AXBOROT XAVFSIZLIGINI TA’MINLASHDA SUN’IY NEYRON TARMOQLARNING ROLI

Ro‘ziyeva Laylo Rajabovna
Navoiy Olimpiya va paralimpiya sport turlariga tayyorlash markazi o‘qituvchisi
laylorozivеva6@gmail.com

Annotatsiya Ushbu maqolada sun’iy neyron tarmoqlarning axborot xavfsizligini ta’minlashdagi roli tahlil qilinadi. Sun’iy intellekt va neyron tarmoqlarning kiberhujumlarni aniqlash, firibgarlikka qarshi kurashish, zararli dasturlarni aniqlash va shaxsiy ma’lumotlarni himoya qilishdagi afzalliklari va cheklovlari o‘rganiladi. Shuningdek, ushbu texnologiyalarning kelajakdagi istiqbollari va rivojlanish yo‘nalishlari ham yoritiladi.

Kalit so‘zlar: Axborot xavfsizligi, sun’iy neyron tarmoqlar, kiberxavfsizlik, firibgarlikni oldini olish, zararli dasturlar, biometrik autentifikatsiya.

Kirish

Raqamli texnologiyalar rivojlanishi bilan axborot xavfsizligini ta’minlash dolzarb masalalardan biriga aylandi. Sun’iy intellekt, xususan, sun’iy neyron tarmoqlar (SNT), kiberxavfsizlik sohasida muhim rol o‘ynaydi. Ushbu tadqiqotda sun’iy neyron tarmoqlarning axborot xavfsizligini ta’minlashdagi o‘rni va imkoniyatlari ko‘rib chiqiladi. Sun’iy neyron tarmoqlar inson miyasi faoliyatidan ilhomlanib yaratilgan hisoblash tizimlaridir. Ular o‘z-o‘zini o‘rgatish, ma’lumotlarni qayta ishlash va mustaqil qaror qabul qilish qobiliyatiga ega. SNT axborot xavfsizligida tahdidlarni aniqlash, hujumlarni bashorat qilish va oldini olish uchun keng qo‘llaniladi. Neyron tarmoq xavfsizligi raqamli tizimlarni murakkab kiber tahdidlardan himoya qilishda muhim ahamiyatga ega. An'anaviy xavfsizlik choralari rivojlanayotgan hujumlarga qarshi

yetarli emasligi sababli, neyron tarmoqlar moslashuvchan va aqlli himoya mexanizmlarini taklif qiladi.

Axborot xavfsizligida sun’iy neyron tarmoqlarning qo‘llanilishi.

- Kiberhujumlarni aniqlash: SNT tarmoq trafikini tahlil qilib, odatiy bo‘lmagan xatti-harakatlarni aniqlaydi.
- Firibgarlikni oldini olish: Moliyaviy tranzaksiyalarni monitoring qilish orqali firibgarlikni bashorat qilishga yordam beradi.
- Zararkunanda dasturlarni aniqlash: SNT zararli dasturlarni aniqlash va klassifikatsiya qilishda samarali ishlaydi.
- Shaxsiy ma’lumotlarni himoya qilish: Biometrik autentifikatsiya tizimlarida ishlatiladi.

Sun’iy neyron tarmoqlarning afzalliklari ma’lumotlarni chuqur tahlil qilish va yuqori aniqlikdagi natijalar taqdim etish hamda hujumlarni real vaqtda aniqlash va ularga qarshi tezkor javob berish. Bundan tashqari o‘z-o‘zini o‘rgatish va yangi tahdidlarga moslashish qobiliyatini o’z ichiga oladi. Kamchiligi esa katta hajmdagi ma’lumotlarni qayta ishlash uchun yuqori hisoblash resurslarini talab qiladi va noaniq yoki buzilgan ma’lumotlarga nisbatan sezgir hisoblanadi. Shu bilan birga neyron tarmoqlarning ishlash jarayoni tushuntirish qiyin bo‘lgan «qora quti» modelga asoslangan. Kelajak istiqbollarida sun’iy neyron tarmoqlarning rivojlanishi bilan kiberxavfsizlik tizimlari yanada samarali bo‘lishi kutilmoqda. Xususan, avtomatlashtirilgan hujumga qarshi tizimlar, o‘zini-o‘zi himoya qila oladigan tarmoqlar va ilg‘or firibgarlikni oldindan aniqlash texnologiyalari ishlab chiqilishi rejalashtirilmoqda.

Xulosa

Sun’iy neyron tarmoqlar axborot xavfsizligini ta’minlashda kuchli vosita hisoblanadi. Ularning imkoniyatlaridan samarali foydalanish kiberhujumlarga qarshi kurashish va ma’lumotlarni himoya qilishda muhim ahamiyatga ega. Biroq, ushbu

texnologiyaning cheklovlarini inobatga olib, uni rivojlantirish va takomillashtirish ustida doimiy tadqiqotlar olib borish zarur.

Foydalanilgan adabiyotlar

1. National Research Council, Division of Behavioral, Social Sciences, Board on Behavioral, Sensory Sciences, Committee on Developments in the Science of Learning with additional material from the Committee on Learning Research, & Educational Practice. (2000). How people learn: Brain, mind, experience, and school: Expanded edition (Vol. 1). National Academies Press.

2. Prieto, A., Prieto, B., Ortigosa, E. M., Ros, E., Pelayo, F., Ortega, J., & Rojas, I. (2016). Neural networks: An overview of early research, current frameworks and new challenges. Neurocomputing, 214, 242-268.

3. Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. Sensors, 21(5), 1809.

4. Setia, H., Chhabra, A., Singh, S. K., Kumar, S., Sharma, S., Arya, V., … & Wu, J. (2024). Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. Cyber Security and Applications, 2, 100037.

5. Peñalvo, F. J. G., Maan, T., Singh, S. K., Kumar, S., Arya, V., Chui, K. T., & Singh, G. P. (2022). Sustainable stock market prediction framework using machine learning models. International Journal of Software Science and Computational Intelligence (IJSSCI), 14(1), 1-15.