以国产开源促进《信息安全管理》课程教学改革实践*

郭燕慧 邹仕洪 徐国胜 张熙 李剑

北京邮电大学网络空间安全学院，北京 100876

摘 要 本文针对传统信息安全管理教育中实践教学不足的问题，提出了一种基于国产开源社区的信息安全管理教学方法，将国产开源软件与国产开源社区引入课程体系，通过信息安全管理的理论教学、国产开源社区功能理解、开源生态安全管理实践及过程性、多层次的教学评价四个阶段，使学生能直接参与真实的开源社区活动，在与全球技术发展同步的动态、开放式学习环境中解决实际安全挑战，提升安全实战能力。

关键字 信息安全管理，人才培养，国产开源软件，实践教学，社区参与

The Practice of Promoting the Teaching Reform of the "Information Security Management" Course through Domestic Open-Source Resources

Yanhui Guo Shihong Zou Guosheng Xu Xi Zhang Jian Li

School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing 100876, China
yhguo@bupt.edu.cn;zoush@bupt.edu.cn;guoshengxu@bupt.edu.cn;zhangx@bupt.edu.cn;lijian@bupt.edu.cn

Abstract—This paper addresses the issue of insufficient practical teaching in traditional information security management education by proposing a teaching method based on domestic open-source communities. The approach integrates domestic open-source software and communities into the course curriculum, encompassing four stages: theoretical teaching of information security management, understanding the functions of domestic open-source communities, practical exercises in managing open-source ecosystem security, and a multi-layered, process-oriented teaching evaluation. This method enables students to directly engage in real open-source community activities, tackling actual security challenges in a dynamic and open learning environment that keeps pace with global technological advancements, thereby enhancing their practical security skills.

Keywords—Information Security Management,Talent Development,Domestic Open-Source Software,Practical Teaching, Community Participation

1 引 言

在当今数字化时代，信息技术的快速发展已经深刻改变了我们的工作和生活方式。随着网络技术的广泛应用，信息安全问题也日益突出，成为全球关注的热点问题[1]。在网络安全领域中，一直有一个重要的实践原则——“三分技术、七分管理”，即 70%的网络安全问题无法通过纯技术手段解决，而是需要依靠组织严格的安全管理制度和检查措施去规避[2]。由于网络安全管理工作涉及措施制定、策略规划、资产管理、人员定位、检查审计等诸多方面，而组织信息安全工作更会受组织性质、组织人员、网络环境、应用系统等多重因素影响，培养具备扎实理论知识和过硬实践能力的信息安全管理人才[3]，已成为教育界和业界面临的共同挑战。

传统的信息安全管理教育往往受限于组织安全问题的敏感性和复杂性而偏重于理论教学，而缺乏足够的实践操作[4]，这导致学生在理论知识和实际能力之间存在较大的脱节。开源软件及其社区，以其开放性、实时性和互动性的特点，为信息安全管理教育提供了一个理想的实践平台[5]。近年来，中国开源生态迅速发展，顶级开源项目数量稳步上升。中国现已成为全球开源领域的重要力量[6][7]。将国产开源社区引入课程，

*基金资助：本文得到北京邮电大学教改项目-面向网络安全人才实战能力培养的《信息安全管理》课程建设（2023YB37）资助。

使学生接触更多安全运维、管理过程中遇到的真实问题和相关解决方案，不仅能让学生在实际环境中应用理论知识，还通过与全球开发者的交流和合作，提升学生的技术水平和创新能力。

本文探讨了国产开源软件及其社区在信息安全管理实践教学中的作用和意义，通过信息安全管理的理论教学、国产开源社区功能理解、开源生态安全管理实践，帮助学生在信息安全管理领域建立实践经验，提升创新和解决问题的能力,为网络空间安全专业高层次实战型人才的培养探索新的模式。

2 开源软件及其社区对于信息安全管理教学的作用和意义

2．1 开源软件及其社区

开源的本质在于开放共享、协作创新[8]。开源软件是基于开源思想开发的软件，其源代码被公开发布，允许任何人自由使用、修改和分发。它是一种更可靠、更安全和性能更优的软件解决方案。开源软件的主要特点包括：

（1）可访问性：源代码对所有人开放，使得用户和开发者可以自由查看、学习和修改代码。

（2）协作性：开源项目鼓励来自全球的贡献者参与，促进了跨文化、跨地区的合作开发。

（3）透明性：开发过程、决策和讨论通常是公开的，这增加了软件的可信度和安全性。

（4）灵活性：用户可以根据自己的需要自由修改和定制软件，提高了软件的适用性和灵活性。

（5）持续性：依靠社区的力量，即使原始开发者停止维护，项目也可以继续发展和进步。

开源社区，作为开源软件发展的核心，由地缘空间分散但拥有共同兴趣爱好的开发者根据相应的开源软件许可证协议，以民主、合作的形式进行软件的共同开发、维护、增强等知识创造与传播活动的网络平台，同时也为成员展开交流学习与共同治理的网络组织[9]。

开源软件是群体智慧的结晶，开源社区聚集大量爱好者共同参与开发、测试、维护等。社区成员通过各种方式如文档、教程、讨论论坛和在线会议等，积极分享知识和经验,使新成员能够快速地学习和成长。同时，开源社区作为一个创新的实验平台，鼓励成员自由探索新思维，共同推进社区的发展[10]。

2．2 开源实践对于信息安全管理教学的意义

（1） 真实生动的组织形态

国产开源社区是一个真实且生动的组织形态。参与开源社区的学生将加入由全球各地成员组成的多元化团队，通过在线协作工具与团队成员进行跨时区、跨文化的沟通。这种环境要求学生积极参与项目的日常运作，体验项目管理、代码审查和漏洞修复等实际操作。这不仅增强了学生的沟通和协作能力，还使他们理解团队合作在信息安全管理中的重要性。在开源社区中，学生通过真实的项目任务提升技术能力，并学会如何在团队中高效合作和解决冲突，从而真正理解信息安全管理的复杂性和多样性。

（2） 快速更新和多化样的信息技术

开源项目的高更新频率意味着新的功能、补丁和安全修复不断推出，学生在参与开源项目时，可以及时学习和应用这些最新的技术，保持与行业发展的同步。开源社区涵盖了从操作系统、数据库到中间件、应用软件等各种类型的软件项目，学生可以根据自己的兴趣和专业方向选择不同的项目，获得广泛的实践经验，提升他们在不同技术领域的综合能力。相较于传统的更新缓慢的实验教学环境[11]，开源社区的开放性和实时性使学生能够在实际环境中了解和应对不断变化的信息安全威胁。

（3） 产教融合的天然平台

在开源社区中许多企业既作为贡献者也作为使用者，表现十分活跃[12]。学生在参与开源项目的过程中，接触到大量真实的企业项目，学习到企业级项目的开发规范和流程，了解企业的需求和标准。这不仅缩小了高校教育与企业需求之间的差距，还为学生提供了就业前的实战训练，增强了他们的就业竞争力。企业的参与可为高校教学提供最新的行业动态和技术支持，提升教学的质量和效果[13]。同时，企业也在这一过程中扩大项目影响力，吸引更多的高质量贡献者加入。

（4） 思政教育的鲜活载体

在信息安全领域，国产软件的安全性和自主可控性越来越受到重视。通过将国产开源社区如 OpenKylin、OpenHarmony 等引入教学，使学生掌握信息安全技术和管理方法，了解其在国家关键信息基础设施中的应用，认识到国产软件在国家安全中的重要性，激发爱国情怀和社会责任感，在潜移默化中得到思政的教育。此外，开源社区的开放性和透明性还为课程的思政教育提供了丰富的素材和案例，引导学生思考技术与社会、国家安全等问题，帮助他们树立正确的价值观和职业道德。

3 基于开源实践的信息安全管理教学方法

本文提出了一种基于开源实践的信息安全管理教学方法，该方法利用开源社区的实际环境作为培养信息安全管理人才的平台。通过直接参与到开源社区中，学生可以在真实的环境下学习和实践信息安全管理。教学框架包括理论教学、国产开源社区功能理解、开源生态安全管理实践以及过程性、多层次教学评价，如图 1 所示。

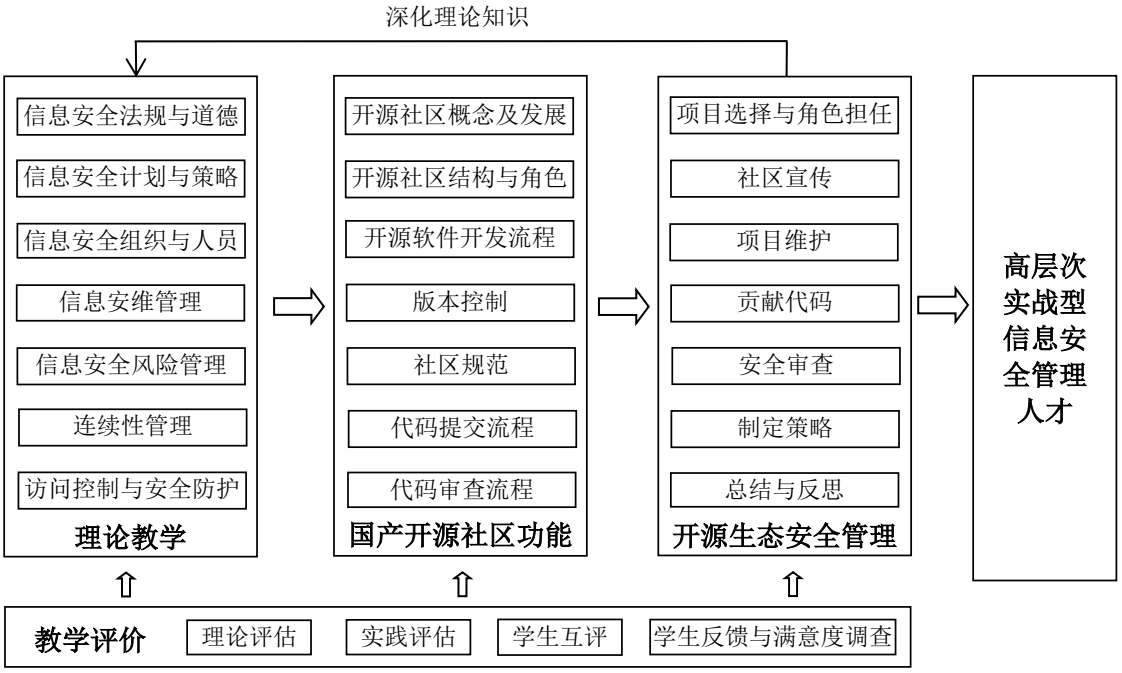

图 1 基于开源实践的信息安全管理教学框架

3.1 理论教学

教师将系统地向学生讲解信息安全管理的核心理论，包括信息安全法规与道德、信息安全计划与策略、风险管理等基础内容。课程将涵盖信息安全管理的核心概念和基本原理，帮助学生建立全面的知识框架。

首先，教师介绍信息安全管理的基本要素，包括保密性、完整性和可用性（CIA 三要素）。学生需要理解这些要素在信息安全中的关键作用，并能够辨识和解释它们如何在实际环境中应用。课程将通过具体示例，展示如何在保护敏感信息的过程中保持其保密性，确保数据的完整性，以及保证系统和数据在需要时可用。

接下来，课程将深入探讨信息安全的威胁、漏洞和风险的基本概念。教师解释漏洞的概念，包括软件、硬件和操作环境中的安全缺陷及其对信息系统的潜在影响，并探讨如何通过漏洞评估和修复来减少风险。课程将系统讲解风险管理的流程，包括风险识别、评估、优先级排序、应对措施和持续监控，帮助学生掌握全面的风险管理技能。

信息安全管理的总体框架是课程的另一个重要内容。教师讲解信息安全管理体系（ISMS）的构建，包括政策、程序和控制措施的制定与实施，并介绍 ISO/IEC 27001 等国际标准，学生需要理解如何通过系统化的管理和控制来维护信息安全，并确保其符合法律法规和行业标准。

为了加深学生对理论知识的理解和应用，课程还将通过案例研究和客座讲座的方式进行教学。教师选择具有代表性的实际案例进行深入分析，帮助学生理解不同安全事件的背景、处理过程和结果。例如，教师讲解某个著名的数据泄露事件，分析事件的发生原因、应对措施及其对企业和用户的影响。通过这些案例，学生可以看到信息安全管理理论在实际环境中的应用和效果。

此外，课程将邀请行业专家和开源社区成员进行客座讲座。这些讲座将涵盖当前信息安全领域的最新动态和发展趋势，提供前沿的实践经验和见解。学生将有机会与专家互动，提出问题，讨论实际工作中的挑战和解决方案。这不仅拓宽了学生的视野和知识面，还帮助他们了解信息安全行业的真实情况，激发他们的学习兴趣，增强职业规划能力。

3.2 国产开源社区功能理解

首先，课程将介绍国产开源社区的基本概念和背景。教师向学生讲授什么是开源社区，国产开源社区的历史背景及其在现代软件开发中的重要地位，解释国产开源社区如何通过协作和共享推动技术创新，提升软件质量，并促进知识的传播和积累。接下来，课程将深入探讨开源软件开发的基本流程，包括项目的启动、规划、执行、监控和收尾。教师将讲解如何制定项目计划、分配任务、管理时间和资源，确保项目按时完成并达到预期目标。

代码提交和代码审查是开源软件开发的重要环节。课程将详细介绍如何使用版本控制系统（如 Git）进行代码提交。学生学习如何创建和管理代码仓库，如何提交代码变更，以及如何使用分支和合并功能来管理代码的不同版本。教师介绍代码提交的流程，包括编写清晰的提交信息、遵循代码风格指南和进行自测。学生还会学习如何进行代码审查。教师将讲解代码审查的目的和流程，包括如何阅读和理解代码变更，如何提供建设性的反馈，以及如何处理代码审查的结果。

版本控制是开源软件开发的核心技术之一。课程将介绍版本控制系统的基本概念和功能，详细讲解如何使用版本控制系统来管理代码的版本历史，跟踪代码变更，并在需要时回滚到之前的版本。学生将学习如何使用标签和发布功能来管理软件的不同发布版本，以及如何处理版本控制中的冲突和合并问题。

此外，课程还会介绍开源社区的组织结构。学生将了解开源项目的不同角色，包括项目维护者、贡献者、提交者和用户等。教师将解释每个角色的职责和权限，以及他们如何在项目中进行有效的协作。学生将学习如何在开源项目中分工合作，包括如何分配任务、如何使用协作工具（如邮件列表、讨论论坛和即时通讯工具）来协调工作。教师将分享开源社区中的最佳实践，帮助学生在实际项目中进行有效的团队协作。

3.3 开源生态安全管理实践

在开源生态安全管理实践阶段，首先需要为学生选择合适的国产开源项目。这一选择过程通常是教师与企业合作，基于当前信息安全需求和学生的专业方向进行的。学生根据自身兴趣和专业背景，在合作企业的开源社区中选择特定的开源项目进行贡献。此外，学生不仅可以进行代码贡献，还可以参与开源社区的管理工作，如项目维护、文档编写和安全审计等。学生在这一过程中担任不同的角色，包括项目维护者、贡献者、安全审计员和社区支持人员等。通常，学生从贡献者开始，通过贡献代码、撰写文档和参与项目讨论等活动等方式积累经验，逐步深入。

期间，教师和企业会定期组织反馈和评估会议，引导学生对实践结果进行总结与反思，包括项目整体情况评估、成果总结、存在问题及改进建议，并进行项目展示和汇报。在总结与反思过程中，学生会自发地思考技术与社会、国家安全等问题，潜移默化地增强学生的社会责任感和爱国情怀。与行业专家和开源社区成员共同探讨信息安全管理最新技术和发展趋势，观摩他们的实践成果，聆听他们分享的经验和心得，使学生亲身感受到身边榜样的力量，激励学生不断挑战自我，追求卓越。

3.4 过程性、多层次教学评价

为了确保基于开源实践的信息安全管理教学方法能够有效实施并达到预期的教学目标，课程采用过程性评价与终结性评价相结合的模式，通过过程性跟踪与多层次观测相结合的方式，实现教学评价的持续改进功能。

开源社区实践分为两个阶段：模拟开源社区阶段和真实开源社区阶段。在模拟开源社区阶段，学生以小组形式在 GitHub 或 Gitee 等平台上搭建并维护开源社区。每个小组成员不仅负责本组开源社区的管理与维护，同时作为参与者积极介入其他小组的社区活动。这一阶段的主要考查学生对开源社区运作机制的熟悉程度，以及协作能力、代码管理能力以及社区治理能力；在真实开源社区阶段，学生在掌握开源社区的基本管理和实践技能后，进一步投身于真实的开源社区.在此阶段，对学生学习情况的考查观测点主要包括代码贡献质量、社区参与度以及技术学习与创新能力。

此外，组织项目展示和答辩，由教师和行业专家评定学生的整体表现。最后，在教师评议的基础上结合学生互评，对学生在团队合作和技术创新等方面的表现进行综合评估。

表 1 关于学生反馈与满意度调查

评价指标	满意（%）	一般（%）	不满意（%）
课程内容认可程度	64.3	25.7	10.0
教学方法满意程度	54.3	31.4	14.3
开源社区实践活动满意度	70.0%	22.9%	7.1%
整体课程综合满意度	65.7%	25.7%	8.6%

为了进一步了解学生的学习体验和对课程的改进建议，教学评价还包括学生反馈与满意度调查。这些调查主要通过问卷和座谈会进行，评价指标包括学生对课程内容的认可度、对教师教学方法的满意度、对

开源社区实践活动的满意度以及对整体课程的综合满意度。

通过问卷调查和座谈会收集的反馈显示，本次信息安全管理课程的教学改革成果显著。学生在学习体验、实践能力提升以及课程满意度等多个方面都给予了积极的评价（见表 1）。

在问卷调查中，有学生分享道：“这是我第一次参与开源社区，之前觉得参与开源社区高不可攀，实际上手后发现并没有想象中那么难。” 这一反馈真实地反映了学生在面对开源社区时心态的转变，从最初的畏惧到逐渐适应，说明课程在激发学生探索精神和提升其解决问题的能力方面取得了成功。

此外，另一名学生表示：“通过这次课程，我对信息安全管理在各个领域的应用有了更深入的理解，尤其是开源社区中的安全实践部分，让我收获颇丰。”这一评价不仅体现了学生对信息安全领域的浓厚兴趣，更进一步证明了教学改革在激发学生自主学习能力方面的积极效果。

图 2 OpenKylin 社区中 CVE-2022-3437 漏洞修复实例

4 教学实践效果

4.1 国产开源社区软件漏洞修复

在开源生态安全管理实践中，课程选择了国产开源社区 OpenKylin 和 OpenHarmony 作为主要实践平台。学生在授课教师的引导下，加入 OpenKylin 和 OpenHarmony 社区，成为正式贡献者，并承担具体项目的 issue，主要参与社区中多个组件的漏洞修复工作。学生首先明确漏洞修复的目标，通过 CVE 通报和项目官方开源渠道等方式获取相关补丁，详细分析漏洞的成因，并基于补丁进行漏洞修复，将修复内容合入项目，完成整个修复流程。以下是具体的实践案例，展示了学生在开源生态安全管理实践中的学习和收获。

案例：OpenKylin 社区中 CVE-2022-3437 漏洞修复

在开始漏洞修复之前，学生具备了 C/C++编程基础、Git 的基本知识并学习了缓冲区溢出漏洞的原理。他们加入 OpenKylin 开源社区并签署贡献者许可协议（CLA），配置开发环境，确保符合社区规范。接下来，学生详细分析了 CVE-2022-3437 漏洞，理解其形成原因和影响范围，并确定造成漏洞的代码文件。

随后，学生通过访问官方库，使用 Git 命令搜索与 CVE 相关的 commit，并生成补丁文件以供修复工作使用。在提取并应用补丁后，学生确保补丁没有冲突，并进行验证测试，确认修复效果。补丁合入后，学生更新项目的 changelog，记录项目名称、更新后的

小版本号、漏洞修复事件、贡献者信息及更新时间，确保版本更新历史和变更详情得到记录。

最后，学生推送代码，并在 Gitee 上提交 Pull Request 进行代码审查。确保代码没有冲突，所有更改符合项目的编码规范和贡献者指南，并清楚描述所做的更改。OpenKylin 社区维护者和核心开发人员进行代码审查，提出改进意见或建议。审核通过后，补丁被合并到项目代码中，漏洞修复工作完成，如图 2 所示。

4.2 使能和促进学生加入并积极贡献开源社区

目前，北京邮电大学是 OpenHarmony 高校技术俱乐部的成员，此外还有院级的 OpenKylin 俱乐部、摇光开源安全协会。北邮 OpenHarmony 技术俱乐部，成员 140 余名，参与了 OpenHarmony 漏洞挖掘、修复、验证工作总计 50 余个，包括静态规则提取和动态 POC 构建。OpenKylin 俱乐部现有 118 名成员，修复了 OpenKylin 平台下近 100 个 CVE 漏洞，这些漏洞涉及 44 个知名的开源组件，如 Git、apache2、bash 和 sudo。该俱乐部日常还与麒麟公司联手组织多种活动，在北京邮电大学举办了 OpenKylin 高校开源沙龙等活动，邀请 OpenKylin 开源社区的知名开发者和学者分享开源项目的开发经验和社区治理模式。摇光开源安全协会现有 178 名成员，定期举办开源安全研讨会、技术分享会和项目实践活动。协会组织学生积极参与校企联合活动。例如，开放原子技术沙龙邀请企业技术专家分享前沿技术和实际案例，华为校园公开课“创新引领未来 · 共建鸿蒙世界”介绍 OpenHarmony 在信息安全管理中的应用，开源春耕计划组织学生参观腾讯公司，使学生了解企业在开源软件开发和管理中的实践经验。

学生踊跃报名中央网信办指导的 2024 年开源安全奖励计划，从原创开源软件、开源漏洞挖掘、开源软件重写到国内开源社区贡献，各自施展课上所掌握的技能为自主开源生态建设做出贡献。

5 结束语

通过深入分析国产开源软件及其社区在信息安全管理教育中的关键作用，提出了一种基于国产开源实践的信息安全管理教学方法，从理论教学、国产开源社区功能理解、开源生态安全管理实践及过程性、多层次教学评价四个主要阶段的教学设计及实践，展示了将国产开源软件纳入信息安全管理实践教学中的有效性。

这种教学改革不仅提高了学生的实际操作和理论知识的应用能力，还促进了他们对信息安全行业的深刻理解和积极参与。通过与国产开源社区的合作，学生能够更好地适应未来的信息安全工作环境，为其职业发展打下坚实的基础，助力国产开源社区高校人才培养，推动开源社区的繁荣与发展。

综上所述，基于开源软件的信息安全管理教学方法为信息安全教育提供了一种创新且有效的解决方案。随着信息安全挑战的不断增加，这种实践导向的教学模式将有助于培养更多具有实际操作能力和创新思维的信息安全专业人才，推动信息安全教育的持续发展。

参 考 文 献

[1] 钟雷,刘温国.2021 年全球网络空间安全态势综述[J].保密科学技术,2021(12):5-11.

[2] 徐洪峰,陶志勇.企业信息安全管理体系研究[J].现代信息科技,2020,4(17):139-141+144.

[3] 韩鹃,宋晓峰,王玉芳,等.信息安全技术课程思政建设的探索与实践[J].计算机技术与教育学报,2021,第 9 卷(1):38-42.

[4] 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(08):109-110.

[5] 黄启春.基于特色项目制与开源人才培养的软件工程专业学位研究生创新能力培养实践[J].中国信息界,2024(02):25-27.

[6] 邓燕萍.共筑开源生态，赋能千行百业[J].产城,2023(11):42-45.

[7] 乔文豹,李宁,梁旭,等.开源运动和 ChatGPT 引起的高校跨专业计算机教育改革[J].计算机技术与教育学报,2023,第 11 卷(4):61-65.

[8] 黄鑫. 中国开源软件前景光明[N]. 经济日报,2023-12-29(006).

[9] 夏小雅,赵生宇,韩凡宇,等.面向开源协作数字生态的信息服务与数据挖掘[J/OL].计算机科学:1-13[2024-05-23].

[10] 王学伟,冯峥,束克东.开源创新研究动态与展望[J].商丘师范学院学报,2023,39(10):71-78.

[11] 李攀攀,朱蓉,杜选,等.基于开源软件的网络空间安全专业实践教学探索[J].嘉兴学院学报,2021,33(01):140-144.

[12] 荆琦,冯惠.产教融合下的双轨制开源教学模式探索——以北京大学“开源软件开发基础及实践”课程为例[J].高等工程教育研究,2023(01):14-19+66.

[13] 林涛.基于开源理念的信息类专业人才培养探究[J].中国标准化,2022(22):218-222+226.