课程思政理念下“信息安全管理”案例教学研究*

郭燕慧 陆天波 段蓬勃

北京邮电大学网络空间安全学院，北京，100876

摘 要 没有网络安全就没有国家安全，为落实网络安全人才的人才安全培养要求，需要对“信息安全管理”课程实施课程思政。本文以课程思政教育理念和课程观来规划、组织“信息安全管理”的教学。在剖析课程特点、明确课程思政目标的基础上，提出系统的思政案例教学方案。以云服务安全风险分析为例，展示了信息安全管理课程思政案例教学的基本过程，探讨了知识讲授与思政教育相融合的具体方式。在学生学习教师讲授的案例和小组完成案例的过程中，达成知识传授、能力培养和价值引领相结合的“三全育人”目的。

关键字 网络空间安全，课程思政，信息安全管理，案例教学

Study of Case Teaching for Information Security Management Based on the Idea of Curriculum Ideological and Political Education

Guo Yanhui Lu Tianbo Duan Pengbo

College of Cyber Security
Beijing University of Posts and Telecommunications
Beijing 100876,China

Abstract—Without cyber security, there is no national security. In order to put the talent security training requirements of cyber security into effect, it is necessary to implement curriculum ideological and political education in the course of "information security management". This paper reorganizes the teaching of "information security management" based on the idea of curriculum ideological and political education. On the basis of analyzing the characteristics of the curriculum and clarifying the objectives of curriculum ideological and political education, this paper puts forward a systematic case teaching scheme of ideological and political education. Taking cloud service security risk analysis as an example, this paper demonstrates the basic process of ideological and political case teaching in information security management, and explores the specific way of the integration of knowledge teaching and ideological and political education. In the process of students learning the cases taught by teachers and completing the cases in groups, the goal of "Three Aspected Education " which combining knowledge transferring, ability training and value guiding will be accomplished.

Key words—Cyber Security, Curriculum Ideological and Political Education, Information Security Management, Case Teaching

1 引 言

习近平总书记面对互联网发展趋势提出：没有网络安全就没有国家安全，没有信息化就没有现代化，网络安全已经提升到国家战略。网络空间安全是一个攻守方博弈的过程，攻守方都需要知识和技术。掌握了网络空间安全技术， 既可以用于维护网络空间安全， 维护国家、社会安全，也可以利用这些技术在网络上进行违法活动， 从事危害党和国家安全的行为。因此，我们培养的网络空间安全人才首先要是政治合格，技术至上的黑客文化绝不可取。我们要充分利用学校课堂这个主阵地，有效利用思政课程和课程思政，给学生扣好人生第一粒扣子，帮助他们树立起正确的人生观、世界观、价值观，增强文化自信和民族自信，厚植爱国主义情怀，立志献身祖国网络空间安全事业，有良好职业素养和人文情怀，有坚实的专业基础知识和实践能力，有安全思维和科研创新能力，能够参与解决复杂的网络空间安全工程问题。

课程思政是指“以构建全员、全程、全课程育人格局的形式将各类课程与思想政治理论课同向同行，形成协同效应，把立德树人作为教育的根本任务的一种综合教育理念[1]”。其实质“是一种课程观，不是增开一门课，也不是增设一项活动，而是将高校思想政

*基金资助：北京邮电大学研究生教育教学改革项目“《信息安全管理》课程思政实践研究”（2021Y025）.

治教育融入课程教学和改革的各环节、各方面，实现立德树人润物无声[2]”。

案例是人们在生产生活当中所经历的典型的富有多种意义的事件陈述。案例教学法以学生认知经验为指导选择符合教学内容的代表性案例，以案例为基本素材引导学生分析、探究、思考、讨论，在一系列自主活动中完成既定教学目标，内化知识与情感，提高实际问题解决能力。作为一种教学手段，案例教学法的目的是服务于知识迁移的有效性，即让学习活动在特定条件下更高效地在学生身上发生。技能性、应用性、综合性以及多因素复杂条件下的混沌决策更适于案例教学法，因而案例教学法在社会人文学科领域和职业教育领域均得到了广泛的应用[3][4][5][6]。

网络空间安全是一个理论与实践结合紧密的实用性的学科，面向网络空间安全专业人才培养的课程思政建设中，采用案例教学可以收到事半功倍的效果。《信息安全管理》课程强调“三分技术，七分管理”，既有较强的理论性，也有一定的实践性，集中体现了网络空间安全学科的特点，是培养网络空间安全所需要的高素质复合型人才的必修课。本文以《信息安全管理》课程为例，研究如何运用案例教学法将网络空间安全专业教育与思想政治教育进行有机结合，对于增强高校网络空间安全课程思政教学方法的有效性具有现实意义。

2 “信息安全管理”课程思政教育的内涵与抓手

案例教学法作为一种教学手段，其作用的发挥取决于对教学内容的理解程度。对学科领域的专业属性或教学目标属性理解的越深刻，在案例教学法的运用上就会越到位。

2.1 “信息安全管理”课程思政教育的内涵

信息安全管理是指通过维护信息的机密性、完整性和可用性来管理和保护信息资产，是对组织或机构信息安全实施过程中的人员，物质及资金的统筹管理。信息安全管理是知识、技能、艺术的综合体。知识对应着验算反思，强调科学理性。思维方法的学习、训练、掌握和运用，可以改善个人的思考和行为方式，促进正确价值观的形成。技能对应着体验反思，强调实践训练。专业技能是把双刃剑，用好了可以推动社会发展，用不好可以引发社会问题，关键要看掌握专业技术的人是否具有正确的专业伦理，专业行为是否符合专业规范，思想行为是否违背职业道德。而艺术对应着心灵反思，强调情境感悟。科技的发展带来工作和生活的便利，但同样引起一系列的情感与社会问题。专业知识、技术和产品背后所蕴含的人文素养、道德情感、社会服务、国家骄傲、工匠精神等，对良好行为习惯的养成、真善美良好品质的形成、国家大局意识和社会服务意识的产生有无形的推动力量。

“信息安全管理”课程思政是通过课程知识结构的优化，把科技理性（学科理性）与人文理性、思政理性有机融合起来，以潜移默化的形式将社会主义核心价值观、信息安全人员职业道德、法律意识、社会责任感等思政要素融入课程教学过程，实现知识传授、技能提升和价值引领的目的。

2.2 “信息安全管理”课程思政教育的抓手

（1） 所属行业具备天然的德育教育优势

从所属行业而言，国家层面制订有《中华人民共和国网络安全法》、《网络安全等级保护管理办法》、信息安全从业人员职业道德规范等法规体系和行业自律标准，并提出了信息安全从业人员职业素养和道德方面的基本要求，如《CISP职业道德准则》：①维护国家、社会和公众的信息安全；②诚实守信，遵纪守法；③努力工作，尽职尽责；④发展自身，维护荣誉。这些规定和规范均涉及德育教育问题，是信息安全课程教学必须要落实的问题。这就要求课程教学在传授知识、培养能力的同时，必须结合信息安全业务处理进行职业道德规范教育，这是课程教学的使命，也是课程实施思政教育的天然优势。

（2）社会现实为课程思政提供了丰富的案例资源

由于信息安全的特殊性，一旦出现问题，对社会的危害较大，这就要求信息安全从业人员必须严格自律。但在现实环境中，信息技术从业人员的职业操守现状并不乐观，各类安全事件时有发生。2016年10月21日，美国东海岸(世界最发达地区)发生世界上瘫痪面积最大(大半个美国)、时间最长(6个多小时)的分布式拒绝服务(DDOS)攻击。2017年5月12日爆发的“WannaCry”勒索病毒，通过将系统中数据信息加密，使数据变得不可用，借机勒索钱财。病毒席卷近1 50个国家，教育、交通、医疗、能源网络成为本轮攻击的重灾区。2018年8月3日，台积电遭到勒索病毒入侵，几个小时之内，台积电在中国台湾地区的北、中、南3个重要生产基地全部停摆，造成约2.55亿美元的营业损失。这些安全事件也成了课程实施思政教育天然的、独特的宝贵资源，为课程实施思政教育提供了现实的案例支持，能使学生真实感受信息安全的管理的重要性，提升教育效果。

（3） 课程特点使得课程与思政培养水乳交融

由于信息安全的特殊性，一旦出现问题，对社会的危害较大，这就要求信息安全从业人员必须严格自律。但在现实环境中，信息技术从业人员的职业操守现状并不乐观，各类安全事件时有发生。2016年10月

21日，美国东海岸(世界最发达地区)发生世界上瘫痪面积最大(大半个美国)、时间最长(6个多小时)的分布式拒绝服务(DDOS)攻击。2017年5月12日爆发的“WannaCry”勒索病毒，通过将系统中数据信息加密，使数据变得不可用，借机勒索钱财。病毒席卷近1 50个国家，教育、交通、医疗、能源网络成为本轮攻击的重灾区。2018年8月3日，台积电遭到勒索病毒入侵，几个小时之内，台积电在中国台湾地区的北、中、南3个重要生产基地全部停摆，造成约2.55亿美元的营业损失。这些安全事件也成了课程实施思政教育天然的、独特的宝贵资源，为课程实施思政教育提供了现实的案例支持，能使学生真实感受信息安全的管理的重要性，提升教育效果。

3 “信息安全管理”课程思政案例教学的流程与要点

案例的核心价值在应用。引入案例教学应准确判断案例能使学生掌握哪些专业知识，获得哪些方面的思政教育，让学生能够在有限的课堂时间内，既完成理论知识学习，又受到思政育人案例的启发。因此，在制定信息安全管理思政案例教学方案时，首先，要在明确具体章节和知识点的基础上，选择出贴切而形象地与之相结合的案例。其次，在科学地制定出思政教学的目标、方法及内容的基础上[7]，有引领、有计划地将专业知识与思政元素有机结合。从引出话题、讨论发言、教师讲授等各个环节自然嵌入，注重随机应变和灵活机动。最后，要及时对案例教学进行效果评估与反思。通过对案例教学效果的评估，了解案例选择是否合理，是否达到了预期教学目标，是否充分发挥了信息安全管理课程的人文情怀与社会关怀[8]，同时又可以为其他教师实施思政案例教学提供借鉴。据此，教学流程可分为三步走，即教学准备阶段、教学实施阶段、教学转化阶段[9]。

3．1 教学准备-筛选与匹配

“教学准备阶段”是整个案例教学活动的起点，其核心任务是案例筛选，要点是针对教学目标，匹配教学案例。

信息安全管理课程讲述信息安全管理的基本方法和原理，信息安全风险评估及分级防护，以及构建信息安全管理体系的基本流程和相关的标准和法规。主要内容包括：信息安全风险评估、分级防护、物理与环境安全、安全运维、业务连续性与灾难恢复等信息安全管理体系的内容及其最新进展。目前能应用于信息安全管理课程思政的案例非常丰富，为实现知识传授与立德树人有效结合，用学生感兴趣、听得懂的案例实现对知识的融会贯通，采取分阶段分层级的案例编排方式，围绕核心知识点，达成其知识目标、能力目标和情感目标（详见表 1）[10][11][12]。信息安全管理的实施是按章节分阶段介绍的，故在第一层级上对每一章，以一个针对性很强的案例开篇，使学生直接面对信息安全管理实际需求中的问题。而后，以这个案例中的问题为出发点，传授知识、讲解技术和方法来解决这个问题。在这个过程中把应掌握的信息安全管理的原理和方法讲授给学生，强调思维方法的学习、训练、掌握和运用，同时把开篇案例中的问题予以解决。这一个层级的案例选择和使用上，针对性和典型性是最重要的案例特征，枝蔓不能太多，不然会干扰教学重点内容的进行。第二个层级：总体基本原理讲授完成之后，归纳综合所学内容，使用案例来帮助学生学会分析和解决复杂问题，掌握专业技能、引发职业道德思考。第三个层级则进一步挖掘案例中所蕴含的人文精神，追求真善美的良好品质。这两个层次的案例除了了典型性目的性之外，更要考虑它们的综合性和发散性。

表 1 信息安全管理课程思政案例分阶段、分层示例

案例主题	第一层级：知识目标	第二层级：能力目标	第三层级：价值目标
信息安全风险评估	风险评估的要素与流程	风险分析与防范	居安思危、家国情怀
访问控制	访问控制的模型和方法、系统与网络安全技术、物理安全技术	纵深防御	辩证思维、求真务实、不断探索、刻苦钻研
业务连续性管理	容灾、备份技术、业务练性计划	业务连续性计划制定与实施	危急意识、忧患意识
运维安全	配置管理、冗余容错、介质管理、脆弱性测试	安全级别的续维护	精益求精、工匠精神
信息安全法规道德	计算机犯罪的分类与特点、典型的信息安全法规	知法、守法、企业合规	职业道德、国家大局意识和社会服务意识

3．2 教学实施-思考与讨论

“教学实施阶段”是案例教学的重心，其核心任务是按照教学计划完成决策研讨，教学的要点是对案例学习过程的有效干预和方法指导，将思考引向深入，并构建平等对话、鼓励质疑的研讨氛围。

在案例资料准备充分的基础上，必须要教会学生以一定的思考方式和策略来面对不断出现的新问题。在课程开始阶段，老师一般准备以下问题进行案例分析示范：组织所处的外部环境是怎样的？目前问题可能牵扯到的各方有哪些？可以获得的相关信息来源有

哪些？可能有助于问题解决的信息安全管理方法有哪些？确立打算使用的信息安全管理方法，以及备用的方法？讨论有无其他可能的解决方法？由其人、其事还能联想到其他吗？感悟是什么？等等。针对以上每个方面再列示出小的思考方面和步骤，以帮助学生逐步形成解决问题的有效思考习惯。

讨论一开始，教师可以鼓励一些善于表达的学生先发言，调动起课堂研讨的氛围。但如果遇到没有学生主动发言的情况，教师采取提问的方式也不失为一种应对之策。当有学生开始发言时，他们的观点可能引起其他学生不同的看法，当其他学生有不同的见解时，他们就更有主动发言的欲望，这样课堂气氛很快就会被调动起来。教师一方面要尽可能地调动学生参与讨论，另一方面要善于倾听，及时引导和掌控全局。最后，教师要做好研讨的总结点评工作。研讨课的点评既是对学生研讨内容的概括总结，也是对学生价值观的再次引导。研讨的目的就是让学生说出自己的看法，教师要对学生的观点表达情况给出明确的点评。课程思政以“立德树人”为主旨，学生的发言很多时候是其价值观的自然流露，对此，教师必须进行明确的价值引导，对于正确的价值观要给予充分肯定，而对于带有错误倾向的价值观要坚决指出问题并做出正确引导。

3．3 教学转化——应用与内化

“教学转化阶段”是案例教学的成果应用，其核心任务是完成知识迁移、能力的内化及素养的提升。

在信息安全管理课程中，通过安排 3-5 人的小组来共同准备一个案例方案，来完成课后的转化任务。案例的分析准备过程由学生在课前集体完成。在上课的时候，每个小组选派代表来陈述他们对于案例的认识，分析的方法，解决的方案，以及选择这样做的最重要考虑是什么。当陈述讲解完毕之后，要求学生针对其他小组的案例分析解决方案进行评价和比较，以检验并提高学生的信息安全管理综合能力，强化国家安全意识与自身的职业道德素养。例如，可设定“分级防护措施案例分析”题目，学生积极讨论，分享各自知道的访问控制事故，给出相应的预防方法，在学好信息安全管理和技术的同时，努力增强安全意识、提高思政修养。为了更好地培养学生的团队精神和过程控制思维，使学生及时完成相关任务，教师制定严格的任务点完成时间，主要包括以下几个阶段：分组及题目选择、英文参考文献、课程思政自学内容、题目进展汇报、案例考核等。学生也可以自选题目，融入与课程密切相关的思政内容，这样更能调动学生的学习主动性，也可以及时了解学生关心的问题。学生选择的题目与课程核心知识点联系紧密，学生主动查找其中蕴含的课程思政元素，从被动学习转变为主动学习。

4 信息安全管理课程思政案例教学实践

接下来以“信息安全风险评估——云服务安全分析”教学案例，来分析信息安全管理课程思政案例育人的教学设计过程。

4．1 明确核心知识点和教学目标

信息安全风险评估主要对信息系统面临的风险参照相关评估标准和管理规范进行辨识与分析，对系统中面临的威胁、脆弱性和可能造成的损失进行风险值计算，并针对不同的风险制定相应的安全措施。其显性目标是，使学生理解信息安全风险评估的基本思想；运用信息安全风险评估技术来保障组织安全；理清组织的安全需求，使组织做出正确的战略决策。其隐性目标在于，使学生了解国家时事政治、社会文化状况和科学技术水平，明确信息安全从业者的使命和责任[13][14][15]。具体来说：在知识目标方面，使学生了解信息安全风险评估要素，掌握信息安全风险分析法的内涵与分析方式；在能力目标方面，使学生需要具备观察问题、分析问题和评估问题的综合能力；在情感目标方面，激发学生探索创新、实现自我价值与抱负的渴望，增强学生为国家发展贡献力量的动力，引导学生树立法律责任、社会责任意识，提升信息安全职业道德素养。

4．2 课堂教学组织

（1） 专业知识讲解

风险评估理论最早由欧美核电厂提出，信息安全领域风险研究始于 19 世纪 60 年代，美国国防科学委员会委托相关工业公司历经两年多的时间对当时大型机做了一次大规模的风险评估。信息安全风险评估的关键是对信息系统资产的分类，并依据其资产进行风险识别、估计和评价，然后实现全面的、综合的分析。在传统的信息安全风险评估工作中，主要围绕资产、威胁以及脆弱性三种要素进行。 在资产评估过程中，必须要 从业务评估入手，对企业资产进行识别，并对资产进行分类， 确保资产的安全性。 对资产的评估必须要建立在业务主线的 基础上，通过对软硬件、数据、人员、设备、服务及其他等类型的资产进行分类评估，具有较强的逻辑性。

20 世纪 90 年代，我国信息安全风险评估工作标准化研究开始启动，2006 年由原国信办发布《关于开展信息安全风险评估工作的意见》（国信办 2006 年 5 号文）；同时，随着信息安全等级保护制度的推行，公

安部会同有关部门出台了一系列政策文件，主要包括：《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》等；国家信息安全标准化委员会颁发了《信息安全风险评估规范》（GB/T 20984~2007）、《信息系统安全等级保护基本要求》（GB/T22239- 2008）等多个国家标准。围绕信息安全风险评估制定的国际标准和国家标准为信息安全风险评估工作提供了重要依据。

（2）案例引入与分析

案例：随着物联网、5G 和大数据时代的到来，云计算、人工智能等技术迅速发展，在给人们带来方便的同时，安全问题也不容忽视。 2010 年 9 月，由于微软在美国、欧洲和亚洲的数据中心的一个没有确定的设置错误出现多次托管服务中断，这是微软首次爆出重大的云计算数据突破事件。2011 年 4 月 22 日，亚马逊云数据中心服务器由于其 EC2 系统设计存在漏洞和设计缺陷大面积宕机，这一事件被认为是亚马逊史上最为严重的云计算安全事件。2017 年 7 月 13 日，由于供应商 Nice Systems 一名员工人为失误，导致美国电信公司 Verizon 的 600 万名用户信息被公开泄露在网上。2019 年 10 月，亚马逊旗下云平台 Amazon Web Services（AWS）遭到了黑客发起的 DDoS 攻击，被迫中断服务达 8 个小时。而在大约同一时间，谷歌的云平台也遭到了类似攻击，波及了谷歌计算引擎、谷歌 Kubernetes 引擎、Cloud Bigtable 和谷歌云存储服务，并致使多个用户数据包丢失。云计算是网络技术与传统计算机技术结合发展的一种新型产物，是通过利用多种商业模式提供强大的计算能力，并最终将其向终端用户进行提供，以便实现高速率的信息处理以及高效率的服务。上述案例表明，云计算背景下，组织的安全运维工作发生了改变，数据安全问题、稳定性问题尤为突出，如何对信息安全风险进行有效评估成为当下企业需要重点思考的问题。

分析：

导致云服务安全问题的威胁来自三个方面：第一，云计算软件的配置错误或者软件中的瑕疵。第二，黑客窃取数据，为了取乐或者赚钱。第三，员工处理数据的疏忽。云平台安全风险评估关注云计算平台业务层面的风险，其评估对象为云服务业务流程涉及的组件及设备，评估范围覆盖了云服务业务在信息系统层面的数据流、数据处理活动及其关联关系。评估过程覆盖了基础设施、虚拟化控制、管理平台和安全防护等多种类型的对象，针对多种指标进行综合风险分析，并且在监管、业务和客户的要求下做出相应的调整。

从云服务安全事件的现实威胁来看，黑客行为是信息安全从业者不能触碰的法律红线；而爱岗敬业、精益求精，发挥信息安全守护者的权威性、增强人们对信息安全行业的认可与信赖，则是每个信息安全从业者应当坚守的道德底线。

从云服务业务来看，目前主流的几家提供云服务的企业有亚马逊 AWS、微软 Azure、阿里云、腾讯云和华为云。其中，国内多家云高层管理人员多次在重要会议和演讲上表明了对云安全的重视程度，并相应制定了云安全实行策略。阿里云、腾讯云等国内云计算企业的安全白皮书的更新频率和内容完整度都充分优于微软 Azure 等国外企业。在标准认证方面有着如下排名：阿里云>微软 Azure>腾讯云>亚马逊 AWS=华为云。综合态度、执行力、标准认证三方面评判多家著名企业，其在云安全方面的相对排名为：阿里云>腾讯云=微软 Azure>亚马逊 AWS=华为云。

从云服务监管要求看，我国云计算相关标准的研制从 2013 开始，已逐步形成较为完备的体系。2019 年新推出的等保 2.0 标准，更是适应云计算技术的发展，增加了云计算安全扩展要求。

20 世纪 90 年代时，中国在计算机相关领域处于落后位置，标准的制定基本由西方发达国家进行。鉴于前人的教训，我国在后期云计算安全发展上充分利用新时代大好条件，在云计算实践、云计算标准化、云安全管理及合规方面，逐步取得领先地位，提振了国人的科技自信和文化自信，增强了民族自信心和自豪感，为全社会营造一种积极向上的热情氛围，具备潜在的长久影响力。

在案例分析阶段，教师围绕设定问题进行互动式随机提问，使学生能够在表达自身观点和倾听他人观点的过程中反复地进行自我批判与思考，逐渐理顺自身的逻辑思路，不断完善和补充自身的知识体系，并在此过程中逐渐形成对知识、能力、情感的自我构建。进一步还可安排学生进行分组讨论，令学生在与组内成员讨论的过程中进行群体思维碰撞，逐渐在小组内部形成共同观点。在群体思维碰撞与达成小组意见的过程中，能够拓宽学生视野和培养的学生团结协作精神，并将知识构建与逻辑完善从个人层面向群体层面拓展。教师还可以引导小组代表发言，进一步完善问题的解决思路，从而在更大范围内实现学生知识与逻辑的补充构建与拓展，形成整合性知识，提高学生学习成效。

（3）案例总结

为系统地了解组织业务和所处的环境背景，在运用信息安全风险评估的过程中，通常需要分析有关国家/行业政策以及经济、社会文化以及科学技术发展现状。因此，在具体管理实践中运用信息安全风险评估来分析组织的业务和环境，要比本案例中更加复杂和深入。这就要求当代大学生除了学习专业知识外，还

应立足国际视野，关注社会，关心当下经济形势及科技发展趋势，吸取中华优秀传统文化的精华，积极投身于我国科技强国事业中去。

4．3 教学效果评估

信息安全管理课程思政采用案例教学方式，以兴趣为驱动，让思考在讨论中深入，令科技与人文内化于心，以期达到知行合一的育人效果。为了综合评估这一方法的教学效果，在课程结束后对学生进行了问卷调查。问卷就课程思政教学对于提升学习兴趣、加深专业知识理解、提升分析解决问题能力以及领悟信息安全职业操守、激发家国意识与社会担当等项目进行了调研。发放问卷 65 份，回收有效问卷 65 份，有效率 100%。结果可见，90%以上的学生对于信息安全管理课程思政的案例教学效果给予了肯定(见表 2)。

表 2 信息安全管理课程思政案例教学影响效果问卷调查结果

效果 / 影响	很好		较好		一般		无	
	人次	百分比	人次	百分比	人次	百分比	人次	百分比
提高学习兴趣	41	63.08%	15	23.08%	5	7.69%	4	6.15%
加深专业知识理解	43	66.15%	14	21.54%	5	7.69%	3	4.62%
提升分析解决问题能力	38	58.46%	17	26.15%	6	9.23%	4	6.15%
领悟信息安全职业操守	37	59.68%	18	29.03%	7	11.29%	0	0.00%
激发家国意识与社会担当	35	59.32%	16	27.12%	6	10.17%	2	3.39%

5 结束语

课程思政，课程是基础，思政是根本[16]。思政案例教学在管理学课程中很好地实现了专业知识与思政教育的结合，潜移默化地完成了德育与智育的有机统一，为高校教师推进课程思政改革提供了一种切实可行而且高效的途径，能够提升学生的综合素养。通过思政案例循循善诱的讲解，不仅能够通过让学生逐步代入案例角色，做到理论学习与管理实践并重，使其学习效率得以提高、学习兴趣得以提升；而且有助于培养学生的家国情怀和社会主义核心价值观，让学生意识到自己作为社会主义接班人必须珍惜当下的美好生活，树立正确的世界观、人生观、价值观，努力学习专业知识，树立良好的爱国主义情怀，使自己成为德才兼备的后备管理人才。

参 考 文 献

[1] 韩飞. 高校“课程思政”教育理念的科学定位[J]. 黄冈职业技术学院学报，2018,(3):24-28.

[2] [高德毅，宗爱东. 课程思政:有效发挥课堂育人主渠道作用的必然选择[J]. 思想理论教育导刊,2017(1):31-34.

[3] 张峰. 计算机专业课教学中案例驱动教学模式的实践[J]. 榆林学院学报. 2010. 20(2):74-76

[4] 汪茂泰. 《政府经济学》课程教学案例选择的实践和思考[J]. 西部学刊. 2020 (14):50-52

[5] 李冬梅.案例教学在“财政学”教学改革过程中应用效果探析[J].河北地质大学学报,2021,44(04):137-140.

[6] 杜庆贵.案例教学法视角下刑法学课程思政研究[J].淮南职业技术学院学报,2021,21(03):90-92.

[7] 陆道坤. 论课程思政的教学设计与实施［J］. 思想理论教育， 2020(10) :16-22.

[8] 高国希. 构建课程思政体系的教育哲学审视［J］. 思想理论教育， 2020(10): 4-9 .

[9] 谭俊峰. 案例教学法的内涵、类别及应用[J]. 北京经济管理职业学院学报. 2020,35(03):42-49

[10] 马成昌.“课程思政”背景下思政课程教学方法的现象学呈现[J].山西高等学校社会科学学报,2019,31(08):29-33.

[11] 李陈,曲大维,孟卫军.案例教学法在专业课“课程思政”中的应用[J].宁波教育学院学报,2019,21(04):1-4.

[12] 吴中华.案例教学在课程思政建设中的应用研究[J].中国乡镇企业会计,2020(09):241-242.

[13] 毕方明,杨文嘉,韩丽霞.信息安全管理与工程课程思政在线教学改革探讨[J].科教文汇(中旬刊),2021(03):109-110.

[14] 张伟,黄海平,陈云芳.新工科背景下网络空间安全专业课程思政建设探讨[J].科教导刊(上旬刊),2020(07):81-83.

[15] 张明真,徐钢涛,李勇强.信息安全与管理专业课程思政实施设计研究[J].河南农业,2021(06):25-27.

[16] 张大良. 课程思政: 新时期立德树人的根本遵循[J]. 中国高教研究， 2021(1) : 5-9.