 DOI: https://doi.org/10.12345/jxffcxysj.v7i5.16516

Discussion on Ideological and Political Education of Network Security Application Courses in the Era of Classified Protection 2.0 of Cybersecurity

Jianhui Li

Software Engineering Institute of Guangzhou, Guangzhou, Guangdong, 510990, China

Abstract

In the era of network security level protection 2.0, in order to better cultivate the comprehensive quality of network security technical talents, this paper proposes the combination of network security level protection with ideological and political courses in the teaching process of network security application course, the ideological and political teaching of the network security application curriculum is planned and launched from the overall level of the network security application curriculum group, for network programming courses, network security attack and defense and penetration courses, and network security assessment courses, integrate different curriculum ideological and political elements from different levels, and combine with the characteristics of the professional, integrating grade protection standards and norms, relevant laws and regulations and socialist core values, that is, from surface to point implementation, and then to achieve the teaching effect from the point to surface.

Keywords

level protection; ideological and political courses; network security

等保 2.0 时代网安应用课程思政教学探讨

李检辉

广州软件学院，中国·广东 广州 510990

摘　要

在网络安全等级保护2.0时代，为了更好地培养网络安全技术人才的综合素养，提出了在网络安全应用课程的教学过程中将网络安全等级保护与课程思政相结合，从网络安全应用课程群的整体层面来规划和开展网络安全课程思政教学，对网络编程类课程、网络安全攻防与渗透类课程以及网络安全测评类课程，从不同层面融合不同的课程思政元素，并结合专业的特点，有侧重地在这三类课程中分别融入等级保护标准规范、相关的法律法规和社会主义核心价值观，即从面到点实施，进而达到从点到面的教学成效。

关键词

等级保护；课程思政；网络安全

1 引言

2017 年实施的《中华人民共和国网络安全法》正式宣告在网络空间安全领域，中国将网络安全等级保护制度作为基本国策，等级保护进入 2.0 时代 [1]；2019 年 12 月，网络安全等级保护新的标准体系（等保 2.0）开始实施，以适应新技术的发展，解决云计算、物联网、移动互联和工控领域对网络安全等级保护工作的需求，扩展了网络安全等级保护的广度和深度，网络安全行业的业务也随着快速增长，有些网络安全测评机构的业务量增长达到 300%，这在一定程度上反映出越来越多的信息系统运营或使用单位正在开展和落实等级保护工作。

【基金项目】广州软件学院校级“一师一优”项目——网络安全测评（项目编号：NT3006）；广州软件学院校级“质量工程”建设项目–广州软件学院–广州腾科网络技术有限公司网络工程科产教融合实践教学基地（项目编号：SJJD202204）。

【作者简介】李检辉（1981–），男，中国广东梅州人，硕士，讲师，从事计算机应用技术、信息安全技术研究。

2 等保 2.0 时代课程思政教学的重要性

在等保 2.0 背景下，大力培养符合网络空间安全时代要求的人才，不仅仅是企业的需求，也是国家建设网络安全保障体系的需求。然而，网络安全技术是一把双刃剑 [2]，既可以服务社会，也可能成为网络攻击者危害国家、社会或个人安全的工具。在网络安全人才培养过程中，不仅要聚焦于培

养什么样的人和如何培养人，更重要的是为谁培养人[3]，需要特别关注所培养的人才是否能一直为国家的网络安全建设服务。因此，应有目的、有计划地在网络安全专业技术教学中引导学生树立正确价值观，培养科学精神和创新精神，提升网络安全意识和法律法规知识水平，而这正是当前课程思政教学的元素。在网络空间里，如果将网络安全人才比作地球的话，那么，专业技术可以看作是太阳的光和能，思政则是月亮。而这颗月亮正是网络安全人才背后的光明，引领着他们在黑暗中不迷失方向。

3 等保 2.0 与思政教学相结合

网络安全等级保护是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。为了开展网络安全等级保护工作，国家制定了一系列等级保护的标准要求，并出台了相应的法律法规。标准要求是国家网络安全建设的规范，而法律法规是标准要求得以实施的保障。法律是一种完善的道德，起到普遍伦理价值准则的作用，在道德的基础上加上一个强力制裁，从而弥补道德的天然缺陷[4]。因此，这些标准要求和法律法规不仅是等级保护教育的重要内容，也是思政教育的重要内容，如图 1 所示。

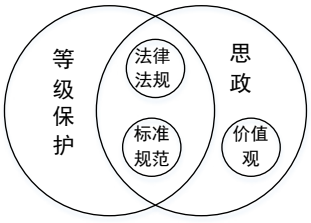

图 1 等级保护与思政教学

同时，等级保护工作的落实离不开社会主义核心价值观。在网络安全专业课程教学中，应进行社会主义核心价值观教育，才能引导网络安全人才更好地遵守法律法规及执行国家的标准规范。中华人民共和国网络安全法规定“国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施增强全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境”。

4 等保 2.0 与思政教学融入设计

在专业课程教学中，首先要把专业知识教好，才能真正体现出专业课程的特点和优势。并在此基础上，使这门专业课程起到一定的思想政治教育作用[5]。在课程思政教学中，应分清主次。根据专业培养计划，每门专业课程的学时是既定的，并不充溢，因此，在教学设计时，应将网络安全应用课程系列看作一个整体，针对不同类型的课程，有重点地结合不同思政教学元素，从面到点实施思政教学内容，从点到面完成思政教学成效。依照等级保护的不同工作环节，可将网络安全的应用课程分成以下三类课程：网络编程类、攻防与渗透类和安全测评类。结合专业的特点，将等级保护和课程思政相结合，有侧重地在这三类课程中融入标准规范、法律法规和价值观教育。如图 2 所示网络安全应用课程与思政教学融合点关系图。

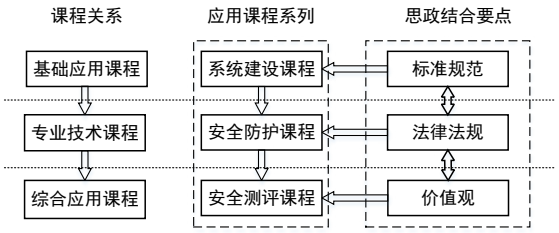

图 2 网络安全应用课程与思政教学融合点关系图

①网络编程是基础应用课程，是建设网络应用系统的基础。在这类课程中结合国家标准规范，是完善专业技术教育的需要，中华人民共和国网络安全法规定“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求”。因此，将标准规范作为这类课程的思政元素融入教学时，可以水到渠成。

②攻防渗透课程属于专业技术核心课程。攻防渗透技术是网络应用系统的防护手段，是国家建设网络安全体系的保障。在这类课程中结合法律法规教育，是这类课程思政教学的重心。通过提升学生的法律意识，合法合规地应用安全技术与安全工具，为国家网络安全建设服务。

③安全测评课程属于综合应用课程。安全测评是对网络安全应用系统进行安全管理的措施。测评是一种合规的工作，工作人员坚持正确的价值观，才能保证这种合规的公平公正。在测评课程中结合社会主义核心价值观教育，提升网络安全测评人员综合素养，是测评岗位的要求。

4.1 网络编程课程与标准规范

在等保 2.0 时代，网络应用系统建设单位在系统的整个生命周期都需要开展等级保护的工作。网络应用系统的设计，不单单是满足业务功能需求，还要合规，即达到网络安全等级保护的要求。因此，在系统设计开发阶段就必须重视安全功能的实现，而不是在等级保护测评不达标后再进行整改。

然而，网络编程课程基本上只是针对应用系统业务功能的教学，涉及到法律法规知识很少。在网络安全系列课程中，编程课程属于基础类课程，前期课程中只有网络安全技术基础课中有相关法律法规的概述，而涉及等级保护的安全测评与风险评估课程是属于后期的综合课。在目前排名较前的线上学习网站，如中国大学 MOOC、慕课网等，还搜索不到网络安全等级保护直接相关的课程；而腾讯课堂也只有一门由安全技术公司发布的等级测评师培训课程。

在这种环境下，编程课的学生对网络安全等级保护制

度与网络应用系统的关系认识不足，甚至有些学生对等级保护的认知处于零水平。从学生的实训作品、竞赛作品以及毕业设计中发现，多数作品业务功能虽完善，但是安全方面非常薄弱，甚至连身份鉴别的口令复杂度都没有考虑，而这个只是等级保护二级系统的一个最基本的指标要求；对于通信程序，多数学生还停留在 HTTP 协议时代，不懂得或从未考虑过在设计中应用安全的通信协议。

因此，针对这类课程，应有计划地以课程思政的方式，在教学中融入等级保护的知识，尤其是信息安全技术网络安全等级保护安全设计技术要求。可以从以下几个方面展开：

①网络安全专业的编程课以网络编程为主，所以可以将等级保护基本要求中的通用要求指标与编程的主要模块进行对标教学，包括身份鉴别、访问控制、日志审计、安全通信以及数据备份等。

②由于等级保护 2.0 涉及面广，内容较多，在有限的课时中通过课程思政的方式融入等级保护的内容还是不够的。所以，可以通过选修课的形式开设“网络安全等级保护”课程，这不但可以让网络安全专业的学生受益，也有利于网络工程与软件工程的学生更好地去理解网络安全等级保护，从而提升安全编程敏感度。

③同时，也要注重师资水平的提升。大多数编程课的教师主要还是专注于编程本身，对网络安全技术掌握得较少，因此，首先需要对这些教师进行等级保护的培训，同时在思政教学设计过程中，也需要网络安全专任教师的指导，可以通过成立安全编程教研室方式进行。只有这样，才能更好地将等级保护的知识融入编程的各个模块中。

4.2 攻防渗透课程与法律法规

在与安全技术企业学术交流中，企业非常强调技术人员的法律意识以及对政治的敏感度。如果安全技术人员没有坚定的信念，很容易游走在网络灰色地带。对于企业来说，一个安全技术人员稍有不慎，给企业带来的损失远大于其所能带来的效益，而且安全的修复花费甚至不可估量。近几年，内部员工恶意操作导致的安全事件频出，如员工利用安全技术将“爬虫”程序植入网站删除相关数据代码、内部员工因不满上司利用掌握的访问权限删除服务器数据库等，给企业带来巨大损失。

网络安全专业课程中，攻防与渗透类课程是比较核心的技术应用课程，如 WEB 安全防护、网络安全攻防、渗透测试等等，主要学习安全技术应用与安全工具应用。安全技术与安全工具既可能沦为黑客犯罪助攻，也可以是网络安全护手，这完全在于网络安全人员能否在工作中合法地使用它。因此，在教学中，要适当地融入法律法规要求，厘清政治红线、法律底线和道德底线 [6]，增强学生的法律意识和安全意识，提高学生对可为与不可为的判别能力。

多数专业教师或多或少地都有在课堂上引入相关的法律条例，但是没有系统地、有计划地将其融入教学中去。以课程思政的形式，将相关法律条例的讲解作为思政教学元素，恰到好处。可以结合个人信息保护法，网络安全法以及地方条例，从以下几个方面展开：

①有关网络安全技术的教学，如身份鉴别、访问控制等，可结合信息安全条例中的规定“未经允许进入计算机信息系统或者非法占有、使用、窃取计算机信息系统资源”“窃取、骗取、夺取计算机信息系统控制权”“窃取他人账号和密码，或者擅自向第三方公开他人账号和密码”等，告诫学生不能利用譬如口令破解技术、漏洞分析利用技术、服务器提权技术去非法入侵计算机。

②有关安全工具的应用方面，如协议分析工具、数据包拦截工具等等，可结合安全条例中的规定“未经允许，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改或者增加”，以及网络安全法中的“任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法”等。

③攻防课程的应用性强，学生群体思维方式较为直接 [6]。在攻防课堂上，单纯的思政理论灌输显得生硬。因此，在教学设计中，适当地通过一些反面案例进行法律法规解读，比如，2018 年，某知名企业的安全工程师郑某到新加坡参加 CTF 比赛，在入住酒店后，利用安全技术及工具破解了酒店 WIFI 服务器的管理员密码，并将该密码和服务器的漏洞信息公布于其个人博客上。该博文引起了新加坡网络安全局（CSA）的注意，随后郑某被新加坡国家法院判罚 5000 美元。郑某的行为或是源自好奇与炫耀，然而这种“无法律意识”却很可能被他人用于非法目的，给酒店造成严重损失。这种案例对学生有非常直接的警醒作用，同时也能够调节课堂气氛，提升学生的专注度。

4.3 安全测评课程与价值观

网络安全测评主要包括等级测评和风险评估，基于国家等级保护基本要求，是一种合规性的工作，从业人员必须具备正确的价值观，才能在安全测评工作中坚持严肃工作作风和科学精神，以体现测评的客观性、科学性和公正性。在专业教学中，应加强社会主义核心价值观教育，促使学生养成严谨的处世态度和敬业守信的职业素养。由于网络安全类课程教师本身理工科出身，在教学过程中本能地注重知识与技能的传授，容易忽略人文精神的宣扬 [7]。因此，以课程思政为契机，有计划在专业教学中融入价值观的教育。可以从测评工作的以下环节展开：

①测评实施环节。在网络安全测评实施过程中，测评人员可以获得授权对被测评企业进行漏洞扫描及渗透测试。因此在教学中，要引导学生充分地理解测评工作应合法合规地开展，在测评工作中务必要有严谨的态度，否则“一不小心”就有可能犯罪了。在宁川非授权渗透测试案例中，某网络科技公司的员工李某在负责向运营商提供等级保护测评业务时，获得了官方授权，可以对目标网站进行网络渗透测

试，这本属于正常业务行为。但是这个官方授权的时间是有明确的时间范围的，而李某恰在未授权的时间段内对网站进行渗透测试，造成网站系统运行不正常。这种行为已经违反了《中华人民共和国网络安全法》第 27 条规定：“任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。”已构成《中华人民共和国刑法》第 285 条的非法侵入计算机信息系统罪，然而李某却没有意识到自己的违法行为。

②测评信息处理环节。测评人员在测评工作中需要收集被测评企业的信息，可以接触到被测评企业的商业秘密，以及在测评中获得敏感信息和漏洞信息。因此，测评机构会与委托单位签署保密协议，要求测评机构不得泄露在等级测评服务中知悉的商业秘密、重要敏感信息和个人信息；不得擅自发布、披露在测评服务中收集的网络信息、系统漏洞等网络安全信息等等。而测评机构通常也会与测评人员签订安全保密责任书，明确测评人员的安全保密义务和法律责任；各地方安全保护条例也有相关的规定，比如《广东省计算机信息系统安全保护条例》第三十一条明确指出，计算机信息系统安全等级测评机构等安全服务机构和从事计算机信息系统安全保护工作的人员应当保守用户秘密，不得擅自向第三方泄露用户信息，不得非法占有、使用用户的信息资源。虽然有诸多法律层面的限制，但是在实际的测评工作中，测评人员能否严格遵守协议规定保密数据，是否会经不起诱惑利用所得信息去获得不当得利，还在于测评人员是否有正确的价值观和职业道德修养水平。

③测评报告环节。出具测评报告是测评工作的最后环节。在等保 2.0 的背景下，测评业务需求急增，测评机构也越来越多，测评机构因违规被处罚的事件频发，主要是因为测评机构在出具测评报告时，未能做到公平公正。2018 年，成都某信息技术服务有限公司对客户网站进行安全测评时，弄虚作假，未如实出具测评报告，测评分数虚高，使得一些本应当提前可以修复的网络安全隐患漏洞没有得到有效处置，导致网站被黑客攻击入侵后无法追踪溯源。

5 结语

在网络空间安全阶段，国家级的网络攻击不断增加，网络安全风险正在不断增加。网络空间安全人才是国家提升网络空间安全竞争力的决定性力量，网络空间安全人才培养也上升到了国家战略的高度 [8]。因此，对于安全技术人员的综合素质培养的要求也愈加严格。在人才培养中结合思政教学，是中国社会主义特色教育的方向和要求，也是在等保 2.0 时代培养符合网络空间安全人才的有效途径。在课程思政教学融入设计中，根据网络安全应用课程的特点，通过以面到点的方式切入，针对不同类型的课程，融入不同的思政要素，从而达到以点到面的思政教学成效，以培养具有综合素质的安全技术人才。

参考文献

[1] 王斯梁,冯暄,蔡友保,等.等保2.0下的网络安全态势感知方案研究[J].信息安全研究,2019(9):828-833.

[2] 李古月,胡爱群.网络空间安全专业课程思政教学探索与实践——以东南大学“网络空间安全新进展”课程为例[J].网络与信息安全学报,2022(2):183-189.

[3] 王学俭.新时代课程思政的内涵、特点、难点及应对策略[J].陕西现代职业教育研究,2020(3):131-136.

[4] 戴茂堂.论道德法律化之误[J].理论学刊,2007(12):66.

[5] 刘建军.课程思政:内涵、特点与路径[J].教育研究,2020,41(9):28-33.

[6] 鲁艳蓉.网络空间安全专业课程思政融合路径探究[J].计算机教育,2022(6):1-4+9.

[7] 张延红,王海洲,朱春.计算机类课程思政实践探索——以计算机网络课程为例[J].计算机教育,2020(5):93-96.

[8] 李晖,张宁.网络空间安全学科人才培养之思考[J].网络与信息安全学报,2015,1(1):18-23.