学士学位授权授予出新规:

不再招收第二学士学位生 新设三种学士学位类型

《光明日报》 邓晖

从今年7月起,我国学位授予单位不再招收第二学士学位生。此外,为确保学位证书的权威性,对获得多个学士学位的学生都只发一个证书,所获各类学位情况在证书上予以注明——记者7月27日获悉,为规范学士学位授权授予工作,健全学士学位管理制度,提高学士学位授予质量,国务院学位委员会发布《学士学位授权与授予管理办法》。除上述变化外,《办法》还明确了学士学位授权审核的权责,提出了标准和程序等相关要求,并对中外合作办学中学士学位授予问题和第二学士学位作出规定。

"新中国学士学位制度建立近40年来,较好地满足了高等教育快速发展的需要。但随着本科教育规模不断扩大,也产生一些新问题,如部分学士学位授权审核不规范、制度设计对复合型人才培养支持不足、学位授予质量监管处置有空白等。"国务院学位委员会办公室负责人向记者表示,该《办法》设置三年过渡期,过渡期期间,高校按原有政策执行,2022年起所有高校按新规执行。

第二学士学位 本月起停止招生

此次办法中,最先成为焦点的,是已经实施35年的第二学士学位将正式退出历史舞台。

记者了解到,1984年以来,为了尽快地培养一批国家急需的知识面宽、跨学科的高层次专门人才,少数高校试办了第二学士学位班;1987年,《高等学校培养第二学士学位生的试行办法》印发,明确规定"第二学士学位在层次上属于大学本科后教育,与培养研究生一样,同是培养高层次专门人才的一种途径"。

"第二学士学位是在改革开放初期,针对我国研究生教育非常薄弱的情况,以及我国人才结构实际,根据国家建设需要,提出的一种应急性人才培养渠道。"上述负责人告诉记者,随着我国高等教育的快速发展,尤其是研究生教育的蓬勃发展,为弥补研究生教育不足而设立的第二学士学位已基本完成了历史使命。

现实中的数据可以显示这种变化。相关报道显示,2001年,经教育部批准,武汉大学等36所高校获批进行软件工程专业第二学士学位招生。2012年,报考武大软件工程专业第二学士学位的考生人数仅为招生计划的一半。当年,招生计划为183人,仅96人报考,其中21人参加了校方单独组织的笔试,最终有19人被录取。近年来,部分高校不断减少第二学士学位生的培养专业与人数,某些大学甚至停止了第二学士学位招生。

"高校目前实行的第二学士学位,很多也是双学士学位和辅修学士学位的模式,为此,此次文件提出不再招收第二学士学位生。"上述负责人表示。

三种学士学位类型 推动复合型人才培养

第二学位降温直至退出历史舞台的背后,是复合型人才培养的不断升温。开设计算金融专业、创新本科"混合班"教学……今年招生季,越来越多的复合型人才培养方式闯入公众视野。这也成为推动此次《办法》出台的另一种现实需要。

"近年来,围绕着复合型人才培养和优质资源共享,各高校积极探索,积累了经验,取得一定成效,但也存在着部分做法缺乏政策依据的问题。"上述负责人告诉记者。

记者注意到,为分类推动复合型人才培养,此次《办法》提出设置辅修学士学位、双学士学位、联合学士学位三种学士学位类型。文件规定,对于全日制学生在本校自主选择读多个学位的,可以采取辅修学士学位方式;对于学校主导开展的复合型人才培养,可以采取双学士学位方式,对招生、培养、毕业等进行整体设计,由省级学位委员会审批;对于校际之间正式开展的复合型人才联合培养项目,可以采取联合学士学位方式,推进优质资源共享,报省级学位委员会审批。

"各省应制定双学位、联合学位项目的审批细则,从严审批管理。如双学位项目所依托的学科专业应具有博士学位授予权,且分属两个不同的学科门类。"上述负责人还告诉记者,为确保学位证书的权威性,对于获得多个学士学位的都只发一个证书:"所获各类学位情况在证书上予以注明。"

定期进行质量抽检 建立申诉复议通道

长期以来,对学士学位的质量监督比较薄弱,一直成为关注焦点。记者注意到,为加强管理,填补政策空白,《办法》要求省级学位委员会建立学士学位授权与授予质量的评估制度和抽查制度,将学士学位质量监督纳入学位质量保障体系,并建立申诉复议通道。

《办法》规定,省级学位委员会应建立学士学位授权与授予质量评估制度和抽检制度,原则上在学士学位授予单位完成首次学位授予后对其进行质量评估,并定期对学士学位授予单位和授权专业进行质量抽检,加强对双学士学位、辅修学士学位、联合学士学位的质量监管;建立完善高等学历继续教育学士学位授予质量监督机制;对存在质量问题的学士学位授予单位或授权专业,可采取工作约谈、停止招生、撤销授权等措施。

《办法》同时要求,学士学位授予单位应建立相应的学位授予救济制度,处理申请、授予、撤销等过程中出现的异议,建立申诉复议通道,保障学生权益。

5G物联网时代,如何保证智能驾驶安全?

新华社 余俊杰

5G时代,万物互联,信息通信技术正与汽车产业加速融合,智能汽车、自动驾驶已成为行业研发风向标。然而,在智能汽车产业蓬勃兴起的背后,作为交通关键信息基础设施重要资产的车联网,也逐渐成为黑客们的攻击目标。

如何加强汽车网络安全防护,成了跨领域、多行业共同关心的话题。

7月23日至25日,由国家互联网应急中心、国家市场监督管理总局缺陷产品管理中心、中国网络空间安全协会和中国互联网发展基金会联合指导的第二届汽车安全与召回技术论坛在浙江宁波举行,与会代表们聚焦车联网发展趋势和核心防护技术研发,探讨如何保障智能驾驶行业平稳健康发展。

国家互联网应急中心实验室主任李政介绍,理论上,黑客可以通过网络攻击任意一台网联汽车,窃取车内数据,甚至夺取驾驶控制权。

据中国信通院发布的汽车电子网络安全标准化白皮书(2018)显示,近年来国内外发生过数百起智能驾驶安全漏洞事件:2015年两名黑客远程入侵了正在行驶的吉普汽车,造成减速、制动失灵等问题,导致克莱斯勒公司全球召回140万辆汽车并安装了系统补丁;腾讯科恩实验室分别在2016年和2017年两次实现远程无接触式破解特斯拉汽车,可在驻车和行驶状态下远程控制车辆。

"数据、网络、软件这些非实物要素,它们的漏洞和威胁构成新的安全隐患。"国家市场监督管理总局质量发展局副局长王赟松表示,网联汽车的初心是为了更便捷和安全,不能因为新技术增加更多风险。

国家互联网应急中心高级工程师范乐君介绍,汽车最容易受攻击的是通信和娱乐系统,黑客通过入侵手机网络、WiFi、蓝牙等通道,找到车载App漏洞进行攻击,就能获取用户在这些App上的隐私数据、历史记录,实现监听或促发导航偏离。

"如果将一辆汽车比作一幢房子,车联网让房子的门窗不断增加,受到的攻击频率自然水涨船高。"范乐君说,如果能为每扇门窗都配上安全阀,以技术管技术,便能尽可能减少隐患,掌握智能驾驶安全保护主动权。

"首先要具备技术、法律、安全三方面的保证,基于智能网联的自动驾驶大规模应用才能实现。"中国汽车工程研究院股份有限公司副总经理周舟介绍。

业内多名专家表示,要降低被入侵风险,最核心的是控制权限,加强加密工作,建立一套自主、完整的安全网络体系。

浙江吉利控股集团总工程师刘卫国建议,提高汽车网络安全防护,首先车企要确保软件开发安全,减少代码漏洞,从源头端减少风险。

国家互联网应急中心副总工程师陈训逊表示,每个数据接口都要做好加密,并对汽车健康数据进行实时监控。此外,车辆要加装安全硬件模块,并加强对云端服务器的数据传输处理过程保护。

业内专家建议,车主要注意车载软件及时更新,修复漏洞;汽车外接设备和网络时,应先确定其安全性;最重要的是,离开车时切勿忘记熄火锁车。

"随着5G的到来,汽车的动力系统也将实现网络化。届时,车联网的安全防控能力必须进一步升级。"范乐君说,目前国内急需培育一批既懂网络安全又对汽车工程有所了解的专业人员。同时,需要让整车制造企业及汽车零部件企业全面认清当前车联网安全形势,不断提升防护水平,构建适应汽车产业智能化、网联化转型的主动安全体系。