Application of AHP to security protection ability comprehensive evaluation during classified evaluation

Jing Yuan, Weihong Ren
MPS Information Classified Security Protection Evaluation Center
The Third Research Institute Of Ministry Of Public Security
Beijing, China
yuanj1101@163.com

***Abstract*—On the basis of analyzing the situation of classified evaluation, this paper brings forward a security protection ability evaluating indicators system based on AHP. According to the algorithm of AHP, the hierarchical architecture, the computing method of indicator weights and synthetic weight are established. Finally, the problem of security protection ability evaluation in classified evaluation is solved.**

Keywords-Classified protection; AHP(Analytic Hierarchy Process); classified evaluation; security protection ability

I. INTRODUCTION

The classified protection of information security has been a Chinese national policy since 2003[1]. The work of classified evaluation is currently in progress in most departments. But the comprehensive evaluation method of classified evaluation is imperfect. On the basis of analyzing the situation of classified evaluation, this paper brought forward a security protection ability evaluating indicators system. According to the evaluating indicator system, the information system's security protection ability is mapped to the outcomes during classified evaluation. So it makes up the shortage of classified evaluation.

II. RESEARCH BACKGROUND

Ministry of Public Security cooperating with other three Ministries published requirement "Classified Protection of Information Security Government Rule" (MPS [2007]43), which regulates five actions of classified protection: classification, officially record, construction and improvement, classified evaluation and superintendence. Classified evaluation must be implemented regularly in critical Information system [2].

In order to facilitate the progress of classified protection, the policy system and the standard system are constituted for classified protection. Among the standard system, GB/T22239-2008 'Baseline for classified protection of information system' (abbreviated as *baseline*) is the chief basis to guide information system construction. It raises security protection ability from Grade 1 to Grade 5. It describes the technology and management security controls for each grade[3], but it doesn't explain the mapping from security controls to security protection ability.

With the development of classified protection, the work planned at the primary stage has been fully implemented[4]. But there is some difference between the effect and the major expectation of classified protection.

Now classified evaluation includes security control catalog evaluation and overall evaluation. The former validates the security function of the components of information system according to *baseline*. The latter is a further evaluation aiming at the non-conformities of security control catalog evaluation from the whole information system. And then the security function conclusion, not the security protection ability conclusion, is given based on the two evaluation consults. So a method should be studied to evaluate security protection ability during classified evaluation which can map security controls to security protection ability, and then derive security protection ability conclusion of information system.

III. SUMMARY OF ANALYTIC HIERARCHY PROCESS(AHP)

AHP is a decision-making method for prioritizing alternatives when multiple criteria must be considered[5]. Generally the hierarchy has at least three levels: the goal, the criteria, and the alternatives. These judgments are expressed in terms of pairwise comparisons of items on a given level based on the next higher level. Each of the pairwise comparisons represents an estimate of the ratio of the weights of the two criteria being compared. By analyzing the sorted results of various items of a given level and of overall levels, the optimal solution is determined.

First, we design a security protection ability evaluation indicators system, and ascertain the relationship of each indicator of evaluation indicator system through issuing questionnaire to experts and collecting feedbacks, and calculate importance weights of each level with AHP. And then we score items to the outcome of security control catalog evaluation and overall evaluation. At last, we get the score for security protection ability of information system. The essential steps are listed as below: a) problem identification and building hierarchy model as Fig.1, b) judgment matrix construction, calculating items weights and coincidence test, and c) calculating combination weight and the score of security protection ability.

Published by Atlantis Press, Paris, France.

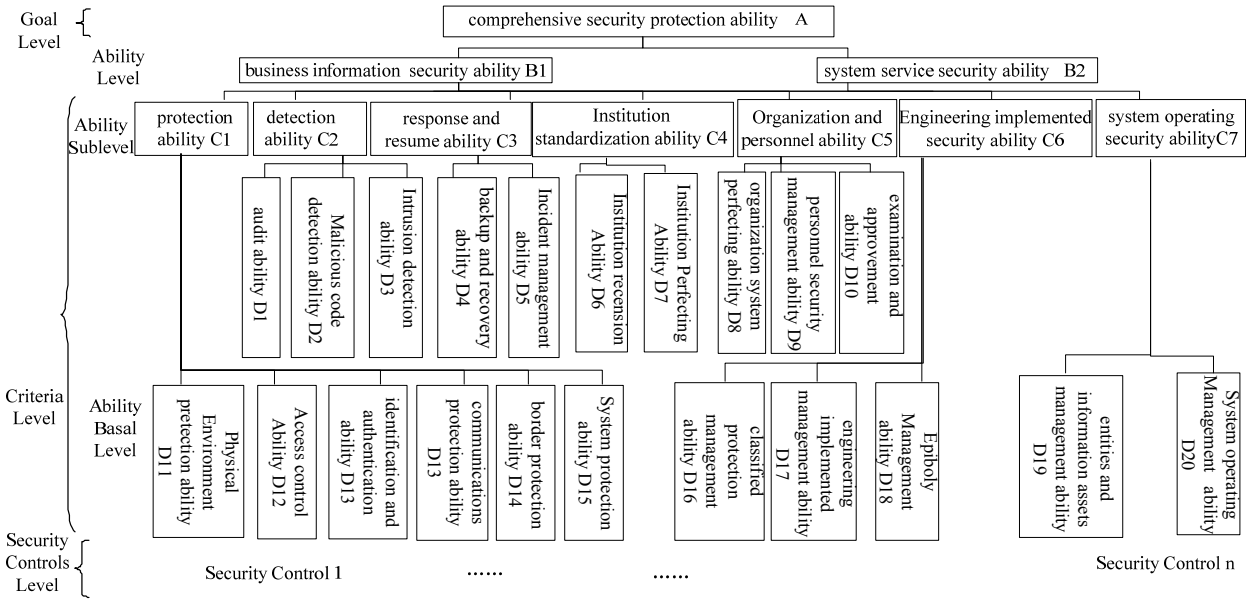

Figure 1. The Security Protection Ability Hierarchy model

IV. SECURITY PROTECTION ABILITY COMPREHENSIVE EVALUATION

A. *Build the hierarchy model*

According to AHP, the security protection ability evaluation indicators system of information system has three levels: the goal, the criteria and the controls[6] (Fig.1). The uppermost goal level which is the ultimate target only has one item, comprehensive security protection ability. The criteria level, namely protection ability level, can be further divided into ability level, ability sublevel and ability basal level. And the alternatives level is security controls level whose items are mapped to 264 security controls (e.g., network access control, change management) from *baseline*. Fig.1 shows the hierarchy model building for one information system.

To facilitate description, the paper marks goal level as A, ability level as B, ability sublevel as C, ability basal level as D, and security controls level as E. And all items of indicators system are labeled according their levels.

B. *Construct the judgment matrix to acquire evaluation indicators weights*

Reasonable indicators weights are the key point of security protection ability comprehensive evaluation. In order to get the result of comprehensive analysis during classified evaluation, there must be indicators weights suitable for information system of different grades. Generally, judgment matrix is used to acquire the indicators weights.

1) Judgment matrix and indicator weight of level B with respect to level A

In judgment matrix of level B, the value of the indicator for the business information security ability B1 should be the grade of business information security, and the value of the indicator for the system service security ability B2 should be the grade of system service security. According to the grade of business information security labeled as *ls* and the grade of system service security labeled as *la*, the judgment matrix for level B is:

$$A_B = \begin{bmatrix} 1 & ls/la \\ la/ls & 1 \end{bmatrix} \quad (1)$$

In level B, the maximum characteristic root (λ_{max} =2) and normalized Characteristic vector (W_B=$\left[\frac{ls}{ls+la} \quad \frac{la}{ls+la}\right]$) are the indicator weights of business information security protection ability and system service security protection ability respectively. The coincident rate *C.R*=0<0.1. For instance, the level B judgment matrix of an information system with Grade S2A3G3 is $S=\begin{bmatrix} 1 & 2/3 \\ 3/2 & 1 \end{bmatrix}$. Characteristic vector can be acquired by addition after coincident testing, namely the normalized sum of row vector in matrix S is the weight vector *A*=(0.4,0.6).

2) Judgment matrix and indicator weight of level C with respect to level B

In information system of different grade, the indicators weights of level C are not the same with respect to level B. They may change according to the higher level(level B) , business information security or system service security. The characters of the 5-Grade classified protection ability are shown in TABLE I. Grade 1 emphasizes security defense ability. Based on Grade 1, Grade 2 emphasizes detection ability.

Thereby, judgment matrix A_C can be acquired through the review result from expert. With the maximum characteristic root and characteristic vector after calculating, the normalized weight of level C with respect to level B is as below.

$$W_C = \begin{bmatrix} W_{B1C1} & \cdots & W_{B1Cn} \\ W_{B2C1} & \cdots & W_{B2Cn} \end{bmatrix} \quad (2)$$

W_{B1Cn} represents the weight of the *n*th indicator of level C with respect to B1 and W_{B2Cn} is the weight of the *n*th indicator with respect to B2. *n* is a positive integer from 1 to 7.

Take Grade 2 for example. The specific calculating process of weight of indicator in level C with respect to B1 and B2 is as below.

a) The weight of indicator in level C with respect to B1.

- Construct the judgment matrix as shown in Table II.
- Calculate the maximum characteristic root:

$$\lambda_{max}=7.07077\tilde{}. \quad (3)$$

- Calculate and normalize characteristic vector:

$$W_{B1C}=\{0.33,0.13,0.07,0.13,0.07,0.05,0.22\}. \quad (4)$$

- Coincidence testing:

$C.R.=\frac{C.I.}{R.I.}=\frac{\lambda_{max}-n}{R.I.\ (n-1)}$ =0.0089<0.10 (referring to table that *R.I.* =1.32) . (5)

So the coincidence of the judgment matrix is acceptable.

b) The weight of indicator in level C with respect to B2.

- Construct the judgment matrix as shown in Table III.

TABLE I. GRADE OF SECURITY PROTECTION ABILITY

Grade of Security protection ability	Security management maturity	Technology strength
Grade 1	Performed	Prevented
Grade 2	Planned and Performed	Effective Detection
Grade 3	Consistent Policy	Fast Resume
Grade 4	Key Defined	All Controled
Grade 5	Continuously Improving	Sufficiency Validated

TABLE II. JUDGMENT MATRIX OF LEVEL C WITH RESPECT TO LEVEL B1

B1	C1	C2	C3	C4	C5	C6	C7
C1	1	3	4	3	4	5	2
C2	1/3	1	2	1	2	3	1/2
C3	1/4	1/2	1	1/2	1	2	1/3
C4	1/3	1	2	1	2	3	1/2
C5	1/4	1/2	1	1/2	1	2	1/3
C6	1/5	1/3	1/2	1/3	1/2	1	1/4
C7	1/2	2	3	2	3	4	1

TABLE III. JUDGMENT MATRIX OF LEVEL C WITH RESPECT TO LEVEL B2

B2	C1	C2	C3	C4	C5	C6	C7
C1	1	2	2	3	2	5	1
C2	1/2	1	1	2	1	3	1/2
C3	1/2	1	1	2	1	3	1/2
C4	1/3	1/2	1/2	1	1/2	2	1/3
C5	1/2	1	1	2	1	3	1/2
C6	1/5	1/3	1/3	1/2	1/3	1	1/5
C7	1	2	2	3	2	5	1

- Calculate the maximum characteristic root:

$$\lambda_{max}=7.01327. \quad (6)$$

- Calculate and normalize characteristic vector:

$$W_{B2C}=\{0.25,0.13,0.13,0.07,0.13,0.04,0.25\}. \quad (7)$$

- coincidence testing:

$C.R.=\frac{C.I.}{R.I.}=\frac{\lambda_{max}-n}{R.I.\ (n-1)}$ =0.0017<0.10 (referring to table that *R.I.*=1.32) (8)

So the coincidence of the judgment matrix is acceptable.

c) The indicator weight matrix of level C with respect to level B for the security protection ability of Grade 2.

$$W_C=\begin{bmatrix}0.33, & 0.13, & 0.07, & 0.13, & 0.07, & 0.05, & 0.22\\ 0.25, & 0.13, & 0.13, & 0.07, & 0.13, & 0.04, & 0.25\end{bmatrix}. \quad (9)$$

Table IV is an example of the weights for level C with respect to level B through the process and methods above.

3) Judgment matrix and indicator weight of level D with respect to level C and level E with respect to level D

The indicator weights of level D with respect to level C and those of level E with respect to level D will not change from grade to grade. They also don't change according to the business information security or system service security. The weight is stable. So the weight vector can be acquired through the process of building the judgment matrix, calculating the maximum characteristic root, calculating and normalizing characteristic vector. Refer to the example in judgment matrix and indicator weight of level C with respect to level B.

4) Synthetic weight

The synthetic weight is the weight *W* of undermost level(level E) with respect to the upmost level(level A). According to AHP, calculation formula of synthetic weight from control level E to ability level B is as below.

$$W_B=W_C\times W_D\times W_E\ . \quad (10)$$

TABLE IV. WEIGHTS OF LEVEL C

Grade	Ability level	C1	C2	C3	C4	C5	C6	C7

1	**B1**	0.3	0.1	0.1	0.1	0.1	0.1	0.2
	B2	0.25	0.1	0.15	0.1	0.1	0.1	0.2
2	**B1**	0.33	0.13	0.07	0.13	0.07	0.05	0.22
	B2	0.25	0.13	0.13	0.07	0.13	0.04	0.25
3	**B1**	0.2	0.15	0.15	0.15	0.1	0.05	0.2
	B2	0.2	0.15	0.15	0.15	0.1	0.05	0.2
4	**B1**	0.2	0.15	0.15	0.2	0.1	0.05	0.15
	B2	0.2	0.15	0.15	0.2	0.1	0.05	0.15

5) Synthetic Score

The synthetic score is the product of the ultra score of indicators in ability level D and the synthetic weight W_B. The ultra score of indicators in ability level D depends on the result of security control catalog evaluation and overall evaluation. The synthetic score of level D is the product of security control catalog evaluation score and the weight of indicator in level E with respect to level D. The score is divided into two types: the score of business information security ability and the score of system service security ability. The calculation formulas are as below respectively.

$$S_{\mathrm{s}} = \sum_{i=1}^{m} W_{\mathrm{s}i} P_i \quad S_{\mathrm{a}} = \sum_{i=1}^{m} W_{\mathrm{a}i} P_i \quad . \tag{11}$$

Therein, S is the synthetic score of level D. W is the weight and P is the score of corresponding control level. Similarly, the indicator scores of level C, B and A depend on the score of the corresponding lower level and its weight. The calculation formulas are the same as above.

Finally the score of security protection ability of information system is acquired through the calculations above. As a result, the mapping from the evaluation outcome to security protection ability comes true.

V. CONCLUSION

The hierarchy model and successful application in security protection ability evaluation during classified evaluation illustrate that the security protection ability evaluating indicators system based on AHP is an effective quantized method. And the method solves the problems related to mapping the security controls to security protection ability during classified evaluation.

REFERENCES

[1] The General Office of the Central Committee of the Party, the General Office of the State Council, "Requirement about the work of enhancing information security assurance. (GOCCP[2003]27), " August 2003.

[2] MPS, Protection of State Secrets Bureau, State Bureau of Cryptologic Admistration, State Office of Informatization, "Regular for information security classified protection management. (MPS[2007]43) , " June 2007.

[3] GB/T 22239-2008 Information security Technology - Baseline for classified protection of information system.

[4] Qiquan Guo, "The New process of information classified protection.," The twelfth Information security session of China, April 2011.

[5] Shubai Xu, The theory of Analytic Hierarchy Process,Tianjin : Tianjin University publishing House,1988.

[6] Gangquan Xu, "The Application of AHP in decision-making," Journal of Xi' an Institute of Finance & Economics,189(4):39-42,2005.