基于 A-Delphi 方法的信息系统安全评价模型研究*

袁小珂
(中国民航飞行学院 计算机学院,四川 广汉 618307)

摘 要:针对信息系统安全评价现有方法中各评价指标由研究者主观提出的实际情况,提出了一种新的综合层次分析法并结合德尔菲法的 A-Delphi 方法构建分层结构评价体系,运用该评价体系建立了一个适用于信息系统安全评价的通用数学模型。最后利用模糊综合评价法在该模型基础上对一个实际信息系统进行了安全等级评估。

关键词:A-Delphi;层次分析;信息系统;模糊综合评价;权重
中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2012)08-0054-04

Research of information system security evaluation model based on A-Delphi method

Yuan Xiaoke
(Computer School of Civil Aviation Flight University of China, Guanghan 618307, China)

Abstract: Aiming at the actual situation of evaluation index which proposed by researchers subjectively in information system security evaluation method, this paper proposes a new A-Delphi method which is comprehensive analytic hierarchy process(AHP) and the Delphi method to construct layered structure evaluation index system,and uses the evaluation index system to establish a general mathematic model which is suitable for information system security evaluation.Finally,the fuzzy comprehensive evaluation method is used in the proposed model to evaluate a real information system.

Key words: A-Delphi; AHP; information system; fuzzy overall evaluation; weight

网络信息系统处于开放的互联网环境中,存在着普遍的安全风险。因此,在信息系统投入正式使用前以及使用过程中都需要对其功能目标、技术性能、应用效果等进行评价,从而为系统的改进和推广提供指导。在信息系统安全评估中,很多评估对象包含了大量的主观因素,很难以定量的方式进行分析;目前大多数研究都采用了定量与定性分析相结合的方法来完成具体系统的评价。具体的评估方法很多,比较常见的有层次分析法 AHP(Analytic Hierarchy Process)、德尔菲法(Delphi)等[1-2]。在目前的评价体系中,评估指标的选取通常基于系统可能遭受的风险事件,通过对选择的风险事件作具体分类进而作相应的评价。在此类评估中,风险事件的选择显然影响了对系统的最终评价结论。本文通过引入模糊理论,结合层次分析法和德尔菲法(A-Delphi)对信息系统的安全评价构建了一种新的分层结构评价体系,并进行相应的具体分析。

1 分层结构的安全评估体系构建

对信息系统安全评价的现有研究中,通常都以系统可能遭受的风险事件来作为评估的具体指标。如国内学者李廷元等提出的基于风险事件分类的信息系统评估模型,将系统风险分为了网络安全、系统安全、应用安全和运行安全几方面,从而进行信息系统的安全评估[3];黄丽民等则将安全制度实施对信息系统的风险引入到评估体系中,将网络信息系统的评价指标分为物理安全、安全制度、安全技术措施、网络通讯安全和系统安全五个方面[4]。在这些研究中,安全体系的构建都是由研究者提出来,并选择一些具体的评估指标。显然,这种方式构建的安全体系不可避免地存在一定的主观性。本文采用层次分析法与德尔菲法的 A-Delphi 方法相结合来完成安全评估指标选取和体系的构建。

* 基金项目:国家自然科学基金(60879022)

1.1 应用 A-Delphi 方法构建评估体系

信息系统安全评价体系构建的首要任务是确定评价指标，可按以下步骤完成。

(1)对基本的评价指标进行收集整理，从而得到评价指标的原始数据库。通过对国内外相关评价体系的研究，在广泛征求专家和信息系统使用人员以及管理维护人员意见的基础上，初步筛选出 30 项安全评估指标，制作出专家评分意见表，评分意见表中对某指标的评价采用 AHP 法来进行。

通常，专家采用 9 级评估标度表即可分别完成对各初选指标的评价，这种 1~9 评估标度方法存在较大的主观性。参考文献[5]对这种标度方法进行了深入研究，并与指数标度方法进行了对比，认为指数标度符合人们心理感觉判断，而 1~9 标度则与人们心理感觉判断差距太大；指数标度下判断矩阵的一致性符合人们思维判断一致性，而 1~9 标度下判断矩阵的一致性与人们思维判断一致性不符；指数标度符合客观排序，1~9 标度常与客观排序相反；指数标度具有良好的数学结构，满足有界封闭性和自治性，1~9 标度的数学结构则很差[5]。因此，在层次分析法的应用中，舍弃 9 级评估标度，采用指数标度构造判断矩阵。

定义 1 若因素 A 与因素 B 重要性程度之比为 m，则有相邻两级客观重要性比率：

$\alpha=\sqrt[k]{m}$，k 为韦伯常数。

将 9 级评估标度向指数标度转换，如表 1 所示，即取 $k=8$(重要程度分为 9 级)，$m=9$，则可知 $\alpha=\sqrt[8]{9}\approx 1.316$。本文选取该 α 值来构造判断矩阵。

表 1 9 级标度与指数标度对照表

重要性程度	同等重要	稍微重要	明显重要	强烈重要	极端重要
1~9 标度	1	3	5	7	9
指数标度	α^0	α^2	α^4	α^6	α^8
α 取 1.316	1	1.732	3	5.194	9

(2)由 Delphi 法完成安全评估指标的筛选和确定。首先确定 n 名该领域的专家，由专家对评分意见表打分，然后对回收的专家评估意见进行相关统计分析。根据对第一轮专家评估意见的统计分析，决定是否进行新一轮专家评分。该过程持续到专家的评估意见趋于一致时结束，此时可得到按专家关注度由高到低排列的评估指标序列。从该序列中选择前面的若干项指标即可构成具体的安全评估体系，以便后续工作中应用该评估体系对信息系统进行评估。

在统计分析过程中，可采用动态的模糊聚类方法对专家的评估意见进行聚类，若某位专家对某一指标 t_i 的评估与其他专家的评估意见相差很大，则可以剔除该专家对该项指标的本次评价。

定义 2 设 $\xi(0<\xi<1)$是预设的门限值，令：

$M_\xi=\{i|e_i\geqslant\xi, i=1,2,\cdots,n\}$

则有：$\overline{m}=\frac{1}{|M_\xi|}\sum_{i=1}^{n}m_i$

其中，n 为专家人数，m_i 为第 i 位专家对指标 t_i 的评价，e_i 为第 i 位专家对 m_i 的确信度，$|M_\xi|$表示集合 M_ξ 的元素个数。

在不同次的处理过程中，可以根据实际情况不断修正 ξ 的取值，直至满足要求为止。

1.2 专家对评估指标打分的统计分析

在 1.1 节中给出了评估指标的筛选和确定过程，在该过程中各专家对某评估指标在指标序列中的最终排序受多种因素影响，如专家的学术地位、专家对指标的关注度等。参考文献[6]选择以下函数对专家打分进行统计分析。

(1)专家权威程度 β_R

在一轮专家评分结束后的统计分析中，针对不同学术地位的专家，其评分意见分别分配不同的权重。β_R 一般可由专家对问题的熟悉程度 β_1、专家决策的依据 β_2 以及专家的学术地位 β_3 加权平均得到。计算公式为：

$$\beta_R=\frac{\beta_1+\beta_2+\beta_3}{3}$$

(2)专家关注度 K

该指标反映了某专家对一项指标 i 是否关心。可用以下公式计算：

$$K=\frac{m_i'}{m}$$

其中，m_i' 为参与对指标 i 评分的专家数，m 为专家总数。

(3)指标的加权算术平均值 $\bar{\beta}_i$

指标的加权平均值体现了专家对该指标评分的集中程度。加权平均值越大，该指标相对越重要。计算公式为：

$$\bar{\beta}_i=\frac{1}{m}\sum_{j=1}^{m}\beta_R\beta_{ij}$$

其中，β_{ij} 为专家 j 对指标 i 的评分值。

(4)指标的满分频率 k_i'

要素 i 满分频率越大，说明对该要素作出满分评价的专家人数越多，因而其重要性越大。计算公式为：

$$k_i'=\frac{m_i'}{m_i}$$

其中，m_i' 为对要素 i 作出满分评价的专家数；m_i 为参与要素评分的专家数。

(5)指标等级和 S_j

指标等级和反映专家对每个指标排序的次序总和，等级和越小，表明这个指标越重要。计算公式为：

$$S_j=\sum_{i=1}^{m_i}\beta_{ij}$$

1.3 安全评估体系的层次结构

综合考虑每一评估指标的加权算术平均值、指标满

分频率、指标等级和等因素评价各指标相对重要性的大小，并按重要性进行指标筛选，这样就可以确定最终评价指标。本文按上述方法构建的分层安全评估体系最终结果如表 2 所示。

表 2 信息系统安全评价指标体系

一级要素	二级要素	三级要素	具体描述
评价指标集 U	静态评价 $u1$	物理安全 $u11$	物理环境的安全
		网络安全 $u12$	网络通信安全、网络结构安全等
		系统安全 $u13$	操作系统、数据库平台等的安全
		应用安全 $u14$	身份认证、权限控制等
		运行安全 $u15$	系统变更、日常运行、备份等
	动态评价 $u2$	预警能力 $u21$	对系统风险的预测
		检测能力 $u22$	实时动态检测系统的漏洞和脆弱性
		保护能力 $u23$	对信息以及信息系统的保护作用
		反应能力 $u24$	对安全事件的处理
		反击能力 $u25$	对威胁来源的跟踪等

按照上述方法构建的信息系统安全评估指标体系与以往的相关研究中直接给出的评价体系相比较，由于前者采用了综合层次分析法和德尔菲法的 A-Delphi 方法来完成指标选取，显然避免了研究者本身的主观随意性，因此该指标体系客观性更好，更能准确反映信息系统的安全特性的各个方面。

2 模糊综合评价

结合以上给出的安全评价体系，下面给出信息系统模糊综合评价的相应过程。模糊综合评价方法是以模糊数学理论为基础、基于最大隶属度原理、综合考虑信息系统各种安全因素而对系统进行综合评价，最终确定评价对象所属安全等级的方法。隶属度函数的确定一般有模糊统计法、带确信度的德尔菲法以及二元比对排序法等。本文采用带确信度的 Delphi 法——专家调查法确定隶属度函数。

(1)模糊集的确立

定义 3 设 U 是论域，且 $U=\{u_1,u_2,\cdots,u_m\}$；其中 u_i $(i=1,2,\cdots,m)$ 为系统评价的二级要素，由该要素包含的三级要素评价确定；相应的权重集 $\omega=(\omega_1,\omega_2,\cdots,\omega_m)$，显然有 $\sum_{i=1}^{m}\omega_i=1$。$u_i=\{u_{i1},u_{i2},\cdots,u_{in}\}$；其中 $u_{ij}(j=1,2,\cdots,n)$ 为 u_i 的下级要素；相应的权重集 $\omega_i=(\omega_{i1},\omega_{i2},\cdots,\omega_{in})$，有 $\sum_{j=1}^{n}\omega_{ij}=1$。

上述各权重系数直接影响最终评价结果，因此必须合理设置。有多种不同方法确定权重系数，这里采用综合 Delphi 法和熵值法来完成。用 Delphi 法进行指标的主观权重 ω_{ij}' 设置，用熵值法进行指标的客观权重 ω_{ij}'' 设置，最后用乘法集成法完成组合权重的确定，组合权重公式为：

$$\omega_{ij}=\omega_{ij}'\omega_{ij}''/\Sigma\omega_{ij}'\omega_{ij}''$$

式中，$i=1,2,\cdots,m$；$j=1,2,\cdots,n$。

定义 4 设 V 是待确定隶属度的模糊评价集，且 $V=\{v_1,v_2,\cdots,v_k\}$；$v_1\sim v_k$ 为根据需要建立的从高至低的评价等级。被评价对象的各个因素可以是模糊的，也可以是非模糊的，但经过模糊评价计算后，这些因素对 V 中各评价等级有明确隶属度。

评价等级的划分越细，最终评价越准确；但评价等级过细，又会导致统计分析等实际工作量的大幅增加。因此在等级划分时要折中考虑。

(2)模糊评价矩阵求解

采用基于单因素评价方法确定评价对象的隶属度。所谓单因素评价是指从论域 U 中单因素 v_i 出发进行评价，以确定信息系统对模糊评价集 V 中评价等级 v_j 的隶属度，由此确定 U 到 V 的模糊评价矩阵。对应的综合模糊评价矩阵为：

$$\boldsymbol{R}=(r_{ij})_{m\times k}$$

其中，r_{ij} 表示因素 u_i 对评价等级 v_j 的隶属度，则有：

$$r_{ij}=\frac{v_{ij}}{\sum_{j=1}^{k}v_{ij}}\quad(i=1,2,\cdots,m;j=1,2,\cdots,k)$$

(3)模糊综合评价

对论域 U 上的权重集 $\omega=(\omega_1,\omega_2,\cdots,\omega_m)$ 通过 $\boldsymbol{R}$ 变换为模糊评价集 V 上的模糊集，可以得到模糊评价模型为：

$$S=\omega\circ\boldsymbol{R}=[\omega_1,\omega_2,\cdots,\omega_k]\circ\begin{bmatrix}r_{11}&r_{12}&\cdots&r_{1k}\\r_{21}&r_{22}&\cdots&r_{2k}\\\cdots&\cdots&\cdots&\cdots\\r_{m1}&r_{m2}&\cdots&r_{mk}\end{bmatrix}=[s_1,s_2,\cdots,s_k]$$

其中，$\circ$ 为模糊合成算子。通过对模糊合成算子 $\circ$ 进行分析，本文选择算子 $M(\bullet,\oplus)$。将 S 进行归一化处理后有 $S'=[s_1',s_2',\cdots,s_k']$，其中，$s_i'=s_i/\sum_{j=1}^{k}s_j(i=1,2,\cdots,k)$。$S'$ 即为模糊综合评价模型。由评价模型 S' 可知，$s_1',s_2',\cdots,s_k'$ 分别表示论域 U 对模糊评价集 V 中评价等级 $v_1,v_2,\cdots,v_k$ 的隶属度。

(4)评价结论

基于上述模糊综合评价模型，按照最大隶属度原则，对信息系统的最终评价结论为：

$$s''=\max[s_1',s_2',\cdots,s_k']$$

3 应用实例

下面运用第 2 节中的方法对某信息系统进行相应的评价。

(1)参照第 1 节中的分层安全评估体系，首先建立模糊集：因素集 $U=\{u_1,u_2\}$；其中，$u_1=\{u_{11},u_{12},u_{13},u_{14},u_{15}\}=\{$物理安全，网络安全，系统安全，应用安全，运行安全$\}$，$u_2=\{u_{21},u_{22},u_{23},u_{24},u_{25}\}=\{$预警能力，检测能力，保护能力，反映能力，反击能力$\}$。模糊评价集 $V=\{v_1,v_2,v_3,v_4,v_5\}=\{$非常好，比较好，一般，比较差，非常差$\}=\{1,0.75,0.5,0.25,0\}$。

(2)确定各评价因素的权重值。按照第 2 节的方法，采用综合 Delphi 法和熵值法完成权重设置,如表 3 所示。

表 3 各评价因素权重设置

一级要素	二级要素	权重值	三级要素	权重值
U	u_1	0.486	u_{11}	0.15
			u_{12}	0.17
			u_{13}	0.13
			u_{14}	0.25
			u_{15}	0.30
	u_2	0.514	u_{21}	0.24
			u_{22}	0.20
			u_{23}	0.31
			u_{24}	0.15
			u_{25}	0.10

(3)求解模糊评价矩阵。应用 Delphi 法选定 8 位信息安全领域的专家完成对各评价指标的打分，并对打分结果进行统计分析，归一化处理后得到的模糊评价矩阵为：

$$\boldsymbol{R}_1=\begin{bmatrix}0.20 & 0.14 & 0.28 & 0.21 & 0.17\\ 0.23 & 0.16 & 0.27 & 0.14 & 0.20\\ 0.12 & 0.24 & 0.27 & 0.22 & 0.15\\ 0.17 & 0.28 & 0.21 & 0.24 & 0.10\\ 0.18 & 0.15 & 0.34 & 0.19 & 0.14\end{bmatrix}$$

$$\boldsymbol{R}_2=\begin{bmatrix}0.15 & 0.18 & 0.27 & 0.21 & 0.19\\ 0.20 & 0.13 & 0.26 & 0.27 & 0.14\\ 0.18 & 0.14 & 0.28 & 0.18 & 0.22\\ 0.23 & 0.19 & 0.21 & 0.25 & 0.12\\ 0.22 & 0.12 & 0.24 & 0.16 & 0.27\end{bmatrix}$$

(4)模糊综合评价。由 ω_1=(0.15，0.17，0.13，0.25，0.30)，ω_2=(0.24，0.20，0.31，0.15，0.10)可得到：

$$\boldsymbol{R}=\begin{bmatrix}0.1812 & 0.1944 & 0.2775 & 0.2009 & 0.1460\\ 0.1883 & 0.1531 & 0.2591 & 0.2137 & 0.1868\end{bmatrix}$$

再根据二级要素的权重值 ω 及 R，可计算得出：

S'=(0.1846，0.1731，0.2680，0.2073，0.1670)

按照最大隶属度原则，可知该信息系统的安全评价结论为 s''=0.2680，即安全性评价为一般安全。

本文针对信息系统安全评价现有方法中各评价因素由研究者主观提出的实际情况，提出综合层次分析法和德尔菲法的 A-Delphi 方法构建分层结构评价体系，并运用该评价体系对一个具体的信息系统安全等级进行了实际评估。从评估结果来看，以 A-Delphi 方法构建的分层安全评价体系改进了原有评价方法中广泛存在评价指标选取的主观性；结合该分层评价体系，再使用多级模糊综合评价，使最终评价结果更为准确合理。

参考文献

[1] 张丽.模糊综合评价管理信息系统[J].空军工程大学学报，2001，2(5)：91-94.

[2] 邵培基.AHP 方法综合评价管理信息系统[J].系统工程理论与实践，2000，20(10)：63-67.

[3] 李廷元，范成瑜，秦志光，等.基于风险事件分类的信息系统评估模型研究[J].计算机应用，2009，29(10)：2806-2808.

[4] 黄丽民，王华.网络安全多级模糊综合评价方法[J].辽宁工程技术大学学报，2004，23(4)：510-513.

[5] 吕跃进，张维，曾雪兰.指数标度与 1-9 标度互不相容及其比较研究[J].工程数学学报，2003，20(8)：77-81.

[6] 赵桂红，田纱纱.基于德尔菲法的机场停机坪安全指标筛选研究[J].中国民航大学学报，2008，26(6)：61-64.

[7] 王莲芬，许树柏.层次分析法引论[M].北京：中国人民大学出版社，1990.

[8] 许树柏.层次分析法原理[M].天津：天津大学出版社，1988.

[9] 成卫青，龚俭.网络安全评估[J].计算机工程，2003，29(2)：182-186.

(收稿日期：2011-11-29)

作者简介：

袁小珂，男，1976年生，博士，讲师，主要研究方向：网络与信息安全、空管信息处理。