Software Engineering and Applications 软件工程与应用, 2024, 13(2), 165-172
Published Online April 2024 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2024.132017

Hans汉斯

气象现代化信息网络安全治理技术研究

姜　慧，程　铭，陈艳丽，樊　杰

菏泽市气象局，山东　菏泽

收稿日期：2024年1月19日；录用日期：2024年3月27日；发布日期：2024年4月7日

摘　要

随着各类信息技术的不断涌现和发展，在推动气象业务现代化发展的同时，气象发展的外部环境逐渐趋于复杂化，各类网络安全问题频繁发生，网络安全形式日益严峻。本文针对菏泽市气象局气象信息网络现状进行分析，剖析气象业务现代化发展中面临的网络安全问题，不断加强信息网络安全管理工作和提升安全防护技术手段。技术层面，从加强终端软件安全防御和网络安全设备规划，完善优化信息网络安全架构；管理层面，从建立安全运营中心、加强网络安全管理制度建设、监控预警应急通报、经费保障和宣传培训等方面，提出提升气象现代化信息网络安全治理技术。推动实现网络安全治理能力现代化，为气象事业高质量发展提供坚实的网络安全保障。

关键词

气象业务，现代化，网络安全，治理技术

Research on the Security and Governance Technology of Meteorological Modern Information Network

Hui Jiang, Ming Cheng, Yanli Chen, Jie Fan

Heze Meteorological Bureau, Heze Shandong

Received: Jan. 19th, 2024; accepted: Mar. 27th, 2024; published: Apr. 7th, 2024

Abstract

With the continuous emergence and development of various information technologies, while promoting the modernization of meteorological services, the external environment of meteorological development is gradually becoming more complex, and various network security issues occur frequently, making the form of network security increasingly severe. This article analyzes the current

文章引用：姜慧，程铭，陈艳丽，樊杰．气象现代化信息网络安全治理技术研究[J]．软件工程与应用，2024，13(2)：165-172. DOI: 10.12677/sea.2024.132017

situation of the meteorological information network of Heze Meteorological Bureau, analyzes the network security issues faced in the modernization of meteorological business development, continuously strengthens information network security management work, and improves security protection technology. At the technical level, we will strengthen terminal software security defense and network security equipment planning, and improve the information network security architecture; At the management level, it is proposed to enhance modern meteorological information network security governance technology by strengthening network security operation management, monitoring and early warning emergency notification, funding guarantee, and publicity and training. Promote the modernization of network security governance capabilities and provide solid network security guarantees for the high-quality development of meteorological undertakings.

Keywords

Meteorological Operations, Modernization, Cyber Security, Governance Technologies

1. 引言

“没有网络安全就没有国家安全，没有信息化就没有现代化”，气象事业高质量发展离不开信息化支撑，也离不开气象网络安全保障。气象业务信息化系统是国家级的关键信息基础设施，对各项生产经营活动有着重大的意义[1]。云计算、大数据、物联网、人工智能及移动互联网等新技术快速融入气象业务，促进了气象事业的快速发展。随着各类信息技术的不断涌现和发展，在推动气象网络现代化发展的同时，气象事业发展的外部环境逐渐趋于复杂化，各类网络安全问题频繁发生。网络是气象数据传输和共享的基础平台，一旦出现问题，就会影响数据的传输和安全，对防灾减灾工作也会产生较大影响，所以开展气象信息网络安全治理技术研究尤为主要。

2. 气象信息网络现状

气象部门网络结构按照用途和安全等级划分主要分为三类：承载气象部门核心业务的气象业务专网，气象专网通过专线实现国、省、市、县四级节点的互连互通；用于公众气象服务的政务外网、用于政府部门间信息交换的政务专网。网络安全遵循“木桶原理”，市级部门作为“安全木桶”的重要环节，同时也成为信息安全木桶的短板。深化市级气象网络安全治理势在必行，尤为重要[2]。《网络安全法》的正式实施，将网络安全问题提到了前所未有的高度，国家层面对网络空间安全重视程度不断提升，这对气象部门网络安全综合防御能力提出了前所未有的高要求。它是我国第一部专门用于规定网络安全方向的国家法律，也是气象行业信息安全建设必需遵循的工作规范，在气象网络安全治理方面具有重要的指定意义。随着网络安全上升为国家战略，国家近期发布的多个法律法规文件都对网络安全提出了要求。伴随着《网络安全法》的颁布与实施，等级保护工作也进入 2.0 时代，《网络安全法》第二十一条明确规定“国家实行网络安全等级保护制度”[3] [4] [5] [6] [7]。

菏泽市气象部门网络安全防护和基础保障体系不完善，面临新的威胁防不胜防。通过对网络现状的分析，菏泽市气象局近几年来已经建设了一批网络安全防护基础设施，部署了防火墙、奇安信态势感知系统，免费的终端和服务器杀毒软件等网络安全软件和设备，开展了信息安全等级保护 1.0 工作，具备基本的安全防护能力。但随着气象现代化进程的不断推进及网络安全已上升为国家战略，距等保 2.0 标

准体系建设还有一定的差距，网络安全防护和基础保障体系不完善，当前的网络架构已不能适应气象信息化发展。气象部门是关系国计民生的重要基础性部门，随着信息技术的迅猛发展，气象部门对信息系统的依赖日益加重。当前，气象部门正在全面推进气象信息化，对气象网络安全治理提出了更高的要求，如何建立一个规范的、完整的、稳定的网络安全治理体系，已成为气象信息化发展的重要课题。

3. 气象现代化发展中的网络安全问题

在中国气象局的统一领导和要求下，国家级和省级单位网络安全技术力量和防护能力较强，中国气象局预报司印发了《气象网络安全基础架构设计方案(2019 年)》，该方案对国家级和省级节点做了详细的安全设计和区域划分，基本满足了顶层气象事业发展的需求。通过对网络安全现状进行分析和开展风险评估工作发现，市级气象部门网络安全防护体系并不完善，结合国内外气象部门的相关数据分析，随着信息化的高速发展，对气象网络平台造成安全隐患的情况主要是病毒威胁、非法访问、平台信息非法盗取、黑客攻击等危害，严重影响气象信息网络系统安全和气象业务平台的正常运行，导致各类网络安全事件产生的问题主要包括以下几个方面。

3.1. 网络病毒和非法入侵

气象网络信息安全平台最大的威胁是网络病毒和非法入侵，随着各类新型信息技术不断发展，各种新型病毒的种类在不断更新，在很短的时间内发动攻击，形成以快打慢的攻击局面；前期存在多个业务服务器被植入木马，并以该服务器为跳板对内网多台服务实施网络攻击，导致平台被病毒感染，影响气象业务的正常运行，给业务信息网络的正常运行带来极大的安全风险，严重的甚至导致网络全面崩溃，给气象部门带来巨大的损失。

3.2. 整体防御能力弱

随着云计算、大数据、移动互联网等技术在气象业务中迅速应用推广，与之匹配的安全防护技术部署滞后。地市级节点自行开展网络安全建设，缺乏统筹，网络安全结构不规范，防护能力不均衡，防护短板大量存在，风险感知和整体的安全防御能力较弱。网络安全设备部署零散、各级气象部门安全信息不互通，安全设备缺乏联动机制，潜在风险的监测预警能力弱[8]。网络安全工作范畴和深度在不断拓展，攻击手段不断丰富，新的未知威胁防不胜防，气象部门目前面临网络安全设备老旧，没有充足的资金采购设备，无法有效阻止新的恶性软件和病毒的入侵。网络安全基础保障体系建设还需要与时俱进，不断完善。

3.3. 网络安全监管不足

信息安全管理工作缺乏有效的监督，对网络安全的重视程度不够，缺乏流程化、规范化的网络安全管理和运维体系，网络安全管理体系是网络安全体系的中枢。2020 年中国气象局组织制定了《中国气象局网络安全管理办法(试行)》，相关省级气象部门也制定了关于落实网络安全管理工作责任等相关的制度文件。但一直以来，气象网络安全缺少顶层设计，气象网络安全建设和管理缺少规范指导，不能及时对标国家法律法规、政策文件和技术标准规范，从而迅速跟进完善气象部门网络安全制度，部门内安全管理规章制度等不健全，气象数据安全管理措施不够。

4. 提升气象现代化信息网络安全治理技术

在实际业务中，为保证气象部门网络安全体系能够充分地发挥作用，需要根据气象部门的网络系统的实际特点和发展的实际需求治理。在设计和构建网络安全体系的过程中，一定要遵循实用性、安全性、规范性、可靠性等原则，在保证气象部门网络安全的基础上，在原有的系统结构上合理地提高网络技术的安全性[9] [10]。在构建网络安全体系的过程中，还需要充分地考虑到设备的选择情况，积极地选择最

恰当、最有效的设备。而且，还需要充分地考虑到关键设备之间所具有的关联度，确保关联度科学、合理，从而在最大的程度上减少设备出现故障的概率，保证气象部门能够安全、高效地进行工作。

4.1. 终端实现软件防御

更新建立个人电脑及服务器终端的 IP 地址档案。当出现网络病毒入侵时，可依据备案的 IP 地址档案，及时溯源到感染病毒终端，快速查杀病毒，有利于将病毒感染造成的损失降到最低。终端统一部署安装专业“奇安信天擎”杀毒软件，病毒库和补丁库自动更新，实时监测修补系统漏洞，针对性调整防护，强化管理措施、提高风险控制、漏洞加固等工作，提高终端层面的网络安全防护；对重要网络安全设备的管理员地址进行限制，设置的口令应符合要求且定期更换。

4.2. 加强网络安全设备规划

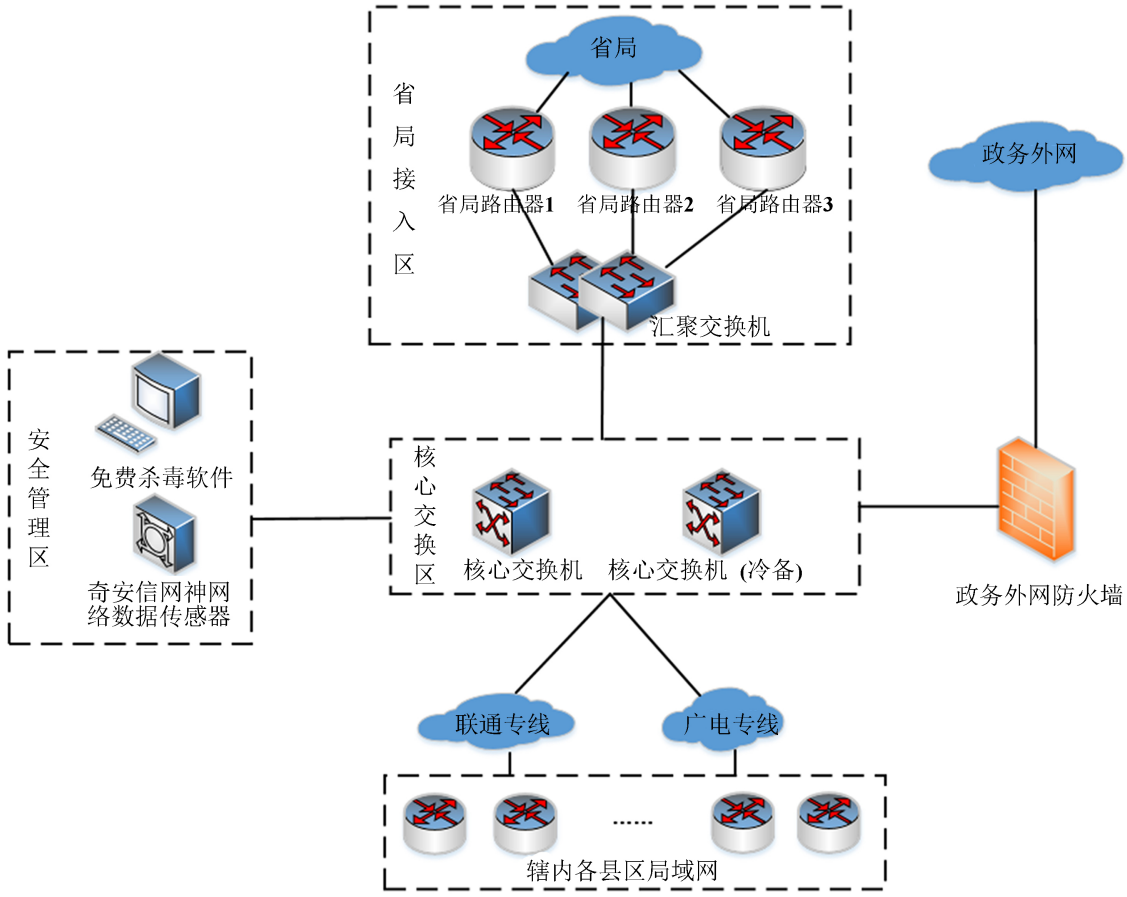

Figure 1. Topology diagram of meteorological information network transformation for Heze Meteorological Bureau
图 1. 菏泽市气象局气象信息网络改造的拓扑图

抵御网络风险最好的方法是加强网络安全设备部署规划。在不同的网络安全区域，布置相应的网络安全设备，可以提高气象部门的网络安全防御能力。当前，菏泽市气象部门网络安全防护和基础保障体系不完善，面临新的威胁防不胜防。通过对网络现状的分析，网络安全隐患主要表现在：1) 在网络安全防护上，对区域边界的防护相对薄弱，当前的外网防火墙老旧，特征库和病毒库已过期，无法对其他互连区域网络攻击进行有效、及时的阻拦；2) 部分外联区域缺乏区域边界的设计。上行至省局、下行至县

局均与市局的本地核心交换机直接对接，无任何安全防护措施。当网络攻击对外联区域的主机、网络发生恶意和非法攻击时，其在内网漫游的同时，也会轻而易举对市级部门本地局域网发起攻击，这将直接影响市局内部信息化安全。3) 缺少日志审计设备。不能对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录进行记录，当发生网络事件时，无法对日志采集、管理和审计。菏泽市气象局气象信息网络改造前的拓扑图如图 1 所示。

为增强全市气象部门网络安全防护水平，针对菏泽市气象局网络架构的薄弱环节，在下联区、外联区进行网络安全加固，同时，严格参照《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》等国家标准以及行业规范进行设计。设计完善后的网络拓扑结构如图 2。

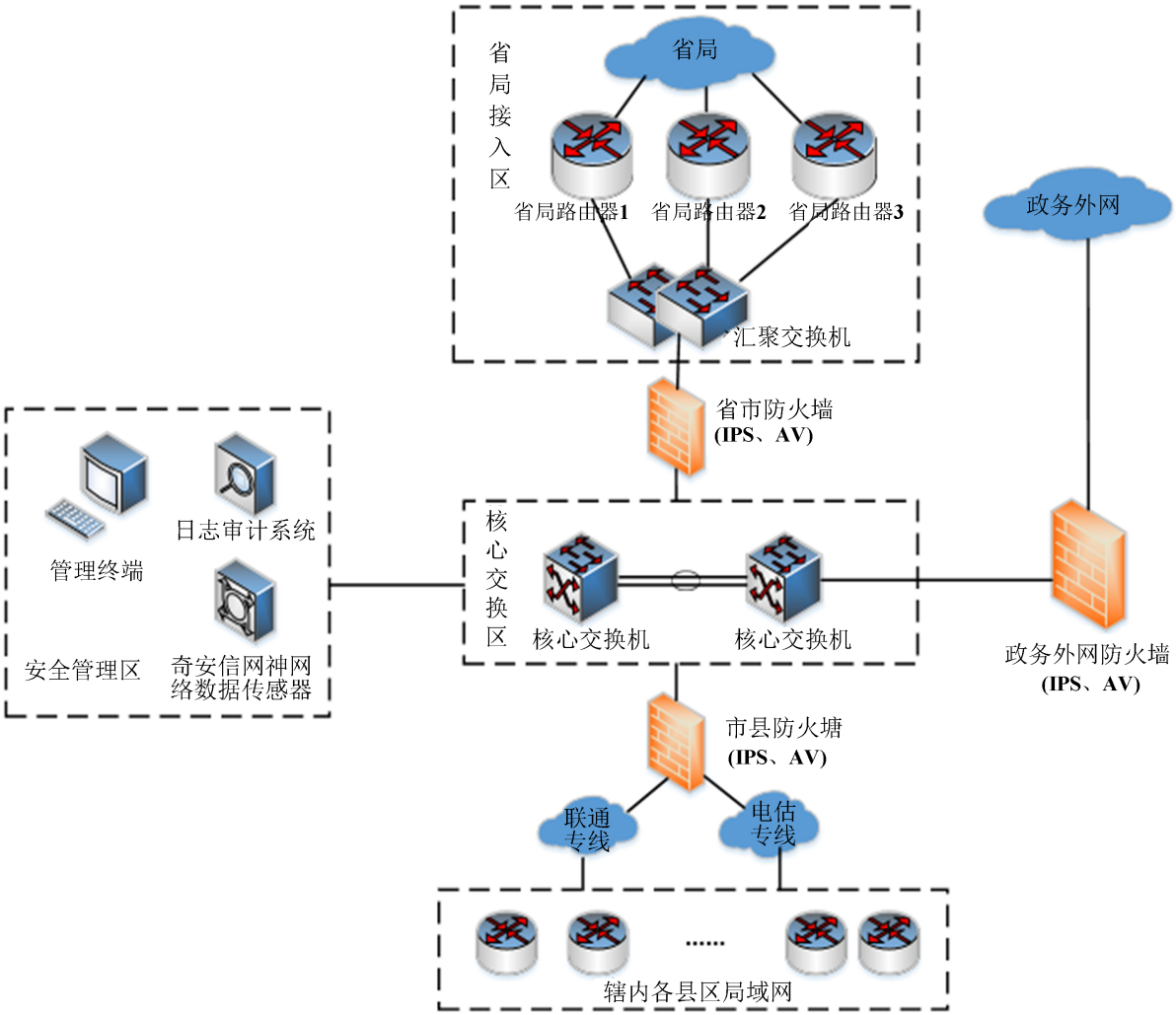

Figure 2. Topology map of the optimized meteorological information network of Heze Meteorological Bureau
图 2. 菏泽市气象局气象信息网络优化后的拓扑图

菏泽市气象局气象信息网络优化后的拓扑图如图 2 所示，气象内网通过专线线路和省局内网互联，通过防火墙与政务外网互联，气象内网架构，分为省局接入区、边界防护区、核心交换区、核心业务区、安全管理区。通过更新部署防火墙、日志审计等网络设备，可以进一步完善网络安全架构，加强气象信息网络安全。

省局接入区：省市之间通过三条专线经市局汇聚交换机接入到市局核心交换机，三条线路形成(20 M + 200 M + 100 M)的广域网出口结构，能实现网络设备和链路的多冗余负载功能，进一步提升省－市宽带网速度及性能。

市县接入区：市县之间通过联通、电信两条 100 M 专线，接入市局核心交换机，两条线路之间实现自动切换，保证气象数据传输质量。

边界防护区：对于气象部门内部的网络安全体系来说，防火墙是最重要的一道硬件防御系统。在网络边界采取必要的授权接入、访问控制、入侵防范等措施实现对内部的保护是安全防御必要的手段。在核心交换区到政务外网的边界更新部署一台含 IPS、AV 的防火墙。通过入侵防御(IPS)模块，针对用户行为分析检测，将网络中一些不合法的入侵有效检测出来，对网络进行监测，提供对内、外部攻击和误操作时的实时保护；通过防火墙的防病毒模块，实现对恶意代码的检测和清除，保护气象部门内部免收外网恶意流量和病毒的攻击。根据业务实际需求，配置合理的访问控制策略。

安全管理区：增加部署一台日志审计设备。通过统一的日志审计平台，将重要网络安全设备的日志收集到日志平台进行统一管理、统一分析，将相关日志留存 6 个月以上，网络管理员可以进行监控或查询。奇安信态势感知系统，是集检测、响应处置、风险预测、可视于一体的大数据安全分析系统，可帮助用户监测资产、监控业务、感知威胁和风险。电脑终端统一部署省局下发的“奇安信天擎”杀毒软件，及时全面查杀病毒，加强了软件防护能力。

4.3. 建立安全运营中心

面对严峻的网络安全威胁形势和气象业务快速发展，传统的网络安全设备和防护方式不能防护全部的网络威胁，仍会有部分威胁绕过所有防护进入内网，传统的技术手段无法感知全局的网络安全威胁，产生相应的告警信息，网络安全管理员需花费大量的时间和精力分析告警日志，无法实现对类似高级持续性威胁(APT)攻击的各个阶段进行有效的检测。APT 攻击是指不断利用新型的攻击手段，持续性地对特定目标进行网络攻击的一种形式，可利用零日漏洞等手段绕过传统网络安全设备的防线，对当前网络安全产生巨大的威胁。态势感知安全防护技术，基于多维度的海量数据，对数据挖掘与关联分析，从全局视角识别安全威胁，并对受害目标及攻击源头进行精准定位，并做出相应处置，构建高效智能的安全管理环境，为网络安全运营人员提供决策与行动依据。

按照纵深防御的理念，经过多年不断的网络安全建设，地市级气象信息网络架构不断完善，网络安全防护体系建设不断增强，地市级气象部门已部署了一系列的网络设备、安全设备及监测措施，比如：下一代防火墙、入侵检测系统、漏洞扫描、安全准入、终端杀毒软件、日志审计等系统，呈点状防御系统。但是无法形成一个有机的整体，存在众多的局限性。大量网络安全日志和事件无法进行系统的分析处理，对安全运营造成很大的难度，严重影响安全运营工作效率。态势感知技术实现了与传统安全防护设备的融合关联，通过流量采集、日志分析等手段，利用传统网络安全防护设备，进行威胁情报的分析和感知，实现对网络安全态势的集中管控感知，有机地将网络设备、人员、技术有机的结合起来。山东省各地级市气象部门配备了奇安信探针采集流量，通过探针收集市－县级监测流量，并通过大数据分析技术对流量进行监控，统一分析排查，并形成各类安全监测告警信息。市级气象部门负责安全运营的各级安全技术人员，按照流程对安全事件进行流转处置，对不同级别的安全告警进行分工处理，并进行定期安全事件回顾，持续改进提升安全有效性，使地市级气象信息网络系统具备了攻击溯源的能力。态势感知技术在地市级气象网络安全防护体系中的融入，符合网络安全等级保护 2.0 技术标准中“一个中心，三重防护”的思想。在气象网络安全防护系统中应用态势感知技术，是气象信息化发展的需求和行之有效的解决方案，提升了地市级气象部门的威胁监测和预警能力。

4.4. 加强网络管理制度建设

建立网络安全管理体系首先要制定网络安全管理制度，网络安全管理制度是组织网络安全的最高方针，需要以国家级网络安全法律和标准为指导，行业网络安全标准为依据制定，对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等各方面建设。制度建立后需加强培训，对网络安全责任部门人员还需要进行特殊培训，保持网络安全工作的主动性和紧迫感。建立网络安全管理体系，其次要加强组织领导工作，成立网络安全和信息化领导小组，按照管理要求，制定和完善网络安全相关制度，对安全管理制度的合理性和适用性不断进行评审和修订，从制度方面严格规范信息安全工作，使信息网络安全管理工作有章可循。

4.5. 加强监控、预警、通报和应急

将网络安全情况统一纳入 24 小时值班监控。建立常态化网络安全信息汇集与分析研判机制，综合本单位网络安全运行情况及接收的网络安全信息通报，及时研判、发布、报送网络安全监测预警信息。在安全可控的前提下，鼓励利用社会力量提升气象部门网络安全监测预警能力。建立健全网络安全信息通报机制。网络安全应急响应是为预防和减少网络安全突发事故的发生，控制、减轻和消除突发事件引起的危害及造成的损失，规范突发事件发生后的上报及处理流程，提高突发事件处置能力，最大程度地预防和减少突发事件造成的损失而建设的体系。制定完善各级网络安全事件应急预案和各信息系统的应急预案，建立应急技术队伍，明确网络安全应急流程，切实提高应急预案的可行性和可操作性。制定网络安全应急演练方案，每年至少开展一次网络安全应急演练。按照等级保护工作要求，做好重要数据备份，建立重要信息系统应急备份机制，推动应急备份系统建设。

4.6. 加大经费保障和宣传培训

加大网络安全相关人力、财力、物力的支持和保障力度，将网络安全经费纳入年度预算，统筹安排专项经费开展网络安全建设和保障工作；加强网络安全宣传与人才培养，积极参与国家网络安全宣传周活动，并在其它时间每年组织 1~2 次网络安全宣传活动；采取多种方式加强网络安全培训，实现网络安全培训全员化、常态化，新入职员工培训和领导干部培训需安排网络安全内容；强化网络安全人才培养，提高网络安全人才专业技能。

5. 结语

信息化技术的不断发展在给我们带来便利的同时，意味着气象信息化发展将会面临更为复杂的发展环境，这就对气象部门的网络安全方面的治理技术提出了更高的要求，网络安全体系是一个动态的系统工程，技术防御手段需与时俱进。气象部门需要根据信息技术高态势发展趋势，不断提高防范和抵御风险的能力，加强信息网络安全管理工作和提升安全防护技术手段，推动实现网络安全治理能力现代化，为气象事业发展提供坚实的网络安全保障。

基金项目

山东省气象局青年科研基金项目“地市级气象信息网络安全架构标准化设计研究”(2022SDQN20)。

参考文献

[1] 刘东君, 何恒宏, 谭震, 等. 气象网络安全治理体系研究[J]. 网络安全技术与应用, 2019(2): 90-92.

[2] 赵冰, 王旭, 贺永兴. 浅谈海南气象信息网络安全建设[J]. 网络安全技术与应用, 2019(12): 134-136.

[3] 张朝. 医院网络安全等级保护 2.0 管理体系建设实践[J]. 网络空间安全, 2020, 11(3): 30-33.

[4] 李丹, 杨向东, 马卓元, 等. 等保 2.0 视域下的网络安全工作思考[J]. 网络安全技术与应用, 2019(10): 11-12.

[5] 马力, 祝国邱, 陆磊. 《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J]. 信息网络安全, 2019, 19(2): 77-84.

[6] 任婷, 于城. 从新技术角度谈等级保护 2.0 [J]. 信息通信技术, 2018, 12(6): 12-17.

[7] 李丹, 杨向东, 马卓元, 等. 等保 2.0 视域下的网络安全工作思考[J]. 网络安全技术与应用, 2019(10): 11-12.

[8] 鲍磊磊, 吴锐涛, 姜淑杨. 地市级气象信息网络安全架构标准化设计研究[J]. 网络安全技术与应用, 2022(1): 103-105.

[9] 陈虹, 林廷柄. 网络安全技术在气象信息系统中的应用[J]. 数字技术与应用, 2019, 37(4): 203-204.

[10] 曲洁, 范昡玲, 陈广勇, 等. 新时代下网络安全服务能力体系廸设思路[J]. 信息网络安全, 2019, 19(1): 83-87.