信息系统安全程度的分析与评估

摘 要

本文综合考虑多篇文献及相关资料，确定了影响信息系统安全的三个主要因素：防护措施与能力、外部环境和信息自身价值[1]以及其下属的若干二级因素，形成层状结构，并对其进行定量分析。

对于问题一，首先采用了 AHP（层次分析法）计算出各因素的权重，其次运用模糊评估法进行了评估。通过前两种方法得到大量样本数据后，再利用 BP 神经网络法拟合出函数，从而使今后使用该模型时只需输入相关数据便可直接得到评估结果。

对于问题二，我们选取了防护措施与能力这一因素。基于客观性的考虑，我们对数据标准化后，用了模糊理论和熵权理论求解各个二级因素的权重，求解一级因素的重要程度，为了将数据量化，此处评价等级用 1-5 的数字代替。

问题三是问题一、二中模型的实际应用，借助 matlab 软件，计算出安卓手机系统的安全程度，并将两种模型进行了比较。

关键词：层次分析法 模糊理论 BP 神经网络法 数据规范化 熵权理论

目 录

一、问题重述

斯诺登事件为我们敲响了信息安全的警钟，也让我们更进一步认识到当前网络信息安全所面临形势的严峻性。保障我国网络信息安全，是当前面临的重要问题。信息安全度量是业界公认的一个难题，信息安全度量一般需要回答两个问题：信息系统安全不安全?信息系统的安全程度是多少？ 通过查阅相关资料。请你们小组解决以下问题：

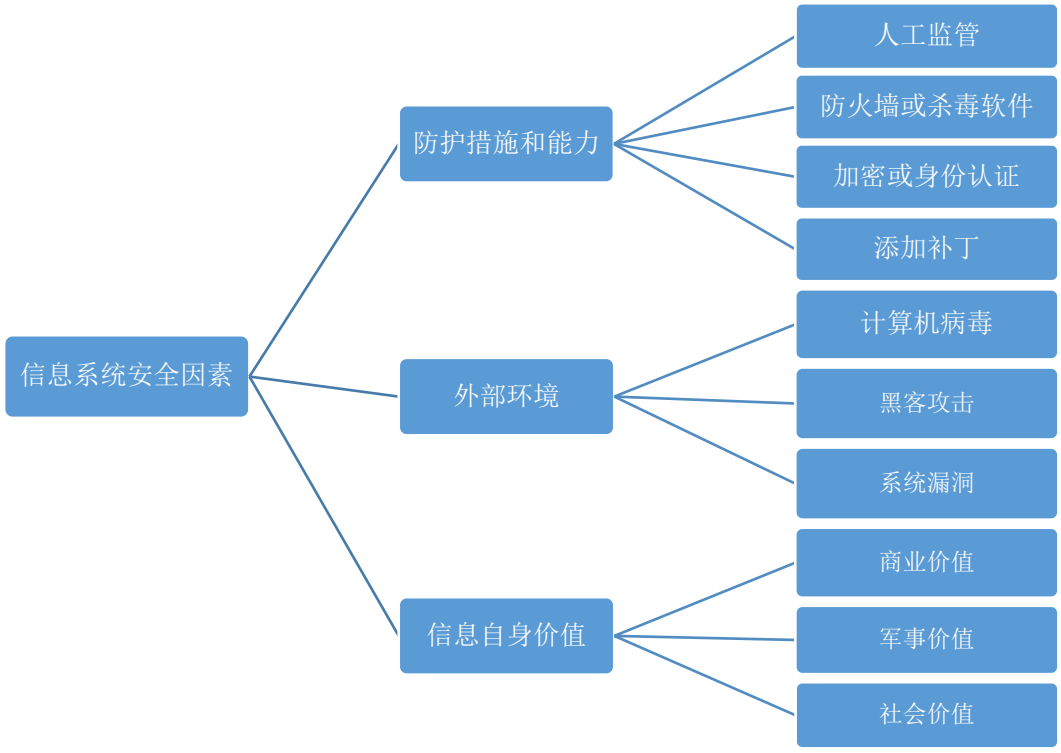
问题 1，基于“2015 年信息安全事件汇总报告”（http://mt.sohu.com/20160113/n434399073.shtml）以及其它网络数据，建立一个计算信息系统（孤立隔离，或广泛互联的系统）的安全程度的数学模型。

问题 2，选取一个重要的信息安全度量指标，说明选取的理由，并给出计算该指标的数学模型。

问题 3，利用上述两个模型，具体对你们小组成员所持有的手机信息系统进行研究，给出计算结果，并进行简单分析与比较。

二、问题分析

本题目是围绕信息系统的安全评估展开的，我们需要找寻影响信息系统安全的因素，并且分析计算各因素的权重，从而解决一系列的问题。
对于信息安全的因素，我们认为如下图所示：



[1]

问题一让我们评估信息系统的安全程度，实际上就是计算各因素权值，这里我们采用了层次分析法计算出各因素权值，再利用模糊理论和风险度量公式求解出评估结果。为了方便今后使用该模型的使用，最后我们采用 BP 神经网络对数据进行整合处理，通过 BP 神经网络可以直接得出安全系统的安全程度，减少了主观因素对结果的影响。

问题二中我们选择了防护措施与能力这一指标，对数据标准化后，利用模糊理论和熵权理论建立了该因素的模型。

第三问是一道比较、分析的综合题目，主要是对前两问所建立模型的综合应用。

三、模型假设

1、假设本文未列因素对信息系统安全无影响。
2、假设专家对各因素的评价标准不因时间而发生变化且较为公正。
3、假设信息系统的安全程度不会中途改变。

四、符号说明

A 表示因素集
B 表示评价集
C 表示隶属度矩阵
D 表示底层指标因素权重向量
F 表示中层指标因素权重向量
E 表示各评价等级权重向量

p 表示不确定事件发生的概率

q 表示不确定事件造成损失的概率

$\overline{p}$ 表示不确定事件未发生的概率

$\overline{q}$ 表示不确定事件未造成损失的概率

R 表示风险评估结果

$R(x)$ 表示风险函数

k_{ij} 表示因素的重要性之比

RI 表示同阶平均随机一致性指标
CI 表示一致性指标
CR 表示随机一致性比率
K 表示判断矩阵

$\lambda_{\max}$ 表示判断矩阵的最大特征根

n 表示输入层层的节点数
l 表示隐含层的节点数

e表示允许误差
α表示学习速率
k表示某一时刻
$w(k)$表示k 时刻的权值向量

$D(k)$表示k时刻的负梯度

η表示动量因子

U_i表示防护措施与能力对a_i的相对重要性

5、模型的建立与求解

5．1 问题一[2]

5．1.1 问题分析

信息系统的安全风险，是指信息系统在不同安全特性下的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响，我们可以根据不确定事件发生的可能性和负面影响的程度来识别信息系统的安全风险。

本文中采用 1997 年赵恒峰提出的风险度量公式：$\bar{p}$表示不确定事件未发生的概率，$\bar{q}$表示不确定事件未造成损失的概率大小；显然有$p = 1 - \bar{p}$，$q = 1 - \bar{q}$，由概率测度为变量的风险函数可表示如下：

$$R(x) = f(\text{不确定事件发生的概率测度，不确定事件造成损失的概率测度})$$

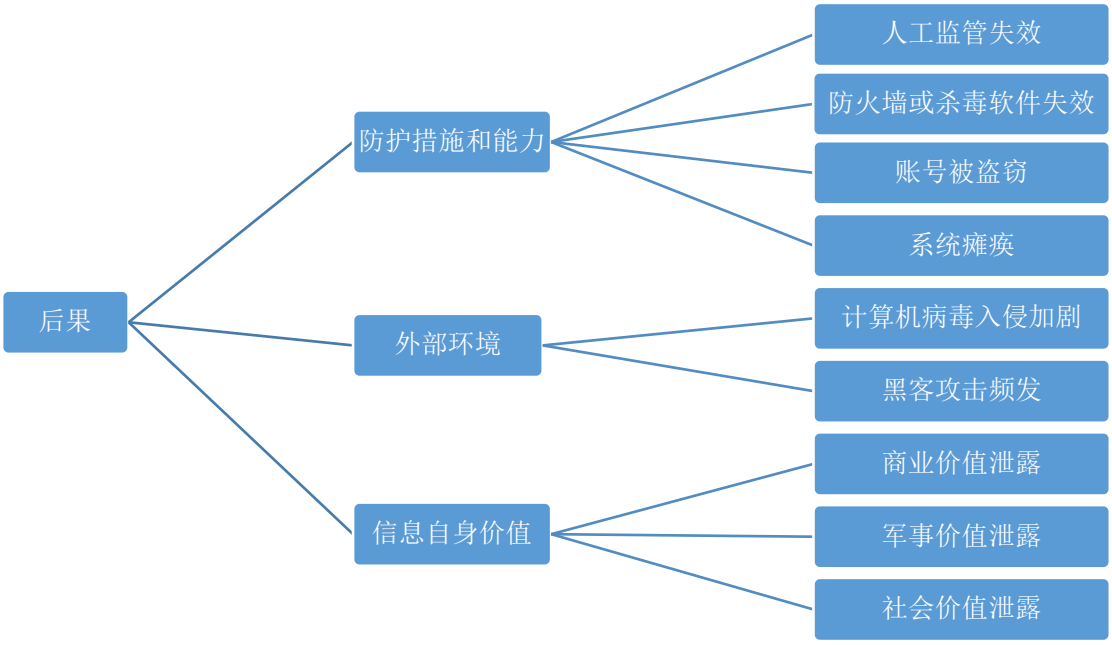
$$= 1 - \text{不确定事件未发生概率} \times \text{不确定事件未造成损失的概率测度}$$

$$= 1 - \bar{p} \cdot \bar{q}$$

$$= 1 - (1 - p)(1 - q)$$

$$= p + q - p \cdot q$$

当安全问题发生时，造成的后果如下图：



5.1.2 层次分析法计算各因素的权重[3]

(1)方法介绍

层次分析法（Analytic Hierarchy Process 简称 AHP）是在 20 世纪 70 年代初由 T.L.Saaty 等人提出的一种简便、实用的多准则决策方法。人们在处理决策问题时，往往需要考虑多种因数，在决策前，需要从各种可行的方案中选出一个最佳方案，这就需要对这些诸多因数进行比较。而这些因数的重要性往往难以准确地数量化，故一般的数学方法难于解决这类决策问题。层次分析法为这类问题的决策提供了一种定性与定量相结合的新的简便、实用的方法。

(2)计算

1）建立层次结构

应用层次分析法处理决策问题时，首先要把影响决策的各种因数层次化并构造出一个有层次的结构模型。在这个层次结构模型下，复杂的各种因素被分为若干层次。

2）构造判断矩阵

对第一层的各指标之间进行两两对比之后，按 9 分位比率排定各评价指标的相对优劣顺序，依次构造出评价指标的判断矩阵。层次分析法中采用一种相对标度来加以衡量，即 1-9 标度法，如下表：

1	表示两个因素相比，具有同样重要性
3	表示两个因素相比，一个因素比另一个因素稍微重要
5	表示两个因素相比，一个因素比另一个因素明显重要
7	表示两个因素相比，一个因素比另一个因素强烈重要
9	表示两个因素相比，一个因素比另一个因素极端重要

2,4,6,8	上述两相邻判断的中值
倒数	若因素 i 与因素 j 的重要性之比为 a_{ij}，则因素 i 与因素 j 的重要性之比为 $a_{ij} = \frac{1}{a_{ji}}$

3）权重系数的计算

运用 1-9 标度法，通过逐对比较一级因素构造判断矩阵 K ，然后计算判断矩阵的最大特征值和它的特征向量，经归一化后即可计算出一级因素相对于信息系统安全的权重系数。

4）判断矩阵的一致性检验

一致性检验指标如下：

$$CI = \frac{\lambda_{\max} - n}{n - 1}$$

其中 $\lambda_{\max}$ 是判断矩阵的最大特征根， n 为判断矩阵的阶，当 $CI = 0$ 即 $\lambda_{\max} = n$ 时，可以证明矩阵是一致矩阵。

同时，为了确定矩阵非一致性容许的范围，再引入一个随机一致性指标 RI ， RI 的取值如下表：

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

在这里，对于 1、2 阶判断矩阵， RI 只是形式上的，因为 1、2 阶判断矩阵总具有完全一致性。当阶数大于 2 时，判断矩阵的一致性指标 CI 与同阶平均随机一致性指标 RI 之比称为随机一致性比率，记为 CR 。当

$$CR = \frac{CI}{RI} < 0.1$$

时，即认为判断矩阵具有满意的一致性，否则就需要调整判断矩阵，并使之具有满意的一致性。

(3)举例

确定系统在人工监管、防火墙或杀毒软件、加密或身份验证和添加补丁方面的权重系数。根据风险度量表，两两比较各风险影响因素，得到判断矩阵：

$$\begin{pmatrix} 1 & \frac{1}{5} & \frac{1}{3} & \frac{1}{5} \\ 5 & 1 & 5 & 3 \\ 3 & \frac{1}{5} & 1 & \frac{1}{3} \\ 5 & \frac{1}{3} & 3 & 1 \end{pmatrix}$$

由附件程序代入得最大特征值为4.1981，相对应的的特征向量归一化后为$(0.0636,0.5439,0.1219,0.2706)$，该特征向量即为该方面的脆弱性在系统整体脆弱性中所占的比重，即为其权重向量。一致性检验中，$CI = 0.066$，$CR = 0.074 < 0.1$，一致性可以接受。同理，再得到其他因素对各种评价目标的权重系数。

5.1.3 多级模糊综合评判的方法得到系统风险的量化评估

(1) 模糊综合评判法介绍

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事物或对象做出一个总体的评价。它具有结果清晰，系统性强的特点，能较好地解决模糊的、难以量化的问题，适合各种非确定性问题的解决。[4]

一般过程：

1、根据实际需要建立因素集；

2、由各个因素对评价对象的影响程度得到权重集；

3、通过对数据适当的处理，由专家主观评价打分，求得关于等级的隶属度，得到评价集；

4、由权重集和评价集得到评价结果。

(2)求解步骤：

1）根据层次分析法中所建立的信息系统风险分析的层次结构，建立信息系统风险评价因素集合$A = \{a_1 \dots a_n\}$（n为二级指标因素数）。同时，由层次分析法得到各评价指标相应的权重系数。然后构造评判集，对于不同指标，可以设立不同的评判集。设评价所确立的等级集合的评判集为$B = \{b_1 \dots b_n\}$

2）请若干专家作为评判组，参照评判集B， 对因素集A 中的各因素进行评价，给出各因素的评语， 得到因素集A对评价集B的归一化后的隶属度矩阵C。

3）在计算底层指标评价结果时，各因素相应的权向量为$D = \{d_1 \dots d_n\}$，则该指标的评价结果为$D \times C$。在求得二级指标评价结果后，同理也求出一级指标各因素的权重系数，得到权向量$\mathrm{F} = \{f_1 \dots f_m\}$(m 为一级指标因素数)，然后，对评判集 B，各指标赋予相应的权重，得到归一化后的指标权向量$E = \{e_1 \dots e_n\}$，得到风险发生概率和发生后果的评价结果，即$\mathrm{F} \times (\mathrm{D} \times \mathrm{C}) \times \mathrm{E}$。

4）最后，根据风险度量公式$R = p + q - p \cdot q$，求出评估结果R。

5.1.4 利用模糊神经网络对信息系统安全程度直接量化评估

（1）BP 神经网络结构介绍

BP 网络（Back Propagation），是 1986 年由 Rumelhart 和 McCelland 为首的科学家小组提出，是一种按误差逆传播算法训练的多层前馈网络，由输入层、输出层和若干隐含层组成，每层由若干个节点组成，每一个节点代表一个神经元，相邻层的神经元通过权连接，同层各神经元互不相连接。BP 网络能学习和存贮大量的输入-输出模式映射关系，而无需事前揭示描述这种映射关系的数学方程。

以 3 层 BP 神经网络的建模为例（这与我们所分的信息系统安全层次相符），

输入层和隐含层的节点数分别为n和l，输出层为一个单节点输出。设定好 BP 神经网络参数（允许误差e和学习速率α），将学习样本按顺序输入到 BP 神经网络中，通过神经网络的迭代算法可使网络输出值与训练样本总体的实际值的均方误差降低到满意的程度，从而获得稳定的网络结构和连接权值。

其中，为解决 BP 神经网络学习收敛速度慢、容易陷入局部极小值而无法得到全局最优解的问题，本文采用动量法，通过降低网络对于误差曲面局部细节的敏感性，有效地抑制网络陷于局部极小，改进算法为：

$$w(k+1)=w(k)+\alpha[(1-\eta)D(k)+\eta D(k-1)]$$

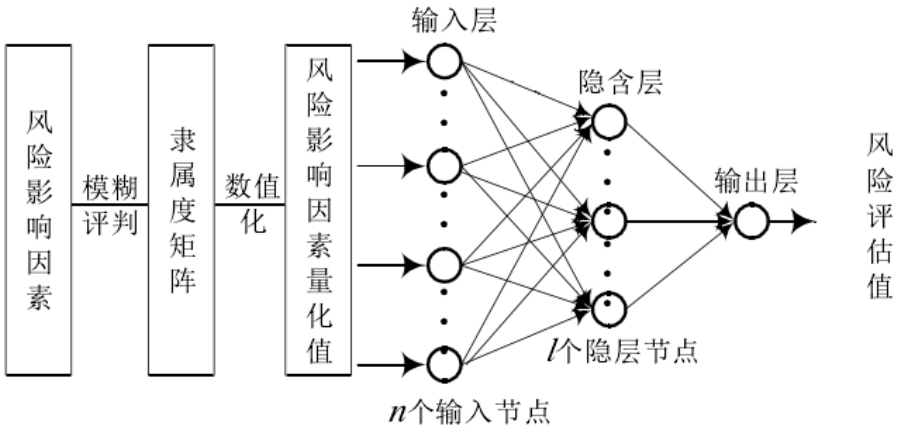
式中，$w(k)$为k 时刻的权值向量；$D(k)$为k时刻的负梯度；$D(k-1)$为$k-1$ 时刻的负梯度；α为学习速率，$\alpha>0$；η为动量因子，$0\le\eta<1$。

对于网络隐含层节点，则采用$l=1\log_2 n$的方法来确定。

相应的程序见附表。

（2）信息系统安全量化评估的求解

在前两小节中，我们已经利用层次分析法和模糊评估的模型，将信息系统安全程度的影响因素进行量化处理和一致性处理，并且得到了评估结果，从而由大数据可以得到大量的学习样本。再通过 BP 神经网络的学习算法，可以得到影响因素与评估结果的网络结构和连接权值。接下来就可以利用以下模型结构直接得出安全程度评估：



5．2 问题二[5]

5.2.1 指标的选取与理由

我们选择防护措施与能力这一指标，因为防护措施与能力是信息系统安全的内因，具有可控性，我们可以通过加强人工监管、升级系统、填补漏洞、定期修改密码等手段不断的提高信息系统的安全程度。攘外必先安内，只有先把内部因素解决好，才能更好的适应外部环境。

5.2.2 数据标准化

在防护措施和能力这一一级指标下，还有 4 个二级因素，各个因素的单位不尽相同，为了后续的计算，要先将数据标准化，在这里我们采取离差标准化，公式如下：

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

5.2.3 建立模糊集合及隶属度矩阵

各因素对于一级指标的估计具有一定的模糊性，所以在这里我们应用了模糊理论。

首先我们建立一个因素集 $A = \{a_1, a_2, a_3, a_4\}$，集合中的元素分别对应着人工监控、防火墙、加密或身份验证、添加补丁。

其次我们对于防护措施与能力建立一个评价集 $B = \{b_1, b_2, b_3, b_4, b_5\}$，$b_1$至$b_5$的含义如下表：

编号	程度	说明
b_1	十分重要	说明安全防护与能力这一指标对这一因素而言十分重要
b_2	重要	说明安全防护与能力这一指标对这一因素而言重要
b_3	一般	说明安全防护与能力这一指标对这一因素而言一般重言
b_4	不太重要	说明安全防护与能力这一指标对这一因素而言不太重要
b_5	不重要	说明安全防护与能力这一指标对这一因素而言不重要

根据专家的意见，可以构造出模糊映射 $f: A \to F(B)$，f 表示 A 中元素对评判集 B 中各评语的支持程度。即可得到 A 中元素对于评判集 B 的隶属矩阵

$$C = \begin{Bmatrix} c_{11}, c_{12}, c_{13}, c_{14}, c_{15} \\ c_{21}, c_{22}, c_{23}, c_{24}, c_{25} \\ c_{31}, c_{32}, c_{33}, c_{34}, c_{35} \\ c_{41}, c_{42}, c_{43}, c_{44}, c_{45} \end{Bmatrix}$$（c_{ij}表示风险因素 a_i 对评价集中元素 b_j 的支持程度）。

向量 A 中的各个元素重要程度并不相同，所以我们将各因素的权向量设为 $D = \{d_1, d_2, d_3, d_4\}$。

为了将评价量化，我们设定评价为十分重要时取值“1”，评价为重要时取值“2”，评价为一般时取值“3”，评价为不太重要时取值“4”，评价为不重要时取值“5”，从而得到评价集权重向量$E = \left\{\frac{1}{15}, \frac{2}{15}, \frac{1}{5}, \frac{4}{15}, \frac{1}{3}\right\}$。

由此我们可以得出防护措施与能力的影响程度$Z = D \times C \times E^T$。

5.2.4 计算熵权

(1)熵权[6]

按照信息论基本原理的解释，信息是系统有序程度的一个度量，熵是系统无序程度的一个度量；如果指标的信息熵越小，该指标提供的信息量越大，在综合评价中所起作用理当越大，权重就应该越高。

(2)计算

防护措施与能力的相对重要性可以用以下式子计算：

$$U_i = -\sum_{j=1}^{5} c_{ij} \ln c_{ij}$$

当$c_{ij}\left(j = 1、2、3、4、5\right)$相等时（即等于$\frac{1}{5}$），U 取得最大值$U_{\max} = \ln 5$，我们就可以用这个数值对所求得的$U_i$进行归一化处理。

式子如下：

$$U_i = -\frac{1}{\ln 5} \sum_{j=1}^{5} c_{ij} \ln c_{ij}$$

为了使因素a_i对评估的贡献程度与U_i成正比，所以取$1 - U_i$来作为因素a_i的权重，再次进行归一化处理，得到

$$D_i = \frac{1}{n - \sum_{i=1}^{n} U_i}\left(1 - U_i\right)$$

5.3 问题三

5.3.1 模型一

按照模型一，首先通过构造判断矩阵，计算信息系统安全事件发生概率，得到各因素的权重系数，如下表：

评价目标	影响因素	权重系数
防护措施和能力	人工监管	0.0636
	防火墙或杀毒软件	0.5439
	加密或身份认证	0.1219
	填加补丁	0.2706
一致性检验	CR=0.074	

外部环境	计算机病毒	0.6370
	黑客攻击	0.2583
	系统漏洞	0.1047
一致性检验	CR= 0.037	
信息自身价值	商业价值	0.6370
	军事价值	0.2583
	社会价值	0.1047
一致性检验	CR=0.037	

同理,计算信息系统安全事件发生的后果,得到各因素的权重系数,如下表：

评价目标	影响因素	权重系数
防护措施和能力	人工监管失效	0.0636
	防火墙或杀毒软件失效	0.5439
	账号被盗窃	0.1219
	系统瘫痪	0.2706
一致性检验	CR=0.074	
外部环境	计算机病毒入侵加剧	0.6667
	黑客攻击频发	0.3333
一致性检验	CR=0	
信息自身价值	商业价值泄露	0.6370
	军事价值泄露	0.2583
	社会价值泄露	0.1047
一致性检验	CR=0.037	

构造判断矩阵，计算中层指标对目标层的权重系数，如下表：

评价目标	影响因素	权重系数
信息系统安全事件发生概率	防护措施和能力	0.540
	外部环境	0.163
	信息自身价值	0.297
一致性检验	CR=0.0079	
信息系统安全事件发生后果	防护措施和能力	0.540
	外部环境	0.163
	信息自身价值	0.297
一致性检验	CR=0.0079	

接下来，对各因素构建评价集，不妨令 V={风险程度低，风险程度较低，风险程度中等，风险程度较高，风险程度高}，评价结果如下表：

中间层评价指标	底层评价指标	风险程度				
		低	较低	中等	较高	高
防护措施和能力（概率）	人工监管	0.4	0.2	0.2	0.1	0.1
	防火墙或杀毒软件	0.1	0.3	0.2	0.2	0.2
	加密或身份认证	0.4	0.2	0.1	0.2	0.1

	填加补丁	0.5	0.2	0.1	0.1	0.1
外部环境（概率）	计算机病毒	0.2	0.3	0.2	0.1	0.2
	黑客攻击	0.2	0.2	0.3	0.1	0.2
	系统漏洞	0.6	0.1	0.1	0.1	0.1
信息自身价值（概率）	商业价值	0.5	0.2	0.1	0.1	0.1
	军事价值	0.4	0.2	0.2	0.1	0.1
	社会价值	0.2	0.1	0.4	0.1	0.2
防护措施和能力（后果）	人工监管	0.4	0.2	0.2	0.1	0.1
	防火墙或杀毒软件	0.1	0.3	0.2	0.2	0.2
	加密或身份认证	0.4	0.2	0.1	0.2	0.1
	填加补丁	0.5	0.2	0.1	0.1	0.1
外部环境（后果）	计算机病毒入侵加剧	0.4	0.2	0.1	0.1	0.2
	黑客攻击频发	0.3	0.2	0.3	0.1	0.1
信息自身价值（后果）	商业价值	0.5	0.2	0.1	0.1	0.1
	军事价值	0.4	0.2	0.2	0.1	0.1
	社会价值	0.2	0.1	0.4	0.1	0.2

由以上数据可得信息系统安全事件发生的可能性和后果的评估结果如下表：

	评价因素	风险程度				
		低	较低	中等	较高	高
信息系统安全事件发生的可能性	防护措施和能力（概率）0.540	0.2639	0.2544	0.1608	0.1666	0.1544
	外部环境（概率）0.163	0.2419	0.2532	0.2154	0.1000	0.1895
	信息自身价值（概率）0.297	0.4428	0.1895	0.1572	0.1000	0.1105
信息系统安全事件发生的后果	防护措施和能力（后果）0.540	0.2639	0.2544	0.1608	0.1666	0.1544
	外部环境（后果）0.163	0.3667	0.2000	0.1667	0.1000	0.1667
	信息自身价值（后果）0.297	0.4428	0.1895	0.1572	0.1000	0.1105

将评价集 V 数字量化，令 V=[0.1,0.3,0.5,0.7,0.9],这可以理解为数字从 0.1 至 0.9 数字越大，风险越大，相对地安全程度越小。则最终得：

p=0.4137

q=0.4058

故 R= $p+q-p\cdot q$ =0.652

从这个结果来看，该系统的安全程度较低，风险程度较大。

由于这里设计的样本数据有限，暂无法利用基于大数据的 BP 神经网络算法进行评估。

5.3.2 模型二

因为无法收集到专家的意见，所以我们对 50 名使用安卓系统的同学进行了调查，形成专家意见

评价 / 因素	b_1	b_2	b_3	b_4	b_5
a_1	6	12	18	14	0
a_2	31	5	9	5	0
a_3	28	14	5	3	0
a_4	12	33	4	1	0

（单位：人）

得到隶属度矩阵：

评价 / 因素	b_1	b_2	b_3	b_4	b_5
a_1	0.12	0．24	0.36	0.28	0
a_2	0.62	0.10	0.18	0.10	0
a_3	0.56	0.28	0.10	0.06	0
a_4	0.24	0.66	0.08	0.02	0

据上述式子可以求得：

$$D = \{0.1390, 0.2623, 0.2552, 0.3435\}$$

可以得出防护措施与能力的影响程度 $Z = 0.1280$

可知该系统安全措施与能力方面做的不错，风险较小。

比较：模型一相较于模型二考虑因素更加全面，但模型一采用的层次分析法主观性更强，而模型二采用的熵权法更具客观性。虽然模型二计算得到系统安全措施与能力方面做的不错，但是因为信息系统的安全程度由多方面影响，所以两个结果并不矛盾。

6. 对模型的评价

6.1 对模型一的评价

优点：

1、该模型将神经网络和层次分析法以及模糊评估法结合在一起，相辅相成，逻辑性强，既考虑了专家对影响信息系统安全的各因素的主观评价，合理地量化了各指标，同时通过样本学习，降低了评估过程中的人为因素，又较好的保证了评价结果的客观性，提高了系统安全评估的自适应能力。

2、在通过层次分析法和模糊评估法获取大量学习样本后，可以采用 BP 神经网络算法简化运算步骤，增强了实际可操作性。

缺点：

1、 影响信息系统安全的因素过于繁杂，分类方法也多种多样，很难确保所构建的指标体系全面而准确。

2、 网络公布数据与模型指标所需数据可能不匹配，数据采集比较困难。

3、 专家对各因素的评价可能会随信息技术的发展而发生变化，故直接利用神经算法得到评估结果具有短期性。

6.2 对模型二的评价

优点：该模型采用熵权法，具有客观性，相对于那些主观赋值法，精度较高，能够更好的解释结果。并且结合性好，不仅可以单独使用，也可以依据实际情况与其他方法结合使用。

缺点：各指标的权重过于依赖于样本，样本的波动可能会影响最终结果，并且这种方法只能用于求权重。

参考文献：

[1] 吕欣. 信息安全度量理论和方法研究[A]. 中国计算机学会计算机安全专业委员会、中国电子学会计算机工程与应用学会计算机安全保密学组.全国计算机安全学术交流会论文集（第二十二卷）[C].中国计算机学会计算机安全专业委员会、中国电子学会计算机工程与应用学会计算机安全保密学组:,2007:5.

[2]肖龙. 信息系统风险分析与量化评估[D].四川大学,2006.

[3] 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，1990,5-10.

[4]百度百科：模糊综合评价法

[5]赵冬梅,张玉清,马建峰. 熵权系数法应用于网络安全的模糊风险评估[J]. 计算机工程,2004,18:21-23.

[6]百度百科：熵权

Email：572423908@qq.com

队员电话：张佳丽 13041082531

邱奇粮 13161894964

庄大伟 13241811629