SUN’IY INTELLEKT VA AXBOROT XAVFSIZLIGI

Mavlonova Zulayho Allamurod qizi
Axborot texnologiyalari va menejment universiteti talabasi

Annotatsiya: *Ushbu maqolada sun’iy intellekt (SI) va axborot xavfsizligi o‘rtasidagi o‘zaro bog‘liqlik tahlil qilinadi. Sun’iy intellekt texnologiyalarining rivojlanishi axborot xavfsizligi sohasida yangi imkoniyatlar va tahdidlarga olib kelmoqda. Maqolada SI yordamida axborot xavfsizligini ta'minlash, shuningdek, SI tizimlarining o‘zlari qanday xavf-xatarlar bilan yuzma-yuz kelishi ko‘rib chiqiladi. Ushbu tahlil natijasida sun’iy intellektning axborot xavfsizligini oshirishdagi roli va muhimligi haqida xulosa chiqariladi.*

Kalit so‘zlar: *Sun’iy intellekt, axborot xavfsizligi, kiberxavfsizlik, tahdidlar, himoya mexanizmlari, mashinani o‘rganish.*

Kirish

Sun’iy intellekt (SI) so‘nggi yillarda tez sur'atlar bilan rivojlanmoqda va bu texnologiya ko‘plab sohalarda, jumladan, axborot xavfsizligida ham keng qo‘llanilmoqda. Axborot xavfsizligi – bu ma'lumotlarni himoya qilish va ularni nojo‘ya kirishlardan saqlash jarayonidir. Sun’iy intellekt ushbu jarayonda yangi imkoniyatlar yaratadi, lekin shu bilan birga yangi tahdidlarga ham olib kelishi mumkin. Ushbu maqolada sun’iy intellekt va axborot xavfsizligi o‘rtasidagi munosabatlar, SI yordamida axborot xavfsizligini ta'minlash usullari va SI tizimlariga nisbatan yuzaga keladigan xavf-xatarlar ko‘rib chiqiladi.

Asosiy qism

Sun’iy intellekt (SI; inglizcha: artificial intelligence, AI) – inson intellektiga taqlid qilishga qodir bo‘lgan mashinalar yaratishga qaratilgan fan va texnologiya sohasi.

Sun'iy intellek atamasi 1956-yilda Jon Makkarti tomonidan fanga kirgizilgan bo'lib (Makkarti va b. 2006), bunda aqlli raqamli texnologiyalar nazarda tutilgan edi. Hozirga kelib sun'iy intellect keng sohaga aylanib, undan komputer texnologiyalari, falsafa, tilshunoslik, psixologiya va boshqa fanlarda ham foydalanilmoqda. Sun'iy intellect dasturlari oldiga qo'yilayotgan yangi talablar asosida bu sohaga turlicha ta'rif berish mumkin. Sun;iy intellektga qo;yilgan hozirgi talablar bu insondek fikrlash qobiliyatiga ega bo'lsih (kuchli Al dasturlari), isnon tafakkuri jarayoni inobatga olinmagan ammo vazifalarni bajaruvchi dasturlar (kuchsiz Al dasturlar) va inson tafkkaruni inobatga oladigan ammo uni o'zi uchun maqsad qilib olmagan turlarga ajratish mumkin.

Sun’iy intellekt – bu kompyuter tizimlarining inson fikrlash qobiliyatlarini takrorlashga qaratilgan texnologiya bo‘lib, u ma'lumotlarni tahlil qilish, mashinani o‘rganish va qaror qabul qilish jarayonlarini o‘z ichiga oladi. SI yordamida quyidagi imkoniyatlar mavjud:

• Ma'lumotlarni tahlil qilish: Sun’iy intellekt katta hajmdagi ma'lumotlarni tezda tahlil qilib, muhim xulosalar chiqarishi mumkin. Bu axborot xavfsizligida potentsial tahdidlarni aniqlashda foydali bo‘ladi.

• Avtomatlashtirilgan monitoring: SI tizimlari real vaqt rejimida axborot tizimlarini kuzatib borishi va potentsial xavflarni aniqlashi mumkin.

• Tahdidlarni prognoz qilish: Mashinani o‘rganish algoritmlari yordamida avvalgi tajribalar asosida kelajakdagi tahdidlarni oldindan aniqlash imkonini beradi.

Sun’iy intellektdan kiberxavfsizlik sohasida qo‘llanadigan amaliy vazifalar doirasi doimiy ravishda kengayib bormoqda va vaqti kelib undan foydalanmaydigan loyiha va jamoalar qolmaydi. Kiberxavfsizlik sohasi jiddiy kadrlar tanqisligini boshdan kechirayotganini hisobga olsak, hozirdanoq har birimiz aynan sun’iy intellektdan foydalanishni o‘rganishni boshlashimiz va yuzaga keladigan muammolarni hal qilishda ishtirok etishimiz mumkin.

Sun’iy intellektdan kiberxavfsizlik sohasida qo‘llanadigan amaliy vazifalar doirasi doimiy ravishda kengayib bormoqda va vaqti kelib undan foydalanmaydigan loyiha va jamoalar qolmaydi. Kiberxavfsizlik sohasi jiddiy kadrlar tanqisligini boshdan kechirayotganini hisobga olsak, hozirdanoq har birimiz aynan sun’iy intellektdan foydalanishni o‘rganishni boshlashimiz va yuzaga keladigan muammolarni hal qilishda ishtirok etishimiz mumkin.

Sun’iy intellekt tizimlari iterativ va dinamikdir. Ular ko’proq ma’lumotlarni tahlil qilish davomida aqlli bo’lib, tajribadan “o’rganadilar” va borgan sari qobiliyatli va avtonom bo’lib boradilar. Boshqa tomondan, ma’lumotlarni tahlil qilish (DA) – bu ixtisoslashgan tizimlar va dasturiy ta’minot yordamida ulardagi ma’lumotlar to’g’risida xulosa chiqarish uchun katta ma’lumotlar to’plamlarini o’rganadigan statik jarayon hisoblanadi.

Sun’iy intellekt ko‘pgina xakerlar uchun bot-tarmoqlarini tashkil etish va qo‘llab-quvvatlash hamda zararli dasturiy ta’minot kodini yashirishda “ko‘makchi”ga aylandi. Ammo u ijtimoiy muhandislik elementlariga ega kiberhujumlarni tayyorlash jihatidan ko‘proq xavf tug‘diradi. Bu bugungi kunda sun’iy intellekt o‘qishi va tahlil qilishi uchun mavjud bo‘lgan ma’lumotlarning aksariyati aynan inson faoliyati va turli xil xizmatlarning iste’molchisi sifatida, shu jumladan, uning afzal ko‘rgan va zaif tomonlariga tegishli bo‘lgani bilan bog‘liq hisoblanadi.

Sun'iy intellektga asoslangan kiberxavfsizlik tizimlari real vaqt rejimida katta hajmdagi ma'lumotlarni tahlil qilish qobiliyatiga ega,bu esa tahdidlarni tezroq va aniqroq aniqlash va ularga javob berish imkonini beradi.Kelajakda murakkab va rivojlanayotgan kiber tahdidlarni aniqlash uchun AIalgoritmlarini yanada takomillashtirish imkoniyatlari mavjud, bu esa kiberxavfsizlikning yanada faol va samarali yondashuviga olib keladi.

Sun’iy intellektning rivojlanishi bilan birga axborot xavfsizligiga tahdidlar ham ko‘paymoqda.

Axborot xavfsizligi (inglizcha: Information Security, shuningdek, inglizcha: InfoSec) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma’lumotlar qanday shaklda bo‘lishidan qat’iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Masalan:

- Kiberhujumlar. SI yordamida amalga oshiriladigan kiberhujumlar yanada murakkablashmoqda. Masalan, avtomatlashtirilgan botlar yordamida hujumlari o'tkazilishi mumkin.
- Ma'lumotlarning manipulyatsiyasi. Sun’iy intellekt yordamida ma'lumotlarni manipulyatsiya qilish va soxta ma'lumotlarni tarqatish imkoniyatlari oshmoqda.
- Xavfli algoritmlar. Ba'zi hollarda, sun’iy intellekt tizimlari o‘zlari zararli faoliyatni amalga oshirish uchun dasturlanishi mumkin.

Sun’iy intellekt axborot xavfsizligini ta'minlashda quyidagi usullar orqali samarali qo‘llanilishi mumkin:

- Anomaliyalarni aniqlash. SI yordamida odatiy faoliyatdan chetga chiqadigan anomaliyalarni aniqlash va ularga tezkor javob berish mumkin.
- Xavf-xatarlarni baholash. Sun’iy intellekt algoritmlari yordamida kiberxavfsizlik holatini baholash va potentsial tahdidlarni aniqlash jarayonlarini avtomatlashtirish mumkin.
- O‘rganish va moslashuvchanlik. Mashinani o‘rganish yordamida tizimlar yangi tahdidlarga moslashishi va o‘zlarini himoya qilish strategiyalarini yangilashi mumkin.

1- rasm. Sun’iy intellekt mutaxassisligi

Xulosa

Xulosa sifatida aytish mumkinki, sun’iy intellekt va axborot xavfsizligi o‘rtasidagi munosabatlar murakkab va ko‘p qirrali. Sun’iy intellekt axborot xavfsizligini ta'minlashda yangi imkoniyatlar yaratadi, lekin shu bilan birga yangi tahdidlarga ham olib keladi. Kiber hujumlar, ma'lumotlarning manipulyatsiyasi va xavfli algoritmlar kabi tahdidlar sun’iy intellektning salbiy tomonlaridan biridir. Biroq, sun’iy intellektning imkoniyatlari – anomaliyalarni aniqlash, xavf-xatarlarni baholash va moslashuvchanlik kabi jihatlar axborot xavfsizligini kuchaytirishga xizmat qiladi. Shu sababli, sun’iy intellektni axborot xavfsizligini ta'minlashda samarali qo‘llash uchun ehtiyotkorlik bilan yondashish zarur.

So’nggi yillarda sun’iy intellekt axborot xavfsizligi bo’yicha mutaxassislarning sa’yi- harakatlarini kuchaytirish uchun zarur texnologiyaga aylandi. Xavfsizlik nuqtai nazaridan, sun’iy intellekt xavflarni aniqlashi va birinchi o’ringa qo’yishi, tarmoqdagi har qanday zararli dasturni darhol aniqlashi, hodisalarga javob berishi va bosqinlarni boshlanishidan oldin aniqlashi mumkin.

Foydalanilgan adabiyotlar

1. NIST Interagency or Internal Report 7298 Glossary of Key Information Security Terms (en). Gaithersburg, MD, USA: Revision 2, 2013.

2. NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems (en). Gaithersburg, MD, USA: National Institute of Standards and Technology, 1996.

3. Russell, S., Norvig, P. (2020). "Artificial Intelligence: A Modern Approach." Pearson.

4. Anderson, R. (2019). "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley.

5. O ’zR Prezidentining«Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shar tsharoitlar yaratish chora- tadbirlari to ’g ’risida»gi qarori.PQ-4996-son.17.02.2021y.

6. А.Фишман . Искусственный интеллект: возможности и угрозы . ИТБезопасность (it-world.ru) . Журнал IT Manager. 01.06.2021

7. David Poole Alan Mackworth Artificial Intelligence: Foundations ofComputational Agents, Cambridge University Press, 2010

8. Руслан Рахметов Искусственный интеллект в информационной безопасности/www.securityvision.ru/blog/iskusstvennyy-intellekt- v informatsionnoy-bezopasnosti

9. “Kiber xavfsizlik muammolari va ularning eng yangi texnologiyalarda yuzaga kelish trendlarini o’rganish”, Dilmurod Rahkmatov.

10. Using Artificial Intelligence in Cybersecurity | Balbixity.