

An Information Security Management System Based on “Five-in-one”

Li Wencui, Shu Xinjian^a, LiXiong, Gao Hui, Liu Bo, Wang Chunying and Yang Ying^b

Information&Telecommunication Co. of State Grid Henan Electric Power Company, Zhengzhou, 450052, China

^aemail:sxji@chinaren.com, ^bemail:yangzying@126.com

Keywords: five-in-one; information security; three-dimensional management

Abstract. On the basis of “five-in-one” theoretical system, this paper constructs the information security prevention management system which includes responsibility system, standard system, process system, assessment system, institutional system. This system realizes the three-dimensional management of information security from extensive to fine, from point to surface.

Introduction

Information security “five-in-one” management system is based on information security fuzzy simulation system. It regulates how to carry out something according to the institution and adopt what kind of standard, how to reach the target evaluation, rewards and punishments. On the basis of automatic recognition, classification, early warning of information security risk through artificial intelligence, this system can realize an all-round management from before-hand(collect and submit the security state information), intermediate(fuzzy simulation system) to afterwards(security hidden danger disposal) [1-2]. “Five-in-one” information security management system shown as Fig.5 can realize information security hidden danger investigation through some control means.

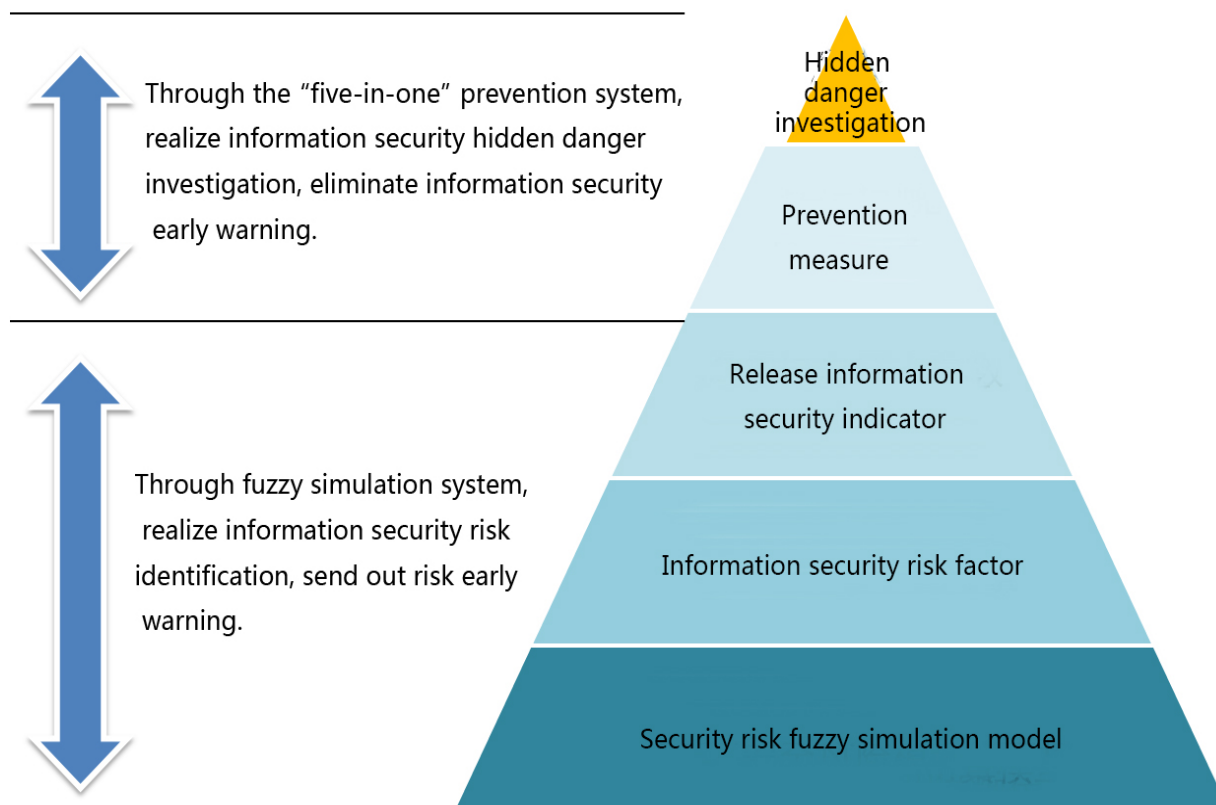


Fig. 1 Management system effect schematic diagram

Construct the Information Security Management Organizational System, Definite Responsibility

Establish “information security prevention leading group”. On the basis of this group, carry out the security policy that “safety first, prevention first, comprehensive control”, promote the information security risk prevention level to the higher hierarchy. Establish information security responsibility system, through clear grade of information security risk management and responsibility of people at all levels, formulate an integrated information security risk management system. Some units, such as information management department, business management department, information system operation department, they must work independently to ensure the quality of the implements of each management measure and the good state of hardware equipment, software system, data, users, physical environment and infrastructure. At the same time, eliminate the information security management blind area, lay a solid foundation for the electric grid information security management [3-4].

Construct the Information Security Standard System, Definite Working Node Quality

Information security prevention system is a new innovation that re-optimize the formulation of standard and utilize these standards comprehensively. Information security standard system construction includes 4 aspects. First, three grades of information security risk, for example, the second grade includes 4 dimensions, the third grade includes 54 dimensions. Classified management is the first step of fine management, classified thought is the guide thought of fine information security management. Second, information security risk factor standard. On the basis of risk classification, which are the information security effect factors? Which are the security factors? Which are the hidden danger factors? Which kind of risk grade these factors should be? All of these need to formulate a scientific assessment standard. This standard is the core of the whole information security prevention system, it determines the prevent ability of this system. Third, there are internal fuzzy calculation standards of intelligent transformation, intelligent analysis, intelligent clustering, intelligent display model in the fuzzy simulation system. These standards are the key factors whether the artificial intelligence can play its role, they can determine whether fuzzy simulation system can guide the hidden danger investigation effectively [5-6]. Fourth, the related working quality standards of risk management and investigation.

Construct the Information Security Process System, Definite Work Flow

Before the construction of information security prevention system, the collection of information security data is dispersed. It is difficult to realize the closed-loop management from risk analysis to management measure implement. All of these easy to cause inefficiency of the whole emergency management work, lacking of propulsion, operating not smooth and so on.

To solve this problem, this paper provides a new method. Through the comprehensive risk management and internal control, construct a more scientific, effective risk management model, establish the information security fuzzy simulation system, the realize the close-loop management that from risk identification to the implement of control measure. The concrete business flow includes factor collection, indicator release, measure registration, measure implement auditing and assessment, hidden danger exhaust. These five layers is integrated. No matter decision-maker, managers or key user, each of them can query every business flow link clearly.

Construct the Information Security Evaluation System, Cash the Rewards

First, strengthen information security risk management through the assessment and supervision model. Combined with risk factor collection, flow management, control measure registration and implement, formulate information security risk check index. Some indexes, such as task processing timely rate, work delay rate, flow complement rate, they can reflect the work situation of information security participants correctly. Some indexes, such as data complete rate, data timely

rate, measure assessment situation, they can reflect the work situation of key users correctly. Through the assessment and supervision, the system can provide a reliable basis for information and security whole process management. At the same time, aiming at the problems in the information security risk management, make policy to promote the implement of the information security measure, ensure the risk management play its role effectively.

Secondly, utilize assistant decision-making and analysis function to strengthen assessment and supervision. On the basis of information security risk index, assessment and supervision, combined with assistant decision-making and analysis function, adopt multi-dimensions analysis method to form the corresponding analysis report and formulate the corresponding control measure. All of this can promote the management level and guide the development of information security work successfully.

Conclusion

This paper constructs the information security prevention management system which is on the basis of “five-in-one” theoretical system. This system realizes the three-dimensional management of information security from extensive to fine, from point to surface. At the same time, each unit can make information security countermeasures and emergency plans according to the existing different information security characters based on this system. These countermeasures and emergency plans can guide the development of information security work and the prevention and of the security incidents.

References

- [1]Xie Ying-jun, Zhang Da-hua. The Research on The Information and Communication Risk Management of Electric Power Enterprise. The Symposium of 2012 Electric Communication Management, 2012, 11.
- [2]Zhen Chen; Fuye Han; Junwei Cao; Xin Jiang; Shuo Chen. Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System[J]. Tsinghua Science and Technology , 2013,2.
- [3]Yang Bin, Zhang Da-hua, Xie Ying-jun. The Research and Design of Intelligent Electric Grid Communication Management System. Telecom Science, 2011.
- [4]YANG Mengke; ZHOU Xiaoguang; ZENG Jianqiu; XU Jianjian. Challenges and Solutions of Information Security Issues in the Age of Big Data [J]. China Communication, 2016,3.
- [5]Information security assurance lifecycle research [J]. The Journal of China University of Posts and Telecommunications, 2007,12.
- [6]Current International Cooperation and Developments in Information Security[J]. Contemporary International Relations, 2007,8.