一种信息系统安全风险的灰色模糊综合评估方法*

罗 佳[1],杨世平[2]

(1.贵州大学 计算机科学与信息学院,贵州 贵阳 550025;
2.贵州大学 明德学院,贵州 贵阳 550004)

摘 要:针对信息系统安全风险因素的灰色性和模糊性,以及信息安全风险评估过程中存在的主观性,将灰色统计评估法、模糊综合评判法和层次分析法结合,建立一种信息系统安全风险的灰色模糊综合评估模型。通过灰色统计法建立模糊隶属度矩阵,层次分析法确定风险因素权重,以此来评估量化系统风险,该方法能较好地量化评估信息系统安全风险。

关键词:信息系统安全风险评估;威胁;脆弱性;灰色统计;灰色模糊综合评估模型

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1674-7720(2010)13-0044-03

A grey fuzzy comprehensive evaluation method of information system security risk

LUO Jia[1], YANG Shi Ping[2]

(1.College of Computer and Information, Guizhou University, Guiyang 550025, China;
2.College of Mingde, Guizhou University, Guiyang 550004, China)

Abstract: In view of the nature of gray and ambiguous for information systems security risk factors and the process of information security is subjective, the methods of gray statistical evaluation, fuzzy comprehensive evaluation method and analytic hierarchy process are combined to set a model of grey fuzzy comprehensive evaluation. Fuzzy membership degree matrix were established through the gray statistical method, the risk factors weights AHP were determined, which can quantize to assess the risk. The method can be objective and quantitative assessment of information systems security risks.

Key words: information security risk assessment; threat; vulnerability; grey statistics; grey fuzzy comprehensive evaluation model

随着信息技术的飞速发展,来自信息领域,网络世界的威胁频繁出现,信息系统及所承载的信息和服务的安全性变得尤为重要。信息和信息服务在保密性、完整性、可用性等方面出现漏洞都将给组织带来不同程度的影响。开展信息安全风险评估,对网络和信息系统的资产价值、潜在的安全威胁、薄弱环节进行分析,可以做到心中有数,可以发现信息系统中存在的主要安全问题,并找到解决这些问题的方法,有针对性地进行管理。通过识别分析信息系统风险要素的相互关系和层次结构,建立一种信息系统灰色模糊多层风险综合评估模型。利用专家评判法构造系统风险要素指标评判样本矩阵,确立风险评价灰类的等级数、灰类的灰数及白化权函数,通过灰色统计法计算出灰色评价权矩阵,即模糊综合评判矩阵。通过模糊综合评判法量化评估系统资产面临威胁发生的可能性及威胁利用脆弱性产生的后果,以此量化系统资产及系统面临的风险,该方法可以减少评估的主观性。

*基金项目:贵州省科学技术基金项目(黔科合J字[2007] 2204号)

1 信息安全风险评估方法

目前国内外存在很多风险评估的方法,但还没有统一的信息安全风险分析的方法。从计算方法上分为定性分析方法、定量分析方法、定性与定量相结合的分析方法[1-2]。

1.1 定量评估方法

定量评估方法是指运用数量指标对风险进行评估,定量分析方法的优点是用直观的数据来表述评估的结果,看起来一目了然,而且比较客观。但也常常为了量化,容易简单化、模糊化,会造成误解和曲解。而且由于数据统计缺乏长期性,计算过程又容易出错,所以定量

分析的细化非常困难。

1.2 定性评估方法

定性分析方法主要依据研究者的知识、经验、历史教训、政策走向及特殊变例等非量化资料对系统风险状况做出判断。典型的定性分析方法有德尔菲法、矩阵法等。定性分析方法的优点是避免了定量分析方法的缺点，可以挖掘出一些蕴藏很深的思想，使评估的结论更全面深刻，但它的缺点也显而易见，即主观性强，对评估者要求很高。

1.3 定性与定量结合的评估方法

信息系统风险评估是个复杂的过程，需要考虑的因素很多，有些评估要素是可以用量化的形式来表达，而对有些要素的量化又是很困难甚至是不可能的。定量分析是定性分析的基础和前提，定性分析应该建立在定量分析的基础上，不能将定性分析方法与定量分析方法简单地割裂开来，而是将这两种方法结合起来，采用综合分析方法。主要的综合分析方法有层次分析法、概率风险评估和模糊综合评价法等。

2 信息安全风险评估的计算方法[3]

风险是威胁发生的可能性，是薄弱点被威胁利用的概率潜在的函数，$R=R(A,T,V)=R(L(T,V),P(I_a,V_a))$ 其中 A 为资产；T 为威胁；V 为脆弱性；I_a 为资产的重要程度；V_a 为资产的脆弱性；$L(T,V)$ 为威胁利用资产脆弱性的可能性；$P(I_a,V_a)$ 为作用的资产价值及其脆弱性的严重程度[3]，风险计算原理如图 1 所示。

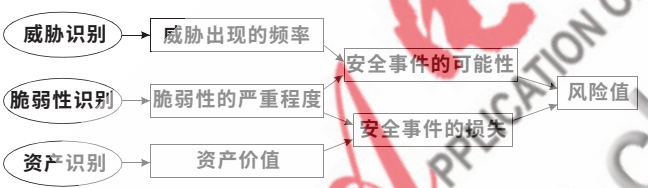

图 1 风险计算原理图

3 信息系统安全风险的模糊综合评判模型

3.1 信息安全风险要素关系

信息安全风险评估是围绕着资产、脆弱性和威胁展开的。通过信息安全风险要素关系图可知，风险是潜在的安全事件发生的可能性和后果，评估量化风险，就是量化安全事件发生的可能性和后果。在应用灰色综合评估方法评估信息系统的风险时，应先建立信息系统风险评估指标体系，通过对信息系统的风险本质进行分析，可建立风险评估指标体系[4]，信息安全风险评估指标体系如表 1 所示。

3.2 确立评价指标集

设评价因素集 $u=\{u_1,u_2,\cdots,u_n\}$，根据所建立的评估指标体系，第一级评价指标为：$\{u_1,u_2,u_3,u_4,u_5,u_6\}$，第二级指标为：$u_1=\{u_{11},u_{12},u_{13},u_{14},u_{15},u_{16}\}$，$u_2=\{u_{21},u_{22}\}$，$u_3=\{u_{31},u_{32}\}$，$u_4=\{u_{41},u_{42},u_{43}\}$，$u_5=\{u_{51},u_{52},u_{53}\}$，$u_6=\{u_{61},u_{62}\}$。

表 1 信息安全风险评估指标体系

	一级指标	二级指标
安全事件发生的可能性	威胁发生的可能性	威胁源的行为动机
		威胁源的技术能力
		威胁源拥有的资源
		威胁源的风险承受能力
		威胁源受惩罚的可能性
		资产对威胁源的吸引力
	脆弱性	脆弱性的暴露程度
		脆弱性被利用的难易程度
	安全措施的有效性	安全技术有效性
		安全管理策略有效性
安全事件发生产生的影响	资产价值	资产的可用性
		资产的有效性
		资产的完整性
	系统能力	系统延迟
		系统削弱
		系统中断
	系统恢复费用	系统信息恢复费用
		系统服务恢复费用

3.3 评判指标权重的确立[5]

在多层次评估中，各个评估指标的重要程度通常是不同的，权重的确定是否合理、科学，直接影响着评价的准确性。权重的构造通过 AHP 法来确定。可以将人的主观判断用数量形式表达和处理，可以同时处理可定量和不易定量因素，也可以提示人们对问题的主观判断是否一致。可分为 4 个步骤：(1)建立问题的递阶层次结构；(2)构造两两比较判断矩阵；(3)由判断矩阵计算被比较元素的相对权重；(4)计算各层元的组合权重。先对第二层次的要素以第一层为准则进行两两比较并根据评定尺度确定其相对重要度，建立判断矩阵：

$$\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \end{bmatrix}$$

其中，b_{ij} 表示从判断准则考虑要素 b_i 对 b_j 的重要程度，而判断尺度的取值按相对重要程度取 1~9 之间的自然数。根据第二层次的判断矩阵，利用方根法计算各元素的相对权重。先求出特征向量 $\boldsymbol{M}$，$\boldsymbol{M}=(m_1,m_2,\cdots,m_n)$，其中 $m_i=(b_{i1},b_{i2},\cdots,b_{in})^{\frac{1}{n}}$，对 $\boldsymbol{M}$ 进行归一化处理得到排序权向量 $\boldsymbol{W}$：

$$\boldsymbol{W}=(W_1,W_2,\cdots,W_n)$$

其中，$w_i=m_i/\sum_{i=1}^{n}m_i$。

计算矩阵的最大特征根：$\lambda_{max}=\sum\frac{(AW)_i}{nw_i}$。再进行一致性检验，一致性指标为：

$CI=(\lambda_{max}-n)/n-1$

其中，n 为判断矩阵的阶数。当 $CI<0.1$ 时，表明矩阵一致性成立，各项权重无逻辑错误。通过 AHP 法可以计算出一级指标，二级指标权重向量。

3.4 信息系统风险评价等级和评分标准[6]

按照《GB/T 20984-2007 信息安全技术信息安全风险评估规范》的要求，结合安全保护等级的分级和国际危机管理的分级惯例，将风险的评价等级分为五级，即很高、高、中、低、很低，为将定性指标转换为定量指标，应相应地对各个指标赋值。按照 5 分制原则确定各等级的赋分，则 5 个评定等级分数分别为 5、4、3、2、1，指标等级介于两者之间的相应的评分为 4.5、3.5、2.5、1.5、0.5 各值。

3.5 评价样本矩阵及评价灰类的确定[7]

3.5.1 评价样本矩阵的确定

设有 n 位专家参与评价，d_{ti} 表示第 t 位专家对第 $i=(1,2,\cdots,m)$ 个指标给出的评分，这样全部专家对评价指标的评价数据构成评价样本矩阵：

$$\boldsymbol{D}=\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & \cdots & d_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{bmatrix}$$

3.5.2 确定评价灰类

由于专家水平的局限性及认识角度上的差异，只能给出一个灰数的白化值。为了真正反映属于某类的程度，需要确定评价灰类，即：要确定评价灰类的等级数、灰类的灰数及白化权函数。评价灰类要根据评价等级，通过定性分析确定。这里设有 5 个评价灰类分别是很高、高、中、低、很低。第 1 类：$j=1,\otimes\in[5,\infty)$，第 2 类：$j=2,\otimes\in(0,4,8)$，第 3 类：$j=3,\otimes\in(0,3,6)$，第 4 类：$j=4,\otimes\in(0,2,4)$，第 5 类：$j=5,\otimes\in(0,1,2)$。以灰类的样本 d_{ij} 为横坐标，以灰数确认度 f 为纵坐标的最少信息图像，称为灰类的白化权函数，各类的白化权函数分别设为：$f_1(d_{ti})$，$f_2(d_{ti})$，$f_3(d_{ti})$，$f_4(d_{ti})$，$f_5(d_{ti})$，根据白化权函数定义可设 5 个白化权函数分别为：

$$f_1(d_{ti})=\begin{cases} d_{ti}/5, & d_{ti}\in[0,5] \\ 1, & d_{ti}\in[5,\infty] \\ 0, & d_{ti}\in[-\infty,0) \end{cases} \quad f_2(d_{ti})=\begin{cases} d_{ti}/4, & d_{ti}\in[0,4] \\ 2-d_{ti}/4, & d_{ti}\in[4,8] \\ 0, & d_{ti}\in[0,8] \end{cases}$$

$$f_3(d_{ti})=\begin{cases} d_{ti}/3, & d_{ti}\in[0,3] \\ 2-d_{ti}/3, & d_{ti}\in[3,6] \\ 0, & d_{ti}\notin[0,6] \end{cases}$$

$$f_4(d_{ti})=\begin{cases} d_{ti}/2, & d_{ti}\in[0,2] \\ 2-d_{ti}/2, & d_{ti}\in[2,4] \\ 0, & d_{ti}\notin[0,4] \end{cases} \quad f_5(d_{ti})=\begin{cases} 1, & d_{ti}\in[0,1] \\ 2-d_{ti}, & d_{ti}\in[1,2] \\ 0, & d_{ti}\notin[0,2] \end{cases}$$

3.6 计算灰色评价系数

用灰色统计法，由各灰数的白化权函数求出 d_{ti} 属于第 $j(j=1,2,3,4,5)$ 个评价灰类的权 $f_j(d_{ti})$，据此可以确定评价矩阵的灰色统计数 n_{ij} 和第 i 个指标属于各个评价灰类的总灰色统计数 n_i，$n_i=\sum_{j=1}^{5}n_{ij}$。

3.7 综合计算灰色模糊评价结果[8]

由 AHP 法确定的各因素的权重向量 W_i 和模糊隶属度矩阵，根据模糊综合评判法进行综合评判。首先进行二级综合评判，根据二级评判因素集 $u_1=\{u_{11},u_{12},u_{13},u_{14},u_{15},u_{16}\}$，$u_2=\{u_{21},u_{22}\}$，$u_3=\{u_{31},u_{32}\}$，$u_4=\{u_{41},u_{42},u_{43}\}$，$u_5=\{u_{51},u_{52},u_{53}\}$，$u_6=\{u_{61},u_{62}\}$ 的评判矩阵 $\boldsymbol{R}_1,\boldsymbol{R}_2,\boldsymbol{R}_3,\boldsymbol{R}_4,\boldsymbol{R}_5,\boldsymbol{R}_6$ 及 $\boldsymbol{W}_i$ 可得二级综合评判为：$\underset{\sim}{A}_i\circ\boldsymbol{R}_i=\underset{\sim}{\boldsymbol{B}}_i$（其中。为模糊合成算子）。

利用综合评判得到的 $\underset{\sim}{B}$ 对评判结果做出判定。常用的判定准则有大隶属度原则和加权平均原则，为避免综合失效，均衡考虑各因素权重，通常采用加权平均原则，量化评判结果为[9]：

$$L=\sum_{i=1}^{k}v_i b_i^n/\sum_{i=1}^{k}b_i^n \quad (n=1 \text{ 或 } n=2)$$

可以计算出安全事件发生可能性 $L_p=\sum_{i=1}^{5}v_i b_i/\sum_{i=1}^{5}b_i(n=1,j=1,2,3,4,5)$。

安全事件发生后产生影响 $L_c=\sum_{i=1}^{5}v_i' b_i'/\sum_{i=1}^{5}b_i'$。

信息系统风险是安全事件发生概率及其后果的函数，若已知安全事件发生概率及后果的函数，则关于风险的计算为：

$$R(x)=R(p,c)=\sum_{i=1}^{n}p_i u(c_i),$$

可求得风险值：$R=L_p\times L_c$。

灰色模糊综合评判法是将灰色理论与模糊综合评价法结合起来，并将定性与定量计算相结合的一种方法。由于信息系统风险的灰色模糊性，通过识别分析信息系统风险要素的相互关系和层次结构，建立一种信息系统灰色模糊多层风险综合评估模型，量化评估系统资产面临安全事件发生的可能性及安全事件发生产生的后果，该方法可以减少评估的主观性，使系统风险量化评估结果更客观，从而采取相应的措施来降低风险，使风险降低到一个可接受的水平。

参考文献

[1] 范红，冯登国，吴亚非.信息安全风险评估方法与应用[M].北京：清华大学出版社，2006.
[2] 王英梅，王胜开，程湘云.信息安全风险评估[M].北京：电子工业出版社，2007.
[3] 吴亚非，李新友，禄凯.信息安全风险评估[M].北京：清华大学出版社，2006.
[4] 胡勇.信息系统风险量化评估指标体系[J].四川大学学

报(自然科学版),2006,43(5):1048-1052.

[5] 史简,郭山清,谢立.一种实时的信息安全风险评估方法[J].计算机工程与应用,2006(1):109-110.

[6] 冯建湘,唐嵘,王双维.软件质量的灰色关联分析及其应用[J].计算机工程,2004,30(9):91-92.

[7] 刘思峰,方志耕.灰色系统理论及其应用[M].北京:科学出版,1991.

[8] 梁保松,曹殿立.模糊数学及其应用[M].北京:科学出版社,2007.

[9] 范红,冯登国.信息安全风险评估实施教程[M].北京:清华大学出版,2006.

(收稿日期:2009-12-12)

作者简介:

罗佳,女,1983年生,硕士研究生,主要研究方向:网络与信息安全。

杨世平,男,1952年生,博士,教授,研究生导师,主研究方向:网络与信息安全。