

模糊综合评价在信息系统安全等级定级中的应用*

谢茂森¹, 杨青²

(1. 四川文理学院 数学与财经学院, 四川 达州 635000;

2. 安徽省芜湖市鸠江区滨河学校, 安徽 芜湖 241000)

摘要: 信息系统安全等级定级由业务信息安全和系统服务安全组成, 业务信息安全和系统服务安全的评价指标又由受侵害的客体、对客体的侵害程度、抵抗能力和恢复能力等组成。因此, 信息系统安全等级定级是一个多层评价模型。针对以上指标评价难以量化、准确度不高的问题, 运用模糊综合评价方法, 建立模糊综合评价模型对信息系统进行安全等级定级, 基于我国现行的信息系统安全等级定级采用五级的规定, 模型选定评判等级为{一级, 二级, 三级, 四级, 五级}, 采用模糊层次分析法确定信息系统安全等级指标体系中的各级指标权重关系, 引进一致性指标检验判断矩阵的有效性。通过学生综合信息管理系统对模型进行实证分析, 结果表明, 应用模糊综合评价方法在因子的定量化和定级方面更加准确和可靠。

关键词: 模糊综合评价; 安全等级; 隶属度; 权重

中图分类号: X914

文献标志码: A

文章编号: 1672-6693(2014)05-0089-06

信息安全等级保护是中国的一项基本制度。信息系统安全等级定级是指对国家安全、法人和其他组织及公民的专有信息以及公开信息的存储、传输、处理, 这些信息的信息系统划分成不同等级, 进行安全保护。实现信息安全等级保护, 能够有效地提高中国信息和信息系统安全建设的整体水平, 有利于在信息化建设过程中同步建设信息安全设施, 保障信息安全与信息化建设相协调; 有利于为新信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务, 有效控制信息安全建设成本; 有利于优化信息安全资源的配制, 对信息系统分级实施保护, 重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全; 有利于明确国家、法人和其他组织、公民的信息安全责任, 加强信息安全管理; 有利于推动信息安全产业的发展, 逐步探索出一条适应社会主义市场经济发展的信息安全模式。

信息安全等级保护工作分系统定级、系统备案、建设整改、等级测评、监督检查等5个环节。信息系统定级是落实等级保护工作的第一步, 对等级保护工作的实施具有指导性作用。从等级保护角度看, 安全级别定不准, 系统备案、建设整改、等级测评等工作就失去了针对性; 从定级单位自身的安全需求看, 结合本单位业务需求、信息安全建设现状, 从自身安全需求出发, 进行针对于信息安全的规划与建设。

中国信息系统的安全等级保护分为5个级别。由于信息系统安全包括业务信息安全和系统服务安全, 与之相对应的受侵害客体和对客体的侵害程度可能不同。因此, 信息系统定级也由业务信息安全和系统服务安全两个方面确定。目前的定级方法是对这两个方面的安全同等对待, 从业务信息安全角度反映的信息系统安全等级保护称为业务信息安全等级保护, 从系统服务安全角度反映的信息系统安全等级保护称为系统服务安全等级保护, 将业务信息安全等级保护和系统服务安全等级保护的较高者确定为定级对象的安全等级保护^[1-2]。

对一个具体的信息系统定级时主要依据信息系统受侵害的客体对象、对客体的侵害程度, 信息系统的抵抗能力和恢复能力来综合确定一个安全等级。但信息系统安全等级定级是一个多因素、多指标的复杂过程。影响安全等级定级的因素具有不确定性且难以精确描述。因而, 须对这些诸多因素进行综合才能做出合理的评价。现行的信息系统安全等级的原则和方法没有对定级提供可量化的操作步骤, 定级中也没有考虑各个因素对系统安全的影响程度的不同^[3]。模糊综合评价法是一种基于模糊数学的综合评价方法, 根据模糊数学的隶属度理论把安全等级定级中定性评价转化为定量评价, 即用模糊数学对受到多种因素制约的安全等级定级做出一个总体

* 收稿日期: 2013-12-04 修回日期: 2013-12-25 网络出版时间: 2014-9-17 22:37

作者简介: 谢茂森, 男, 副教授, 重庆师范大学校友, 研究方向为智能信息处理、模糊系统和模糊集等, E-mail: dazouxms@163.com

网络出版地址: <http://www.cnki.net/kcms/detail/50.1165.N.20140917.2237.017.html>

的评价,进而划分详细等级,有利于对信息系统中使用的信息安全产品实行按等级管理,对信息系统中发生的信息安全事件分等级响应、处置^[4-6]。

1 信息系统安全等级定级中的指标体系

对信息系统进行科学、准确定级的前提就是构造相关的评价指标体系。在遵循综合性、科学性以及可获得性原则基础上,将信息系统安全等级指标体系概括为等级保护对象受到破坏时受侵害的客体、对客体造成侵害的程度、抵抗能力和恢复能力等 4 个方面,并构造了信息系统安全等级定级指标体系层次结构图,如表 1 所示^[1,7]。

1.1 受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下 4 个方面:一是公民、法人;二是个别组织或机构的合法权益;三是社会秩序、公共利益;四是国家安全。

1.2 对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定的。由于对客体的侵害是通过等级保护对象的破坏实现的,因此,对客体的侵害外在表现为对等级保护对象的破坏,通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度有 4 种:一是造成一般损害;二是造成中等程度损害;三是造成严重损害;四是造成特别严重损害。

1.3 抵抗能力

抵抗能力是指信息系统能够应对威胁的能力所构成的系统的安全保护能力之一,不同等级系统所应对抗的威胁主要涉及威胁源(自然、环境、系统、人为)、动机(不可抗外力、无意、有意)、范围(局部、全局)、能力(工具、技术、资源等)等 4 个方面。

威胁源——是指任何能够导致非预期的不利事件发生的因素,通常分为自然(如自然灾害)、环境(如电力故障)、IT 系统(如系统故障)和人员(如心怀不满的员工)等 4 类。

动机——与威胁源和目标有着密切的联系,不同的威胁源对应不同的目标有着不同的动机,通常可分为不可抗外力(如自然灾害)、无意的(如员工的疏忽大意)和故意的(如情报机构的信息收集活动)。

范围——是指潜在威胁的危害范畴,分为局部和整体两种情况;如病毒威胁,有些计算机病毒的传染性较弱,危害范围是有限的;但是蠕虫类病毒则相反,它们可以在网络中以惊人的速度迅速扩散并导致整个网络瘫痪。

能力——主要是针对威胁源人为的情况,它是衡量攻击成功可能性的主要因素。主要体现在威胁源占有计算资源的多少、工具的先进程度、人力资源(包括经验)等方面。

1.4 恢复能力

在某些情况下,信息系统无法阻挡威胁对自身的破坏时,如果系统具有很好的恢复能力,那么即使遭到破坏,也能在很短的时间内恢复系统原有的状态。能够在一定时间内恢复系统原状态的能力,构成了另一种安全保护能力——恢复能力。恢复能力主要从恢复时间和恢复程度上来衡量其不同级别。恢复时间越短、恢复程度越接近系统正常运行状态,表明恢复能力越高。

2 模糊综合评价安全等级定级模型

模糊综合评价法是一种基于模糊数学的综合评标方法。该综合评价法根据模糊数学的隶属度理论把安全等级定级中的定性评价转化为定量评价,即用模糊数学对受到多种因素制约的安全等级定级做出一个总体的评价,进而划分详细等级,有利于对信息系统中使用的信息安全产品实行按等级管理,对信息系统中发生的信息安全事件分等级响应、处置。应用单层次模糊综合评判模型就很难得出正确的评判结果。所以在这种情况下,就需要将评判因素集合按照某种属性分成几类,先对每一类进行综合评判,然后再对各类评判结果进行类之间的高层次综合评判。这样,就产生了多层次模糊综合评价模型^[4,8]。

表 1 信息系统安全等级定级指标体系层次结构

		因素层
信 息 系 统 安 全	业 务 信 息 安 全 T_1	受侵害的客体 T_{11}
		对客体的侵害程度 T_{12}
		抵抗能力 T_{13}
		恢复能力 T_{14}
	系 统 服 务 安 全 T_2	受侵害的客体 T_{21}
		对客体的侵害程度 T_{22}
		抵抗能力 T_{23}
		恢复能力 T_{24}

2.1 建立评价对象的因素集

将指标体系中准则层建立准则集合 $U = \{U_1, U_2, \dots, U_k\}$, k 为按其影响准则的类型划分的个数, 满足 $\bigcup_{i=1}^k U_i = U, U_i \cap U_j = \Phi (i \neq j)$, 对评价的第 i 个准则 $U_i, U_i = \{u_{i1}, \dots, u_{ij}, \dots, u_{im}\} (i = 1, 2, \dots, k), m$ 为第 i 个准则的评价因素的个数。

2.2 建立评语集合

设 $V = \{v_1, v_2, \dots, v_n\}$ 是由评判等级组成的评语集合, 其中 $v_i (i = 1, 2, \dots, n)$ 是对事物的评判等级, 中国现行信息系统安全等级定级采用五级, 因此 $V = \{v_1, v_2, v_3, v_4, v_5\} = \{\text{一级, 二级, 三级, 四级, 五级}\}$ 。

2.3 确定各评价因素的权重

构造好内部独立的递阶层次指标体系, 该体系将评价因素自顶向下不断具体化, 把一级指标分为 k 个评价准则、二级指标细分为 m 个评价因素的两层结构, 现将每一层按照以下方法设定权重系数。

(1) 采用模糊层次分析法确定信息系统安全等级指标体系中的各级指标权重关系。根据已建立的层次结构模型, 对同一层次的指标两两比较其相对重要性, 得到相对权值的比值 $a_{ij} = W_i / W_j$, 满足: $a_{ij} = 1 / a_{ji}, i \neq j, i, j = 1, 2, \dots, k, a_{ij} > 0$, 成对比较矩阵的一般形式如表 2 所示, 在指标权重方案选择时, 避免过分依赖专家和决策者的偏好以及主观判断, 将引用九分位比例标度法对因素重要性程度赋值。

表 2 层次分析法因素成对比较矩阵

指标	U_1	U_2	\dots	U_k
U_1	a_{11}	a_{12}	\dots	a_{1k}
U_2	a_{21}	a_{22}	\dots	a_{2k}
\vdots	\vdots	\vdots	\vdots	\vdots
U_k	a_{k1}	a_{k2}	\dots	a_{kk}

(2) 采用方根法计算各因素的权重。计算判断矩阵每一行的乘积 $P_i = \prod_{j=1}^k a_{ij}, i = 1, 2, \dots, k, \bar{w}_i = \sqrt[k]{P_i}$, 按照公式 $w_i = \bar{w}_i / \sum_{i=1}^k \bar{w}_i$ 将 \bar{w}_i 向量归一化, 得到判断矩阵的特征向量 $w = (w_1, w_2, \dots, w_k)$ 。

(3) 判断矩阵的一致性检验。相应的计算公式如下: 计算最大特征根: $\lambda_{\max} = \sum_{i=1}^k \frac{(\lambda W)_i}{n W_i}$; 计算一致性指标: $CI = \frac{\lambda_{\max} - n}{n - 1}$; 计算一致性比例: $CR = \frac{CI}{RI}$ 。

一般认为, 当 $CR < 0.1$ 时, 判断矩阵的一致性是可以接受的。

(4) 建立权重系数向量。满足一致性检验后, 所得到准则层和因素层的权重系数向量分别为 W, W_i , 其中 $W = (w_1, w_2, \dots, w_i, \dots, w_k), w_i$ 为第 i 个评价准则的权重值, 且 $0 < w_i \leq 1, \sum_i w_i = 1$, 同理可计算 W_i 。

2.4 确定定级隶属矩阵

将已建好的评价对象的因素集和评语集建立对应关系, 因素集 U, U_i 分别对评语集 V 做映射得到每一层的评价矩阵 R 和 R_i 。 R_i 是第 i 个准则因素对评价等级集合 V 的模糊映射, 即 $f: U_i \rightarrow V$, 得到第 k 个一级指标中的因素 i 对等级的隶属向量 $R_i^{(k)} = (r_{i1}^{(k)}, r_{i2}^{(k)}, r_{i3}^{(k)}, r_{i4}^{(k)}, r_{i5}^{(k)})$, 确定 $r_{ij}^{(k)} (j = 1, 2, 3, 4, 5)$ 值的方法有多种, 本文按照如下方法确定: 可先成立由若干人组成的评价小组(设成员有 m 名), 对评价小组人员的评分结果进行统计整理, 若得到对于指标 T_{ij} 有 m_1 个 v_1 评价, m_2 个 v_2 评价, m_3 个 v_3 评价, m_4 个 v_4 评价, m_5 个 v_5 评价, 那么 $r_{ij}^{(k)} = m_j / \sum_{j=1}^5 m_j$, 从而得到业务信息安全(或系统服务安全)的 4 个因素评价矩阵分别为

$$R^{(1)} = \begin{pmatrix} r_{11}^{(1)} & r_{12}^{(1)} & r_{13}^{(1)} & r_{14}^{(1)} & r_{15}^{(1)} \\ r_{21}^{(1)} & r_{22}^{(1)} & r_{23}^{(1)} & r_{24}^{(1)} & r_{25}^{(1)} \\ r_{31}^{(1)} & r_{32}^{(1)} & r_{33}^{(1)} & r_{34}^{(1)} & r_{35}^{(1)} \\ r_{41}^{(1)} & r_{42}^{(1)} & r_{43}^{(1)} & r_{44}^{(1)} & r_{45}^{(1)} \end{pmatrix}, \quad R^{(2)} = \begin{pmatrix} r_{11}^{(2)} & r_{12}^{(2)} & r_{13}^{(2)} & r_{14}^{(2)} & r_{15}^{(2)} \\ r_{21}^{(2)} & r_{22}^{(2)} & r_{23}^{(2)} & r_{24}^{(2)} & r_{25}^{(2)} \\ r_{31}^{(2)} & r_{32}^{(2)} & r_{33}^{(2)} & r_{34}^{(2)} & r_{35}^{(2)} \\ r_{41}^{(2)} & r_{42}^{(2)} & r_{43}^{(2)} & r_{44}^{(2)} & r_{45}^{(2)} \end{pmatrix}$$

$$R^{(3)} = \begin{pmatrix} r_{11}^{(3)} & r_{12}^{(3)} & r_{13}^{(3)} & r_{14}^{(3)} & r_{15}^{(3)} \\ r_{21}^{(3)} & r_{22}^{(3)} & r_{23}^{(3)} & r_{24}^{(3)} & r_{25}^{(3)} \\ r_{31}^{(3)} & r_{32}^{(3)} & r_{33}^{(3)} & r_{34}^{(3)} & r_{35}^{(3)} \\ r_{41}^{(3)} & r_{42}^{(3)} & r_{43}^{(3)} & r_{44}^{(3)} & r_{45}^{(3)} \end{pmatrix}, \quad R^{(4)} = \begin{pmatrix} r_{11}^{(4)} & r_{12}^{(4)} & r_{13}^{(4)} & r_{14}^{(4)} & r_{15}^{(4)} \\ r_{21}^{(4)} & r_{22}^{(4)} & r_{23}^{(4)} & r_{24}^{(4)} & r_{25}^{(4)} \\ r_{31}^{(4)} & r_{32}^{(4)} & r_{33}^{(4)} & r_{34}^{(4)} & r_{35}^{(4)} \\ r_{41}^{(4)} & r_{42}^{(4)} & r_{43}^{(4)} & r_{44}^{(4)} & r_{45}^{(4)} \end{pmatrix}$$

则 (T, V, R) 构成了一个模糊综合评价模型。

2.5 多因素多层次模糊综合评价

综合评价的过程是首先根据每个评价层次上的权重系数向量和隶属矩阵得到相应层次的综合评价结果,实现从底层因素层到准则层、最后到目标层的评判过程。

$$R_i = W_i \otimes R^{(i)} = (W_1^{(i)}, W_2^{(i)}, W_3^{(i)}, W_4^{(i)}) \otimes \begin{pmatrix} r_{11}^{(i)} & r_{12}^{(i)} & r_{13}^{(i)} & r_{14}^{(i)} & r_{15}^{(i)} \\ r_{21}^{(i)} & r_{22}^{(i)} & r_{23}^{(i)} & r_{24}^{(i)} & r_{25}^{(i)} \\ r_{31}^{(i)} & r_{32}^{(i)} & r_{33}^{(i)} & r_{34}^{(i)} & r_{35}^{(i)} \\ r_{41}^{(i)} & r_{42}^{(i)} & r_{43}^{(i)} & r_{44}^{(i)} & r_{45}^{(i)} \end{pmatrix}$$

其中 $i=1$ 代表业务信息安全, $i=2$ 代表系统服务安全, “ \otimes ” 为模糊算子。进一步

$$P = W \otimes R = (\omega_1, \omega_2) \otimes \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

P 为最后的模糊综合评判结果, 可以根据最大隶属度原则得到信息系统安全等级定级。

3 应用实例与分析

3.1 实例描述

学生信息综合管理系统, 主要是用来管理学生成绩、选课信息、图书借阅信息等。侵害的客观方面(客观方面是指定级对象的具体侵害行为、侵害形式以及对客体的造成的侵害结果)表现为: 一旦信息系统遭到入侵、修改、增加、删除等不明侵害(形式可以包括丢失、破坏、损坏等), 会对学生、法人和其他组织的合法权益造成影响和损害, 可以表现为: 影响正常工作的开展, 导致社会不安, 造成不良影响, 引起法律纠纷等^[6,9]。信息系统受到破坏后对侵害客体的侵害程度分都为 5 级。

首先, 对于各因素 $T_{ij} (i, j=1, 2, 3, 4)$ 的评价结果如表 3 所示。

由于各指标因素对等级对象所起的作用不一样, 采用上文介绍的方法确定各级指标的权重, 根据各层指标对定级的重要性。采用方根法计算指标的权重向量如表 4 所示。

由公式 $\lambda_{\max} = \sum_{i=1}^k \frac{(\lambda W)_i}{n W_i}$ 带入数据可求得该判断矩阵最大特征根 $\lambda_{\max} = 5.608$, 其中 λ 是由专家调查法所确定的量化打分系数。按照公式 $\omega_i = \overline{\omega}_i / \sum_{i=1}^k \overline{\omega}_i$ 将 W_i 向量归一化, 得到对应的特征向量, 然后对得到的成对比较矩阵做一致性检验, 可知满足一致性检测要求。因此, 特征向量 W 可以作为评估的权重向量, 按同样的方法计算各因素的权重向量如下:

$$W_1 = (0.44, 0.28, 0.10, 0.18), W_2 = (0.41, 0.08, 0.40, 0.12)$$

由模糊综合评价公式

$$R_i = W_i \otimes R^{(i)} = (W_1^{(i)}, W_2^{(i)}, W_3^{(i)}, W_4^{(i)}) \otimes \begin{pmatrix} r_{11}^{(i)} & r_{12}^{(i)} & r_{13}^{(i)} & r_{14}^{(i)} & r_{15}^{(i)} \\ r_{21}^{(i)} & r_{22}^{(i)} & r_{23}^{(i)} & r_{24}^{(i)} & r_{25}^{(i)} \\ r_{31}^{(i)} & r_{32}^{(i)} & r_{33}^{(i)} & r_{34}^{(i)} & r_{35}^{(i)} \\ r_{41}^{(i)} & r_{42}^{(i)} & r_{43}^{(i)} & r_{44}^{(i)} & r_{45}^{(i)} \end{pmatrix}$$

选择模糊算子进行上述矩阵运算, 得到这一级的评价结果。本文选择模糊算子 (\otimes, \oplus) 为: $a \otimes b = ab, a \oplus b = a + b - ab$ 。例如, 将 W_1 和 $R^{(1)}$ 进行模糊合成运算得到

表 3 信息系统安全等级定级

因素	信息系统安全等级矩阵					
	一级	二级	三级	四级	五级	
T_1	T_{11}	0.1	0.5	0.4	0	0
	T_{12}	0.2	0.5	0.3	0	0
	T_{13}	0.1	0.6	0.3	0	0
	T_{14}	0.2	0.4	0.4	0	0
T_2	T_{21}	0.2	0.7	0.1	0	0
	T_{22}	0.2	0.4	0.4	0	0
	T_{23}	0.1	0.6	0.3	0	0
	T_{24}	0.2	0.4	0.4	0	0

表 4 层次分析法求解权重

$\overline{\omega}_i = \sqrt[k]{\prod_{j=1}^k a_{ij}}$	$\omega_i = \frac{\overline{\omega}_i}{\sum_{i=1}^k \overline{\omega}_i}$	权重向量
1.888	0.339	0.34
1.245	0.223	0.22
0.450	0.082	0.08
0.758	0.136	0.14

$$R_1 = W_1 \otimes R^{(1)} = (0.44, 0.28, 0.10, 0.18) \otimes \begin{pmatrix} 0.1 & 0.5 & 0.4 & 0 & 0 \\ 0.2 & 0.5 & 0.3 & 0 & 0 \\ 0.1 & 0.6 & 0.3 & 0 & 0 \\ 0.2 & 0.4 & 0.4 & 0 & 0 \end{pmatrix} = (0.1387, 0.4184, 0.3206, 0, 0)$$

由于 $\sum_{j=1}^4 r_{ij} \neq 1$, 所以对其进行归一化处理得(仍记为 R_1)

$$R_1 = (0.1580, 0.4784, 0.3653, 0, 0)$$

根据最大隶属度原则, 学生信息综合管理系统业务信息安全等级保护综合评价为二级。其次, 考虑系统服务安全等级, 采用与上述同样的方法, 计算学生信息综合管理系统系统服务安全模糊综合评价为 $R_2 = (0.1752, 0.5711, 0.2536, 0, 0)$ 。根据最大隶属度原则, 学生信息综合管理系统系统服务安全等级保护综合评价为二级。业务信息安全等级保护和系统服务安全等级保护的较高者为二级。因此, 学生信息综合管理系统的安全等级保护确定为二级。

在完成第二级模糊综合评价后, 不一定将业务信息安全等级保护和系统服务安全等级保护的较高者确定为信息系统安全等级保护的最终等级, 而是在第一级模糊综合评价的基础上, 再进行第二级模糊综合评价。如

$$P = W \otimes R = (\omega_1, \omega_2) \otimes \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = (0.6, 0.4) \otimes \begin{pmatrix} 0.1865 & 0.4482 & 0.3653 & 0 & 0 \\ 0.1752 & 0.5711 & 0.2536 & 0 & 0 \end{pmatrix} = (0.1741, 0.4544, 0.2984, 0, 0)$$

归一化后的结果是: $P = (0.1878, 0.4902, 0.3219, 0, 0)$ 。根据最大隶属度原则, 学生信息综合管理系统业务信息安全等级保护综合评价为二级。最终说明该系统的整体防护能力做得好, 达到国家对相关信息系统的安全等级定级要求, 说明该系统在所有因素层上的综合表现令人满意。

4 结论

信息系统安全等级定级是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的系统划分不同等级进行安全保护, 是信息系统安全保护工作的首要环节和关键环节, 是开展信息系统备案、建设整改、等级测评、监督检查等工作的重要基础。

应用模糊数学方法建立模糊综合评价模型对信息系统进行安全等级定级。结果表明, 应用模糊综合评价方法在因子的定量化和定级方面更加准确和可靠, 所获得各等级的最终评价价值, 不仅能反映各等级之间的相对级别, 而且也可直接反映出各种情形的绝对等级, 为综合改善信息系统安全等级定级提供比较可靠的科学依据。通过模型进行实证分析, 采用模糊综合评价模型进行安全等级定级, 结果合理、简便、有效、直观, 为信息系统安全等级定级提供一个可以量化的较为科学的数学模型。

参考文献:

[1] 公安部信息安全等级保护评估中心编. 信息安全等级保护政策培训教程[M]. 北京: 电子工业出版社, 2010. 06.
 Edited by Information Security Protection Evaluation Center of Ministry of Public Security. Information security protection policy training course[M], Beijing: Electronic Industry Press, 2010.

[2] 李蓉. 网络信息技术的应用[J]. 电子设计工程, 2013, (14): 137-139.
 Li R. The network information technology application[J]. Electronic Design Engineering, 2013(14): 137-139.

[3] 周焕盛. 安全等级划分方法研究综述[M]. 北京: 科学出版社, 2004.
 Zhou H S. Summary of safety level classification[M]. Beijing: Science Press, 2004.

[4] 骆正山, 陈红玲, 郑楠. 多因素模糊综合评判模型的风险投资项目评估应用研究[M]. 西安: 西安科技大学出版社, 2006.
 Luo Z S, Chen H L, Zheng N. Multi-factor fuzzy comprehensive evaluation model application research to the risk of investment projects[M]. Xi'an: Xi'an University of Science and Technology Press, 2006.

[5] 章文辉, 杜百川, 杨盈昀. 模糊层次分析法在广播电视信息安全保障评价指标体系中的应用研究[J]. 电子学报, 2008, 36(10): 2060-2064.
 Zhang W H, Du B C, Ying Y Y. FAHP application to radio and television information security evaluation system[J].

- Acta Electronica Sinica, 2008, 36(10):2060-2064.
- [6] 张吉军. 模糊层次分析法(FAHP)[J]. 模糊系统与数学, 2000, 14(2):80-88.
- Zhang J J. Fuzzy analytic hierarchy process (FAHP) [J]. Fuzzy Systems and Mathematics, 2000, 14(2):80-88.
- [7] 陆向艳, 钟诚, 杨柳. 威胁分析的网站安全风险评估方法[J]. 计算机应用, 2009, 29(S2):94-96.
- Lu X Y, Zhong C, Yang L. Threat analysis website security risk assessment methodology[J]. Computer Applications, 2009, 29(S2):94-96.
- [8] 肖龙, 戚沔, 李千目. 基于 AHP 和模糊综合评判的信息安全风险评估[J]. 计算机工程与应用, 2009, 45(22):82-85.
- Xiao L, Qi M, Li Q M. Information security risk assessment based on AHP and fuzzy comprehensive evaluation [J]. Computer Engineering and Applications, 2009, 45(22):82-85.
- [9] Yu S, Pei W. Risk driven dynamic test based on fuzzy comprehensive judgment theory[J]. Journal of Communication and Computer, 2010, 7(6):1-5.

Application of Fuzzy Comprehensive Evaluation on the Level of Security Classification Information System

XIE Maosen¹, YANG Qing²

(1. Institute of Mathematics and Finance, Sichuan University of Arts and Science, Dazhou Sichuan 635000;

2. Binhe School, Jiujiang District, Wuhu Anhui 241000, China)

Abstract: Information systems security level classification consists of business information security and system security services, business information security and system services security are aggrieved by the infringement object, the degree of violation to the object, resistance and resilience, etc., therefore, the information system security is a multivariate and multi-level classification evaluation model. Aiming at the problem of the difficult to quantify and low accuracy on classifying the security level of information system, this paper established fuzzy comprehensive evaluation model to classify the security level of information system with the method of fuzzy mathematics. In this model, based on the fact that using five levels to classify the information systems security level, the judges grade is $\{level1, level2, level3, level4, level5\}$, using fuzzy analytic hierarchy process (FAHP) to determine the weight of the relationship between the indicator system, by introducing the consistency index test the effectiveness of the judgment matrix. The model is empirically analyzed by general information management system, and the fuzzy comprehensive evaluation method is adopted to classify the security level. It shows that it is more accurate and reliable in quantitative and grading of factor by fuzzy comprehensive evaluation.

Key words: fuzzy comprehensive evaluation; security level; membership degree; weight

(责任编辑 游中胜)