malicious insiders, International Journal of Business Process Integration and Management, 8(2): 114-119. https://doi.org/10.1504/IJBPIM.2017.083794
[23] Matthews, G., Reinerman-Jones, L., Wohleber, R., Ortiz, E. (2017). Eye tracking metrics for insider threat detection in a simulated work environment. Proceedings of the Human Factors and Ergonomics Society, 61(1): 202-206. https://doi.org/10.1177/1541931213601535
[24] Takabi, H., Hashem, Y., Dantu, R. (2018). Prediction of human error using eye movements patterns for unintentional insider threat detection. Proceedings of the IEEE 4th International Conference on Identity, Security, and Behaviour Analysis. https://doi.org/10.1109/ISBA.2018.8311479
[25] IAEA Preventive and protective measures against insider threats. (20018). International Atomic Energy Agency, Vienna, Austria.
[26] Duran, F.A., Conrad, S.H., Conrad, G.N., Duggan, D.P., Held, E.B. (2009). Building a system for insider security. IEEE Security & Privacy, 7(6): 30-38. https://doi.org/10.1109/MSP.2009.111
[27] Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T., Whitty, M. (2014). Understanding insider threat: a framework for characterising attacks. Proceedings of the IEEE Security and Privacy Workshops, 214-228. https://doi.org/10.1109/SPW.2014.38
[28] Kammuller, F., Nurse, J.R.C., Probst, C.W. (2016). Attack tree analysis for insider threats on the IoT using Isabelle. Proceedings of the 4th International Conference on Human Aspects of Security, Privacy and Trust.
[29] Musman, S., Turner, A.J. (2018). A game oriented approach to minimizing cybersecurity risk. International Journal of Safety & Security Engineering, 8(2): 212-222. https://doi.org/10.2495/SAFE-V8-N2-212-222
[30] Chim, L., Bilusich, D., Lord, S., Nunes-Vaz, R. (2017). A risk-based layered defence for managing the trusted insider threat. Journal of Information System Security, 13(3): 151-173.
[31] Bilusich, D., Chim, L., Nunes-Vaz, R.A., Lord, S. (2018). There is no single solution to the 'insider' problem but there is a valuable way forward. WIT Transactions on Engineering Sciences, 121: 135-146. https://doi.org/10.2495/RISK180121
[32] Nunes-Vaz, R., Lord, S., Bilusich, D. (2014). From strategic security risks to national capability priorities. Security Challenges, 10(3): 23-49.
[33] Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., Longstaff, T., Spitzner, L., Haile, J., Copeland, J., Lewandowski, S. (2005). Analysis and detection of malicious insiders. Proceedings of the International Conference on Intelligence Analysis.
[34] Cole, E., Ring, S. (2006). Insider threat: protecting the enterprise from sabotage, spying, and theft, Syngress, Rockland MA.
[35] Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6): 472-484. https://doi.org/10.1016/j.cose.2005.05.002
[36] Catrantzos, N. (2010). Tackling the insider threat, ASIS International Foundation CRISP Report.
[37] Montelibano, J., Moore, A. (2012). Insider threat security reference architecture. Proceedings of the 45th Annual Hawaii International Conference on System Sciences, pp. 2412-2421. https://doi.org/10.1109/HICSS.2012.327
[38] Park, S., Ruighaver, A.B., Maynard, S.B., Ahmad, A. (2012). Towards understanding deterrence: information security manager's perspective. Proceedings of the International Conference on IT Convergence and Security, pp. 21-37. https://doi.org/10.1007/978-94-007-2911-7_3
[39] Australian Government. (2016) Managing the insider threat to your business: A personnel security handbook.
[40] Buckley, O., Nurse, J.R.C. Legg, P.A. Goldsmith, M., Creese, S. (2014). Reflecting on the ability of enterprise security policy to address accidental insider threat. Proceedings of the Workshop on Socio-Technical Aspects in Security and Trust, pp. 8-15. https://doi.org/10.1109/STAST.2014.10
[41] Stavrou, V., Kandias, M., Karoulas, G., Gritzalis, D. (2014). Business process modeling for insider threat monitoring and handling. In: Eckert, C., Katsikas, S.K., Pernul, G. (eds.) Trust, Privacy, and Security in Digital Business, Springer, 119-131. https://doi.org/10.1007/978-3-319-09770-1_11
[42] Forcht, K.A. (1994). Computer security management, Boyd & Fraser, Danvers MA.
[43] Straub, D.W., Welke, R.J. (1998). Coping with systems risk: security planning models for management decision making. Management Information Systems Quarterly, 22(4): 441-469.
[44] Stolfo, S., Bellovin, S.M., Evans, D. (2011). Measuring security. IEEE Security & Privacy, 9(3): 60-65. https://doi.org/10.1109/MSP.2011.56
[45] Pan, L., Tomlinson, A. (2016). A systematic review of information security risk assessment. International Journal of Safety & Security Engineering, 6(2): 270-281. https://doi.org/10.2495/SAFE-V6-N2-270-281
[46] Nunes-Vaz, R., Lord, S., Ciuk, J. (2011). A more rigorous framework for security-in-depth. Journal of Applied Security Research, 6(3): 372-393. https://doi.org/10.1080/19361610.2011.580283
[47] Lord, S., Nunes-Vaz, R. (2013). Designing and evaluating layered security. International Journal of Risk Assessment and Management, 17(1): 19-45. https://doi.org/ 10.1504/IJRAM.2013.054377
[48] Nunes-Vaz, R., Lord, S. (2014). Designing physical security for complex infrastructures. International Journal of Critical Infrastructure Protection, 7(3): 178-192. https://doi.org/10.1016/j.ijcip.2014.06.003
[49] Rowe, C., Seif Zadeh, H., Garanovich, I.L., Jiang, L., Bilusich, D., Nunes-Vaz, R., Ween, A. (2017). Prioritizing investment in military cyber capability using risk analysis. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 16(3): 1-13. https://doi.org/10.1177/1548512917707077
[50] ISO/IEC 31000:2009 Risk Management – Principles and Guidelines.

NOMENCLATURE

C	consequence
P	probability
R	risk