Bibliografia

[1] Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress.

[2] Barreno, M., Nelson, B, Joseph, A. i Tygar, J. (2010) The security of machine learning. Machine Learning, 81(2), 121 – 148.

[3] Barreno, M., Nelson, B., Sears, R., Joseph, A. i Tygar, J. (2006). Can machine learning be secure? W: ASIACCS'06.

[4] Bubnicki, Z. (1974). Identyfikacja obiektów sterowania. Warszawa: PWN.

[5] Chen, T., Liu, J., Xiang, Y., Niu, W., Tong, E. i Han, Z. (2019). Adversarial attack and defense in reinforcement learning-from AI security view. Cybersecurity, 2.

[6] Chhabra, A., Roy, A. i Mohapatra, P. (2019). Strong Black-box Adversarial Attacks on Unsupervised Machine Learning Models. Cybersecurity, 11. Suspicion-Free Adversarial Attacks on Clustering Algorithms.

[7] Chhabra, A., Roy, A. i Mohapatra, P. (2020). AAAI 2020 Main Technical Conference, cyt. jako: arXiv:1911.07015 [cs.LG].

[8] Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A. i Mukhopadhyay, D. (2018). Adversarial Attacks and Defences: A Survey, cyt. jako: arXiv:1810.00069 [cs.LG].

[9] Cichosz, P. (2009). Systemy uczące się. Warszawa: WNT.

[10] Dalvi, N., Domingos, P., Sumit, M. i Verma, D. (2004). Adversarial classification. W: Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'04). ACM Press.

[11] Deldjoo, Y., Di Noia, T. i Merra, F.A. (2020). Adversarial Machine Learning in Recommender Systems: State of the art and Challenges, cyt. jako: arXiv:2005.10322 [cs.IR].

[12] Gleave, A., Dennis, M., Wild, C., Kant, N., Levine, S. i Russell, S. (2020). Adversarial Policies: Attacking Deep Reinforcement Learning, cyt. jako arXiv:1905.10615 [cs.LG].

[13] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. i Bengio, Y. (2014). Generative Adversarial Networks, cyt. jako: arXiv:1406.266.

[14] Huang, L., Joseph, A., Nelson, B., Rubinstein, B. i Tygar, J. (2011). Adversarial machine learning. W: Proceedings of the 4th ACM workshop on Security and artificial intelligence (AISec '11). ACM Press.

[15] Kloft , M. i Laskov, P. (2010). Online Anomaly Detection under Adversarial Impact. W: Y. Whye Teh i M. Titterington (red.), Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics (Proceedings of Machine Learning Research), Vol. 9. PMLR, Chia Laguna Resort, Sardinia, Italy.

[16] Kurzyński, M. (1997). Rozpoznawanie obrazów. Metody statystyczne. Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej.

[17] Laskov, P. i Kloft , M. (2009). A framework for quantitative security analysis of machine learning. W: Proceedings of the 2th ACM workshop on Security and artificial intelligence (AISec'09). ACM Press.

[18] Li, B., Wang, Y., Singh, A. i Vorobeychik, Y. (2016). Data Poisoning Attacks on Factorization-Based Collaborative Filtering, cyt. jako: arXiv:1608.08182.

[19] Liderman, K. (2017). Bezpieczeństwo informacyjne. Warszawa: Wydawnictwo Naukowe PWN.

[20] McDaniel, P., Papernot, N. i Celik, Z. (2016). Machine Learning in Adversarial Settings. IEEE Security & Privacy, May/June.

[21] Mitchell, T.M. (1997). Machine Learning. McGraw-Hill.

[22] Muñoz-González, L. (2019). The Security of Machine Learning Systems. W: AI in Cybersecurity. Springer.

[23] Nelson, B. (2010). Behavior of Machine Learning Algorithms in Adversarial Environments. Technical Report No. UCB/EECS-2010-140. Electrical Engineering and Computer Sciences, University of California at Berkeley.

[24] Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. i Swami, A. (2017). Practical Black-Box Attacks against Machine Learning. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). New York: ACM.

[25] Popper, R. (2002). Logika odkrycia naukowego. Warszawa: Wydawnictwo Naukowe PWN.

[26] Ricci, F., Rokach, L. i Shapira, B. (2011). Introduction to Recommender Systems Handbook, Recommender Systems Handbook. Springer.

[27] Surma, J. (2011). Business Intelligence: Making Decisions Through Data Analytics. New York: Business Expert Press.

[28] Surma, J. (2017). Cyfryzacja życia w erze Big Data: człowiek, biznes, państwo. Warszawa: Wydawnictwo Naukowe PWN.

[29] Wang, Sh., Nepal, S., Rudolph, C., Grobler, M., Chen, Sh., Chen, T. (2020). Backdoor Attacks against Transfer Learning with Pre-trained Deep Learning Models. IEEE, Surya Nepal.