DOI:10.19850/j.cnki.2096-4706.2021.16.037

科研院所安全信息系统节点风险评价研究

惠建新[1]，娄洪伟[2]，乔德志[3]

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

摘　要：风险对组织及其资产存在破坏的可能性，它是安全评估的重要因素之一。文章采用定性分析与定量分析相结合的方法进行风险评估，在确定评价对象的基础上，建立一种基于知识的定性分析法，提出风险等级设定和风险防范措施，实践运行证明，该评价体系具有安全性高、稳定性好、易操作、高可靠等优势，可极大提高风险评估效率。

关键词：节点风险；信息安全；系统网络测评

中图分类号：TP39　　**文献标识码：**A　　**文章编号：**2096-4706（2021）16-0153-05

Research on Node Risk Assessment of Security Information System in Scientific Research Institutes

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

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

Abstract: Risk has the possibility of damage to the organization and its assets, which is one of the important factors of safety assessment. In this paper, it is the combination use of qualitative analysis and quantitative analysis for risk assessment. On the basis of determining the evaluation object, a knowledge-based qualitative analysis method is established, and the risk level setting and risk prevention measures are put forward. The practical operation shows that the evaluation system has the advantages of high security, good stability, easy operation and high reliability, which can greatly improve the efficiency of risk assessment.

Keywords: node risk; information security; system network evaluation

0　引　言

经过多年的系统改造工作，大部分安全项目承研单位的安全信息系统都配置了必要的安全产品，建立了安全策略以及系统内相关的风险管制目标和针对每种节点风险评价所采取的各种控制措施。

然而，安全信息系统的节点风险评价缺失，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，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问题，而且评估结果太过依赖专家的主观性判断，对最终结果造成干扰。

安全网络的节点管理不等同于网络系统管理。应用安全网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，包括涉密网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及其他属性。业务对资产依赖度越高，资产的价值越高，其面临的风险系数越大，越应该加强相关保密工作。不完整识别资产与风险，不能形成完整的安全保密需求，不能全面确保涉密网络运行的效能。因此形成资产与风险识别的标准、方法及体系对于确定节点风险管理范围及进行安全节点网络的管理至关重要。

收稿日期：2021-07-04

基金项目：中国科学院十三五信息化专项项目（XXH13507-2）

1　安全信息系统节点风险评价价值

1.1　安全信息系统的节点风险评价的意义

风险评价的目的是通过一系列措施对系统进行检查、评价，及时发现系统运行过程中存在的风险，并对风险等级、重要程度进行评价，指导系统运维人员解决系统中存在的问题、完善系统安全防护措施。应当每年由信息化管理部门和运维部门共同进行系统风险评价。

1.2　安全信息系统节点风险审计作用

系统安全审计是发现系统问题、降低系统风险的重要手段，单位如果没有建立完善的系统安全审计机制，将导致无法及时发现系统运行过程中存在的问题、用户违规行为等。单位应当建立完善的系统安全审计机制，安全审计员组织定期对信息系统的各种日志进行分析、对用户使用情况进行检查，掌握系统运行情况，不断完善信息系统安全防护措施、降低系统风险。

1.3　系统数据备份与恢复的管理

数据备份机制是保证信息系统正常运行、故障恢复的重

要手段，单位如果没有建立完善的备份恢复机制，在遇到系统故障时系统应用、安全防护措施将遭受彻底性破坏，并且无法修复。数据恢复过程要严格管理，必须严格履行审批，由系统管理员和安全管理员共同操作，对系统进行调研、分析，在保障系统安全的前提下进行数据恢复工作。

建立系统备份和恢复的制度及操作规程，并制定详细的数据恢复步骤和方法，使用模拟环境进行测试，验证备份操作过程的可靠性。单位还应定期对重要系统进行恢复演练，用来判断数据备份、恢复过程是否可靠。系统管理员和安全安全员严格按照备份和恢复管理规定执行，尤其是数据恢复操作过程的测试和演练，如果忽视这部分工作，即便是做了很详细周密的备份计划、恢复方法，因为方案没有得到演练、验证，遇到系统故障时往往无法顺利地完成恢复工作，对信息系统的正常运行、数据安全造成巨大损失。

1.4 节点风险防病毒系统和系统补丁的管理

防病毒系统是信息系统重要的安全保障，如果缺乏病毒防护，系统中数据和业务将遭受严重破坏。单位应制定防病毒系统策略，运维人员按照要求部署防病毒系统，并定期升级防病毒系统病毒库文件。信息系统服务器、终端计算机、网络设备如存在重大安全隐患，容易被终端用户或者恶意程序利用，从而破坏系统服务、安全系统，严重影响系统的正常运行。单位应当制定系统补丁管理策略，在新增服务器、终端计算机时统一安装系统补丁，定期对系统重要资源进行安全扫描，及时发现系统安全漏洞，并及时下载补丁文件进行修复。

依据“规范定密、准确定级；依据标准，同步建设；突出重点，确保核心；明确责任，加强监督”的指导思想，从物理安全、运行安全、信息安全风险、安全风险管理、产品选型与安全服务等方面对科研院所安全网进行安全风险防护设计。系统安全风险防护框架图如图 1 所示。

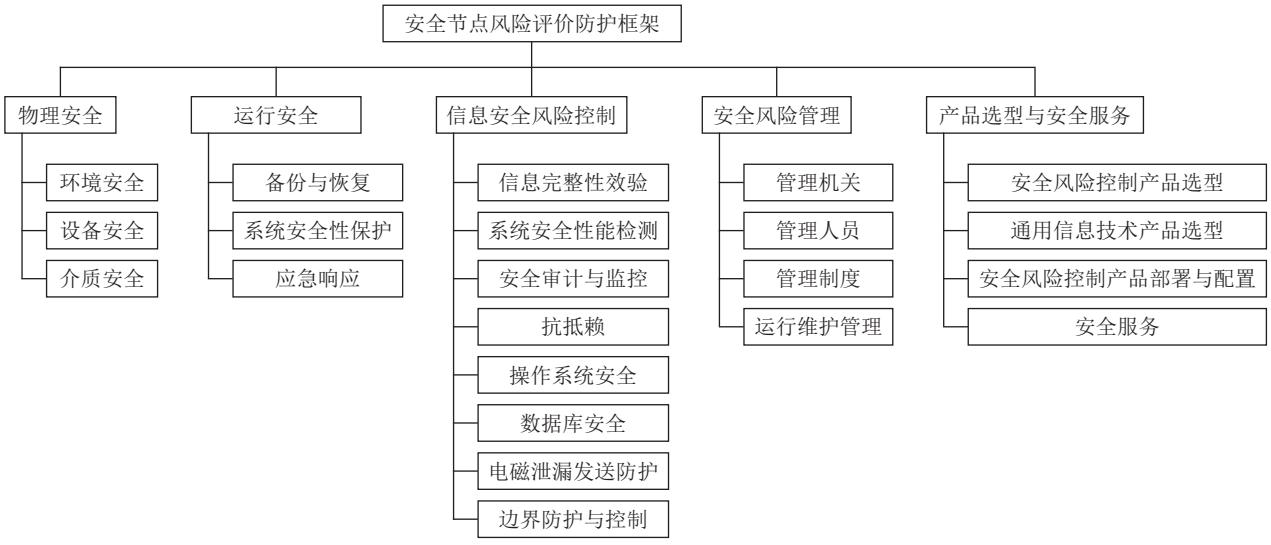

图 1 安全节点风险评价防护框架

2 安全信息系统节点评价对象及风险分析

2.1 安全信息系统节点风险评价对象

安全信息系统网络划分为安全管理域、应用服务器安全域和用户终端安全域。硬件方面包括：各域之间用防火墙等设备隔离开来；交换机上做 IP 地址和 MAC 地址的绑定；所有不使用端口逻辑关闭，物理断开；主交换部署 IDS 系统，及时发现网络中的攻击行为；部署漏洞扫描系统，定期扫描网络设备的漏洞；应用安全域使用证书来确定用户身份，保证用户对应用访问的身份认证、访问控制和安全审计，同办公和文档相关的数据和信息处理集中在服务器，用户终端无信息使用痕迹；与程序开发和仿真业务相关的仍保留原有的分布式方式。软件方面包括：用户终端安装登录管理软件，以 USB KEY 方式进行登录；用户终端安装安全管理软件，对 USB 口、COM 口、串口等进行管理；用户终端安装证书读取等基础模块，可以访问应用服务器的各种资源。

评价涉及的风险点有：物理安全风险、运行安全风险、信息安全保密风险、管理风险、物理与设施管理风险。用户认证包括终端用户身份认证和应用层用户身份认证，两者都统一使用基于 USB KEY 和口令的双因子身份认证，保证用户一 KEY 登录所有应用。

访问控制措施：主要通过防火墙的包过滤加上应用层的身份认证来进行，保证只有授权的用户才能访问相应的服务器及应用，未授权用户不能看到服务器及上面的应用。对于不同等级的安全域间的通信，应实施有效的访问控制策略和机制，禁止高密级信息由高等级安全域流向低等级安全域。根据终端和服务器功能用途的不同，将全网划分为三个安全域，安全域划分情况如图 2 所示。

2.2 安全信息系统节点风险现状调查

信息系统风险是指：人为或自然的威胁与攻击，直接或间接地利用系统存在的脆弱性和漏洞所造成的不确定性事件及其后果。实现对信息系统风险进行有效管理，将信息系统风险控制在可接受范围内，科学分析和评估信息系统的风险分布和风险强度很有必要。通过对科研院所安全网的技术和管理脆弱性分析、对威胁源和攻击类型的判别，以及定性的风险分析，可以确定科研院所安全网存在的安全风险、严重程度和影响范围，风险分析过程如图 3 所示。

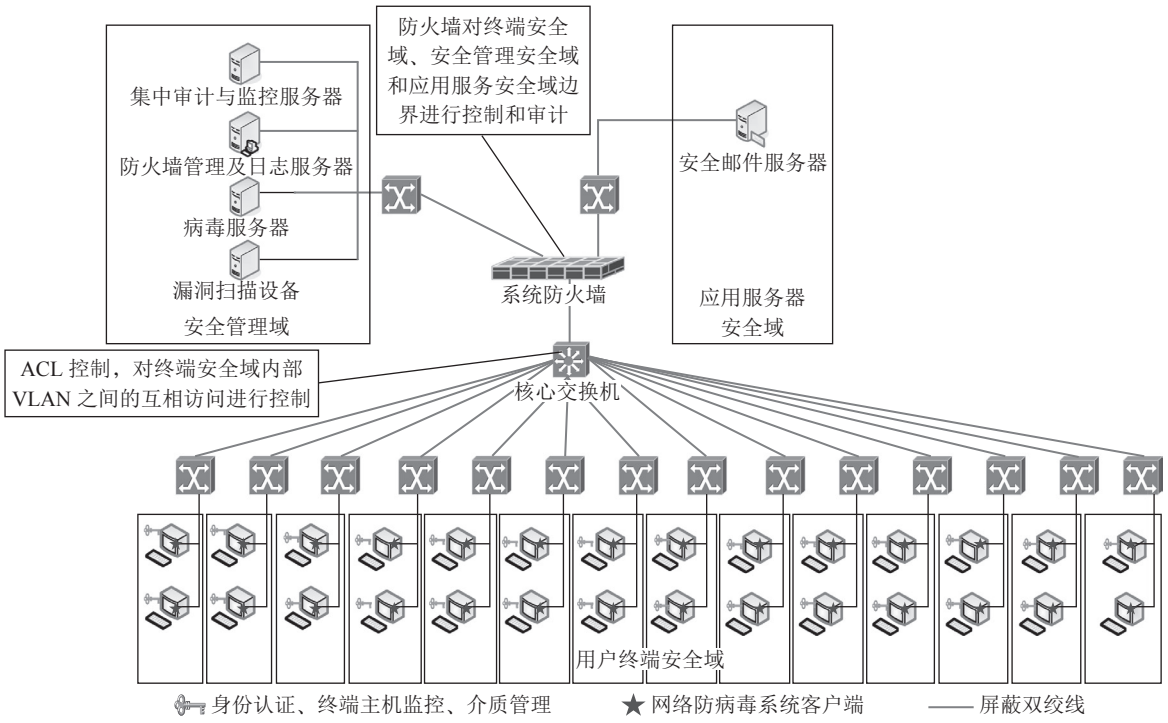

图 2　安全信息系统网络拓扑示意图

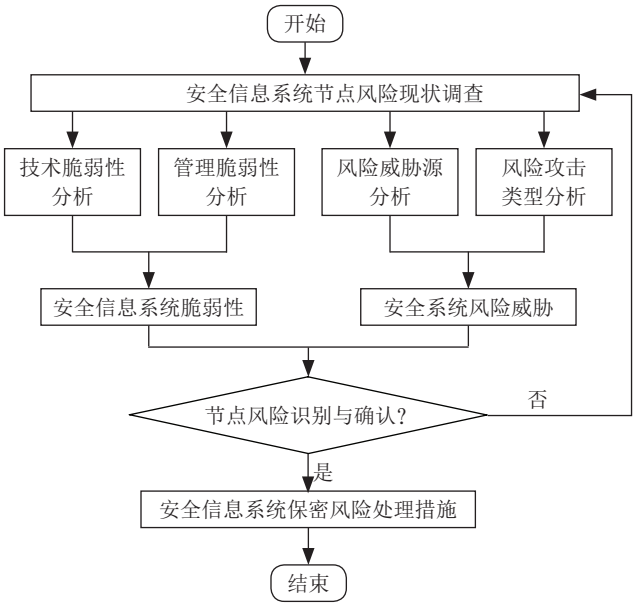

图 3　风险分析过程示意图

通过一个完整的风险分析过程，可以全面掌握科研院所安全网中的信息安全处理措施（包括技术措施与相应的管理措施），可以对系统的风险状态有一个相对客观的了解。风险状态信息的获取可以通过技术调查、访谈以及获取操作记录与日志等方式进行，力求客观。风险的状态信息可以为科研院所安全网的安全风险建设方案的制定提供有力支持。

2.3　安全信息系统节点风险脆弱性分析

脆弱性分析是在对安全网络基础设施建设完成后未做安全风险建设前的脆弱性分析。针对科研院所安全网内不同类型的安全信息资产（各类信息资源、应用系统、软硬件资源、网络平台等）和安全风险管理制度进行分类脆弱性分析，并结合人员访谈和安全检查进行脆弱性识别。根据脆弱性对资产的暴露程度、技术实现的难易程度、流行程度等，采用等级方式对已识别的脆弱性的严重程度进行赋值。同时，根据脆弱性被威胁利用可能性大小、造成影响的程度，采用定性的分析方法，将脆弱性安全等级从低到高划分五个等级。脆弱性分析主要分析技术脆弱性和管理脆弱性，如表 1 所示。

表 1　弱性等级表

等级值	脆弱性等级	等级描述
5	很高	如果被威胁利用，将对安全信息资产造成完全损害及特别重大影响
4	高	如果被威胁利用，将对安全信息资产造成重大损害及影响
3	中等	如果被威胁利用，将对安全信息资产造成一般损害及影响
2	低	如果被威胁利用，将对安全信息资产造成较小损害及影响
1	很低	如果被威胁利用，对安全信息资产造成的损害及影响极低或可以忽略

2.4　安全信息系统节点风险安全审计

2.4.1　安全审计需求分析

根据对系统脆弱点的分析、系统运行性能和安全需求确定系统安全审计的范围，为安全事件的事后追查提供足够信息。

安全信息系统安全审计标准由网络审计标准、数据库审计标准、主机监控审计标准和应用审计标准等组成。

2.4.2 审计范围

安全信息系统安全审计的范围包括：对服务器操作系统、启明星辰防火墙、“三合一”系统、榕基漏扫系统、北信源主机监控与审计系统、瑞星网络版防病毒软件、涉密邮件系统七个安全产品产生的审计日志进行查看，每月形成安全审计报告。

2.4.3 审计事件

安全信息系统审计事件主要包括：服务器、涉密终端和安全保密产品的启动与关闭；审计功能的启动和关闭；系统内用户增加、删除；用户权限的更改；系统管理员、安全保密管理员和安全审计员所实施的操作；用户的违规操作等。

2.4.4 网络审计

重点对以下类型的网络行为进行审计：

（1）文件传输类行为审计：FTP 上传与下载、FTP 命令交互。

（2）终端类行为审计：远程桌面 RDP、TELNET、SSH 等尝试连接事件。

2.4.5 主机监控审计

对安全信息系统计算机终端上的以下操作进行设置、监控和审计：

（1）软件安装监控：明确在计算机终端上允许安装、必须安装和禁止安装的软件，对违规安装 / 卸载软件的行为进行“提示”处理。

（2）进程执行监控：明确在计算机终端上禁止运行的服务，对违规启动服务的行为进行上报处理，并自动关闭相关服务。

（3）进程保护标准：在计算机终端上保护相关的重要进程（如瑞星、安全登录与文件保护系统的关键进程）。

3 安全信息系统节点风险评价研究

3.1 安全信息系统节点风险计算方法

根据科研院所安全网的特点，整个风险分析过程采用基线评估方法，科研院所的安全网的安全风险由安全事件造成的损失（安全事件造成的损失 =F（资产价值，脆弱性严重程度））和安全事件的可能性（安全事件的可能性 =L（威胁出现频率，脆弱性））共同确定的，即：安全风险值 =R（安全事件的可能性，安全事件造成的损失）。由于涉密信息系统中内的涉密资产都具有高等级保护价值，一旦发生安全事件，都会产生一定的影响。因此，安全信息系统的风险以涉密资产的脆弱性和威胁（发生可能性和影响程度）为分析基础，将涉密事件造成的损失作最大化处理，安全风险值近似等于安全事件的可能性。

通过风险分析矩阵，节点风险值 = 节点资产重要性程度值 × 威胁风险系数；确定科研院所安全网的风险等级，如表 2 所示。

为实现对风险的控制与管理，对风险评估的结果进行等级化处理，根据风险对系统所造成的危害程度，我们将风险定性分析，如表 3 所示，划分为 5 个不同的等级。

表 2 风险计算矩阵

威胁发生	脆弱性严重程度				
	1	2	3	4	5
1	2	4	7	11	14
2	3	6	10	13	17
3	5	9	12	16	20
4	7	11	14	18	22
5	8	12	17	20	25

表 3 风险等级划分

风险值	1 ～ 5	6 ～ 11	12 ～ 16	17 ～ 21	22 ～ 25
风险等级值	1	2	3	4	5

参照 BMB22-2007 标准要求，对不符合 15 项基本测评项必须整改的风险类别直接沿用较高等级，如表 4 风险等级描述。

表 4 风险等级描述

等级值	风险等级	风险级别定义
1	极小	风险发生导致系统受到极小影响，信息泄密的可能性极小
2	较小	风险发生导致系统受到较小影响，信息泄密的可能性较小
3	中等	风险发生导致系统受到中等影响，信息泄密的可能性较大
4	较大	风险发生导致系统受到较大影响，信息泄密的可能性较强
5	极大	风险发生导致系统受到极大影响，信息泄密的可能性极大

根据以上对科研院所安全网的脆弱性分析与威胁分析，再根据国家的相关规定，确定安全网的风险及风险等级。

3.2 安全信息节点风险的判定

节点运维管理风险评价的原则：“防控风险：管理和技术同等重要”。通过对基本制度、组织机构及岗位设置、运维工作机构、责任分工、责任履职、运维工具、设备管理、风险监测、经费与档案管理 10 个方面进行监督检查和风险评价，风险赋值不是风险评价的最终目的，其核心是明确不同威胁，及安全资产所产生风险的相对值，以百分制的定量表示，提出四个风险等级和防范措施。评价等级界定为：

（1）得分在 80 分以上的为绿色，相对安全，风险度低。

（2）得分在 60 分至 80 分的为黄色，有风险，加强安全。

（3）得分在 59 分以下的为红色，风险度高，要求整改。

（4）得分在 40 分以下的和发生泄密事故事件的，停止

使用节点，整改后达到黄色的，方可开始节点使用。

3.3 残留风险点与风险规避措施

科研院所安全网的安全风险建设是不断完善、不断增强的过程，建设完成后，还可能存在以下安全风险：

（1）系统中计算机终端的机箱没有采取上锁等措施，存在用户私自更换计算机终端中的硬盘导致信息泄漏的风险。

残余风险处理策略：该风险目前可以接受。通过对所有计算机终端贴易碎封条并加强监督检查，防止用户私自打开机箱。

（2）没有采用安全操作系统和安全数据库。

残余风险处理策略：该风险目前可以接受。科研院所已经及时对安全终端和服务器的操作系统进行了加固，同时采用了补丁、安全策略配置和服务优化来进行操作系统和数据库的安全增强。

（3）操作系统、数据库补丁和防病毒软件升级包分发到各终端和服务器时间滞后，存在系统内设备受到“O Day”攻击的风险。

残余风险处理策略：该风险目前可以接受，主要基于以下考虑：

1）从系统漏洞被发现到厂商提供针对性补丁必然存在时间差，从新型病毒出现和采取针对性查杀措施必然存在时间差，“0 Day”攻击在整个信息安全界都是不可避免的。

2）科研院所安全网通过严格控制信息输入和软件安装使用控制，防止有害程序和信息进入网内，可以降低未知病毒和恶意代码对系统的威胁。

3）科研院所安全网建立了统一的系统补丁和升级包分发机制，每周（突发事件紧急处理）下载最新的补丁和升级包到补丁分发服务器，通过管理服务器检查未安装补丁和升级包的终端和服务器后，通过人工通知方式要求安装。

4 结 论

综上所述，信息系统节点安全有着重要意义，为加强风险管理，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，通过项目建设研究，给出具体的解决措施，每个研究所应根据其集团总部的要求围绕自身进行全面、系统、整体分析考核，修订制度标准，在把握好法律规定的前提之下，着重要解决业务工作与风险工作的深度融合问题。

此外，进一步明晰安全信息系统节点风险责任体系，落实“业务工作谁主管、风险工作谁负责”的工作原则，充分明确各业务职能部门在风险管理体系中的管理职责，通过提前策划、充分辨识、查找风险管理风险点，消除风险管理盲区，将风险管理要求植入相应的科研生产和经营管理流程及环节中，在业务流程之中自动并行完成，既确保国家秘密安全，又精简烦琐、提高效率，彰显出管理效益。

参考文献：

[1] 刘玉林，王建新，谢永志．涉密信息系统风险评估与安全测评实施 [J]. 信息安全与通信风险，2007（1）：142−144.

[2] 李舸．信息安全风险评估的漏洞分析及评估方法改进 [D]. 重庆：重庆大学，2007.

[3] 陈曦．网络安全监察系统中风险评估方法的研究 [D]. 北京：北方工业大学，2008.

[4] 鲁娟．给水管网脆弱性评估研究 [D]. 合肥：合肥工业大学，2007.

[5] 肖薇薇．企业内网网络安全体系的设计与实现 [D]. 大连：大连海事大学，2011.

[6] 沈鸣．企业网络安全风险评估研究 [D]. 上海：上海交通大学，2009.

[7] 杨洋，姚淑珍．一种基于威胁分析的信息安全风险评估方法 [J]. 计算机工程与应用，2009，45（3）：94−96+100.

[8] 范红，吴亚非．国家信息安全风险评估标准化工作的几点思考 [C]// 中国信息协会信息安全专业委员会年会．中国信息协会信息安全专业委员会年会文集．张家界：出版社不详，2004：187−195.

[9] 何湘．基于 BS7799 标准的信息安全风险评估研究与实践 [D]. 重庆：重庆大学，2008.

[10] 吴兰．信息系统安全风险评估方法和技术研究 [D]. 无锡：江南大学，2007.

[11] 王丽平．政府接入网安全体系设计与实现 [D]. 长春：长春理工大学，2006.

[12] 周师熊，周亦群．信息网络安全技术讲座（1） [J]. 中国数据通信，2001（6）：55−60.

[13] 柯敏毅，肖俊林．网络安全评估的量化研究 [J]. 网络安全技术与应用，2006（9）：18−20.

[14] 张雷．军工企业涉密信息系统安全管理技术研究 [J]. 决策与信息（中旬刊），2013（5）：83−86.

[15] 顾华杰．信息系统风险评估方法综述 [J]. 无线互联科技，2014（9）：84−85+182.

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