人防信息系统中网络安全防护技术的应用研究

韩亚琼
张家口市人防动员办公室　河北　张家口　075051

摘　要：随着信息技术的飞速发展，人防信息系统作为国家安全和军事行动的重要支撑，其网络安全防护技术的重要性日益凸显。本文旨在探讨人防信息系统中网络安全防护技术的应用现状、面临的挑战以及未来的发展趋势，以期为提升人防信息系统的安全防护能力提供参考。

关键词：人防信息系统；网络安全防护技术；应用

引言

人防信息系统承载着国家军事机密、作战指挥、情报侦察等重要信息，其安全性直接关系到国家安全和军事行动的成败。然而，随着网络攻击手段的不断升级和多样化，人防信息系统面临着前所未有的安全威胁。因此，加强人防信息系统的网络安全防护技术研究与应用，对于确保国家安全和军事优势具有重要意义。

1 人防信息系统中网络安全防护技术的应用现状

1.1 防火墙技术

防火墙作为网络安全防护的第一道防线，在人防信息系统中发挥着举足轻重的作用。防火墙技术通过在网络边界设置访问控制策略，对进出网络的数据流进行监控和过滤，有效限制了非法访问和攻击行为。在人防信息系统中，防火墙技术被广泛应用于内外网隔离。通过设置严格的访问控制规则，防火墙能够确保内部网络与外部网络之间的隔离，防止外部网络中的恶意用户或攻击者直接访问内部网络资源。这些规则可以基于IP地址、端口号、协议类型等多种因素进行设定，实现精细化的访问控制。同时，防火墙还能够对内部网络中的不同区域进行细分，通过设置不同的安全区域和访问控制策略，实现更精细化的安全管理，进一步提高系统的安全性。除了内外网隔离，防火墙技术还在访问控制和入侵检测方面发挥着重要作用。通过配置合理的访问控制策略，防火墙能够限制用户对网络资源的访问权限，防止未经授权的访问和操作。例如，可以设置只允许特定IP地址或用户组访问某些敏感资源，或者限制某些高风险操作的执行。此外，现代防火墙还集成了入侵检测功能，能够对网络流量进行实时监测和分析，通过对比正常网络行为和异常网络行为，及时发现潜在的攻击行为，如端口扫描、DDoS攻击等，并采取相应的防御措施，如阻断攻击源、隔离受感染系统等，有效防止攻击行为的扩散和蔓延。

1.2 入侵检测技术

入侵检测系统（IDS）是人防信息系统中防范黑客攻击、病毒传播等安全威胁的重要手段之一。入侵检测技术通过实时监测网络流量和系统日志，分析网络行为和系统状态，发现异常行为和潜在威胁，并及时报警和响应。在人防信息系统中，入侵检测系统通常被部署在网络的关键节点和关键服务器上，对进出网络的数据流进行实时监测和分析。入侵检测系统可以采用基于签名的检测方法，通过比对已知攻击行为的特征签名来识别潜在的攻击行为。同时，也可以采用基于异常的检测方法，通过建立正常网络行为的模型，实时监测网络流量中的异常行为，如流量突增、异常访问模式等，及时发现潜在的攻击行为。一旦发现攻击行为，入侵检测系统能够立即报警，并提供详细的攻击信息和攻击源追踪信息，为系统的安全防护提供有力支持[1]。此外，入侵检测系统还能够与防火墙、安全审计系统等其他安全防护技术相结合，形成完整的网络安全防护体系。通过共享安全信息和协同工作，这些技术能够相互补充和增强，提高系统的整体安全防护能力。例如，入侵检测系统可以与防火墙联动，当检测到攻击行为时，自动更新防火墙的访问控制策略，阻断攻击源的访问。

1.3 数据加密技术

数据加密技术是保障人防信息系统中数据机密性和完整性的重要手段。通过对传输和存储的数据进行加密处理，数据加密技术能够确保数据在传输过程中不被窃取或篡改，在存储过程中不被非法访问或泄露。在人防信息系统中，数据加密技术被广泛应用于敏感信息的传输和存储过程中。对于需要传输的敏感信息，如军事指令、作战计划等，系统通常采用端到端的加密方式。在发送端，数据被加密成密文后传输；在接收端，密文被解密成明文后使用。这种加密方式能够确保数据在传输过程中不被窃取或篡改。对于需要存储的敏感信息，如

人员档案、武器装备资料等，系统则采用数据库加密或文件加密等方式。数据库加密可以对数据库中的敏感数据进行加密存储，确保数据在存储过程中不被非法访问或泄露；文件加密则可以对文件进行加密处理，确保文件在传输和存储过程中的安全性。此外，数据加密技术还能够与其他安全防护技术相结合，如访问控制、身份认证等，形成更加完善的网络安全防护体系。例如，可以结合身份认证技术，只有经过身份验证的用户才能访问加密的数据；或者结合访问控制技术，限制对加密数据的访问权限，进一步提高数据的安全性和可靠性。

1.4 零信任架构

零信任架构是一种全新的网络安全防护理念，它假设网络中的所有设备和用户都是不可信的，通过严格的身份验证和访问控制策略来确保系统的安全性。在人防信息系统中，零信任架构的应用可以有效提升系统的安全防护水平，降低安全风险。零信任架构的核心思想是“永不信任，始终验证”。在人防信息系统中，这意味着无论用户身处何地、使用何种设备访问系统，都需要经过严格的身份验证和访问控制才能获取相应的资源和服务。为了实现这一目标，零信任架构通常采用多因素身份验证技术，如密码、生物特征（如指纹、面部识别）、智能卡等，提高身份验证的准确性和可靠性。同时，系统还会对用户的身份、设备状态、访问环境等多种因素进行综合评估，确定用户的访问权限和风险等级。在访问控制方面，零信任架构采用基于角色的访问控制（RBAC）或基于属性的访问控制（ABAC）等策略，根据用户的角色、权限和属性来限制其对系统资源的访问和操作。这种细粒度的访问控制策略能够确保用户只能访问其所需的资源，防止未经授权的访问和操作[2]。此外，零信任架构还强调对网络流量的持续监测和分析。通过部署安全监测和分析系统，实时监测网络流量中的异常行为和潜在威胁，如未经授权的访问尝试、数据泄露等。一旦发现异常行为或潜在威胁，系统能够立即报警，并采取相应的防御措施，如阻断访问、隔离受感染系统等，防止攻击行为的扩散和蔓延。

2 人防信息系统中网络安全防护技术面临的挑战

2.1 网络攻击手段的不断升级

随着网络技术的迅猛发展，黑客攻击手段也在持续升级和多样化。传统的防火墙、入侵检测等安全防护技术，在面对如零日漏洞攻击、高级持续性威胁（APT）、勒索软件等新型网络攻击时，显得力不从心[3]。为了应对这一挑战，人防信息系统需要不断更新和升级安全防护技术，引入更智能、更先进的防御机制，如基于行为分析的入侵检测、深度学习算法在恶意软件检测中的应用等，以提高系统的自我防御和应对能力。

2.2 内部威胁的日益严重

内部威胁是人防信息系统面临的另一大安全挑战。内部人员可能因个人利益、不满情绪或被外部势力策反等原因，泄露敏感信息或故意破坏系统安全。因此，人防信息系统需要加强内部安全管理，实施严格的访问控制和身份认证机制，同时加强对内部人员的安全教育和背景审查，确保人员可靠性。

2.3 供应链安全的复杂性

人防信息系统的建设和运行离不开各种软硬件设备和服务的支持。然而，供应链中的任何一个环节存在安全漏洞都可能对系统安全造成威胁。供应商的代码、硬件组件、第三方服务等都可能成为攻击的入口。为了确保供应链的安全，人防信息系统需要建立严格的供应商管理制度，对供应商进行安全审查和评估，确保其产品和服务符合安全标准。同时，还需要加强对供应链中各个环节的监控和管理，及时发现并修复潜在的安全漏洞，确保人防信息系统的整体安全。

3 人防信息系统中网络安全防护技术的未来发展趋势

3.1 智能化安全防护技术

智能化安全防护技术是未来网络安全领域的重要发展方向，它依托于人工智能技术的快速发展，特别是机器学习和深度学习技术的突破。传统的网络安全防护手段往往依赖于静态的规则和签名，难以应对日益复杂和多变的网络威胁。而智能化安全防护技术则通过引入人工智能技术，实现了对网络威胁的自动识别和响应，极大地提升了系统的安全防护能力。机器学习技术能够通过对大量历史数据的学习，建立网络行为的正常模型。当系统检测到与正常模型不符的行为时，即可判定为潜在的网络威胁，并采取相应的防护措施。这种基于行为的检测方式，相比传统的基于签名的检测方式，具有更高的准确性和灵活性。此外，机器学习技术还能够根据网络威胁的演变，不断更新和优化模型，保持防护系统的有效性。深度学习技术在智能化安全防护中也发挥着重要作用。通过构建深层的神经网络模型，深度学习技术能够挖掘出网络数据中的深层特征，实现对复杂网络威胁的精准识别。例如，深度学习技术可以应用于恶意软件的检测中，通过对恶意软件的行为特征进行深度学习，建立恶意软件识别模型，从而实现对新型恶意软件的快速识别和防御。未来，智能化安全防护技术将进一步与人防信息系统融合，形成智能化的安全防护体系。这个体系将具备自我学习、自我适应和自我优化的能

力，能够实时感知网络威胁的变化，动态调整防护策略，确保人防信息系统的安全稳定运行。

3.2 云安全防护技术

随着云计算技术的广泛应用，云安全防护技术也成为了网络安全领域的重要发展方向。云计算技术以其资源弹性、按需服务、高可扩展性等优势，在人防信息系统中得到了广泛应用。然而，云计算环境也带来了新的安全挑战，如云环境中的数据泄露、身份冒用、恶意攻击等。因此，构建云安全防护平台，实现对云环境中各种安全威胁的实时监测和响应，是确保云环境安全可靠的关键。云安全防护技术主要包括云安全访问控制、云数据加密、云安全审计等方面。云安全访问控制通过身份认证、权限管理等手段，确保只有合法的用户才能访问云资源。云数据加密则通过对云中的数据进行加密处理，防止数据在传输和存储过程中被窃取或篡改。云安全审计则通过对云环境中的操作行为进行记录和分析，发现潜在的安全风险[4]。未来，云安全防护技术将进一步发展，形成更加完善的安全防护体系。一方面，云安全防护技术将与其他安全技术如智能化安全防护技术、量子安全防护技术等相结合，形成多层次、立体化的安全防护体系。另一方面，云安全防护技术将更加注重数据的隐私保护和合规性，确保云环境中的数据符合相关法律法规的要求。此外，云安全防护技术还将向自动化、智能化的方向发展。通过引入机器学习和深度学习技术，云安全防护系统能够自动识别和响应网络威胁，减少人工干预，提高防护效率。同时，云安全防护系统还能够根据网络威胁的演变，不断优化和调整防护策略，保持防护系统的有效性。

3.3 量子安全防护技术

量子计算技术的快速发展，为网络安全防护带来了新的机遇和挑战。传统的网络安全防护手段在面对量子计算攻击时可能变得无效，因此，量子安全防护技术成为了未来的重要研究方向。通过引入量子密钥分发、量子加密等量子安全技术，可以实现对传统安全威胁的有效防御，提升系统的安全防护水平。量子密钥分发技术是一种基于量子力学原理的密钥分发方法，能够实现密钥的安全传输，防止密钥在传输过程中被窃取或篡改。与传统的密钥分发方法相比，量子密钥分发技术具有更高的安全性，因为任何对密钥的窃听或篡改行为都会被立即发现。量子加密技术则利用量子力学的特性，对信息进行加密处理，使得加密后的信息在量子计算攻击下仍然保持安全。量子加密技术可以应用于人防信息系统中的数据传输和存储过程中，确保信息的机密性和完整性。未来，量子安全防护技术将进一步发展，形成更加完善的量子安全防护体系。一方面，量子安全防护技术将与其他安全技术如智能化安全防护技术、云安全防护技术等相结合，形成多层次、立体化的安全防护体系。另一方面，量子安全防护技术将更加注重实用性和可扩展性，以满足人防信息系统对安全防护的实际需求。此外，量子安全防护技术的发展还将推动相关标准和规范的制定和完善。随着量子计算技术的不断发展和应用，制定统一的量子安全防护标准和规范，将有助于推动量子安全防护技术的普及和应用，提高人防信息系统的整体安全防护水平。

结语

人防信息系统的网络安全防护技术是确保国家安全和军事优势的重要保障。面对不断升级的网络攻击手段和日益严重的安全威胁，我们需要不断加强网络安全防护技术的研究与应用，提升系统的安全防护能力。同时，我们还需要关注智能化、云化、量子化等未来发展趋势，为人防信息系统的安全防护提供有力支持。

参考文献

[1]中国人防科学技术信息学会第十六届学术年会在京举办[J].情报理论与实践,2024,47(11):209.

[2]郭培馨.人防科技工业涉密信息系统风险管理研究[D].北京邮电大学,2023.

[3]陈凤.网络信息时代人防科技创新管理模式变革相关思考[J].产业创新研究,2023,(04):26-31.

[4]刘霄,王平.面向人防工程无线网络的信息安全防护问题研究[J].科技创新与应用,2021,11(34):87-90.