KIBERXAVFSIZLIK TIZIMIDA SUN'IY INTELLEKTNING TUTGAN O‘RNI

Avazbek Sayfiddinov
Toshkent davlat yuridik universiteti
avazbeksayfiddinov23@gmail.com

Annotatsiya: Kibertahdidlar ko‘lami va murakkabligi bo‘yicha o‘sib bormoqda va bu o‘z tarmoqlari va ma’lumotlarini himoya qilishga urinayotgan tashkilotlar uchun katta muammo tug‘dirmoqda.[1] Sun’iy intellekt (AI) xavfsizlik guruhlariga ushbu muhit bilan hamnafas bo‘lishda yordam beradigan muhim vosita sifatida paydo bo‘lmoqda. AI va mashinani o'rganish algoritmlari zararli dasturlarni aniqlashdan tortib, insayder tahdidlarni aniqlashgacha bo'lgan kiberxavfsizlik operatsiyalarini o'zgartirish imkoniyatiga ega. Biroq, AIdan foydalanish tashkilotlar tushunishi va kamaytirishi kerak bo'lgan xavflarni ham keltirib chiqaradi. Ushbu maqola bebaho texnologiya sifatida, balki puxta nazoratni talab qiladigan texnologiya sifatida kiberxavfsizlikda AIning hozirgi va kelajakdagi roli haqida umumiy ma'lumot beradi.

Kalit so‘zlar: Sun’iy intellekt, kibertahdid, kiberxavfsizlik, zararli dastur, mashinani o‘rganish.

AI vazifalarni avtomatlashtirish, naqshlarni aniqlash va bashorat qilish qobiliyati tufayli kiberxavfsizlikning ko'p jihatlari uchun juda mos keladi. Xavfsizlik guruhlari odamlar qo'lda tahlil qila oladiganidan ko'ra ko'proq ma'lumotlar, ogohlantirishlar, zararli dastur na’munalari va xavfsizlik hodisalari bilan kurashmoqda.[2] AIning naqshni aniqlash qobiliyati ushbu ma'lumotlar oqimini qayta ishlashga yordam beradi. Mashinani o‘rganish algoritmlari foydalanuvchi yoki qurilmaning noodatiy xatti-harakatlari asosida paydo bo‘layotgan hujumlarni aniqlaydigan modellarni yaratish uchun tarmoqdagi oddiy va zararli faoliyatdan iborat ma’lumotlar to‘plamida o‘qitilishi mumkin.[3] Quyida kibermudofaa choralarini kuchaytirish uchun sun’iy intellektning eng yaxshi ilovalari keltirilgan:

Zararli dasturiy ta'minotni aniqlash – AI algoritmlarini mutaxassis tomonidan to'liq tahlil qilmasdan yangi zararli dastur namunalarini aniqlash uchun zararli dastur kodlari ma'lumotlar bazalarida o'qitilishi mumkin. Bu qo‘lda qo‘llash usullariga nisbatan hujum kodining ancha yuqori qismini tahlil qilish imkonini beradi.[4] Chuqur o‘rganish modellari zararli dasturlarning xususiyatlariga asoslanib umumlashtirishi va mutlaqo yangi variantlarni aniqlashi mumkin.

Tarmoq monitoringi – AI vositalari oddiy tarmoq trafigini o'rganishi va kiberhujumlar yoki ichki tahdidlar haqida signal berishi mumkin bo'lgan anomaliyalar yuzaga kelganda ogohlantirishlarni ishga tushirishi mumkin. Ushbu anomaliyalarni aniqlash tarmoq faoliyatining murakkabligi va hajmi tufayli juda qiyin. Sun'iy intellektning naqshni aniqlash qobiliyatlari an'anaviy qoidaga asoslangan monitoringga qaraganda vazifaga ko'proq mos keladi.[5]

Firibgarlikni aniqlash – AI oddiy xatti-harakatni aks ettiruvchi profillarni ishlab chiqish uchun katta miqdordagi moliyaviy mijozlar

ma'lumotlarini tahlil qilishi mumkin. Ushbu profillar foydalanuvchining qonuniy xatti-harakatlari bilan solishtirganda statistik ko'rsatkichlar bo'lgan to'lov yoki tizimga kirish harakatlarini topish uchun yangi tranzaksiya ma'lumotlarini real vaqt rejimida tahlil qilish imkonini beradi.[6] Bu hisobni o'g'irlash, moliyaviy o'g'irlik yoki insayderdan noto'g'ri foydalanishni tezroq aniqlash imkonini beradi.

Spamni filtrlash – Elektron pochta spamlarini filtrlash xavfsizlikda AIning dastlabki namunasini taqdim etadi. Mashinani o'rganish usullari spam filtrlariga elektron pochta xabarlarining matn tarkibini tahlil qilish va spamni oddiy elektron pochtadan ajratib turadigan statistik naqshlarni aniqlash imkonini beradi. Algoritmlar yangi xatlarni spam yoki haqiqiy deb tasniflash uchun ushbu naqshlarni qo'llashi mumkin.[7]

Foydalanuvchi va qurilma xatti-harakatlari tahlili - AI foydalanuvchi yoki qurilma faoliyatidagi naqshlarni tahlil qilish orqali oddiy xatti-harakatlarni aks ettiruvchi modellarni yaratishi va xavfsizlik xavfi yoki tahdidini ko'rsatishi mumkin bo'lgan noaniq hodisalarni aniqlashi mumkin. Bu buzilgan foydalanuvchi hisoblari, kiberhujumlar yoki siyosat buzilishini aniqlash imkonini beradi.[8] AI bilan xatti-harakatlar tahlilining asosiy afzalliklari qoidalar yoki imzolarni ishonchli aniqlash qiyin bo'lgan murakkab naqshlarni tahlil qilish qobiliyatini o'z ichiga oladi.

Xavfsizlikni tartibga solish, avtomatlashtirish va javob berish (SOAR) – AI tahdidlarga javob berishni tezlashtirish uchun xavfsizlik vositalari bo‘ylab ish oqimlarini tartibga soluvchi SOAR platformalari orqali o‘sib borayotgan avtomatlashtirish rolini o‘ynamoqda.[9] Mashinani o‘rganish aqlli avtomatlashtirish va kuzatish haqida ma’lumot beruvchi naqshni aniqlashni ta’minlash orqali SOAR imkoniyatlarini yanada kengaytiradi. AI bilan

jihozlangan SOAR xavfsizlik operatsiyalari samaradorligi va izchilligini oshiradi.

Kiberxavfsizlik uchun AIning xavflari va muammolari

AI kiberxavfsizlik uchun o'yinni o'zgartiruvchi texnologiya bo'lishni va'da qilganidek, u ehtiyotkorlik bilan amalga oshirish va nazorat qilish orqali hal qilinishi kerak bo'lgan yangi xavflarni ham keltirib chiqaradi:

AI bilan tushuntirish mumkin bo'lgan qiyinchiliklar – Bugungi kunda qo'llaniladigan eng kuchli AI algoritmlarining ko'pchiligi murakkab neyron tarmoqlar bo'lib, ular yuqori aniqlikka ega, lekin asosan "qora qutilar" sifatida ishlaydi, ularning natijalari ortidagi asosiy sabablarni tushuntirmaydi. Tushuntirishning yo'qligi xavfsizlik guruhlari uchun juda muammoli bo'lishi mumkin, agar AI modeli biznes operatsiyalariga ta'sir qiladigan noto'g'ri qaror qabul qilsa. Davom etayotgan AI tadqiqotlari neyron tarmoqlarni yanada tushunarli qilishga qaratilgan.[10]

AIga haddan tashqari ishonish – Avtomatlashtirilgan echimlarga haddan tashqari ishonch tufayli xavfsizlik guruhlari inson tajribasi va mulohazalari hisobiga sun'iy intellektga haddan tashqari ishonib qolishlari mumkin. Insoniy tahlilchilarni to‘liq almashtirishdan ko‘ra ko‘paytirish va yaxshilash uchun sun’iy intellektdan oqilona foydalanilishini ta’minlash muhim. Odamlar xavfsizlik hodisalari atrofidagi biznes kontekstini ko'rib chiqish va mas'uliyatli xavf qarorlarini qabul qilish uchun faol ishtirok etishlari kerak.[11]

Avtomatlashtirishning salbiy ta'siri – AI zararli dasturlarni tahlil qilish kabi sohalarda foydali avtomatlashtirishni ta'minlasa-da, juda ko'p avtomatlashtirish xavfsizlik uchun salbiy tomonlarga ham ega bo'lishi mumkin. Haddan tashqari avtomatlashtirish ishchi kuchining malakasini yo'qotishi

mumkin, chunki ba'zi vazifalar eskirgan. Tahlilchilar hodisalarni sinchkovlik bilan tekshirish uchun hali ham zarur bo'lgan an'anaviy xavfsizlik texnikasidan foydalanish malakasini yo'qotishi mumkin. Ishchi kuchi o'z malakalarini moslashtirish uchun doimiy ravishda qayta tayyorlashga muhtoj.[12]

AI manipulyatsiyasi va qochish hujumlari – AI xavfsizlik vazifalari uchun hamma joyda paydo bo'lganligi sababli, tajovuzkorlar zararli harakatlarni yashirish uchun algoritmlarni manipulyatsiya qilishga va ulardan qochishga harakat qilishadi. Spam xatlar spam-filtrlarni chetlab o'tishning innovatsion usullarini ishlab chiqqanidek, AI himoyasini aldash uchun yangi usullar qo'llaniladi.[13] Algoritmlar paydo bo'layotgan hujumlarga moslashish uchun doimiy sozlash, qayta tayyorlash va yangi ma'lumotlar kiritishni talab qiladi.

Sun'iy intellektdan mas'uliyatli va axloqiy foydalanish – AI xavfsizlik operatsiyalarida katta rol o'ynaganligi sababli, tashkilotlar mas'uliyatli boshqaruv bilan uning axloqiy jihatdan qo'llanilishini ta'minlashi kerak. AI modellari xodimlar monitoringi, firibgarlikni tekshirish yoki tarmoqqa kirish huquqlari kabi masalalar bo‘yicha nohaq yoki noxolis qaror qabul qilishga olib keladigan noto‘g‘ri modellarni o‘rnatishi mumkin.[14] Modelning potentsial tarafkashliklarini tahlil qilish va kamsituvchi natijalarning oldini olish uchun proaktiv nazorat talab qilinadi.

Kiberxavfsizlikda AI kelajagi

Mas'uliyatli nazoratga muhtoj bo'lishiga qaramay, AI kelgusi o'n yil ichida tobora ortib borayotgan tahdidlarga duch kelayotgan raqamli, bog'langan dunyoda kiberxavfsizlik texnologiyasini inqilob qilishi kutilmoqda. Kelajakda paydo bo'lishi mumkin bo'lgan ba'zi ilovalar quyidagilardan iborat:

Bashoratli sun’iy intellekt xavfsizlik modellari – AI tashkilot va uning sohadagi tengdoshlari bo‘ylab aniqlangan tajovuzkorlarning yangi xatti-harakatlarini oldindan ko‘rish, zaifliklarni proaktiv tarzda aniqlash, kelajakdagi xavfsizlik stsenariylarini modellashtirish va hodisalar ro‘y berishidan oldin profilaktika nazoratini belgilash uchun kelajakdagi ko‘rinishga ega bo‘ladi.[15]

AI tomonidan kengaytirilgan inson tahlilidan kengaytirilgan foydalanish – odamlar va sun'iy intellektning kuchli tomonlarini muvozanatlash uchun sun'iy intellektni kuchaytirish modellarini ko'proq qabul qilish kutilmoqda, bunda AI katta hajmdagi ma'lumotlarni qayta ishlash va eng shubhali tahdidlarni yuborish orqali tergov va tahdidlarni modellashtirishning dastlabki bosqichlarini tezlashtiradi. insoniy tahlil.[16] Imkoniyatga asoslangan mehnatni taqsimlash umumiy xavfsizlik samaradorligini maksimal darajada oshiradi.

Boshlash uchun asosiy xavfsizlik funksiyalarini avtomatlashtirish – AI uchun yangi tashkilotlar ko'pincha muvaffaqiyatsizlik xavfi yuqori bo'lgan ilg'or foydalanish holatlarini sinab ko'rishadi. Sohaning ilg‘or amaliyoti oddiyroq xavfsizlik jarayonlari atrofidagi konsepsiyaning sun’iy intellektni isbotlashi bilan boshlanadi va so‘ngra qiyinroq muammolarni hal qilishdan oldin o‘rganishlar ko‘lamini asta-sekin kengaytiradi.[17] Dastlabki muvaffaqiyatlar AIga tashkilot ishonchini yaratadi. ikal sanoat uchun AIning ixtisoslashuvi – Korxona xavfsizligini aniqlash uchun umumiy AI etuklashishda davom etsa-da, vertikal sanoatning noyob tahdid modellariga moslashtirilgan sun'iy intellekt sezilarli darajada o'sadi. Algoritmlar sog'liqni saqlash, moliyaviy xizmatlar, chakana savdo, davlat va boshqa vertikallarda mijozlar uchun kontekst va aniqlikni yaxshilaydigan sanoat nuanslarini o'rganish uchun sohaga oid ma'lumotlardan foydalangan holda o'qitiladi.[18]

Insayder tahdidlarni aniqlash – Xavfsizlik sohasida sun'iy intellekt uchun eng tez rivojlanayotgan ilovalardan biri bu potensial insayder tahdidlarni aniqlash uchun xodimlar faoliyati, kirish jurnallari va elektron pochta xabarlaridagi modellarni modellashtirishdir. Tashqi tajovuzkorlar ko'pincha ichki ma'lumotlarga kirishga ishonishadi. Insayder tahdidlarini aniqlash uchun AI xatti-harakatlari tahlili davlat va xususiy sektor tashkilotlari uchun asosiy ustuvor vazifadir.

Xulosa

Kiberxavflarning ko'lami va murakkabligi AI tomonidan boshqariladigan tobora avtomatlashtirilgan xavfsizlik texnikasini talab qiladi. Zamonaviy kibertahdidlarning hajmi va murakkabligini moslashtirish faqat qo'lda inson texnikasi yordamida imkonsiz bo'lib bormoqda. AI kibermudofaa uchun o'yinni o'zgartiruvchi texnologiya bo'lishni va'da qilmoqda. Biroq, modellar tushunarli, adolatli bo'lishini ta'minlash va ularni almashtirishdan ko'ra inson xavfsizligi guruhlarini kuchaytirishga yo'naltirilganligini ta'minlash uchun ehtiyotkorlik bilan boshqarilishi kerak. Doimiy sozlash uchun moslashuvchanlik bilan muvozanatlangan sun'iy intellekt nazorati salbiy oqibatlarning oldini olish bilan birga, algoritmlarda mustahkam innovatsiyalarni ta'minlaydi. Sun'iy intellektdan mas'uliyatli foydalanish unga raqamli himoyaga muhtoj bo'lgan dunyoda kiberxavfsizlikni kuchaytirishda juda qimmatli rol o'ynashga imkon beradi.

Foydalanilgan adabiyotlar

1. Voo, J., Hemavathi, A., Pu, C. et al. Cyber threat intelligence and analytics. SN COMPUT. SCI. 1, 160 (2020). https://doi.org/10.1007/s42979-020-00160-9

2. Al-Hawawreh, Mousa and Sitnikova, Elena, Identification of Threat Intelligence Services Providers: An Overview (October 27, 2018). 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018, Available at SSRN: https://ssrn.com/abstract=3321459

3. Jordan, Micheal and Mitchell, Tom, Machine learning: Trends, perspectives, and prospects, Science 17 Jul 2015, Vol. 349, Issue 6245, pp. 255-260, DOI: 10.1126/science.aaa8415

4. Hou, Shifu and Saas, Arsene and Ye, Yanfang and Chen, Ling, Deep4MalDroid: A Deep Learning Framework for Android Malware Detection Based on Linux Kernel System Call Graphs, 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 2019, Pages 359-366, ISBN 978-1-7281-0868-2, https://doi.org/10.1145/3350546.3352541.

5. Garcia-Teodoro, Pedro and Diaz-Verdejo, Jesus and Macia-Fernandez, Gabriel and Vazquez, Enrique, Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers & Security, Volume 28, Issues 1–2, 2009, Pages 18-28, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2008.08.003.

6. Carminati, Maria and Caron, Roberto and Maggi, Federico and Epifani, Igino and Zanero, Stefano, BankSealer: A decision support system for online

banking fraud analysis and investigation, Computers & Security, Volume 53, 2015, Pages 175-186, ISSN 0167-4048

7. Narayan, Abhishek and Gama, Joao and Robles-Kelly, Antonio and Gaber, Mohamed Medhat, Ensemble learning and artificial intelligence for fighting spam, Ensemble machine learning, Chapter 13, pp 339-361, ISBN 978-1-4419-9326-7

8. Fadlullah, Zubair Md and Tang, Feng and Mao, Bo and Kato, Nei, State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems, in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2432-2455, Fourthquarter 2017

9. ontes, Elvis and Silva, Plinio and Lima, Adriana and Bastos, Rafael and Jino, Mario, Technology Overview of Artificial Intelligence Applied in Cybersecurity, 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2019, Pages 12-17

10. Guidotti, Riccardo and Monreale, Anna and Ruggieri, Salvatore and Turini, Franco and Giannotti, Fosca and Pedreschi, Dino, A Survey Of Methods For Explaining Black Box Models, ACM Comput. Surv. 51, 5, Article 93 (August 2018), 42 pages, https://doi.org/10.1145/3236009.

11. Galetsi, Pinelopi and Katsikas, Steven, Security, privacy and trust in the IoT, Internet of Things Principles and Paradigms, Chapter 7, 2016, Pages 239-259, ISBN 9780128053959, https://doi.org/10.1016/B978-0-12-805395-9.00007-X.

12. Brandes, Lisa and Vargas, Alicia, Cybersecurity Education in a Rapidly Evolving Cyber Landscape, Journal of Cybersecurity Education, Research and Practice: Vol. 2020: No. 1, Article 5.

13. Biggio, Battista and Fumera, Giorgio and Roli, Fabio, Security evaluation of pattern classifiers under attack, in IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 4, pp. 984-996, April 2014, doi: 10.1109/TKDE.2013.57.

14. Jobin, Anna and Ienca, Marcello and Vayena, Effy, The global landscape of AI ethics guidelines, Nature Machine Intelligence 2019 1:9, 1 September 2019, https://doi.org/10.1038/s42256-019-0088-2.

15. Géron, Aurélien, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, 2nd Edition. O'Reilly Media, 2019. ISBN: 9781492032649.

16. Al Falasi, Aisha and Al Falasi, Falah and Al-Muhairi, Maytha, Artificial Intelligence Models for Cyber Security Incident Handling and Response: A Survey, 2022 4th International Conference on Smart Computing and Informatics (SCI), 2022, Pages 1-7, doi: 10.1109/SCI55520.2022.9679620.

17. Ponemon Institute. The Value of Artificial Intelligence Based Cybersecurity in the Enterprise. Published January 2019, Accessed from https://www.lumu.io/ponemon-report/

18. Apruzzese, Giovanni and Colajanni, Michele and Ferretti, Stefano and Mirto, Michele and Vargiu, Eloisa, On the Effectiveness of Machine and Deep Learning for Cyber Security, 2018 10th International Conference on Cyber Conflict (CyCon), 2018 Pages 371-390, doi: 10.23919/CYCON.2018.8405021.

19. Якубова, М. (2020). Применение альтернативных правовых методов разрешения инвестициаонных споров в Республике Узбекистан. Общество и инновации, 1(2/S), 261-268.

20. Abdurakhmanova, N. (2023, November). Examining the Developing Legal Landscape for Healthcare Smart Contracts. In International Conference on Legal Sciences (Vol. 1, No. 8, pp. 10-18).

21. Туракулова, Н. А. (2023). ПОРЯДОК И УСЛОВИЯ РЕГИСТРАЦИИ ГЕОГРАФИЧЕСКИХ ПОКАЗАТЕЛЕЙ В ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ УЗБЕКИСТАН И СТРАН ЕС: СРАВНИТЕЛЬНЫЙ АНАЛИЗ. DENMARK" THEORETICAL AND PRACTICAL FOUNDATIONS OF SCIENTIFIC PROGRESS IN MODERN SOCIETY", 14(1).

22. Yakubova, M. (2021). APPLICATION OF ALTERNATIVE METHODS OF INVESTMENT DISPUTE RESOLUTION IN THE REPUBLIC OF UZBEKISTAN: APPLICATION OF ALTERNATIVE METHODS OF INVESTMENT DISPUTE RESOLUTION IN THE REPUBLIC OF UZBEKISTAN. TSUL Legal Report International electronic scientific journal, 2(1), 94-100.