文章编号:1000-582X(2012)06-147-08

RS-UM 信息系统安全保障评估模型

张雪芹[1,2],江常青[3],徐萃华[1],林家骏[1]

(1.华东理工大学 信息科学与工程学院,上海 200237;2.杭州师范大学 杭州市电子商务与信息安全重点实验室,浙江 杭州 310036;3.中国信息安全测评中心,北京 100089)

摘 要:以 GB/T20274 信息系统安全保障评估框架为基础,介绍了信息系统安全保障模型及其评估指标体系,给出了评估方法的形式化描述和评估流程,提出了一种基于粗糙集(rough set,RS)和未确知测度(unascertained measure,UM)理论的信息安全评估模型。在标准处理阶段,模型采用粗糙集理论获取关键指标,简化评估指标体系;在综合评估阶段,采用未确知测度模型分析客观数据,实现了对信息系统安全保障能力的定量化综合评价。

关键词:安全测评;信息系统安全保障评估模型;粗糙集;未确知测度

中图分类号:TP393.08 **文献标志码**:A

RS-UM based information system security assurance evaluation model

ZHANG Xue-qin [1,2], *JIANG Chang-qin*[3], *XU Cui-hua*[1], *LIN Jia-jun* [1]

(1. East China University of Science and Technology, Shanghai 200237, P. R. China; 2. Key Laboratory of E-Business and Information Security, Hangzhou Normal University, Hangzhou 310036, Zhejiang, P. R. China; 3. China Information Technology Security Evaluation Center, Beijing 10089, P. R. China)

Abstract: Based on the information system security assurance evaluation framework (GB/T20274), the information system security assurance model and evaluation index system are introduced, and the formalization evaluation method and flow are presented. An information security evaluation model is proposed by applying rough set (RS) and unascertained measure (UM) theory. At the criterion pre-process period, rough set theory is used to obtain the key evaluation indexes and construct the reduced index set to simplify the original complex index system. At the evaluation period, unascertained measure model is adopted to analyze the evaluation data to implement a quantitative integration evaluation on the information system security assurance ability.

Key words: security evaluation; information system security assurance evaluation model; rough set; unascertained measure

对信息系统的安全性进行先期评估是防范各种信息系统安全问题的一种有效手段。2006 年,中国信息安全测评中心发布了《GB/T 20274 信息系统安全保障评估框架》草案。该评估框架从管理、技术和管理角度出发,对信息系统整个生命周期内的系统保密性、完整性和可用性进行评估,考察各种技术、

收稿日期:2011-12-25

基金项目:国家自然科学基金资助项目(60773094);杭州电子商务与信息安全重点实验室开放基金资助项目(HZEB201009)

作者简介:张雪芹(1972-),女,华东理工大学博士,副教授,主要从事网络安全、安全测评、模式识别方向研究,(Tel)021-64252530;(E-mail)zxq@ecust.edu.cn。

管理、工程措施的实施能力，有利于建立有效的信息系统安全保障体系，将系统风险控制到最小[1-2]。在评估中通常会面临2个问题：第一，由于安全评估指标涉及数量庞大，实际评估中往往难以逐条实施。同时庞大的指标体系在使用中产生的积累误差容易造成总体安全测量的偏差。因此如何优化约简评估指标，降低评估模型维数，简化评估过程，降低评估成本是一个值得研究的问题。第二，由于信息系统是一个受诸多不确定性因素影响的复杂系统，在对信息系统安全要素的描述中往往大量采用自然语言，传统的基于概率论和数理统计理论的评估模型难以适用，这使得评估实际上成为一种对定性描述的度量问题。

在经典集合论和模糊集合论，指标重要度的度量一般是通过经验赋予各个指标一个“加权系数”来进行刻画。但为了确定该“加权系数”往往需要大量的先验信息。粗糙集理论是由波兰学者Z. Pawlak在1982年提出的一种处理不确定和不精确性问题的新的数学工具[3-5]。该理论无需提供问题处理所需的数据集合之外的任何先验信息，如概率分布、隶属度等，就能在有效地度量指标重要性，在保留关键信息的前提下获取约简属性集。目前，已在模式识别、数据挖掘、机器学习等领域得到了成功的应用[6-8]。常用的信息系统风险定量评估方法有层次分析法和模糊评判法。但是层次分析法评价模型中评价因子一般采用主观方法确定，评判矩阵受评判标准支配，评估结果的正确度取决与评判标准的客观程度。而模糊评判法中模糊合成运算存在信息丢失，模糊集量化具有主观性，其“取大取小”原则也存在有一定的不足[9-11]。基于未确知集合的未确知系统理论与方法是1990年王光远院士基于拓扑空间概念的提出一种处理不确定性信息的数学工具，它具有严谨的推理逻辑，在推理时不造成新的信息损失。已在煤矿安全评价、软件可靠性评价等定量综合评估领域得到有效应用[12-14]。

1 信息系统安全保障模型和评估框架

1.1 模型简介

GB/T20274信息系统安全管理保障评估框架给出了信息系统安全保障模型[2]。标准指出，信息系统安全保障指在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。信息系统安全保障是一种多维的立体的保障体系，它从从信息系统安全保障的目标、时间、空间和能力4个维度建立和规范了信息系统的综合保障，如图1所示。

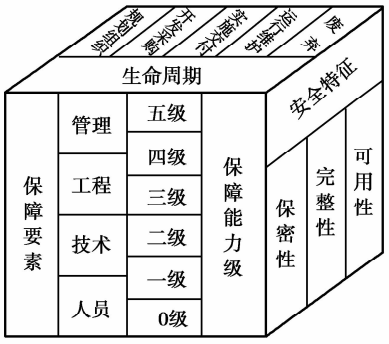

图1 基于CMM的信息系统安全保障模型

1)安全保障目标维。信息系统保障的基本目标就是保证其所创建、传输、存储和处理的信息的保密性、完整性和可用性特征。不仅是保护信息和资产的安全，更重要是通过保障信息系统安全保障信息系统所支持的业务的安全，从而达到实现组织机构使命的目的；

2)安全保障时间维。信息系统安全保障应贯穿信息系统的整个生命周期，包括规划组织、开发采购、实施交付、运行维护和废弃五个阶段，以获得信息系统安全保障能力的持续性；信息系统的保障是动态的，在系统生命周期的某一时间的保障与过去相关，并影响未来的保障。

3)安全保障空间（对象）维。信息系统安全保障需要从技术、工程、管理和人员4个领域进行综合保障。即，由合格的信息安全专业人员，使用合格的信息安全技术和产品，通过规范、可持续性改进的工程过程能力和管理能力进行建设和运行维护，达到安全保障的信息系统。

4)安全保障能力维：信息系统安全保障能力由技术保障能力，管理保障能力，工程保障能力构成。为了有效度量组织机构信息系统安全保障水平的能力，信息系统安全保障模型将能力成熟度模型(capability maturity model，CMM)与信息安全保障相结合，采用能力成熟度分级模型作为度量尺度，直接反映安全保障水平的成熟程度。信息系统安全保障能力级别按成熟性排序，分为6个级别。

能力级别 0:未实施;

能力级别 1:基本执行;

能力级别 2:计划跟踪;

能力级别 3:充分定义;

能力级别 4:量化控制;

能力级别 5:持续改进

从能力级别 0 到能力级别 5 表示依次增加的保障能力,其中有效级别为 5 级,能力级别 0 通常不使用。

1.2　信息系统安全保障评估指标体系和评估流程

1)评估指标体系

根据信息系统安全保障模型,信息系统安全保障控制要求(控制域)包括安全技术保障控制要求、安全管理保障控制要求和安全工程保障控制要求。针对每一控制域,其指标体系使用控制类—控制子类—控制组件的层次化的组织结构,如图 2 所示。其中,第一级安全要素为控制类,控制类是最通用的一组安全保障控制要求的组合。类的所有的成员关注同一个安全问题,区别在于覆盖不同的安全保障目的。第二级安全要素为控制子类。类的成员称为子类。控制子类是若干组安全保障控制要求的组合,要求针对同一个安全保障目的,但在强度和程度上有所区别。第三级安全要素是控制组件。控制组件是实现其安全保障控制子类的安全保障控制目的的信息安全保障具体控制措施。

根据 GB/T20274 标准,信息系统安全管理保障要求评估指标涉及 12 个控制类,38 个子类,109 个组件;工程保障要求评估指标涉及 3 个控制类,15 个子类,74 个组件;技术保障要求评估指标涉及 11 个控制类,66 个子类,135 个组件[2]。

2)评估方法

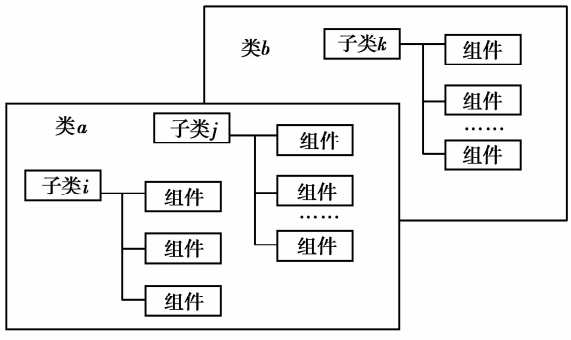

图 2　安全保障评估指标体系结构示例

从 1)的介绍可以看出,信息系统安全保障评估指标体系呈现树状层次结构。设信息系统 S,其安全保障控制域包括管理要求、技术要求和工程要求 3 个方面,记为:$S=\{s^1,s^2,s^3\}$。属于控制域 s^p($p\in[1,3]$)的控制类集合记为 $e^p=\{e_1^p,e_2^p,\cdots,e_k^p\}$,$k$ 为控制域 s^p 中包含的控制类个数。属于类 e_i^p($i\in[1,k]$)的控制子类集合记为:$e_i^p=\{e_{i1}^p,e_{i2}^p,\cdots,e_{im}^p\}$,$m$ 为类 e_i^p 中包含的控制子类个数。属于子类 e_{ij}^p($i\in[1,k]$,$j\in[1,n]$)的控制组件的集合记为 $e_{ij}^p=\{e_{ij1}^p,e_{ij2}^p,\cdots,e_{ijn}^p\}$,$n$ 为控制子类 e_{ij}^p 中包含的控制组件个数。各指标采用能力成熟度级度量,度量尺度的集合定义为:$D=\{d_0,d_1,\cdots,d_5\}$(实际采用$\{d_1,\cdots,d_5\}$),$d_0,d_1,\cdots,d_5$ 之间存在一个偏序关系"$\leqslant$"。在评估中,每个安全要素到度量尺度集合上都有一个映射 f,这个映射可由对此安全要素的下一级元素的综合评估得到。如:控制子类 e_{ij}^p 的能力成熟度级为:$f_{e_{ij}^p}(d(e_{ij1}^p),d(e_{ij2}^p),\cdots,d(e_{ijn}^p))$,$n$ 为子类 e_{ij}^p 中包含的控制组件个数;控制类 e_i^p 能力成熟度级:$f_{e_i^p}(d(e_{i1}^p),d(e_{i2}^p),\cdots,d(e_{im}^p))$,$m$ 为类 e_i^p 中包含的控制子类的个数;控制域 s^p 安全保障能力成熟度级为:$f_{s^p}(d(e^1),d(e^2),d(e^3))$,$p$ 为信息系统 S 中包含的控制域的个数,$p=3$;则,整个信息系统 S 安全保障能力成熟度级为:$f_s(d(s^1),d(s^2),d(s^3))$。

通过对上述各级指标的分层和综合评估,可以最终得到信息系统安全保障能力成熟度级。信息系统安全保障能力越高,则系统风险越低。

3)评估流程

针对上述评估模型和评估指标体系,基于信息系统安全管理保障框架的评估流程如图 3 所示。

1)用户信息描述:评估方就评估对象相关材料进行审阅,制定评估方案和评估计划等。

2)标准处理:选定评估标准,挑选相应评估指标;

3)数据输入:根据评估标准和评估指标,设计调查问卷和各类检测表单,实施问卷调查和各种基于技术工具的检测。

4)综合测评分析引擎:根据获得的数据,对评估对象进行综合评估,最终生成测试评估报告。

2　基于粗糙集的评价指标选取

从前面的叙述可以看出,整个信息系统安全保障评价指标体系非常复杂,实际评估中,如果参照标准逐一实施,即没有必要也难以实施。事实上,针对不同的行业和业务系统,由于其安全侧重点不同,并

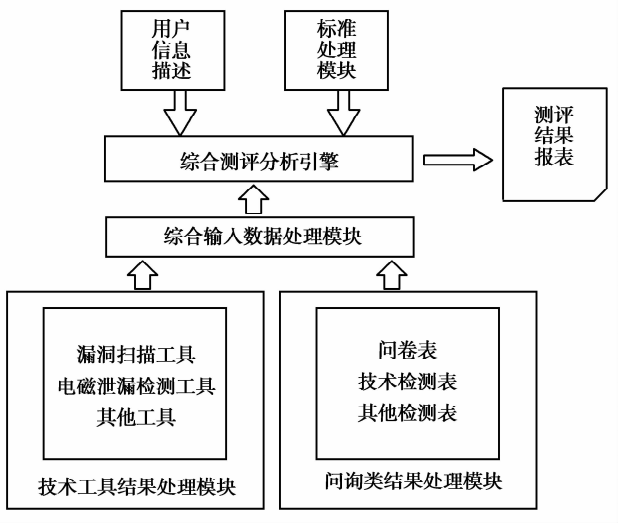

图3 评估流程

不需要使用全部指标。因此应在标准处理阶段对评估指标进行处理,选取关键指标进行评估。

2.1 粗糙集相关理论

1)信息系统(决策表)

在粗糙集理论中,现实世界的信息系统可用一张信息表表示,称为决策表。

定义1(决策表):设 $S=\{U,A,V,f\}$ 为一个信息系统,其中,$U=\{U_1,U_2,\cdots,U_m\}$ 为有限非空集合,称为论域对象空间;$A=\{a_1,a_2,\cdots,a_A\}$ 为属性的非空有限集合。A 中的属性又可分为2个不相交的子集,即条件属性集 C 和决策属性集 D,即:$A=C\cup D$, $C\cap D\neq\phi$。V 是 Q 中属性值的集合,$V=\cup V_a$,其中 $a\in A$,V_a 为属性 a 的值域;$f:U\times A\rightarrow V$ 为信息函数,对于 $a\in A$,$x\in U$, $f(x,a)\in V_a$,它指定 U 中每一对象的属性值。

2)等价关系

粗糙集理论将分类与知识联系在一起,并用等价关系 R 表示分类。

定义2(等价关系):令 $a\in A$,$x\in U$, $f(x,a)\in V_a$,对于任一子集在 U 上的等价关系 R 定义为 $R=\{(x,y)\in U\times U:f(x,q)=f(y,q),q\in A\}$。若 $(x,y)\in R$,则称 x 和 y 是等价的。等价关系记为 IND(R),也常简记为 R。

若 R 是 U 上的一个等价关系,则 $U/R=U/\mathrm{IND}(R)=\{X_1,X_2,\cdots,X_n\}$ 表示 R 产生的分类,称为 U 的一个知识。

3)属性约简和核

属性约简指不含多余属性并保证分类质量与原属性集的分类质量相同的最小条件属性子集。通过对信息系统的属性约简,可以获得比原信息系统更直观的知识,分类的效果。

定义3(属性约简)设论域为 U,R 为一等价关系族,$r\in R$,若 $U/\mathrm{IND}(R)=U/\mathrm{IND}(R-r)$,则称 r 在 R 中是可约去的。否则称 r 在 R 中是不可约去的。若 $P=R-\{r\}$ 中的任何元素都是不可约去的,则称 P 为 R 的一个约简。

定义4(核)R 的所有约简的交集称为 R 的核,记为 $\mathrm{Core}(R)$,即 $\mathrm{Core}(R)=\cap\mathrm{Red}(R)$。

4)差别矩阵

差别矩阵法是波兰华沙大学科学家 A. Skowron 在1991年提出的,利用这个工具可以将复杂信息系统中的全部不可分辨关系(等价关系)表达出来,是求取核属性和属性约简的有用工具。

定义5(差别矩阵)设信息系统 $S=\{U,A,V,f\}$,则用 $\boldsymbol{M}(S)$ 表示 $n\times n$ 阶的矩阵 (c_{ij}),$c_{ij}=\{a\mid(a\in A)\wedge a(u_i)\neq a(u_j)\quad,\forall u_i,u_j\in U\quad,\forall i,j=1,2,\cdots,n\}$,该矩阵称为 S 的差别矩阵。

定理1 $\mathrm{Core}(C)=\{a\mid(a\in C)\wedge(\exists c_{ij}((c_{ij}\in\boldsymbol{M}_{n\times n})\wedge(c_{ij}=\{a\})))\}$,即信息系统的核等于该信息系统的差别矩阵中所有简单属性(单个属性)元素组成的集合。

2.2 基于粗糙集的信息系统安全保障评估指标约简

1)混合启发式约简算法

在一个信息系统中的所有属性(评价指标)对于决策(评估)来说并不是同等重要的,属性的重要性度量了属性对信息系统的分类能力。在保持知识库分类能力不变的条件下,删除其中不相关或不重要的冗余知识称为知识约简。知识约简是粗糙集理论中的核心内容之一[15-16]。但是 Wong S. K. M. 和 Ziarko 在1985年已经证明找出一个信息系统或决策表的最小约简是 NP-hard 问题,因此采用的启发式约简算法来简化计算复杂度。其基本思想是:由信息系统或决策表的核为起始点,根据属性重要性的某种测度,不断选择最重要的属性加入约简集中,直到获的到信息系统或决策表的一个最优或次优属性约简集。

启发式一:依据可辨识矩阵的定义可知,当某个属性在可辨识矩阵中出现的频率越高,该属性可区分的对象数就越多,进而表明它的重要性就越大。因此,采用属性在可辨识矩阵中的出现频率作为启

发条件，来对决策表进行约简。

启发式二：通常，在以属性重要度为启发因子的属性约简迭代计算过程中，当属性重要度相同时，采用任意选取一个属性加入约简集。但是，很明显，这会增加约简集输出的不确定性。通过结合专家经验权重或历史权重（通过对历史数据的计算获取），当某几个属性在可辨识矩阵中出现的频率相同时，选择权重较大的加入属性加入约简集将更为加合理。

基于差别矩阵和属性重要性的混合式启发属性约简算法描述如下

输入：信息系统 S={U,A,V,f}。

输出：核集 C^*、属性约简集 Red(C)。

算法步骤如下

1）令约简集 Red(C)=ϕ，计算信息系统 S 的差别矩阵 $\boldsymbol{M}(S)$，计算核属性集 Core(C)，令 Red(C)=Core(C)；

2）$\forall c_{ij}(i,j=1,\cdots,n)$，如果 $c_{ij} \cap \mathrm{Red}(C) \neq \phi$，则令 $c_{ij}=0$；

3）$\forall c_{ij}(i,j=1,\cdots,n)$，如果所有 $c_{ij}=0$，转 5）；否则转 4）；

4）统计差别矩阵中 $\boldsymbol{M}(S)$ 中每个条件属性出现的频率，选取出现次数最多的作为 a^*。如果存在多个条件属性出现频率相同，则选取权重最大的一个作为 a^*。

$\mathrm{Red}(C)=\mathrm{Red}(C)\bigcup\{a^*\}$，转至 2）；

5）输出 Red(C)，得到一个约简。

利用混合式启发式算法能够提高约简的求解速度，在解空间不复杂的情况下，通常可以求得到唯一的最优解或次优解。

3　示例分析

根据粗集理论，设论域（对象的集合）$U=\{u_1,u_2,\cdots,u_m\}$ 为 m 个同类被评估系统。其管理保障控制域的控制类构成指标集合 $C=\{c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10},c_{11},c_{12}\}$。决策属性集 $D=\{\mathrm{MCML}_1,\mathrm{MCML}_2,\mathrm{MCML}_3,\mathrm{MCML}_4,\mathrm{MCML}_5\}$，MCML 指管理保障能力成熟度级，简记为 $D=\{d_1,d_2,d_3,d_4,d_5\}$，取值对应为{1,2,3,4,5}。

设有决策表如表 1 所示。

表 1　信息系统决策表

参数	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	d
u_1	3	3	3	3	2	2	2	3	3	3	2	2	3
u_2	3	3	3	3	3	1	3	2	4	3	3	2	2
u_3	4	3	3	2	3	2	2	4	4	3	2	2	4
u_4	2	2	2	3	2	2	2	3	3	3	2	2	2
u_5	3	2	3	3	3	2	3	3	3	2	3	3	3
u_6	1	2	3	2	2	1	3	3	3	3	2	3	1
u_7	2	2	3	2	2	1	2	2	3	2	3	2	2
u_8	3	3	4	4	3	1	3	4	3	3	3	1	3
u_9	3	3	3	3	3	2	3	3	4	3	2	3	3
u_{10}	1	1	3	2	2	1	3	3	3	3	2	1	1
u_{11}	2	2	3	2	2	1	2	2	3	2	3	2	2
u_{12}	4	4	4	3	3	4	3	4	3	3	3	3	4
u_{13}	3	3	3	3	3	1	3	3	4	3	2	3	3
u_{14}	3	2	3	3	3	1	3	3	4	3	2	3	2
u_{15}	2	2	3	3	2	2	2	2	3	3	2	2	2

则经过计算，该控制类的核指标为{ c_1 }，约简指标集为{ c_1 , c_2 , c_6 , c_8 }。

4 基于未确知测度的层次评估

4.1 未确知测度

由于信息系统的安全评估中存在着许多未确知问题，将未确知理论引入到信息系统风险评估模型中，将使得评估模型更清晰、更合理。通常，使用未确知测度进行多指标综合测度评价包括3个步骤：1)单指标未知测度确立。2)指标权重确定。3)多指标综合测度评价[12-17]。

考虑评价对象 $X=\{x_1,\cdots,x_n\}$，评价 $x_i(1\leqslant i\leqslant n)$ 有 m 项指标，记为 $I=\{I_1,\cdots,I_m\}$，x_{ij} 表示 x_i 在 $I_j(1\leqslant j\leqslant m)$ 下的观测值，$D=\{d_1,\cdots,d_K\}$ 为评价空间，d_k 为第 k 个评价等级。

1)单指标未知测度

对象 x_i 关于指标 I_j 的观测值 x_{ij} 不同时，则该指标使 x_i 处于各评语等级的程度也不同. 设 x_{ij} 使 x_i 处于第 k 个评价等级 d_k 的程度为 u_{ijk}，则 u_{ijk} 称为未确知测度，表示对程度的一种测量结果。测度必须满足“非负有界性、可加性、归一性”3条测量准则，单指标测度矩阵表示如下

$$(\mu_{ijk})_{m\times k}=\begin{bmatrix}\mu_{i11} & \mu_{i12} & \cdots & \mu_{i1k}\\ \mu_{i21} & \mu_{i22} & \cdots & \mu_{i2k}\\ \vdots & \vdots & & \vdots\\ \mu_{im1} & \mu_{im2} & \cdots & \mu_{imk}\end{bmatrix},\quad (i=1,2,\cdots,n)。\tag{1}$$

2)指标权重确定

在未确知综合评价中，指标权重的精确度和科学性直接影响评价的结果。权重确定的典型方法有熵值法、聚类分析法、德尔菲法、层次分析法等。其中，熵值法能够反映指标信息熵值的效用价值，其给出的指标权重有较高的可信度。研究采用熵值法确定各指标权重。

已知对象 x_i 关于指标 I_j 的观测值 x_{ij} 使 x_i 处于 $d_1,\cdots,d_k$ 等级的未确知测度为

$$\boldsymbol{\mu}_j^i=(\mu_{ij1},\mu_{ij2},\cdots\mu_{ijk})。$$

则由测度 $\boldsymbol{\mu}_j^i$ 所确定的信息熵为

$$H(j)=-\sum_{k=1}^{K}\mu_{ijk}\lg\mu_{ijk}。\tag{2}$$

令

$$V_j^i=1-\frac{1}{\lg K}H(j)=1+\frac{1}{\lg K}\sum_{k=1}^{K}\mu_{ijk}\lg\mu_{ijk}。\tag{3}$$

于是

$$\boldsymbol{W}_j^i=\frac{V_j^i}{\sum_{j=1}^{m}V_j^i},(0\leqslant W_j^i\leqslant 1,\sum_{j=1}^{m}W_j^i=1)。\tag{4}$$

$W_j^i=\{w_1^i,w_2^i,\cdots,w_m^i\}$ 即为指标 I_j 关于 x_i 的分类权重。

一般而言，指标的离散程度越强，熵值就越大；反之，熵值就越小。在利用多个指标对事物进行综合评价时，对某个指标，若各个个体的值没有太大区别，则该指标在综合分析中所起的作用不大；反之，若对某个指标而言，各个个体的值有很大的波动，即该指标的离散程度很大，则这个指标对综合分析有很重要的影响。

3)多指标综合测度

令

$$\boldsymbol{\mu}^i=\boldsymbol{W}^i(\mu_{ijk})_{m\times k}=(w_1^i,w_2^i,\cdots,w_m^i)。\begin{bmatrix}\mu_{i11} & \mu_{i12} & \cdots & \mu_{i1k}\\ \mu_{i21} & \mu_{i22} & \cdots & \mu_{i2k}\\ \vdots & \vdots & & \vdots\\ \mu_{im1} & \mu_{im2} & \cdots & \mu_{imk}\end{bmatrix}。\tag{5}$$

由此可得多指标综合测度 $\boldsymbol{\mu}^i=(\mu_{i1},\mu_{i2},\cdots\mu_{ik})$。

4)评价准则

获取多指标综合测度后，还需要通过设置置信度 λ 得到最终评价等级。设 $\lambda>0.5$，通常取0.6或0.7，令

$$k_0=\min_k[(\sum_{l=1}^{k}u_{il})\geqslant\lambda,k=1,2,\cdots,K]。\tag{6}$$

4.2 示例分析

下面以信息系统安全管理保障中某控制子类为例，说明如何采用未确知测度模型进行定量评估。

设信息系统安全管理保障控制域 s^1 中有12个控制类，某控制类 e_i^1 包括3个子类，其子类对象集合为{ e_{i1}^1 , e_{i2}^1 , e_{i3}^1 }。子类 e_{ij}^1 下有6个组件，组件集合为{ e_{ij1}^1 , e_{ij2}^1 , e_{ij3}^1 , e_{ij4}^1 , e_{ij5}^1 , e_{ij6}^1 }，评价空间 $D=\{\mathrm{MCML}_1,\mathrm{MCML}_2,\mathrm{MCML}_3,\mathrm{MCML}_4,\mathrm{MCML}_5\}$，简记为 $D=\{d_1,d_2,d_3,d_4,d_5\}$，由于评价空间为定性指标，为了获得单指标测度矩阵，模型采用多个决策者(专家)的共同参与决策(即群决

策），然后统计专家评价结果的方法获得指标值。例如，对控制子类 e_{i1}^1，10 名专家参与其下组件评分，如对 e_{ij1}^1，有 3 个专家评为 d_2 级，4 个专家评为 d_3 级，3 个专家评为 d_4 级，则单指标测度经过归一化，可加性处理，得到 $\mu_{11k}=\{0,0.3,0.4,0.3,0\}$。其余组件指标的测度确定方法相同，则对控制子类 e_{i1}^1 的单指标测度矩阵

$$(\mu)_{6\times5}=\begin{array}{c} \begin{matrix} d_1 & d_2 & d_3 & d_4 & d_5 \end{matrix} \\ \begin{bmatrix} 0 & 0.3 & 0.4 & 0.3 & 0 \\ 0 & 0.4 & 0.5 & 0.1 & 0 \\ 0.1 & 0.4 & 0.4 & 0.1 & 0 \\ 0.1 & 0.2 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.3 & 0.4 & 0.2 & 0 \\ 0 & 0.3 & 0.3 & 0.3 & 0.1 \end{bmatrix} \end{array} \begin{matrix} e_{ij1}^1 \\ e_{ij2}^1 \\ e_{ij3}^1 \\ e_{ij4}^1 \\ e_{ij5}^1 \\ e_{ij6}^1 \end{matrix}。$$

根据信息熵计算公式，指标权重为：$W^1=\{w_1^1,w_2^1,\cdots,w_6^1\}=\{0.322\ 8,0.414,0.257,0.0657,0.204,0.184\}$，则该控制子类综合测度为{0.052 067，0.494 78，0.595 43，0.279 65，0.024 97}。取置信度 $\lambda=0.6$，则 $0.052\ 67+0.494\ 78+0.595\ 43=1.142\ 8>0.6$，$k_0=3$，该子类的能力成熟度级为 $MCML_3$。

5　结　论

针对《信息系统安全保障评估框架》，分析了其评估指标体系，给出了评估方法的形式化描述和评估流程，首次提出了一种基于 RS-UCS 的信息系统安全保障评估模型，与该模型相关的评估软件原型开发已经完成。该模型的应用为实现定量与定性相结合的信息系统安全保障评估提供了一个新的综合评价方法。

参考文献：

[1] 江常青. 基于模型的信息系统安全评估研究[D]. 北京：博士论文，2007，2.

[2] GB/T 20274. 信息系统安全保障评估框架[S]，2006.

[3] 王国胤，姚一豫，于洪. 粗糙集理论与应用研究综述[J]. 计算机学报，2009，32(7)：1229-1246.
WANG GUO-YING，YAO YI-YU，YU HONG. A survey on rough set theory and applications [J]. Chinese Journal of Computers，2009，32 (7)：1229-1246.

[4] 苗夺谦，李道国. 粗糙集理论、算法与应用[M]. 北京：清华大学出版社，2008.

[5] PAWLAK Z. Roughsets[J]. International Journal of Computer and Information Science，1982：89-93.

[6] 石夫乾，孙守迁，徐江. 基于粗糙集的感性知识关联规则挖掘研究[J]. 计算机集成制造系统，2008，8，14(2)：407-411.
SHI FU-QIAN，SUN SHUO-QIAN，XU JIANG. Association rule mining of Kansei knowledge based on rough set [J]. Computer Integrated Manufacturing Systems，2008，8，14(2)：407-411.

[7] 陈志杰，王永杰，鲜明. 一种基于粗糙集的网络安全评估模型[J]. 计算机科学，2007，34(8)：98-100.
CHEN ZHI-JIE，WANG YONG-JIE，XIAN MING. An evaluation model of computer network security based on rough set[J]. Computer Science，2007，34(8)：98-100.

[8] WANG X，LV J K，WU W. A novel hybrid approach of rough sets and neural networks for extracting classification knowledge [J]. International Journal of Systems and Control，2007，2：80-87.

[9] WEIRI F T，KABLAN M M. Using fuzzy decision making for the evaluation of the project management internal efficiency [J]. Decision Support Systems，2006，42(2)：712-726.

[10] XU N P，FENG D. Information systems risk evaluation based on the AHP-Fuzzy algorithm [C]//International Conference on Networking and Digital Society 2009 (ICNDS'09)，May 30-31，2009. GuiYang，China：IEEE Computer Society，2009，2：178-180.

[11] 张益，陈淑燕，瞿高峰. 信息系统安全风险的属性评估方法[J]. 数学的实践与认识，2005，35(3)：28-33.
ZHANG YI，CHEN SHU-YAN，QU GAO-FENG. Attribute model comprehensive evaluation of security risk of information system[J]. Mathimatics In Practice and Theory，2005，35(3)：28-33.

[12] 曹庆奎，杨艳丽，于瑞龙. 基于未确知集的煤矿安全评价[J]. 煤炭学报. 2007，32(2)：181-185.
CAO QING-KUI，YANG YAN-LI，YU RUI-LONG. The coal mines safety appraisal based on unascertained set[J]. Journal of China Coal Society. 2007，32(2)：181-185.

[13] ZHANG Y Q, SUN S J. Software reliability modeling based on unascertained theory[J]. Journal of Software, 2006,17(8):1681-1687.

[14] WILCOX R C, AYYUB B M. Uncertainty modeling of data and uncertainty propagation for risk studies[C]// 4th International Symposium on Uncertainty Modelling and Analysis. [S. l]:IEEE, 2003,184-191.

[15] WANG Z. Reduction algorithms based on discernibility matrix: the ordered attributes method[J]. Journal of Computer Science and Technology, 2001, l6(6): 489-504.

[16] 支天云,苗夺谦. 二进制可辨矩阵的变换及高效的属性约简算法的构造[J]. 计算机科学, 2002, 29(2): 140-142.
ZHI TIAN-YUN, MIAO DUO-QIAN. The binary discernibility matrix's transformation and high efficiency attributes reduction algorithm's conformation [J]. Computer Science,2002,29(2):140-142.

[17] 刘开第,曹庆奎,庞彦军. 基于未确知集合的故障诊断方法[J]. 自动化学,2004,30(5):747-756.
LIU KAI-DI, CAO QING-KUI, PANG YAN-JUN. A method of fault diagnosis based on unascertained set [J]. Acta Automatica Sinica,2004,30(5):747-756.

(编辑 侯 湘)

(上接第 146 页)

[19] SUNDARAJAN S, KEERTHI S S. Predictive approaches for choosing hyperparameters in gaussian processes[J]. Neural Computation, 2001, 13(5): 1103-1118.

[20] SPIEGELHALTER D J, THOMAS A, BEST N, et al. BUGS 0.5 Examples Volume 1 (version i) [EB/OL]. (1999-06-08) [2010-03-11]. http://www.stat.ufl.edu/system/man/BUGS/eg05vol1/.

(编辑 侯 湘)