科学技术与教育 2026年第8期
ISSN: 3079-4455

网络安全运营体系在智慧校园建设中的研究

张立倩*，王耀庚
内蒙古农业大学计算机与信息工程学院，内蒙古呼和浩特，中国
*通讯作者

【摘要】随着数字化教育改革的持续推进，智慧校园已成为高校信息化建设的核心方向。高校持续推进智慧校园平台搭建、教学数字化转型、校园数据资源整合工作，校园网络承载的业务数据、师生隐私数据、科研核心数据体量持续增长，网络攻击、数据泄露、系统故障等安全风险日益凸显。传统被动式、碎片化的网络安全防护模式已无法适配智慧校园常态化、一体化的运行需求。本文基于智慧校园建设背景，结合网络安全建设现状，分析当前校园网络安全运营存在的短板与问题，构建适配农林类高校的常态化网络安全运营体系，从组织架构、技术防护、运维机制、管理制度、应急保障五个维度完成体系设计与落地应用。实践表明，该运营体系能够有效提升校园网络安全防护能力、风险处置效率和数据安全管控水平，为高校智慧校园安全稳定运行提供保障，也为同类农林院校网络安全建设提供参考借鉴。

【关键词】智慧校园；安全运营体系；高校信息化建设
【基金项目】中国高校产学研创新基金新一代信息技术创新项目（编号：2021ITA11002）

1.引言

在数字中国建设与教育数字化转型的双重背景下[1]，全国各大高校全面推进智慧校园建设，依托大数据、云计算、物联网、人工智能等技术，实现教学、科研、管理、服务全场景数字化升级。智慧校园打破了传统校园的信息孤岛，构建起一体化的校园数字服务平台，极大提升了高校工作效率与服务质量。但与此同时，校园网络边界持续泛化、业务系统日趋复杂、数据资源高度集中，使得高校网络成为网络攻击的重点目标。病毒入侵、非法访问、数据泄露、系统瘫痪等安全事件，严重威胁智慧校园的稳定运行[2]。

高校作为教育、科研核心阵地，具备用户基数大、人员流动性强、数据类型多、网络开放度高等特点，相较于企业网络，校园网络的安全防护难度更高[3]。内蒙古农业大学作为自治区重点农林类高校，近年来积极响应教育数字化政策，陆续建成智慧教务系统、校园一卡通平台、科研数据管理系统、线上教学平台、智慧后勤管理系统等核心业务模块，全面推进智慧校园一体化建设。随着校园数字化业务的全覆盖，原有静态、被动的安全防护模式逐渐暴露出诸多漏洞，安全运营碎片化、风险预警滞后、应急处置能力不足等问题，制约了智慧校园的高质量发展。

在此背景下，构建一套常态化、系统化、智能化的网络安全运营体系[4]，实现校园网络安全的主动防御、动态管控、闭环管理，成为智慧校园建设的核心任务。本文结合学校实际建设情况，探究网络安全运营体系的构建路径与应用价值，为高校智慧校园安全体系标准化建设提供实践依据。

2.智慧校园背景下网络安全运营核心内涵

2.1 网络安全运营体系定义

网络安全运营体系是依托网络安全技术、管理制度、人员团队、应急机制构建的一体化安全管理体系。区别于传统单一的设备防护，其核心是实现“常态化监测、主动化预警、精细化管控、快速化处置、闭环化整改”的动态安全运营模式[5]。在智慧校园场景中，网络安全运营体系覆盖校园网络基础设施、各类业务系统、师生终端设备、校园数据资源等全要素，贯穿系统建设、运行、维护、迭代等全生命周期，是保障智慧校园稳定运行的核心支撑。

2.2 智慧校园对网络安全运营的新要求

智慧校园的数字化、网络化、智能化特征，对网络安全运营提出了全新要求。

第一，从防护模式来看，传统边界防护

模式已无法适配无边界校园网络，需要建立全域动态防护机制。第二，从防护目标来看，安全防护从单纯的网络设备防护，转变为数据安全、业务安全、终端安全、人员安全的全方位防护。第三，从运营模式来看，需要摆脱人工被动运维模式，依托智能化技术实现风险自动监测、精准研判、快速处置。第四，从管理体系来看，需要建立标准化、制度化的运营流程，实现安全工作权责清晰、闭环管理。

3.智慧校园网络安全运营现状及问题

3.1 校园信息化建设现状

近年来，内蒙古农业大学持续加大信息化建设投入，完成校园骨干网络升级，实现教学区、宿舍区、办公区无线网络全覆盖，建成校级数据中心，整合教务、学生、科研、财务、后勤等十余项核心业务系统，实现师生一站式线上服务。同时，学校搭建了科研数据平台，积累了大量草原生态、农牧业科研、校园管理等核心数据。智慧校园建设初具规模，全面支撑学校教学科研、行政管理和社会服务工作。

3.2 网络安全运营现存主要问题

随着智慧校园业务的全面落地，学校原有网络安全防护体系的短板逐渐凸显，具体问题集中在四个方面。

一是安全防护模式被动滞后。学校原有安全体系以防火墙、入侵检测系统等硬件设备为主，属于静态边界防护，仅能抵御常规网络攻击。对于新型 APT 攻击、钓鱼邮件、终端病毒入侵、数据窃取等新型网络威胁识别能力较弱，缺乏主动监测和预警能力，往往在安全事件发生后才能被动处置，存在极大的安全隐患[6]。

二是安全运营体系碎片化。学校网络安全工作由网络中心统筹，缺乏专职安全运营团队，运维人员兼顾网络搭建、系统维护、设备检修等多项工作，安全运营专业化程度不足。同时，各业务系统独立运维，教务、科研、后勤等部门数据相对独立，安全管控标准不统一，形成安全管理孤岛，无法实现全域安全联动。

三是数据安全管控能力较弱。智慧校园建设过程中，学校汇聚了大量师生个人信息、财务数据、科研核心数据，但目前缺乏完善的数据分级分类管理机制，数据传输、存储、共享、销毁全流程管控不足[7]。部分科研人员、师生网络安全意识薄弱，存在弱密码、随意点击陌生链接、私自接入外网设备等行为，极易引发数据泄露风险。

四是安全管理制度与应急机制不完善。学校现有网络安全管理制度多为通用性制度，未结合智慧校园业务场景细化，制度落地性不强。同时，缺乏标准化的应急处置流程，面对网络瘫痪、系统攻击、数据泄露等突发安全事件，存在处置流程不清、响应速度慢、复盘整改不到位等问题，无法形成安全闭环管理。

4.智慧校园网络安全运营体系构建

结合学校智慧校园建设实际和现存安全问题，本文从组织架构、技术防护、运维流程、制度体系、应急保障五个维度，构建全方位、常态化、智能化的校园网络安全运营体系，实现校园网络安全的全域管控和动态防御。

4.1 优化安全运营组织架构

搭建“校级统筹、部门协同、专人负责”的三级安全运营组织架构。第一层级为学校网络安全工作领导小组，由校领导牵头，统筹全校网络安全规划、制度制定和资源保障工作。第二层级为信息化建设与管理中心，作为核心执行部门，负责网络安全日常运营、风险监测、系统维护和技术支撑。第三层级为各二级学院、职能部门安全联络员，负责本部门业务系统安全自查、安全宣传和隐患上报。同时，组建专职网络安全运营小组，配备专业化运维人员，明确岗位职责，细化分工，解决以往权责模糊、兼职运维、专业能力不足的问题，实现安全工作专人专管、全域覆盖。

4.2 构建智能化技术防护体系

基于智慧校园网络架构，升级改造现有安全设备，构建“边界防护、终端管控、云端监测、数据防护”四位一体的智能化技术防护体系。首先，升级校园网络防火墙、入侵防御系统、VPN 安全网关，强化网络边界防护，精准拦截恶意访问、网络攻击和异常流量，筑牢校园网络第一道防线。其次，部署校园终端安全管理平台，对全校办公电脑、教学设备、学生终端进行统一管控，实现终端病毒查杀、漏洞扫描、非法设备接入拦截、系统补丁自动更新，解决终端安全管控盲区。同时，搭建校园网络安全态势感知平台，整合全网流量、系统日志、设备运行数据，依托大数据分析技术，实现网络安全风险的实时监测、智能研判、自动预警，精

准识别钓鱼攻击、暴力破解、数据异常传输等安全隐患，将传统被动防护转变为主动防御。此外，针对学校农林科研核心数据，搭建数据安全防护系统，落实数据分级分类管理，对核心科研数据、师生隐私数据进行加密存储、权限管控、操作溯源，实现数据全生命周期安全防护。

4.3 建立标准化闭环运营运维机制

为解决安全运营碎片化、流程不规范的问题，建立常态化、闭环式的安全运营运维机制。一是落实日常巡检机制，制定每日、每周、每月巡检清单，对校园网络设备、业务系统、服务器、数据中心进行常态化巡检，及时排查系统漏洞、设备故障、安全隐患。二是建立风险整改闭环机制，对态势感知平台监测的风险隐患、上级部门通报的安全问题，实行“发现-研判-整改-复核-归档”全流程管理，明确整改时限和责任人，杜绝隐患遗留。三是完善漏洞修复机制，定期开展校园网络安全漏洞扫描、渗透测试，针对高危漏洞立即修复，中低风险漏洞限期整改，定期更新系统补丁和安全策略。四是建立常态化安全核查机制，每季度开展全校网络安全专项排查，重点核查科研系统、财务系统、学生管理系统等核心平台的安全状态，全面消除安全隐患。

4.4 完善网络安全管理制度体系

根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、以及教育行业网络安全管理规范[8-10]，结合学校智慧校园建设实际，修订完善校园网络安全管理制度体系。细化校园网络安全管理办法、智慧校园业务系统安全规范、校园数据安全管理办法、网络设备运维管理制度等专项制度，明确各部门、各岗位的网络安全职责，规范网络使用、系统运维、数据管理、设备接入等行为。

与此同时，建立安全考核机制，将网络安全工作纳入各部门年度绩效考核，对安全工作落实到位、隐患整改及时的部门予以表彰，对违规操作、隐患逾期未整改、引发安全事件的部门和个人予以追责，通过制度约束保障安全运营工作落地执行。

4.5 搭建全方位应急保障体系

为应对突发网络安全事件，构建完善的应急保障体系。首先，制定校园网络安全突发事件应急预案，明确网络瘫痪、系统被攻击、数据泄露、病毒入侵等各类突发事件的处置流程、责任分工、响应机制，规范突发事件处置流程。其次，建立 7×24 小时网络安全应急响应机制，运维人员全天候值守，确保突发安全事件能够第一时间响应、第一时间处置，最大限度降低损失。

此外，定期开展网络安全应急演练，通过模拟网络攻击、数据泄露、系统故障等场景，提升运维团队的应急处置能力和各部门的协同配合能力。同时，建立安全事件复盘机制，对每一起安全隐患和突发事件进行复盘总结，分析问题根源，优化安全策略和应急预案，持续提升校园网络安全应急保障能力。

5.体系应用成效分析

本文构建的网络安全运营体系在高校智慧校园落地应用后，能够有效解决以往校园网络安全防护被动、管理碎片化、风险管控薄弱的问题，取得显著的应用成效。

一是安全防御能力显著提升。通过搭建智能化态势感知平台和全方位技术防护体系，校园网络风险识别准确率大幅提升，能够提前预判和拦截各类新型网络攻击，网络入侵、病毒感染、异常访问等安全隐患数量大幅下降，校园网络整体安全防御水平实现从被动防护向主动防御的转变。

二是安全运营效率大幅提高。标准化的闭环运维机制和专业化的团队架构，实现了校园网络安全的常态化、精细化管理，漏洞排查、隐患整改、风险处置效率显著提升，彻底解决了以往运维混乱、权责不清、整改滞后的问题，保障了各类智慧校园业务系统稳定运行。

三是数据安全得到有效保障。通过落实数据分级分类、加密存储、权限管控、操作溯源等防护措施，学校师生隐私数据、科研核心数据的泄露风险大幅降低，实现了数据全生命周期安全管控，为学校科研创新、教学管理提供了数据安全保障。

四是师生安全意识全面提升。依托常态化网络安全宣传、专项培训、应急演练，全校师生网络安全防范意识和规范用网能力显著提高，私自接入设备、弱密码使用、随意点击陌生链接等违规行为大幅减少，构建了全员参与的校园网络安全防护氛围。

6.问题与展望

在体系落地应用过程中，学校网络安全运营工作仍存在部分短板。一是网络安全智

能化水平仍有提升空间，人工智能、自动化运维技术的应用深度不足；二是师生常态化安全培训体系不够完善，针对性、场景化的安全培训较少；三是跨部门安全协同机制仍需优化，各部门安全联动效率有待提升。

未来，高校将持续优化网络安全运营体系。一是深化智能化技术应用，依托人工智能、大数据技术优化态势感知平台，实现安全风险自动化研判、自动化处置，提升安全运营智能化水平。二是构建常态化、分层化的安全培训体系，针对教职工、学生、运维人员开展差异化安全培训，强化全员网络安全素养。三是完善跨部门协同机制，打通各业务系统安全数据壁垒，实现全域安全联动管控。四是持续跟进网络安全新技术、新态势，动态优化安全策略和防护体系，适配智慧校园持续迭代的建设需求，全力保障学校智慧校园安全、稳定、高质量发展。

7.结论

智慧校园建设是高校教育数字化转型的核心载体，而网络安全运营体系是智慧校园稳定运行的安全基石。本文结合学校智慧校园建设现状，分析了当前高校校园网络安全运营存在的普遍问题，从组织、技术、运维、制度、应急五个维度构建了系统化的校园网络安全运营体系，并完成落地应用与实践验证。该体系有效弥补了传统校园网络安全防护的短板，实现了校园网络安全的动态防御、闭环管理、全域管控，全面提升了学校智慧校园安全防护能力。同时，本研究的实践经验，能够为全国同类农林高校及普通高校的智慧校园网络安全建设提供参考借鉴，助力高校教育数字化安全、有序、高质量发展。

参考文献

[1] 李玉顺，韩梦莹.教育强国背景下人工智能赋能教育教学创新：未来图景、实践路径与风险审思[J].中国电化教育，2025，（8）：13-21.
[2] 王芬，韩晶晶.大模型在高校网络安全防护中的应用研究[J].网络安全技术与应用，2025，（12）：74-76.
[3] 朱晓飞.基于网络安全新形势下的高校动态运营体系研究[J].网络安全技术与应用，2025，（10）：95-97.
[4] 田文君，王罕.智慧校园网络安全运营体系的构建[J].办公自动化，2025，30（6）：37-39.
[5] 程小白，张艺，陈智林.高校校园安全评价指标体系构建与实践应用[J].中国人民警察大学学报，2026，42（7）：56-63.
[6] 范向军，赵小芳.基于蜜罐技术的高校网络安全主动防御系统设计[J].智能物联技术，2025，57（4）：118-122.
[7] 陈沛沛，侯文庆，荣江.智慧校园数据共享中的安全隐患与应对策略[J].科技与创新，2025，（18）：192-195.
[8] 郑爽，李赟，张伟，等.人工智能时代的安全保密管理挑战与启示[J].中国信息安全，2026，（6）：85-88.
[9] 陈毅飞，李萌，乔焰，等.安全可信的数据要素流通综述[J].软件学报，2026，37（6）：2607-2646.
[10] 郭亚涛.多维数据融合背景下个人信息安全风险与防控策略[J].中国信息化，2026，（5）：72-73