**广播电视与视听新媒体行业网络安全监管研究**

**朱小斌**

**韶关市广播电视台 广东韶关 512000**

**摘要：**现阶段的广播电视行业以及视听新媒体行业正在趋向于实现平稳快速的发展，视听新媒体主要建立在网络信息化的技术支撑平台作为保障的前提下，因此凸显了监管广播电视网络数据传输安全的必要性。在目前的现状下，新媒体与广播电视传统视听媒体的全面融合过程仍然存在着网络信息的安全威胁隐患，进而导致了广播电视的融媒体信息传播过程受到不良的影响。本文主要探讨了网络安全监管融入于视听新媒体以及广播电视行业发展的总体技术方案，合理健全广电行业与新媒体行业现有的网络安全监督管理架构。

**关键词：网络视听平台；网络安全；网络架构**

在当前时期的广播电视以及融媒体行业迅猛发展的总体趋势推动促进下，新媒体对传统广播电视行业发起挑战的同时也为其创造了前所未有的发展机遇。视听新媒体构成了广播电视受众全面分享以及实时接收广播电视节目信息数据的关键实现途径，视听新媒体的网络信息传播过程能否保证最基本的网络信息安全，在根本上关系到视听新媒体与广播电视的健康发展。由此能够确定，全面完善建立广电视听新媒体的信息传输过程安全保障以及风险防范机制具有突出的必要性。

**一、广播电视与视听新媒体行业网络安全监管的目前实施状况**

广播电视行业目前已经表现为快速发展的总体态势，现阶段的广播电视行业正在全面趋向于信息化、智能化以及自动化的总体技术转型。广播电视的信息传播形式目前由于网络技术的冲击影响，因此决定了网络视听新媒体将会占据主导的数据信息传播地位。近些年以来，视听新媒体与传统的广播电视传播媒体已经促进实现了更加紧密的媒体全面融合，客观上显示出网络信息化的视听媒体实践优势[1]。

广播电视的媒体信息传输以及数据资源的传播共享主要依靠于光纤网络作为基础的平台支撑，通过布置广电信息传输与发送的分配器来促进达到全面接入无线网络传播信号的目标[2]。在此前提下，广播电视的传播数据以及传输信号各个阶段步骤主要依靠于智能化的信号发送以及信号转换的技术手段，确保实现了清晰以及完整的广电节目数据、图像与声音信息传播效果。现阶段的网络新兴媒体已经广泛融入到广播电视的节目信息生成、信息传输处理以及信息接收过程，网络信息化的新兴媒体本身具备了较为明显的快捷性与实时性，从而在根本上优化了广播电视的传统媒体信息接收以及转化与处理机制。

但是与此同时，现阶段的网络病毒入侵、非法访问以及黑客侵入等常见的安全风险因素也具有普遍存在的特征，如安全漏洞不断被发现，黑客的技巧和破坏能力不断提高，网络安全形势日趋严峻。我们如果未能做到全面关注于广播电视媒体以及网络新兴媒体的安全监管工作，则会容易产生广播电视的数据信息资源严重损失。由此可见，做好综合性以及全面性的视听新媒体行业与广电行业安全监督控制工作，具有显著的安全保障作用。

**二、广播电视与视听新媒体行业网络安全监管的核心技术要点**

（一）病毒防护以及入侵检测技术

面对网络安全问题越来越复杂，安全威胁正在飞速增长，尤其是基于应用的新型威胁，如隐藏在 HTTP 等基础协议之上的应用层攻击问题、web2.0 安全问题、木马后门、间谍软件、僵尸网络、DDoS 攻击、网络资源滥用（P2P 下载、IM 即时通讯、网游、视频）等，给广播电视与视听新媒体行业的信息网络造成严重的破坏，严重影响了广播电视与视听新媒体行业的进一步发展，因此，针对广播电视网络的病毒防护以及入侵检测等技术运用显得尤为重要。广播电视网络的病毒防护技术，重点针对于破坏性的网络攻击病毒来采取全方位的可行防范技术手段。我们通过采取全面识别以及准确检测网络非法入侵因素的专业方法，同时，结合实际编订详尽的内部技术防范手册，组建专项工作小组并做好功能性分工，开展各类网络攻防演练完善工作流程和及时修复漏洞。并且根据不同系统以及不同板块进行网络安全设备布局，如：网络视听类平台应配置堡垒机、WAF防火墙、日志审计、NF防火墙等；素材传输系统则需要配置网间媒体文件安全传输设备、媒体素材安全上载设备等。通过对智能协议识别、协议异常检测、流量异常检测、会话关联分析，以及状态防火墙等多种技术对于具有异常表现形式的网络入侵因素给予更加精准的测试判断，据此实现了全面测试入侵病毒以及系统安全破坏因素的目标。在目前的现状下，针对广电网络系统专门实施的系统入侵检测以及病毒防护方案已经逐步获得了健全完善，集中体现在网络杀毒软件、边界管理设备、系统端口管控以及网络防火墙的协同作用发挥。



（二）网络数据库技术

网络数据库的安全保障技术属于核心性的广电视听新媒体安全防护技术，在广电网络的基本组成架构中，网络数据库的价值与作用就是全面存储以及转发实时性的广播电视信号传输数据，据此实现了科学管理以及精准分类的目标。现阶段的广电部门网络数据库普遍存在着较为庞大的数据资源存储规模特征，从而体现了严格保护广电网络数据库安全的必要性[3]。简而言之，网络数据库技术保证了数据的可靠性和可用性；利用并发控制机制保证数据的一致性和完整性；实现数据的实时同步和复制，确保多个数据库之间的数据一致性。

（三）访问身份的验证技术

不法分子只有做到了成功进入广电网络的系统数据库，才能据此实现盗取信息数据以及破坏广电网络正常运行的企图。因此，全面设置自动化的访问身份检测验证机制具有重要的网络安全监督与保障意义[4]。目前运用于验证以及检测网络访问身份的信息技术手段呈现出多样性的总体发展特征，从而决定了全面维护广电网络信息安全中的访问身份验证手段必须要合理采用。系统经过专业性的验证检测以后，对于不具备合法进入以及访问身份的主体将会发出报警信号，提示广电网络的监管人员予以警惕。加密和身份验证等技术最大限度地保护了数据的安全性，防止未经授权的访问和篡改，保障了数据安全；

**三、广播电视与视听新媒体行业网络安全监管的架构完善措施**

（一）集中式网络的分布管理

集中式网络在当前阶段已经广泛采用于视听新媒体以及广电行业领域，集中式的广播电视安全传输网络由于具备了非常强大的数据整合处理实践功能，从而显著影响到广播电视网络的数据共享以及信息传播。采取分布式的广电网络创新管理实践思路，总体上有助于广播电视网络的良好实践作用获得最大程度的体现发挥，构建了多元化与全方位的广电网络资源共享平台。

（二）网络传输信号管理

广播电视的网络系统实时传播数据信号必须要保证良好的精准程度，否则如果缺少了数据传输全面实施过程中的精准性因素作为基本的保障前提，那么将会导致广电网络的传输信息过程存在频繁中断或者遭受外界作用破坏的可能性[5]。在此基础上，我们目前有必要更加重视广播电视网络的传输信号安全监督工作，旨在做到提前防范以及准确预测网络传输的信息风险隐患。信息安全的监控系统终端主要设计为子系统与主系统的互联模式，采取远程自动化的监控管理安全保障机制。

（三）网络数据库的信息共享管理

广播电视的网络数据库具有全面共享网络信息资源的作用，也决定了现有信息资源必须要得到更大程度的共享。采取分级管理的广播电视信息资源安全共享机制，有助于合理扩大广电部门数据库的资源共享具体适用范围，采取全方位的资源共享以及受众参与机制，从而有效确保了广播电视受众的资源共享。

**结束语：**

经过分析可见，现阶段的广播电视网络正在全面融入于视听新媒体受众的生活实践领域，充分展现出视听新媒体特有的信息传输快捷性、实效性与安全性优势。然而从广播电视的网络媒体融合发展角度加以分析，可见当前阶段发展环境下的网络安全监管力度还很薄弱，从而导致了广播电视网络的信息数据资源共享实践过程普遍遇到多个层面的信息安全威胁。为了促进实现网络视听新媒体的技术转型目标，那么目前的完善思路应当体现在健全广电网络数据库的安全防范监督机制，采取集中式网络的分布管理技术来妥善维护广电网络的数据信息传播过程安全。

**参考文献：**

[1]马玉红.广播电视与视听新媒体行业网络安全监管探讨[J].传媒论坛,2021,04(13):10-11.

[2]郝东亮.省级广播电视与视听新媒体监测监管平台设计方案[J].广播与电视技术,2020,47(04):98-103.

[3]曹林.新媒体网站安全技术与安全体系的建设[J].传播力研究,2022,02(30):103.

[4]李宇.辽阳广播电视台广电网络安全监管系统的设计分析[J].广播电视信息,2022(09):76-80.

[5]张智南,柯贤良,傅爱民.基于SECaaS模式的网络安全监管服务化研究[J].信息技术与网络安全,2021,37(08):23-26.