ISSN 2181-3187

AXBOROT XAVFSIZLIGIDA SUN'IY INTELLEKT TIZIMLARINI QO'LLANILISHI

Raxmatullayev Doston Asad o'g'li
Muhammad al-Xorazmiy nomidagi TATU qarshi filiali
AT kafedrasi o'qtuvchisi
Bekmatov Akmal Kurbonmaxmatovich
Muhammad al-Xorazmiy nomidagi TATU qarshi filiali
AT kafedrasi o'qtuvchisi
Dilmurodov Zuhriddin Do`stmurod o'g'li
Muhammad al-Xorazmiy nomidagi TATU qarshi filiali
AT kafedrasi o`qtuvchisi

Kalit so'zlar: sun'iy intellekt, axborot xavfsizligi, raqamli iqtisodiyot, ovozli autentifikatsiya, biometrik ma'lumotlar, kiberjinoyat

Axborot xavfsizligi sohasida sun'iy intellektni qo'llashning asosiy yo'nalishlarini ko'rib chiqish va tahlil qilishga bag'ishlangan. Ta'kidlanishicha, intellektual tizimlarning keng joriy etilishi jamiyatni axborotlashtirish va virtuallashtirish, shuningdek, kibertahdidlar sonining ko'payishi, ularning murakkabligi va xilma-xilligining ortishi bilan bog'liq.

Sun'iy intellekt texnologiyalari jamiyat va davlat faoliyatining barcha sohalariga asta-sekin kirib bormoqda. Ushbu texnologiyalarning xilma-xilligi allaqachon bizga ular hal qiladigan deyarli cheksiz vazifalar haqida gapirishga imkon beradi. Mamlakatimizda ham jamiyat, hukumat va biznesni intellektuallashtirish amalga oshirilmoqda: 2019-yilda, xususan, "2030 yilgacha bo'lgan davrda sun'iy intellektni rivojlantirish milliy strategiyasi" tasdiqlangan bo'lib, uning matnida sun'iy intellekt o'rin olgan. "raqamli davlat" rivojlanishining yagona mumkin bo'lgan yo'li sifatida. Ilmiy doiralarda biz bir vaqtning o'zida bir emas, balki bir vaqtning o'zida bir nechta aqlli tizimlarni ma'lum bir sohaga joriy etish haqida ko'proq gapiramiz, bu sinergik ta'sirga erishishga imkon beradigan yagona gibrid muhitga ("yumshoq hisoblash" tushunchasi) birlashtirilgan. ishlatiladigan texnologiyalarning har biridan foydalanishdan.

Kiber tahdidlar soni doimiy o'sishni ko'rsatadi; ularning murakkabligi va xilma-xilligini oshirish. O. M. Maxalina va V. N. Maxalinning fikriga ko'ra, Rossiyada bitta kiber hodisa oqibatlarini bartaraf etish uchun o'rta biznesning xarajatlari taxminan 1,6 million rublni tashkil qiladi; yirik kompaniyalar ushbu maqsadlar uchun taxminan 16,1 million rubl sarflaydilar. Axborot xavfsizligiga tahdidlar deganda axborot sohasidagi milliy, korporativ va shaxsiy manfaatlarga zarar yetkazish xavfini yaratuvchi

ISSN 2181-3187

harakatlar va omillar majmui tushunilishi mumkin. Jahon hamjamiyatining axborotni muhofaza qilish borasidagi tashvishi ma’lumotlarni himoya qilish bo‘yicha bir qator davlatlararo me’yoriy hujjatlarning tasdiqlanishiga olib keldi; Biz, masalan, kompyuter tizimlarining shaxsiy va korporativ ma'lumotlar bilan ishlash tamoyillariga qat'iy muvofiqligini ta'minlashni nazarda tutuvchi "Ma'lumotlarni himoya qilishning umumiy qoidalari (GDPR)" (2018) ni ta'kidlaymiz.

Ikki parallel tendentsiyaning kombinatsiyasi sun'iy intellektga asoslangan tizimlar ma'lumotni himoya qilish uchun samarali vosita bo'la oladimi yoki yo'qmi degan ko'plab munozaralarni keltirib chiqardi. So'nggi o'n yil ichida axborot xavfsizligi sohasida sun'iy intellekt tizimlarining qo'llanilishi haqidagi bahslar davom etmoqda.

Axborot xavfsizligini ta’minlashda sun’iy intellektning dolzarbligini makroiqtisodiy ko‘rsatkichlar ham tasdiqlashi mumkin: 2019-yilga borib, axborot xavfsizligi sohasida qo‘llaniladigan sun’iy intellekt texnologiyalarining jahon bozori taxminan 8 milliard dollarga yetadi, prognozlarga ko‘ra, 2025-yilga kelib, bu 30 milliard dollar yoki undan ko'proqqa oshadi.

Shu bilan birga, sun'iy intellekt orqali ma'lumotlarni himoya qilishning zamonaviy usullarini mukammal deb bo'lmaydi. Aksincha, tegishli dasturiy ta'minotni ishlab chiquvchilar tobora ko'proq foydalanilayotgan tizimlarni sezilarli darajada yaxshilash zarurligi haqida gapirmoqdalar. Misol sifatida, ma'lumotlarni himoya qilishga qaratilgan sun'iy intellektni rivojlantirishning ba'zi muhim muammoli sohalarini ko'rib chiqing. Birinchidan, o'z-o'zini o'rganish tizimi foydalanuvchi xatti-harakatlaridagi og'ishlarni farqlashi kerak, lekin ayni paytda ularni aniqlaydi. Mijoz ongsiz, beixtiyor, tasodifan maxfiy ma'lumotlarga kirishni ta'minlashi mumkin.

Sun'iy intellekt axborotni himoya qilishning zarur darajasini ta'minlay olishi uchun uni to'g'ri joriy etish, mavjud tizimlarga integratsiyalash va o'qitish kerak. Bu paradoksal, ammo o'z-o'zidan ma'lumotlarni himoya qilish uchun mo'ljallangan intellektual tizimlarning joriy etilishi himoya tizimida ulkan "buzilish" ga olib kelishi va jismoniy yoki korporativ foydalanuvchining xavfsizlik darajasini sezilarli darajada kamaytirishi mumkin.

Shunga o'xshash muammo - bu sun'iy intellekt qo'llaniladigan vaziyatda yuzaga keladigan qochish hujumi. Uchinchi tomon, tizim va uning ishini boshqaradigan shaxs uchun sezilmaydigan tarzda, kiritilgan qiymatlarni o'zgartiradi, natijada tizimning o'zidan noto'g'ri xulosalar paydo bo'lishiga olib keladi. Ushbu turdagi tahdidlarga qarshi kurashishning yagona samarali usuli sifatida qarama-qarshilik mashg'ulotlari o'quv bosqichida tizimni noto'g'ri ma'lumotlarni tahliliy namunaga kiritmaslikka va ularni axborot aralashuvi sifatida tasniflashga o'rgatish imkonini beradigan raqib mashg'uloti deb ataladi.

Ko'pgina sun'iy intellekt tizimlari allaqachon o'zlarini murosaga keltirishga muvaffaq bo'lgan va shuning uchun ma'lumotlarni himoya qilish jarayonida "aqlli"

ISSN 2181-3187

tizimni qachon va qanday joriy etish har doim ham aniq emas. S.M.Avdoshin va E.Yu.Pesotskaya bu borada “ishonchli sun’iy intellekt” (Ishonchli sun’iy intellekt) atamasini juda asosli ishlatib, uni ishonch tamoyili asosida ishlab chiqilgan tizimlar majmui sifatida izohlaydilar; texnologiya egalari tomonidan sun'iy intellekt imkoniyatlarini suiiste'mol qilish xavfi istisno qilinadigan tizimlar; natijalariga ishonish mumkin bo'lgan tizimlar.

Sun'iy intellektga asoslangan vositalardan foydalanish, birinchidan, axborotni himoya qilish tizimida zaiflik holati yuzaga kelganda tezkor choralar ko'rish zarurati va ikkinchidan, malakali mutaxassislarning etishmasligi bilan bog'liq. Ideal vaziyatda kompaniyada kechayu-kunduz axborot xavfsizligi xizmati bo'lishi kerak - ish soatlaridan keyin himoya qilishni ta'minlash uchun. Bundan tashqari, hujumdan oldin kiberjinoyatchilar ko'pincha DDoS hujumini yoki tarmoqni skanerlashni faollashtirish orqali "chalg'itish" ni amalga oshiradilar, bu esa mutaxassislarni chalg'itishi va bunday dastlabki hujumlarga qarshi turish uchun ishchi resurslarni "tortib olishi" mumkin.

Axborot xavfsizligi sohasida intellektual intellektni amalga oshirishning alohida va juda muhim amaliy vektori bu firibgarlikka qarshi kurashdir. Spoofing (spoofing hujumi) raqamli dunyoda juda keng tarqalgan noqonuniy faoliyat bo'lib, tizimda soxtalashtirilgan autentifikatsiyani amalga oshirishga qaratilgan (qoida tariqasida, bu holda biz biometrik ma'lumotlar va ovozli kiritish orqali autentifikatsiya haqida gapiramiz). Buzg'unchi boshqa birovning hisobiga kirib, keyinchalik foydalanish uchun shaxsiy yoki korporativ ma'lumotlar segmentini oladi. Spoofingga qarshi chora-tadbirlarning aksariyati sun'iy intellekt tizimlariga asoslangan. Axborotni muhofaza qilish jamiyat oldida turgan ustuvor vazifalardan biriga aylandi. Axborot xavfsizligi masalasi har qachongidan ham dolzarbdir, chunki kiberjinoyatlar ko'lami doimiy ravishda o'sib bormoqda. Kibertahdidlarga qarshi kurashishning mumkin bo'lgan vositalaridan biri bu sun'iy intellekt texnologiyalaridir. Axborot xavfsizligi sohasidagi aksariyat zamonaviy echimlar qandaydir tarzda sun'iy intellektga asoslangan. Shu bilan birga, axborot xavfsizligi sohasida sun'iy intellektning joriy etilishi ko'plab xavf-xatarlar bilan bog'liq bo'lib, shu sababli ma'lumotlarni qayta ishlash sohasidagi mutaxassislar sun'iy intellekt tizimlari uchun shaxsiy ma'lumotlarni himoya qilish vositalarini ishlab chiqish bo'yicha sa'y-harakatlarini birlashtiradi yaqin kelajakda paydo bo'ladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Avdoshin, S. M. Ishonchli sun'iy intellekt raqamli himoya usuli sifatida / S. M. Avdoshin, E. Yu. Pesotskaya // Biznes informatika. - 2022. - №2. - S. 62-73.

2. Aliev, A. A. Aliev, M. Z. K. Musaeva, Biometrik ma'lumotlarni himoya qilish tizimlari // Ta'lim fanlaridagi akademik tadqiqotlar. - 2021. - №4. - S. 393-396.

ISSN 2181-3187

3. Marshall, E. Sun'iy intellekt xavfsizligi

4. Aseeva, I. A. Sun'iy intellekt va katta ma'lumotlar: amaliy foydalanishning axloqiy muammolari. (tahliliy sharh) / I. A. Aseeva // Ijtimoiy va gumanitar fanlar. Mahalliy va xorijiy adabiyotlar. Ser. 8, Fan fanlari: Abstrakt jurnal. - 2022. - №2. - S. 89-98.

5. Afanas'eva, D. V. Ma'lumotlar xavfsizligida sun'iy intellektdan foydalanish / D. V. Afanas'eva // Izvestiya TulGU. Texnik fan. - 2020. - №2. - S. 151-154.