**BIBLIOGRAPHY**

1. Bo, T., Chen, Y., Wang, C., Zhao, Y., Lam, K.Y., Chi, C.H. and Tian, H., 2019, November. TOM: A Threat Operating Model for Early Warning of Cyber Security Threats. In *International Conference on Advanced Data Mining and Applications* (pp. 696-711). Springer, Cham.
2. Petrenko, S.A. and Makoveichuk, K.A., 2017. Big data technologies for cybersecurity. In *CEUR Workshop* (pp. 107-111).
3. Vigneswaran, K.R., Vinayakumar, R., Soman, K.P. and Poornachandran, P., 2018, July. Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.
4. Ramaki, A.A. and Atani, R.E., 2016. A survey of IT early warning systems: architectures, challenges, and solutions. *Security and Communication Networks*, *9*(17), pp.4751-4776.
5. Park, J. and Park, M., 2016. Qualitative versus quantitative research methods: Discovery or justification?. *Journal of Marketing Thought*, *3*(1), pp.1-8.
6. Brannen, J. ed., 2017. *Mixing methods: Qualitative and quantitative research*. Routledge.
7. Abildgaard, J.S., Saksvik, P.Ø. and Nielsen, K., 2016. How to measure the intervention process? An assessment of qualitative and quantitative approaches to data collection in the process evaluation of organizational interventions. *Frontiers in Psychology*, *7*, p.1380.

8) Zheng, W.K. and Liu, K., 2017, May. Research on network intrusion detection technology in dynamic and complex background. In *2017 2nd International Conference on Materials Science, Machinery and Energy Engineering (MSMEE 2017)*. Atlantis Press.