电子信息工程中网络安全等级保护加固方案的设计

吕　宁
东明县机关事务服务中心　山东　菏泽　274500

摘　要：随着信息技术的飞速发展，电子信息工程在各个领域得到了广泛应用。然而，网络安全问题也日益突出，成为制约电子信息工程进一步发展的重要因素。本文旨在探讨电子信息工程中网络安全等级保护加固方案的设计，通过分析网络安全等级保护的重要性、现状与挑战，提出一套切实可行的加固方案，以期提升电子信息工程的网络安全防护能力。

关键词：电子信息工程；网络安全；等级保护；加固方案

引言

随着信息技术的迅猛发展，电子信息工程已成为现代社会不可或缺的一部分，广泛应用于各个领域，极大地推动了社会进步与发展。然而，伴随着网络技术的广泛应用，网络安全问题也日益凸显，成为制约电子信息工程进一步发展的重要因素。网络安全等级保护作为保障网络安全的重要手段，对于维护国家安全、社会稳定以及保护个人隐私和财产安全具有重要意义，电子信息工程中网络安全等级保护面临着诸多挑战，如法律法规体系尚不完善、技术标准不统一、安全意识薄弱以及新型网络攻击手段的不断涌现等。这些问题给电子信息工程的网络安全带来了严重威胁，亟需采取有效的加固措施来提升网络安全防护能力。

因此，本文旨在探讨电子信息工程中网络安全等级保护加固方案的设计，通过分析现状与挑战，提出切实可行的加固方案，以期为保障电子信息工程的网络安全提供有力支持。电子信息工程作为信息技术的核心领域，涵盖了通信、计算机、控制等多个方面，广泛应用于军事、经济、社会等各个领域。随着网络技术的不断进步，电子信息工程的网络化、智能化水平不断提高，但同时也面临着日益严峻的网络安全威胁。因此，研究电子信息工程中网络安全等级保护加固方案具有重要意义。

1 网络安全等级保护的重要性

网络安全等级保护是根据国家相关法律法规和政策要求，对网络和信息系统实施的分等级、分层次的安全保护。其重要性主要体现在以下几个方面：

保障国家安全和社会稳定：网络和信息系统已经成为国家关键基础设施的重要组成部分，其安全性直接关系到国家安全和社会稳定。通过实施网络安全等级保护，可以确保关键网络和信息系统的安全稳定运行，防止因网络攻击等原因导致国家安全和社会稳定受到威胁。

保护个人隐私和财产安全：随着网络应用的普及，个人隐私和财产安全问题日益突出。通过实施网络安全等级保护，可以加强对个人信息的保护，防止个人隐私泄露和财产损失。

促进电子信息工程健康发展：网络安全是电子信息工程发展的基石。通过实施网络安全等级保护，可以提升电子信息工程的整体安全防护水平，为其健康发展提供有力保障。

2 电子信息工程中网络安全等级保护的问题

2.1 法律法规体系尚不完善

虽然我国已经出台了一系列关于网络安全等级保护的法律法规，但体系尚不完善，存在一些空白和漏洞。一方面，现有的法律法规对于网络安全等级保护的标准和要求规定得不够细致，缺乏具体的操作指南，导致在实际执行过程中难以准确把握和执行。另一方面，随着信息技术的快速发展，新的网络威胁和攻击手段层出不穷，而相关法律法规的更新速度却相对滞后，无法及时应对新出现的安全风险，网络安全等级保护的法律法规在执行力度和监管机制上也存在不足，导致一些违法违规行为得不到有效遏制。

2.2 技术标准不统一

由于缺乏统一的技术标准，不同行业和领域的网络安全等级保护实施情况存在差异，导致整体防护水平参差不齐，新的网络威胁和攻击手段层出不穷，而技术标准的制定和更新往往滞后于技术的发展，导致现有标准难以全面覆盖和应对新的安全挑战。不同行业、不同领域的信息系统具有各自的特性和需求，难以制定出一套适用于所有场景的统一技术标准。因此，在实际操作中，往往需要根据具体情况制定个性化的安全保护方案。网络安全等级保护的技术标准涉及多个部门和领域，包括网络安全、信息技术、法律法规等，各部门之

间在标准制定和执行过程中可能存在协调不足的问题，也加剧了技术标准的不统一。

2.3 安全意识薄弱

对于信息安全的基本概念和重要性认识不足，往往忽视了信息系统中潜在的安全风险，缺乏主动防范和应对安全威胁的意识。还有在实际工作中，可能忽视或违反既定的安全规范和操作流程，如不定期更新密码、随意使用未经授权的软件或设备等，这些行为都可能为信息系统带来安全隐患。而且，对于新兴的网络攻击手段和技术缺乏了解，难以有效识别和防御新型的网络威胁，这也体现了安全意识的不足，在面临安全事件或事故时，可能缺乏有效的应急响应和处理能力，无法迅速、准确地采取措施减轻损失。

2.4 高级持续性威胁（APT）

随着网络攻击技术的不断发展，APT等新型攻击手段给网络安全等级保护带来了新的挑战。网络攻击手段的不断频繁增加，已成为当前网络安全领域面临的一大挑战。随着信息技术的迅猛发展和广泛应用，网络空间成为了攻击者瞄准的新目标。攻击者利用不断演进的技术手段，如高级持续性威胁、零日漏洞利用、分布式拒绝服务攻击等，对网络系统进行渗透、破坏和数据窃取。这些攻击手段不仅种类繁多，而且变化迅速，给网络安全防护带来了极大的困难。网络攻击手段的增加也反映了攻击者背后的动机多样化，包括经济利益、政治目的、恶作剧等。这种多样化的动机驱使攻击者不断创新和尝试新的攻击方法，以突破网络防御体系。

3 电子信息工程中网络安全等级保护加固方案的设计

3.1 完善法律法规体系

保护网络安全的法律主要包括《网络安全法》、《数据安全法》、《个人信息保护法》等，这些法律为网络安全提供了基本的法律框架和保障。为了进一步加强网络安全等级保护，完善法律法规体系是至关重要的一环。

在做法上需要不断修订和完善现有法律，以适应不断变化的网络安全威胁和攻击手段。例如，针对新型网络攻击手段，应及时制定或修订相关法律法规，明确其法律性质和处罚措施，为打击网络犯罪提供有力法律武器。其次，加强法律法规之间的衔接和协调，形成完整、统一的网络安全法律体系。网络安全涉及多个领域和方面，需要不同法律法规之间的紧密配合和协同作战。因此，在制定和修订法律法规时，应注重与其他相关法律法规的衔接和协调，避免出现法律空白或冲突。除此之外，也要加强法律法规的宣传和普及工作，提高全社会的网络安全意识和法律意识。通过广泛宣传网络安全法律法规和案例，增强公众对网络安全的重视程度和自我保护能力，形成全社会共同维护网络安全的良好氛围。

3.2 统一技术标准与规范

制定一套科学、全面、具有可操作性的技术标准与规范体系，对于提升网络安全等级保护水平具有重要意义。统一的技术标准与规范能够确保网络安全技术和产品的兼容性、互操作性和一致性，避免因为技术差异而导致的安全漏洞和风险。同时，明确的技术要求和测试方法，可以帮助组织和机构更好地评估和选择适合的网络安全解决方案，提高网络安全防护的有效性和针对性；统一的技术标准与规范还能够促进网络安全技术的创新和发展，为网络安全产业提供清晰的发展方向和市场需求，推动产业链上下游的协同发展，加强对技术标准与规范的宣传和培训，提高相关人员的认知度和执行力。

3.3 提升安全意识与技能

通过提升基层工作人员的安全意识与技能，并实现规范化培训可以有效加固网络安全等级保护。基层工作人员作为网络安全的第一道防线，他们的安全意识和技能水平直接关系到整个网络系统的安全。因此，加强他们的安全意识和技能培训至关重要。具体而言，提升基层工作人员的安全意识，使他们能够充分认识到网络安全的重要性，时刻保持警惕，及时发现和报告潜在的安全风险。同时，通过规范化培训，使基层工作人员掌握必要的安全技能和知识，能够熟练应对各种网络安全事件，有效阻止攻击者的入侵和破坏。规范化培训还应包括定期的安全演练和实战训练，让基层工作人员在实际操作中不断锻炼和提升安全技能。此外，培训还应涵盖最新的网络安全威胁和攻击手段，使基层工作人员能够及时了解并应对新的安全挑战。

3.4 实施多层次防御策略

网络安全多层防护策略是一种综合性的防御体系，旨在通过多个层次的安全措施来增强网络系统的防护能力。它包括但不限于物理层安全、网络层安全、系统层安全和应用层安全。物理层安全关注网络设备的物理保护，防止未授权访问；网络层安全利用防火墙、入侵检测系统等手段监控和过滤网络流量；系统层安全强化操作系统和数据库的安全性；应用层安全则通过加密技术、身份验证等手段保护应用程序和数据的安全。这种多层防护策略能够有效降低网络攻击的风险，提高整体网络安全水平。

企业，应构建全面的网络安全防护体系，包括部署

防火墙、入侵检测系统等技术手段，对内外部流量进行监控和过滤。同时，企业应定期进行安全审计和漏洞扫描，及时发现并修复潜在的安全隐患。此外，企业还应加强员工的安全意识培训，确保每位员工都能成为网络安全的第一道防线。

政府，应制定和完善网络安全法律法规，为网络安全等级保护提供法律支撑。政府还应加强与国际社会的合作，共同应对跨国网络威胁。在监管方面，政府应建立严格的网络安全监管机制，对关键信息基础设施进行重点保护，确保国家安全和社会稳定。

技术人员，则需不断提升自身的专业技能，紧跟网络安全技术的最新发展。他们应熟悉并掌握各种网络安全工具和技术手段，为企业和政府机构提供专业的安全咨询和服务。此外，技术人员还应积极参与网络安全事件的应急响应工作，快速有效地应对各类网络攻击和威胁。

3.5 加强密码管理与应用

总来的来说加强密码管理与应用既是微观的技术方式也是普及到社会大众的宏观安全理念。在密码的设计上不论是技术部门还是个人家用，密码策略应明确规定密码的长度、复杂度要求，如密码必须包含大小写字母、数字和特殊字符，且长度不少于8位，尤其是公用的网络设备应禁止使用常见的弱密码，如生日、电话号码等，并鼓励用户定期更换密码，以降低被猜测或破解的风险。

在各个APP和基站等网络上进行多因素认证，要求用户在登录时除了提供密码外，还需通过其他验证方式，如手机验证码、指纹识别或硬件令牌等。这种方式能显著提升账号的安全性，即使密码泄露，攻击者也无法轻易登录用户账号。

还有就是加强密码存储与传输的安全性，对于存储在系统中的密码，应采用加密方式进行存储，确保即使系统被攻破，密码信息也不会轻易泄露。同时，在密码传输过程中，应采用安全的加密协议，防止密码在传输过程中被截获或篡改。

3.6 建立应急响应机制

做好应急响应机制是实现网络安全的主要环节。网络威胁日益复杂多变，攻击手段不断翻新，任何网络系统都可能面临潜在的威胁。建立一个有效的应急响应机制，可以在攻击发生时迅速作出反应，最大限度地减少损失。应急响应机制有助于提升组织的整体韧性，通过预定义的流程和策略，组织可以在遭受攻击时快速恢复关键业务功能，确保业务连续性，减少因网络安全事件导致的业务中断。

许多行业标准和法规都明确要求组织必须建立并实施网络安全应急响应计划，以应对可能的安全事件，通过定期的应急演练和培训，组织可以不断提升其应对网络安全事件的能力，增强员工的安全意识和技能。这不仅有助于在实际攻击中更好地应对，也能提升组织的整体网络安全防护水平。

4 结论与展望

本文通过对电子信息工程中网络安全等级保护加固方案的设计进行研究，提出了一套切实可行的加固方案，旨在提升电子信息工程的网络安全防护能力。然而，随着网络技术的不断发展和网络安全威胁的不断演变，加固方案也需要不断更新和完善。未来的研究应重点关注以下几个方面：跟踪网络安全技术的发展趋势，及时将新技术、新方法应用于加固方案中；加强对新型网络攻击手段的研究和防范，提升加固方案的有效性和针对性；深化对相关人员网络安全意识和技能的培养，形成持续的网络安全教育和培训机制。总之，电子信息工程中网络安全等级保护加固方案的设计是一个系统工程，需要政府、企事业单位和社会各界的共同努力和持续关注。通过不断完善加固方案、提升网络安全防护能力，我们可以为电子信息工程的健康发展提供有力保障。

参考文献

[1]赵麓,刘衍峰.习近平关于网络强国的重要论述探析[J/OL].南京邮电大学学报(社会科学版),1-11[2024-07-31].

[2]我国牵头提出的国际标准《网络安全物联网安全与隐私家庭物联网指南》发布[J].信息技术与标准化,2024,(07):6.

[3]周景贤,邹莹芝,田润,等.面向实战能力的智慧机场网络安全防护技术体系建设[J].民航学报,2024,8(04):150-154.