ISSN：3078-8994
EISSN：3104-4492

基于实战演练结果的等级保护要求动态调整研究

佘瑾南　佘帅彦　王宇博　文瑞阳　范　军

联通数字科技有限公司，北京 101300

摘　要：在信息技术飞速发展的今天，信息安全所受到的威胁也变得越来越复杂，常规的静态安全防护措施已经不能满足动态变化的安全需求。等级保护要求是信息安全管理中的一种重要手段，对确保信息系统安全发挥着至关重要的作用。现有等级保护体系普遍存在静态化管理和动态需求相脱节，实战演练成果反馈不到位，安全评估和实际防护措施不相适应等诸多问题。针对上述问题，提出一种以实战演练结果为主线的动态调整机制，突出通过加强演练结果数据反馈和运用，并促进等级保护和实时监控深度融合等手段来达到灵活优化等级保护需求的目的。通过这些优化措施可以促进信息系统应对安全威胁，保证其防护策略跟上时代步伐，适应动态环境下安全需求。

关键词：等级保护要求；实战演练；动态调整；信息安全

0. 引言

在互联网与信息技术飞速发展的今天，网络安全问题越来越突出，信息系统安全问题也成了社会各界所关注的重点。等级保护制度是我国信息安全管理中的一项重要内容，其目的是通过采取科学的分级保护措施来保障信息系统安全地运行。在科技不断进步与安全威胁多样化的背景下，传统等级保护需求逐渐显现出静态管理与缺乏灵活调整等缺陷。在如今的复杂安全背景下，如果等级保护的要求不能根据实际的安全威胁和技术的演变及时作出调整，那么它将难以有效地应对新出现的安全问题[1]。因此根据实战演练结果进行动态调整就成了信息安全管理的迫切要求。本论文将深入讨论如何建立灵活，动态的等级保护需求调整机制来增强信息系统应对安全威胁变化的适应性与防护能力。

1. 等级保护要求的重要性

1.1 保障信息安全的重要手段

等级保护制度是国家网络安全管理的基础框架，意在凭借分级、差异化防护和持续改良增强信息系统安全水平，设计重点原则为“分级管理、重点防护”，划分信息系统为不同安全等级，力求有限资源下实现安全投入的最佳分配。实际运行时，等级保护要求不只是安全防护的制度依据，也是组织搭建安全管理体系、执行安全责任的核心手段，凭借分级防护体系的建立，网络基础设施与信息系统可以明确安全边界跟管理边界，有效防范外部攻击跟内部风险叠加带来的隐患。等级保护的执行助推了安全管理从“经验主导”向“标准导向”转变，让信息安全保障从技术范围延伸到组织制度范围，达成安全建设的长期稳定性[2]。

信息化快速发展，网络空间威胁变得多样化、智能化以及持续化，传统防护手段不容易应对复杂变化的攻击情况，以等级保护要求分级防护为重点，让防御体系从被动转为主动预警，为信息安全给出了系统化的方向，重点价值是借助制度化标准，将安全防护融入系统全生命周期，包含设计规划、建设部署以及运行维护各环节，形成闭环控制。借助明确划分安全等级跟责任界限，助推行业和部门间安全管理的协同一致，对核心信息基础设施实行等级保护要求后，防护措施更加具备可测量性与可验证性，为安全审计及风险管理给予了量化参照。

1.2 适应不同层级的安全需求

信息系统在类型、功能、服务对象等方面有明显不同，安全威胁的来源与程度也因行业属性、业务范围和系统规模而变化，等级保护要求的重点优势之一是分层分类的设计理念，让安全防护措施可以跟系统风险等级对应，高等级系统需具备精进的访问控制、可信计算、入侵检测等能力，用以抵御高强度攻击；低等级系统则关注基础防护与运行可用性的平衡，力求成本跟安全之间的合理协调。凭借差异化防护措施，防止资源过于集中或出现防护漏洞，保证整体安全体系的均衡与高效，等级保护制度的实行让组织能依照业务属性以及数据敏感性选取适合的防护深度，达成安全资源的最佳分配。

分级保护要求实际执行时形成了一套可扩展的安全框架，帮助组织在动态环境中持续保持合规与安全，云计算、大数据和人工智能技术广泛应用后，信息系统架构更加繁复，传统静态防护方式不容易应对新兴风险，等级保护制度借助层次化防护模型，把技术、管理跟运维三大要素融合起来，建立了可持续发展的安全治理体系。不同等级的安全要求不只规定了技术标准，也明确了管理职责与应急措施，形

ISSN：3078-8994
EISSN：3104-4492

成从规则到执行的全流程安全保障。

2. 等级保护要求的存在问题

2.1 静态化管理与动态需求脱节

等级保护要求的设计初衷是应接信息系统面对的安全威胁，技术发展和威胁形态一直变化，现有的等级保护体系出现了管理偏固定的问题，要求一旦确定，容易形成固定的形式，不容易快速适应外部环境的变化，信息技术快速发展，新攻击手段以及威胁类型不停出现，静态安全防护措施不容易应接。等级保护要求执行时，安全需求的动态特性跟固定管理模式形成强烈反差，防护手段面对突发安全事件时显得无能为力[3]。

信息系统实际运行时会遭遇各种突发状况，例如外部网络攻击、内部数据泄露等，但是现有的等级保护要求没有设立快速响应的机制，在某些情况下，信息系统的风险等级发生变化，但等级保护要求没能及时跟进，此类要求的固定性，让许多信息系统面对安全威胁时缺乏灵活应对的能力，不容易快速升级防护手段或改变安全方法。这一种一成不变的管理方式，使得等级保护要求跟实际运营中的动态安全需求比较难匹配，减少了防护效果的及时性以及适应能力，等级保护要求的不匹配问题还折射出政策与执行的延迟，伴随信息化建设持续推进，许多新技术被引入信息系统，像云计算、物联网等。不过现有等级保护体系的标准与防护手段依然注重传统技术框架，没能全面顾及新兴技术，这使得等级保护体系不容易跟上技术发展的节奏，形成一种“滞后性”的安全管理，不能及时满足快速变化的网络安全环境提出的防护需求。

2.2 实战演练结果反馈不足

信息安全管理里，实战演练是检验防护措施效果的重要方式，借助模仿真实攻击场景，能整体了解现有安全体系的实际运作情况，但目前不少组织完成等级保护要求后，常忽视利用演练结果优化工作，实战演练的结果没能很好地融入等级保护的动态优化机制，致使实际安全事件发生后，防护手段不容易依据演练结果迅速精进，闭环安全管理没能实现。

演练结果缺乏有效反馈的原因之一是缺少系统化的分析和处理机制，虽然演练期间收集了大量安全事件数据与防护漏洞，但此类数据一般流于表面，没能深度挖掘，很多情况下，演练结果只是简单归入总结部分，未融入实际的等级保护精进环节。缺乏详细的分析以及反馈机制，致使演练的作用没能完全发挥，无法为后续的安全改良给予实用的帮助，反馈的不足还表现在跨部门协作的欠缺，等级保护要求的执行需要多个部门跟职能的配合，例如信息技术部门、安全管理部门以及应急响应团队等。演练结果的反馈一般只局限在某个部门或者层级，缺乏全员加入和横向交流，这样的零散信息传递让演练中发现的问题不容易快速送达相关部门，拖慢了整体安全防护方针的精进，反馈机制的缺陷还使得等级保护要求无法切实融入实际的安全措施，削弱了组织应对安全威胁的实力[4]。

2.3 安全评估与实际防护措施不匹配

安全检查是等级保护要求执行时不能缺少的一环，它帮助组织了解现有信息系统的实际安全状况，目前的安全检查常出现与防护措施不符的情况，这样的不符体现在多个地方，囊括检查标准跟实际风险的差别、检查结果跟防护手段的不衔接等方面。许多信息系统实行等级保护安全检查时，大多更关注技术指标以及合规性要求，却忽视了实际运行中的安全威胁，一些防护手段虽符合标准，但没能针对实际攻击方式，致使面对高级持续性威胁（APT）时缺乏应对能力。

评估跟防护措施的脱节突出体现在缺少动态机制，传统安全分析一般按固定周期开展，结果可能关联后续防护手段，但伴随信息系统发展以及威胁变化，静态方式已无法满足动态需求，许多结果没能及时融入防护手段精进，致使防护方法停留在旧有状态，不容易应对新型攻击形式。冗杂网络环境下，结果没能贴合实际风险识别，拖累了安全防护能力，外部机构与实行单位信息不对等，结果跟实际措施差距明显，忽略了系统运行中的细节问题，后续改良未及时执行，这样的脱节使信息系统出现防护漏洞，不容易建立有效防御体系。

3. 等级保护要求的优化对策

3.1 构建基于实战演练的动态调整机制

建立依据实战演练的灵活精进机制，是加强等级保护体系适应性跟反应能力的重点，信息安全环境持续变动，传统的固定管理方式不容易应对繁复的安全威胁，所以需把实战演练当作安全管理的重点部分，让其与等级保护要求紧密结合，实现灵活改良。凭借设计一套系统化的演练机制，可以模拟各种现实攻击情景，验证等级保护要求应接实际安全事件的能力与适配性，演练中发现的问题跟漏洞，需及时反馈，为优化安全要求给予参照，保证防护措施紧跟最新的安全需求。

演练的动态调整机制不光是防护措施的简单更新，还应是信息系统安全要求、检验标准及管理流程的全面核查，演练结果需借助数据分析、风险判断等方法转化为优化安全的详细行动计划，演练中若发现部分防护措施不容易应接高危攻击，系统等级保护要求需按实际威胁层级重新评定，同样对安全防护手段实行及时改良。这样的灵活精进机制可以保证安全策略跟随威胁变化跟技术发展持续优化，规避静态管理可能引发的风险，为实现高效运作，应

ISSN：3078-8994
EISSN：3104-4492

搭建专门的安全反馈与响应平台，该平台应可以实时跟踪演练进展，及时收集演练结果，自动处理反馈信息。同样的，平台还需整合演练数据、历史事件数据、外部安全情报等资源，形成更准确的安全风险分析模型，供相关部门制定跟精进等级保护要求时参照，借助这样一套全面、多维的反馈机制，信息安全管理可以做到“知己知彼”，快速应接持续变化的网络安全威胁，增强防护水平 [5]。

3.2 强化演练结果的数据反馈与应用

增进演练结果的数据反馈与应用，是增强等级保护要求效益的核心方法，虽然实战演练在信息安全管理中有重要作用，但目前演练结果缺乏详细剖析以及实际使用，限制了其价值的发挥，所以建立一个高效、合理反馈机制，把演练数据转化为防护措施精进的依据，变成增加安全管理水平的必要选择。数据反馈的首要步骤是保证演练结果的准确跟全面，演练中的每个环节都要有严格的数据采集规范，攻击模拟、应急响应、恢复流程等核心指标需详细记录，这些数据不只是对演练结果的简单汇总，还应借助大数据分析技术深度挖掘，找出系统防护的短板跟潜在隐患。凭借分析演练里发现的漏洞根源，可以掌握哪些防护措施没有起到应有作用，为接下来精进等级保护要求给予准确参照，建立完整的数据采集、存储和处理机制，保证演练结果可以快速反馈到安全管理中并得到使用。

演练结果反馈要与风险评估模型相结合，评估防护措施的实效，通过对演练过程中暴露出的漏洞进行分析，快速判断是否对系统等级保护需求产生影响，针对漏洞严重程度及时调整防护策略。反馈内容不局限于报告总结，要通过数据分析、趋势预测等方式对未来安全态势形成判断，适时调整防护要求。演练结果要与全员共享，以保证技术，安全管理及决策层对防护措施调整情况能有充分了解。加强演练结果运用既优化了等级保护需求，又促进了安全管理完善，增强了全员安全意识，同时通过部门间协同合作保证信息系统不断优化。

3.3 推动等级保护与实时监控的深度融合

实时监控系统可以持续跟踪信息系统安全状态，为潜在风险给出实时预警，把等级保护要求与实时监控紧密结合，能在安全威胁刚出现时快速发现问题并采取针对性措施，实时监控不只给予即时的安全状态信息，还能在安全事件发生时自动启动应急响应机制，凭借监控系统反馈的威胁信息，灵活改变防护方略。这样的融合让等级保护体系不再局限于传统的周期性检查，而是迈向动态、实时的安全防护形式，借助整合监控数据跟防护要求，可以实现防护措施的自动优化，保证信息系统运行时始终保持高效的防御能力。

在具体操作中，实时监控需和等级保护要求相协调，实时监控系统可根据所获安全信息灵活变更信息系统防护水平，当系统遭受大规模分布式拒绝服务（DDoS）的攻击时，该监控系统能够迅速评估当前的安全状态，并自动提高其防护能力，同时采取更为严格的防护手段。借助深度融合监控跟随等级保护需求，该安全体系能够对不同等级攻击做出迅速响应，并有效降低体系面临威胁的概率，这种融合不仅加速防护系统反应速度，也使防护方略优化更智能化，降低了人工操作时延，增强了应急处理能力，确保了信息系统处于冗杂状态。

4. 结论

该研究讨论了等级保护需求在现有信息安全环境下的适用情况及存在问题，并提出一种根据实战演练成果进行动态调整的机制。通过加强演练结果数据反馈和运用，以及促进等级保护和实时监控深度融合等措施，能够有效地提高等级保护需求的灵活性、适应性，进而提高信息系统防护能力。这些优化措施在提高应对新兴威胁响应速度的同时，也保证了防护策略得到及时更新与优化，满足了信息技术的发展要求。

参考文献：

[1] 刘红 . 基于等级保护要求的数字化实验室信息安全建设 [J]. 认证技术 , 2021, 000(006):56-58.

[2] 张杨 , 代勇 . 等级保护要求下医院信息安全管理的有效对策探析 [J]. 数字技术与应用 , 2024, 42(12):86-88.

[3] 王建 , 王天屹 , 翟亚红 , 等 .IEC 62443 系统安全要求与等级保护基本要求对比研究 [J]. 综合智慧能源 , 2021, 43(2):72-76.

[4] 杜红军 , 徐世亮 . 基于等级保护的公共体育中心网络安全实施探讨 [J]. 江西通信科技 , 2020(3):2-6.

[5] 任国强 . 一种用于等级保护建设的信息系统安全性能评估方法 :CN202210720822.1[P]. CN115470482A[2025-10-29].

作者简介：余瑾南（1999.07—），男，汉，江苏省宿迁市泗洪县，本科，工程师，研究方向：网络安全。