

DOI: 10.13678/j.cnki.issn1674-5531.2014.03.013

军校学员信息安全素养 培育体系构建研究

马明田, 李石磊, 欧庆于, 叶清, 杨金宝, 周大伟

(海军工程大学 信息安全系, 武汉 430033)

摘要: 从学员岗位任职能力要求出发, 围绕培养目标、内容、途径、评价、支撑环境五个方面, 对军校学员信息安全素养培育体系构建进行了研究, 为创新发展传统保密安全教育内容、形式, 提高军校学员信息安全保密素养提供了有益参考。

关键词: 军校学员; 信息安全; 素养; 培育体系

中图分类号: E251.3

文献标志码: A

文章编号: 1674-5531(2014)03-0057-05

Construction of cultivating system of information security accomplishment for cadets

MA Ming-tian, LI Shi-lei, OU Qing-yu, YE Qing, YANG Jin-bao, ZHOU Da-wei

(Dept. of Information Security, Naval Univ. of Engineering, Wuhan 430033, China)

Abstract: Based on the connotation of the information security accomplishment and the requirements of the working duty, the construction of the cultivating system of the information security accomplishment is presented with focus on the following aspects: goal, content, approach, evaluation and supporting environment. The proposed cultivating system can innovate both the content and the format of the traditional secrecy-maintained education and provide valuable references to enhance the information security accomplishment of cadets.

Key words: cadets; information security; accomplishment; cultivating system

当前, 信息技术迅猛发展, 涉密载体日益数字化、网络化、轻便化、隐性化, 军事秘密存储处理和传输环节隐患明显增多, 技术泄密风险加大。据统计, 世界主要国家军事秘密信息的泄露, 有80%以上是通过信息系统网络造成的。究其原因, 又有80%以上是由于内部操作人员信息安全意识淡薄、防范知识欠缺, 违规操作、违反制度和

疏忽大意造成的。军校学员肩负着打赢未来信息化战争的重任, 其保密素质的高低影响着军队信息化建设的成败。因此, 笔者认为将信息安全教育纳入军校教育训练内容, 科学构建军校学员的信息安全素养培育体系, 对于积极应对当前严峻、复杂的国际形势, 打好防间保密主动仗具有重要的基础性、前瞻性的作用。

收稿日期: 2014-05-30; 修回日期: 2014-07-16。

基金项目: 海军工程大学教育科研基金资助项目(NUE2013209)。

作者简介: 马明田(1960—), 男, 高级工程师。

一、信息安全素养的内涵及军校学员信息安全素养岗位任职的能力要求

(一) 军校学员信息安全素养内涵

信息安全素养内涵来源于信息素养的概念,是指在信息化条件下,人们对信息安全的认识,以及对信息安全所表现出来的各种综合能力,包括信息安全意识、信息安全知识、信息安全能力、信息伦理道德等具体内容^[1]。对于军人而言,信息安全素养可具体化为针对维护军事秘密信息安全所表现出来的察觉、识别、发现和解决当前存在的信息安全问题的能力,并内化为规范自身安全行为的修养,具体包括意识、知识、技能、法律、道德等方面的综合素质。作为信息安全素养的五个核心要素,意识起先导作用,知识起基础作用,技能起核心作用,法律起规范和威慑作用,道德起导向作用。

(二) 军校学员信息安全素养岗位任职要求

面对当前海上维权斗争日趋尖锐,敌对势力加紧对我国实施战略遏制和围堵,泄密形式多样化的严峻形势,军事信息保密已经成为涉及国家安全、国防建设的重大课题,加速构建军事信息安全保密综合防范体系是一项迫在眉睫的战略性工作。而我军人员的信息安全素养将处于基础性支撑地位,信息安全素养已从军校学员军事素养的隐性部分提升至显性部分,成为学员日常学习、生活及未来工作的必然要求。为积极适应信息技术迅猛发展的新形势,必须从“根”上抓起,通过科学构建学员信息安全素养培育体系,使其增强保密观念、敌情意识,熟悉保密法规要求,掌握必要的保密知识、方法、技能,从而为履行保密职责义务、执行保密法规、做好保密工作打牢思想和工作基础。

二、完善军校学员信息安全素养培育体系的对策

信息安全素养培育体系,从根本上讲涉及“培育什么样的人”及“怎样培育人”两方面的命题。与专业化背景下的信息安全学科教育不同,信息安全素养教育的侧重点将不仅是教会一种技术,更是传授一种观念和思考问题的方法,内容涵盖

面广,知识体系更新迅速。因此,必须以满足不同岗位人才的多种保密需求为宗旨,以多元的人才培育目标为取向,采取多样的培育、评价方式,从而达到提升教育绩效的目的。秉承以人为本、素质教育、多样化和系统性的现代教育理念,重点从培育目标、内容、途径、评价、支撑环境五个方面进行构建。

(一) 确立军校学员信息安全素养培育多元目标体系

培育目标是指通过培育教育活动,使培育对象达到基本要求和规格标准,是其余要素运行的基石和指导。依据素质教育理念,培育目标应包括认知目标、技能目标、情感目标,要坚持摒弃以往以知识目标为主、学生靠死记硬背实现学习目标的局面,形成多元目标的立体式培养格局。因此,结合信息安全素养内涵,军校学员信息安全素养培育目标从认知、技能、情感三个层面可统一描述为:以学员自身发展需求作为基本出发点,使学员了解军事信息安全的基本概念,认清信息安全面临的复杂形势,了解信息的泄露与丢失对国家和军队造成的巨大危害,切实筑牢保密思想防线;熟悉常用涉密载体的物理安全保密技术与方法,掌握有关信息技术的安全隐患和防止失泄密的方法、手段;熟悉信息安全保密法律法规、技术标准和规章制度的主要内容;了解信息安全保密管理基本方法、主要措施和手段,最终在普及信息安全保密知识、提高信息安全意识的基础上,培育学员的信息安全保密素养。

(二) 丰富军校学员信息安全素养培育内容体系

培育内容是培育体系的核心,是培育目标的具体体现。信息安全素养的培育不同于特定专业或学历教育,根据信息安全素养的内涵,重点应培养学员良好的信息安全思维方式和日常操作习惯,主要包含以下五个方面^[2-3]。

1. 信息安全保密意识。主要表现为对信息安全保密重要性的认识以及在工作、生活中对相关内容的敏感性。重要性认识主要包括对信息安全保密重要作用与地位的认识,认可信息安全保密对学员学习、科研、生活、工作的重要性,以及对国家、军队、单位的重要意义。敏感性主要包括对信

息安全保密问题的警觉程度,对违法、违规、误操作的行为及其导致的对国家、军队和个人造成危害性的警觉程度,同时还应包括对信息安全保密学习的主动程度,主动关注保密法规、保密案例、保密工具等方面的主题以及能够主动学习保密方面的新知识、新技术等。

2. 信息安全保密知识。主要涉及信息安全保密工作相关的理论与技能等基础知识。基础理论知识主要包括两点:一是信息安全保密的基本知识,如信息安全保密的内涵、属性、发展趋势、地位作用等;二是军队保密工作的基本知识,如军事秘密的内涵、构成要素、存在方式、划分等级等。随着信息技术的发展,技能基础知识主要包括涉密载体、通信及网络信息三个方面的内容:一是涉密载体的安全隐患和防护知识,如窃听、窃照的基本概念及防窃听、防窃照的基本方法,保密区域安全防护的基本要求,涉密文档的管理要求,计算机防电磁辐射泄密,信息设备防内置的具体方法等;二是通信信息的安全隐患和防护知识,如电话网、移动通信网、蓝牙通信网、无线局域网的信息安全保密隐患、防护技术及使用管理要求等;三是网络信息的安全隐患和防护知识,如计算机终端和网络安全面临的主要威胁、防护技术及使用管理要求等。

3. 信息安全保密技能。传统的保密教育原理性、说教性内容较多,使学员丧失学习的积极性,需要按照学以致用原则,强化保密技能培育。信息安全保密技能主要包括信息安全工具的使用能力与信息安全的处理能力。信息安全工具的使用能力又包括两个方面:一是设置与防御能力,能够正确设置操作系统的三级密码,安装防护软件,设置浏览器的安全级别,邮件系统的过滤功能,定期整理和备份重要资料并存放至安全介质等;二是检测与发现的能力,能够利用防护软件及时检测操作系统及软件是否存在漏洞,存储介质、E-mail 及其附件是否存在病毒,以及能够利用相关知识、技能判断和识别出危险及不良网站等。信息的安全处理能力包括两方面内容:一是反应与分析的能力,能够在终端设备遭受物理故障或系统受病毒攻击时快速做出反应等;二是解决与恢复的能力,能够备份和恢复系统、重新安装或恢复

常用软件,正确使用数据恢复软件等。

4. 信息安全保密法律知识。主要涉及对国家、军队相关法律的了解及严格遵守。在国家层面,要了解并自觉遵守《刑法》《保密法》《保守国家秘密法实施办法》等法律条文中有关保密的规定与措施;在军队层面,要了解并自觉遵守《保密条例》、“三大条令”中的相关保密条款、秘密载体管理制度及相关规定等;在单位层面,要自觉遵守有关终端安全、网络使用、信息传输等的保密规章制度,遵守使用电话网、无线局域网、蓝牙等的管理要求,以及使用互联网的保密要求等。

5. 信息安全保密道德规范。指个体成员在信息获取、使用、创造和传播过程中应该遵守一定的伦理规范,不得危害他人信息安全。即主要涉及个人自律能力的培育,一方面严格要求自己按保密要求规范使用信息资源、设备、系统和设施以及不随意泄露个人信息等;另一方面,自觉对不良行为进行抵制,不利用网络从事危害国家安全、泄露国家秘密等违法犯罪的活动以及不制作、复制、查阅、传播思想反动和内容不健康的信息,能及时认识和改正不良的安全保密行为和习惯等。

上述五个方面内容相辅相成,构成一个统一完整的内容体系,军校应按照学用相结合、注重实效的要求,在摸清军队各级岗位人员信息安全素养基本要求的前提下,针对工作、生活需求与军校学员当前能力、素养的差距,完善课程标准,增补教学内容,努力体现出培育内容体系的基础性、适用性、先进性、科学性和前瞻性。同时,由于信息安全保密技术发展日新月异,因此信息安全素养培育教学内容必须经常更新,要能够反映出最新的保密形势以及科研成果,才能使教学效果具有现实意义。

(三) 创新军校学员信息安全素养培育体系

培育体系是培育对象在培育过程中进入和参与一系列认识与实践活动的系统过程。在教学实施过程中,关键是充分调动教学对象的积极性,变被动教育为自我教育,使信息安全素养的培育与提高变成学员的自觉追求。因此,需要重点从教学活动的组织安排和教学方法的创新两方面来构建信息安全素养培育体系。

1. 教学活动的组织安排。在内容安排上,可

针对不同教学对象,采用不同的教学内容,组织相适应的教学实施计划,达到重点突出、层次分明的效果。可采用模块化、层次化、专题化思路,将教学内容划分为保密常识(包括现有的保密法规、制度,主要的失泄密途径和隐患等)、保密理论(包括保密管理的内容、方法和程序等)、保密技能(包括载体保密、网络保密、通信保密等)、前沿技术探索、保密实践多个层次,设置“专题精讲、演示实践、网络自学、研讨交流、综合演练及参观见学”等多个教学模块,突出其综合性、实践性和应用性^[4]。

保密素养的培育不可能“一蹴而就”,因此在时间安排上,可将整个在校学习期间分阶段、分层次进行,使军校学员在学习过程中,信息安全素养培育工作不断档,并实现整体强化效果。教育形式可大体分为入学保密教育、计算机公共课程、信息安全保密课程、主题教育和毕业保密教育等。其中,入学保密教育主要介绍当前我军保密工作面临的复杂形式、信息安全保密的主要威胁、失泄密案例分析与安全防范以及军队的有关保密规定。通过教育,使学员增强对安全保密工作和维护国家国防安全的重要性的认识,提高其对信息安全和保密问题的敏感性,为学员今后学习和工作打下良好的保密基础。同时,针对传统计算机公共课程重应用、轻安全,缺乏相关安全知识内容的问题,在诸如计算机文化基础、办公自动化、网页制作、数据库等相关课程中增加相关信息安全法律法规和道德伦理、信息安全知识与技能等内容。如操作系统安全配置方法、计算机病毒的防范与查杀、电子商务站点安全构建等,使学员在工作和日常生活中养成重视信息安全要求的意识并具备相关能力。信息安全保密课程是军队院校的一门军事基础必修课,可系统介绍军队保密工作基本情况,涉密实体、通信系统与计算机网络信息安全保密技术,信息安全保密法规体系与管理。主题教育主要以贴近学员日常生活的信息安全主题形式开展,选择某一技术主题或当前最新的热点信息安全问题,采用专题讲座或网络自学等多种方式进行,加深学员对某一技术专题的理解。毕业保密教育在学员毕业前夕进行,主要介绍信息安全保密工作法规体系与组织管理机制,警示

毕业生要时刻绷紧“保密”这根弦,遵守保密法规,增强保密观念。

2. 教学方法的创新综合。在教学实施过程中,要充分调动军校学员的积极性,变被动教育为自我教育。灵活运用研讨式、案例式、推演式、探究式、情景式、问题式等教学方法,开展多种形式相结合的课堂教学实践探索研究。在课堂中进行安全教育,结合当代军校学员的心理特点,突出学员最想了解的重点、难点问题,注意发挥其主体性和参与性,变灌输式教学为启发式教学。通过教员和学员一起交流讨论、发表意见,透过热点时事将学员的学习兴趣引入到课程学习中,最终达到提高教学效果的目的。

(四) 完善军校学员信息安全素养培育评价体系

培育评价是培育模式的调控性因素,对培育模式其余要素进行监控,目的是通过调节与反馈,促进培育模式各环节的优化组合以提高培育质量。军校要改革评价考核方式,将以课程结束考试为主向“多次”综合衡量转变,坚持总结性评价和形成性评价相结合,坚持自我评价和他人评价相结合,推广专题答辩、综合作业等考核方式,结合能否从技术层面理解并自觉严格遵守相关保密规定等综合评定,实现由书本知识向自身信息安全防护能力的转变。同时,要结合军校学习生活实际,进行各种形式的保密检查,通过保密检查,监督保密法律法规的贯彻执行情况,检查学生的具体保密行为是否符合保密法规的要求、保密设施的配置和保密环境的情况,以及有无泄密事件的发生及对泄密事件的查处情况。在检查中发现、解决问题,通过此途径,评价学生的保密素养,并起到督促和提升作用。

(五) 建设军校学员信息安全素养培育环境体系

军校学员信息安全素养的培育离不开保障资源和相应组织机制的支持,主要应做好以下三个方面工作。

1. 积极配置软硬件资源条件。保密教育的具体实施方式和方法从某种程度上决定着学员对教育内容的接受效果,而信息安全素养的培育,需要各种软硬件资源的支持。一方面,可设计窃密与

保密技术演示实验,让教育对象亲身体验各类泄密隐患和威胁的技术演示,通过技术原理的深刻揭示和“亲眼目睹”整个泄密过程的发生,使教育对象心理产生强烈触发、震动,使其不仅对信息化条件下强化保密管理的意义有更深刻的理解,更对学习、掌握保密知识与防范技能产生主动性和紧迫感;另一方面,借助具体软硬件资源,为学员搭建一个实践操作平台,提高他们的动手能力和在实际环境中发现问题、解决问题的能力,有效地加深学员对信息安全保密知识的理解,为学员未来工作积累宝贵的经验,并打下坚实的基础。

2. 完善多部门组织协调机制。信息安全素养培育涉及内容范围广、时间跨度长,因此军校内部各部门应建立完善的组织协调机制,多渠道、多方式建立信息安全素养培育的长效机制。如教务部门应积极承担协调本科学员信息安全素养各个阶段的培养计划及实施安排;组织、协调相关教员和学员参加信息安全素养培育的宣讲;检查本科学员信息安全知识考查、素养测验、综合测评的实施情况与工作质量等。保密、保卫部门作为学校保密和安全工作主管部门,应负责组织、实施保密知识竞赛、保密教育月(周)等形式多样的信息安全保密宣传活动。教育技术中心作为学校信息资源整合以及优质资源开发部门,应协助教学实施单位设计和制作信息安全警示教育片、信息安全保密网站等。承担信息安全保密课程的相关教研室,应积极和上述部门合作,关注最前沿的知识动态,收集、更新、整理对于教学有意义的信息,努力探讨加强军校学员信息安全素养培育的策略、方法、途径,确保教学实效。

3. 构建文化氛围环境。学校可利用网络、广播、报刊、图片展览等新闻舆论工具开展信息安全和保密宣传教育。举办保密专题讲座、保密知识竞赛、保密教育月(周)、保密技术与设备成果展,组织学员观看计算机安全警示教育资料片、相关的谍战影片,利用学校的宣传栏、展板、橱窗张贴《保密法》图解、相关信息安全保密条令条例,举办

信息安全和保密图片展、保密知识问卷调查,订购保密杂志、发送保密知识手册、印发保密教育宣传材料,每年定期举行信息安全与保密培训,开展信息安全保密普法教育,举办网络价值观的辩论赛、讨论会,营造良好的文化氛围环境,帮助学员树立信息安全和保密意识,掌握相关知识,提高防范及处理能力,规范信息安全保密行为并养成良好的习惯。

三、结束语

随着社会和军队信息化建设迅猛发展,军队每一位成员基本都拥有自己的电脑、智能手机等各类上网终端,军队各类信息系统也已嵌入到各个单位、部门和作战单元。网络在工作、学习、生活中无处不在,网络失泄密的风险进一步加大,从固定终端发展到移动终端领域,全面提高军校学员信息安全素养已迫在眉睫。从军队信息化建设的实际需求出发,以学员为主体,围绕培育目标、内容、途径、评价、支撑环境多个要素,努力构建集知识传授、能力培育和素质教育于一体的信息安全素养培育体系,使受教育者产生心理认同,变被动要求为自觉行动,对于做好新形势下的军校学员信息安全教育工作,切实提高军校学员信息安全素养具有重要的现实意义。

参考文献:

- [1] 刘枫. 大学生信息安全素养分析与形成 [J]. 计算机教育, 2010, 10(21): 77-80.
- [2] 沈霞娟, 高东怀, 许浩, 等. 大学生信息安全素质教育探索 [J]. 信息安全与通信保密, 2014(3): 54-55.
- [3] 路程伊, 杨诏旭, 谢百治. 本科生信息安全保密素养多元培养模式的探索与实践 [J]. 中国医学教育技术, 2012, 26(6): 629-632.
- [4] 周萌, 樊强, 李大维, 等. 新形势下军队院校保密教育工作的几点思考 [J]. 海军工程大学学报(综合版), 2013, 10(4): 49-51.