高校校园网络安全运维体系优化与管理策略研究

洛 言

（淮南职业技术学院，安徽 淮南 232001）

摘 要：高校校园网络安全运维体系是保障高校信息化基础设施安全稳定运行、保护教学科研数据安全与维护师生个人信息权益的核心支撑。当前高校网络安全面临外部威胁持续演进、内部风险日益复杂、技术体系快速迭代与管理要求不断提高的多重压力，传统以边界防护为主的网络安全运维模式已难以有效应对日益复杂的网络安全形势。本文立足于高校校园网络的现实特征与安全需求，系统解析高校网络安全运维体系的核心构成要素、面临的挑战与优化方向，并从安全技术体系升级、安全管理制度完善、应急响应能力强化与安全人才培养四个维度构建网络安全运维体系优化与管理策略框架，为高校网络安全运维能力的系统性提升提供理论支撑与实践指引。

关键词：高校校园网络；网络安全；运维体系；安全策略；应急响应；数据安全

中图分类号：TP393.0 **文献标识码：**A **文章编号：**3106-2709（2026）08-0018-06

DOI：10.62022/NCAR.issn3106-2709.2026.08.004

Research on Optimization and Management Strategies for the Cybersecurity Operation and Maintenance System of University Campus Networks

Yan Luo

(Huainan Vocational and Technical College, Huainan, Anhui 232001)

Abstract: The cybersecurity operation and maintenance system of university campus networks serves as the core support for ensuring the secure and stable operation of university information infrastructure, protecting the security of teaching and research data, and safeguarding the personal information rights and interests of faculty and students. At present, university cybersecurity faces multiple pressures, including the continuous evolution of external threats, increasingly complex internal risks, rapid iteration of technological systems, and ever-higher management requirements. The traditional cybersecurity operation and maintenance model centered on perimeter protection can no longer effectively address the increasingly complex cybersecurity landscape. Based on the practical characteristics and security needs of university campus networks, this paper systematically analyzes the core components, challenges, and optimization directions of university cybersecurity operation and maintenance systems. It further constructs a framework for optimization and management strategies for cybersecurity operation and maintenance systems from four dimensions: upgrading the security technology system, improving security management systems, strengthening emergency response capabilities, and cultivating cybersecurity talent, thereby providing theoretical support and practical guidance for the systematic enhancement of university cybersecurity operation and maintenance capabilities.

Keywords: university campus networks; cybersecurity; operation and maintenance system; security strategies; emergency response; data security

1 高校校园网络安全运维体系的内涵特征与现实挑战

1.1 高校校园网络的构成特征与安全边界分析

高校校园网络是支撑高校教学、科研、管理与服务信息化运行的综合性基础设施，其网络架构呈现出规模庞大、结构复杂、用户多元与应用多样的显著特征。从物理构成来看，高校校园网络由有线网络基础设施、无线网络覆盖系统、数据中心与服务器集群、网络安全管理平台以及各类接入终端设备等多个层次组成。有线网络以光纤与铜缆为传输介质，覆盖教学楼、图书馆、实验室、行政楼、学生宿舍与教工住宅等各类建筑，构成了校园网络的主干骨架。无线网络以Wi-Fi技术为主体，实现了校园公共区域与室内空间的广泛覆盖，为移动终端的便捷接入提供了条件。数据中心集中承载了校园门户网站、教务管理系统、科研管理系统、电子邮件服务、在线学习平台与各类业务应用系统，是校园网络的数据中枢与服务核心。

高校校园网络的安全边界呈现出显著的模糊化与动态化特征。传统基于物理边界的安全模型假设网络具有明确

作者简介：洛言，本科，助教，研究方向为校园网络运维、网络安全管理体系。

的内外界限，通过防火墙等设备在边界处实施访问控制。在云计算、移动互联与物联网技术广泛应用的背景下，校园网络的服务范围已从校园物理空间延伸至校外访问、公有云服务与移动终端，安全边界从固定的物理边界转变为动态的逻辑边界。校园网络中大量存在的物联网设备（包括智能门禁、视频监控、环境监测、智能照明等）进一步增加了网络的暴露面与安全风险，许多物联网设备的安全防护能力较弱，成为潜在的安全薄弱环节。

1.2 高校网络安全威胁的类型特征与演变趋势

高校网络安全威胁的类型涵盖恶意代码攻击、网络入侵与渗透、拒绝服务攻击、数据泄露与窃取、内部威胁与人为失误以及供应链安全风险等多个类别。恶意代码攻击以勒索软件、挖矿木马、蠕虫病毒与后门程序为主要形式，通过钓鱼邮件、漏洞利用或移动存储介质传播，对校园网络中的终端设备、服务器与存储系统构成直接威胁。网络入侵与渗透以窃取敏感数据、控制关键系统或建立持久化访问为目标，攻击者通常通过社会工程学、弱口令破解或漏洞利用等方式获取初始访问权限，然后在内网进行横向移动与权限提升，最终达成攻击目标。拒绝服务攻击通过消耗目标系统的带宽、计算资源或连接数使其无法提供正常服务，对校园网络的可用性构成严重威胁。

高校网络安全威胁的演变趋势呈现出攻击手段的智能化、攻击目标的精准化与攻击组织的有序化三个显著特征。智能化趋势体现为攻击者越来越多地运用人工智能技术辅助漏洞发现、密码破解与社会工程学攻击，提高了攻击的效率与成功率。精准化趋势体现为攻击者不再盲目地广泛撒网，而是针对高校的具体资产与人员进行精细化的情报收集与攻击策划，提高了攻击的隐蔽性与破坏性。有序化趋势体现为网络攻击的组织化程度不断提高，有组织的攻击团体以经济利益或特定目的为驱动，对高校网络实施持续性的、有策略的攻击活动[1]。

1.3 高校网络安全运维体系的核心构成要素

高校网络安全运维体系是由安全组织架构、安全管理制度、安全技术措施、安全运维流程与安全应急响应五个核心要素构成的有机整体。安全组织架构明确了网络安全工作的领导体制、责任分工与协调机制，通常由网络安全工作领导小组、信息化管理部门、安全运维团队与各单位安全员等层级构成，为安全工作的开展提供了组织保障。安全管理制度涵盖了安全策略文件、操作规程、管理办法与记录表单等层级的制度文件，为安全工作的规范化开展提供了制度依据。

安全技术措施是网络安全运维的技术保障基础，包括防火墙、入侵检测与防御系统、防病毒系统、数据备份与恢复系统、身份认证与访问控制系统、日志审计系统与安全态势感知平台等技术手段的部署与运行。安全运维流程规范了日常安全巡检、漏洞扫描与修补、安全配置核查、补丁更新管理、日志分析与安全事件处置等日常运维工作的流程与标准。安全应急响应明确了安全事件的发现、报告、分析、处置、恢复与总结的全过程管理要求，为安全事件的快速有效处置提供了流程支撑。

1.4 高校网络安全运维体系面临的挑战与优化需求

高校网络安全运维体系面临的挑战可以从技术层面的快速演进、管理层面的体系化不足与资源层面的投入有限三个维度进行概括。技术快速演进的挑战体现为网络安全威胁的技术手段不断翻新，攻击技术的迭代速度超过了防护技术的更新速度，安全运维团队需要持续跟踪最新威胁态势并调整防护策略，这对安全人员的专业技能与学习能力提出了较高要求。网络环境的变化（包括IPv6的部署、5G的应用与物联网设备的激增）带来了新的安全风险，现有的安全防护措施可能无法有效覆盖新的攻击面[2]。

管理体系化不足的挑战体现为部分高校的网络安全管理制度未能形成完整的体系，制度之间存在衔接不畅或覆盖不全的问题，制度的执行力度与监督机制有待加强。安全意识培训的覆盖面与实效性有待提升，部分用户的安全意识仍然薄弱，成为安全链条中最为脆弱的环节。资源投入有限的挑战体现为网络安全的人力、物力与财力投入相对不足，安全运维团队的人员编制有限，难以应对日益繁重的安全运维任务。

2 高校网络安全运维体系的技术架构优化

2.1 网络安全防御技术架构的分层设计与协同联动

网络安全防御技术架构应遵循纵深防御的理念，在网络边界、网络内部、主机系统、应用系统与数据层面构建多层防御体系。边界防御层部署防火墙、入侵防御系统与防分布式拒绝服务攻击系统，对进出校园网络的流量进行访问控制与威胁检测。网络内部防御层部署网络流量分析系统、内网入侵检测系统与网络准入控制系统，对内部网络流量进行持续监测与异常识别。主机系统防御层部署防病毒软件、主机入侵检测系统与补丁管理系统，对服务器与终端设备进行安全加固与威胁检测。应用系统防御层部署Web应用防火墙、数据库防火墙与应用系统安全审计系统，对应用层的访问请求与数据操作进行安全控制与审计。

各防御层之间的协同联动是提升整体防御效能的关键。协同联动的实现需要建立统一的安全信息收集与处理平台，汇聚各安全设备的告警信息与日志数据，通过关联分析识别出跨越多个防御层的攻击行为。安全事件响应流程中，不同防御层之间应有明确的信息传递与协同处置机制，当一个防御层检测到攻击行为时，相关防御层应同步采取相应的防护措施，形成协同联动的防御合力。

2.2 安全监测与态势感知平台的构建与优化

安全监测与态势感知平台是网络安全运维体系中的核心分析系统，其功能为对校园网络中各类安全数据的实时采集、处理与综合分析，输出对网络安全态势的整体判断与对潜在威胁的早期预警。平台的数据采集层对接各类安全设备、网络设备、服务器与业务系统的日志数据与告警数据，通过标准化的数据接口与协议进行数据汇聚。数据处理层对采集到的原始数据进行清洗、格式化、归并与富化处理，将分散的数据转化为统一格式的结构化数据。分析层运用规则引擎、统计分析与机器学习等方法对处理后的数据进行分析，识别异常行为与安全威胁。

态势感知平台应具备对校园网络整体安全状态的持续监测能力，通过可视化仪表盘呈现网络安全态势的关键指标，包括当前告警数量与等级分布、安全事件的类型与趋势、重点资产的防护状态与脆弱性状况。平台应支持对历史数据的回溯分析，为安全事件的调查取证与威胁溯源提供数据支持。平台的优化方向包括数据源的扩展、分析模型的改进与响应能力的提升，通过接入更多类型的安全数据、引入更智能的分析算法与建立更高效的联动机制，不断提升平台的监测预警能力。

2.3 数据安全保护与隐私防护的技术措施

数据安全保护是高校网络安全运维体系的重要组成内容，其核心目标是保障校园网络中存储、传输与处理的各类数据的机密性、完整性与可用性。数据安全保护的技术措施覆盖数据的全生命周期，包括数据采集、传输、存储、使用、共享与销毁等环节。在数据采集环节，应明确数据采集的范围与目的，对个人信息的采集遵循最小必要原则。在数据传输环节，应采用加密协议保障数据在网络传输过程中的机密性与完整性，校内重要数据传输应使用加密通道，对外数据传输应满足合规要求。

在数据存储环节，应对重要数据进行加密存储，对敏感数据实施分级分类管理，建立数据备份与恢复机制以保障数据的可用性。在数据使用环节，应实施最小权限原则与访问控制机制，对数据访问行为进行记录与审计，对涉及个人信息的查询与导出操作实施审批与留痕。隐私防护技术措施包括数据脱敏、匿名化处理与差分隐私保护等，在保障数据可用性的前提下降低个人隐私泄露的风险。数据安全保护的技术措施应与管理措施相结合，形成数据安全保护的整体方案[3]。

2.4 校园网络安全技术架构的发展趋势与演进方向

校园网络安全技术架构的发展趋势呈现出零信任化、智能化、一体化与主动防御化的方向演进。零信任安全模型是校园网络安全技术架构演进的重要方向，其核心理念是“从不信任、始终验证”，在网络内部取消默认的信任关系，对每一次访问请求进行身份验证与授权。零信任模型的实施需要构建基于身份的微隔离机制，将网络划分为更细粒度的安全域，对域间访问进行精细化控制。身份认证的强度应从单一密码认证向多因素认证方向升级，提高身份验证的安全性。

智能化的趋势体现为人工智能技术在网络安全领域的深度应用，包括基于机器学习的异常行为检测、自动化安全响应与威胁情报的智能分析等。安全运营的智能化转型有助于解决安全人员短缺与安全事件数量增长之间的矛盾，提高安全运维的效率与质量。一体化的趋势体现为安全能力的平台化集成与统一管理，通过建设统一的安全管理平台整合各类安全工具与数据源，提升安全运营的整体效率。主动防御化的趋势体现为从被动响应向主动防护的转变，通过威胁狩猎、攻击面管理与安全态势预测等手段，在攻击发生之前识别并消除潜在的安全风险。

3 高校网络安全管理体系的制度构建与流程优化

3.1 网络安全管理制度体系的层级结构与内容框架

高校网络安全管理制度体系应构建由顶层策略、中层规范与底层操作细则三个层级组成的完整结构。顶层策略是学校网络安全工作的纲领性文件，明确了网络安全工作的指导思想、基本原则、总体目标与组织架构，为全校网络安全工作提供了方向指引与制度依据。顶层策略的制定应充分考虑学校的办学定位、信息化发展水平与网络安全风险状况，体现学校对网络安全工作的重视程度与治理决心。中层规范包括各类专项安全管理办法与实施细则，对网络安全工作的各领域、各环节做出具体的规定，涵盖人员安全管理、系统安全管理、数据安全管理、网络安全事件管理、安全运维管理等内容。底层操作细则是具体安全操作流程的标准化文件，规定了各项安全操作的具体步骤、执行标准与记录要求，为一线运维人员提供了可执行的操

作指南。

3.2 网络安全责任制与人员安全管理的落实机制

网络安全责任制的核心是将网络安全工作分解为可落实、可检查、可问责的具体责任事项，将责任明确到具体的岗位与人员。学校网络安全工作领导小组应承担网络安全工作的领导责任，统筹全校网络安全工作的规划与决策。信息化管理部门应承担网络安全工作的管理责任，负责网络安全工作的组织实施与日常管理。各业务部门与院系应承担本部门网络安全工作的主体责任，落实本部门信息系统的安全防护与安全事件的第一时间处置。系统管理员、安全管理员与审计管理员应承担具体的安全管理与操作责任。责任制的落实需要建立责任清单与考核机制，定期对各部门网络安全工作的落实情况进行检查评估。

人员安全管理贯穿聘用前、在岗期间与离岗后的全周期。聘用前应进行背景审查与安全承诺签署，在岗期间应进行持续的安全培训、安全意识教育与绩效考核，离岗时应完成权限回收、资产移交与保密协议签署。安全培训的内容应根据培训对象的不同进行针对性的设计，面向全体师生开展基础安全意识培训，面向系统管理员与安全运维人员开展专业技能培训，面向中高层管理人员开展安全治理培训。

3.3 安全运维流程的标准化与常态化管理

安全运维流程的标准化是保障安全运维工作质量的重要基础。安全运维流程应覆盖日常巡检、安全监测、漏洞管理、补丁更新、配置审核、事件处置与变更管理等核心运维活动。日常巡检流程规定了巡检的频率、内容、方法与记录要求，确保对网络设备、服务器、安全设备与关键系统的运行状态进行定期的检查。安全监测流程规定了安全事件的发现与报告通道，要求运维人员持续关注安全告警、日志异常与威胁情报信息。漏洞管理流程规定了漏洞的发现、评估、修补与验证的全过程管理，要求对校园网络中的信息系统进行定期的漏洞扫描与风险评估。

安全运维的常态化管理要求将安全运维工作嵌入日常的运维活动中，形成持续运转的工作机制。常态化管理的实现需要建立安全运维工作的标准化操作文档、明确各项运维工作的操作步骤与质量标准、建立运维工作的记录与统计机制。通过运维数据的积累与分析，持续优化运维流程与提升运维质量。

3.4 管理制度执行力的提升与持续改进机制

管理制度执行力的提升需要从制度设计的可操作性、执行的监督机制与执行的激励约束三个方面进行改进。制度设计应充分考虑执行的实际条件与能力，避免提出超出执行能力的要求。制度的表述应清晰明确，避免产生歧义与多种解读。制度发布前应征求执行部门的意见，确保制度的可执行性。执行的监督通过定期检查、专项审计与绩效评估等方式进行，对制度执行情况进行持续的跟踪与评估。定期检查关注制度要求的落实率与执行质量，专项审计关注重点制度与关键环节的执行情况，绩效评估将制度执行情况纳入相关岗位的绩效考核体系。

持续改进机制要求建立制度执行的反馈与优化闭环。在制度执行过程中发现的问题与不合理之处，应及时反馈至制度制定部门进行修订完善。通过定期的制度评审与更新，使制度体系始终适应网络安全形势的变化与学校信息化发展的需要。持续改进的闭环机制是保障制度体系生命力的关键，使制度不断完善、执行效力持续提升。

4 高校网络安全应急响应体系与事件处置能力建设

4.1 网络安全应急响应体系的组织架构与职责分工

网络安全应急响应体系应建立由应急指挥中心、应急响应技术团队、应急联络协调组与外部专家支持组组成的组织架构。应急指挥中心是应急响应的最高决策机构，由网络安全分管领导担任指挥长，负责重大安全事件的决策指挥与资源协调。应急响应技术团队承担安全事件的技术处置工作，由安全运维人员、网络管理员与系统管理员组成，负责安全事件的初步分析、技术处置与系统恢复。应急联络协调组负责应急过程中的信息传递、对外沟通与舆情监测，保障应急过程中信息的准确传递与有效沟通。外部专家支持组由外部安全专家、安全厂商技术人员与法律顾问组成，在重大安全事件中提供技术支持与法律指导。

应急响应各角色之间的职责分工应在应急响应预案中予以明确，避免在事件发生时出现职责不清或响应缺位的情况。指挥中心、技术团队、联络协调组与外部支持组之间应建立清晰的指挥链与信息传递通道，保障应急响应工作的高效协同。应急响应组织应定期进行演练与评估，验证组织架构的有效性与各角色的履职能力。

4.2 安全事件分级分类与应急响应流程设计

安全事件的分级分类是应急响应预案设计的基础，其目的是根据不同级别与类型的安全事件匹配差异化的响应资源与响应流程。安全事件的分级依据事件的危害程度、影响范围与紧急程度划分为特别重大事件、重大事件、较大事件与一般事件四个级别。特别重大事件指对校园网络

的整体运行、关键数据或重大教学科研活动的安全造成严重影响的事件，需要启动最高级别的应急响应。重大事件指对部分系统的正常运行或较多用户的数据安全造成严重影响的事件，需要启动高级别的应急响应。较大事件指对个别系统或少数用户造成影响的事件，由安全运维团队直接处置。一般事件指影响范围较小、危害程度较低的事件，由一线运维人员按照标准操作流程处置。

应急响应流程应涵盖发现与报告、初步研判、信息通报、应急处置、系统恢复与事后总结等环节。发现与报告环节明确了安全事件的发现渠道与报告路径，要求发现人第一时间向安全运维团队报告。初步研判环节由安全运维团队对事件的性质、范围与影响进行快速评估，确定事件的级别与响应等级。信息通报环节根据事件的级别与影响范围，向相关人员通报事件信息与处置进展。应急处置环节根据事件的类型与级别调用相应的处置预案，执行隔离、清除、修复等处置措施。系统恢复环节在确认威胁已清除后，将受影响系统恢复至正常运行状态。事后总结环节在事件处置完成后进行全面的复盘分析，总结经验教训、优化应急响应预案。

4.3 应急演练与攻防对抗的实战化训练

应急演练是检验应急响应体系有效性、提升应急响应能力的实战化训练手段。应急演练的类型包括桌面推演、专项演练与综合演练三种形式。桌面推演以情景模拟的方式，组织应急响应相关人员讨论特定场景下的应急响应流程与决策方案，检验预案的完整性与人员的熟悉程度。专项演练聚焦某一特定类型的安全事件（如勒索软件攻击、网站篡改等），检验针对特定事件类型的处置能力与流程的有效性。综合演练模拟复杂的、跨系统的安全事件场景，检验应急响应体系的整体协同能力与综合处置能力。应急演练应制定详细的演练计划，明确演练的目标、场景、参与人员与评价标准，演练结束后应进行全面的总结评估。

攻防对抗是网络安全应急响应能力建设的重要实践手段。在可控的环境下组织安全攻防对抗活动，由攻击方模拟真实攻击行为、防守方进行监测与防御，检验与提升安全防护与应急响应的实际能力。攻防对抗中发现的安全薄弱环节应纳入后续的整改计划中进行完善，提升的防护能力应在后续的攻防对抗中进行验证。

4.4 安全事件的事后分析与持续改进机制

安全事件的事后分析是应急响应流程中的重要环节，其目标是从已发生的安全事件中提取经验教训，防止同类事件的再次发生。事后分析的内容包括事件的根本原因分析、处置过程的回顾评价与改进措施的制定实施。根本原因分析应追溯至漏洞产生的源头，分析导致漏洞发生的技术因素、管理因素与人为因素。处置过程的回顾评价应识别处置过程中的有效做法与不足之处，为应急预案的优化提供依据。改进措施的制定应明确具体的改进内容、责任人与完成时限，改进措施的实施效果应在后续的安全事件中进行验证。

持续改进机制要求安全事件的事后分析结果能够有效转化为安全防护措施与应急响应能力的持续提升。每次安全事件处置完成后，应形成完整的事件分析报告。安全事件的分析报告应作为安全培训的案例素材，用于提升全体人员的安全意识与安全技能。通过建立安全事件的数据库，积累事件的特征数据与处置经验，为后续的安全监测与应急响应提供参考。

5 高校网络安全人才培养与安全意识教育

5.1 网络安全人才需求的现状与培养方向

高校网络安全面临的人才需求涵盖了安全运维、安全管理、安全研发与安全教育等多个方向。安全运维方向需要掌握网络安全设备的配置与维护、安全事件的监测与处置、漏洞扫描与修复等技能，是网络安全工作中需求量最大的方向。安全管理方向需要具备安全管理体系的规划与建设、安全策略的制定与执行、安全风险的评估与管控等能力，对管理能力与系统思维有较高的要求。安全研发方向需要具备安全工具的开发、安全系统的构建与安全技术的研究等能力。安全教育方向需要具备安全培训课程的设计与实施、安全意识的宣传与普及等能力，对教学能力与沟通能力有较高的要求。

高校网络安全人才的培养应构建理论与实践并重的培养体系。理论教育涵盖网络安全基础知识体系，包括网络协议安全、操作系统安全、密码学基础、安全开发、安全管理与安全法律规范。实践训练通过网络安全实验室、安全实训平台、攻防对抗与安全竞赛等方式进行，使学生在真实或接近真实的环境中锻炼安全技能。安全竞赛与攻防对抗是提升学生实践能力的有效途径。

5.2 网络安全意识教育的体系化实施

网络安全意识教育是提升全体师生网络安全防护能力的基础性工作。意识教育的对象应覆盖全校师生员工，不同群体的安全意识教育内容与方式应有所差异。面向普通学生的意识教育应以普及性内容为主，包括密码安全、防钓鱼邮件、防网络诈骗、个人信息保护、移动终端安全等，

通过新生入学教育、主题班会、安全宣传周等渠道进行。面向教职工的意识教育应增加与工作相关的内容，包括数据安全保护、科研信息安全、办公设备安全、远程办公安全等。

意识教育的形式应多样化、常态化，结合线上与线下两种渠道开展。线下的意识教育形式包括安全专题讲座、安全宣传展览、安全知识竞赛、安全主题班会等。线上的意识教育形式包括安全微课、安全知识推送、安全测试与安全互动游戏等。通过线上线下相结合的多元化教育方式，提高意识教育的覆盖面与实效性。意识教育的效果应通过定期的安全知识测试与安全行为观察进行评估，评估结果用于指导意识教育内容的更新与方法的改进。

5.3 安全运维团队的专业能力建设与职业发展

安全运维团队的专业能力建设是保障网络安全运维质量的关键。能力建设的内容应涵盖安全技术能力、安全运营能力与安全管理能力三个维度。安全技术能力包括网络安全设备的配置与维护、安全漏洞的检测与修复、安全事件的监测与处置等硬技能。安全运营能力包括安全态势的感知与评估、安全事件的分析与溯源、安全策略的优化与调整等综合能力。安全管理能力包括安全制度的执行与监督、安全项目的规划与管理、安全风险的评估与管控等管理能力。

能力建设的途径包括内部培训、外部培训与岗位实践等多种方式。内部培训由团队内部的技术骨干或外聘专家开展，内容紧密贴合实际工作需求，周期灵活、成本较低。外部培训包括安全认证培训、技术研讨会与行业交流活动，使团队成员接触行业前沿的技术与最佳实践。岗位实践是在实际工作中锻炼与提升能力的重要途径，通过参与真实的安全事件处置、安全评估项目与安全建设项目的实施，在实战中积累经验与提升能力。

5.4 高校网络安全文化建设与全员参与机制

高校网络安全文化建设是将安全意识与安全行为内化为全校师生自觉行动的重要途径。安全文化的建设应从制度文化、行为文化、物质文化与精神文化四个层面协同推进。制度文化层面通过完善安全管理制度与规范，将安全要求融入学校的管理体系与工作流程，形成“有章可循、违章必究”的制度环境。行为文化层面通过安全意识的持续教育与安全行为的正向激励，引导师生养成良好的安全行为习惯，使“安全无小事”成为全校师生的共识。物质文化层面通过安全标识系统、安全宣传阵地与安全设施的建设，营造安全的工作学习环境，使安全元素融入师生的日常视觉体验。精神文化层面通过安全先进表彰、安全典型宣传与安全价值倡导，培育“人人讲安全、事事重安全”的校园安全氛围。

全员参与机制是网络安全文化建设的重要保障。安全参与的平台包括安全建议通道、安全志愿者队伍与安全自治组织等。安全建议通道为师生提供报告安全隐患、提出安全建议的便捷渠道。安全志愿者队伍招募具有安全兴趣与能力的师生参与安全宣传、安全巡查与安全活动的组织。安全自治组织由学生自发成立，在学工部门与信息化管理部门的指导下开展网络安全相关活动。

6 结论

高校校园网络安全运维体系的优化与管理在高校信息化发展与安全保障中占据核心的战略地位，其体系完整性与运行效能通过安全技术架构的分层防御能力、安全管理制度的规范化水平、应急响应的时效性以及安全人才培养的系统性等多重维度得以综合呈现，是衡量高校信息化治理能力与安全保障水平的关键标尺。高校网络安全运维的相关主体今后应当锚定安全技术能力与管理治理效能协同提升的核心目标，系统推进网络安全防御技术架构中零信任模型的适配部署与安全监测态势感知平台的智能化升级，网络安全管理体系中制度体系的动态优化与安全责任制考核的常态化运行，应急响应体系中事件分级分类预案的精细化编制与攻防对抗实战化训练的定期开展，以及人才培养体系中专业安全队伍建设与全员安全意识教育的体系化推进，以此构建起技术先进、制度完善、响应高效、人才充足的高校校园网络安全运维体系，切实服务于高校信息化健康稳定发展与师生个人信息安全保护的根本目标。

参考文献：

[1]李岩.基于机器学习的网络安全态势感知关键技术探究[J].教育教学研究前沿，2024，2（10）：16-18.

[2]赵震森.数据加密技术在计算机网络信息安全中的应用[J].人工智能研究，2025，2（2）：37-39.

[3]王宇.高校基于运维管理平台的网络安全体系建设[J].信息产业报道，2024（9）：0078-0080.