DOI:10.19850/j.cnki.2096-4706.2021.11.042

科研院所安全信息系统管理体系构建

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：对集团内相关安全机制和管理方法进行了研究。在此基础上，提出了对“系统、网络、运维、用户”四个层面的信息安全管理举措，形成了统一的一体化安全管理体系，实现了从管理理念到技术保障、系统建设、运维支持和用户应用的全方位信息安全管理架构。在有关单位执行过程中，保证了系统的安全性、完整性、实用性；能有效提高安全信息系统的安全管理水平和安全保障能力。该体系对安全信息系统建设、评价、运维具有指导作用。

关键词：ISMS；系统管理；体系框架；安全信息

中图分类号：TN915.08　　**文献标识码**：A　　**文章编号**：2096-4706（2021）11-0158-05

Construction of Security Information System Management 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: The relevant security mechanism and management methods within the group are studied. On this basis, it puts forward information security management measures at four levels of "system, network, operation and maintenance, user", forms a unified integrated security management system, and realizes comprehensive information security management architecture from management concept to technical support, system construction, operation and maintenance support, and user application. In the execution process of the relevant units, the security, integrity and practicability of the system are guaranteed; it can effectively improve the security management level and security guarantee ability of security information system. The system plays a guiding role in the construction, evaluation, operation and maintenance of security information system.

Keywords: ISMS; system management; system framework; security information

0　引　言

随着新一轮军工保密资格审查认证工作的不断推进和深入开展，全国安全信息系统分级保护测评要求不断提高，多年以来，安全信息系统不断更新“补丁”、持续设备改造升级；安全信息相关单位的安全信息系统均按照要求配置相关技术手段和安全保密产品；搭建安全保密策略、强化了“三员”（安全信息系统配备的系统管理员、安全保密管理员、安全审计员）岗位以及职能职责。但对保密管理尚存在认识误区：如将信息安全产品和方案理解成一道坚固的静态防线，而非随保密工作环境变化和新增风险进行的动态管理；单纯地将一本安全保密规章制度作为应付检查的“利器”。在实际保密工作中，不能因地制宜地保证保密工作范围内各项工作的可控性，不能保证管理能持续覆盖保密工作中出现的新层面与环节，导致实际工作时“理想”与“现实”错位。结果很可能是“有而无防”“防而不密”，各种安全产品成为“摆设”，空有技术措施投入，徒有管理人员，而安全信息系统依然是安全漏洞频出。

“工欲善其事，必先利其器”，作为相关承研单位必不可少的信息流转及处理环境和手段，安全信息系统在安全生产过程中起着越来越大的作用，它不仅便利各类信息的流转和利用，工作效率得到极大提高。与此同时，对安全信息的数字化、数据集中化处理过程中的极大风险也随之而来，“安全信息系统”安全风险、安全漏洞问题也深受困扰。安全信息系统在投入使用之前，虽经过测评并取得使用许可证，其安全信息系统的管理、使用过程中将会产生新的风险，可能形成失泄密隐患。

“工欲善其事，必先利其器”，安全信息系统作为相关承研单位必不可少的信息流转以及处理环境和手段安全生产过程中，起着越来越大的作用，它在为各类信息的流转和利用提供便利，使得工作效率得到极大提高的同时，也给安全信息的数字化、数据集中化处理过程带来了极大的风险，安全信息系统也深受安全风险、安全漏洞问题困扰。安全信息

收稿日期：2021-05-05
基金项目：中国科学院十三五信息化专项项目（XXH13507-2）

系统在投入使用之前，虽经过测评并取得使用许可证，但其安管理、使用过程中将会产生新的风险，可能形成泄密隐患。

1 安全信息管理难点及存在的安全问题

1.1 安全信息系统工作现状

“事件驱动”背景下，应深刻认识到信息安全管理的重要性。新态势下，科研院所保密工作有以下工作特点和规律：承研单位信息安全保密管理在强化保密观念、落实保密制度、增强技术防护能力、提高人员素质等方面的薄弱环节，缺少新态势下信息安全保密管理运维标准。解决安全项目承研单位安全信息系统安全保密管理问题，需要实现由间断教育向连续的系统教育转变，着力于增强科研人员的保密意识；实现由主要依靠行政手段管理向综合运用法律、行政、技术手段管理转变，着力于依法治密；实现由偏重对密级文件的管理向着重抓好计算机网络安全保密管理转变，着力于科技治密；实现安全人员队伍建设由非专业化向专业化转变等成为各单位在安全信息系统管理中的核心问题，着力于提高治密能力；急须构建安全信息系统运维管理及节点风险评价体系。

1.2 存在的问题与原因

1.2.1 标准制度繁杂且方法落实欠缺

在监督检查过程中缺乏有力抓手，制度、标准及规范的落实上，措施和手段“柔软无力”，“理想”与“实际”形成了“两条线”。为此，奋力构建统一的一体化，安全管理系统体系，让安全信息系统管理真正落地，迫切需要梳理安全制度和管理办法。

1.2.2 缺乏安全运维标准和规范

运维环节是安全信息系统生命周期中的重要环节，在落实运维和审计方面的控制点时，使用信息系统的单位在落实分级保护要求的过程中，会遇到一些困扰，例如：（1）如何合理安排操作规程，解决因松散的管理方式而出现的鉴别信息被遗忘、泄露或者权限遭到滥用等威胁的问题？（2）如何以高效的方式获取足够的抽样样本，从而证明结果判定的准确性？在互联网络设备、主机和数据库的访问控制、账号管理、口令策略以及权限管理和审计管理测评等环节中，如何快速定位各环节的脆弱性和威胁情况，并追溯相关安全事件？（3）在实现各类访问权限控制方面，如何将自主访问控制和强制访问控制措施落地？（4）如何借助相关技术工具及技术手段，把握长效的监督，以确保管理措施的顺利执行和实现？（5）如何达成对各类资源、设备客体访问日志信息的统一管理、实现高级查询和“靶向”定位？管理员如何统一部署主机、制定网络设备的安全审计措施？

鉴于上述问题，信息化部门急切需要建立统一的安全运维管理、执行和控制规范体系，且在安全运维系统中进行固化，使安全运维工作依规范执行，从流程操作环节进行控制。此外，对相关管理运维事件的问题分析、处置过程、操作结果进行“留痕”可追溯管理，构建运维知识库，增强安全运维的效率、确保质量和服务水平。

1.2.3 管理随意化与风险评估主观化

目前普遍采用的方法是根据信息系统资产、脆弱性和威胁各要素最终赋值结果进行风险计算，存在不确定信息难以量化的问题，难以有效地对安全信息系统进行网络安全评价。而且掩盖了资产要素对保密性、完整性和可用性的不同需求，导致参与计算的脆弱性要素存在重复计算的问题，而且评价结果太过依赖专家的主观性判断，对最终结果造成干扰。

2 安全信息系统管理体系构建与实现

2.1 安全信息系统安全性管理主要问题

2.1.1 资产与风险的部分识别

安全信息系统的管理不等同于普通网络系统管理。应用安全信息系统以服务科研相关的安全工作需要切实了解在此过程中相关的资产。这里的资产包括对组织或相应任务有价值的所有事件，包括安全信息系统软硬件设备、存储的文件和数据等。了解这些资产对于组织或任务的价值以及其他属性。业务对资产依赖度越高，资产的价值越高，其系统面临的风险越大，越应该加强相关保密工作。不完整识别资产与风险，就不能形成完整的安全保密需求，不能全面确保安全信息系统的效能。因此形成资产与风险识别的标准、方法以及体系对于确定保密管理范围并进行安全信息系统网络的管理至关重要。

2.1.2 安全信息系统管理工作组织机构、机制及政策落实

安全信息系统管理不仅是信息技术层面的管理。保密安全需要通过行政管理来实现目标确定、责任划分、资源匹配、过程规范、风险处置、残余风险接受标准、能力意识培训等。探寻科学的方法，依据任务、组织保密战略需求、现有管理架构和资源规划无法实现安全信息系统管理工作机构和制度，严格执行安全信息系统体系管理工作，亦是安全信息系统体系管理建设应该重点关注的问题，任何一项的缺失都会增加保密工作的风险。

2.1.3 信息与通信安全和物理安全

信息与通信安全和物理安全是安全信息系统正常运行的保障，其技术层面的工作主要涉及每个操作层次的防护、控制措施，比如安全信息系统网络配置管理、系统管理、变更管理、边界管理、黑客与病毒侵害防范等。对于每一项控制措施的目标、资源分配、完整性、局限性都需要进行深入的分析，形成规范性操作控制，才能保证安全信息系统平稳、正常运行，达到建设目的。

2.2 安全信息系统体系框架

失败是成功之母，一切都是努力的结果。早在我国试行分级保护测评之前，信息安全管理体系（Information Security Management System, ISMS）已作为国际标准有了丰富的理论基础和案例经验，近十年来，不断补充、修改、完善，约三分之一的安全信息技术管理员解决技术问题，其余三分之二则负责制定政策和程序并处理应急规划、促进安全意识、安全评价、风险分析。目前，全球企业强力构筑信息安全坚固堡垒，在安全信息系统管理上遇到的各种问题，都可在ISMS思想中找到答案，该体系方法有效、能够搭建起安全信息系统安全、保密管理体系框架，能够提高系统安全、保密管理的效率和质量，保证信息的安全性、完整性、

可用性。一套完整的安信息系统安全管理制度体系框架如图 1 所示。

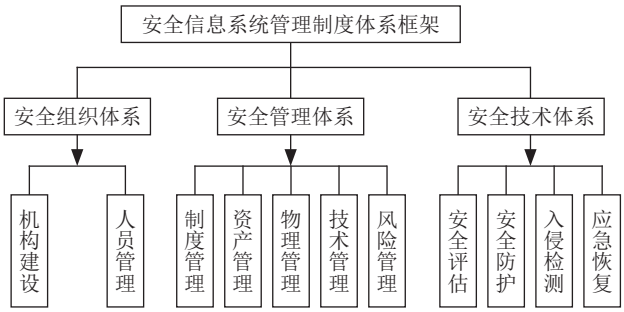

图 1　信息系统安全管理制度体系框架

本项目的目标是依据组织和任务的保密需求，具体定义科研相关安全信息系统管理体系的要素，形成科学分析方法，进而建设出适合于我们保密工作的安全信息系统管理体系。

2.3　安全信息管理体系框架实施步骤

信息世界中，攻防是永恒的话题，信息安全管理是指“相对处于没有危险和不受内外威胁的状态”，即通过不断加强维护自身安全能力建设，管理体系和技术体系来确保实现信息安全管理的目标。制度管理、资产管理、物理管理、技术管理和风险管理构成了统一的安全管理体系，这是实现安全目标的保障。安全评价、安全防护、入侵检测、应急恢复构成了安全技术体系，而做好安全保密管理工作的核心是安全组织体系中机构建设、人员管理。实施步骤如图 2 所示。

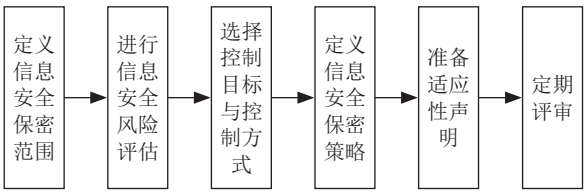

图 2　安全信息系统管理体系实施步骤

建立安全信息管理体系框架，必经的几个步骤：（1）定义信息安全保密范围。保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。（2）进行信息安全风险评估。对信息系统的资产价值、潜在威胁、薄弱环节、已采取的防护措施等进行分析，判断安全事件发生的概率。（3）选择控制目标与控制方式。安全信息系统数据安全为目标，人防技防为控制方式。（4）定义信息安全保密策略。保障信息安全，切实推行安全管理，积极预防风险。（5）准备适用性申明。针对风险评估结果，制定风险应对措施时，选择哪些控制措施，不选择哪些控制措施，控管结果可能会有差异。（6）定期评审。加强对安全生产制度的管理，及时评审和修订。

3　安全信息管理体系实现

3.1　安全信息管理体系

根据“业务谁主管、保密谁负责”的原则，保密机构、信息化管理部门和业务职能部门根据相关职责分工，如：各单位科研生产、人力资源、信息化、新闻宣传、外事等职能部门，应当明确安全信息系统管理职责，结合各自业务工作实际，归口负责业务工作范围内的安全信息系统运维管理工作和相关工作制度制定，制定细化管理制度与要求。

安全信息系统应重点围绕组织机构、管理人员、管理责任、制度建设、管理策略、管理工具六个方面进行运维管理。管理围绕信息交换，设备管理展开，对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，提出意见和建议，预先部署和防范；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。安全计算机及移动存储介质保密管理系统如图 3 所示。

图 3　安全计算机及移动存储介质保密管理系统

对安全信息系统风险隐患及事件发生情况进行统计分析，每一年自评估，每两年度开展一次风险评价，依据评价结果分为绿、黄、红三个等级，根据不同等级进行警示通报。对于风险防控不落实，或违反规定、发生安全信息系统安全事件事故，给单位创新发展造成严重后果及影响的单位要予以通报批评，对相关人员进行严肃处理，并将单位和个

人列入警示名录；对于积极开展安全信息系统安全风险研究，认真落实防范措施，应视情况向有关单位安全信息系统安全的单位和个人予以奖励。

各单位信息化管理部门对安全信息系统运维管理的职责有：（1）负责信息系统、信息设备和存储设备的安全保密管理。（2）组织制定信息安全策略、管理制度和操作规程等体系文件。（3）指定或者委托内部机构负责信息系统、信息设备和存储设备的运行维护。（4）监督运维管理操作是否合规。（5）检查运维机构对安全信息系统网络安全运行状况的监控是否到位。（6）监管运维机构是否定期编写审计报告和安全风险评价报告。（7）监管运维机构是否及时落实安全隐患、安全漏洞和安全风险的整改措施。

各单位保密工作部门对安全信息系统运维管理的职责有：（1）是否遵循安全信息系统网络安全保密工作流程以及相关管理制度。（2）运行维护的相关操作是否经过审批后实施。（3）日常操作记录是否全面完整。（4）是否定期编写提交运行报告和安全审计报告。

3.2　安全信息管理体系试用情况及成果

该体系统稿撰写完成后，在有关科研院所、航天系统单位、地方保密局试用并征询意见，各试用单位反馈该管理体系能够坚持底线思维，有力加强风险管理，丰富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，试用效果良好。

课题研究组编制完成了：（1）《强化归口管理，落实保密责任》的报告，从信息化保密责任有哪些、怎么问责、管理档案如何建档做了详细介绍。（2）《研究所信息系统管理实践与思考》的报告，从研究所信息系统基本情况、研究所信息系统管理实践、信息系统未来的几点思考和对院安全信息系统管理的建议做了详细分析和介绍。（3）《正确、准确、精确——日常保密管理的理念、做法与思考》的报告，从研究所信息系统开展安全信息系统管理的理念、做法和思考做了详细说明，对运维风险查找、评价和消除做了实践演示。（4）《安全信息系统运维手册》的报告，从研究所信息系统开展安全信息系统管理的理念、做法和思考做了详细说明，对运维管理、日常使用作实践演示。

4　结　论

世界正经历百年未有之大变局，大变局带来大挑战，也带来大机遇，须因势而谋，应势而动，顺势而为。信息化浪潮席卷全球，信息安全面临前所未有的新挑战、新情况、新问题，本文通过梳理科研院所现行的相关管理制度、执行标准、规范规定等分析“信息差”“理想化”“想当然”等错误认识和短视思想。构建相关统一标准、统一方法、统一制度体系，具体为：（1）统一纷杂标准、方法、规范，建立了统一的一体化，安全管理系统体系，让安全信息系统管理真正落地，理顺安全制度和管理办法。（2）统一相关操作规程、回答和解决了实际管理过程中遇到的相关问题，提供了操作过程中出现问题的“最优答案”，重点在运行维护和监督审计方面回答了：1）如何合理安排操作规程，设法规避因松散的管理方式而出现的“鉴别信息被遗忘、泄露或者权限遭到滥用等威胁”，构建起科学高效操作规程。2）如何高效的方式获取足够的抽样样本证明结果判定的准确性，针对互联网络有关设备、主机及数据库的访问控制、用户管理、口令策略、权限管理及安全审计管理中，并且能快速定位上述环节的脆弱性和威胁，追溯相关安全事件。3）为实现各类访问权限控制，如何将自主访问控制和强制访问控制措施落地。4）如何保证管理措施的顺利执行和实现，在技术工具及技术手段助力下，把握长效的监督，瞄准等级保护提升相关管理制度的执行力。5）怎样对各有效资源、设备客体访问日志信息的统一管理和高效运维、实现了高级查询和“精准”定位；管理员如何统一部署主机、制定网络设备的安全审计措施。

提出对“系统、网络、运维、用户”四个层面的信息安全管理举措，构建起统一的一体化安全管理体系，满足从管理理念到技术保障、系统建设、运维支持和用户应用的全方位信息安全管理架构。试用过程中实现信息的安全性、完整性、实用性，该体系对安全信息系统安全建设、评价标准、运行维护具有指导作用。

参考文献：

[1] 郭夏言，周洁 . 基于 ISMS 思想的涉密信息系统安全保密管理体系框架研究与构建 [J]. 保密科学技术，2011（8）：14-16.

[2] 李晨旸，张晓梅，李媛 . 一种基于层次分析法的大规模信息系统风险评估方法 [J]. 计算机应用与软件，2013，30（10）：322-325.

[3] 张红卫，惠建新，张永兵，等 .H-ADCP 回归方程拟合及应用系统的研究 [J]. 计算机技术与发展，2015，25（9）：194-198.

[4] 李嵩，孟亚平，孙铁，等 . 一种基于模型的信息安全风险评估方法 [J]. 计算机工程与应用，2005（29）：159-162.

[5] 何敏 . 新形势下军队院校信息安全保密管理问题及对策研究 [D]. 长沙：国防科学技术大学，2011.

[6] 井光山 . 信息安全管理体系（ISMS）及其构架（一） [J]. 信息安全与通信保密，2001（6）：64-65.

[7] 百度文库 . 信息网络安全知识普及教育培训教程——信息安全基础 [EB/OL].（2021-01-22）.https://wenku.baidu.com/view/96e1f3cdb968a98271fe910ef12d2af90242a8b4.html.

[8] 蔡荣生，郭洪林，林宁 . 信息系统的安全性管理 [J]. 中国人民大学学报，2005，19（3）：121-126.

[9] 张淮，王健宇 . 涉密信息系统安全保密风险管控思路 [J]. 保密科学技术，2016（10）：20-21.

[10] 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.

[11] 张振华 . 廊坊供电公司信息安全管理的研究和应用 [D]. 北京：华北电力大学（北京），2010.

[12] 刘行，杨维永，赵甫 . 基于等级保护的安全运维系统的研究与设计 [C]// 第二届全国信息安全等级保护测评体系建设会议 . 上海：《信息网络安全》编辑部，2012：68-70.

[13] 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.

[14] 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.

[15] 焦迪 . 有关构建政务信息系统密码应用（下转165页）

4 结　论

在分析网络和计算机攻击分类法现有研究成果的基础上，本文提出了一种基于响应的攻击分类法，以全面满足 AIR 系统在响应决策中建立攻击与响应对应关系的需求，填补现有研究的空白，文中对该分类法的攻击源、攻击方式和攻击结果三大组成维度进行了详细介绍，同时介绍了实例测试情况，该分类法在实际应用中切实可行，对 AIR 系统的研究起着重要作用。

本方法在攻击分类法领域进行了新的尝试。虽然该分类法已获得初步应用，易于分类攻击和建立与响应的对应关系，但它还存在进一步完善之处，对组合攻击的处理就是一个例子，该类攻击由多种不同的攻击方式组成，但本方法对其响应还是单独响应，依然值得深入研究，另外，新型攻击层出不穷，本分类法必须保持同步，后续研究将立足于这些方面，以不断完善。

参考文献:

[1] HAN W J，XUE J F，YAN H. Detecting anomalous traffic in the controlled network based on cross entropy and support vector machine [J].IET Information Security，2019，13（2）：109-116.

[2] HUBBALLI N，SANTINI J. Detecting TCP ACK storm attack：a state transition modelling approach [J].IET Networks，2018，7（6）：429-434.

[3] KONING R，GRAAFF D B，POLEVOY G，et al. Measuring the efficiency of SDN mitigations against attacks on computer infrastructures [J].Future Generation Computer Systems，2019，91：144-156.

[4] KOTENKO I，DOYNIKOVA E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics [J].The Journal of Defense Modeling and Simulation：Applications，Methodology，Technology，2018，15（2）：181-204.

[5] HOUNSOU J T，NSABIMANA T，DEGILA J. Implementation of Network Intrusion Detection System Using Soft Computing Algorithms（Self Organizing Feature Map and Genetic Algorithm）[J].Journal of Information Security，2019，10（1）：1-24.

[6] FALAYE A A，OLUYEMI E S，VICTOR A N，et al. Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network [J].International Journal of Mathematical Sciences and Computing，2017，3（4）：37-51.

[7] SGOURAS K I，KYRIAKIDIS A N，LABRIDIS D. Short-term risk assessment of botnet attacks on advanced metering infrastructure [J].IET Cyber-Physical Systems Theory & Applications，2017，2（3）：143-151.

[8] NGUYEN T A T，DANG T K. Privacy preserving biometric-based remote authentication with secure processing unit on untrusted server [J].IET Biometrics,2019，8（1）：79-91.

[9] 肖圣龙，陈昕，李卓 . 面向社会安全事件的分布式神经网络攻击行为分类方法 [J]. 计算机应用，2017，37（10）：2794-2798+2805.

[10] JYOTHIRMAI P，RAJ J S，SMYS S. Secured Self Organizing Network Architecture in Wireless Personal Networks [J]. Wireless Personal Communications，2017，96（4）：5603-5620.

[11] YAN Q，GONG Q，YU F R. Effective software-defined networking controller scheduling method to mitigate DDoS attacks [J]. Electronics Letters，2017，53（7）：469-471.

[12] RRUSHI J. NIC displays to thwart malware attacks mounted from within the OS [J].Computers & Security，2016，61：59-71.

[13] ZHAO Y H，HE X，ZHOU D H. Optimal joint control and triggering strategies against denial of service attacks a zero-sum game [J]. IET Control Theory and Applications，2017，11（14）：2352-2360.

[14] MOUSTAKAS K，DROSOU A，TZOVARAS D，et al. Border gateway protocol graph：detecting and visualising internet routing anomalies [J].IET Information Security，2016，10（3）：125-133.

[15] FALAYE A A，OLUYEMI E S，VICTOR A N，et al. Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network [J].International Journal of Mathematical Sciences and Computing，2017，3（4）：37-51.

作者简介：汤冠楚（1998—），男，汉族，江西萍乡人，本科，研究方向：计算机与网络攻击分类法。

（上接 161 页）管理体系的建议 [J]. 信息安全与通信保密，2021（1）：70-76.

[16] 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.

[17] 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.

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

[19] 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）：197.

[20] 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.

[21] 新文化网 . 学习《国家安全法》百问百答 [EB/OL].（2016-04-17）.https://www.sohu.com/a/69772023_160796.

[22] 百度百科 .ISO17799 [EB/OL].[2021-04-10]. https://baike.baidu.com/item/ISO17799/2894602?fr=aladdin.

[23] 岳浩 . 信息安全管理体系的建设 [C]// 上海空港（第 8 辑）. 上海：上海世纪出版股份有限公司科学技术出版社，2008：3.

[24] 孙强，郝晓玲 .IT 治理信息安全管理：标准、理解与实施（一）[EB/OL].（2004-11-19）.http://www.itgov.org.cn/Item/467.aspx.

[25] 百度文库 .isms 信息安全管理体系 [EB/OL].（2020-08-10）.https://wenku.baidu.com/view/f9cb43f0876fb84ae45c3b3567ec102de3bddff7.html.

[26] 顾力平，邹珊刚 . 信息安全风险管理的 EPDCA 模型 [J]. 工业工程与管理，2008（2）：14-18.

作者简介：惠建新（1978—），男，汉族，江苏盐城人，工程师，硕士，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，研究方向：安全信息系统设计与开发、安全网运维；娄洪伟（1982—），男，汉族，吉林长春人，高级工程师，硕士，研究方向：网络安全架构研究、安全网建设与维护。