XODJAYEVA Mavlyuda Sabirovna
O'zbekiston xalqaro islom akademiyasi, Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi dotsenti, texnika fanlari nomzodi, m.xodjayeva@iiau.uz

AXBOROT XAVFSIZLIGIGA TAHDILARNI OLDINI OLISH MUAMMOLARI VA ULARNING ECHMLARI

ПРОБЛЕМЫ ПРЕДОТВРАЩЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ РЕШЕНИЯ

PROBLEMS OF PREVENTING THREATS TO INFORMATION SECURITY AND THEIR SOLUTIONS

Annotatsiya: *maqolada sun'iy intellekt tizimlar, ularni qo 'llash sohalari, sun'iy intellekt tizimlardan foydalangan holda antivirus dasturini yaratishda algoritmlar, ishlab chiqish, zamonaviy dasturlash tillari, ulardan maqbulini tanlash, zararli dasturlar holati va xususiyatlarini o'rganishda avvalo sun'iy intelekt algoritmlarini o'rganish, algoritm ishlab chiqish jarayonlari, ekspert tizimni ishlab chiqish algoritmini tuzib olish, SI tizimini yaratish uchun eng maqbul dasturlash tilini tanlash, antivirus dasturini yaratilish jarayoni keltirib o 'tilgan va tushuncha berilgan.*

Kalit so'zlar: *sun'iy intellekt tizimlar, dasturlash tillari, potentsial zararli dastur, blok sxema, ekspert tizimi ishlab chiqish algoritmi;*

Аннотация: в статье рассамтриваются системы искусственного интеллекта, области применения искусственного интеллекта, выбор наиболее оптимального языка программирования, обучение и процессы разработки алгоритма искуственного интеллекта, также экспертной системы, создание блок схемы и разработка антивирусной программы.

Ключевые слова: системы искусственного интеллекта, языки программирования , алгоритм, блок схема, потенциально вредоносное ПО, экспертные системы

Abstract: *artificial intelligence systems are being considered in the state, areas of application of artificial intelligence, selection of the most optimal programming language, training and methodological development of artificial intelligence algorithms, expert systems, creation of flowcharts and development of anti-virus programs.*

Keywords: *artificial intelligence systems, programming languages, algorithm, block diagram, potentially malicious software, expert systems*

KIRISH

Sun'iy intellect (SI) – bu kompyuter yoki kompyuter tomonidan boshqariladigan robotning odatda odamlar bajaradigan vazifalarni bajarish qobilyatidir, chunki ular inson aql zakovati va aql idrokni talab qiladi.

Mashinalar ayniqsa kompyuter tizimlari tomonidan inson aqli jarayonlarini simulyatsiya qilish suniy intellektning o'ziga xos ilovalariga eksport tizimlari tabiiy tilni qayta ishlash nutqni aniqlash, va mashinaviy ko'rish kiradi.

Nima uchun sun'iy intellect muhim? Sun'iy intellect bizning yashash, ishlash tarzimizni o'zgartirishimiz uchun muhim. U biznesda odamlar tomonidan bajariladigan vazifalarni, jumladan, mijozlarga xizmat ko'rsatish, firibgarlikni aniqlash va sifat nazoratini avtomatlashtirish uchun samarali foydalanilgan. Bir qator sohalarda sun'iy intellekt fazifalarni odamlarga qaraganda ancha yaxshi bajara oladi.

Tabiyki, yuqoridagi fikrlardan kelib chiqib, Sun'iy intellektni qo'llash sohalarini keltirib o 'tish mumkin: Sog'liqni saqlash tizimida, bunda bemorning natijalarini yaxshilash, xarajatlarni kamaytirish va sog'liqni saqlash samaradorligini oshirishda, bunda sun'iy intellekt ilovalariga tabiiy tasvirlash dori-darmonlarni toppish, va shaxsiylashtirilgan tibbiyotni o'z ichiga oladi.

Moliya sohasida sun'iy intellect risklarni boshqarishni yaxshilash savdoni avtomatlashtirish va moliya sohasida mijozlar tajribasini yaxshilashda, shuningdek, sun 'iy intellect ilovalariga firibgarlikni aniqlash, chatbotlar va algoritmik savdo kiradi. [1]

Biznesda suni'y intellektga asoslangan chatbotlar mijozlarga xizmat ko'rsatish vakillariga mijozlarning so'rovlari va tashvishlarini hal qilishda yordam berish uchun tobora ko'proq foydalanilmoqda.

Avtonom transport vositalarida yo'llar va transport vositalarida harakatlanish to'siqlarini

 ISSN 2181-9572

aniqlash, to’siqlarni aniqlash va real vaqtda qaror qabul qilishda yordam berish uchun ishlatiladi

Vertual yordamchilar siri kabi sun’iy intellektga asoslangan virtual yordamchilar rejalashtirish, eslatmalar va veb-qidiruvlar kabi vazifalarni bajarishda yordam berishi mumkin. Shuningdek ular aqilli uy qurilmalarini boshqarishi va musiqa orqali o’yin kulguni taqdim etishi mumkin.

MAVZUNING MAQSAD VA VAZIFALARTI

Elektron axborot hajmini ortishi, uni saqlash bilan bog‘liq bo‘lgan muammolar hajmini ham ortishiga olib keladi. Ushbu muammolarni hal qilishda mavjud bo‘lgan usullar esa, kundan-kunga yangilanaveradi. Bunday katta hajmdagi ma’lumotlar bilan ishlashda inson omili qaysidir ma’noda yetarli bo‘lmasligi mumkin. Barcha sohalarda bo‘lgani kabi, ertangi ilm-fan ravnaqi hisoblanayotgan sun’iy intelekt tizimlari axborot xavfsizligini ta’minlash sohasida ham o‘zining muqim o‘rnini egallab kelmoqda. Agar kelajak sun’iy intelekt tizimlarini internetning yuqori pallasi sifatida ko‘rsak, axborot xavfsizligi ushbu pallaning asosidir. Shu o ‘rinda ayrim statistik ma’lumotlarni keltirib o ‘tish mumkin Unga ko ‘ra, 2025-yilga borib SI sohasi kapitallashuvi $190 miliard darajasiga chiqishi kutilmoqda. 2021-yil holatiga ko‘ra esa ushbu yilning dastlabki uch choragi mobaynida sohani rivojlantirishga $60 milliard summada mablag‘ yo‘naltirilgan. Bugungi kunda 75% ilovalar dastur kodlarida SI algoritmlaridan foydalanmoqda. [2].

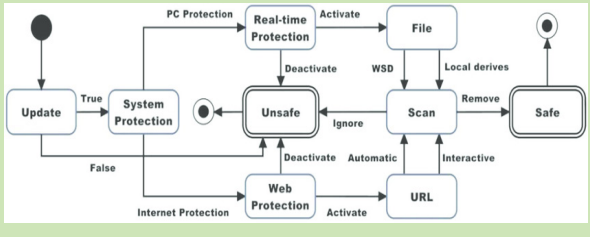
Sun’iy intellekt (SI) bugungi darajasi har bir potentsial zararli dastur yoki kibertahdid hodisasini avtomatik ravishda aniqlab olish imkoniyatiga ega emas, lekin u yomon va yaxshi xatti-harakatlarni modellashtirishni birlashtirganda, hatto eng ilg‘or zararli dasturlarga qarshi muvaffaqiyatli va kuchli qurol bo‘lishi mumkin.

SI tizimining ushbu muammoni hal qilish mantig‘i tizim ma’lumotlar bazasini to‘g‘ri deb hisoblangan harakatlar bilan to‘ldirishga asoslanadi. Agar dasturning qilayotgan harakati to‘g‘ri deb hisoblangan chegaradan chiqsa demak dastur zararli dasturdir, uni bloklash va o‘chirib yuborish kerak.

Sun’iy intelekt texnologiyalarini va zararli dasturlar holati va xususiyatlarini o ‘rganishda avvalo sun’iy intelekt algoritmlarini o’rganish, ekspert tizimni ishlab chiqish algoritmini tuzib olish, antivirus dasturini testlash, antivirus dasturini viruslar bilan tanishtirish, antivirus bazasini local holda kompyuterda tashkil qilish kabi jarayonlarni ko ‘rib chiqish talab etiladi.

MUHOKAMA VA NATIJALAR

Shuni ta ‘kidlaash kerakki, Sun’iy intelekt tizimlarini qo‘llab dastur yaratish bir qancha qiyinchiliklarni tug‘diradi. Sun’iy intelekt tizimini shakllantirishda avvalo ishni tashkillashtirish masalasiga e‘tiborni qaratish kerak bo‘ladi, ya‘ni, dastavval dasturning hamma uchun tushunarli bo‘lgan blok sxemasi tarzida algoritm tuzib olinadi. [12]



1-rasm. Dasturning blok sxemasi

1-qadam. Yechilishi talab qilinayotgan masalani aniqlashtirish: bu qadam eng birinchi hamda eng muhim qadam hisoblanadi. Bu qadamning mohiyati quyidagicha agar qayerga qarab ketayotganingni bilmasang yugurishdan foyda yo‘q.

2-qadam. Ma’lumotlarni tayyorlash: ma’lumotlarning asosan ikki xil turi mavjud, ya’ni strukturaviy va strukturasiz ma’lumotlar.

Strukturaviy ma’lumotlar: barqaror bo‘lishini ta’minlash uchun qat’iy formatga ega bo‘lgan ma’lumotlar.

Strukturasiz ma’lumotlar: qat’iy formatga ega bo‘lmagan ma’lumotlarning har qanday shakli strukturasiz ma’lumotlar sifatida tasniflanadi. Har qanday video, audio va tasvir fayllari bunga misol bo‘lishi mumkin.

3-qadam. Algoritm tanlash. Bu qadam SI tizimini yaratishning asosiy qismi yoki eng muhim qismi xisoblanadi. Bu jarayonda qo‘llanilish sohasiga qarab, algoritm o‘z shaklini o‘zgartirishi mumkin.

4-qadam. SI tizimini yaratish uchun eng maqbul dasturlash tilini tanlash: Dasturlash tilini tanlashda turli xil variantlar mavjud. C++, java va python kabi zamonaviy tillar mavjud. Bu o ‘rinda

Python dasturlash tili SI tizimlarini yaratish, hamda kod yozish uchun eng yaxshi tanlov hisoblanadi.

5-qadam. Platformani tanlash: Quyidagi platformalar SI tizimni yaratish jarayonini yengillashtirish va modellarni yaratishda yordam berish uchun qurilgan. Microsoft Azure Machine Learning, Google Cloud Prediction API, TensorFlow va boshqalar. Mazkur mashhur platformalar foydalanuvchiga ma'lumotlarni oldindan qayta ishlash, modelni o'qitish va baholash kabi masalalarda yordam beradi.

Albatta antivirus dasturini yaratish juda murakkab jarayon, hamda bu juda katta jamoaviy kuch va ulkan resurslarni talab qiladi. Antivirus dasturini yaratilish jarayonini bir necha bosqichlarga bo'linadi. Albatta bu bosqichlar to'g'ri va aniq belgilangan ketma-ketlikda bo 'lishi kerak.

1-qadam. Dastur tuzish uchun kerakli platforma va dasturlash tili tanlab olish jarayoni. Buning uchun Windows operatsion tizimi uchun Python dasturlash tilining Grafik User Interface (GUI) yaratishga mo'ljallangan PyQt5 kutubxonasidan foydalanish kerak bo 'ladi.

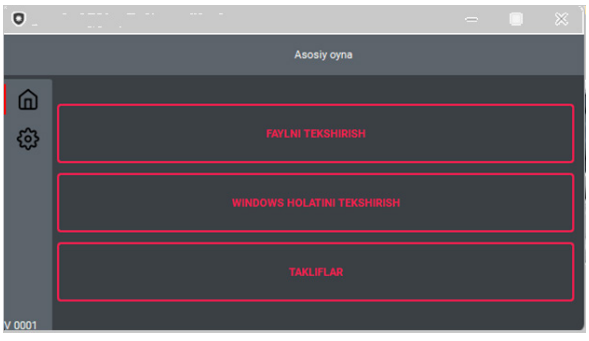
2-qadam. Dastur ishlashi uchun bir necha kutubxonalar zarur, shuning uchun ularni, kutubxonalarni import qilib olinadi.

3-qadam. GUI tuzilgandan so'ng, dasturning asosiy vazifalarini amalga oshiradigan kutubxonalari tanlangandan so'ng, boshqa kerakli kutubxonalarini import qilib olindi.

4-qadam. Fayllarni virusga tekshirish algoritmi. Bunda bir muncha samarali hisoblangan "hashing" usulini qo'llash tanlandi. Ushbu usul fayllarning unikal identifikatsiyasi sifatida ishlatiladi. Faylni hash funktsiyasi orqali ishlatib, faylning o'zining identifikatorini olish mumkin. Agar bir faylning identifikatori o'zgartirilsa, fayl o'zgartirilgan holatda bo 'ladi.

5-qadam. Tekshirilgan fayllarni hash qiymatini bazaga yozib borish jarayoni. Bu jarayon eng muhim jarayon hisoblanadi. Chunki bu qadamda yaratayotgan antivirus tizimini zararli dasturlar haqida o'qitishni amalga oshiriladi.

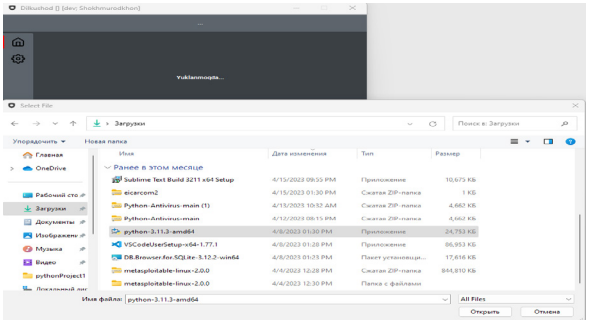
6-qadam. Natijaga erishish qadami. Antivirus dasturi o'zi o'qitilgan, tanishtirilgan zararli faylni ko'rishi bilan uni virus deb ko'rsatadi hamda unga qarshi chora ko'rish kerakligi haqida ogohlantirish beradi.



1-rasm. Dastur ko 'rinishi

Uning pastidagi dastur oynasining header qismida Asosiy oyna tugmasi mavjud. Dasturning chap ustunida home(icon) rasmi hamda settings(icon) rasmi va ustunning eng ostida dasturning versiyasi joylashgan(v0001).

Dasturning asosiy oynasida joylashgan 3 ta tugmachaning birinchisi orqali faylni tekshirish mumkin.



2-rasm. Tekshirish uchun faylni tanlash oynasi

Faylni tanlab fayl ustiga sichqonchani ikki marta bosish yoki tanlab ochish tugmasi bosiladi va fayl yuklab olinadi. Oddiy holatda dastur local holda, ya'ni bilimlar bazasi orqali tekshiriladi.

XULOSA

Virus dasturlarni aniqlash uchun SI tizimlaridan foydalanadigan antivirus dasturlarni o'qitish va sinov tizimlari uchun juda muhimdir. Shu nuqtayi nazardan olib qaraganda antivirus tizimlarining ishonchliligi uning bilimlar bazasining kengligiga bog'liqdir.

Antivirus dasturi barcha kompyuter texnologiyalari uchun juda muhim dasturiy mahsulot hisoblanadi. Ammo, bugungi kunda barcha davlat idoralari yoki istalgan kompyuter foydalanuvchilari foydalanayotgan antivirus

ISSN 2181-9572

dasturiga e’tibor bilan qaralsa, barchasi chet davlat kompaniyalari tomonidan yaratilganligi, bazalari begonalar qolida saqlanayotgani hamda istalgan vaqtda antivirus yaratuvchisi tomonidan noto‘g‘ri maqsadda foydalana olishiga imkoniyat mavjudligini hisobga olish zarur. Shu nuqtai nazardan milliy antivirus tizimini yaratish masalasi muhim hisoblanadi va buni yaqin kelajakda amalga oshirish, uni muvofiqlashtirish, takomillashtirish kabi jarayonlarni amalga oshirish kerak.

Sun’iy intellect sohasi juda kata imkoniyatlar taqdim etadi, texnologik yutuqlar va innovatsiyalar. Biroq zarur bo’lgan qiyinchiliklarni ham keltirib chiqaradi. Sun’iy intellektdagi bazi asosiy qiyinchiliklarga quyidagilar kiradi. Sun’iy intellektni joylashtirishning axloqiy oqibatlari, ish joyini almashtirish bo’yicha tashvishlar, taminlash algoritmik adolat va shaffoflik, va sun’iy intellect bilan bog’liq potentsial xavflarni boshqarish tizimlari.

Sun’iy intellect samaradorlikni oshirish, qaror qabul qilish jarayonlarini takomillashtirish hamda o’sish va innovatsiyalar uchun yangi imkoniyatlar yaratish orqali turli sohalarda inqilob qilish potentsialiga ega bo’lgan kuchli texnologiya. Biroq bu shuningdek, ehtiyotkorlik bilan tartibga solish va mas’uliyatli amalga oshirish orqali hal qilinishi kerak bo’lgan ish joyini almashtirish va shaxsiy hayot bilan bog’liq muammolar kabi axloqiy muammolarni keltirib chiqarishi ham mumkin.

FOYDALANILGAN ADABIYOTLAR RO’YHATI

1. D. Cole, “Artificial intelligence and personal identity”, Synthese, vol. 88, no. 3, pp. 399-417, 1991. Available: 10.1007/bf00413555. [1]

2. M. Stefik, “Artificial intelligence applications for business management”, Artificial Intelligence, vol. 28, no. 3, pp. 345-348, 1986. Available: 10.1016/0004-3702(86)90055-x. [2]

3. G. Babu, N. Anandakuma and D. Muralidhar, “Countermeasures Against DPA Attacks on FPGA Implementation of AES”, Journal of Artificial Intelligence, vol. 5, no. 4, pp. 186-192, 2020. [3]

4. G. Qin, T. He and J. Chen, “Model of preventing URL attacks based on artificial immunity”, Journal of Computer Applications, vol. 32, no. 5, pp. 1400- 1403, 2019.

5. N. Lee, “Artificial Intelligence and Data Mining,” Counterterrorism and Cybersecurity, pp. 323–341, 2021.

6. L. Shellberg, “A Cyber Chase in Cyber Space: How International Law Must Address the Threat of Cyber Attacks or Suffer the Consequences”, SSRN Electronic Journal, 2022.

7. H. R. Nemati, Information security and ethics: concepts, methodologies, tools, and applications. Hershey Pa.: Information Science Reference, 2019.

8. T. Tagarev, “Intelligence, Crime and Cybersecurity”, Information & Security: An International Journal, vol. 31, pp. 05-06, 2021.

9. R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007. 10. D. Hutchison, M. Atiquzzaman, H.-H. Chen, T. Kanade, T.-hoon Kim, J. Kittler, J. M. Kleinberg, C. Lee, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. P. Rangan, J. H. Park, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and S.-S. Yeo, Advances in Information Security and Assurance. Berlin, Heidelberg: Springer Berlin Heidelberg.

11. M. Zajko, “Canada’s cyber security and the changing threat landscape”, Critical Studies on Security, vol. 3, no. 2, pp. 147-161, 2019.

12. R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007. 13. H. Bidgoli, Handbook of information security. Hoboken, NJ: John Wiley, 2006.

14. H. Zhuge, “Semantic linking through spaces for cyber-physical-socio intelligence: A methodology”, Artificial Intelligence, vol. 175, no. 5-6, pp. 988- 1019, 2021.

15. C. Blackwell and H. Zhu, Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2nd ed. Cham : Springer International Publishing, 2022.

16. A. R. Dengel, K. Berns, T. M. Breuel, F. Bomarius, and T. R. Roth-Berghofer, KI 2021: advances in artificial intelligence 41st Annual German Conference on AI, KI 2021, Kaiserslautern, Germany, September 23-26, 2021 ; proceedings. Berlin: Springer, 2021.

17. С. Е. Кузнецов “**Подходы к оценке защищенности программного обеспечения от негативных информационных воздействий” 2014 г.**

18. R.G. Smith va J. Eckroth, «AI ilovalarini qurish: kecha bugun va ertaga», *AI Mag.* , jild. 38, yo‘q. 1, 6-22-betlar, 2020 yil.

19. Kevin P. «Machine Learning: A Probabilistic Perspective» - Murphy. 254 pg, 2023.