



IMPROVING METHODS FOR DETECTION AND PREVENTION OF CYBERATTACKS BASED ON ARTIFICIAL INTELLIGENCE

Mirjamolova Muxlisa Abdug'affor qizi

Senior Lecturer, Department of Information Systems and
Technologies,

Tashkent State University of Economics, Uzbekistan

mirjamolova.muxlisa@mail.ru

Abstract: *This in the article artificial intellect and mechanical education from technologies using modern cyberattacks determination and prevent to take issues research Network traffic analysis to make, anomalies detection , attacks classification and real -time security in mode provide opportunities seeing Also, artificial intellect to the models adversarial threats against and from them protection methods analysis will be done.*

Key words: *cybersecurity, cyberattack, artificial intelligence, machine education , network security, anomaly , adversarial attack.*

Information and communication technologies intense development all in the fields digital from technologies use of the scale to the expansion take is coming. Electronic government, digital economy, remote education, electronic commerce and banking services development with one in line information to systems relatively Cyber threats are also increasing. Modern cyberattacks complicated to the structure has to be, attackers different automated tools and advanced from technologies is using. Therefore information systems in defense traditional security tools with one in line artificial intellect from technologies use current to the point is spinning [1].

Cybersecurity systems main from the duties one online normal activity determination and from it difference doer suspicious actions own on time from determining consists of . Traditional attacks determination systems , usually in advance known was attacks for created rules and to signatures relies on. Such systems known attacks in determining effective although , new , modified or previously unknown was to threats relatively limited to opportunities has . Mechanical education algorithms and big in size network information analysis to do through different features between dependencies determination and suspicious activity automatic accordingly designation opportunity gives [2].

Artificial intellect based on cybersecurity in systems information assembly , cleaning , features separate to get , model teaching and the results assessment such as stages done Initially network from devices packets , connections , protocols , ports , IP addresses and other technician indicators will be collected . Next in stages excess or wrong information again This is processed . process model accuracy and work to the speed directly impact shows .

Mechanical education methods two main to the group separation possible : control under and uncontrolled Training . Supervision under The model in teaching is normal and harmful from traffic organization found designated information package based on is taught . In this classification algorithms new traffic in advance designated to classes For example , the system is connected normally , DDoS attack , ports scan or other harmful activity types differentiation possible [3].

Uncontrolled education in methods and information in advance designated to classes not separable . Algorithm information in the content general laws determines and usual from behavior noticeable at

the level difference doer samples anomaly as This defines approach previously unknown was cyberattacks in determining important importance has . However such normal in systems and anomalous activity right separation complicated to be possible .

Last in years deep teaching algorithms are also cybersecurity in matters wide is being used . Neuron networks big in size from data complicated features automatic accordingly separate to take to the possibility has . Convolutional neuron networks network in the data local dependencies in detection , recurrent neuron networks and time according to sequences analysis in doing application possible . Therefore deep education methods network attacks determination and in classification promising from directions one is [4].

Cyberattacks determination model efficiency assessment for one how many from the criteria use necessary . Most many applicable indicators accuracy , precision, recall and F1-criterion are considered . Accuracy of common test samples how many right classified shows , by precision model considered an attack samples inside really attack those who were share Recall represents there is attacks how many that was determined The F1 criterion is the difference between precision and recall . balance assessment opportunity gives .

Cybersecurity in systems lie positive the results are also serious problem If the system is a normal user activity permanent accordingly attack as if it is determined , security to employees excess loading to the surface On the contrary , it is harmful . normal activity as acceptance to do further serious to the consequences take arrival possible . Therefore cyberattacks determination system in creation only high to accuracy not , maybe of errors Pay attention to the character too. focus necessary [5].

Artificial intellect technologies development with one of AI models in a row to oneself against aimed at Threats also appear Adversarial attacks are happening . so attacks , in which to the model presented being done to the information human for almost imperceptible , but model - dependent impact doer changes is included . In cybersecurity such approach attack determination model distraction and harmful activity hide for usage possible [6].

Adversarial threats against in the fight model stability education , training information protection and the model different attack scenarios based on from the test transfer important . From this except for the data in advance again performance , features selection , adversarial samples based on education and one how many models the results combine such as from methods use possible . Such approaches artificial intellect based on cybersecurity systems reliability to increase service does .

Real time in mode working cybersecurity in systems information fast again work separately importance has . On the network every one connection far time during analysis to do practical in terms of ineffective to be possible . Therefore the model working on the way out not only accuracy , maybe calculation complexity and answer to give considering the speed to take Especially corporate networks , financial organizations and big in size information real- time in systems monitoring of cybersecurity in the mode important structural part is considered .

Artificial of intellect again one important opportunity — cyberattacks automatic answer return process For example , the system suspicious connection when he/she finds out to the administrator message send , malicious IP address temporarily blocking or relevant network resource activity limit possible . Such automation human

intervention reduce , threaten answer to give time reduces . However automatic answer mechanisms working on the way out wrong decisions because of legal users of activity limitation considering the possibility to be taken need .

In cybersecurity artificial from the intellect of use promising from directions one hybrid models working Hybrid in systems to the signature based determination , rule analysis and mechanical education algorithms together is used . Such approach known attacks fast determination with together unknown also detect anomalies opportunity creates . Also , federative education from technologies use through secret information central to the server without sending models teaching opportunity This is personal and corporate information protection to do point from the point of view important is considered .

Analyses this shows that artificial intellect based on cybersecurity systems big in size information automatic analysis to make , anomalies determination and cyberattacks fast answer to give opportunities However , the AI model efficiency education your information quality of data representativeness , model architecture and assessment to the methodology depends on . From this In addition , AI models to oneself adversarial attacks against existence security systems in design separately attention demand does .

Conclusion as artificial , so to speak intellect and mechanical teaching from technologies use modern cyberattacks determination and prevent to take important from directions Especially the network real - time traffic in mode analysis to do , unknown anomalies detection , attacks automatic classification and to them fast answer return opportunities this of technologies practical importance increases . In the

future hybrid AI models , federated education methods and adversarial attacks resistant algorithms develop cybersecurity systems reliability further increase possible.

Used literature :

1. Buczak AL, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. - 2016. - Vol. 18, No. 2. – P. 1153–1176. <https://doi.org/10.1109/COMST.2015.2494502>.
2. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges // Cybersecurity. - 2019. - Vol. 2. – Article 20. <https://doi.org/10.1186/s42400-019-0038-7>.
3. Sommer R., Paxson W. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // 2010 IEEE Symposium on Security and Privacy. – IEEE, 2010. – P. 305–316. <https://doi.org/10.1109/SP.2010.25>.
4. Shone N., Ngoc TN, Phai VD, Shi Q. A Deep Learning Approach to Network Intrusion Detection // IEEE Transactions on Emerging Topics in Computational Intelligence. - 2018. - Vol. 2, No. 1. – P. 41–50. <https://doi.org/10.1109/TETCI.2017.2772792>.
5. Ferrag MA, Maglaras L., Moschoyiannis S., Janicke H. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study // Journal of Information Security and Applications. - 2020. - Vol. 50. – Article 102419. <https://doi.org/10.1016/j.jisa.2019.102419>.

6. Goodfellow IJ, Shlens J., Szegedy C. Explaining and Harnessing Adversarial Examples // International Conference on Learning Representations (ICLR). - 2015.
7. Mirjamolova MA, Tursunboev Sh.Y. Modern information systems electronic government and services field digitization features // Results of National Scientific Research. - 2023. - Vol. 2, No. 5. – B. 436–442.