DOI:10.19850/j.cnki.2096-4706.2021.13.033

科研院所安全信息系统运维标准研究

惠建新[1]，乔德志[2]，娄洪伟[3]

（1· 中国科学院紫金山天文台，江苏 南京 210023；2· 中国科学院大连化学物理研究所，辽宁 大连 116023；3· 中国科学院长春光学精密机械与物理研究所，吉林 长春 130033）

摘　要：文章对科研院所安全信息系统运维现状进行了分析研究，依照国家有关体系规定的要求，提出了建立科研院所安全运维标准的意见。该标准意见具有可靠性、普适性、稳定性，能够通过技术和管理手段提高运维和审计水平，降低运维成本，并能提供安全可靠的运行环境。实现了问题牵引，靶向解决安全信息系统运维要害，可有力支撑科研院所信息化工作。

关键词：安全信息系统；运维体系；三员人员；安全防护

中图分类号：TP309　　**文献标识码：**A　　**文章编号：**2096-4706（2021）13-0128-06

Research on Operation and Maintenance Standard of Safety Information System in Scientific Research Institutes

HUI Jianxin[1], QIAO Dezhi[2], LOU Hongwei[3]

(1.Purple Mountain Observatory, Chinese Academy of Sciences, Nanjing 210023, China; 2. Dalian Institute of Chemical Physics, Chinese Academy of Sciences, Dalian 116023, China; 3.Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China)

Abstract: This paper analyzes and studies the current situation of operation and maintenance of safety information system in scientific research institutes, in accordance with the requirements of relevant national systems, puts forward suggestions on establishing safety operation and maintenance standards for scientific research institutes. The standard opinion is reliability, universality and stability, it can improve the level of operation and maintenance and audit through technical and management means, reduce operation and maintenance costs, and provide a safe and reliable operating environmentin. It realizes problem traction, aims to solve the key points of operation and maintenance of safety information system, and can effectively support the informatization work of scientific research institutes.

Keywords: safety information system; operation and maintenance system; three personnel; safety protection

0　引　言

承担国家安全科研生产任务的科研院所，是国家科研力量的中坚，在科研过程中，安全信息系统运维工作尤为关键，随着新一轮体系论证深入开展，面对新问题、新挑战、新要求，科研院所面对审查认定所带来的巨大压力，在应对标准变化带来的前期准备工作仓促、内部管理目标的单一化，安全管理易偏向“粗放式”和“教条式”，出现为了迎合审查认定而开展安全工作，具体表现为：“标准有明确要求的才做”“标准要求做到什么程度就到什么程度”，甚至，个别研究所为了通过审查认定而采取“审查认定查什么就准备什么”或者“拿来主义”，不经思考、生搬硬套、照搬照抄等方式，由此，完全背离了安全信息系统运维监督管理的初衷，本末倒置了研究所内部管理对于信息安全管理的需求。

目前对于科研院所而言，在新的认定标准中，安全信息系统运维管理建设是最大的风险点，如：责任制落实不到位、定密不准确、知悉范围控制不精确、涉密人员管理有空档，计算机及通讯管理未知因素太多，试验设备（或工控设备）管理技术手段不够，宣传报道管理由于定密不准，审查就会把握尺度不精细。如果安全信息运维管理与研究所科研管理的实际不能有机结合，或者结合不紧密，仍然形成“两张皮”。安全信息系统运维外循环的安全管理，无从落地，纸上空谈，漏洞也必然存在，隐患危害巨大。

本文针对上述问题，就安全信息系统运维管理，开展“做什么”“怎么做”“谁来做”逐一剖析和解答。依国家规定要求，建立适合科研机构安全运维标准意见，在指导科研单位开展信息安全系统运维建设、实现通过技术和管理手段提高运维和审计水平，降低运维成本，并能提供安全可靠的运行环境，实现了问题牵引，靶向安全信息系统运维要害，支撑科研院所信息化工作。

1　安全信息系统运行维护分析

信息系统运维涉及工作主要有：

（1）运行维护管理和安全控制，运行管理和安全控制的目的是：保证系统不断变化和种类繁多的运行管理活动得到控制，信息系统的安全运行，操作人员应对信息系统实行

收稿日期：2021-06-18

基金项目：中国科学院十三五信息化专项项目（XXH13507-2）

正确和安全的操作。

（2）策略变更管理和安全控制，使用标准的方法和步骤，尽快地实施变更，确保在发生安全配置、安全设施、系统结构和业务应用等变化时，确保变更所导致的信息资产安全性降低、业务中断或业务影响降到最低。

（3）安全状态监控，安全等级不同的信息系统，安全监控方面要求采用的手段和监控内容有别。

（4）安全事件处置和应急预案，安全事件采取响应分级对待与事件处置机制，可根据相关标准建立合适的应急响应机制，保障业务系统的持续运行。

（5）运行检查和升级改进，在信息系统运行维护过程中，信息系统变更、安全状态改变等，情况常规事件时有发生。故而，定期对信息系统运行状况安全检查，并依据检查结果对信息系统进行持续改进。

但是对于安全信息系统，通常大家知道的就是分级保护和BMB标准，对于其他可能就知之甚少。所以本文研究过程中就要解决和回答以下一系列的为什么。

1.1 信息系统运维管理保障

因安全信息系统非普通的公共信息系统，该系统是需要保护国家秘密的安全的信息系统，所以安全信息系统必须要按照国家安全相关的法律法规来进行管理，要在组织机构、人员和经费上得到保障。

信息安全是指：运行信息系统中的数据以及信息系统的软件、硬件受到保护的程度，以及，防止威胁系统正常运行以及盗取系统中的知识、数据等信息而采取的措施。诚然，信息安全是一种思维方式，非依靠某一种技术就能实现的，无绝对的信息安全。

1.2 信息系统运维人员职责及履职

2013年的“斯诺登事件”提醒我们，大数据时代要以信息安全为主转变为数据、信息安全并重，制定防范与处置重大失泄密安全事故预案，自“严防死守”转变为“预防为先、攻防结合”，积极提高信息化管理水平。强化对网络和信息系统安全策略的管理，严密检测各种数据信息的流向，逐步实现“事先有措施、事中能监视、事后可追踪”。安全信息系统“三员”必须要认真履职，权限要划分合理。三员的职责划分是：

（1）系统管理员职责为信息系统服务器设备、网络设备的安装及维护，把握系统运行情况，确保物理安全；负责网络日常监控、维护，负责系统设备的维护，保证设备稳定运行。负责编写系统管理、网络运行部分的审计报告内容。

（2）安全管理员负责部署安全产品，制定和实施相关安全策略，负责信息系统中的用户账号管理，定期分析日志，及时解决和处理相关安全事件；负责编写安全管理系统安全日志、安全事件部分的审计报告内容。

（3）安全审计员负责根据安全审计策略，对系统的日志进行检查及抽查。对系统管理员、安全管理员的操作行为进行审计、跟踪分析和监督检查。根据系统管理员、安全管理员对于系统日志的分析，发现问题，及时纠正。组织定期完成审计报告。

1.3 安全信息系统的设备运维管理

涉密终端计算机的安全防护体系是一个比较复杂的系统，包括无线设备拆除、操作系统安装要求、密码设置、系统安全配置、安全产品安装等方面。如果没有制定新增涉密终端计算机的安装操作过程文件，系统管理人员在新增涉密终端计算机时没有可遵守和参考的标准，很容易操作不规范、遗漏重要的安全设置。系统管理人员还应记录涉密终端计算机的操作具体操作过程，这样作为系统管理工作的证据，同时也方便后续检查是否遗漏了哪些设置；再有安全信息系统的服务器、网络设备维修、报废和软硬件安装、更新，格式化和重装系统等，如果疏于管理，操作时不经过审批和记录，很容易就造成失泄密事件发生。

1.4 安全防护系统管理

运维人员明确各自职责，在安全防护系统管理方面，系统管理员应负责承载安全产品服务器的安装、安全防护系统的网络地址分配等任务。职责明确、分工具体，管理过程不能存在交叉、替代，保证操作过程统一、权责明晰。安全产品是安全信息系统的重要安全保障，单位应规范其管理过程，安全产品管理过程不规范容易造成系统安全措施失效，起不到安全防护的作用，同时影响到信息系统的正常运行。安全管理员具体负责安全产品的测试选型、策略配置、策略下发、终端计算机安全管理系统客户端安装管理等。单位应制定安全产品的管理规定和操作过程，安全管理员应按照制度规范操作，详细记录操作日志。

1.5 应用系统管理

应用系统是安全信息系统的重要资产，承载信息系统中的主要业务。应用系统的管理应实现分权分责，应明确系统管理员和安全员的职责，避免权责不清、工作交叉、替代。系统管理员应主要负责应用系统的服务器安装、数据库安装配置、基础数据账号的配置等工作。系统管理员负责具体业务功能、包括权限设置、业务规则设置、监控分析等。应用系统管理不规范容易造成系统中业务混乱，涉密电子文件在信息系统中得不到有效控制，造成涉密文件被非授权人员非法获取、通过非正常途径输出涉密信息等。单位应制定安全信息系统中应用系的管理规定和操作过程，运维人员应按照制度规范操作，详细记录操作日志。

2 安全信息系统运维管理

2.1 运维管理原则

安全信息系统运维原则是：稳定、安全、安全、可控、高效。

2.2 运维制度、操作规程

安全信息系统运维工作机构应制定运维管理制度，并经信息化管理部门审核后签发。安全信息系统运维工作机构应根据运维管理制度建立运维操作规程，规范具体运维工作。

2.3 运维人员管理

明确信息系统运维人员的任职条件，制定考核程序，经过考核后上岗工作，运维工作人员应签订安全承诺书。定期对安全信息系统运维人员工作情况进行考核，根据考核

情况进行奖惩，存在无法胜任信息系统管理工作的情况应及时调整。

安全信息系统管理“三员”人员，不能以其他用户身份登录系统；不能查看和修改任何业务数据库中的信息；不能增删改日志内容。三员应由本单位内部人员担任，要求政治上可靠，熟悉安全信息系统管理操作流程，具有较强的责任意识和风险防控意识；并签署安全承诺书。三员管理业务范围及边界如图 1 所示。

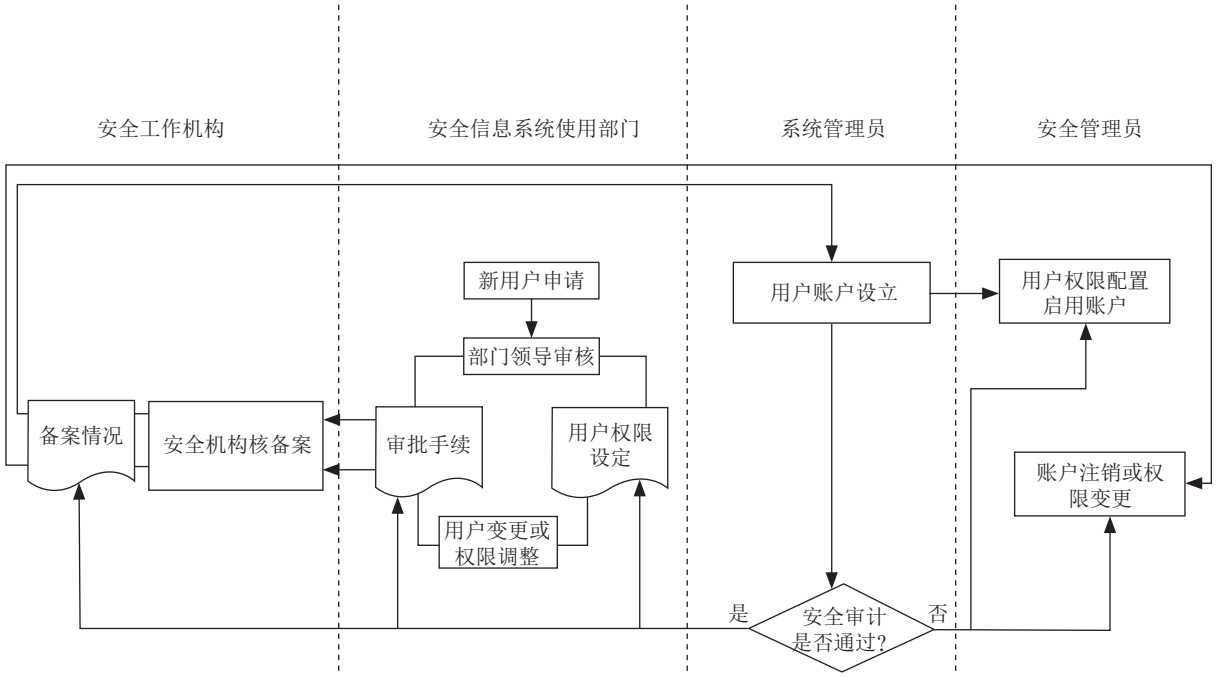

图 1 三员管理业务范围及边界

安全系统终端登录身份鉴别：对于安装 Windows 操作系统的安全系统终端，禁止使用远程桌面和远程登录功能，对于本地登录，不再单纯依靠 Windows 系统本身的登录认证机制，需在进行 Windows 用户认证的同时，采用 USB Key 对登录用户进行身份认证，同时 USB Key 使用口令（PIN 码）进行使用保护。

USB Key 与安全信息终端连接，在安全信息终端启动时，必须插入 USB Key，并输入正确的访问口令，才能进入 Windows 系统。涉密计算机终端本地登录身份鉴别的处理流程如图 2 所示。

2.4 应用系统管理

应用系统管理中各系统管理员职责和相关要求如以下所示：

（1）系统管理员职责是安全系统中应用系统服务器的安装配备，负责安装部署应用系统、安装配置相关的数据库系统、配置应用系统账户，如图 3 所示。

（2）安全管理员负责信息系统中应用系统的配置账号权限、设置业务规则设置，负责监控分析应用系统运行情况。

（3）应用系统部署操作规程。

（4）检查应用系统在身份认证、权限划分、安全审计、数据安全方面的系统功能是否符合安全要求。

（5）按照信息系统服务器安装配置要求安装与配备应用服务器。

（6）在服务器上安装与部署应用系统以及相关的数据库等系统。

（7）配置系统管理员、安全管理员、安全审计员权限。

（8）配置终端用户账号及默认密码，要求用户首次登录后修改默认密码。

（9）配置应用系统数据、文件管理流程及策略，保证敏感数据的存储、传输、输出等过程符合安全要求。

（10）安全审计员职责是审计系统管理员和安全管理员操作。

（11）应用系统安装部署、变更、废止应履行审批手续，经信息化管理部门审批。系统管理员和安全管理员接到《应用系统管理审批表》后，进行操作，安全审计员负责审计系统管理员和安全管理员操作，详细记录操作内容。

2.5 应用软件管理

系统管理员在应用软件管理中应负责的主要事项如下：

（1）系统管理员负责信息系统用户终端计算机各种应用软件的安装与卸载。

（2）信息系统内用户终端计算机常用软件可建立软件白名单，终端用户可下载并安装白名单内软件，无须进行审批。

（3）系统管理员负责信息系统应用软件白名单管理，将白名单内软件上传至信息系统公共下载网站，提供下载服务。

（4）上传、变更白名单软件应履行审批手续，经信息化管理部门审批。安全管理员《软件审批表》后，负责对上传的软件进行安全检查，确保没有敏感信息，系统管理员负责上传文件。安全审计员负责审计系统管理员和安全管理员操作。

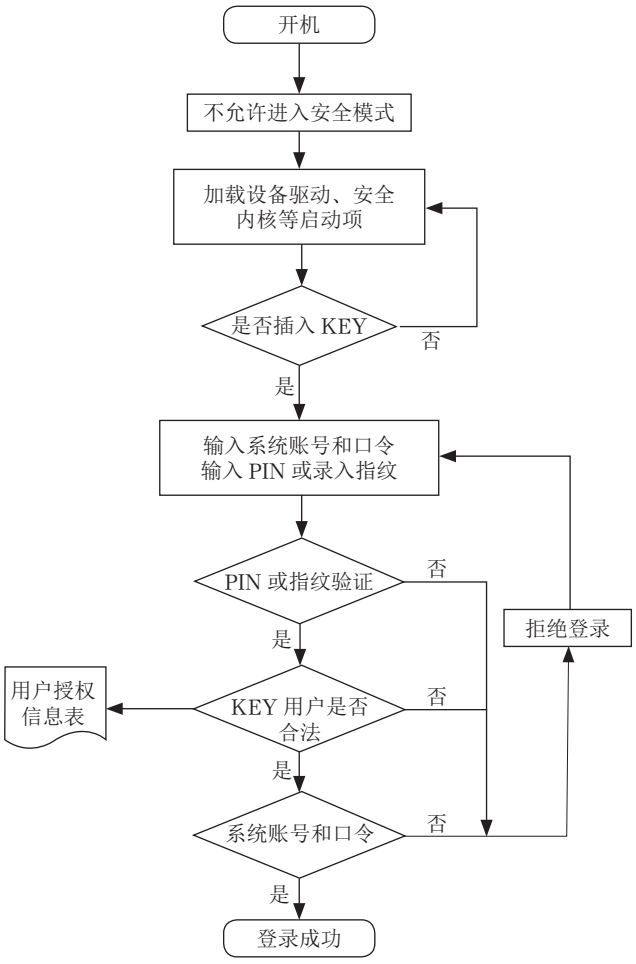

图 2　操作系统身份鉴别流程示意图

3　安全信息系统运维标准的意见

3.1　信息系统运维管理是一个系统性管理

安全信息系统运维管理水平直接影响安全信息系统的使用效果，面对复杂的运维内容和类型繁多的软硬件设备，通过明确归口管理，从制度上确定运维管理体系；通过健全组织机构、配备合适人员来“强身体”；通过执行法律法规和规章制度来“正思想”，增强人员能力素质；通过配置运维工具、保证正常运维经费，按程序和规范做“正确事”，并以加强安全防护体系完善和技术创新提升运维“攻防”能力，共同协作推动安全信息系统运维工作向更全面、更迅速、更专业、更智能的方向发展。

提出工作重点是安全信息系统运维管理应重点围绕制度建设、组织机构、管理责任、运维管理人员、运维工具、设备和信息交换等可能存在的重大风险和问题，总体要求是要充分认识安全信息系统运维管理和节点安全的重要意义，坚持底线思维，加强风险管理，建设和完善预警监测体系，防范和化解安全信息系统运维中发现的重大安全风险。

（1）围绕信息领域安全和关键核心技术开展安全信息系统安全风险研究，向国家有关部门提出对策建议，着力解决国家安全信息系统安全急需的重大科技问题。

（2）开展安全信息系统安全风险评价工作，建立评价、审核、防范措施落实、监督检查和评价警示机制，建设并运行安全信息系统管理的预警监测体系，实现安全信息系统运维安全，风险全过程监测预警。

（3）建立和完善安全信息系统安全风险隐患及事件事故处置流程，制定落实奖惩制度，压实安全信息系统运维安全风险管理工作责任。

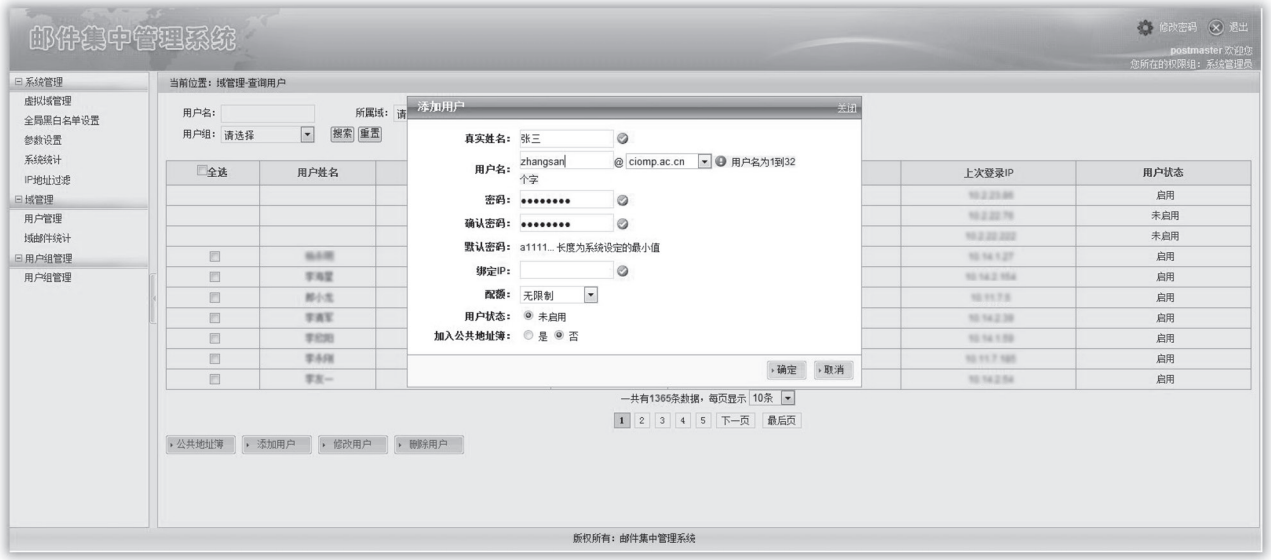

图 3　信息安全邮件集中管理系统

3.2　规范安全信息系统“三员”的职责和工作标准

安全信息系统的运维工作是由使用者发现系统故障后，提出申请联系安全信息系统管理员，系统管理员对故障进行初步判断并开始处理，如需要安全员参与，则安全员按权限完成相应工作，最终解决问题完成该次安全信息系统的运维动作，安全审计员随后对上述“两员”工作进行审计。一些研究所由于体量较小，“三员”可能不能完全专职，或兼任其他岗位，所以对“三员”的岗位职责和工作标准必须有清

楚的界定和要求。

明确了安全信息系统“三员”的岗位职责。

3.2.1 系统管理员

相关职责：安全系统相关参数的制定、配置与监控管理；如运行条件、技术性能、空间分配、参数设置等。

（1）负责网络系统、服务器系统等的日常运行管理和维护技术支持。

（2）在安全管理员的配合下，定期升级安全设备及其规则库。

（3）配合安全管理员定期进行病毒查杀、处理。

（4）对系统日志、策略配置文件等数据定期备份。

（5）负责定期分析网络设备、操作系统等的系统日志，发现系统异常、错误或报警等分析原因，提出解决办法并加以实施。

（6）负责网络与系统运行状况的统计分析，定期编写安全运行报告。

（7）根据安全系统需求变化，不断优化系统运行环境。

3.2.2 安全管理员

负责安全信息系统络的安全评价，安全策略、用户权限以及有关参数设置等日常安全管理工作。

（1）主要职责是提出文档化的安全系统、安全策略文件编制建议，实施各类安全设备的安全策略。

（2）负责实施安全系统用户权限分配和调整。

（3）协助系统管理员完成操作系统的各项配置，制定和实施安全策略。

（4）检查分析安全设备、操作系统和应用系统用户操作日志，负责对用户及安全审计员的操作行为进行审计。

（5）负责对安全管理系统日志审计、异常事件和行为进行统计分析，定期形成审计报告。

（6）负责网络安全日志、事件统计分析，定期开展风险评价和形成风险评价报告。

3.2.3 安全审计员

其职责是对安全管理员的操作行为进行审计、跟踪、分析和监督检查，及时发现违规行为和异常行为，包括系统日志分析、安全事件的分析、取证等。

（1）对系统管理员和安全管理员制定和更改操作系统、应用系统、网络设备、安全设备的安全策略、用户权限以及参数设置等进行审核和监督。

（2）定期检查维护记录，“检查有痕”通过记录，实施监督。

（3）负责对系统管理员和安全管理员的异常操作和行为进行统计分析，定期形成审计报告。

3.3 引入安全信息系统信息设备接入和应用管理的操作规范

信息设备是安全信息系统的“骨架”，涉及设备种类、型号、功能等较为复杂，按照运维场景区分为服务端运维和用户端运维。其中，服务端运维主要针对服务器、路由器、交换机、磁盘阵列等机房设备；用户端运维主要针对计算机、显示器、集线器、签字板等接入终端设备；系统运维工作包括设备的接入维护、保养、更新、升级、故障检测及排除；系统安全运维包括应用系统、账号、访问控制、数据备份、应急预案等，这些工作需要明确的操作规范。

提出了上述系统运维工作的技术标准和操作规范，如：服务器、网络设备运维管理；安全防护系统管理；应用系统管理；应用软件管理；账号及权限管理；数据备份与恢复管理；防病毒系统、系统补丁管理；访问控制管理；机房管理维护；应急响应管理；安全审计和风险评价管理等，以及工作中所使用的表格。

4 结 论

安全信息系统运维管理和节点安全有着重要意义，为坚持底线思维，加强风险管理，建设和完善预警监测体系，防范和化解安全信息系统运维中发现的重大安全风险，采取的主要措施有：

（1）开展安全信息系统预警体系，建立评价、审核、防范措施落实、监督检查和评价警示机制，建设并运行维护系统安全预警监测体系，实现系统安全风险全过程监测预警。

（2）建立和完善安全信息系统安全风险隐患及事件事故处置流程，制定落实奖惩制度，压实安全信息系统运维安全风险管理工作责任。

（3）根据我们在研究管理过程中发现重大难点与问题，围绕信息领域安全和关键核心技术开展安全信息系统安全风险研究，向国家有关部门提出对策建议，着力解决国家安全信息系统安全急需的重大科技问题。

安全信息系统运维管理应重点围绕制度建设、组织机构、管理责任、运维管理人员、运维工具、设备和信息交换等可能存在的重大风险和问题，开展风险辨识、分析、监测和评价，提出意见建议，前瞻部署和防范；在制度建设方面，要制定管理标准规范和运维制度，涉及运维外包的要有针对外包运维的管理和考核制度；在组织机构方面，要高度关注运维工作，建立运维工作领导机构和工作机构，严格落实防范措施；在管理责任方面，要明确业务部门在运维管理体系中的职责，各负其责；在人员管理方面，要合理配备运维管理人员、明确职责，严格考核；在运维工具方面，选取上先进的信息化应用充分提高运维效率和运维水平；在设备管理方面，要标识清晰、准确，存放位置相对固定，专人管理；在信息交换方面，要准确区分安全域，确保信息安全可控；在风险监测方面，建立系统监控平台，及时发现风险隐患，提高运维效率。

参考文献：

[1] 王伊然，于奇平，刘奥祥 . 云计算信息系统安全整体防护策略研究 [J]. 河南科技，2018（7）：7-9.

[2] 李英 . 集团级管理的标准化管理信息系统设计与实现 [D]. 西安：西安工业大学，2014.

[3] 刘文慧 . 信息安全风险评估量化方法研究 [J]. 数字通信世界，2018（5）：252+104.

[4] 康冉 . 公安网络安全系统的设计与实现 [D]. 济南：山东大学，2010.

[5] 王连海 . 中船重工财务公司综合信息平台设计与实现 [D]. 成都：电子科技大学，2011.

（下转 135 页）

3.4 根据底层指标值计算安全值

底层指标值的获取采取现场测评的方式，这里需要得到资产、威胁、脆弱性的具体赋值。传统计算方式是采用“相乘发”计算风险值。针对第 1 个二级指标，资产重要性赋值 A=5，威胁发生频率赋值 T=3，脆弱性赋值 V_1=2，V_2=1，V_3=1，V_4=2。通过计算可以得到风险值 R_{421} 为 2·783 2，R_{422} 为 1·968 0，R_{423} 为 1·968 0，R_{424} 为 2·783 2。风险值 R 为 1-5 标度的反向值，R 越大，安全性越差。本文计算的评估值 E 为百分制的正向值，因此需要公式（6−R）× 20 将风险值转为评估值，为 72·488 0。同理可以计算出其余 71 个二级测评指标的评估值。然后逐层求解风险值，计算出 10 个一级指标安全值 E_n 和 1 个综合安全值 E。经计算该水厂 SCADA 系统信息安全综合值为 70·57，安全级别属于中等偏上。

3.5 结果分析

该水厂风险评估的安全值为 70·57，安全程度处于中等偏上，存在一定的安全隐患。从计算结果可以看出，重点应该从计算环境、管理中心、管理人员、运维管理 4 个方面采取适当防护措施，提高系统安全性。

计算环境方面测评存在最大的风险是 SCADA 系统身份鉴别机制单一，主要是通过账户密码登录，并且密码简单不经常更换，容易导致账户信息泄露。因此需要设置复杂的账户密码并定期更换，必要时采用“双因子”进行身份鉴别。

管理中心方面测评存在最大的风险与计算环境方面的风险具有一致性，应对系统管理员和审计管理员的身份进行鉴别，并规定其工作职责和任务。

管理人员方面测评存在最大的风险是对已经离职的人员，没有及时终止其所有访问权限，可能后期被利益交易、不法利用，给单位造成不可估量的损失。因此需要在人事变动时，对离岗人员办理好交接手续，签订相关保密协议，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，删除账户信息。另外工作人员的安全意识也是非常重要的一个方面，需要定期开展安全意识培训工作。

运维管理方面测评存在最大的风险是主机操作系统的安全软件没有更新，可能会被恶意代码利用，让主机失去正常工作性能。因此需要安装防恶意代码软件的同时定期进行升级和更新防恶意代码库。

4 结 论

本文构建了 SCADA 系统信息安全风险评估的层次结构模型，然后采用对评价指标排序赋值的方法，构造了符合一致性要求的判断矩阵，提高了工作效率。信息安全风险是动态变化的，本文采用的层次分析法不能动态开展评估工作，只能重复性评估达到实时了解系统安全状况，由于风险评估工作数据量大，计算复杂，完成风险评估结果的分析需要花费大量时间。因此可以开发一个评估系统，将计算工作交给电脑来处理，可以解放人力，提高工作效率。

参考文献：

[1] 郭昊，何小芸，孙学洁，等 . 国家电网边缘计算应用安全风险评估研究 [J]，计算机工程与科学，2020，42（9）：1563−1571.

[2] 张炳，任家东，王苧 . 网络安全风险评估分析方法研究综述 [J]. 燕山大学学报，2020， 44（3）：290−305.

[3] 王姣，范科峰，莫玮 . 基于模糊集和 DS 证据理论的信息安全风险评估方法 [J]. 计算机应用研究，2017，34（11）：3432−3436.

[4] 许硕，唐作其，王鑫 . 基于 D−AHP 与灰色理论的信息安全风险评估 [J]. 计算机工程，2019，45（7）：194−202.

[5] 梁智强，林丹生 . 基于电力系统的信息安全风险评估机制研究 [J]. 信息网络安全，2017（4）：86−90.

作者简介：李丹（1993—），女，汉族，湖北孝感人，在读硕士研究生，研究方向：信息安全。

（上接 132 页）

[6] 蒋斌 . 如何做好大数据时代的保密工作 [J]. 保密工作，2019（9）：64−65.

[7] 俞航 . 信息系统安全等级保护制度实施中存在的问题及其对策 [D]. 苏州：苏州大学，2016.

[8] 张惠 . 信息系统运维阶段信息安全风险评估工作研究 [J]. 网络安全技术与应用，2018（6）：15−17.

[9] 张红卫，惠建新 .Web Service 构架下的多语种构件库系统及实现 [J]. 计算机与数字工程，2014，42（4）：616−622+728.

[10] 焦迪 . 有关构建政务信息系统密码应用管理体系的建议 [J]. 信息安全与通信保密，2021（1）：70−76.

[11] 李忠俊，张永峰，宋波 . 企业信息安全应对策略探讨 [J]. 电脑知识与技术 ,2017，13（21）：36−37.

[12] 刘志勋 . 企业信息安全风险及控制策略探究 [J]. 信息系统工程，2016（3）：74.

[13] 章建聪，沈晔 . 浅析通信设计企业保密管理体系的构建 [J]. 保密科学与技术，2020（12）：63−66.

[14] 王洪元，刘晓飞，李晓杰 . 基于医院信息系统探究医院信息管理体系的构建 [J]. 数字通信世界，2020（4）：196−197.

[15] 桂若柏 . 信息安全风险评估模型的研究及其应用 [D]. 重庆：重庆大学，2004.

[16] 学习《国家安全法》百问百答 [EB/OL].（2017−04−18）. http://www.gdqy.gov.cn/xxgk/zzjg/zfjg/qysszbgs/zwgk/zcfg/content/post_86778.html.

[17] 三员职责 [EB/OL].（2017−10−16）.https://max.book118.com/html/2017/0911/133408498.shtm.

[18] IT 治理信息安全管理：标准、理解与实施 [EB/OL].（2004−11−19）.http://www.itgov.org.cn/Item/469.aspx.

作者简介：惠建新（1978—），男，汉族，江苏盐城人，工程师，硕士，主要研究方向：应用系统开发，系统分析与集成，信息系统管理；乔德志（1979—），男，汉族，辽宁大连人，高级工程师，硕士，主要研究方向：安全信息系统设计与开发，涉密网运维；娄洪伟（1982—），男，汉族，吉林长春人，正高级工程师，硕士，主要研究方向：网络安全架构研究，涉密网建设与维护。