Software Engineering and Applications 软件工程与应用, 2024, 13(2), 254-261
Published Online April 2024 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2024.132026

Hans汉斯

护网2022行动背景下民航气象信息系统网络安全建设研究

王　艳

中国民用航空西南地区空中交通管理局贵州分局，贵州　贵阳

收稿日期：2024年1月8日；录用日期：2024年4月22日；发布日期：2024年4月30日

摘　要

随着信息技术的快速发展，民航气象信息系统对于保障航班飞行安全和提高空中交通效率的作用日益凸显。然而，网络安全威胁同样日益严峻，对此类关键信息基础设施的保护尤为重要。“护网2022”行动是国家层面针对网络安全的一次重要检查与演练，目的在于提升关键信息基础设施的网络防护能力。本研究立足于该行动，采用先进的网络安全技术和产品，针对民航气象信息系统建立了一套完善的网络安全防护体系。该体系能够实现对安全态势的全面监控、对潜在风险的实时预警以及对安全事件的快速响应。从技术和管理两个层面，提出了一系列切实可行的安全防护对策，旨在为民航气象信息系统的网络安全建设提供系统化的解决方案，以应对不断变化的网络安全挑战，确保民航气象服务的持续稳定发展。

关键词

护网行动，民航气象信息系统，网络安全建设

Research on Network Security Construction of Civil Aviation Meteorological Information System in the Context of Operation Protect Net 2022

Yan Wang

Guizhou Sub-Bureau of Southwest Air Traffic Management Bureau, CAAC, Guiyang Guizhou

Received: Jan. 8th, 2024; accepted: Apr. 22nd, 2024; published: Apr. 30th, 2024

文章引用: 王艳. 护网 2022 行动背景下民航气象信息系统网络安全建设研究[J]. 软件工程与应用, 2024, 13(2): 254-261. DOI: 10.12677/sea.2024.132026

Abstract

With the rapid development of information technology, the role of civil aviation meteorological information systems in ensuring the safety of flights and improving the efficiency of air traffic is becoming more and more prominent. However, the threat of cybersecurity is also becoming increasingly serious, and the protection of such critical information infrastructures is particularly important. The "Protect Net 2022" operation is an important check and exercise for cybersecurity at the national level, aiming to improve the cyber protection capability of critical information infrastructure. Based on this action, this study adopts advanced network security technologies and products to establish a comprehensive network security protection system for civil aviation meteorological information system. The system is capable of realizing comprehensive monitoring of security posture, real-time warning of potential risks and rapid response to security events. A series of practicable security protection countermeasures are proposed at both technical and management levels, aiming at providing systematic solutions for the network security construction of civil aviation meteorological information system, so as to cope with the ever-changing network security challenges and ensure the sustainable and stable development of civil aviation meteorological services.

Keywords

The Context of Operation Protect Net 2022, Civil Aviation Meteorological Information System, Network Security Construction

1. 引言

民航气象信息系统[1]承担着气象资料收集、情报交换、预报平台、服务支持等重要任务。这些系统在增强民航气象保障能力以及提高飞行效益和减少航空事故发生率等方面发挥了重要作用。“护网 2022”行动不仅强调了加强民航气象信息系统等关键基础设施[2]的网络安全防护，还旨在提高行业对抗网络攻击的能力，保障民航业务连续性和安全稳定运行。在这一行动中，民航贵州空管分局充分应用基于大数据技术的超大型数据平台安全等级保护威胁信息监测与分析系统，制定和实施网络安全解决方案，有效地解决民航气象信息系统网络安全防范较为薄弱的问题。

2. 民航业网络安全现状与挑战

国内外的网络安全形势对民航业都提出了新的挑战。2011 年至今，交通运输部和民航局发布了一系列政策，例如：交通部《关于进一步开展交通运输行业信息安全等级保护工作的通知》以及《民航网络与信息安全管理暂行办法》中明确要求按照“谁主管、谁负责”、“谁运维、谁负责”的原则，信息系统的主管部门及运营、使用单位按照等级保护的管理规范和技术标准进行信息安全建设和管理。

2023 年 11 月，乌克兰情报部门宣称入侵俄罗斯联邦航空运输署，窃取了 300 余次的民航飞机事故报告、820 架民用飞机的维修清单等敏感文件，导致对俄罗斯的飞机备件、软件控制、空中导航所需的气象数据获取等制裁的措施更加精准，飞机故障案例显著增加，直接影响国家安全。

2023 年 1 日，美国航行通告系统出现故障，造成 1300 架次航班被取消，11,000 架次航班被延误。调查显示为意外删除系统文件造成，民航信息系统发展技术的缓慢，应急预案的有效性验证不及时，使得小概率事件引发极大的飞行安全问题。

2023 年 11 月，针对旅客反映航班信息诈骗问题，民航局方高度重视数据治理工作，认真贯彻《网络安全法》《数据安全法》等规定，先后出台 47 + 1 智慧民航数据治理系列规范，指导规范行业单位开展数据共享、数据服务、数据安全等工作[3]-[10]。民航业各组织的发展不平衡，对比其他行业信息安全水平相对滞后。

3. 民航气象信息系统的网络安全现状

3.1. 民航气象信息系统架构与关键组成

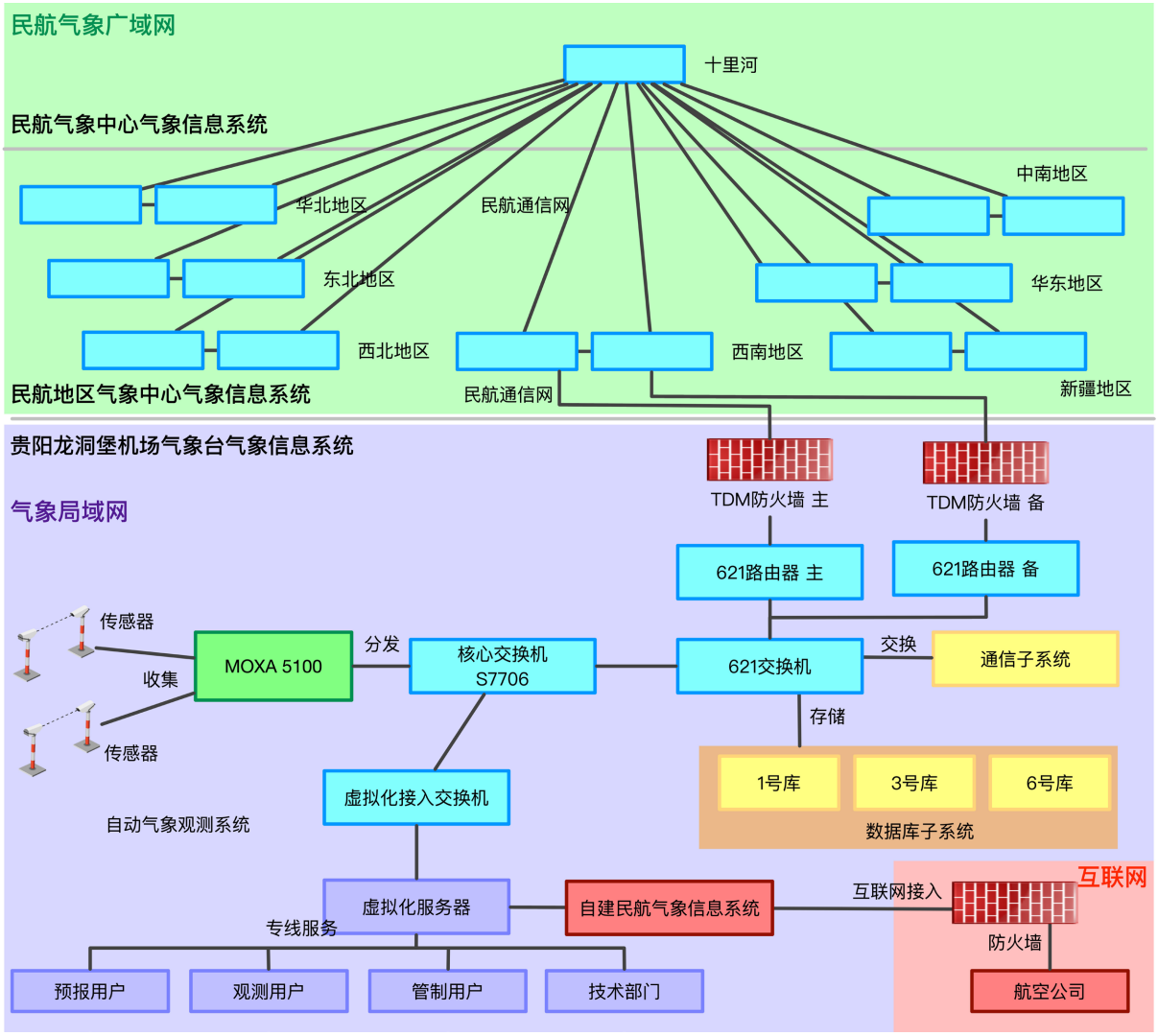

Figure 1. Core network structure of weather information system of Guiyang Longdongbao International Airport Meteorological Station
图 1. 贵阳龙洞堡机场气象台气象信息系统的核心网络结构

民航气象信息系统是基于民航气象数据库系统(新 621 系统) [11]建设而来，分为民航气象中心气象信

息系统、民航地区气象中心气象信息系统和机场气象台气象信息系统。以民航气象中心为核心，七个地区中心构成数据交换网络，每个地区中心下挂多个分局站，共同构建成一套分级，且包含收集、存储、交换、发布、服务等多种功能的气象信息服务关键基础设施。

各级气象信息系统的核心网络结构和主要设备布局相似，以贵阳龙洞堡机场气象台气象信息系统为例，气象资料汇聚到核心交换机 S7706 进行数据的高速转发。各通信子系统和数据库子系统(1 号库、3 号库、6 号库)通过行业特定子网 IP 地址与核心交换机连接。自动气象观测系统通过 MOXA5110 串口服务器实现气象数据单向的采集和分发。在民航气象广域网系统，621 交换机与 621 路由器相连后，经过 TDM 网防火墙连接至民航通信网，完成本场气象资料和气象服务与各级气象信息系统互联互通；在气象局域网系统，多用户气象数据专线服务通过虚拟化技术，提高服务器资源的利用率和灵活性；在互联网接入系统中，航空公司的气象数据服务经过防火墙，从自建民航气象信息系统获取，不直接与核心业务网络相连。整个网络核心节点和数据协议转换设备均设计了冗余路径和统一的配置标准，实现了系统的可靠性和可维护性。贵阳龙洞堡机场气象台气象信息系统的核心网络结构如图 1。

3.2. 民航气象信息系统网络安全痛点

(一) 网络统一管理难度大，网络安全实施“各自为战”。民航气象信息系统包含了数十个业务子系统，各子系统对于安全防护缺乏统一性和规范性。子系统间缺乏日志追踪、追溯机制，无法完全落地整体管理。

(二) 数据安全技术不统一，缺乏标准化技术实现。民航气象信息系统的网络处理、存储技术和传输协议各不相同。数据接入/提供方式有：SFTP、MQ 以及 Https 等；数据存储方式：Oracle、HDFS、Mongodb、HBase 等；数据处理方式：SQL、存储过程以及 Function 函数等[12]。数据接入、存储、传输、提供等软件产品、中间件各自采用了不同的安全技术，但没有形成统一的安全保护方案和技术实现。

(三) 网络安全事件管控缺乏体系化设计，以事后管控为主[13]。民航气象信息系统缺乏体系化的网络安全管理制度和流程，许多网络安全管理比较被动，此次的护网行动也反映出实际防守过程中，完全依靠部署安全防御设备，无法真正实现网络安全事件的全流程主动管理。

4. 民航气象信息系统在护网行动中的网络安全建设。

4.1. 民航气象信息系统的网络安全建设策略

“护网 2022”行动中，民航贵州空管分局于 7 月开展了为期 15 天的网络攻防演习，民航气象信息系统作为民航贵州空管分局下属的关键基础设施重要组成部分参与此次演练。

4.1.1. 民航气象信息系统管理体系建设

(一) 组织领导：成立“护网 2022”防守指挥部和工作专班，执行 7*24 小时值班制度，每日进行“日报告”制度，对网络安全情况进行总结分析，随时对攻防态势、系统日志进行监控和研判。

(二) 资产梳理：对民航气象信息系统相关的网络访问路径及资产进行梳理，形成系统的关联资产与未知资产清单，明确各子系统访问源(包括用户、设备或系统)的类型、位置和途径的网络节点，绘制准确的网络路径拓扑图，结合拓扑图组织各科室评估各系统间互联的必要性及可能存在的风险，明确演习期间如遇特殊情况可中断连接系统，通过全面梳理各子系统可能被访问到的路径和数据流向，为后续安全自查和整改加固等工作提供基础数据。

(三) 隐患排查：重点对与组成系统相关的网络设备、服务器、中间件、数据库、应用系统、安全设备等开展安全自查和整改工作，设置必要的防御规则，仅开放允许业务正常运行所必须的网络和系统资源，做好暴露面管理，即使在不修复漏洞的情况下，也能保证系统不被攻破。

(四) 人员意识：联系工作实际，结合职责和岗位情况，对贵州空管分局气象台全员进行《网络安全法》《数据安全法》《个人信息保护法》等法律规章测试，邀请网络安全专家开展专业技术培训，保证贵州空管分局气象台各层级具备必需的网络基础知识，掌握相关操作技能，尤其针对社工攻击、钓鱼邮件等常见攻击手段进行深度解读，提升职工网络安全意识，让大家安全用网，合规用网，时刻培养良好的网络安全习惯。

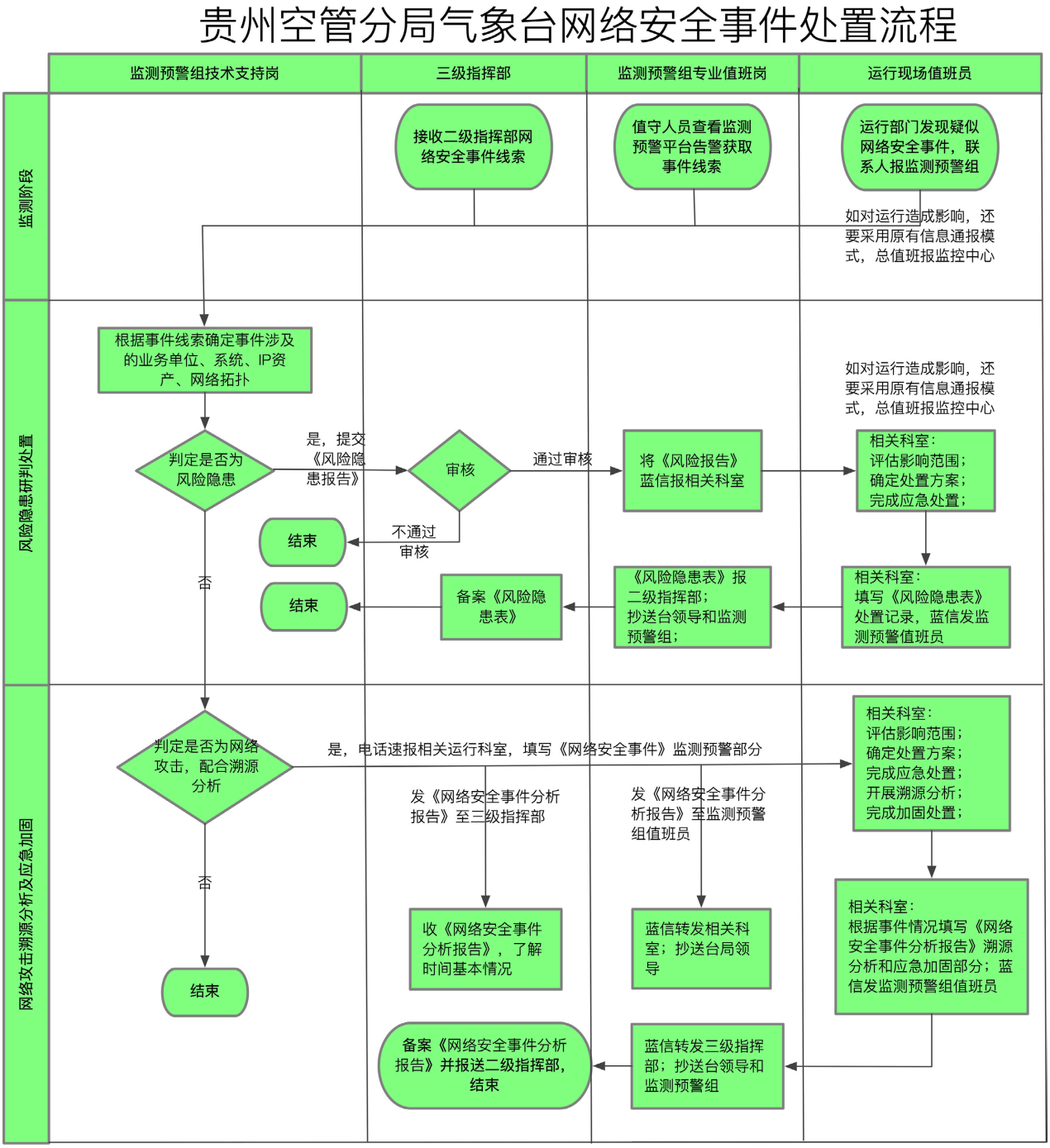

Figure 2. Process for handling cybersecurity incidents at the meteorological station of Guizhou Air Traffic Control Sub-Bureau
图 2. 贵州空管分局气象台网络安全事件处置流程

(五) 处置流程：建立配套的网络安全事件管理制度和处理流程进行保障，保障网络安全事件的及时发现、快速响应和有效处置。在本次护网行动网络安全事件处置流程中，首先监测预警组技术支持岗接收网络安全事件线索，由值守人员查看预警平台告警或运行部门报告疑似事件。确定事件涉及单位、系统、IP 资产和网络拓扑后，评估是否为风险隐患。若为风险隐患，填写《风险隐患报告》并通过审核，报送相关科室并备案；不通过则补充《风险隐患表》。此后，相关科室评估影响范围，确定处置方案，完成应急处置。若判定为网络攻击，电话速报并填写《网络安全事件》监测预警部分，提交《网络安全事件分析报告》至三级指挥部和监测预警组。相关科室进行影响评估、处置方案确定、应急处置、溯源分析和加固处置。最终将《网络安全事件分析报告》备案并报送二级指挥部。贵州空管分局气象台网络安全事件处置流程如图 2。

4.1.2 民航气象信息系统技术防护优化

本次护网行动，民航气象信息系统通过接入中国电信研发的基于大数据技术的超大型数据安全等级保护威胁信息监测与分析系统作为技术防护手段。该系统能够实现对超大型特定场景的脆弱性和威胁自动发现，自动调用插件进行分析，可大幅提高各子系统的监测效率[14]，提升对抗网络攻击的应对与反应能力，确保民航气象信息系统网络环境的安全稳定。

该基于大数据技术的超大型数据安全等级保护威胁信息监测与分析系统简称超大型数据等保威胁监测系统主要由互联网数据监测模块、等级保护数据分类索引模块、调度总线模块、安全威胁分析与展示模块、共 4 个模块构成。该系统功能框图如图 3。

(一) 互联网数据监测模块，该模块基于 Scrapy 框架构建，实时获取和分拣互联网威胁信息、威胁情报和监测信息，以形成威胁信息库、威胁情报库和监测信息库，供其它模块使用；

(二) 等级保护数据分类索引模块：该模块基于 ElasticSearch 数据库构建，通过导入等级保护备案数据，调研数据和测评数据，并结合国家的相关等级保护标准进行资产数据增强和解析，形成超大型互联网平台资产库和等级保护资产库；

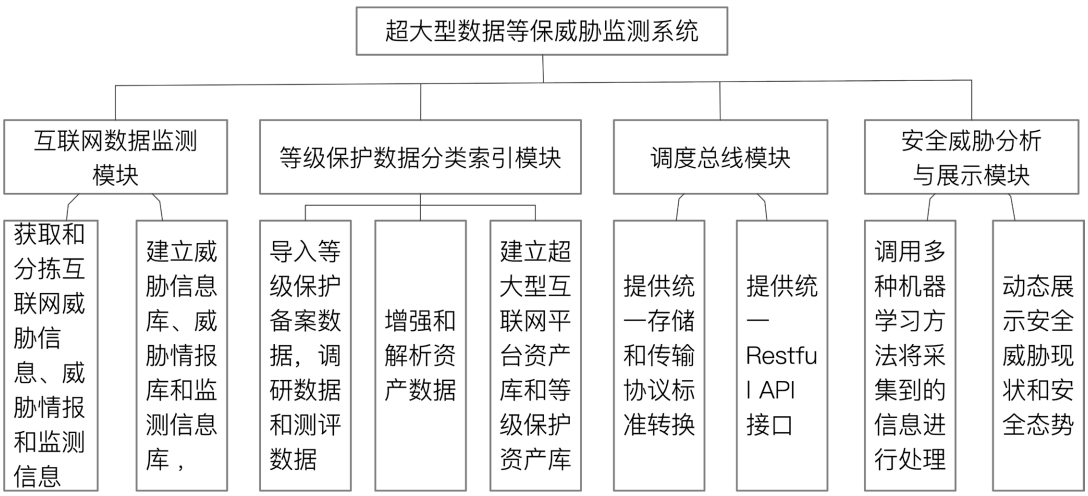

Figure 3. Functional block diagram of the mega data iso-protection threat monitoring system
图 3. 超大型数据等保威胁监测系统功能框图

(三) 调度总线模块，该模块通过自动调用厂商自研插件，提供统一存储和传输协议标准转换和 Restful API 接口，以任务的方式运行；

(四) 安全威胁分析与展示模块，该模块分别与调度总线模块、互联网数据监测模块以及等级保护数

据分类索引模块数据连接，通过调度总线模块控制互联网数据监测模块以及等级保护数据分类索引模块运行，并调用多种机器学习方法将采集到的海量信息进行关联、分类、聚类和协同过滤分析，动态展示安全威胁现状和安全态势。超大型数据等保威胁监测系统漏洞与安全事件统计如图 4。

Figure 4. Vulnerability and security incident statistics for the mega-data isochronous threat monitoring system
图 4. 超大型数据等保威胁监测系统漏洞与安全事件统计

4.2. 系统网络安全建设在护网行动中的实践效果

Figure 5. Security situation monitoring of the civil aviation meteorological information system
图 5. 民航气象信息系统的安全态势监控情况

超大型数据等保威胁监测系统上线至今，累计 600 余天，贵州空管分局民航气象信息系统的网络安全形势总体向好。未发生任何网络安全事件。为了继续验证平台对于入侵事件的告警和追溯能力，贵州空管分局定期邀请专业厂家别从互联网和民航通信网的气象业务支线发起渗透测试和模拟攻击，未发现重大漏洞，也未收到任何不安全事件通报。从监测设备的有效性，安全监测人员的值守效果、分析研判人员的定位能力，应急加固人员的处置能力、以及各个环节各个值守人员对于信息通报的熟悉程度等方面均得到了较好的验证。民航气象信息系统的安全态势监控情况如图 5。

5. 结语

在“护网 2022”行动这一重要背景下，本研究从民航气象信息系统的网络安全建设出发，通过对系统架构的深入分析，讨论了民航气象信息系统目前存在的网络安全痛点，以安全管理体系的完善、技术防护的优化两个纬度，建立了一套针对民航气象信息系统的完善网络安全防护体系，并提出了一系列切实可行的安全策略和优化措施，经过 2 年的测试验证，民航气象信息系统的威胁预警与安全防护能力得到了明显提升，确保了民航气象信息系统在复杂的网络环境中一定时间内的稳定运行。

参考文献

[1] 中国民用航空局空管行业管理办公室. AP-117-TM-2012-05 民用航空气象信息系统技术规范[S]. 北京: 中国标准出版社, 2016.

[2] 衡闻琦. 中国民航业关键信息基础设施安全保护工作开展情况综述[J]. 中国信息安全, 2023(9): 54-57.

[3] 中国民用航空局发展计划司. MH/T 5054-2021 智慧民航数据治理规范框架与管理机制[S]. 北京: 中国标准出版社, 2021.

[4] 中国民用航空局发展计划司. MH/T 5055-2021 智慧民航数据治理规范数据架构[S]. 北京: 中国标准出版社, 2021.

[5] 中国民用航空局发展计划司. MH/T 5056-2021 智慧民航数据治理规范数据质量[S]. 北京: 中国标准出版社, 2021.

[6] 中国民用航空局发展计划司. MH/T 5057-2021 智慧民航数据治理规范数据安全[S]. 北京: 中国标准出版社, 2021.

[7] 中国民用航空局发展计划司. MH/T 5058-2021 智慧民航数据治理规范数据服务[S]. 北京: 中国标准出版社, 2021

[8] 中国民用航空局发展计划司. MH/T 5066-2023 智慧民航数据治理规范数据共享[S]. 北京: 中国标准出版社, 2023.

[9] 中国民用航空局发展计划司. MH/T 5067-2023 智慧民航数据治理规范数据治理技术[S]. 北京: 中国标准出版社, 2023.

[10] 中国民用航空局发展计划司. B-PL-2023-01 智慧民航数据治理典型实践案例[Z]. 2023.

[11] 中国民用航空局空管行业管理办公室. AP-117-TM-03R1 民用航空气象数据库系统业务运行管理规定[S]. 北京: 中国民航出版社, 1996.

[12] 杨乐, 朱国栋, 陈福康. 基于网络安全域的民航气象信息服务系统设计[J]. 民航管理, 2019(6): 72-74.

[13] FreeBuf. 全球最大航空公司遭遇供应链攻击, 大量飞行员敏感数据泄露[EB/OL]. https://www.secrss.com/articles/55951, 2022-09-30.

[14] 刘铸. 大咖护网经系列丨第 2 期护网 2022——未知攻焉知防[EB/OL]. http://www.hackdig.com/09/hack-790986.htm, 2022-09-30.