·安全技术· 文章编号：1000-3428(2019)07-0194-09 文献标志码：A 中图分类号：TP309

基于 D-AHP 与灰色理论的信息安全风险评估

许 硕，唐作其，王 鑫

（贵州大学 计算机科学与技术学院，贵阳 550025）

摘 要： 充分考虑评估信息不确定性对评估结果的影响，提出一种基于 D 数层次分析法（D-AHP）与灰色理论的信息安全风险评估方法。根据相关行业标准识别信息系统的资产、威胁、脆弱性及已有安全措施，构建评估指标体系并建立层次化结构模型。使用 D-AHP 方法求解各指标的影响权重，以解决评估信息不确定性问题。针对评估过程中信息资源不足的灰性特征，运用灰色理论求解灰色评价矩阵。在此基础上，对信息安全风险进行综合评估并直观显示评估结果。分析表明，该方法可利用不确定信息进行风险评估，为制定有针对性的风险管控策略提供参考。

关键词： 信息安全风险评估；D 数理论；D 数层次分析法；灰色理论；模糊偏好关系

中文引用格式： 许硕，唐作其，王鑫. 基于 D-AHP 与灰色理论的信息安全风险评估[J]. 计算机工程，2019，45(7)：194-202.

英文引用格式： XU Shuo，TANG Zuoqi，WANG Xin. Information security risk assessment based on D-AHP and grey theory[J]. Computer Engineering，2019，45(7)：194-202.

Information Security Risk Assessment Based on D-AHP and Grey Theory

XU Shuo，TANG Zuoqi，WANG Xin

（College of Computer Science and Technology，Guizhou University，Guiyang 550025，China）

【Abstract】 Fully considering the influence of uncertainty of evaluation information on evaluation results，an information security risk assessment method based on D-number Analytic Hierarchy Process（D-AHP） and grey theory is proposed. According to the relevant industry standards，the assets，threats，vulnerabilities and existing security measures of information system are identified，the evaluation index system is constructed，and the hierarchical structure model is established. The D-AHP method is used to calculate the influence weights of each index to solve the uncertainty problem of the evaluation information. In view of the grey characteristics of insufficient information resources in the evaluation process，the grey theory is used to solve the grey evaluation matrix. On this basis，the information security risk is assessed comprehensively and the assessment results are displayed intuitively. Analysis show that this method can use uncertain information for risk assessment and provide reference for formulating targeted risk management and control strategies.

【Key words】 information security risk assessment；D-number theory；D-number Analytic Hierarchy Process（D-AHP）；grey theory；fuzzy preference relation

DOI：10.19678/j.issn.1000-3428.0052209

0 概述

信息技术水平的提高促进了社会经济的发展，但同时也使信息安全面临巨大挑战。据统计，因信息安全事件造成的经济损失逐年攀升。风险评估作为保障信息安全的重要措施，已成为国内外学者广泛关注的热点之一[1-2]。

文献[3]基于统计数据与专家经验，通过贝叶斯网络定义信息安全风险要素之间的因果关系，计算概率最高的系统脆弱性传播路径和最大风险估计值。但是，在风险评估过程中，其较难确定贝叶斯网络模型的条件概率。文献[4]使用改进的 Dempster 合成规则进行信息安全风险评估，该方法不仅可以求得各风险要素的权重，而且还可利用合成规则量化系统的总体风险值，从而有效消除网络环境中的不确定性与随机性对评估结果的影响，提高评估的客观性。但是，由于使用证据理论时需假设识别框架为互斥的有限集，导致该方法使用范围有限。文献[5]使用模糊层次分析法（Fuzzy-Analytical Hierarchy Process，F-AHP）对信息系统进行风险评估，其能较客观地反映系统内部层次结构间的关系，通过定性

基金项目： 贵州省科技计划项目（黔科合平台人才[2018]5616）；贵州大学青年教师科研基金项目（贵大青合字(2013)01 号）。

作者简介： 许 硕（1993—），男，硕士研究生，主研方向为信息安全；唐作其（通信作者），副教授；王 鑫，硕士研究生。

收稿日期： 2018-07-25 **修回日期：** 2018-08-30 **E-mail：** zqtang@gzu.edu.cn

分析与定量评估相结合,在一定程度上消除评估信息的模糊性,提高评估精度。但该方法在构建专家评估矩阵时,未考虑专家经验的差异性对评估结果的影响。文献[6]通过灰色网络分析法进行信息安全风险评估,该方法能较好反映风险要素互相依赖、互相影响的关系,可利用有限的信息资源计算出量化的评估结果,但在评估信息不完整的情况下,无法通过该方法求解各评估指标的权重。

针对上述问题,本文提出一种基于 D 数层次分析法(D-number Analytic Hierarchy Process,D-AHP)与灰色理论的信息安全风险评估方法。由于评估结果高度依赖评估专家的主观判断,且专家经验的差异性通常会导致评估信息的不确定性,因此,利用 D 数理论处理不确定性问题时的优势对模糊偏好关系进行改进,将其使用范围扩展至不确定信息领域。将 D 数偏好关系与层次分析法(Analytic Hierarchy Process,AHP)相结合得到 D-AHP 算法,保留 AHP 在对复杂系统进行分析时计算简单、层次逻辑清晰的优势,以使求得的指标权重更科学合理,降低人为主观性对评估结果的影响。在此基础上,通过灰色理论来提高评估精度。

1　信息安全风险评估指标体系构建

1.1　信息安全风险评估

信息安全风险评估依据有关管理要求和技术标准,对信息系统及由其处理、传输和存储的信息的保密性(Confidentiality,C)、完整性(Integrity,I)及可用性(Availability,A)等安全属性进行综合评价。信息安全风险评估通过评估资产面临的威胁以及安全事件发生的可能性,判断安全事件一旦发生将对社会造成的影响[7]。信息安全风险评估流程如图 1 所示。

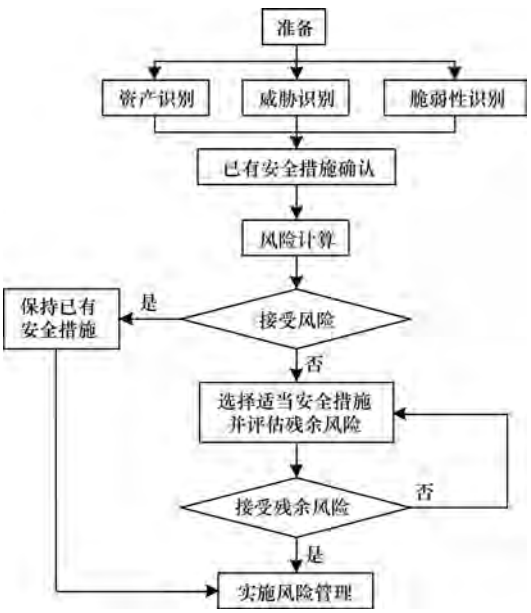

图 1　信息安全风险评估流程

信息安全风险评估涉及资产、威胁、脆弱性以及已有安全措施四大要素。其中,资产具有价值属性。在对资产进行识别后,要对其保密性、完整性和可用性进行赋值。威胁的来源途径可分为环境因素与人为因素,威胁可以通过直接或间接的方式对系统产生影响,在机密性、完整性或可用性等方面对资产造成危害。脆弱性为资产本身固有属性,只有脆弱性被威胁利用,才会对资产造成损害。资产脆弱性可分为技术脆弱性与管理脆弱性 2 类。安全措施分为预防性安全措施和保护性预防措施,系统的已有安全措施确认和脆弱性识别存在一定联系,安全措施的使用将减少资产在技术或管理上的脆弱性。

1.2　指标体系构建

信息安全风险评估的过程较复杂,本文根据 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》[7],结合信息系统实际情况,选取评估指标,建立信息安全评估指标体系。为突出评估重点,对评估指标体系进行适当简化,将资产(U_1)、威胁(U_2)、脆弱性(U_3)和已有安全措施(U_4)设为一级指标,根据这 4 个一级指标遴选出对应的 9 个二级指标。本文构建的信息安全风险评估指标体系如表 1 所示。

表 1　信息安全风险评估指标体系

一级指标	二级指标	描述
资产(U_1)	机密性(U_{11})	数据所达到的未提供或未泄露给非授权的个人、过程或者其他实体的程度
	完整性(U_{12})	保证信息系统不会被非授权用户更改或破坏的特性
	可用性(U_{13})	数据或资源的特性,被授权实体按要求能访问和使用的数据或资源
威胁(U_2)	环境因素(U_{21})	包括自然界不可抗因素和其他物理因素
	人为因素(U_{22})	相关人员有意或无意导致系统故障,造成损失
脆弱性(U_3)	技术脆弱性(U_{31})	涉及物理层、网络层、系统层、应用层等各个层面的安全问题
	管理脆弱性(U_{32})	分为技术管理脆弱性和组织管理脆弱性,前者与具体技术活动有关,后者与管理环境有关
已有安全措施(U_4)	预防性安全措施(U_{41})	预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性
	保护性安全措施(U_{42})	保护性安全措施可以减少安全事件发生后对社会造成的影响

2 理论基础

2.1 D-S 证据理论

D-S 证据理论[8]于 1967 年被提出,通常被用来处理不确定性信息,目前在人工智能、信息融合与模式识别等领域具有广泛应用。D-S 证据理论具有以下优势:

1)证据理论既可以处理由随机性导致的不确定性问题,也可以处理由模糊性导致的不确定性问题。

2)与概率论相比,证据理论无需先验概率和条件概率密度。

3)证据理论可以将证据或信任函数合成为新的证据和信任函数。

但是,使用该理论时也存在一定局限,如需假设识别框架为互斥的有限集,这在一定程度上限制了证据理论的使用范围。

2.2 D 数理论

D 数理论[9]于 2012 年被提出,其是对 D-S 证据理论的改进。D 数理论继承了证据理论在处理不确定性信息时的优势,且能够避免证据理论的使用局限性。D 数理论不再要求识别框架中命题之间的互斥性假设和基本概率分配(Basic Probability Allocation, BPA)的完整性约束,可以更好地处理不确定性问题。目前,该理论已在多个领域进行应用,如投资决策[10]、故障模式与影响分析[11]、桥梁状态评估[12]、高校科研能力评估[13]以及帷幕灌浆效率评估[14]等。D 数的定义和性质如下[9]:

设存在一个有限非空集 Ω 与映射 D:

$$D:\Omega\rightarrow[0,1] \tag{1}$$

即:

$$\sum_{B\subseteq\Omega}D(B)\leqslant 1,D(\theta)=0 \tag{2}$$

则称映射 D 为 D 数,其中,B 是 Ω 的一个子集,θ 是空集。若 $\sum_{B\subseteq\Omega}D(B)=1$,则说明由 D 数表示的信息完整;若 $\sum_{B\subseteq\Omega}D(B)<1$,则说明信息不完整。

设存在一个 D 数 D 和非空有限集 Ω,则 D 的信息完整度 Q 可量化表示为:

$$Q=\sum_{B\subseteq\Omega}D(B) \tag{3}$$

设离散集 $\Omega=\{b_1,b_2,\cdots,b_i,\cdots,b_n\}$,则 D 数的特殊表达形式为:

$$\begin{aligned}&D(\{b_1\})=v_1\\&D(\{b_2\})=v_2\\&\quad\vdots\\&D(\{b_i\})=v_i\\&\quad\vdots\\&D(\{b_n\})=v_n\end{aligned} \tag{4}$$

也可简单表示为:

$$D=\{(b_1,v_1),(b_2,v_2),\cdots,(b_i,v_i),\cdots,(b_n,v_n)\} \tag{5}$$

其中,$v_i>0$ 且 $\sum_{i=1}^{n}v_i\leqslant 1$。

通过 D 数的上述表示形式,可以高效地描述不确定性问题。设存在 D 数:

$$D=\{(b_1,v_1),(b_2,v_2),\cdots,(b_i,v_i),\cdots,(b_n,v_n)\}$$

则其集成可表示为:

$$I(D)=\sum_{i=1}^{n}b_iv_i \tag{6}$$

2.3 模糊偏好关系

模糊偏好关系用符号“>”表示,其通过构造成对比较矩阵的方式,来表示专家对各评估对象的偏好。

设存在一组评估对象 $S=\{S_1,S_2,\cdots,S_n\}$,其模糊偏好关系为:

$$\mu_R:S\times S\rightarrow[0,1] \tag{7}$$

用矩阵的形式表示为 $\boldsymbol{R}=[r_{ij}]_{n\times n}$:

$$\boldsymbol{R}=\begin{bmatrix}r_{11}&r_{12}&\cdots&r_{1n}\\r_{21}&r_{22}&\cdots&r_{2n}\\\vdots&\vdots&&\vdots\\r_{n1}&r_{n2}&\cdots&r_{nn}\end{bmatrix} \tag{8}$$

该矩阵满足:

1)$r_{ij}\geqslant 0$。

2)$r_{ij}+r_{ji}=1,\forall i,j\in\{1,2,\cdots,n\}$。

3)$r_{ii}=0.5,\forall i\in\{1,2,\cdots,n\}$。

其中,r_{ij}表示专家对 S_i相对于 S_j的重要性的偏好程度。r_{ij}的赋值及对应含义如下:

$$\begin{cases}r_{ij}=0,S_j\text{ 比 }S_i\text{ 绝对重要}\\r_{ij}\in(0,0.5),S_j\text{ 比 }S_i\text{ 重要一些}\\r_{ij}=0.5,S_i\text{ 和 }S_j\text{ 同等重要}\\r_{ij}\in(0.5,1),S_i\text{ 比 }S_j\text{ 重要一些}\\r_{ij}=1,S_i\text{ 比 }S_j\text{ 绝对重要}\end{cases}$$

在专家评估信息不完整或不确定的情况下,无法构造出合理的偏好矩阵。因此,模糊偏好关系的使用受到一定限制。本文引用文献[15]中的一个假设:10 名专家对 2 个对象 S_1、S_2进行评估,结果分为以下 2 种情况:

1)经过评估,8 名专家认为 S_1比 S_2重要,且重要程度为 0.7。剩余 2 名专家同样认为 S_1比 S_2重要,但重要程度为 0.6。

2)经过评估,6 名专家认为 S_1比 S_2重要,重要程度为 0.8,但剩余 4 名专家出于谨慎态度,未对 S_1、S_2之间的重要程度进行置评。

上述 2 种情况均无法通过模糊偏好关系进行表示。

2.4　D 数偏好关系

针对模糊偏好关系存在的局限性,文献[15]提出一种 D 数偏好关系的理论。D 数偏好关系利用 D 数理论对模糊偏好关系进行扩展,将偏好关系的适用范围扩大到不确定信息领域,其对应的矩阵称为 D 数偏好矩阵,简称为 D 矩阵。

设存在一组评估对象 $S=\{S_1,S_2,\cdots,S_n\}$,其 D 数偏好关系为:

$$R_D: S\times S\rightarrow D \tag{9}$$

用六矩阵形式表示为 $\boldsymbol{R}_D=[D_{ij}]_{n\times n}$:

$$\boldsymbol{R}_D=\begin{bmatrix} D_{11} & D_{12} & \cdots & D_{1n} \\ D_{21} & D_{22} & \cdots & D_{2n} \\ \vdots & \vdots & & \vdots \\ D_{n1} & D_{n2} & \cdots & D_{nn} \end{bmatrix} \tag{10}$$

该矩阵满足:

1) $D_{ij}=\{(b_1^{ij},v_1^{ij}),(b_2^{ij},v_2^{ij}),\cdots,(b_m^{ij},v_m^{ij})\}$, $D_{ji}=\{(1-b_1^{ij},v_1^{ij}),(1-b_2^{ij},v_2^{ij}),\cdots,(1-b_m^{ij},v_m^{ij})\}$, $\forall i,j\in\{1,2,\cdots,n\}$。

2) $b_k^{ij}\in[0,1]$, $\forall k\in\{1,2,\cdots,m\}$。

3) $D_{ii}=\{(0.5,1.0)\}$, $\forall i\in\{1,2,\cdots,n\}$。

其中,b_k^{ij} 表示第 k 位专家认为第 i 个方案相对于第 j 个方案的重要程度,v_k^{ij} 表示专家对该重要程度的支持度。

根据 D 数偏好关系,前文假设的 2 种情况可分别表示为:

$$\boldsymbol{R}_{D1}=\begin{bmatrix} \{(0.5,1.0)\} & \{(0.7,0.8),(0.6,0.2)\} \\ \{(0.3,0.8),(0.4,0.2)\} & \{(0.5,1.0)\} \end{bmatrix}$$

$$\boldsymbol{R}_{D2}=\begin{bmatrix} \{(0.5,1.0)\} & \{(0.8,0.6)\} \\ \{(0.2,0.6)\} & \{(0.5,1.0)\} \end{bmatrix}$$

2.5　D-AHP 方法

AHP 是一种处理复杂评估问题的结构化方法,其将系统分解成各因素,通过自上而下的层次结构与相对标度,以成对比较的方式将定性判断与定量分析结合到评估决策过程中。AHP 方法通常分为 3 个步骤:

步骤 1　分析系统因素之间的关系,建立层次结构模型。

步骤 2　参考赋值标准,对相同层次中各因素相对于上层次中某一因素的重要性进行成对比较并构建判断矩阵,由判断矩阵计算该因素相对于准则的权重。

步骤 3　计算各方案相对于目标的权重,并按重要程度对各方案进行排序。

但典型 AHP 方法不适用于处理存在不确定信息的主观评价问题。通过 D 数偏好关系对 AHP 进行改进,得到 D-AHP 方法[15],该方法可以更好地应用于不确定环境下的复杂评估决策问题。D-AHP 的结构可分为 3 个层次:目标层,准则层,方案层。层次结构如图 2 所示。

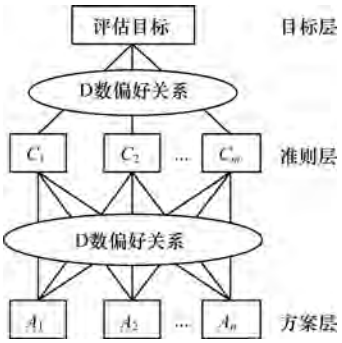

图 2　D-AHP 层次结构

目标层包括决策评估问题的总目标,准则层包括在评估过程中需要考虑的各级指标,方案层由具有各项评估指标的备选方案组成。

2.6　灰色理论

灰色理论[16]广泛应用于结构复杂、难以从定量角度建立精确模型的系统研究,在信息资源不足的情况下,其可以较好地解决评估指标难量化和难统计的问题,使评估结果更精确客观。

在灰色理论中,将取值在某个区间的不确定数称为灰数,用符号"⊗"表示。灰数的可能取值称为白化值,通过白化权函数的形式表达白化值与白化权重之间的关系,进而确定灰数隶属的灰类。针对信息安全风险评估内涵外延均不明确的灰性特征,在评估信息数据少、不确定时,可以使用灰色理论进行分析。

3　信息安全风险评估模型构建

3.1　风险评估层次结构模型

根据 1.2 节构建的评估指标体系,结合信息安全风险评估实际情况,充分考虑评估指标之间的隶属关系,根据已确定的风险评估指标体系,构建信息安全风险评估层次结构模型。其中,信息安全风险为目标层元素,资产、威胁、脆弱性、已有安全措施 4 个一级指标以及机密性、完整性、可用性等 9 个二级指标共同构成准则层。信息安全风险评估层次结构模型如图 3 所示。

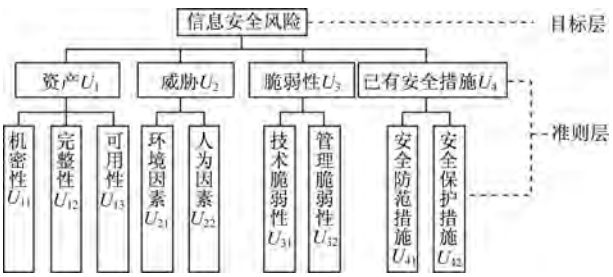

图 3　信息安全风险评估层次结构模型

3.2 评估指标权重计算

为定量表示指标之间的相对重要性,采用 0.1 ~ 0.9 标度对指标权重进行成对比较赋值。各标度及对应含义如表 2 所示。

表 2 标度及含义

标度	含义
0.1,0.2,0.3,0.4	反比较,若指标 U_i 与指标 U_j 的重要性之比为 r_{ij},则指标 U_j 与指标 U_i 的重要性之比 r_{ji} 为 $1-r_{ij}$
0.5	两指标相比,同等重要
0.6	两指标相比,前者比后者稍重要
0.7	两指标相比,前者比后者明显重要
0.8	两指标相比,前者比后者强烈重要
0.9	两指标相比,前者比后者极端重要

在使用 D-AHP 方法时,首先通过 D 数偏好关系求解指标权重,再结合 AHP 层次结构对指标权重进行逐层集成,最终求得综合权重。

使用 D 数偏好关系求解指标权重的步骤如下:

步骤 1 组织参评专家,参考上述评估标度对指标进行成对比较,通过偏好关系表示指标相对于评估目标的重要程度,并构建 D 数偏好矩阵 $\boldsymbol{R}_D$。

步骤 2 根据 D 数的集成表示,将 D 数偏好矩阵转化为确定数矩阵 $\boldsymbol{R}_C$。

步骤 3 构建基于确定数矩阵 $\boldsymbol{R}_C$ 的概率矩阵 $\boldsymbol{R}_P$,计算成对比较的指标间的偏好概率。

步骤 4 将概率矩阵 $\boldsymbol{R}_P$ 转化为三角化概率矩阵 $\boldsymbol{R}_P^{\mathrm{T}}$,并对指标按重要程度进行排序。

步骤 5 根据指标排序结果,将确定数矩阵 $\boldsymbol{R}_C$ 表示为矩阵 $\boldsymbol{R}_C^{\mathrm{T}}$。计算各指标相对权重的详细过程参考文献[15]。

在权重的计算过程中,由式(11)计算 D 数偏好矩阵 $\boldsymbol{R}_D$ 的不一致度系数 $I.D.$:

$$I.D.=\frac{\sum_{i=1,j<i}^{n}\boldsymbol{R}_P^{\mathrm{T}}(i,j)}{n(n-1)/2} \tag{11}$$

其中,$\boldsymbol{R}_P^{\mathrm{T}}(i,j)$ 表示矩阵 $\boldsymbol{R}_P^{\mathrm{T}}$ 中的元素,n 表示成对比较的指标个数。

对各级指标权重进行逐层集成,求解综合权重的过程如下:

1)结合 D 数偏好关系计算结果,设准则层一级 U_i 相对于评估目标的权重向量为 $\boldsymbol{A}=(a_1,a_2,a_3,a_4)$,其中,$a_i$ 为 U_i 相对于评估目标的权重,$a_i\geqslant 0$ 且 $\sum_{i=1}^{4}a_i=1$。

2)设二级指标 U_{ij} 相对于 U_i 的权重向量为 $\boldsymbol{B}_i=(b_{i1},b_{i2},\cdots,b_{in_i})$,其中,$b_{ij}$ 表示 U_{ij} 相对于 U_i 的权重,$b_{ij}\geqslant 0$ 且 $\sum_{j=1}^{n_i}b_{ij}=1$,n_i 表示一级指标 U_i 下所对应的二级指标 U_{ij} 的个数。

3)设 U_{ij} 相对于评估目标的综合权重集 $\boldsymbol{W}=(w_{11},w_{12},\cdots,w_{ij},\cdots,w_{41},\cdots,w_{4n_i})$,其中,$w_{ij}=a_ib_{ij}$ 表示 U_{ij} 相对于评估目标的综合权重,$w_{ij}\geqslant 0$ 且 $\sum_{i=1}^{4}\sum_{j=1}^{n_i}a_ib_{ij}=1$。

3.3 白化权函数与灰色评价矩阵

3.3.1 样本评价矩阵构建

根据已建立的评估指标体系,确定风险评估等级向量 $\boldsymbol{V}=(v_1,v_2,\cdots,v_t)$,其中,$t$ 表示风险等级个数。采用专家打分法,组织 p 位专家参考评估等级向量 $\boldsymbol{V}$ 对各指标进行独立打分。设第 q 位专家对准则层一级指标 U_i 的第 j 个二级指标的评价值为 $d_{ij}^{(q)}$,最终得到样本评价矩阵 $\boldsymbol{D}$ 为:

$$\boldsymbol{D}=\begin{bmatrix} d_{11}^{(1)} & d_{12}^{(1)} & \cdots & d_{ij}^{(1)} & \cdots & d_{nn_i}^{(1)} \\ d_{11}^{(2)} & d_{12}^{(2)} & \cdots & d_{ij}^{(2)} & \cdots & d_{nn_i}^{(2)} \\ \vdots & \vdots & & \vdots & & \vdots \\ d_{11}^{(q)} & d_{12}^{(q)} & \cdots & d_{ij}^{(q)} & \cdots & d_{nn_i}^{(q)} \\ \vdots & \vdots & & \vdots & & \vdots \\ d_{11}^{(p)} & d_{12}^{(p)} & \cdots & d_{ij}^{(p)} & \cdots & d_{nn_i}^{(p)} \end{bmatrix}$$

$$i=1,2,\cdots,n,j=1,2,\cdots,n_i,q=1,2,\cdots,p \tag{12}$$

3.3.2 白化权函数确定

典型的白化权函数有以下 3 种,用于在灰色统计法中构建灰色评价矩阵。

1)上类白化权函数,即 $\otimes\in[d_1,+\infty)$,其定义如下:

$$f_1(d_{ij}^{(q)})=\begin{cases}\dfrac{d_{ij}^{(q)}}{d_1},d_{ij}^{(q)}\in[0,d_1)\\ 1,d_{ij}^{(q)}\in[d_1,+\infty)\\ 0,d_{ij}^{(q)}\in(-\infty,0)\end{cases} \tag{13}$$

2)中类白化权函数,即 $\otimes\in[0,d_1,2d_1]$,其定义如下:

$$f_2(d_{ij}^{(q)})=\begin{cases}\dfrac{d_{ij}^{(q)}}{d_1},d_{ij}^{(q)}\in[0,d_1)\\ \dfrac{2-d_{ij}^{(q)}}{d_1},d_{ij}^{(q)}\in[d_1,2d_1]\\ 0,d_{ij}^{(q)}\notin[0,2d_1]\end{cases} \tag{14}$$

3)下类白化权函数,即 $\otimes\in[0,d_1,d_2]$,其定义如下:

$$f_3(d_{ij}^{(q)})=\begin{cases}1,d_{ij}^{(q)}\in[0,d_1)\\ \dfrac{d_2-d_{ij}^{(q)}}{d_2-d_1},d_{ij}^{(q)}\in[d_1,d_2]\\ 0,d_{ij}^{(q)}\notin[0,d_2]\end{cases} \tag{15}$$

3.3.3　灰色评价矩阵构建

设共有 E 个灰类,通过灰色统计法,确定白化权函数 f_e,计算评价样本 $d_{ij}^{(q)}$ 属于第 $e(e=1,2,\cdots,E)$ 个灰类的白化权值 $f_e(d_{ij}^{(q)})$,从而得到指标 U_{ij} 隶属于第 e 个灰类的灰色统计数 $n_{ij}^{(e)}$ 以及总灰色统计数 n_{ij} 分别如下:

$$n_{ij}^{(e)}=\sum_{q=1}^{p}f_e(d_{ij}^{(q)}) \tag{16}$$

$$n_{ij}=\sum_{e=1}^{E}n_{ij}^{(e)} \tag{17}$$

根据灰色统计数及总灰色统计数,可计算灰色评价权 $z_{ij}^{(e)}$ 为:

$$z_{ij}^{(e)}=\frac{n_{ij}^{(e)}}{n_{ij}} \tag{18}$$

其中,$z_{ij}^{(e)}$ 的值表示所有专家主张 U_{ij} 属于第 e 个灰类的强烈程度,由 $z_{ij}^{(e)}$ 可得 U_{ij} 对于各评价灰类的灰色评价权向量 $\boldsymbol{Z}_i=(z_{ij}^{(1)},z_{ij}^{(2)},\cdots,z_{ij}^{(e)},\cdots,z_{ij}^{(E)})$,进而构建指标 U_{ij} 关于各评价灰类的灰色评价矩阵 $\boldsymbol{Z}$:

$$\boldsymbol{Z}=\begin{bmatrix}\boldsymbol{Z}_1\\ \boldsymbol{Z}_2\\ \vdots\\ \boldsymbol{Z}_i\\ \vdots\\ \boldsymbol{Z}_n\end{bmatrix}=\begin{bmatrix}z_{11}^{(1)} & z_{11}^{(2)} & \cdots & z_{11}^{(e)} & \cdots & z_{11}^{(E)}\\ z_{12}^{(1)} & z_{12}^{(2)} & \cdots & z_{12}^{(e)} & \cdots & z_{12}^{(E)}\\ \vdots & \vdots & & \vdots & & \vdots\\ z_{ij}^{(1)} & z_{ij}^{(2)} & \cdots & z_{ij}^{(e)} & \cdots & z_{ij}^{(E)}\\ \vdots & \vdots & & \vdots & & \vdots\\ z_{nn_i}^{(1)} & z_{nn_i}^{(2)} & \cdots & z_{nn_i}^{(e)} & \cdots & z_{nn_i}^{(E)}\end{bmatrix}$$

$$i=1,2,\cdots,n,e=1,2,\cdots,E \tag{19}$$

3.4　综合评估

根据D数偏好关系求得的三角化实数矩阵 $\boldsymbol{R}_C^{\mathrm{T}}$,

$$\boldsymbol{R}_D=\begin{bmatrix}\{(0.50,1.00)\} & \{(0.10,1.00)\} & \{(0.70,1.00)\} & \{(0.60,0.60),(0.70,0.40)\}\\ \{(0.90,1.00)\} & \{(0.50,1.00)\} & \{(0.70,1.00)\} & \{(0.60,0.80)\}\\ \{(0.30,1.00)\} & \{(0.30,1.00)\} & \{(0.50,1.00)\} & \{(0.80,1.00)\}\\ \{(0.40,0.60),(0.30,0.40)\} & \{(0.40,0.80)\} & \{(0.20,1.00)\} & \{(0.50,1.00)\}\end{bmatrix}$$

2)按 D 数集成表示,将 $\boldsymbol{R}_D$ 转化为确定数矩阵 $\boldsymbol{R}_C$,其表达式如下:

$$\boldsymbol{R}_C=I(\boldsymbol{R}_D)=\begin{bmatrix}0.50\times1.00 & 0.10\times1.00 & 0.70\times1.00 & 0.36+0.28\\ 0.90\times1.00 & 0.50\times1.00 & 0.70\times1.00 & 0.60\times0.80\\ 0.30\times1.00 & 0.30\times1.00 & 0.50\times1.00 & 0.80\times1.00\\ 0.24+0.12 & 0.40\times0.80 & 0.20\times1.00 & 0.50\times1.00\end{bmatrix}=\begin{bmatrix}0.50 & 0.10 & 0.70 & 0.64\\ 0.90 & 0.50 & 0.70 & 0.48\\ 0.30 & 0.30 & 0.50 & 0.80\\ 0.36 & 0.32 & 0.20 & 0.50\end{bmatrix}$$

3)在确定数矩阵 $\boldsymbol{R}_C$ 的基础上,构建概率矩阵 $\boldsymbol{R}_P$,其表达式如下:

$$\boldsymbol{R}_P=\begin{bmatrix}\Pr(U_1>U_1)=0.00 & \Pr(U_1>U_2)=0.00 & \Pr(U_1>U_3)=1.00 & \Pr(U_1>U_4)=1.00\\ \Pr(U_2>U_1)=1.00 & \Pr(U_2>U_2)=0.00 & \Pr(U_2>U_3)=1.00 & \Pr(U_2>U_4)=0.90\\ \Pr(U_3>U_1)=0.00 & \Pr(U_3>U_2)=0.00 & \Pr(U_3>U_3)=0.00 & \Pr(U_3>U_4)=1.00\\ \Pr(U_4>U_1)=0.00 & \Pr(U_4>U_2)=0.10 & \Pr(U_4>U_3)=0.00 & \Pr(U_4>U_4)=0.00\end{bmatrix}$$

4)通过三角化方法将概率矩阵 $\boldsymbol{R}_P$ 转化为 $\boldsymbol{R}_P^{\mathrm{T}}$:

$$\boldsymbol{R}_P^{\mathrm{T}}=\begin{bmatrix}0.00 & 1.00 & 1.00 & 0.90\\ 0.00 & 0.00 & 1.00 & 1.00\\ 0.00 & 0.00 & 0.00 & 1.00\\ 0.00 & 0.10 & 0.00 & 0.00\end{bmatrix}$$

对各指标进行排序:$U_2>U_1>U_3>U_4$,即信息安全风险重要程度由高到低的顺序为:威胁 U_2,资产 U_1,脆弱性 U_3,已有安全措施 U_4。

由式(11)通过矩阵 $\boldsymbol{R}_P^{\mathrm{T}}$ 计算 D 数偏好矩阵 $\boldsymbol{R}_D$ 的不一致度系数 $I.D.=0.016\,7$。经专家组讨论,对各指标按重要程度进行排序,同时结合指标权重,可有效识别出系统信息安全建设中的薄弱环节,为系统风险管理控制策略提供有针对性的建议。

根据 D-AHP 算法求得的权重向量 $\boldsymbol{W}$,以及通过灰色统计法求得的灰色评价矩阵 $\boldsymbol{Z}$,计算综合评价向量 $\boldsymbol{H}$:

$$\boldsymbol{H}=\boldsymbol{W}*\boldsymbol{Z} \tag{20}$$

将综合评价向量 $\boldsymbol{H}$ 和风险等级向量 $\boldsymbol{V}$ 相结合,可求得系统总体的信息安全风险评估值 $\boldsymbol{Risk}$:

$$\boldsymbol{Risk}=\boldsymbol{H}*\boldsymbol{V}^{\mathrm{T}} \tag{21}$$

在实际评估过程中,最直观的方式是以量化评估值的形式表示系统的风险状况,$\boldsymbol{Risk}$ 即为系统最终的风险评估值。结合风险评估等级向量 $\boldsymbol{V}$,可以确定系统的安全风险等级,从而为信息安全建设提供科学有效的参考依据。

4　实验结果与分析

4.1　评估指标权重

本文以某简化的信息系统为例,收集该系统实际运行数据并加以分析。在广泛调研的基础上,根据所建立的信息安全风险评估指标体系,通过问卷调查的形式收集专家评估数据,构建评估指标的 D 数偏好矩阵。以准则层一级指标为例,计算各指标相对于信息安全风险的权重:

1)为确定各一级指标关于信息安全风险的相对重要性,建立基于 D 数偏好关系的 D 数偏好矩阵 $\boldsymbol{R}_D$:

该 *I. D.* 值在可接受范围内。

5)根据指标排序将矩阵 $\boldsymbol{R}_C$ 表示为 $\boldsymbol{R}_C^{\mathrm{T}}$:

$$\boldsymbol{R}_C^{\mathrm{T}}=\begin{bmatrix}0.50 & 0.90 & 0.70 & 0.58\\ 0.10 & 0.50 & 0.70 & 0.64\\ 0.30 & 0.30 & 0.50 & 0.80\\ 0.42 & 0.36 & 0.20 & 0.50\end{bmatrix}$$

根据该矩阵解方程组:

$$\begin{cases}\lambda(a_2-a_1)=0.9-0.5\\ \lambda(a_1-a_3)=0.7-0.5\\ \lambda(a_3-a_4)=0.8-0.5\\ a_1+a_2+a_3+a_4=1\end{cases}$$

$$\lambda>0,a_i\geqslant 0,\forall i\in\{1,2,3,4\}$$

其中,a_i 表示第 i 个一级指标的权重,λ 表示信息的可信程度,其与参评专家关于评估问题的认知能力有关。λ 的取值及说明如下[17]:

$$\lambda=\begin{cases}\lceil\underline{\lambda}\rceil,\text{信息高度可信}\\ n,\text{信息中度可信}\\ \dfrac{n^2}{2},\text{信息低度可信}\end{cases}$$

由于参评专家经验丰富,评估信息高度可信,故 $\lambda=\lceil\underline{\lambda}\rceil=2$。因此,得准则层各一级指标的权重为:$a_1=0.287\,5$,$a_2=0.487\,5$,$a_3=0.187\,5$,$a_4=0.037\,5$。

同理,可求得各二级指标相对于准则层一级指标的权重,以及相对于评估目标(即信息安全风险)的综合权重,计算结果如表 3 所示。

表 3 评估指标权重

目标层	一级指标	权重 a_i	二级指标	权重 b_{ij}	综合权重 w_{ij}
信息安全风险	U_1	0.287 5	U_{11}	0.432 3	0.124 3
			U_{12}	0.251 3	0.072 2
			U_{13}	0.316 4	0.091 0
	U_2	0.487 5	U_{21}	0.666 7	0.325 0
			U_{22}	0.333 3	0.162 5
	U_3	0.187 5	U_{31}	0.247 4	0.046 4
			U_{32}	0.752 6	0.141 1
	U_4	0.037 5	U_{41}	0.721 7	0.027 1
			U_{42}	0.278 3	0.010 4

由表 3 可以看出,各二级指标综合权重向量 $\boldsymbol{W}=(0.124\,3,0.072\,2,0.091\,0,0.325\,0,0.162\,5,0.046\,4,0.141\,1,0.027\,1,0.010\,4)$。

4.2 灰色评价矩阵

将评估等级确定为“很高”“高”“中等”“低”“很低”5 个等级,所对应的分值分别为 5、4、3、2、1。分值越高,说明该项指标存在的风险水平越高。同时确定风险评估等级向量 $\boldsymbol{V}=(5,4,3,2,1)$。现有 5 名专家组成评判组,每人均有多年信息安全风险评估经验,结合该系统实际运行状况,根据预先确定的评估等级向量对各二级指标进行评估赋值,构建样本评价矩阵,见表 4。

表 4 样本评价矩阵

专家	U_{11}	U_{12}	U_{13}	U_{21}	U_{22}	U_{31}	U_{32}	U_{41}	U_{42}
专家 1	3.50	4.00	2.50	4.00	3.50	5.00	2.50	3.50	4.00
专家 2	3.00	4.00	2.50	5.00	5.00	4.50	2.00	3.00	3.50
专家 3	4.00	3.00	3.00	5.00	4.00	3.00	2.50	4.00	3.00
专家 4	3.50	5.00	3.00	5.00	4.50	3.50	3.00	5.00	4.50
专家 5	4.50	3.50	2.50	4.50	3.00	4.00	1.50	3.50	3.50

以一级指标资产 U_1 为例,U_1 所对应的二级指标机密性 U_{11}、完整性 U_{12}、可用性 U_{13} 构成的样本评价矩阵 $\boldsymbol{D}_1$ 为:

$$\boldsymbol{D}_1=\begin{bmatrix}3.50 & 4.00 & 2.50\\ 3.00 & 4.00 & 2.50\\ 4.00 & 3.00 & 3.00\\ 3.50 & 5.00 & 3.00\\ 4.50 & 3.50 & 2.50\end{bmatrix}$$

根据评估等级,将白化权函数分别定义为 $f_1(x)$、$f_2(x)$、$f_3(x)$、$f_4(x)$、$f_5(x)$,各白化权函数的表达式分别如下:

$$f_1(x)=\begin{cases}\dfrac{x}{5},x\in[0,5)\\ 1,x\in[5,+\infty)\\ 0,x\in(-\infty,0)\end{cases}$$

$$f_2(x)=\begin{cases}\dfrac{x}{4},x\in[0,4)\\ \dfrac{8-x}{4},x\in[4,8]\\ 0,x\notin[0,8]\end{cases}$$

$$f_3(x)=\begin{cases}\dfrac{x}{3},x\in[0,3)\\ \dfrac{6-x}{3},x\in[3,6]\\ 0,x\notin[0,6]\end{cases}$$

$$f_4(x)=\begin{cases}\dfrac{x}{2},x\in[0,2)\\ \dfrac{4-x}{2},x\in[2,4]\\ 0,x\notin[0,4]\end{cases}$$

$$f_5(x)=\begin{cases}1,x\in[0,1)\\ 2-x,x\in[1,2]\\ 0,x\notin[0,2]\end{cases}$$

由式(16)计算指标 U_{11} 属于第 $e(e=1,2,3,4,5)$ 个灰类的灰色统计数,得 $n_{11}^{(1)}=3.7$,$n_{11}^{(2)}=4.375$,$n_{11}^{(3)}=3.833$,$n_{11}^{(4)}=1$,$n_{11}^{(5)}=0$。由式(17)可得 U_{11} 的总灰色统计数 $n_{11}=12.908\ 3$,得到 U_{11} 对于各个评价灰类的灰色评价权为:$z_{11}^{(1)}=0.286\ 6$,$z_{11}^{(2)}=0.338\ 9$,$z_{11}^{(3)}=0.296\ 9$,$z_{11}^{(4)}=0.077\ 5$,$z_{11}^{(5)}=0$。则 U_{11} 的灰色评价权向量为:

$\boldsymbol{Z}_1=(0.286\ 6,0.338\ 9,0.296\ 9,0.077\ 5,0)$

由此可分别计算出 U_1 下二级指标 U_{12} 和 U_{13} 对于各个评价灰类的灰色评价权向量为:

$\boldsymbol{Z}_2=(0.311\ 4,0.349\ 3,0.279\ 4,0.059\ 9,0)$

$\boldsymbol{Z}_3=(0.162\ 2,0.202\ 7,0.270\ 3,0.202\ 7,0.162\ 2)$

同理计算所有二级指标的总灰色统计数和灰色评价矩阵权向量,如表 5 所示。

表 5　灰色评价信息

评估指标	总灰色统计数	灰色评价矩阵权向量
U_{11}	12.908 3	(0.286 6,0.338 9,0.296 9,0.077 5,0)
U_{12}	12.525 0	(0.311 4,0.349 3,0.279 4,0.059 9,0)
U_{13}	16.650 0	(0.162 2,0.202 7,0.270 3,0.202 7,0.162 2)
U_{21}	12.266 7	(0.130 4,0.163 0,0.217 4,0.285 3,0.203 8)
U_{22}	13.491 7	(0.200 1,0.250 2,0.308 8,0.203 8,0.037 1)
U_{31}	13.158 3	(0.205 2,0.256 5,0.291 3,0.209 0,0.038 0)
U_{32}	13.258 3	(0.173 5,0.216 8,0.289 1,0.282 8,0.037 7)
U_{41}	12.716 7	(0.298 8,0.334 2,0.288 3,0.078 6,0)
U_{42}	12.908 3	(0.286 6,0.286 6,0.286 6,0.286 6,0)

由灰色评价权向量组成灰色评价矩阵 $\boldsymbol{Z}$:

$$\boldsymbol{Z}=\begin{bmatrix}0.286\ 6 & 0.338\ 9 & 0.296\ 9 & 0.077\ 5 & 0.000\ 0\\ 0.311\ 4 & 0.349\ 3 & 0.279\ 4 & 0.059\ 9 & 0.000\ 0\\ 0.162\ 2 & 0.202\ 7 & 0.270\ 3 & 0.202\ 7 & 0.162\ 2\\ 0.130\ 4 & 0.163\ 0 & 0.217\ 4 & 0.285\ 3 & 0.203\ 8\\ 0.200\ 1 & 0.250\ 2 & 0.308\ 8 & 0.203\ 8 & 0.037\ 7\\ 0.205\ 2 & 0.256\ 5 & 0.291\ 3 & 0.209\ 0 & 0.038\ 0\\ 0.173\ 5 & 0.216\ 8 & 0.289\ 1 & 0.282\ 8 & 0.037\ 7\\ 0.298\ 8 & 0.334\ 2 & 0.288\ 3 & 0.078\ 6 & 0.000\ 0\\ 0.286\ 6 & 0.286\ 6 & 0.286\ 6 & 0.286\ 6 & 0.000\ 0\end{bmatrix}$$

4.3　风险分析

D-AHP 权重计算结果如表 3 所示。通过分析各权重计算结果及权重排序可知,威胁 U_2 是信息安全建设中最需要关注的对象,资产 U_1 次之,而已有安全措施 U_4 对信息系统风险的影响程度最低。因此,在系统运行过程中,应注意以下 4 点:

1)就威胁而言,应重点关注其产生的来源。一方面应注意环境危害或自然灾害以及系统软硬件等方面的故障给系统带来的潜在损害,增强防范意识;另一方面要提高相关技术人员的操作水平及能力,避免人为过失对系统造成的安全损失,同时加强相关人员职业道德水平建设,防止滥用职权及非法访问等行为。

2)应加强对系统资产的保护,同时精确识别其价值,完善相关措施,以确保资产的机密性、完整性及可用性。

3)关注系统资产存在的脆弱性,尤其是管理脆弱性。在系统运行过程中,应完善技术管理与组织管理,并从安全策略的角度出发,完善脆弱性识别等工作。

4)应重视已有安全措施建设。虽然已有安全措施对系统安全风险的影响程度最低,但在日常运行中仍不可忽视各因素对系统产生的不利影响,应周期性巡查系统安全防范措施及安全保护措施,加强

检查力度等。

由式(20)可得综合评价向量 $\boldsymbol{H}$ = (0.192 8, 0.234 0, 0.267 6, 0.213 0, 0.094 1),由式(21)计算出系统总体的信息安全风险评估值 $Risk$ = 3.222 9,由于 3 < 3.222 9 < 4,参考评估等级,将该系统的总体风险等级确定为“中等”,表明该系统运行状况尚可,但还存在一定的安全隐患,故应落实相关管理制度,完善各项应急措施,确保风险状况维持在可控范围内。

5 结束语

本文提出一种基于 D-AHP 方法和灰色理论的信息安全风险评估方法。引入 D 数理论改进模糊偏好关系,以处理由于评估专家经验差异所导致的评估信息不确定等问题。结合层次分析法将定性与定量分析相结合并引入到评估决策过程中,计算各指标的影响权重,降低人为主观性对评估结果的影响。通过灰色理论避免评估过程中信息丢失的现象,充分利用有限的信息资源提高评估的精确性。在此基础上,对信息系统总体安全状况进行综合评估,通过量化的评估结果确定系统当前的安全风险等级。本文评估方法在构建 D 数偏好矩阵的过程中,不一致度系数的取值是否在接受范围内需由评估专家来决定,这在一定程度上增加了专家主观性对评估结果的影响,解决该问题将是下一步的研究方向。

参考文献

[1] SHAMELI-SENDI A, AGHABABAEI-BARZEGAR R, CHERIET M. Taxonomy of information security risk assessment(ISRA)[J]. Computer and Security, 2016, 57:14-30.

[2] AGRAWAL V. A comparative study on information security risk analysis methods[J]. Journal of Computers, 2012, 12(1):57-67.

[3] FENG Nan, WANG H J, LI Mingqiang. A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis[J]. Information Sciences, 2014, 256:57-73.

[4] YU Jingjie, HU Min, WANG Peng. Evaluation and reliability analysis of network security risk factors based on D-S evidence theory[J]. Journal of Intelligent and Fuzzy Systems, 2018, 34(2):861-869.

[5] RODRIGUEZ A, ORTEGA F, CONCEPCCION R. A method for the evaluation of risk in IT projects[J]. Expert Systems with Applications, 2016, 45(C):273-285.

[6] 赵刚,吴天水. 结合灰色网络威胁分析的信息安全风险评估[J]. 清华大学学报(自然科学版), 2013, 53(2):1761-1767.

[7] 中国国家标准化管理委员会. 信息安全技术 信息安全风险评估规范: GB/T 20984-2007[S]. 北京,[出版者不详]:2007.

[8] DEMPSTER A. Upper and lower probabilities induced by a multivalued mapping[J]. Annals of Mathematical Statistics, 1967, 38:325-329.

[9] DENG Y. D numbers: theory and applications[J]. Journal of Information and Computational Science, 2012, 9(9):2421-2428.

[10] HUANG Xiaozhong, WANG Ningkai, WEI Daijun. Investment decision using D numbers[C]//Proceedings of 2016 Chinese Control and Decision Conference. Washington D. C., USA: IEEE Press, 2016:4164-4167.

[11] LIU Huchen, YOU Jianxin, FAN Xiaojun, et al. Failure mode and effects analysis using D numbers and grey relational projection method[J]. Expert Systems with Applications, 2014, 41(10):4670-4679.

[12] DENG Xinyang, HU Yong, DENG Yong. Bridge condition assessment using D numbers[J]. Scientific World Journal, 2014(5):358057.

[13] FAN Zong, WANG Lifang. Evaluation of university scientific research ability based on the output of sci-tech papers: a D-AHP approach[J]. PLoS One, 2017, 12(2):e0171437.

[14] FAN Guichao, ZHONG Denghua, YAN Fugen, et al. A hybrid fuzzy evaluation method for curtain grouting efficiency assessment based on an AHP method extended by D numbers[J]. Expert Systems with Applications, 2016, 44(C):289-303.

[15] DENG Xinyang, HU Yong, DENG Yong. Supplier selection using AHP methodology extended by D numbers[J]. Expert Systems with Applications, 2014, 41(1):156-167.

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

[17] DENG Xinyang, DENG Yong. D-AHP method with different credibility of information[J]. Soft Computing, 2019, 23(2):683-691.

编辑 吴云芳