基于等级保护的关键信息基础设施风险管理研究

董 馨

（新疆智盾信息科技有限公司 乌鲁木齐 830000）

摘 要 关键信息基础设施（CII）能保障社会的稳定、安全，而风险管理对其起着关键作用，它通过对风险的识别、评价与控制来确保CII持续、平稳的运作。然而，以等级保护为基础的CII风险管理在实践中却面临着许多困境。因此，文中提出了强化等级保护标准和实际操作衔接，改进风险评估模型和手段，提高新兴威胁监测和应对能力，强化人员培训和安全意识教育等策略，以提升CII风险管理水平，保障国家关键信息基础设施安全。

关键词： 关键信息基础设施；风险管理；等级保护

中图分类号 TP393

Research on Risk Management of Critical Information Infrastructure Based on Hierarchical Protection

DONG Xin

（Xinjiang Zhidun Information Technology Co., Ltd., Urumqi 830000, China）

Abstract Critical Information Infrastructure (CII) can ensure social stability and security, and risk management plays a crucial role in it. It ensures the continuous and smooth operation of CII through the identification, evaluation, and control of risks. However, CII risk management based on level protection faces many challenges in practice. Therefore, this paper proposes strategies such as strengthening the connection between level protection standards and practical operations, improving risk assessment models and methods, enhancing the ability to monitor and respond to emerging threats, strengthening personnel training and security awareness education, in order to enhance the level of CII risk management and ensure the security of national critical information infrastructure.

Key words Critical information infrastructure, Risk management, Grade protection

0 引言

等级保护制度是我国保障信息安全的基本制度，其在CII风险管理中的应用是确保信息安全的关键环节。然而，在实际操作中，等级保护标准与实际应用之间存在脱节，风险评估方法尚不完善，对新兴威胁的响应能力不足。同时，人员安全意识和培训的缺失也制约了风险管理的有效性。本文旨在探讨基于等级保护的关键信息基础设施风险管理的难题，并提出相应的解决策略，以期为CII的安全防护提供理论支持和实践指导。

1 风险管理在关键信息基础设施中的作用

在信息化社会中，关键信息基础设施（CII）的风险管理显得尤为重要。风险管理在关键信息基础设施中的作用体现在以下几个方面。（1）其通过对潜在风险的识别，评估与控制来保障基础设施安全与稳定，避免因多种威胁而导致系统崩溃或数据泄露等现象。（2）风险管理也有助于组织编制应急响应计划，并迅速应对各类突发事件，以减少事故后的损失。（3）通过不断地监控和管理风险，组织可以及时改进自己的安全策略以适应新威胁环境，并维护信息系统的可靠与安全。

2 基于等级保护的关键信息基础设施风险管理难题

2.1 等级保护标准与实际应用的脱节

等级保护（Classification Protection）标准是我国在信息安全方面的关键规定，其核心目标是通过层次化的保护措施来提高信息系统的整体安全防护能力。但在实践中，等级保护标准和具体运作明显脱节。在制定标准时，通常很难全面覆盖各种信息系统的真实运行环境，使得标准太过抽象而很难直接运用到实际安全防护措施中。部分单位对等级保护标准的执行往往只达到最低要求而没有针对性，且深度不够，导致实际效果不好。另外，科技的飞速发展与威胁环境的变化使等级保护标准适用性有限，部分新出现的科技与威胁还未列入标准，造成标准缺乏实用性与前瞻性[1-2]。

作者简介：董馨（1994—），本科，研究方向为网络安全。

2.2 风险评估方法不完善

风险评估在风险管理中处于核心地位，其通过系统性地分析潜在威胁与漏洞来判断其严重性与可能性，但现有的以等级保护为基础的风险评估方法还不够完善。已有评估方法大多依赖定性分析而缺乏量化标准与模式，使评估结果具有主观性与不一致性。在进行风险评估时，常会忽略新兴威胁与复杂的攻击手段，使得评估结果不能正确地反映风险的现状。例如，传统的评价方式可能没有充分地考虑到高级持续性威胁（APT）和其他新型攻击手段的潜在影响。风险评估的执行通常缺乏系统性与持续性，许多组织只对初始阶段做出评价，忽略定期更新与动态调整的意义。因此，现有风险评估方法还不完善，导致关键信息基础设施风险识别与管理成效较差。

2.3 对新兴威胁的响应能力不足

在科技不断进步、网络环境日趋复杂的今天，新兴威胁类型越来越多，给关键信息基础设施安全防护带来了新挑战。然而，目前很多组织在面对新兴威胁时缺乏高效的预警机制，不能及时发现并处理威胁。传统的安全防护措施通常以已知攻击模式为攻击目标，对于未知威胁缺乏防护能力，致使新兴威胁易绕开既有防线。另外，当组织面临复杂网络攻击时，存在响应速度较慢、处理能力不强、缺乏高效的应急预案与处理流程等问题，从而造成损失的不断扩大。

2.4 人员安全意识和培训的缺失

许多组织对于职工安全培训还不够重视，这使培训的内容过于简单，不能让职工深刻了解安全威胁。当员工面对越来越复杂的网络攻击手段，会缺乏警觉性与应对策略，从而加大组织的安全风险。此外，职工安全知识与技能普遍不足。在目前网络安全情况下，工作人员需要识别并处理多种安全威胁，但在实际情况中，很多工作人员并不了解安全防护的基本措施。例如，他们并不清楚如何设置高强度的密码，或对于常见的网络诈骗方式如钓鱼邮件，他们可能缺乏足够的识别技巧。这导致职工在面对安全事件时，不能及时预警并处理威胁。频繁的人员流动，对安全培训提出了更大挑战。通常情况下，新入职员工不能及时得到全面的安全培训，而老员工离职后可能会带走有价值的安全知识与经验。这类训练的滞后性与知识的丢失严重地影响着组织的整体安全水平与突发事件处理能力[3]。

3 基于等级保护的关键信息基础设施风险管理策略

3.1 加强等级保护标准与实际操作的对接

现有的等级保护标准较为宏观，缺乏与各行业和系统的适配性。每个行业的关键信息基础设施（CII）都有独特的风险和需求，因此针对性较差的标准难以完全覆盖实际需求。为了解决这个问题，技术人员需要根据具体行业的实际情况，定制化地解读和应用等级保护标准。例如，电力行业和金融行业的关键信息基础设施在安全需求、攻击面等方面存在很大差异，因此需要将等级保护标准与行业特定的风险管理措施相结合。加强等级保护标准与实际操作对接的一个重要方向是将标准的实施过程工具化和流程化。这意味着需要开发一套成熟的工具体系，能自动化地完成风险评估、漏洞扫描、应急响应等操作，从而提高执行效率。例如，现有的安全评估工具大多局限于单一功能，如防火墙配置检查或补丁管理，而综合性的工具可以将这些功能整合，自动生成符合等级保护标准的安全评估报告。这不仅有助于安全人员及时发现潜在风险，还能为后续的安全改进提供详细的操作建议。通过这样的工具平台，能更好地将等级保护标准落实到实际操作中。此外，技术创新在推动标准与实践结合方面也发挥着关键作用。人工智能（AI）和机器学习技术可以在大规模网络环境中通过自动化的数据分析，帮助识别异常行为，甚至预测潜在攻击。具体来说，基于机器学习的威胁检测系统可以通过训练模型，识别出传统规则检测系统难以捕捉到的新型威胁，从而补充现有的等级保护体系。例如，银行系统中的交易数据量大且复杂，使用AI技术可以在无监督学习中自动发现异常交易模式，从而对可能的网络攻击进行预警。因此，将等级保护标准与这些新兴技术结合，能有效提升关键信息基础设施的防护能力。

3.2 完善风险评估模型与工具

为了应对关键信息基础设施（CII）面临的多样化威胁，完善的风险评估模型与工具显得尤为重要。当前的风险评估模型通常基于传统的静态评估方法，难以动态响应不断变化的威胁环境。因此，如何开发出更加灵活、智能化的风险评估模型，是提升CII防护水平的关键。一个有效的方向是结合动态风险评估技术，将评估过程从静态转向动态。通过监控基础设施的实时运行状态，动态风险评估可以随时捕捉和分析系统的变化，进而调整防护策略。例如，基于网络流量的实时监控可以自动检测到网络中的异常行为，进而动态调整系统的防御策略，如提高安全控制强度或启用额外的认证手段。在此基础上，可以将数据分析与机器学习相结合。传统的风险评估依赖于人工判断和经验，而现代大数据分析工具则可以通过分析海量数据，快速识别出潜在的风险。具体来说，使用机器学习技术可以建立基于历史数据的预测模型，通过识别出常见的风险模式，工具可以提前对未来可能的攻击做出预警。例如，在航空领域，分析大量飞行器数据的风险评估工具可以识别出特定模式的设备故障风险，进而提前采取维护措施，减少事故发生的概率。对于关键信息基础设施，这种基于数据的风险评估方式同样适用，可以大幅提升评估的准确性和时效性。此外，随着网络攻击手段的日益复杂化，传统的定期风险评估方式已无法满足需求。近年来，基于自动化和智能化技术的风险评估工具逐渐兴起，具备高效、实时的特性。以自适应安全框架为例，该框架能根

据系统当前状态和外部威胁环境的变化，自动调节风险评估模型。例如，在发生攻击时，自适应安全系统会自动识别攻击类型，并通过调整风险评估参数，如提高攻击强度预估，帮助系统更好地防御。此外，区块链技术也为风险评估工具的完善带来了新的可能性。通过区块链技术，关键信息基础设施中的风险评估数据可以实现不可篡改和透明化，确保风险评估过程的公正性和可信性，从而为风险管理提供更可靠的依据[4]。

3.3 提升对新兴威胁的监测与响应能力

随着信息技术的快速发展，关键信息基础设施（CII）面临的威胁也在不断演变。传统的威胁监测手段已难以应对新兴的网络攻击方式，如高级持续威胁（APT）、零日漏洞攻击和物联网设备的攻击。因此，CII的风险管理策略必须具备更强的威胁监测和响应能力，以应对这些复杂的新兴威胁。具体技术措施可以通过引入机器学习和大数据分析技术，增强威胁检测的精准度。利用深度学习算法分析海量网络流量数据，可以发现隐藏在正常通信中的异常行为，如恶意流量的突发增加或系统内部的异常通信。同时，通过威胁情报共享平台，企业可以及时获得全球范围内的新兴威胁情报，提前部署防御措施。此外，快速响应机制是提升防护能力的关键。通过自动化的应急响应工具，如基于人工智能的安全自动化编排和响应（SOAR）系统，可以快速识别和隔离受到攻击的系统，避免威胁扩散。这类工具不仅能提高响应速度，还能减少人为操作的失误。结合态势感知系统（Cyber Threat Intelligence，CTI），CII能实时分析网络状态，预测潜在威胁，从而提高整体的防御能力。

3.4 加强人员培训与安全意识教育

关键信息基础设施的安全不仅依赖于技术手段，还与操作人员的安全意识和技能水平密切相关。许多网络攻击的成功往往源于内部人员的安全意识薄弱，或由于缺乏针对性培训导致操作失误。因此，制定有效的培训和教育策略，是提升整体安全防护能力的关键环节之一。具体的培训方案应包括多层次的内容设计，从基础的安全意识普及到高级的网络安全防护技能培训，并根据岗位职能的不同进行差异化培训。例如，针对普通员工，重点在于提升其对网络钓鱼、恶意邮件等常见威胁的辨别能力，防止因不慎点击恶意链接而导致的安全事故。在技术创新方面，可以引入模拟攻击演练和虚拟现实（VR）技术，增强培训效果。例如，利用红队和蓝队对抗模拟真实的网络攻击场景，通过实战演练，使安全团队更好地掌握应急响应技能。而通过虚拟现实技术，员工可以沉浸在虚拟的攻击场景中，体验不同类型的网络威胁，从而提高对安全风险的感知能力。此外，安全意识教育应结合定期的考核和评估机制，确保培训内容能有效落实到日常工作中。通过这种持续性的培训与教育，可以不断提升CII运营人员的安全意识和技术能力，有效降低内部安全风险，形成强大的安全防护屏障[5]。

4 结语

在当前信息化快速发展的背景下，关键信息基础设施的安全面临着前所未有的挑战。通过深入分析基于等级保护的关键信息基础设施风险管理中存在的问题，并提出切实可行的策略，本文为提升CII的风险管理水平提供了新的视角和方法。加强等级保护标准与实际操作的对接、完善风险评估模型与工具、提升对新兴威胁的监测与响应能力以及加强人员培训与安全意识教育，是确保CII安全稳定运行的关键。

参考文献

[1] 高伟波，李仲琴.针对我国关键信息基础设施领域安全检查的方法与思路[J].网络安全和信息化，2021(10)：125-131.

[2] 王娟，陈爽，张景明.关键信息基础设施安全检查[J].信息安全与通信保密，2021(6)：52-59.

[3] 禄凯，高亚楠，赵帅.关键信息基础设施动态业务信息安全风险管理方法[C]//2020中国网络安全等级保护和关键信息基础设施保护大会论文集，2020：207-212.

[4] 刘蓓.国内外关键信息基础设施安全保护现状综述[J].信息安全研究，2020，6(11)：1017-1021.

[5] 王凤娇，魏军.美国关键基础设施风险管理新方法——国家关键功能集探究[J].中国信息安全，2020(4)：68-71.