网络空间安全视角下的信息安全与等保测评协同机制探索

郭建宇

中国电力科学研究院有限公司，北京，100192；

摘要：本文从网络空间安全视角出发，深入探讨了信息安全与等保测评的协同机制。首先，分析了当前网络空间安全与信息安全的现状，揭示了恶意软件攻击、网络钓鱼等多样化威胁的严峻性。其次，阐述了等保测评的基本原理和实践应用，展示了其在提升信息系统安全防护能力中的重要作用。接着，论证了信息安全与等保测评协同机制的必要性，指出其在优化资源配置、提升安全管理效率等方面的显著优势。最后，设计了协同机制的具体内容和实施步骤，并通过试点验证了其有效性和可操作性。研究结果表明，协同机制能够全面提升信息系统的安全防护能力，为构建安全的网络空间提供有力保障。

关键词：网络空间安全；信息安全；等保测评；协同机制；安全防护

DOI：10.69979/3041-0673.26.01.071

引言

网络空间安全在信息化社会中具有重要战略地位，随着信息技术的快速发展，网络安全威胁日益增多，如恶意软件攻击、网络钓鱼、数据泄露等，严重危害国家安全、企业发展和个人隐私。加强网络空间安全防护已成为当务之急。

信息安全与等级保护测评（等保测评）是保障网络空间安全的核心手段。信息安全通过技术与管理措施保障信息系统的保密性、完整性与可用性；等保测评则依据国家等级保护制度，对信息系统进行风险评估与分级防护，推动安全管理规范化。两者协同可构建多层次、系统化的安全防护体系。

在此背景下，研究信息安全与等保测评的协同机制，对于提升安全防护能力具有重要意义。该机制有助于优化资源配置、提高管理效率，推动技术创新与应用，为构建安全可靠的网络环境提供理论支持和实践路径。

本文围绕网络空间安全视角，系统分析当前安全形势与挑战，阐述等保测评的原理与应用，探讨二者协同的必要性与实施路径，并设计具体协同机制及实施步骤，开展效果评估。旨在为提升我国网络空间安全防护能力提供科学依据和可行方案。

1 网络空间安全与信息安全的现状分析

网络空间安全面临恶意软件攻击、网络钓鱼、数据泄露、DDoS 攻击及内部威胁等挑战。恶意软件通过病毒、木马窃取或破坏数据；网络钓鱼利用伪装信息诱骗用户泄露敏感信息；数据泄露频发，危及个人隐私和企业机密；DDoS 攻击使目标服务器瘫痪；内部威胁则源于组织内部人员的行为，无论是故意还是无意。

信息安全在保障网络安全中至关重要，采用加密技术、访问控制、防火墙等措施防止未授权访问和数据泄露。信息安全管理体系（ISMS）能系统识别、评估和管理风险，增强整体防护能力。普及信息安全教育和培训，可以提升用户的安全意识和防范技能，减少安全事件的发生。信息安全是技术、管理、教育和法律的综合体现。

国际上，美国与欧盟在信息安全领域投入大，技术水平领先且法律体系健全。美国的《网络安全法案》加强了国家级信息安全；欧盟的 GDPR 对数据保护提出了严格要求。我国信息安全起步虽晚，但发展迅速，已出台《网络安全法》、《数据安全法》等法规，促进信息安全体系构建。国内企业在技术研发和人才培养方面取得了进展，但仍面临技术短板和人才缺口问题。

综上所述，网络空间安全威胁复杂多变，信息安全作为基础性因素，在应对这些威胁中发挥关键作用。国内外均致力于建立更完善的安全防护体系，尽管侧重点不同，但在强化立法、技术创新、人才培养等方面的努力一致，共同应对日益增长的网络安全挑战。

2 等保测评的基本原理与实践

等保测评，即等级保护测评，是基于国家信息安全等级保护制度的一项重要工作。其基本原理是根据信息系统的重要性和面临的风险，将其划分为不同的安全等级，并依据相应的标准进行安全建设和测评。等保测评的标准主要包括《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护基本要

求》等，这些标准详细规定了各等级信息系统的安全要求和技术指标。

在信息安全中，等保测评的具体应用体现在多个方面。首先，通过等保测评，可以系统性地识别和评估信息系统的安全风险，发现潜在的安全漏洞和隐患。其次，等保测评推动了信息安全建设的规范化，确保信息系统按照国家标准进行安全设计和实施。此外，等保测评结果为信息系统的安全整改提供了依据，帮助组织有针对性地提升安全防护能力。例如，某金融机构在实施等保测评后，发现其核心业务系统存在多项安全漏洞，随后根据测评结果进行了全面的安全整改，有效提升了系统的安全性和稳定性。

案例分析方面，某大型国有企业在成功实施等保测评的案例中，展现了等保测评在信息安全中的重要作用。该企业信息系统复杂，涉及大量敏感数据和核心业务。在开展等保测评前，企业信息安全状况较为混乱，缺乏统一的安全管理和技术防护措施。通过引入等保测评，企业首先对信息系统进行了全面的安全评估，识别出多项高风险漏洞。随后，依据测评结果，企业制定了详细的安全整改方案，包括加强访问控制、完善数据加密措施、提升网络安全防护等。经过一系列整改措施，企业的信息系统安全等级显著提升，成功通过了三级等保测评，确保了核心业务和数据的安全。

通过上述分析可以看出，等保测评在信息安全中发挥了重要作用，不仅提升了信息系统的安全防护能力，还为信息安全建设提供了科学依据和规范化指导。成功实施等保测评的案例进一步验证了其在实际应用中的有效性。

3 信息安全与等保测评协同机制的必要性

在当前网络空间安全形势日益严峻的背景下，信息安全与等保测评的协同显得尤为重要。首先，信息安全涉及多个层面，包括技术、管理和法律等方面，而等保测评则提供了系统性的安全评估和建设框架。两者的协同能够实现优势互补，全面提升信息系统的安全防护能力。具体而言，信息安全通过技术手段和管理措施保障信息系统的正常运行，而等保测评则通过标准化的评估流程，发现和弥补安全漏洞，确保信息安全措施的有效性。

协同机制对提升网络空间安全的作用主要体现在以下几个方面。首先，协同机制能够实现资源的优化配置，避免重复建设和资源浪费。通过整合信息安全与等保测评的资源，可以形成合力，集中力量解决关键安全问题。其次，协同机制有助于提升安全管理的效率，通过统一的安全标准和流程，简化管理环节，提高响应速度。此外，协同机制还能够促进信息安全技术的创新和应用，推动安全防护能力的持续提升。

然而，当前协同机制在实际应用中仍存在一些问题和挑战。首先，协同机制的顶层设计和统筹规划不足，导致各部门、各环节之间的协同不够顺畅，信息共享和资源整合存在障碍。其次，现有的协同机制缺乏有效的激励机制，难以调动各方参与的积极性，影响协同效果。此外，技术层面的兼容性问题也是一大挑战，不同安全产品和服务的兼容性差，增加了协同实施的难度。

进一步分析，协同机制在实施过程中还面临法律法规不完善、专业人才匮乏等问题。法律法规的不完善导致协同机制缺乏有力的法律支撑，难以形成长效机制。而专业人才的匮乏则直接影响协同机制的实施效果，难以满足复杂多变的安全需求。

综上所述，信息安全与等保测评的协同机制在网络空间安全中具有重要意义，但同时也面临诸多挑战。解决这些问题，需要从顶层设计、激励机制、技术兼容性等多方面入手，全面提升协同机制的效能。

4 网络空间安全视角下的信息安全与等保测评协同机制探索

在明确信息安全与等保测评协同机制的必要性之后，进一步探讨其设计原则和目标显得尤为重要。首先，协同机制的设计应遵循系统性原则，确保信息安全与等保测评在各个层面上的有机融合。其次，高效性原则要求协同机制能够优化资源配置，提升安全管理效率。此外，可操作性原则强调协同机制应具备实际可行的操作流程，便于各方执行。最终，协同机制的目标在于构建一个全方位、多层次的网络空间安全保障体系，实现信息系统的持续安全。

具体而言，协同机制的内容涵盖技术协同、管理协同和法规协同三个方面。技术协同通过整合信息安全技术与等保测评工具，形成统一的技术标准和技术平台，确保技术层面的无缝对接。管理协同则强调建立跨部门、跨层级的管理协调机制，实现信息共享和资源整合。法规协同则需完善相关法律法规，为协同机制提供坚实的法律支撑。

实施步骤方面，协同机制可分为四个阶段。首先，顶层设计阶段，制定总体规划和实施方案，明确各部门职责。其次，资源整合阶段，梳理现有资源，进行优化配置。第三，试点实施阶段，选择典型场景进行试点，验证协同机制的有效性。最后，全面推广阶段，总结试点经验，逐步推广至更广泛的应用场景。

在不同场景下的应用，协同机制展现出显著的适应性。例如，在政府信息系统安全防护中，协同机制能够有效整合各部门资源，提升整体安全水平。在企业信息安全建设中，协同机制有助于企业按照等保标准进行系统建设，降低安全风险。在关键基础设施保护中，协同机制能够实现跨部门、跨领域的协同防护，确保基础设施的安全稳定运行。

通过上述分析可以看出，协同机制在网络空间安全中具有广泛的应用前景和重要的实践意义。通过科学设计和有效实施，协同机制能够全面提升信息系统的安全防护能力，为构建安全的网络空间提供有力保障。

5 协同机制的实施与效果评估

在明确信息安全与等保测评协同机制的设计原则和目标后，其实施过程显得尤为重要。首先，顶层设计阶段需制定总体规划和实施方案，明确各部门职责，确保协同机制的系统性和高效性。其次，资源整合阶段通过梳理现有资源，进行优化配置，为协同机制的顺利实施奠定基础。第三，试点实施阶段选择典型场景进行试点，验证协同机制的有效性和可操作性。最后，全面推广阶段总结试点经验，逐步推广至更广泛的应用场景，确保协同机制的广泛应用和持续优化。

协同机制实施后，效果显著。在政府信息系统安全防护中，协同机制有效整合各部门资源，提升了整体安全水平。在企业信息安全建设中，协同机制帮助企业按照等保标准进行系统建设，降低了安全风险。在关键基础设施保护中，协同机制实现了跨部门、跨领域的协同防护，确保了基础设施的安全稳定运行。

为评估协同机制的实施效果，需建立科学的评估方法和指标体系。评估方法可采用定量与定性相结合的方式，通过数据分析和专家评估，全面衡量协同机制的实际效果。具体指标包括但不限于：资源整合效率、安全管理提升幅度、安全事件发生率、用户满意度等。通过这些指标的综合评估，能够客观反映协同机制的成效，为后续优化提供依据。

综上所述，协同机制的实施过程严谨有序，实施效果显著，评估方法和指标体系科学合理，为网络空间安全提供了有力保障。

6 结论与展望

本研究在网络空间安全视角下，深入探讨了信息安全与等级保护测评（等保测评）的协同机制，取得了一系列重要成果。首先，通过分析当前网络威胁的多样性和严峻性，明确了信息安全在防御恶意软件攻击、网络钓鱼、数据泄露等方面的基础作用。其次，阐述了等保测评的基本原理和应用实践，展示了其在提升信息系统安全防护能力中的关键价值。进一步论证了信息安全与等保测评协同机制的必要性，指出该机制在优化资源配置、提高安全管理效率方面具有显著优势。最后，设计了协同机制的具体内容与实施步骤，并通过试点验证了其可行性和有效性。

然而，研究仍存在不足。一是协同机制的顶层设计尚不完善，部门间协作与信息共享有待加强；二是激励机制和技术兼容性问题尚未有效解决，影响推广落地；三是法律法规保障和专业人才支撑仍显薄弱。

展望未来，应从四个方面推进协同机制优化：加强顶层设计，构建跨层级协作体系；健全激励机制，提升各方参与积极性；推动技术标准统一，增强系统兼容性；完善法规制度，加快专业人才培养。通过以上举措，努力构建更加科学高效的协同机制，全面提升网络空间安全防护能力。

参考文献

[1]段佳宁.基于等保测评的网络安全风险评估与改进研究[J].网络安全和信息化，2025,(05):119-121.
[2]胡赟鹏.网络信息安全等级保护测评方法分析[J].信息与电脑(理论版)，2019，(04):219-220.
[3]张秋妮.安全智能主动防御技术在网络空间中的应用研究[J].软件，2023，44(07):183-186.
[4]沈昌祥.创新发展主动免疫可信计算筑牢网络强国、数字中国安全可信底座[J].网络空间安全科学学报,2023,1(01):1-16.
[5]卢志兴.大数据时代的计算机网络空间安全探析——评《网络空间安全原理与实践》[J].中国科技论文，2023,18(03):359.

作者简介：郭建宇（1995.01—），男，汉，河北保定，中国电力科学研究院有限公司，大学本科，无，网络安全。