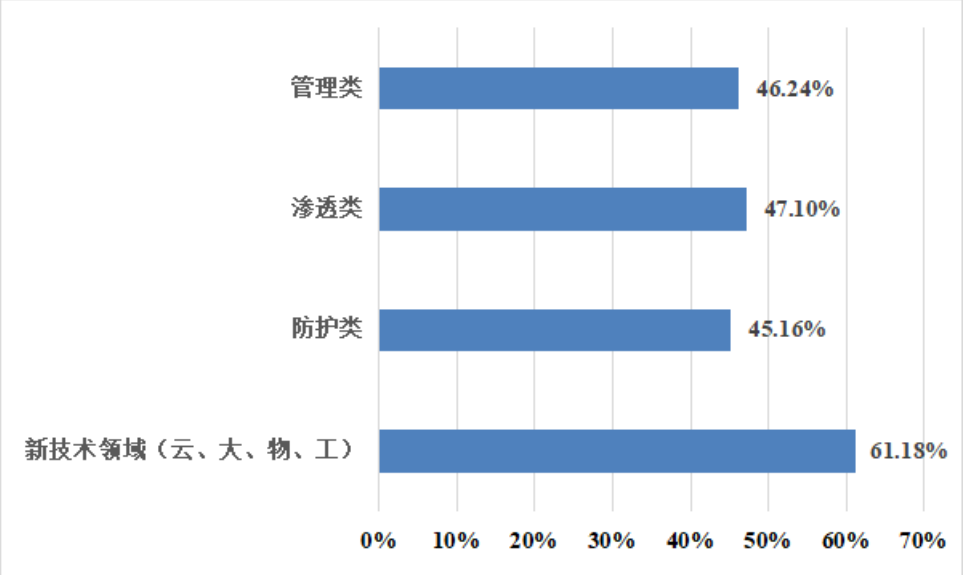


图3-9 网络安全从业者已考取安全资质证书类型

第四章 网络安全产业人才的在校供给分析

第一节 院校网络安全及相关专业人才基本情况

一、在校生对专业的认知情况

根据高等学校网络安全及相关专业人才培养现状调查发现，在校网络安全专业人才中，24.34%的学生对所在专业表示对所学专业的行业发展和就业情况了解程度一般，六成左右（62.01%）的学生对该专业比较了解，了解程度较深的学生占比在13%，剩余2.12%的学生对该专业表示不是很了解。整体来看，超七成（74.54%）的学生对所在专业了解程度较高，近三成学生对所在专业了解程度较低，一定程度上反映了在人才培养和专业建设中仍存在较大不足，可以通过加深校企合作，让企业参与到课程体系设计当中，为在校生提供专业及对口工作的了解机会。

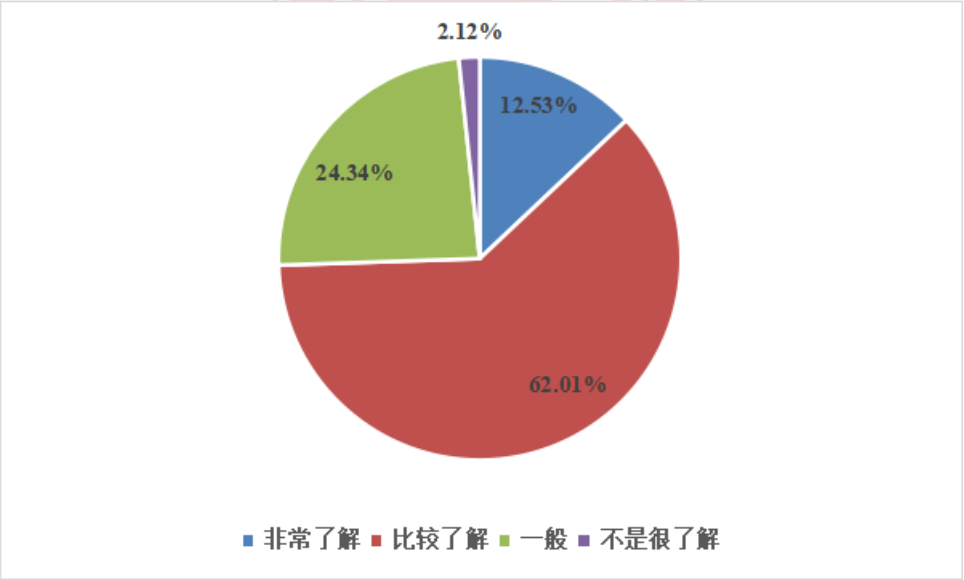


图4-1 在校生[15]对所在专业的行业认知情况[16]

二、在校生选择专业的影响因素

在受访的在校学生中，70.71%的学生表示选择专业的原因是兴趣驱动，56.90%的学生表示原因是出于对就业的考虑，16.32%的学生选择专业原因是来

[15] 以下简称在校生
[16] 注：第三章的所有数据均来自于安恒大数据、工业和信息化部人才交流中心人才大数据中心

自亲友的建议，12.13%的学生出于报录比方面的考虑选择了本专业，7.53%的学生因学校调剂而选择所在专业，4.60%的学生受其他因素影响。

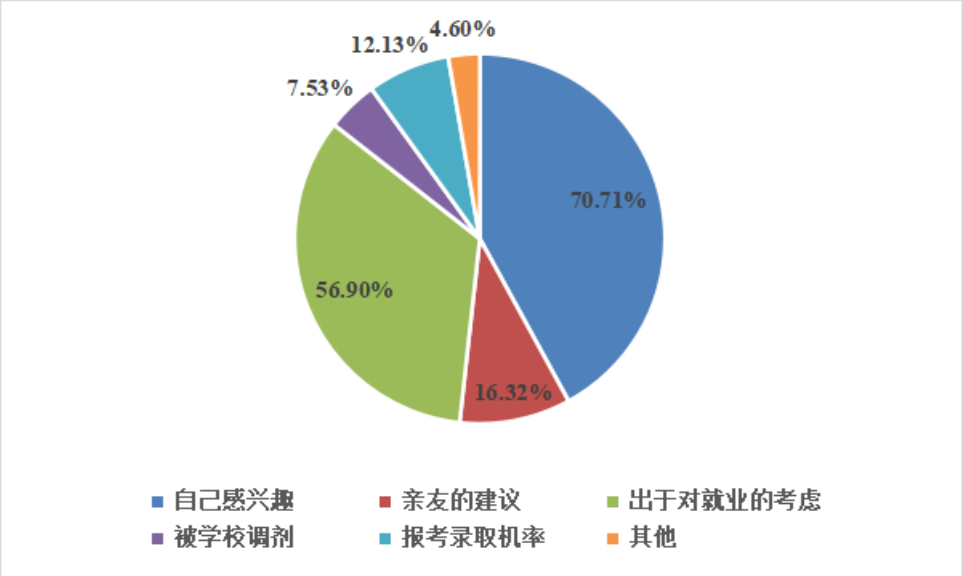


图4-2 在校生选择专业的影响因素

第二节 院校网络安全及相关专业建设情况

一、所在专业培养满意度

通过调查发现，受访学生对本专业培养情况的整体满意度较高，19.58%的学生表示对所在专业非常满意，四成（44.04%）的学生表示对本专业比较满意，但也有27.46%的学生对专业培养的满意度表示一般，对所在专业满意度较低的学生占比6.79%，也有2.13%的学生表示对本专业非常不满意。总体而言，对本专业满意度较高的学生占比不足七成，相关专业建设亟待加强。

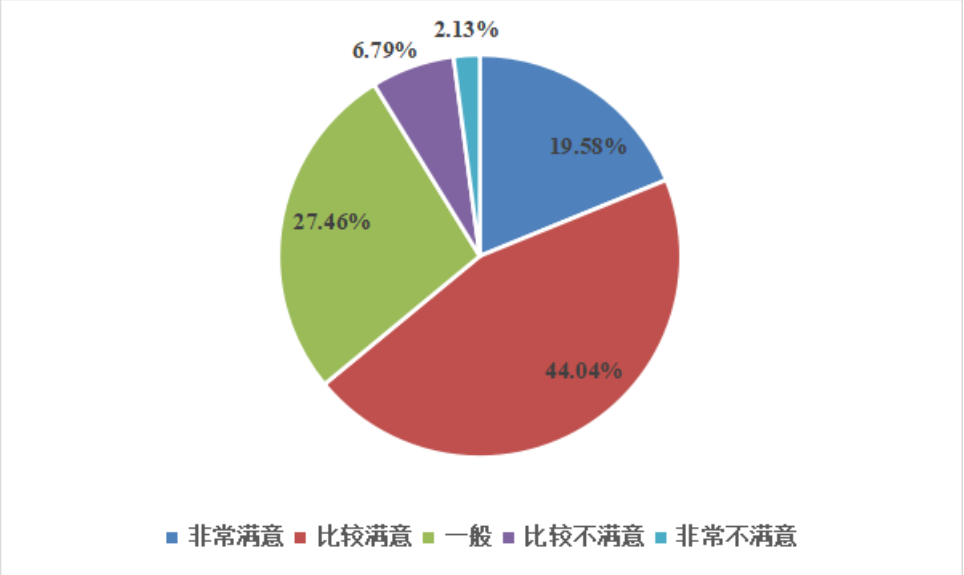


图4-3 在校生对专业培养整体满意度

二、专业课程设置满意度

在受访的在校学生中，18.60%的学生表示对专业课程设置非常满意，42.82%的学生表示对专业课程设置比较满意，28.77%的学生对专业课程设置一般满意，而8.02%的学生的态度为比较不满意，表示非常不满意的学生占比1.79%。整体来看，对本专业课程设置满意度较低的学生占比四成，人才培养方案的亟待改善。

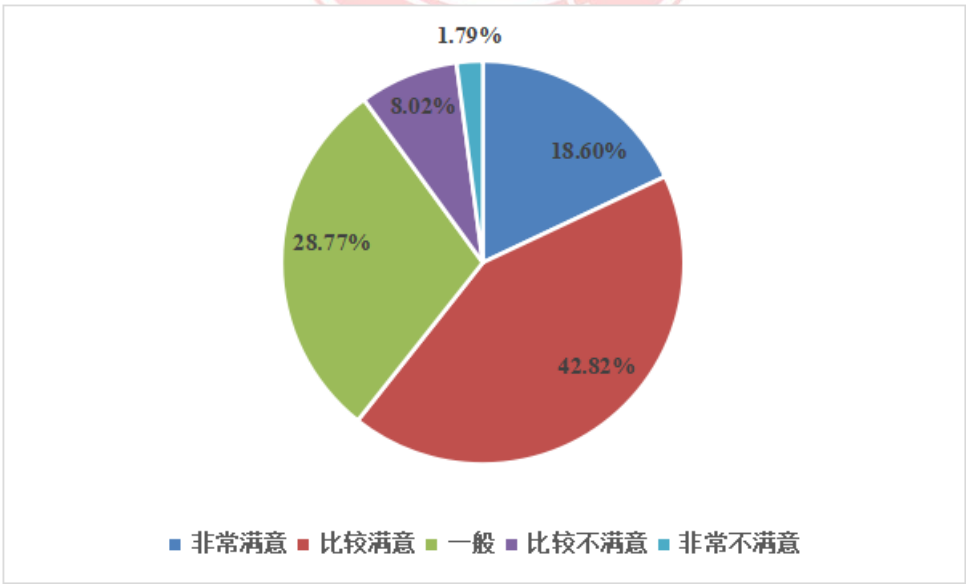


图4-4 在校生对专业课程设置满意度

三、教学设施及条件满意度

通过对各在校学生对网络安全及相关专业对教学设施及条件的调查，有如下统计结果。对本校教学设施及条件非常满意和比较满意的学生占比最多，分别达21.68%和49.95%；其次20.69%的学生认为现有教学设施及条件一般，院校需要持续改进教学条件，加强对教学设施的建设。感到非常不满意和比较不满意的学生分别占2.67%和5.01%。

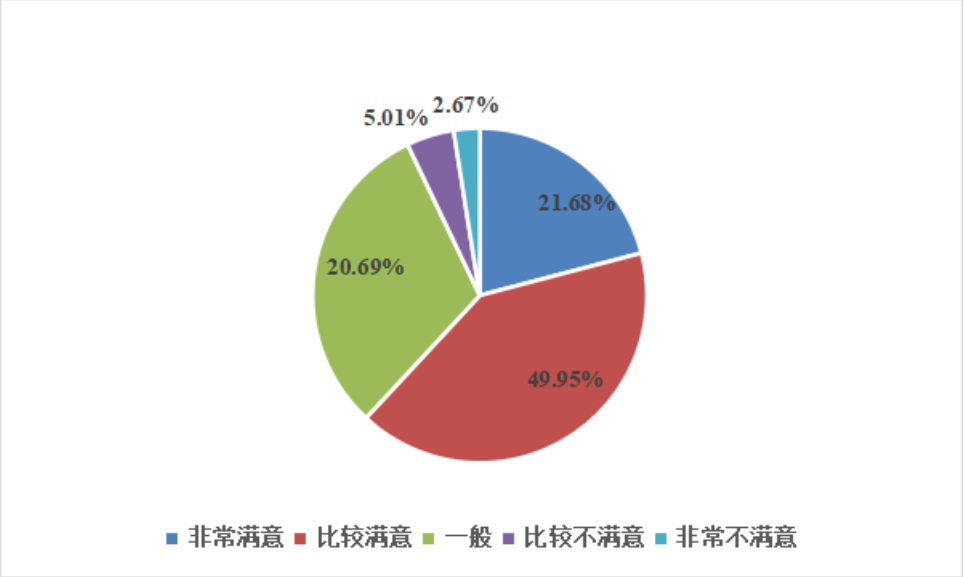


图4-5 在校生对教学设施评价情况

第三节 在校生从业规划分析

一、在校生从业期望基本特征

（一）期待就业单位性质情况

据统计样本显示，近七成（68.17%）的学生希望进入民营企业工作，15.08%的学生期待进入国营企业，有7.45%的学生对进入政府机关有较高期待，进入教科研单位是3.12%学生的选择，也有4.20%的学生选择自主创业或自由职业，受访学生中，有1.98%的学生表示跨国企业是就业选择。间接印证了第二章中所表述的央企、大型科研院所、机关直属单位不再是网络安全人才需求大户，民营企业的安全需求正在逐步提升的现状。

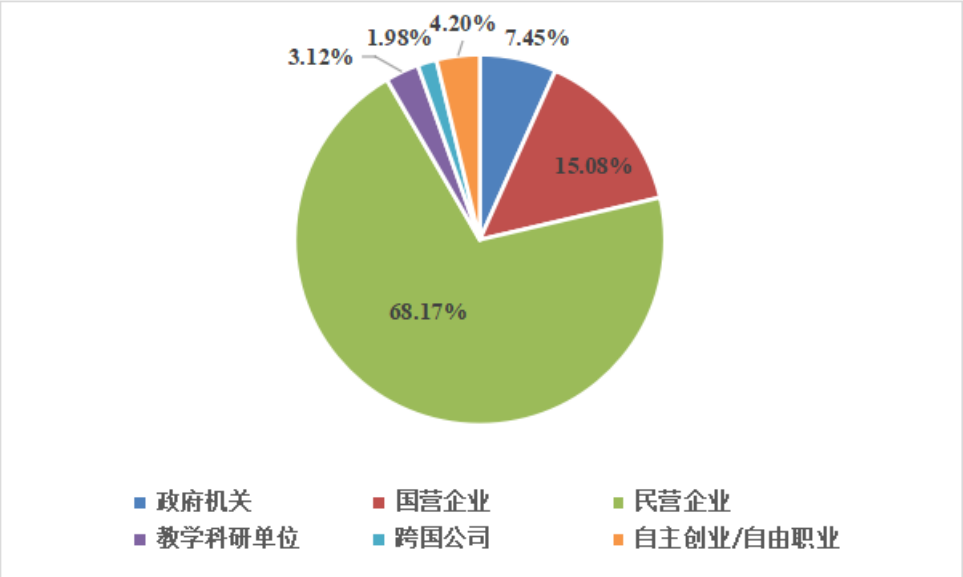


图4-6 在校生对就业单位性质期待情况

（二）专业对口期待情况

根据数据统计显示，逾八成(82.87%)的学生希望就业岗位能够与专业对口，一定程度上反映了网络安全相关专业具有就业吸引力。其中19.12%的学生认为就业岗位一定要专业对口。能接受就业岗位不对口的学生占12.80%，仅有4.33%的学生表示不希望对口，将从事自己想做的方向。

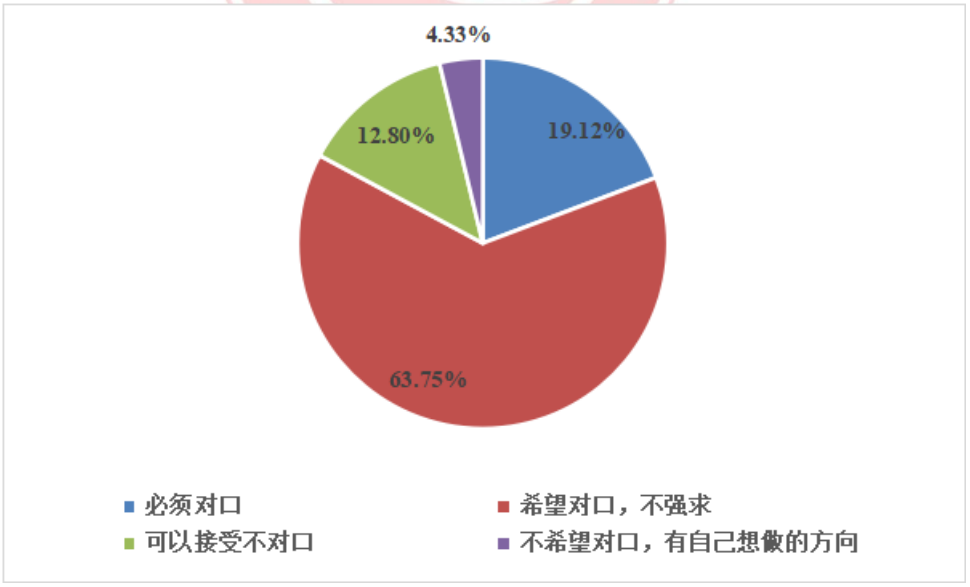


图4-7 在校生对专业对口期待情况

（三）就业城市选择情况

城市关系到行业发展、生活方式及生活质量，是学生就业时考虑的重要因素。受访学生中，近八成（79.95%）的学生首选在一线沿海城市工作，33.89%的学生希望回家乡工作。35.67%的学生希望就职于学校所在地。

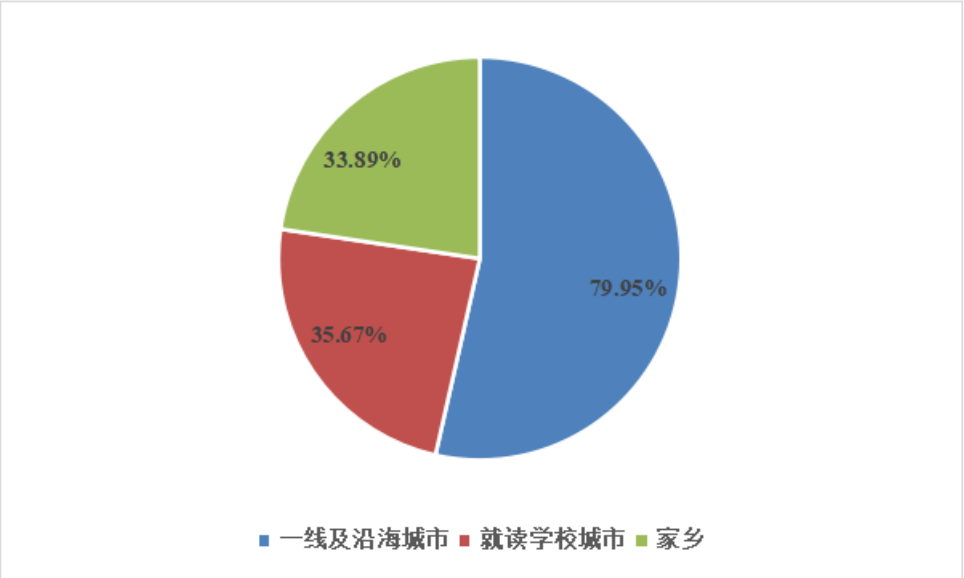


图4-8 在校生意向就业城市

（四）期望薪资水平

在国家政策大力扶持的背景下，网络安全行业就业前景形势大好，受访学生中，79.30%的学生认为，网络安全及相关专业合适的薪酬可达到9000元/月以上。有15.12%的学生认为可达到7000-9000元/月，期望薪酬在5000-7000元/月的学生占4.56%，剩余1.02%的学生认为该专业合适的薪酬在3000-5000元/月。

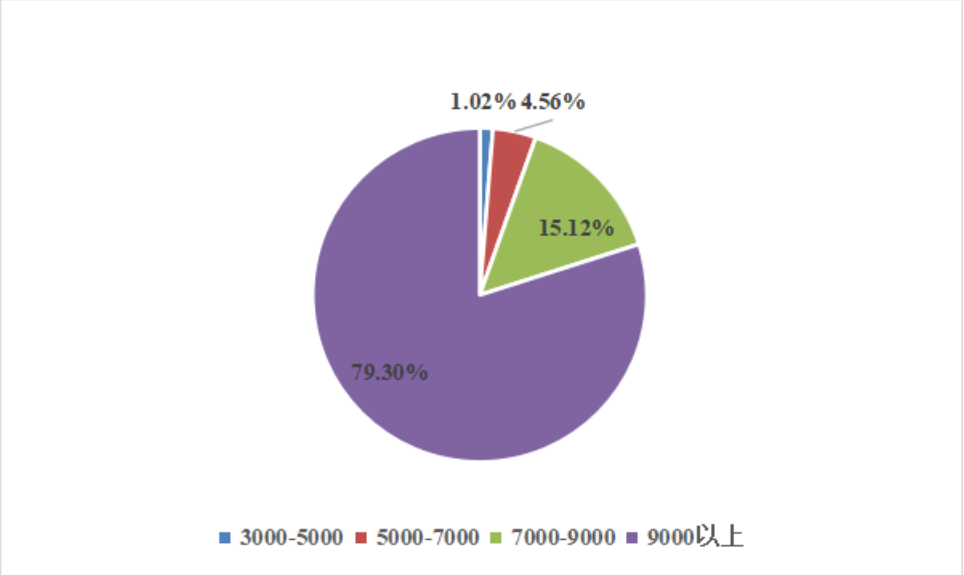


图4-9 在校生期望薪资水平

（五）意向岗位对能力需求情况

在求职过程中，受访者均表示个人竞争力由多方面组成，需将个人能力与意向岗位所需能力进行适配度分析，因此，需了解意向岗位对个人能力需求情况。据样本显示，排名前三位的是专业技能、工作经验和个人素质，其次是学历，最后为学校知名度，这与网络安全行业的专业技能要求有较高契合度。

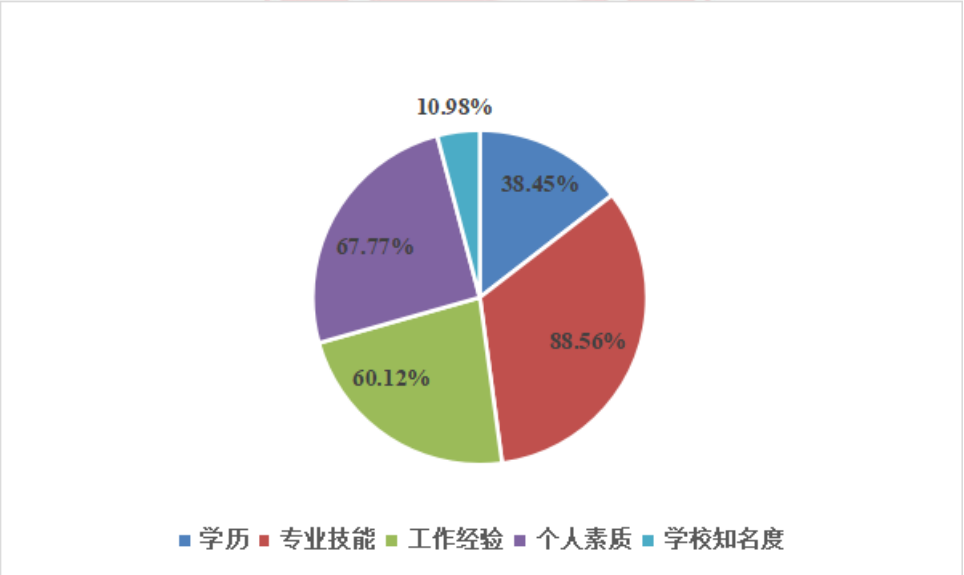


图4-10 在校生意向岗位对能力需求情况

（六）影响就业规划因素

在人才求职过程中，最看重的三项分别为薪资待遇、个人兴趣和专业对口，其中薪资待遇占比最高，达到80.75%，个人兴趣达到66.11%，专业对口达到46.03%。如行业领域和就业地区等也逐渐成为高校学生择业考虑因素的一部分。

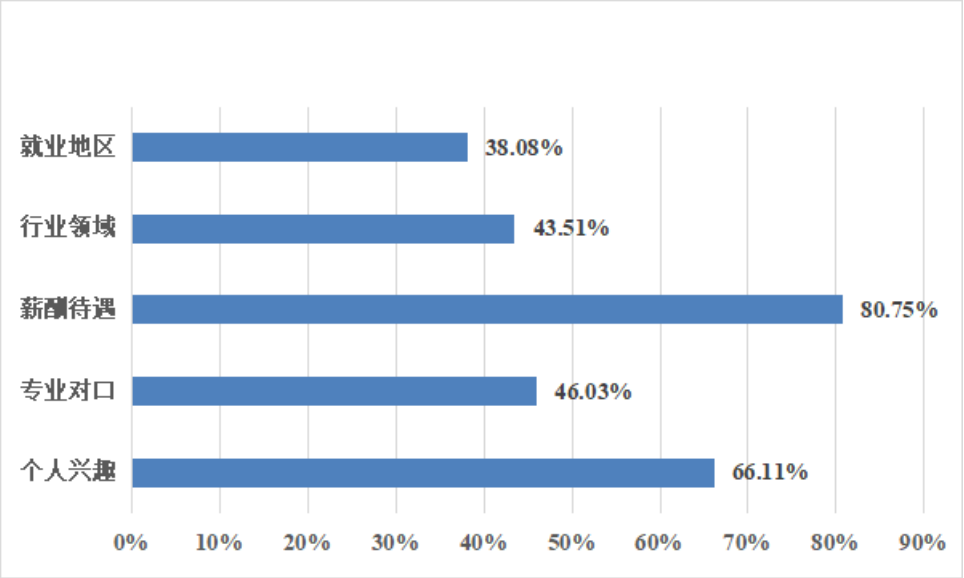


图4-11 影响在校生就业规划因素

二、在校生对网络安全行业从业期望分析

（一）就业前景展望

随着国家对网络安全及相关专业的重视程度越来越高，59.44%的学生表示对毕业前景比较乐观，27.33%的学生对就业前景非常乐观。持一般态度的学生占比15.57%，仅2.11%的学生持悲观态度。

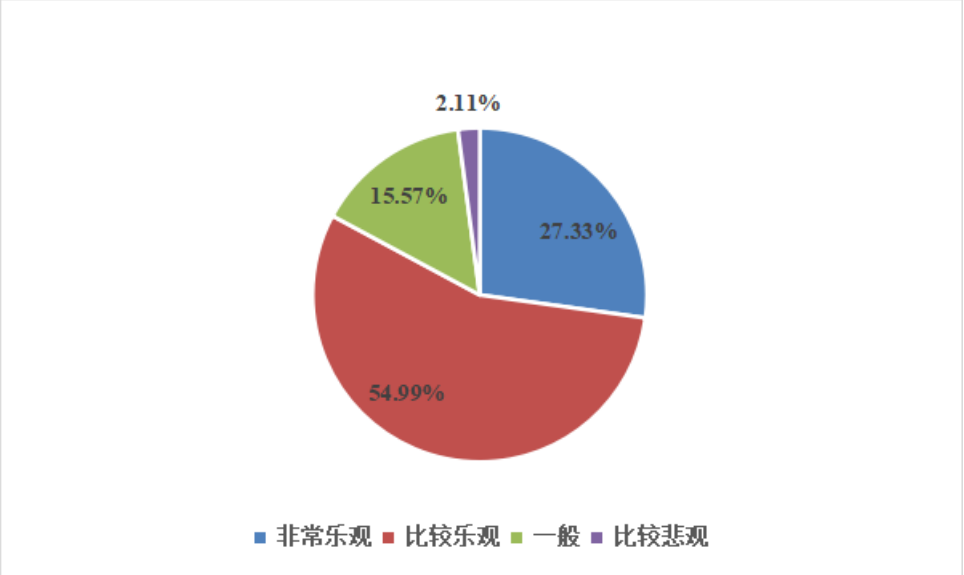


图4-12 在校生就业前景展望情况

（二）对职业要求了解程度

对目标职业要求的了解程度，关系到学生个人职业生涯规划和技能学习情况。据数据显示，受访学生中，有18.70%的学生表示对目标职业有深刻的认知和计划，56.69%的学生表示有较全面的认识和了解，而了解程度较低的学生约两成（19.92%）。

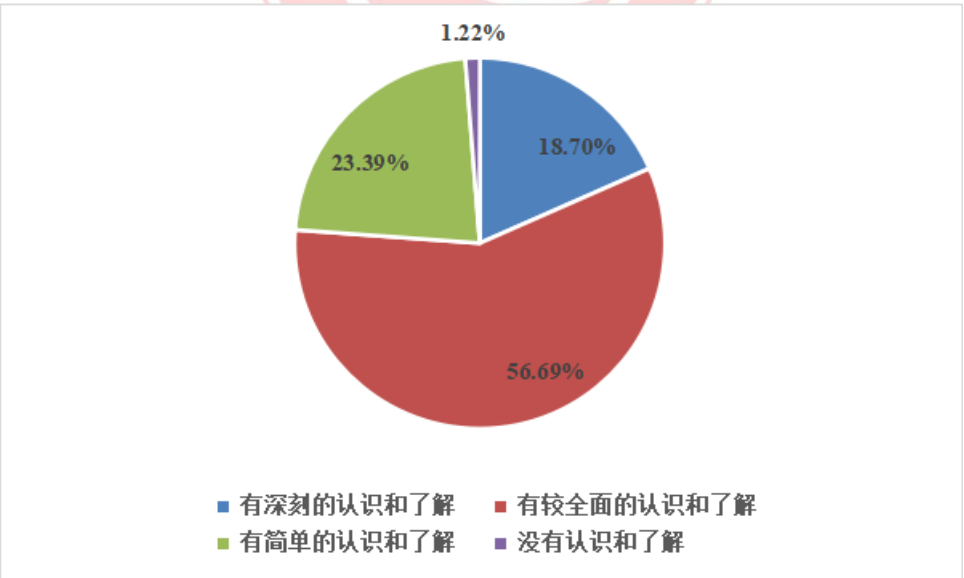


图4-13 在校生对职业要求了解程度

（三）目标就业方向

根据统计结果，29.05%的学生希望从事攻防渗透方向工作，其次是产品研发，占比20.46%，目标从事安全运维和安全运营类工作各占比12.51%，占比最少的是技术支持、应急响应和售前类工作，仅为1.77%和2.45%。

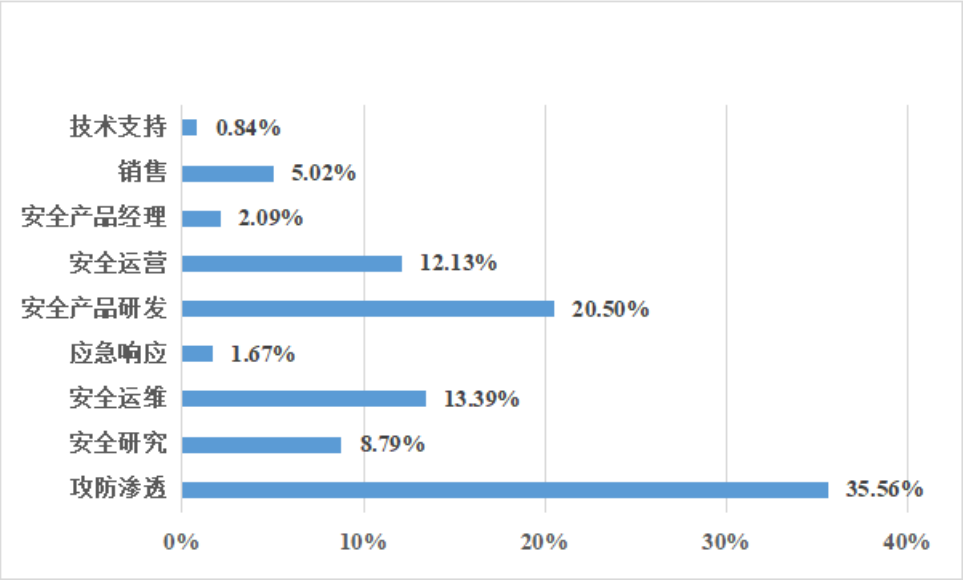


图4-14 在校生期望就业方向

（四）选择网络安全行业原因

受访学生中，选择网络安全行业原因中，最多人选择行业发展前景广阔，其次是个人兴趣，国家政策导向有利好也是学生选择网络安全行业的一大原因。这与现实情况也比较相符，伴随着网络安全在各行业渗透率提高以及网络安全行业巨大的人才缺口，让网络安全及相关专业的就业前景十分广阔。

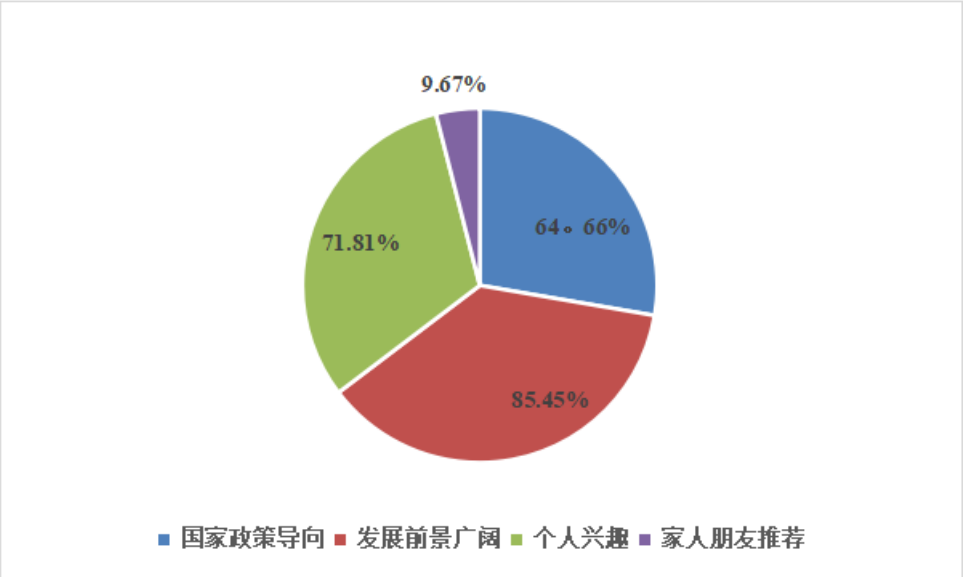


图4-15 在校生对选择网络安全行业原因

三、在校生就业需求分析

（一）就业指导与服务需求情况

学生在就业过程中，需要来自社会各方的指导与支持，在对受访学生进行调查过程中发现，多数学生对增加招聘信息、求职技巧辅导和就业政策宣讲方面的诉求最多，一定程度上反映出企业行业的招聘信息与学校存在不对称的情况。同时，学生对于求职过程中的面试技巧等也相对缺乏，侧面反映出学生的实践类活动亟待增强，需要进一步加大校企合作的力度，向学生传递真实的专业介绍和岗位能力要求。

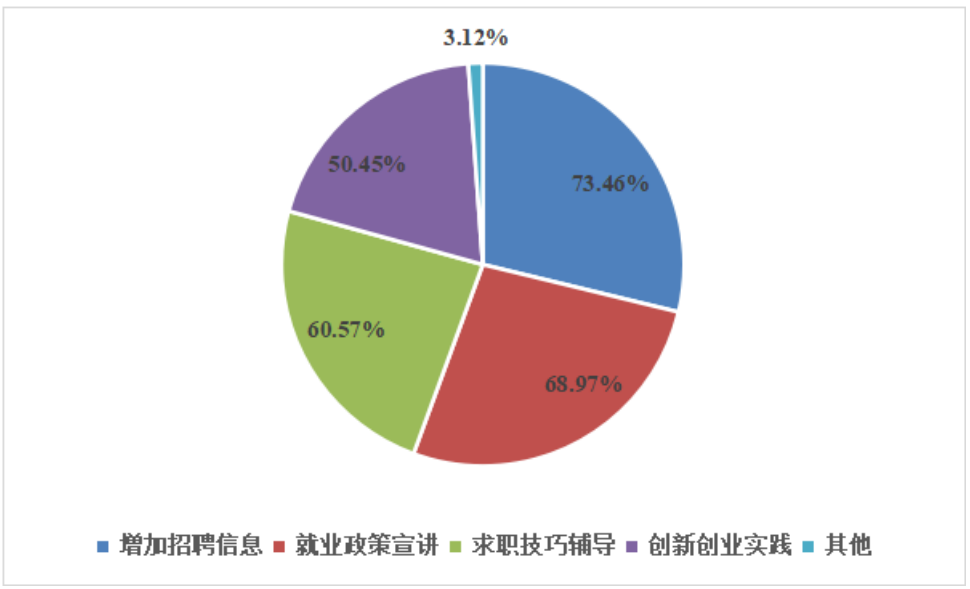


图4-16 在校生对就业指导与服务需求情况

（二）期望企业提供就业帮助的需求

根据样本数据，受访学生中大多数学生在校企合作共建实训基地、提供实习机会方面有较高期待，这也为未来企业招聘与学生就业的双向合作提供改进方向。也有半数以上（53.72%、52.61%）的学生希望企业实训教师能够进入学校上课以及希望企业能够举办专业技能培训班。

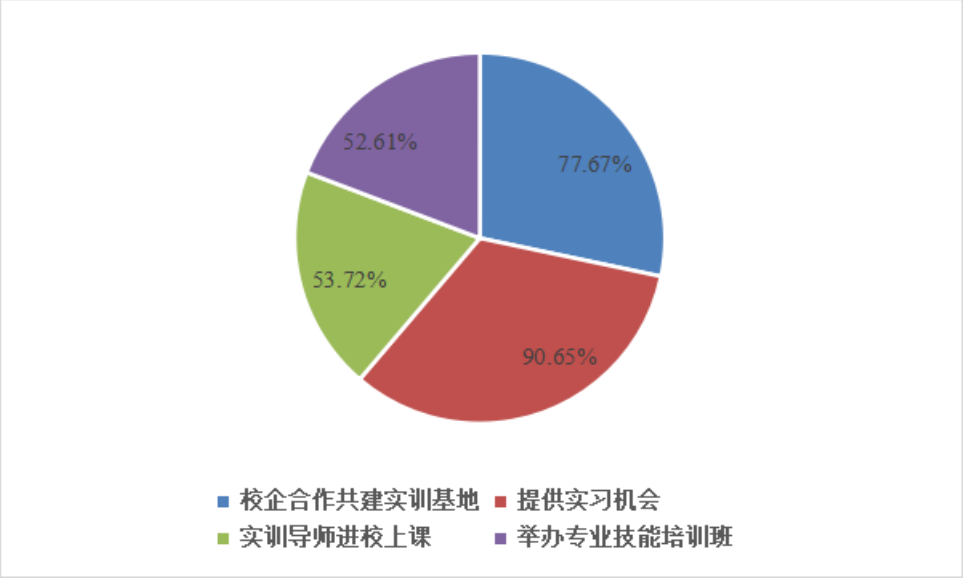


图4-17 在校生对企业提供就业帮助的需求情况

同时，对学生进行了企业培训需求度统计，57.71%的学生表示比较愿意，非常愿意参加企业培训的学生占比34.57%，也有12.60%的学生表示不愿意参加。总体而言，学生对于企业培训需求意向较高。

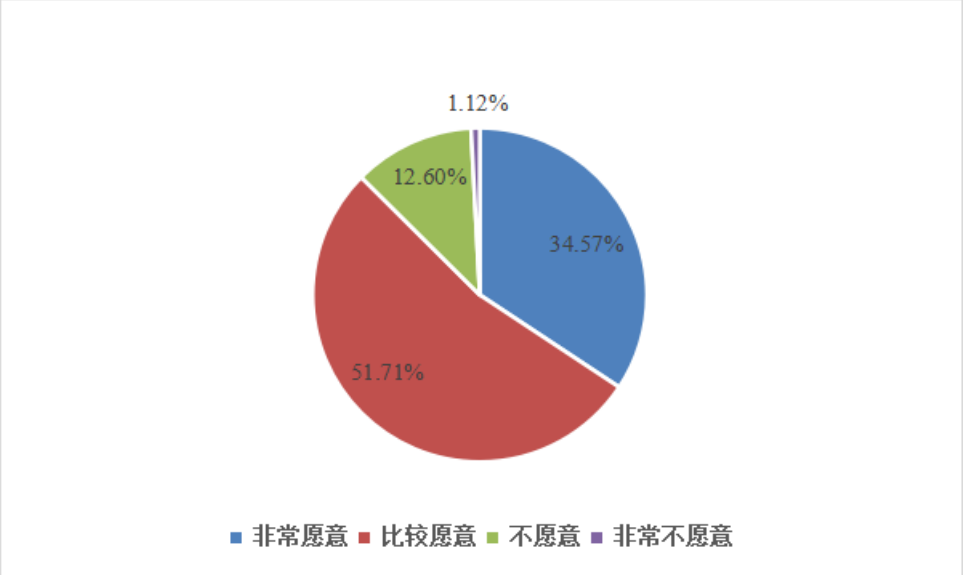


图4-18 在校生对企业培训需求度

（三）求职途径统计情况

据统计结果，校园招聘会、学校招聘信息、老师或校友推荐三种途径占比学生总求职途径最高，分别为74.14%、64.35%和57.37%。其次，招聘网站作为一种重要的求职渠道，占比总求职途径的54.25%。

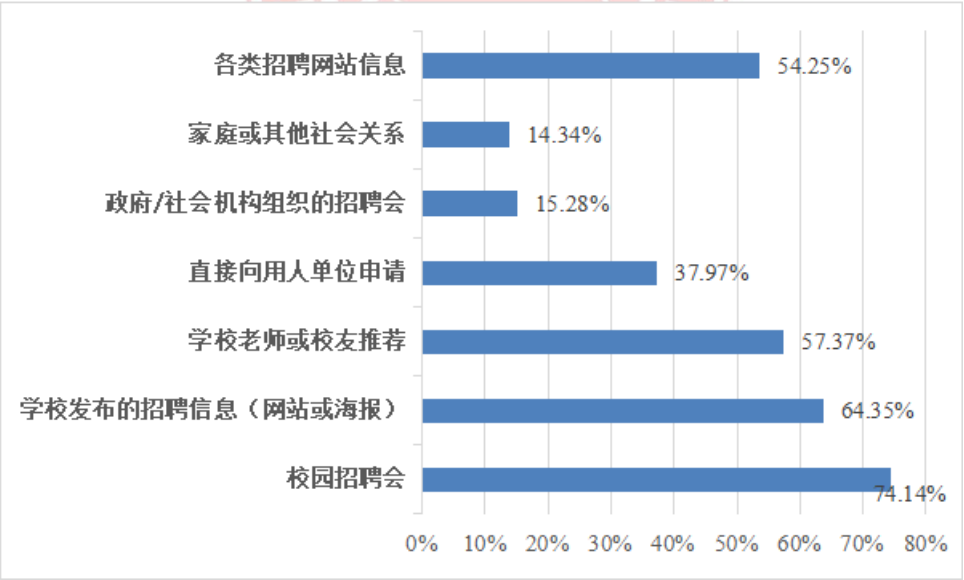


图4-19 在校生求职途径统计

四、在校生网络安全相关证书考取情况

（一）网络安全相关证书了解情况

网络安全行业作为对技术技能要求较高的行业，有一定入职门槛，从业人员需不断提升个人技术技能，并考取相关证书[17]以获得资质。从样本数据来看，近七成（67.66%）的学生对网络安全相关证书较了解，但仅11.58%的学生考取了相关证书，而32.34%的学生并不了解行业相关证书的情况。

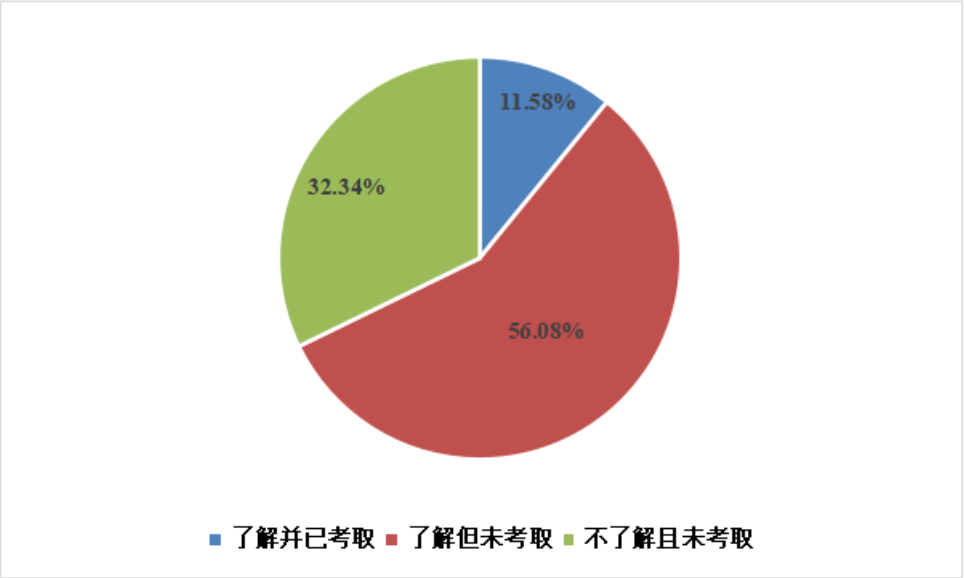


图4-20 在校生网络安全相关证书考取情况

（二）相关证书对就业帮助程度

根据样本数据，绝大多数（90.63%）学生认为考取相关证书对就业是有帮助的，其中33.28%的学生认为考取证书对就业非常有帮助，也有4.12%的学生认为没有帮助，剩余5.05%的学生表示并不了解。这一定程度上反映出从业门槛和企业招聘要求的条件在证书中有一定体现。

[17] 注：如CCRC-CSERE、CISP-PTE等

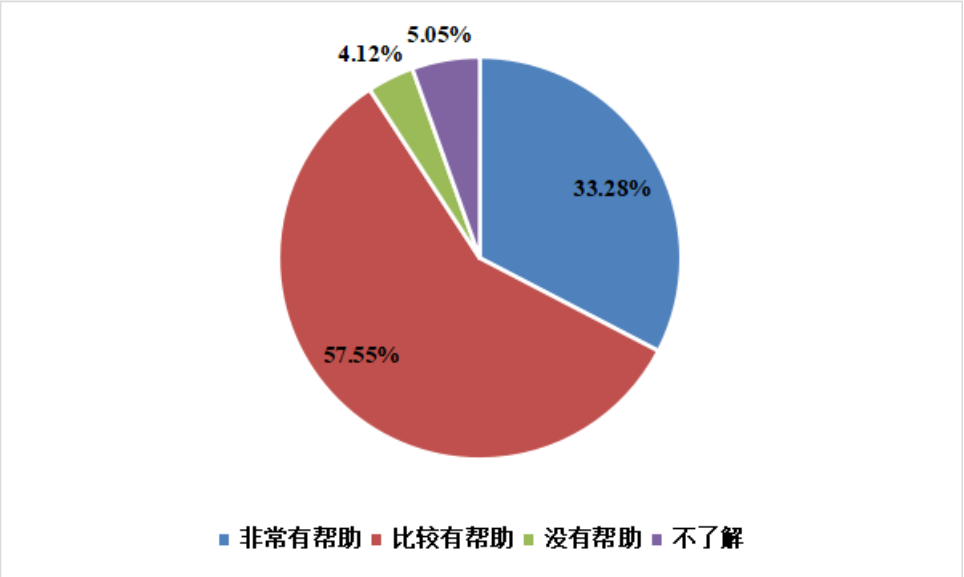


图4-21 相关证书对就业帮助程度

从基本情况来看，网络安全及相关专业人才的性别比例差距依旧明显，男性占比更多；受访学生对专业了解程度总体较高。从专业建设情况来看，多数学生对包括课程设置、教学设施等专业培养相关内容较为满意，但仍存在较大基数需改进之处。从就业规划角度而言，呈现出学生对行业兴趣浓厚，就业热情高涨的态势，选择城市依旧以一线沿海地区为主。同时，调查也显示出本行业招聘信息与院校之间存在一定信息差，企业对于就业学生的帮助可在多提供实习机会、加强与院校合作及提供培训等方面进行。

第五章 网络安全产业人才的在岗供给分析

第一节 网络安全从业人员择业分析

一、职业规划

根据问卷调查显示，网络安全行业从业者超半数在校期间对自己的职业发展有规划，其中有超四分之一人员对自己有非常明确的规划，也有四分之一的人员表示在校期间不太明确自己的职业发展规划。此外，网络安全行业从业者超半数认为职业发展符合在校期间的规划，表明网络安全行业的就业针对性较强，同时结合薪资可以看出，在校期间对于自己有明确职业规划的人中，目前有73.13%的从业者年薪超过了30万，表明职业规划对于未来的就业有一定的帮助。

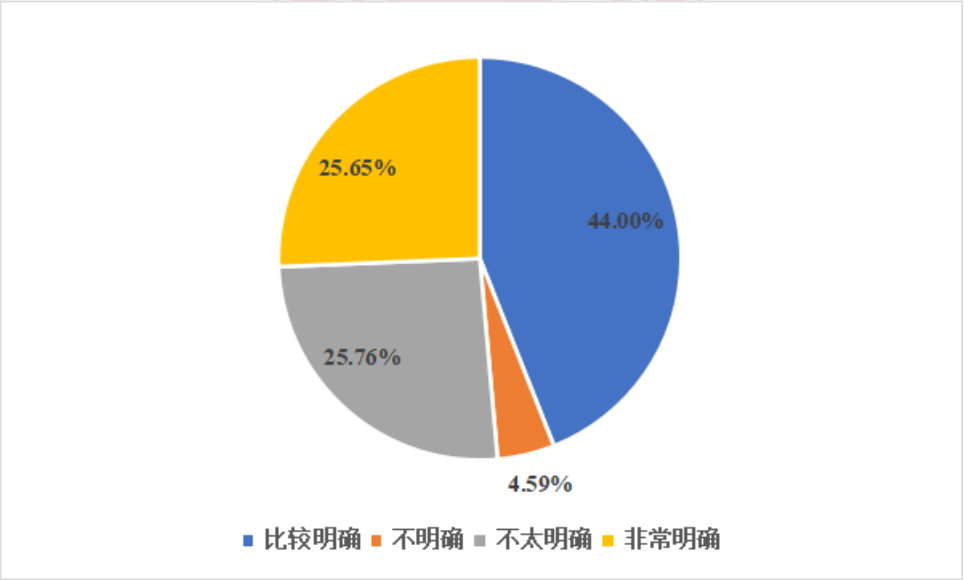


图5-1 网络安全从业者在校期间的职业规划[18]

[18] 注：第四章所有数据均来自安恒大数据、工业和信息化部人才交流中心人才大数据中心

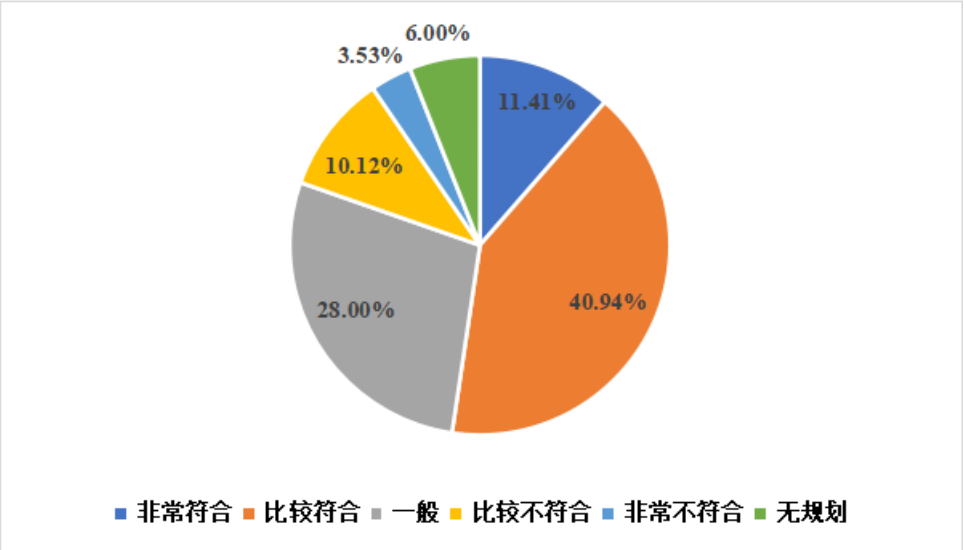


图5-2 网络安全从业者的职业发展现状与在校规划吻合情况

二、网络安全从业人员择业的首要因素

在选择行业时，如第三章所示，待遇薪酬、个人兴趣、专业对口等是在校生最为看重的择业因素，但是从学校进入社会后，发现从业人员在择业过程考虑的因素会更为广泛和全面，首要考虑的影响因素是职业发展前景，为29.41%，其次是兴趣爱好，相较于在校生而言，从业人员占比下降明显，为27.14%。同比往年数据发现，从业人员在择业时越来越重视个人兴趣爱好以及自我价值的实现，其择业观的转变是从业者对自我的重视以及对网络安全行业的发展前景的认可。

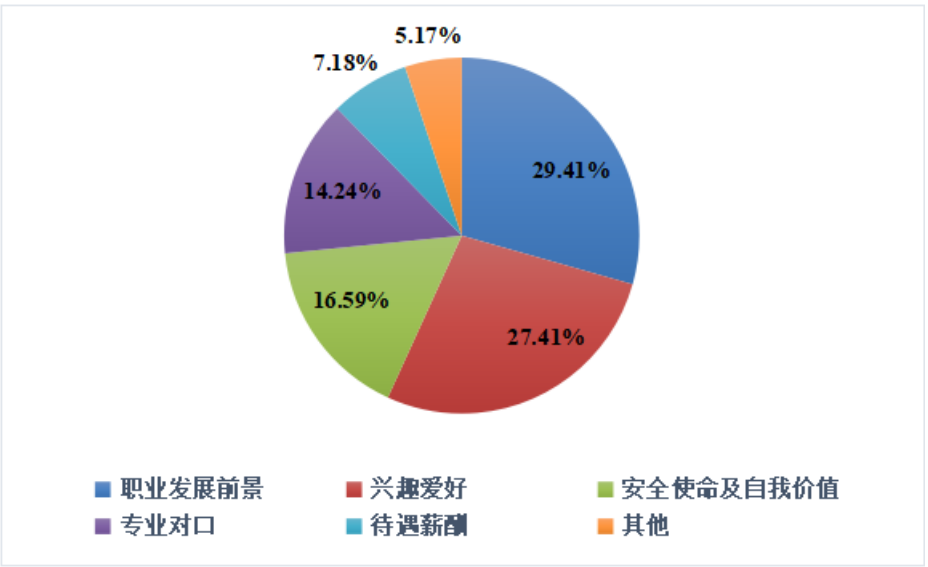


图5-3 网络安全从业人员择业的首要因素

三、网络安全从业人员择业渠道

数据显示，网络安全从业者在择业时，超半数倾向于通过朋友推荐交流方式以及各类招聘网站去寻找合适的工作岗位，直接向用人单位申请的人员占比也较高，达到了40.82%，这也侧面印证了第一章中高端人才平均薪资高于行业平均工资的原因。

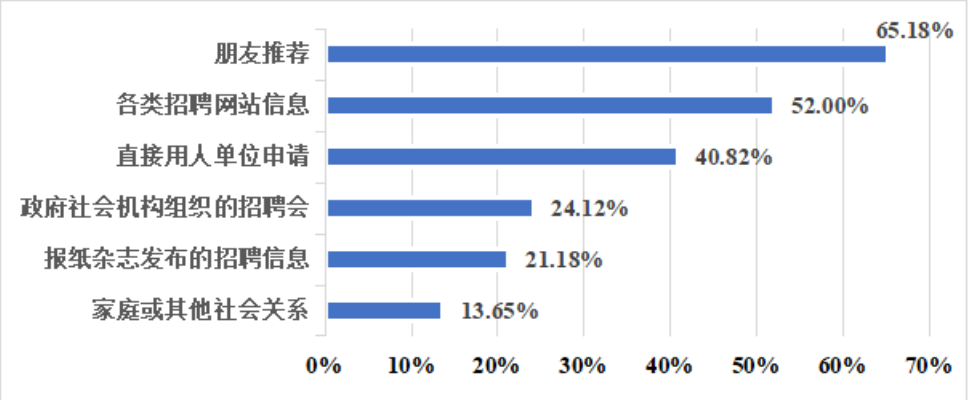


图5-4 网络安全从业人员择业渠道

第二节 网络安全从业人员工作现状

一、网络安全从业人员工作压力及满意度

问卷数据显示，近七成从业人员对目前工作表示有压力，15.88%人员认为目前工作非常有压力，仅7.29%的从业人员对目前工作表示轻松，表明随着网络安全行业的快速发展，工作内容和工作压力也在随之增加。

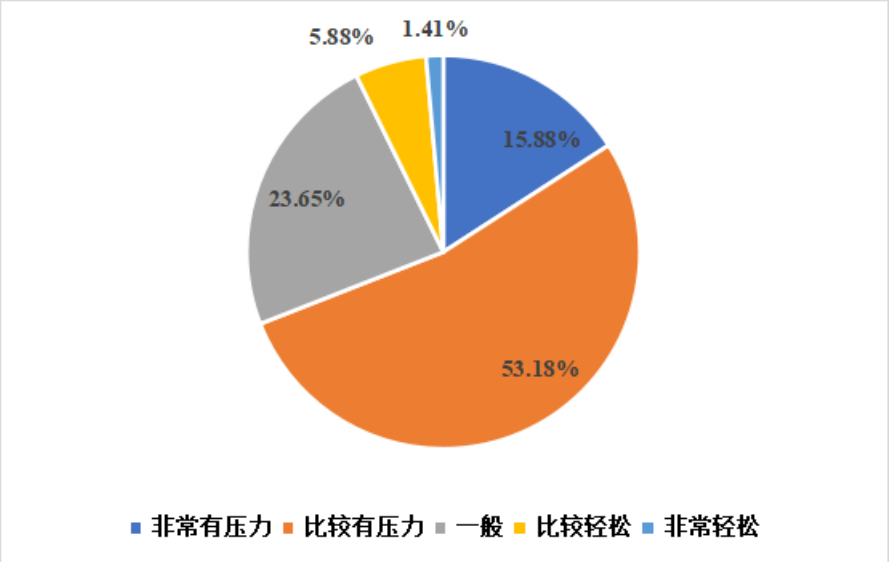


图5-5 网落安全从业人员的工作压力

与之相对应的是，绝大多数（近95%）网络安全从业者都对工作表示满意，不满意人员仅占5.06%，结合网络安全从业者满意程度及工作压力调研分析可见，近七成人员认为所处工作有压力，但绝大多数对自己工作表示满意，可见目前网络安全行业人员能在工作中获得成就感和满足，并正向反馈压力，将压力转化为动力进行良性发展。

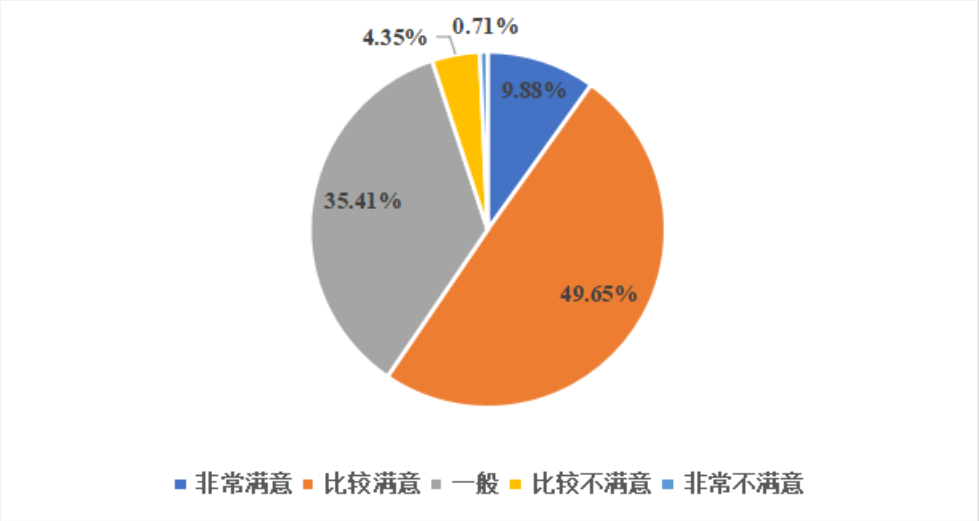


图5-6 网络安全从业人员的工作压力

二、管理制度建立及实施效果

制定完善规章制度，建立员工职业发展通道，对于用人单位而言，具有重要意义，不仅可以建立健康而良好管理秩序，同时能够牵引员工不断自我学习和提升，推动用人单位的可持续发展。四分之一左右网络安全从业者表示公司有建立相应完善的人力资源发展规划和晋升机制，并且效果显著；超六成的从业者认为虽然公司有设立相应的制度管理机制，但在具体实施管理上并不理想，还有14.47%的网络安全从业者表示用人单位并无相应管理制度，可见社会对网络安全从业人员的重视程度还有较大提升空间，用人单位需要进一步加强制度建设和福利保障。

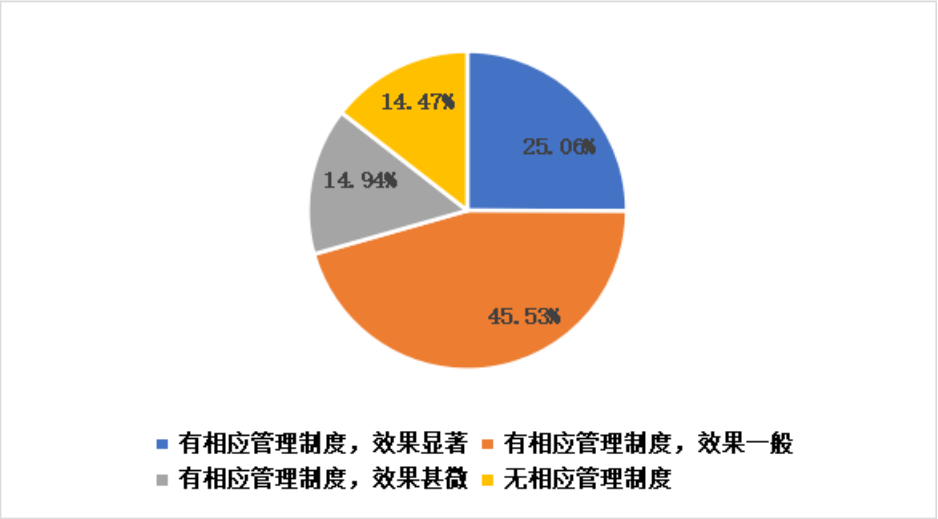


图5-7 用人单位管理制度及实施效果

第三节 网络安全人才流动分析

随着时代的发展和社会的进步，“铁饭碗”的概念正变得陌生，人才流动在所有行业中也变得愈发频繁。结合以往数据和调查问卷发现，2019年网络安全人才的平均跳槽周期为30.56个月，时隔两年，已缩短至17.69个月，与互联网科技企业的人才流动频率相接近。进一步分析发现，职场中25岁以下的年轻人跳槽相对频繁，31.25%的年轻从业者跳槽周期仅为半年，35岁以上的从业者工作稳定性比较高，六成以上的从业者都能在同一家企业工作1-3年。

对于人才流动，薪资待遇、发展晋升和能力提升成为从业者跳槽的主要影响因素。其中，78.94%的从业者认为薪资待遇是导致其跳槽的主要影响因素，其次是个人的晋升前景和能力提升，相较而言，企业规模和行业前景并不在多数人择跳槽考虑范围之内。

虽然人才大规模快速流动带来的技术外溢效应，能够带动行业的快速发展，但对于个体来说，必须要通过一定时间的积累，才能获得个人价值的实质性增长。

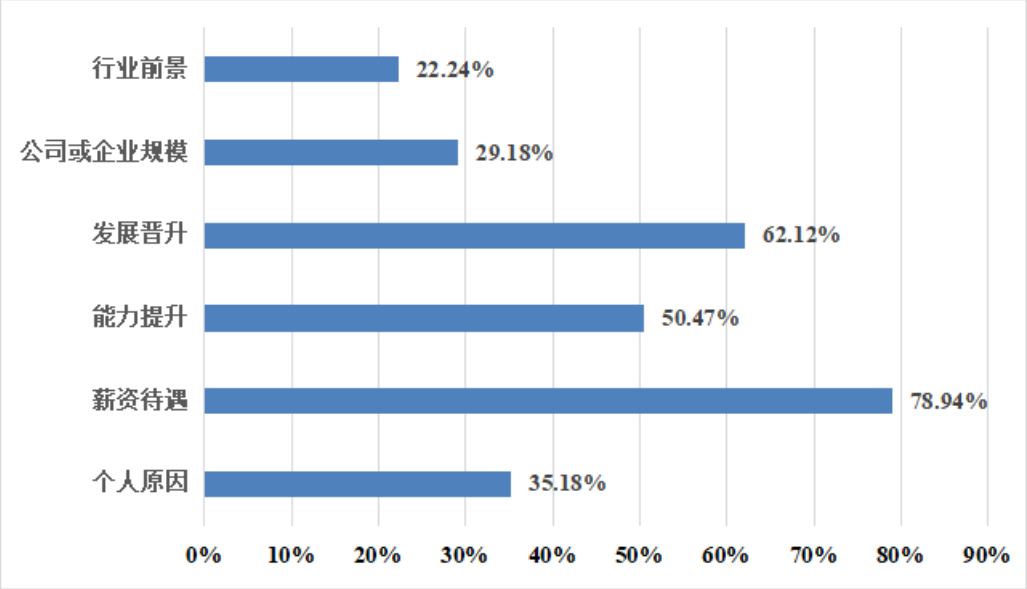


图5-8 网络安全人才流动原因

第六章 网络安全产业人才的发展建议

网络安全作为一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性新兴学科，知识和技术发展迅速，且具有较强的后伴生性和学科交叉特质，因此，专业人才培养难度大，路径复杂且周期长。随着信息技术和各行业的深度融合，网络空间安全与国家安全、社会稳定和公共利益越发相关，各国也将人才队伍建设列为网络空间安全战略的重要举措和保障，在网络安全人才培养方面投入了大量精力。比如欧盟发布的*Cybersecurity Skills Development In The EU*白皮书，对全球主要经济体的网络安全人才现状、缺口和发展情况做了较为详尽的阐述。本章针对上述各国在网络安全人才培养过程中的知识体系建设和人员认证认可方面进行简要阐述，以“他山之石，可以攻玉”的视角，结合我国的网络安全人才培养现状，对网络安全人才队伍建设方面的工作提出建议，希望能够为网络安全人才培养相关的多方主体提供启发和借鉴。

首先，无论是国家安全战略落实角度还是促进网络安全产业发展角度，从上述欧美国家的网络安全人才培养发展情况来看，对我国的网络安全人才培养给予深刻的启示，我们应该做好社会全覆盖的网络安全人才发展顶层设计、政策供给和机制保障。切实开展全民数字素养和网络安全意识提升行动，落实国家安全教育规划中的网络安全进校园政策，通过完善的职业教育、学历教育专业布局和人才培养模式改革，到岗位能力认证标准和要求，建立一个导向和分工明确，指导和保障有力，方法和标准先进的网络安全人才发展体系。

其次，网络安全行业的人才队伍建设涵盖在校生的教育和从业人员能力提升两个阶段，再结合不同的工作岗位和垂直行业，是一项系统工程，也是一个以终身学习为导向的持续过程，涉及政府和主管部门、院校和培训机构等实施主体、教育和培训对象等多个角色协同参与。因此，如何构建一个多元融合协同创新的培养体系是值得深入研究的课题，本文只针对这一过程中涉及到的主要角色提供重点建议。

● 政府和主管部门

中央网信办、教育部、工业和信息化部等主管部门近几年陆续出台的相关

意见和规划中均对网络安全人才培养提供了较完备的政策指引，但具体落实过程中仍缺少可操作性强的政策和实施办法，一方面应结合国家推动的院校教学改革和质量提升计划、产教融合试点城市、试点企业等政策，加大落实力度，完善保障机制；另一方面，完善顶层设计，推动建设一批高质量的实践教学基地、共享式实训基地和产学合作基地，释放行业实训实践资源，切实为在校生实践教学提供实战机会。

● **网络安全产业研究和人才服务机构**

深化产教融合协同育人，推动开展网络安全产业人才岗位能力要求标准制定，并依此拓展完善网络安全产业人才能力评价体系，组织产学研各界共同编制网络安全产业人才能力评价测试大纲及题库。探索建设网络安全产业人才发展创新中心，畅通网络安全产业人才发展路径，进一步发挥网络安全产业人才岗位能力评价要求的指挥棒作用。鼓励企业、高校、科研机构、人才服务机构等通过多种方式健全领军人才激励机制，通过建设网络安全产业人才大数据中心加强人才数据解析，加强高水平国际交流合作，组织开展网络安全创新创业大赛等活动，以产业需求为牵引，培养选拔网络安全专业人才。

● **教育培训实施主体**

无论是以能力产出为导向的OBE教学模式，还是岗位能力胜任评估标准，都强调学有所会，学有所用，知行合一，理实结合，但这一过程需要切实有效的评估方法和评估工具，也需要教育培训主体在师资队伍建设、教学资源建设、人才培养模式改革等方面加大投入。在无法对政策、机制和体制进行改革的情况下，院校人才培养也可在明确的办学定位指导下，摸清行业用人需求，整合各方资源，加大实践教学投入，构建完善的课内课外结合、线上线下融合、校内校外契合的实践能力养成体系，同时将法律法规和职业道德教育融入每一门课程，将安全理念和安全意识融入每一门专业课；而教培机构则需要构建以实际能效评估和业务能力提升为导向的竞赛选拔、培训交流和实战演练多种模式结合的持续性能力提升过程，避免填鸭式、一成不变式的重复服务。

● **相关专业在校生**

对于在校生而言，要脚踏实地，打好专业基础，积极参与假期实践，从而尽早的完成较清晰的职业规划。从事科学研究、基础研发、安全服务和安全运

维等不同工作岗位，对基础素质、综合能力和专业技术均有不同的要求，多数用人单位选拔的是知识结构优化，基础能力扎实的，值得继续培养的人才，实践经验固然重要，基础知识也将决定能力天花板的高底，多参加社团活动和学科竞赛是切实可行的能力提升渠道。

- **从业人员**

积极考取相关认证，重视学习过程，取得认证和知识融通并不矛盾，同时，加强系统性和工程性思维的养成，培养抽象和结构化能力，积极参与各类管理和技术交流活动和行业论坛，有计划的补充基础知识和了解新领域知识，对国家和行业相关法律法规和标准进行深入研究和思考，并紧密的与自身工作结合，养成终身学习的习惯。

- **用人单位**

加大网络安全人才队伍建设方面的投入，周期性开展可持续的培训、竞赛、演练、交流和评估活动，强调以业务能力提升为导向的人才队伍建设体系，建立和完善多层次化的网络安全人员职业路径规划和考核方法，并为上述工作提升经费保障。