文章编号:1001 - 9081(2006)09 - 2111 - 03

一种基于灰色层次分析法的信息安全评估模型

任 帅,慕德俊,朱灵波
(西北工业大学 自动化学院,陕西 西安 710072)
(maxwellren@ mail. nwpu. edu. cn)

摘 要:提出了一种基于灰色层次分析法的信息安全评估模型。首先,以国际信息安全标准 ISO/IEC 17799 和国内信息系统安全的相关评估准则为基础,建立了三层信息安全层次结构模型。之后,使用层次分析法与灰色系统理论对该模型进行求解,使结果更为客观。最后以证券交易网为评估对象进行实例计算,结果得到对方的认可,证明了该模型是合理的、有效的。

关键词:灰色层次分析法; 信息安全评估; 证券交易网; ISO/IEC 17799; 层次分析法
中图分类号: TP309 **文献标识码**:A

Model of information security evaluation based on gray analytical hierarchy process

REN Shuai, MU De-jun, ZHU Ling-bo
(*College of Automation, Northwestern Polytechnical University, Xi'an Shaanxi* 710072, *China*)

Abstract: An information security evaluation model was proposed based on Gray Analytical Hierarchy Process. First, an information security hierarchy model with three-hierarchy was established according to ISO/IEC 17 799 and some domestic information security evaluation criteria. Second, the model was explained by AHP and gray systems theory, thus the result could be more objective. Finally, a case study was carried out to a stock exchange net and the result was acknowledged by the company. Therefore, this model is proved to be feasible and effective.

Key words: gray analytical hierarchy process; information security evaluation; stock exchange net; ISO/IEC 17799; AHP

0 引言

信息安全已经成为当今社会关注的重要问题之一。从 TCSEC、OCTIVE、ISO/IEC 17799 到 GB/T 18336 等一系列信息安全标准的陆续出台,标志着信息安全已经成为一项重要的产业,这给信息安全评估工作提出了越来越高的要求。

评估模型的应用是评估合理与否的关键。本文提出了一种基于灰色层次分析法的信息安全评估模型。通过应用层次分析法[1,2]计算出受评对象各层次的相对权重,再用灰色系统理论[3,4]处理专家的评估数据,这样就不会因为某个人的评估失误而影响整个评估结果,使结果达到客观、公正。

1 信息安全灰色层次评估模型

本文首先以国际信息安全管理实践规范 ISO/IEC 17799[5]和我国信息系统安全的相关评估准则[6~8]为基础,总结出信息安全 7 大要素和各要素的具体内容,并利用国内外广泛认可的信息安全三属性,即机密性、完整性、可用性对各要素进行评估,提出信息安全层次结构。

7 大要素和各要素的具体属性如下:

网络应用安全:网络设备、结构、网络应用服务、操作系统和数据库系统。

人事安全:人事资源、安全意识、安全培训、信息访问控制及维护。

物理安全:环境、设备与电缆和介质。

资产安全:内部资产管理构架、资产责任人的权责规定。

策略与风险控制:策略方针、制度规范、第三层表单文件和过程记录、组织机构、政策和方法。

管理安全:运行、变更控制、废弃和系统技术管理、行政管理、法律法规、投资预算等。

组织体系:决策、管理和执行层。

根据层次分析法原理,评估结构可分为三层:"信息安全"为目标层,"信息安全 7 要素"为准则层,"3 性评估标准"为指标层。这样的结构对评估对象的脆弱性、威胁性、可能发生性及负面影响等各方面的内容给予充分考虑,结构完整,体现了层次与逻辑。

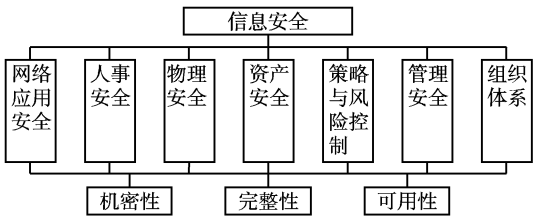


图 1 信息安全层次结构

然后,根据信息安全层次结构,进一步建立了基于灰色层次分析法的信息安全评估模型(如图 2 所示)。此模型可以分为 7 个步骤进行:

(1) 确立专家评估组权重

由于评估者自身素质不同,按重要程度对各组取不同权重,构成专家组权重矩阵**P** 。

收稿日期:2006 - 03 - 07; **修订日期**:2006 - 06 - 02 **基金项目**:西北工业大学研究生创业种子基金资助项目(Z200633)

作者简介:任帅(1982 -),男,山西太原人,硕士研究生,主要研究方向:网络与信息安全; 慕德俊 (1963 -),男,山东荣成人,教授,博士生导师,主要研究方向:自动控制、信息安全; 朱灵波(1980 -),男,浙江人,博士研究生,主要研究方向:智能控制、网络与信息安全.

(2) 构造评估矩阵,确定各要素相对权重

由专家进行判定,构造评估矩阵。矩阵行代表同一层次的评估要素,列代表要素的相对重要性等级,以此行、列建立评估矩阵。“1”代表“√”,“0”代表“无”。利用层次分析法对评估矩阵进行处理可得各要素的权重矩阵。针对本文,准则层 7 要素权重用$\mathbf{W}_i$表示,指标层 3 属性权重用$\boldsymbol{W}_{ij}$表示。

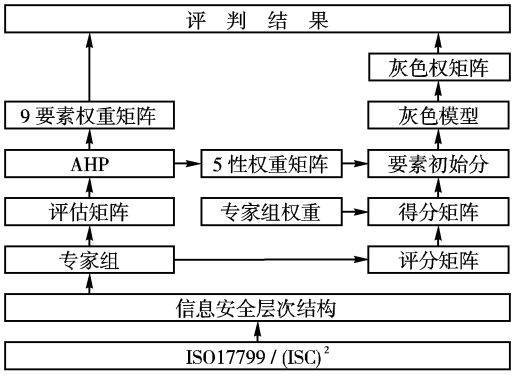


图 2 信息安全灰色层次评估模型

(3) 构建评分矩阵

在评估时,因为底层评估因素是定性而非定量指标,不能形成统一的标准。为此,依照优劣程度,将其分为甲、乙、丙、丁、戊 5 个等级,对应分值为 10,8,6,4 和 2 分,构成等级分值矩阵 $\boldsymbol{C}$,$\boldsymbol{C}$ = (10 8 6 4 2)。指标等级介于两相邻等级时,分值为 9,7,5,3 和 1 分。具体标准将由专家组拟定。用 D_{JI}^{A} 表示专家组 I 对准则层要素 J 的第 A 个指标层属性给出的评分矩阵。

(4) 确定评估要素初始得分

由$\boldsymbol{D}_{JI}^{A}$和$\boldsymbol{P}$可得受评要素的得分矩阵$\boldsymbol{D}_{J}^{A}$:

$$\boldsymbol{D}_{J}^{A} = \boldsymbol{P} \times \boldsymbol{D}_{JI}^{A} \tag{1}$$

由得分矩阵$\boldsymbol{D}_{j}^{A}$和权重矩阵$\boldsymbol{W}_{ij}$可得准则层要素的初始评估分数 d_{Vi}:

$$d_{Vi} = \boldsymbol{D}_{i}^{A} \times \boldsymbol{W}_{ij} \tag{2}$$

(5) 确定评估灰类

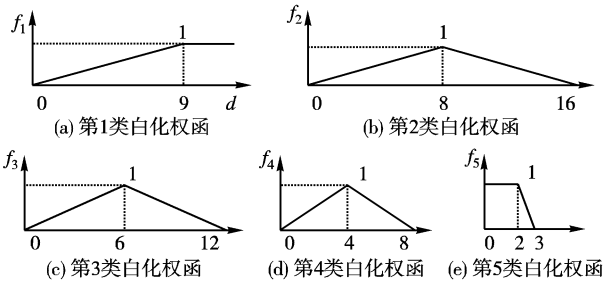
确定评估灰类就是要确定评估灰类的等级数、灰类的灰数以及灰数的白化权函数[9]。白化权函数转折点的值称为阈值。

针对本文的具体对象,通过定性分析确定阈值。设灰类序号为 $k(k = 1, 2, 3, 4, 5)$,有 5 类,它们是甲、乙、丙、丁、戊 5 级,其相应灰数,如表 1 所示。

表 1 5 灰类等级灰数

灰类等级	白化权函数	灰数	图示
第 1 类甲	f_1	$\oplus 1 \in [9, \infty)$	图 3(a)
第 2 类乙	f_2	$\oplus 2 \in (0, 8, 16)$	图 3(b)
第 3 类丙	f_3	$\oplus 3 \in (0, 6, 12)$	图 3(c)
第 4 类丁	f_4	$\oplus 4 \in (0, 4, 8)$	图 3(d)
第 5 类戊	f_5	$\oplus 5 \in (0, 2, 3)$	图 3(e)

由表 1 得相应灰数白化权函数,如图 3 所示:



(a) 第1类白化权函 (b) 第2类白化权函 (c) 第3类白化权函 (d) 第4类白化权函 (e) 第5类白化权函

图 3 5 类灰数的白化权函数

(6) 确立灰色权矩阵

利用$f_k(d_{Vi})$算出准则层要素 J 对于评估指标属于第 K 类的灰色评估系数 n_{Vi}^{k}:

$$n_{Vi}^{k} = f_k(d_{Vi}) \tag{3}$$

由 n_{Vi}^{k} 得各要素的灰色系数 V_i:

$$V_i = [f_1(d_{Vi}) \quad f_2(d_{Vi}) \quad f_3(d_{Vi}) \quad f_4(d_{Vi}) \quad f_5(d_{Vi})]$$

首先对 V_i 进行归一化处理得各要素的灰色评估权矩阵$\boldsymbol{R}_{Vi}$,再由$\boldsymbol{R}_{Vi}$组成矩阵$\boldsymbol{R}$,$\boldsymbol{R}$ 为准则层评估权矩阵,

$$\boldsymbol{R} = [\boldsymbol{R}_{V1}, \boldsymbol{R}_{V2}, \cdots, \boldsymbol{R}_{Vi}]^{T}$$

由$\boldsymbol{R}$ 和$\boldsymbol{W}_i$可确定目标层的灰色权矩阵$\boldsymbol{M}$:

$$\boldsymbol{M} = \boldsymbol{W}_i \cdot \boldsymbol{R} \tag{4}$$

(7) 最终评估结果

根据最大隶属原则,由矩阵$\boldsymbol{R}_{Vi}$可得准则层各要素的级别,由矩阵$\boldsymbol{M}$ 可知目标层的最终等级。

2 应用实例

根据信息安全灰色层次分析评估模型,用某证券运营公司作为实例。该证券公司是负责维护证券交易所运行的公司,其业务严重依赖于 IT 技术及计算机网络,并且拥有大量的需

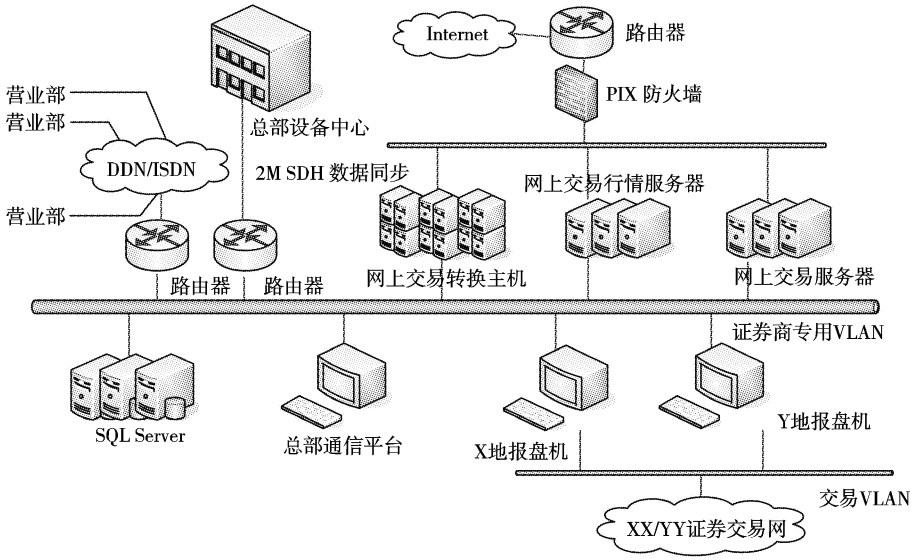


图 4 某证券通信有限公司运营图

要保密的数据,如交易数据、系统运行参数等,该公司的运营图如图 4 所示。

(1) 本例有 5 组专家评估,专家组权重 $\boldsymbol{P}$ 为,$\boldsymbol{P} = (p_1, p_2, \cdots, p_5)^T = (0.2\ 0.2\ 0.3\ 0.2\ 0.1)^T$。

(2) 专家进行判定,得 7 要素评估矩阵 $\boldsymbol{P}_i$,$\boldsymbol{P}_i$ 行代表 7 个信息安全要素:[网络应用安全,人事安全,物理安全,资产安全,策略与风险控制,管理安全, 组织体系],列代表 7 受评者对于信息安全的相对重要性等级:[最重要,相邻中值,很重要,相邻中值,比较重要,相邻中值,稍微重要,相邻中值,不重要]。同理,设矩阵行为信息安全 3 属性:[机密性,完整性,可用性],列表示 3 属性对信息安全 7 要素中具体要素相对重要性等级(等级划分同上文),以此建立 3 属性评估矩阵 $\boldsymbol{P}_{ij}$。

以网络应用安全为例得 $\boldsymbol{P}_{1j}$:

$$\boldsymbol{P}_i = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \boldsymbol{P}_{1j} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

由评估矩阵 $\boldsymbol{P}_i$ 可得 7 信息安全要素的判断矩阵 $\boldsymbol{A}$,由 $\boldsymbol{P}_{1j}$ 可得评估 3 属性的判断矩阵 $\boldsymbol{A}_1$。

$$\boldsymbol{A} = \begin{bmatrix} 1 & 2 & 1 & 3 & 4 & 2 & 4 \\ 1/2 & 1 & 1/2 & 2 & 3 & 1 & 3 \\ 1 & 2 & 1 & 3 & 4 & 2 & 4 \\ 1/3 & 1/2 & 1/3 & 1 & 2 & 1/2 & 2 \\ 1/4 & 1/3 & 1/4 & 1/2 & 1 & 1/3 & 1 \\ 1/2 & 1 & 1/2 & 2 & 3 & 1 & 3 \\ 1/4 & 1/3 & 1/4 & 1/2 & 1 & 1/3 & 1 \end{bmatrix}$$

$$\boldsymbol{A}_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1/2 & 1 & 2 \\ 1/3 & 1/2 & 1 \end{bmatrix}$$

由矩阵 $\boldsymbol{A}$,采用 AHP 和法可得 7 要素对于信息安全的权重矩阵 $\boldsymbol{W}_i$:

$$\boldsymbol{W}_i = (w_1, w_2, \cdots, w_7)^T = (0.2536\ 0.1483\ 0.2536\ 0.0884\ 0.539\ 0.1483\ 0.539)^T$$

由矩阵 $\boldsymbol{A}_1$ 可得相对于网络应用安全,3 属性的权重矩阵 $\boldsymbol{W}_{1j}$:

$$\boldsymbol{W}_{1j} = (w_{11}, w_{12}, w_{13})^T = (0.5390\ 0.2973\ 0.1638)^T$$

同理可得 3 属性其他权重矩阵 $\boldsymbol{W}_{ij}(i = 2,3,\cdots,7)$。

(3) 假设 5 组专家对网络应用安全(以 3 属性为判断依据)进行评分,评分矩阵为 $\boldsymbol{D}_{1I}^A$:

$$\boldsymbol{D}_{1I}^A = [\boldsymbol{D}_{1I}^1, \boldsymbol{D}_{1I}^2, \boldsymbol{D}_{1I}^3, \boldsymbol{D}_{1I}^4, \boldsymbol{D}_{1I}^5] = \begin{bmatrix} 4 & 4 & 5 \\ 3 & 3 & 4 \\ 4 & 4 & 4 \\ 3 & 4 & 3 \\ 4 & 3 & 4 \end{bmatrix}$$

由此,网络应用安全这一要素的 3 个属性的得分矩阵为 $\boldsymbol{D}_1^A$:

$$\boldsymbol{D}_1^A = \begin{bmatrix} \text{机密性} & \text{完整性} & \text{可用性} \\ d_1 & d_2 & d_3 \end{bmatrix} = \boldsymbol{P} \times \boldsymbol{D}_{1I}^A = [3.6\ 3.7\ 4.0]$$

同理得其余 6 个要素的得分矩阵 $\boldsymbol{D}_2^A, \boldsymbol{D}_3^A, \cdots, \boldsymbol{D}_7^A$。

(4) 因为受评要素初始评估分数 $d_{Vi} = \boldsymbol{D}_i^A \times \boldsymbol{W}_{ij}$,则网络应用安全的初始得分 d_{V1} 为:

$$d_{V1} = \boldsymbol{D}_1^A \times \boldsymbol{W}_{1j} = [4.4\ 4.3\ 3.8] \cdot [0.5390\ 0.2973\ 0.1638]^T = 3.6956(\text{分})$$

同理可得其余 6 个要素初始评估分 $d_{V2}, d_{V3}, \cdots, d_{V7}$。

(5) 网络应用安全对评估指标属于各灰色系数为 V_1:

$$V_1 = [f_1(d_{V1})\ f_2(d_{V1})\ f_3(d_{V1})\ f_4(d_{V1})\ f_5(d_{V1})] = [0.4106\ 0.4620\ 0.6159\ 0.9239\ 0]$$

对 V_1 进行归一化处理得网络应用安全的灰色评估权矩阵:

$$\boldsymbol{R}_{V1} = [0.1702\ 0.1915\ 0.2553\ 0.3830\ 0]$$

同理可得 $\boldsymbol{R}_{V2}, \cdots, \boldsymbol{R}_{V7}$。

当 $\boldsymbol{R}_{V2}, \cdots, \boldsymbol{R}_{V7}$ 已知,则矩阵 $\boldsymbol{R}$ 为:

$$\boldsymbol{R} = [\boldsymbol{R}_{V1}\ \boldsymbol{R}_{V2}\ \cdots\ \boldsymbol{R}_{V7}]^T = \begin{bmatrix} 0.1702 & 0.1915 & 0.2553 & 0.3830 & 0 \\ 0.0942 & 0.1060 & 0.1414 & 0.2120 & 0.4464 \\ 0.1617 & 0.1819 & 0.2425 & 0.3638 & 0.0502 \\ 0.1303 & 0.1466 & 0.1955 & 0.2931 & 0.2345 \\ 0.1093 & 0.1230 & 0.1640 & 0.2460 & 0.3577 \\ 0.1702 & 0.1915 & 0.2553 & 0.3830 & 0 \\ 0.0964 & 0.1084 & 0.1446 & 0.2169 & 0.4337 \end{bmatrix}$$

则受评机构总灰色权矩阵 $\boldsymbol{M}$ 为:

$$\boldsymbol{M} = \boldsymbol{W}_i \cdot \boldsymbol{R} = [0.1460\ 0.1642\ 0.2190\ 0.3285\ 0.1423]$$

(6) 评估结果

根据最大隶属原则,由矩阵 $\boldsymbol{R}_{V1}$ 可得网络应用安全的级别为丁。同理,由 $\boldsymbol{R}_{V2}, \boldsymbol{R}_{V3}, \cdots, \boldsymbol{R}_{V7}$ 可判断其他各受评对象的具体等级。由矩阵 $\boldsymbol{M}$(同样根据最大隶属原则)可知受评机构的级别为丁。进一步可得受评机构总体得分状况 N(10 分制):

$$N = \boldsymbol{M} \times C^T = [0.1460\ 0.1642\ 0.2190\ 0.3285\ 0.1423] \cdot [10\ 8\ 6\ 4\ 2]^T = 5.6862(\text{分}) \qquad (5)$$

3 结语

针对信息安全评估,总结出了 7 要素准则层和 3 属性指标层的信息安全层次结构,又提出了基于灰色层次分析法的信息安全评估模型。计算过程运用了 AHP、灰色系统理论等,最大限度减少人为失误带来的损失,步骤清晰,有一定的可操作性。为某证券交易公司进行评估,结果得到对方公司的认可,有一定的实际应用价值。

参考文献:

[1] SAATY TL. The Analytic Hierarchy Process [M]. New York: McGraw-Hill Inco, 1980.

[2] 赵焕臣, 许树柏, 和金生. 层次分析法[M]. 北京: 科学出版社, 1986.

[3] 邓聚龙. 灰预测与灰决策[M]. 武汉: 华中科技大学出版社, 2002. 17 - 44.

[4] 刘思峰, 党耀国, 张岐山. 灰色系统理论及其应用[M]. 北京: 科学出版社, 1999.

[5] ISO/IEC 17799: 2000. 信息技术・信息安全管理实用规则[S].

[6] GB 17859: 1999 计算机信息系统・安全保护等级划分规则[S].

[7] GB/T 18336: 2001. 信息技术、安全技术・信息技术安全性评估准则[S].

[8] GB/T 19715: 2005. 信息技术・信息技术安全管理指南[S].

[9] 邓聚龙. 灰理论基础[M]. 武汉: 华中科技大学出版社, 2002. 61 - 48.