涉密信息系统分级保护研究与探讨

奉春¹ 陈丹丹¹ 廖菊²

(1. 广西科技师范学院, 广西 来宾 546100;

2. 广西来宾市政和小学, 广西 来宾 546100)

摘要: 涉密信息系统分级保护是企事业单位信息系统安全的一项重要工作, 也是一个突出问题、难题, 做好信息化安全工作是保障企事业单位发展的重要条件。本文通过总结作者在涉密信息系统分级保护工作的经验和体会, 分别详细阐述了涉密信息系统分级保护背景、保护重点、保护体会和保护工作措施。

关键词: 涉密信息系统分级保护; 研究; 探讨

在科技飞速发展的当今世界, 计算机网络给人们带来了无穷的智慧和乐趣, 也给网络安全带来风险。因此, 如何防范信息系统的安全保障, 涉及到信息系统分级保护工作。2006年3月22日, 十届全国人大第四次会议讨论通过的《中华人民共和国国民经济和社会发展第十一个五年规划纲要》提出, “积极防御、综合防范, 提高信息安全保障能力”, 体现了国家对信息安全保障工作的高度重视, 中共中央在《关于构建社会主义和谐社会若干重大问题的决定》里也明确提出要“确保国家信息安全”, 再显中央对信息安全工作的重视程度。

一、涉密信息系统分级保护背景

涉密信息系统分级保护是一项长期而艰巨的任务, 要持之以恒, 常态化进行。造成了保密工作的方法、对象、环境等都发生了很大的变化, 在管控与规定涉密人员、知秘的范围与涉密的行为方面都出现了一些新的问题。传统的保密模式很难去适应保密工作的进行与发展, 再加上该项工作的特殊性, 怎样科学高效的开展保密工作, 逐渐演变为当前建设涉密信息系统的瓶颈, 急需引进新的管理办法与思路。结合我国当前安全形式颁发一系列相关管理、技术标准来对涉密信息系统进行规范, 涉密信息系统应当依据信息安全等级保护的基本要求, 按照有关涉密信息系统分级保护的管理规定和技术标准, 结合自身实际情况进行保护; 2014年3月1日实施《中华人民共和国保守国家秘密法实施条例》(中华人民共和国国务院令 第646号); 2021年3月1日, 国家保密局实施《涉密信息系统集成资质管理办法》涉及到涉密信息系统的规划、设计、建设、监理和运行维护等活动。

二、涉密信息系统分级保护重点

涉密信息系统分级保护的重要因素为技术和管理, 两者相辅相成, 缺一不可, 企事业单位、党政机关根据涉密信息系统分级保护自身特点, 制定有针对性和可操作性的管理措施, 并按照措施严格执行。

(一) 技术要求方面

1. 物理安全

(1) 环境安全, 涉密场所(中心机房、数据中心)、重要设备间和要害部位严格按照要求进行建设和改造, 并配备电子监控和门禁系统进行7*24小时无死角监控。

(2) 设备与介质安全, 涉密场所严格按照规定: 应当建立详细信息台帐。使用或携带设备与介质外出时, 按照规定要求, 由专人集中进行管理维护。相关部门应当制定严格的设备与介质标识、安放与保存管理制度, 保证设备与介质在安放与保存过程中的数据安全。

(3) 对涉密信息系统和非涉密信息系统内的计算机进行严格区分, 采取必要的技术手段进行物理隔离, 完善主机监控系统

软件功能, 严格控制主机监控系统客户端, 有效利用域控制功能, 使一般用户无权限更改系统设置。

(4) 注意涉密信息系统严格按照安全域划分。

2. 网络安全

重要涉密场所的涉密信息系统统一安装相关正版专用杀毒软件, 定期进行病毒库升级, 当计算机在空闲时, 自动扫描查杀病毒。

3. 主机安全

加强操作系统自身安全、访问控制、策略设置、系统漏洞等安全防护措施, 安装杀毒软件, 安装保密技术防护专用系统, 定时更新操作系统漏洞补丁和病毒库。

4. 运行安全

(1) 备份与恢复。制定备份与恢复策略实施的规章制度和需求分析。重点做好涉密数据、关键业务数据、关键业务设备备份重点做好恢复预案, 可快速做到信息系统恢复与重建。

(2) 病毒与恶意代码防护。安装网络防病毒软件, 加强存储设备的接入管理, 加强防护策略、防护范围、陪护措施, 提升能力。

(3) 设备接入控制。加强设备接入管理, 控制违规接入设备对系统资源的访问, 并进行安全审计。

(二) 管理要求方面

1. 基本要求

涉密信息系统必须配备系统管理员、安全保密管理员和安全审计员(以下简称三员), 三员应具备信息安全保密知识和业务技能, 认真履行岗位责任和按时完成与责任相关的工作。

2. 人员管理

三员要进行岗前培训, 并参加有关单位举行计算机及信息安全保密管理培训, 考试合格后持证上岗, 各单位按照上级的要求及自身制度要求, 加强对涉密信息系统三员的管理工作, 提升企事业单位、高校科研单位涉密信息安全保密能力, 不断提高管理水平。

3. 系统运行管理

加强涉密场所的安防监控和出入管理, 对涉密场所和重要部位进行安全巡视, 对重要设备设施要进行定期检查。对设备(介质)的使用、信息输入输出制订管理规定, 对系统的运行使用、二次开发明确管理规定, 严格控制用户管理、权限分配、信息系统、神剑网的接入。

三、涉密信息系统分级保护体会

按照上级单位保密要求, 贯彻落实涉密信息系统分级保护工作, 强化对信息安全保密工作的指导、监督和自查。各单位按照上级主管部门的重要批示和指示精神, 尽快采取有效保密措施, 增强敌情观念, 完善技术手段, 完善保密管理制度, 严格信息化管理, 确保信息化安全运行。

(一) 加强涉密信息系统安全分级保密管理工作的领导

各级单位要重视涉密信息系统的分级保护保密工作,并制订了《涉及国家秘密的信息系统分级保护管理办法》,分级保护技术要求、分级保护管理规范、分级保护测评指南等一系列加强计算机信息系统保密管理工作的规定和国家保密标准。为进一步加强计算机信息系统分级保护保密管理工作的领导,相关单位要成立计算机信息系统分级保护保密工作领导小组,组长由党委书记或总经理(校长)兼任,其他部门领导及信息化办公室成员为组员,明确各组成员的工作职责。

(二) 全面推进涉密信息系统分级保护工作

推进涉密信息系统分级保护工作是企业一项长效机制,企业每年进行一次涉密信息系统分级保护工作自查,检查中按照上级主管单位分级技术防护保护的要求,随时接受上级主管单位的检查或整改工作。

(三) 完善涉密信息系统分级保护工作管理制度

为了贯彻上级单位的会议精神,按照信息系统分级保护领导小组的工作部署,制订了《关于加强企业涉密信息系统分级保护安全工作和保密管理的若干规定》(以下简称《规定》),《规定》针对当前涉密信息系统分级保护和保密管理工作中存在的风险和突出问题,着重加强涉密信息系统分级保护安全运行和保密管理,加强职能分工、系统建设、设备和介质使用管理、维修和销毁管理、人员管理、责任追究等方面提出了明确要求,重点加强涉密信息系统分级保护管理制度。

(四) 加快完善保密技术防护专用系统

按照上级主管单位要求,企业要部署主机监控与审计系统、身份认证网关,并结合后期工作不断完善,现按照保密要求,涉密计算机及移动存储介质保密技术防护系统要运行正常,用户终端安装保密技术防护专用系统,提供违规外联监控、移动存储介质监控、操作行为监控、单向多功能导入等功能。在使用此系统时要加强策略部署、策略管理、策略安全控制、策略运行管理及审计管理。

(五) 监督检查、加大涉密信息分级保护惩罚力度

各单位成立涉密信息分级保护机构,主要负责涉密信息系统分级保护日常工作,对日常工作进行督促考核检查,对查出问题的要及时整改,对整改不力的要严加惩罚,对做得好的单位要给予奖励和表扬。在保密督促检查工作中要严格做到“三严”,严查、严罚、严究,力求保密检查工作“零容忍度”,不容忍有泄密行为、违规现象发生、不容忍国家安全和集体利益受到损害。

(六) 加强培训,让员工自觉遵守规章制度

加强员工管理制度培训,严格执行管理制度,严格按照要求执行涉密信息系统,提高涉密信息抗风险能力。1.提高涉密信息系统三员综合业务素质,三员有针对性的参加各种业务培训,可以提高三员的技术水平和管理水平、安全保密监督能力、防范及处理能力得到提高;2.增强员工涉密信息系统分级保护安全保密意识,通过组织员工观看警示教育片。

四、涉密信息系统分级保护工作措施

(一) 明确分工和责任

在实施涉密信息系统分级保护工作中,三员要利用专业知识,按照涉密信息系统分级保护的技术要求和管理规范,组织专业技术人员设计合理的保密要求分级保护方案。相关保密委员会应对总体方案进行监督、检查和指导,并组织相关专业专家进行认证评估。

(二) 加强信息化部门与保密部门的沟通协调

涉密信息分级保护工作涉及到多个部门,在信息技术方面要

多与信息化部门沟通,由其提出前瞻性、科学性的意见和方案,争取信息技术方面的支持和指导,在安全保密方面要多与保密部门沟通,争取在项目实施过程中的监督和检查,通过多部门的配合,确保项目实施的规范和标准。

(三) 项目引进工程监理、信息安全风险评估机制

按照涉密技术标准和国家法律法规及相关国家标准规范,涉密信息系统集成要选择具有保密资格的、国内的监理资质、信息产业信息工程监理单位承担项目监理工作,在工程的设计、招标、施工、验收等过程中全程监控质量、工程进度、投资控制、合同及信息管理并组织协调监理工作。

(四) 实行方案论证制度

通过调研形成方案初稿,监理员和风险评估员对方案进行修改,最后组织专家对方案进行技术可行性和安全保密可行性论证,确保工程的成功实施。

(五) 日常运行维护规范化

为了确保涉密信息系统的安全保密运行,保密部门要联合信息化部门进行定期检查,通过安全检查和持续改进,不断跟踪涉密信息系统的变化进行调整,确保涉密信息系统满足分级保护的安全要求。

(六) 实施系统测评

信息系统建成后,上级主管部门统一组织第三方涉密信息系统分级保护测评,上级主管部门负责规划和组织测评工作。测评机构为国家保密局授权的系统测评机构,一般为涉密信息测评机构或各地分中心,测试按照《涉及国家秘密的信息系统分级保护测评指南》执行。

五、总结与展望

(一) 总结

涉密信息系统按照上级要求,始终围绕大局,全力推进涉密信息系统安全保密工作做深、做实、做强,继续坚持做好安全保密工作原则,动员、组织和依靠广大职工群众,共同做好企业保密工作,维护涉密信息系统的安全工作,在日常管理工作中,做好三员权限分离管理方法即系统管理员负责系统配置、维护、注册用户、删除及角色定位等管理业务;安全保密员负责涉密等级和职务,调整设置不同用户角色和权限;安全审计员负责监督检查审计日志,定期查看系统管理员、安全保密员的系统操作日志。

(二) 展望

涉密信息系统分级保护要与时俱进,按照科学发展观的要求,在网络信息化复杂多变的情况下,作为网络信息化工作者要不断的研究和探索,在边界防护、电磁防漏、终端主机防护、传输线路管控、备份和容灾等方面要有防护措施及应急预案应对突发事件、不断提高信息化队伍建设能力水平,持续改进、完善构建长效机制提升涉密信息系统分级保护管理工作水平。

参考文献:

- [1] 陈金仕,王军元.国有企业涉密信息系统分级保护探讨与体会[J].中国航天科工集团南京电子设备研究所,2011(7).
- [2] 朱修阳,吴圣杰.检察信息系统分级保护研究与体会[J].最高人民检察院检查技术信息研究中心,2009(12).

作者简介:

奉春 毕业于广西民族大学物理与电子工程学院,重庆大学计算机学院软件工程专业硕士研究生,就职于广西科技师范学院。

陈丹丹 毕业于广西师范大学系统理论专业硕士研究生,就职于广西科技师范学院。

廖菊 毕业于柳州地区民族师范学校,就职于广西来宾市政和小学。