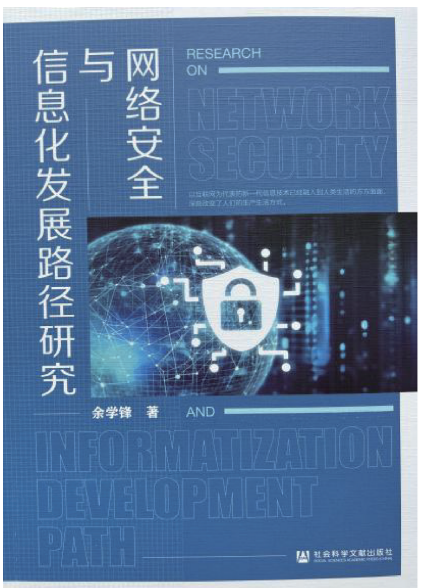
高校信息化安全管理问题与对策
——评《网络安全与信息化发展路径研究》

随着信息技术的飞速发展,高校信息化建设已经成为提高教育质量、培养创新人才的重要手段。然而,信息化带来便捷性和高效性的同时,也伴随着诸多安全隐患。如何确保高校信息系统的安全稳定运行,成为了亟待解决的问题。

网络安全和信息化发展的建设,是国家安全工作的重要保障,也是网络治理现代化的驱动力量。《网络安全与信息化发展路径研究》一书共分为10章。第1章介绍了研究背景和意义、现状等。第2章探讨了健全网络安全保障体系的方法。第3章阐述了“人民至上”思想的生成逻辑、基本内涵和实践对策。第4章分析了构建网络综合治理体系的内涵、问题及路径。第5章讨论了我国互联网核心技术的现况及问题,并给出了突破核心技术的建议。第6章阐述了做大做强互联网企业的意义,以及必须坚持的原则。第7章介绍了依法治网的现实背景、必要性及具体措施。第8章探讨了发展健康繁荣的网络文化的必要性,以及如何营造良好的网络文化氛围和清朗的网络空间。第9章讲述了如何构建具有全球竞争力的网信人才制度。第10章阐述了构建网络空间命运共同体的来源、核心思想、存在形态以及形成路径和价值。该书从安全、产业、人才、文化、技术、法律等方面对我国网络安全和信息化工作的现状、问题等作了梳理,相应地提出了健全网络安全的保障体系。



书名:网络安全与信息化发展路径研究
作者:余学锋
出版社:社会科学文献出版社
ISBN:9787522824901
出版时间:2023年10月
定价:98元

编者指出,推进网络强国建设有其重要性、必要性和时代意义。坚持“人民至上”的发展思想、构建网络综合治理体系、突破互联网核心技术、做大做强互联网企业、依法治网、发展健康繁荣的网络文化、构建具有全球竞争力的网络人才制度,以及构建网络空间命运共同体,是我国网络安全和信息化发展的根本路径。

笔者认为,高校信息化是教育现代化的重要标志。高校信息化安全管理存在诸多问题,如何有效应对这些问题是当前亟待解决的事情。首先是信息安全意识薄弱。高校师生对信息安全的重视程度不够,缺乏基本的信息安全意识和技能。在实际操作中,往往忽视了信息安全的重要性,导致信息泄露、病毒感染等安全问题频发。其次是管理制度不健全。高校信息安全管理制度不健全,缺乏统一的管理规范和操作流程。各部门之间职责不清,信息安全防护措施不到位,导致信息安全风险难以有效控制。然后是技术防护能力不足。高校信息安全技术防护能力不足,难以应对日益严重的网络攻击。一方面,高校网络设备和系统存在安全漏洞,容易被黑客利用;另一方面,高校缺乏专业的信息安全技术人员,难以及时发现和处理安全问题。最后是数据保护不力。高校信息系统中涉及大量敏感数据,如学生个人信息、科研成果等。然而,高校在数据保护方面投入不足,缺乏有效的数据加密和备份措施,导致数据泄露和丢失风险较高。针对以上问题,笔者建议采取如下措施应对。一是高校应建立信息安全风险评估体系。通过系统分析和评估信息系统的安全风险,找出潜在的安全隐患和风险点。具体方法包括:收集和整理信息系统的安全日志、漏洞报告等;运用数据挖掘技术关联分析安全事件,发现异常行为和攻击模式;根据风险评估结果,制定相应的安全防护措施。二是实施动态安全防护策略。高校应根据信息安全风险评估结果,实施动态安全防护策略。一方面,重点防护高风险区域和系统,提高安全防护能力;另一方面,适度防护低风险区域和系统,降低安全防护成本。具体方法为:运用数据挖掘技术预测分析安全事件,提前预警潜在的威胁;根据安全防护需求,调整网络设备和系统的防护策略,提高安全防护效果。三是建立安全事件应急响应机制。高校应建立安全事件应急响应机制,快速、有效地处置突发安全事件。具体方法包括:建立安全事件应急响应小组,负责安全事件的监测、预警和处置;制定安全事件应急响应流程,明确各部门的职责和协作关系;运用数据挖掘技术实时监控和分析安全事件,提高应急响应效率。四是加强信息安全监管和审计。高校应加强对信息安全的监管和审计,确保信息安全管理制度有效执行。具体方法包括:建立信息安全监管机制,定期检查和评估信息系统的运行状况;运用数据挖掘技术溯源分析安全事件,找出安全事故原因和责任;根据监管和审计结果,调整和完善信息安全管理制度。

总之,高校信息化安全管理问题是一个复杂的系统工程,需要从多个角度分析和解决。高校应充分认识到信息安全的重要性,加强信息安全管理,确保信息系统的安全稳定运行。提高高校信息化安全管理的水平,为高校教育事业发展提供有力保障。

(唐蔚南/四川建筑职业技术学院/高级工程师)