Acta Universitatis Bohemiae Meridionales
The Scientific Journal for Economics, Management and Trade
České Budějovice, 2010, XIII., (3), s. 89–95

POUŽITÍ DOMNĚNKOVÝCH FUNKCÍ PŘI AUDITU SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ
USING THE EVIDENTIAL REASONING APPROACH IN AUDITING OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

L. Beránek

Abstract

Audit information security management system (ISMS) is an important element of a well-functioning ISM. As part of an ISMS audit, it is also necessary to determine the audit risk. Various methods exist and are developed for risk assessment, both in practical and theoretical level. These methods can use quantitative methods, or may be based on a qualitative assessment of risks. Current standards (e.g. ISO 27001) for construction and operation of the ISMS remain on operators how to carry out risk identification, relevant analyses and evaluations. Various probabilistic methods or methods based on Bayesian statistics are widely used theoretical methods. However, currently there are no generally accepted methods for calculating risk. This is due to the difficulty of quantifying some events and often subjective nature of the analysis.

In this paper, we introduce an evidential reasoning model (evidential reasoning approach under the Dempster-Shafer theory) for the information systems audit risk assessment. The advantage of this approach is the ability to work with indeterminations and subjective evaluations. The proposed model is applied to the assessment of audit risk in the chosen field of standard ISO 27001.

Key words: Information security management system, Information systems audit, Belief functions, Audit risk, ISO 27001

Abstrakt

Audit systému řízení informační bezpečnosti (ISMS) je důležitým prvkem dobře fungujícího systému ISM. V rámci auditu ISMS je rovněž nezbytné stanovit auditorská rizika. Existují různé metody vyvinuty pro hodnocení rizik. Tyto metody používají kvantitativní metody nebo mohou být založeny na kvalitativním hodnocení rizik. Platné standardy (např. ISO 27001) pro implementaci a provozování ISMS nechávají na provozovateli, jak provádět identifikaci rizik, příslušné analýzy a vyhodnocení. Existují modely používající různých pravděpodobnostních metod nebo metod založených na Bayesovské statistice. Nicméně, v současné době neexistují žádné všeobecně uznávané metody pro výpočet auditorského rizika. Důvodem je obtížnost kvantifikace některých událostí a často subjektivní povahy analýzy.

V tomto příspěvku představujeme model pro určení auditorského rizika při auditu systému řízení bezpečnosti informací založený na Dempster-Shaferově teorii domněnkových funkcí (označované také jako teorie důkazu). Výhodou tohoto modelu je schopnost pracovat s neurčitostí a subjektivními hodnoceními. Navržený model pak aplikujeme na určení auditorského rizika ve zvolené oblasti standardu ISO 27001.

Klíčová slova: Systém řízení bezpečnosti informací, audit informačních systémů, domněnkové funkce, audit rizik, ISO 27001.

Reference

[1] International Organization for Standardization [online]. 2010 [cit. 2010-09-16]. ISO/IEC 27001:2005. Dostupný z WWW: <http://www.iso.org/iso/catalogue_detail?csnumber=42103>.

[2] CRAMM. The total information security toolkit [online]. 2010 [cit. 2010-08-18]. Dostupný z WWW: <http://www.cramm.com/>.

[3] Beránek, L. Auditing Electronic Auction Systems: Knowing the Risks. ISACA Journal: Journal Online [online suplement]. 2010, 4, August, [cit. 2010-08-18]. Dostupný z WWW: <http://www.isaca.org/Journal>. ISSN 1526-7407.

[4] Shafer, G. *A Mathematical Theory of Evidence*. Princeton University Press, 1976, 297 p.

[5] Srivastava, R., Mock, T. Why We Should Consider Belief Functions in Audit Research and Practice. *The Auditor's Report*. 2005, Vol. 28, No. 2.

[6] Srivastava, R., Shafer, G. Belief-Function Formulas for Audit Risk. *The Accounting Review*. 1992, Vol. 67, No. 2.

[7] Sun, L., Srivastava, R., Mock, T. An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*. 2006, Vol. 22, No. 4.

[8] Beránek, L., Tlustý, P., Remeš, R. An Online Auction Trust Model for Based on the Contextual Information. In *Proceedings of the Workshop on the Theory of Belief Functions* (Belief 2010), Brest, France, 1−2 April 2010, Paper 110, s. 1−6.
[9] International Organization for Standardization [online]. 2010 [cit. 2010-09-16]. ISO/IEC 27002:2005. Dostupné z WWW: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm?csnumber=50297>.
[10] Peltier, T. R. *How to Complete a Risk Assessment in 5 Days or Less*. Auerbach Publications, London, 2008, 444 p.

Contact address – Kontaktní adresa:

Ing. Ladislav Beránek, CSc.
Jihočeská univerzita v Č. Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky
Studentská 13
370 05 České Budějovice
E-mail: beranek@ef.jcu.cz
Tel. 389 032 511