信息化时代广电网络的安全管理和应急响应机制

张　莉
中国广电新疆网络股份有限公司乌鲁木齐市分公司　新疆　乌鲁木齐　830000

摘　要：信息化时代，广电网络的安全管理和应急响应机制成为保障其稳定运行和用户数据安全的重中之重。文章探讨了广电网络在安全管理方面面临的挑战，包括技术更新滞后、管理人员素质参差不齐等问题，并提出了加大安全技术研发投入、构建统一的安全管理平台等优化策略。同时本文还强调了应急响应机制的重要性，提出完善预警系统、加强恢复与重建管理等措施。通过综合施策，广电网络能够有效提升安全防护能力和应急响应效率，确保网络运行的安全稳定。

关键词：信息化时代；广电网络；安全管理；应急响应机制

1 信息化时代广电网络概述

1.1 广电网络的发展历程与现状

广电网络作为国家重要的信息基础设施，经历了从地方分散到全国统一的整合过程。广电有线网络全面落实中央关于深化文化体制改革、繁荣发展文化事业和文化产业的重要部署，持续推进广电网络转型发展。从2011年底基本实现一省一网，到2020年我国广电网络股份有限公司的成立，标志着全国有线电视网络整合和广电5G建设一体化发展迈出了重要一步。截至2021年底，22家省级子公司冠以“中国广电”完成统一企业名称更名，为统一运营打下基础。广电网络不断推进融合发展，从传统有线电视运营商转为提供有线电视、有线宽带、新媒体、智慧广电、5G等业务的综合信息服务运营商。伴随三网融合、宽带我国等战略推进，有线网络逐步形成多业态格局。特别是智慧广电工程的扎实推进，有线网络业务模式持续创新，如智慧广电乡村工程、智慧广电固边工程等，为广电网络赢得了新的发展空间。

1.2 信息化时代广电网络的技术架构

广电网络的技术架构主要包括前端系统、传输网络和终端接收设备。前端系统是广电网络的核心部分，负责信号的采集、编码、复用和调制等处理。它涵盖了各类节目源的接入，如卫星信号、地面无线信号以及自办节目等，并通过先进的编码技术（如MPEG-4等）将各类信号转换为数字格式，以提高传输效率和图像质量。传输网络则承担着将前端处理后的信号传输到终端用户的任务[1]。常见的传输方式包括有线网络（如同轴电缆、光纤等）以及无线网络（如地面数字电视广播等）。其中，光纤网络具有传输容量大、损耗低、抗干扰能力强等优点，成为了现代广电网络传输的重要手段。终端接收设备则是用户获取广电网络信息的最后一环，包括电视机顶盒、智能电视等。这些设备负责对接收的信号进行解调、解码，并将其转换为可供用户观看的图像和声音。

1.3 广电网络在信息化时代的作用与价值

在信息化时代，广电网络具有不可替代的作用和价值。广电网络具有传输容量大、覆盖范围广、传输质量高等优势，能够高效地传输和播出广播电视信号，满足广大用户的需求。广电网络还提供了数据传输、宽带互联网接入等服务，进一步丰富了其服务内容，提升了用户体验。广电网络还拥有大量的视频内容资源，可以为用户提供丰富的电视节目和互动体验。广电网络在推进智慧广电工程的过程中，不断拓展服务领域，如智慧广电乡村工程、智慧广电固边工程等，为乡村振兴、数字经济发展等提供了有力支撑。更重要的是，广电网络在保障我国文化安全、信息安全等方面也发挥着重要作用。广电网络作为国家的“信息高速公路”，在传播主流价值观、弘扬正能量等方面具有独特的优势，是国家信息化建设的重要力量之一。

2 信息化时代广电网络安全管理的主要内容

2.1 网络安全管理

在信息化时代，广电网络的网络安全管理至关重要。它主要包括网络架构的安全设计、网络流量的监控与分析、网络入侵的检测与防御，以及网络访问控制与身份认证等关键措施。通过构建安全可靠的网络架构，确保数据传输的完整性和保密性，防止外部攻击和内部泄露。利用先进的网络监控和分析工具，实时监测网络流量，及时发现并应对潜在的安全威胁。通过部署网络入侵检测系统（IDS）和入侵防御系统（IPS），有效阻止恶意攻击和病毒传播。最后，实施严格的网络访问控制和身份认证机制，确保只有合法用户才能访问网络资源，进一步提升网络的安全性。

2.2 内容安全管理

内容安全管理是广电网络安全管理的另一重要组成部分。它主要关注广播电视节目内容的审核与监管，以及用户生成内容（UGC）的管理。为确保广播电视节目内容的合法性和合规性，广电网络需要建立严格的内容审核制度，对节目内容进行全面的审查和筛选，防止不良信息的传播。同时对于用户生成的内容，广电网络也需要加强管理和监控，防止虚假信息、恶意攻击和侵权行为的发生。通过实施内容安全管理，广电网络能够维护良好的传播秩序，保护用户的合法权益。

2.3 设备安全管理

设备安全管理是广电网络安全管理的基石。它涵盖了网络设备、服务器、存储设备以及终端设备等的安全管理。广电网络需要定期对设备进行安全检查和更新，确保设备的安全性和稳定性。建立设备安全管理制度，明确设备的使用、维护和报废流程，防止设备被非法使用或恶意攻击[2]。广电网络还需要加强设备的物理安全防护，如安装防盗锁、监控摄像头等，防止设备被盗或损坏。通过实施设备安全管理，广电网络能够确保设备的正常运行和数据的安全存储，为网络安全提供有力保障。

3 信息化时代广电网络安全管理和应急响应机制存在的问题

3.1 安全管理存在的问题

在信息化时代，广电网络安全管理面临着一系列挑战和问题。随着技术的快速发展，网络攻击手段日益复杂和多样化，传统的安全管理手段和技术已经难以有效应对。广电网络在安全防护方面可能存在技术更新滞后的问题，导致安全漏洞频发，难以保障网络的持续稳定运行。安全管理人员的专业素质和技能水平参差不齐，部分人员缺乏必要的安全意识和防范能力，难以有效识别和应对潜在的安全威胁。广电网络在安全管理方面可能存在制度不完善、执行不力等问题，导致安全管理措施难以得到有效落实，存在安全隐患。

3.2 应急响应机制存在的问题

广电网络在应急响应机制方面同样存在着一些问题。首先，应急响应流程可能不够明确和高效，导致在发生安全事件时，无法迅速启动应急响应机制，及时采取有效措施进行处置。这可能导致安全事件的扩散和升级，造成更大的损失。其次，应急响应团队的专业素质和应急能力可能不足，缺乏必要的培训和演练，难以在关键时刻发挥应有的作用。另外，广电网络在应急响应方面可能存在资源不足的问题，如缺乏必要的应急设备和工具，难以有效应对复杂的安全事件。最后，应急响应机制可能缺乏与其他相关部门的协同和配合，导致在处置安全事件时存在信息不畅、协调不力等问题，影响了应急响应的效果。

4 优化广电网络安全管理和应急响应机制的策略

4.1 加大安全技术研发投入

在信息化时代，广电网络面临的安全威胁日益复杂和多样化，传统的安全防护手段已经难以应对。加大安全技术研发投入，提升广电网络的安全防护能力，是优化安全管理的重要策略之一。广电网络应积极引进和应用先进的安全技术，如人工智能、大数据、区块链等，以提升安全防护的智能化和自动化水平。例如，利用人工智能技术，可以实现对网络流量的智能分析和异常检测，及时发现并处置潜在的安全威胁。利用大数据技术，可以对网络日志进行深度挖掘和分析，发现潜在的安全漏洞和攻击模式。而区块链技术则可以用于保障数据的完整性和不可篡改性，提升数据的安全性[3]。广电网络应加强与高校、科研机构以及安全厂商的合作，共同研发适用于广电网络的安全技术和产品。通过产学研合作，可以推动安全技术的创新和应用，提升广电网络的整体安全防护水平。广电网络还应注重安全技术的持续更新和升级，以适应不断变化的安全威胁环境。通过建立安全技术更新机制，定期对现有安全防护手段进行评估和改进，确保广电网络能够始终保持较高的安全防护能力。

4.2 构建统一的安全管理平台，实现集中化管理

为了提升广电网络的安全管理效率和质量，构建统一的安全管理平台，实现集中化管理是必要的策略。广电网络应建立统一的安全管理中心，负责整个网络的安全策略制定、安全事件监控、安全数据分析以及安全响应等工作。通过集中化管理，可以实现对广电网络安全的全面掌控和高效调度。广电网络应在安全管理平台上集成各类安全工具和系统，如防火墙、入侵检测系统、漏洞扫描系统等，实现对网络安全的全方位防护。通过统一的安全管理平台，可以实现对这些安全工具和系统的统一配置、统一监控和统一管理，提升安全防护的效率和准确性。广电网络还应注重安全管理平台的可扩展性和灵活性。随着网络规模的不断扩大和安全威胁的不断变化，安全管理平台需要能够支持新的安全工具和系统的接入和集成，以满足不断变化的安全管理需求。

4.3 完善安全管理制度，加强制度执行监督

完善的安全管理制度是保障广电网络安全的基础。为了优化安全管理，广电网络需要建立健全的安全管理制度体系，并加强制度执行监督。广电网络应制定详

细的安全管理制度和操作规范，明确各级管理人员和操作人员的安全职责和操作要求。这些制度应涵盖网络架构设计、安全防护措施部署、安全事件处置等方面，确保广电网络在各个层面都能得到有效的安全防护。广电网络应加强对安全管理制度的宣传和培训，提高全员的安全意识和防范能力。通过定期的安全培训和演练，可以增强员工对安全管理制度的理解和掌握，提升他们的安全操作技能和应急响应能力。广电网络还应建立安全管理制度执行监督机制，定期对制度执行情况进行检查和评估。通过监督机制的建立，可以及时发现制度执行中存在的问题和不足，并采取有效的措施进行整改和改进，确保安全管理制度得到有效落实。

4.4 采用先进的监测技术，提高预警准确性

在信息化时代背景下，广电网络面临着来自各方的安全威胁，这些威胁不仅形式多样，而且隐蔽性强，传统的安全防护手段已经难以应对。引入和应用先进的监测技术成为提升广电网络安全防护能力的必然选择。广电网络应首先引入实时的网络流量监测和分析系统。该系统能够全面、细致地监控和分析网络流量的变化，及时发现异常行为。通过实时监测，广电网络可以迅速捕捉到潜在的安全威胁和攻击行为，从而为及时处置提供有力支持。这种实时监测的方式可以大大提高安全响应的速度，减少安全事件对网络运行和用户数据的影响。除了实时监测网络流量，广电网络还应利用大数据技术和机器学习算法对网络日志和事件数据进行深度挖掘和分析。通过挖掘数据中的关联性和模式特征，广电网络可以发现潜在的安全漏洞和攻击模式。这些发现不仅有助于广电网络及时修补漏洞，还能为制定更有效的安全防护策略提供科学依据。广电网络还应建立安全事件预警机制，该机制应根据监测和分析结果，及时发出安全预警信息。通过预警机制，广电网络可以提醒相关人员及时采取措施进行处置，防止安全事件的扩散和升级。这种预警机制不仅可以提高广电网络的安全防护能力，还能为用户数据的安全提供有力保障。

4.5 加强恢复与重建管理

在发生安全事件后，快速恢复和重建广电网络是保障业务连续性和用户权益的关键。加强恢复与重建管理是优化应急响应机制的重要策略。广电网络应建立完善的灾难恢复计划，明确灾难恢复的目标、策略和流程。灾难恢复计划应涵盖数据备份、系统恢复、业务恢复等方面，确保在发生安全事件后能够迅速恢复网络的正常运行[4]。广电网络应定期对灾难恢复计划进行测试和演练，确保计划的可行性和有效性。通过测试和演练，可以发现计划中存在的问题和不足，并及时进行改进和完善。广电网络还应加强恢复与重建过程中的资源调配和协同合作。在发生安全事件后，应迅速调动相关资源和人员，进行紧急处置和恢复工作。加强与相关部门的协同合作，确保信息畅通、协调有力，共同应对安全事件带来的挑战。在恢复与重建过程中，广电网络还应注重经验教训的总结和分享。通过对安全事件的深入分析和总结，可以提炼出有效的应对策略和措施，为今后的安全管理提供有益的借鉴和参考。加强与行业内外的交流与合作，分享安全管理和应急响应的经验和教训，共同提升整个行业的安全防护水平。

结束语

综上所述，信息化时代广电网络的安全管理和应急响应机制是保障其稳定运行的基石。面对日益复杂的安全威胁，广电网络需要不断更新安全防护手段，提升应急响应能力。通过加强技术研发、完善管理制度、采用先进监测技术等措施，广电网络能够有效应对各类安全挑战，确保用户数据的安全和网络服务的稳定。未来，广电网络将继续加强安全管理和应急响应机制建设，为信息化建设提供坚实保障。

参考文献

[1]刘颖.5G网络环境下广播电视网络安全风险分析[J].中国传媒科技,2021(9):50-52.

[2]刘志东,唐璠,谢晓旭.浅谈如何做好广电日常信息安全管理[J].广播电视网络,2022,29(3):69-71.

[3]刘岩峰,李鹏.广电系统中的信息安全技术分析[J].黑龙江广播电视技术,2021(4):72-73.

[4]吕恒月.广电网络中的智能应急广播系统技术探究[J].西部广播电视,2022,43(01):238-240.