高校网络安全意识体系建设研究

那方谏
中国医科大学　辽宁　沈阳　110122

摘　要：高校作为信息汇聚与人才培养的重要阵地，其网络安全意识体系建设关乎学校信息资产安全、学生全面发展及国家网络安全。当前，高校网络安全事件频发，师生安全意识淡薄，管理存在漏洞，亟需系统性建设。本文从重要性出发，分析现状后提出四大策略：加强宣传教育，通过多样化活动与课程渗透；完善管理制度，明确责任与应急预案；提升技术防护，加大投入并建设态势感知平台，培养专业人才，强化师资与学生兴趣培养。研究旨在为构建高校网络安全意识体系提供理论与实践参考，筑牢校园网络安全防线。

关键词：高校网络；安全意识；体系建设

引言：随着数字化时代的深入推进，高校网络应用日益广泛，校园网络已成为教学、科研、管理的核心载体。然而，网络的开放性与复杂性也使高校面临严峻的安全挑战，从数据泄露到钓鱼攻击，各类安全事件频发，暴露出师生安全意识不足、管理机制滞后等问题。高校网络安全不仅涉及学校自身信息资产保护，更与学生信息素养培育、国家网络空间安全紧密相关。在此背景下，构建科学完善的网络安全意识体系，成为提升高校安全防护能力的关键。聚焦高校网络安全意识体系建设，通过分析其重要性与现状，探索切实可行的建设策略，为推动高校网络安全工作规范化、长效化提供思路，助力打造安全、健康的校园网络环境。

1 高校网络安全意识体系建设的重要性

1.1 保障学校信息资产安全

高校拥有海量且至关重要的信息资产，涵盖教学科研数据、师生个人信息以及学校管理数据等。教学科研数据是高校的智慧结晶，从前沿学术研究资料到珍贵实验数据，一旦泄露或遭破坏，多年心血将付诸东流，阻碍学术进步。师生个人信息如身份证号、联系方式等若落入不法分子手中，会给师生带来诸多困扰，甚至造成经济损失。学校管理数据关乎校园运营的各个环节，包括财务信息、招生就业数据等，其安全性直接影响学校的正常运转。加强网络安全意识体系建设，能提升师生和管理人员对信息资产的保护意识，从人为层面减少安全漏洞，结合技术防护与制度保障，全方位守护学校信息资产安全，确保校园数字化环境稳定有序。

1.2 促进学生全面发展

在数字化时代，网络已深度融入学生的学习与生活。具备良好的网络安全意识是学生全面发展的必备素养。一方面，网络安全知识能帮助学生有效识别网络陷阱，如钓鱼邮件、虚假网站等，防止个人信息泄露，保护自身权益，避免因网络诈骗陷入经济困境或遭受心理创伤。另一方面，掌握网络安全技能，有助于学生规范自身网络行为，合理利用网络资源进行学习与交流，提升信息甄别与筛选能力，培养正确的网络价值观。当学生在网络世界中能做到自我保护与自律，便能更加专注于学业提升、技能培养以及综合素质拓展，为未来步入社会，在复杂网络环境下立足与发展奠定坚实基础，实现知识、技能与品德的协同发展。

1.3 维护国家网络安全

高校作为人才培养与知识创新的高地，在国家网络安全战略中占据关键地位。高校师生是未来社会各领域的中坚力量，他们的网络安全意识与素养直接影响国家网络安全的整体水平。通过建设网络安全意识体系，能培养出大批具备网络安全专业知识与责任感的人才，他们毕业后投身不同行业，将在各自岗位上筑起坚固的网络安全防线[1]。

2 高校网络安全现状分析

2.1 网络安全事件频发

高校网络时刻面临着各类攻击威胁，导致安全事件频发。黑客常利用高校网络系统漏洞，恶意篡改学校官网页面，发布不良信息，严重损害学校形象与声誉。教学科研数据也成为重点窃取目标，攻击者通过网络渗透获取珍贵实验数据、学术研究成果，阻碍科研进展。学生个人信息泄露事件屡见不鲜，不法分子以此实施精准诈骗，干扰学生正常学习生活。像某高校曾因系统漏洞，致使大量学生学籍信息被不法分子获取并贩卖。

2.2 师生网络安全意识淡薄

部分师生网络安全意识严重不足。学生群体中，不少人随意连接不明 WiFi，在非正规平台下载软件，易导

致设备被植入恶意程序，个人信息被盗取。对网络诈骗手段识别能力低，轻易相信网络兼职刷单、虚假中奖等信息，陷入诈骗陷阱。教师方面，有的在教学工作中，未妥善保管教学资料，使用简单易破解密码登录办公系统。在科研活动中，忽视数据加密存储，对共享文件权限设置不当，造成数据泄露风险。

2.3 网络安全管理存在漏洞

高校网络安全管理体系存在诸多短板。多数学校虽有网络安全管理部门，但管理职责划分不清晰，部门间协调配合不畅，遇到安全问题相互推诿。网络安全管理制度执行不到位，如设备定期巡检制度流于形式，无法及时发现设备故障与安全隐患。在人员管理上，对新入职员工网络安全培训缺失，老员工培训更新不及时，员工安全意识和技能落后[2]。

3 高校网络安全意识体系建设策略

3.1 加强网络安全宣传教育

3.1.1 开展多样化的宣传活动

高校应综合运用多种宣传渠道，全面普及网络安全知识。在校内设置宣传展板，展示网络安全法规、常见网络攻击手段及防范方法，以图文并茂的形式吸引师生关注。利用校园广播，在课间、午休等时段播报网络安全小贴士与真实案例。同时，发挥新媒体优势，通过学校官网、微信公众号、微博等平台，定期推送网络安全科普文章、短视频。例如制作动画演示钓鱼邮件的识别过程，或发布网络安全知识问答，以趣味互动提升师生参与度，扩大宣传覆盖面，让网络安全意识融入师生日常学习与生活场景，在潜移默化中增强师生对网络安全的重视。

3.1.2 举办网络安全主题活动

定期举办网络安全主题活动，激发师生对网络安全的兴趣与深入探索。开展网络安全知识竞赛，设置初赛、复赛、决赛环节，涵盖网络安全理论知识、实际操作技能等内容，鼓励学生组队参赛，以赛促学。邀请公安部门网络安全专家举办专题讲座，结合典型网络犯罪案例，剖析诈骗手法、数据泄露危害及应对策略，提升师生风险防范意识。组织网络安全主题展览，展示先进网络安全防护设备、技术成果，以及校园网络安全建设成果，让师生直观感受网络安全重要性与技术魅力，营造浓厚的校园网络安全文化氛围，促使师生主动学习网络安全知识。

3.1.3 将网络安全教育纳入课程体系

高校应将网络安全教育融入专业课程与通识教育体系。对于计算机、信息安全等相关专业，开设深度专业课程，系统讲解网络安全原理、技术应用及前沿发展，培养专业人才。在其他专业通识课程中，增设网络安全章节，结合专业特点，介绍网络安全在行业中的应用与潜在风险，如医学专业涉及医疗数据安全，经济专业关注金融网络诈骗防范。

3.2 完善网络安全管理制度

3.2.1 建立健全网络安全管理责任制

高校应明确各部门、岗位在网络安全工作中的具体职责，构建严密责任体系。学校层面成立网络安全与信息化领导小组，由校领导担任组长，统筹全校网络安全工作。各二级学院与职能部门负责人为所在单位网络安全第一责任人，需签署网络安全责任书，将网络安全纳入单位年度考核指标。例如，教学部门要保障教学管理系统、在线教学平台的数据安全与稳定运行；科研部门则负责科研数据存储、传输环节的安全防护。

3.2.2 完善网络安全应急预案

制定详尽且具实操性的网络安全应急预案，是高校应对突发网络安全事件的关键。预案应涵盖常见网络安全事件类型，如数据泄露、网络攻击、系统故障等，并针对不同事件设定应急响应流程。首先明确应急指挥体系，确定应急响应各阶段的负责部门与人员，如网信部门牵头技术处置，保卫部门协助调查取证，宣传部门负责舆情应对。规定事件报告流程，要求发现安全事件后，相关人员第一时间向主管领导与网信部门报告，确保信息及时传递。

3.2.3 加强网络安全监督检查

常态化的网络安全监督检查是保障校园网络安全的重要手段。高校要组建专业监督检查团队，成员包括网信技术专家、安全管理人员等。定期对校园网络基础设施、信息系统、网站等进行全面检查，如每月检查网络设备运行状态，查看是否存在异常流量、端口开放过多等安全隐患；每季度对信息系统进行漏洞扫描，检测操作系统、应用程序漏洞。检查各部门网络安全管理制度执行情况，如人员账号权限管理是否规范，数据存储与传输加密措施是否落实。

3.3 提升网络安全技术防护水平

3.3.1 加大网络安全技术投入

高校应将网络安全技术投入视为校园信息化建设的关键部分。一方面，定期对网络基础设施进行升级，淘汰老旧设备，引入具备先进防护功能的防火墙、入侵检测系统等，增强网络边界防御能力。另一方面，加大对数据存储与处理设备的投入，采用高可靠性存储架构，配备先进的数据加密设备，保障教学科研数据在存储与

传输中的安全性。此外，预留专项资金用于购买最新网络安全防护软件，及时更新病毒库、漏洞库，确保校园网络安全防护技术与时俱进，能有效抵御不断变化的网络攻击手段，为校园网络安全提供坚实的物质基础。

3.3.2 加强网络安全技术研发与合作

高校拥有丰富的科研资源与人才优势，应积极投身网络安全技术研发。鼓励校内相关专业教师与科研人员组建团队，聚焦校园网络安全关键问题，如网络攻击溯源、数据安全防护算法等展开研究。同时，加强与校外科研机构、企业的合作，共建联合实验室、研发中心。通过产学研合作，高校既能获取前沿技术资源，又能将科研成果快速转化应用于校园网络安全实践。例如与网络安全企业合作，引入其先进的网络安全监测技术，共同开发适用于校园网络环境的安全防护系统，提升高校网络安全技术自主创新与应用能力，打造具有高校特色的网络安全技术防护体系。

3.3.3 建设网络安全态势感知平台

构建网络安全态势感知平台是高校实时掌控网络安全状况的重要举措。平台需整合校园网络内各类设备的日志数据、流量数据以及安全设备告警信息等多源数据。利用大数据分析、机器学习等技术，对数据进行深度挖掘与关联分析，精准识别网络中的异常流量、潜在攻击行为以及安全漏洞。通过可视化界面，以直观图表形式呈现校园网络安全态势，让管理人员能实时了解网络安全状况。一旦发现安全威胁，平台及时发出预警，并提供相应处置建议，实现对校园网络安全风险的早发现、早预警、早处置，全面提升高校网络安全防护的主动性与实效性。

3.4 培养专业的网络安全人才队伍

3.4.1 加强网络安全师资队伍建设

高校应着力打造一支高素质的网络安全师资队伍。一方面，积极引进具有丰富行业经验、高学历且专业对口的人才，充实师资力量，例如聘请曾在知名网络安全企业任职，参与过重大网络安全项目的专业人士。另一方面，为现有教师提供多元进修机会，鼓励其参加国内外高水平学术研讨会、专业培训课程，深入学习前沿网络安全技术与理念。定期组织校内师资交流活动，分享教学经验与科研成果，促进教师间知识共享与能力提升。

3.4.2 开展网络安全培训与认证

为提升师生网络安全专业素养，高校应系统开展网络安全培训与认证工作。针对不同群体设计分层培训方案，对非专业师生，开设基础网络安全知识普及培训，涵盖网络安全法规、常见风险及防范措施等内容；对相关专业学生与网络安全工作人员，则组织进阶培训，聚焦网络攻防技术、数据安全管理等专业技能。培训形式可多样化，线上依托优质网络课程平台，提供自主学习资源；线下开展集中授课、实践操作演练。同时，鼓励师生参与权威网络安全认证考试，如 CISA（国际注册信息系统审计师）、CISP（注册信息安全专业人员）等，学校为备考师生提供指导与支持，通过认证提升师生在网络安全领域的认可度与竞争力，打造具备专业资质的校园网络安全人才梯队。

3.4.3 培养学生网络安全兴趣与特长

激发学生对网络安全的兴趣，挖掘其特长，是培养专业人才的关键。高校可开设网络安全兴趣社团，组织社团成员参与网络安全技术交流活动、举办网络安全知识讲座，以趣味性活动吸引学生关注，如开展网络安全主题的 CTF（夺旗赛）校内预选赛，激发学生探索热情。在课程设置上，增设网络安全创新实践课程，提供网络安全项目供学生自主选择参与，在实践中锻炼学生解决实际问题的能力。设立网络安全奖学金，对在网络安全学习、竞赛、科研等方面表现突出的学生予以奖励，激励更多学生投身网络安全领域，逐步培养出一批具有扎实专业基础、浓厚兴趣及突出特长的网络安全后备人才[3]。

结束语

网络安全是高校发展的重要保障，建设高校网络安全意识体系意义重大。从保障学校信息资产安全，到促进学生全面发展，再到维护国家网络安全，每个环节都不容有失。尽管当前高校网络安全存在事件频发、师生意识淡薄、管理存漏洞等问题，但通过加强宣传教育、完善管理制度、提升技术防护水平、培养专业人才队伍等策略，能够逐步构建起坚实的网络安全意识体系。

参考文献

[1]赵学孔,龙世荣.虚拟化技术在高校教育信息化建设中的应用研究[J].教育教学论坛,2020(38):378-379.

[2]崔益军,李宜祥,周俊.高校实验室安全教育途径探讨[J].实验技术与管理,2012,29(09):204-205+218.

[3]李沛霖.新时代我国高校网络文化安全的现实困境与因应路径[J].忻州师范学院学报,2024,40(03):118-125.