SUN’IY INTELLEKT TIZIMLARINI KIBERXAVFSIZLIKNI TA’MINLASHDAGI AXAMIYATI

Akbarova Muattar Raxmatullaevna
Davlat statistika qo‘mitasi huzuridagi Kadrlar malakasini oshirish va statistik tadqiqotlar instituti, 2 kurs doktorant (PhD)
mm.akbarova@mail.ru

Annotatsiya
Ushbu tezis kiberxavfsizlikni ta’minlashda sun’iy intellekt tizimlarining axamiyatiga bag’ishlanadi. Tezisda kiberxavfsizlikni ta’minlashning asosiy prinsiplari, axborot xavfsizligi va kiberxavfsizlik sohasida sun'iy intellektdan foydalanishni avzallik tomonlari ko‘rib chiqilgan.

Kalitli so‘zlar
Kiberxavfsizlik, axborot xavfsizligi, raqamli iqtisodiyot, sun’iy intellekt, aqlli mashinalar, kibertahdid

Ilm-fan va axborot-kommunikatsiya texnologiyalari jadal taraqqiy etib borayotgan bugungi sharoitda dunyoning rivojlangan mamlakatlarida davlat va jamiyat boshqaruvi, iqtisodiyot, sanoat, ijtimoiy himoya, ta’lim, tibbiyot, bandlik, qishloq ho’jaligi, mudofaa, xavfsizlik, turizm va boshqa sohalarda zamonaviy axborot texnologiyalari va sun’iy intellekt imkoniyatlaridan keng foydalanish urfga kirmoqda.

O’zbekistonda ham axborotlashtirish va raqamli iqtisodiyotni rivojlantirish orqali 2030 yilga qadar innovatsion taraqqiy etgan yetakchi davlatlar qatoridan o’rin egallash ustuvor vazifa sifatida belgilangan.

Qayd etish joizki, “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da axborot texnologiyalari va raqamlashtirish borasida jiddiy o’zgarishlar amalga oshirilib, bir qator muhim dasturlar qabul qilindi.

Xususan, O’zbekiston Respublikasi Prezidentining “Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to’g’risida”gi, “Aholiga davlat ijtimoiy xizmatlari va yordam taqdim etish tartib-taomillarini avtomatlashtirish bo’yicha qo’shimcha chora-tadbirlar to’g’risida”gi hamda «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to’g’risida»gi qarorlari va boshqa normativ-huquqiy hujjatlar mamlakatimizda raqamlashtirishni jadallashtirish va ijtimoiy-iqtisodiy sohalarga zamonaviy texnologiyalarni joriy qilishga qaratilgan.

O‘zbekiston respublikasi prezidentining 2021 yil 17 fevralda qabul qilingan «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to’g’risida»gi qarori bilan 2021-2022 yillarda sun’iy intellekt texnologiyalarini o’rganish va joriy etish bo’yicha chora-tadbirlar dasturi bunga yaqqol misol bo‘la oladi. [2]

2022-yil 25-fevralda O‘zbekistonda kiberxavfsizlik sohasidagi munosabatlarni tartibga solish maqsadida “Kiberxavfsizlik to‘g‘risida”gi qonun qabul qilindi.

Qonunda kiberxavfsizlikni ta’minlashning asosiy prinsiplari sifatida quyidagilar keltirilgan:

– qonuniylik;
– kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;
– kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;
– kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;
– O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi.

Kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi. O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi xisoblanadi.

Kiberxavfsizlik hodisalari vakolatli davlat organi yoki kiberxavfsizlikni ta’minlash bo‘yicha ishchi organning mansabdor shaxslari tomonidan tekshiriladi.

Kiberxavfsizlik hodisasi sodir bo‘lgan axborot resursining yoki axborot tizimining egasi, agar u tekshiruv o‘tkazish uchun zarur bo‘lgan resurslarga va texnik imkoniyatlarga ega bo‘lsa, kiberxavfsizlik hodisasining tekshiruvini o‘tkazishi mumkin. Bunda vakolatli davlat organi tekshiruv natijalari to‘g‘risida xabardor qilinishi kerak.

Kiberxavfsizlik subyektlari tomonidan kiberxavfsizlik hodisalariga nisbatan choralar ko‘rish quyidagi shakllarda amalga oshirilishi mumkin:

– dasturiy ta’minotdagi va qurilmalardagi zaifliklarni hamda xatoliklarni bartaraf etish;

– zararli dasturlarni yo‘q qilish, ularning tarqalishini cheklash, kiberhujumlar manbaini texnik jihatdan cheklash;

– axborotlashtirish obyektlarini mavjud kibertahdidlardan ajratib qo‘yish;

– huquqni muhofaza qiluvchi organlarga kiberxavfsizlik hodisalari to‘g‘risida ma’lumotlar taqdim etish [1].

Sun’iy intellektni(SI) rivojlantirish hamda davlat organlari va boshqa tashkilotlar faoliyatida, shuningdek ushbu sohada normativ-huquqiy bazani tayyorlashda maslahatchi sifatida qatnashish uchun «Sber» guruhining (Rossiya) yetakchi mutaxassislari va ekspertlari jalb qilindi. Kiberjinoyatlar soni doimiy va tez ortib bormoqda. Shunday qilib, o‘tgan yil davomida Rossiya iqtisodiyotining xakerlar faoliyatidan ko‘rgan yo‘qotishlari taxminan 6 trillion rublni tashkil etdi. Mutaxassislarning fikricha, hujumchilar ko‘pincha axborot xavfsizligi bo‘yicha mutaxassislar va huquq-tartibot xodimlaridan bir emas, bir necha qadam oldinda bo‘ladi.

Sun'iy intellekt odamlar qila olmaydigan narsani qila olmaydi. Axir, sun'iy intellektning butun asosi inson xatti-harakatlariga taqlid qiladigan mashina yaratishdir. Ammo sun'iy intellekt ishlarni tezroq bajarishi va inson uchun juda ko‘p mehnat talab qiladigan katta hajmdagi ma'lumotlarni tahlil qilishi mumkin. SI zararli dasturlarning belgilarini aniqlash uchun murakkab naqshni aniqlash vositalaridan avtomatik ravishda foydalanishi mumkin. Sun'iy intellekt kuchli texnologiya bo‘lmasa-da va barcha tahdidlarni aniqlay olmasa ham, bu texnologiya mutaxassislarning ogohlantirishlarni o‘rganishga sarflash vaqtini qisqartiradigan muhim vositadir. Va bu, ehtimol, SIning eng muhim afzalligi.

So‘nggi 3-5 yil ichida kibermakondagi rivojlanish va o‘zgarishlar tezligi nafaqat tajribasiz foydalanuvchilarni, balki IT va axborot xavfsizligi sohasidagi tajribali mutaxassislarni ham hayratga solmoqda. Hatto qayta ishlangan ma'lumotlar miqdori, Internetga ulangan qurilmalar yoki ilovalar/xizmatlar sonida ham emas, balki tushunchalar va texnologiyalarning o‘zida ham, har tomonlama raqamlashtirish va ko‘pchilik korxonalarning onlayn rejimga o‘tishida ham eksponensial rivojlanish kuzatilmoqda. 2020 yildagi pandemiya bu tendentsiyani faqat tezlashtirdi. Yuqori va o‘ta yuqori darajali dasturlash tillaridan, kuchli freymworklar va ishlab chiqish muhitlaridan keng foydalanish, bulutli infratuzilmalar hamda virtualizatsiya va konteynerlashtirish texnologiyalarining rivojlanishi misli ko‘rilmagan qisqa vaqt ichida yangi ilovani “yig‘ish” imkonini beradi. Kibertahdidlar ham tezlikda ko‘paymoqda, chunki buzg’unchilar ham shunday yuqori samarali ishlab chiqish vositalaridan o‘z maqsadlari uchun foydalanadilar. Bu kiber qarshi choralar darajasini yangi bosqichga olib chiqadi: agar ilgari buzg'unchilar bilan to‘qnashuvni onglarning kurashi va ma'lumotni himoya qilishning moslashtirilgan vositalari deb ta'riflash mumkin bo‘lsa, endi uni sun'iy kiber intellektlar orasida bo‘ladigan "mashinalar jangi" deb atash mumkin.

Sun’iy intellekt haqidagi tasavvur va bu sohadagi izlanishlar — «aqlli mashinalar» ishlab chiqarishga ilmiy èndoshish birinchi bo’lib Stanford universitetining (AQSh) professori Djon Makkarti tashabbusi asosida 1956 yili tashkil topgan ilmiy tugarakda paydo bo’ldi. [4]

Axborot xavfsizligi va kiberxavfsizlik sohasida sun'iy intellektdan foydalanish 2000 yillarning boshlarida juda oddiy narsalardan, ya’ni ma'lum bir profil mutaxassislari, xususan, virus

tahlilchilarining ishini osonlashtiradigan tizimlarni qurish bilan boshlandi. Bu vaqtga kelib, zararli fayllar namunalari soni shunchalik ko‘payib ketdiki, qo‘lda yoki oddiy avtomatlashtirilgan tahlil endi etarli emas edi. Bular zararli koddagi naqshlarni (o‘xshashlikni) aniqlagan va hech bo‘lmaganda minimal atributga ruxsat beruvchi tizimlar edi. Ya'ni, ular teskari mutaxassislar va virus tahlilchilariga ma'lum ma'lumotlarni taqdim etdilar, bu esa u yoki bu zararli dasturlarni ma'lum bir guruh yoki sinfga tayinlash imkonini berdi. Aslida, bu klasterlash va katta ma'lumotlar bilan ishlash edi. [3]

Sun’iy intellektni(SI) rivojlantirish hamda davlat organlari va boshqa tashkilotlar faoliyatida, shuningdek ushbu sohada normativ-huquqiy bazani tayyorlashda maslahatchi sifatida qatnashish uchun «Sber» guruhining (Rossiya) yetakchi mutaxassislari va ekspertlari jalb qilindi. Kiberjinoyatlar soni doimiy va tez ortib bormoqda. Shunday qilib, o‘tgan yil davomida Rossiya iqtisodiyotining xakerlar faoliyatidan ko‘rgan yo‘qotishlari taxminan 6 trillion rublni tashkil etdi. Mutaxassislarning fikricha, hujumchilar ko‘pincha axborot xavfsizligi bo‘yicha mutaxassislar va huquq-tartibot xodimlaridan bir emas, bir necha qadam oldinda bo‘ladi.

Axborot xavfsizligi sohasida sun'iy intellektdan foydalanish 2000 yillarning boshlarida juda oddiy narsalardan, ya’ni ma'lum bir profil mutaxassislari, xususan, virus tahlilchilarining ishini osonlashtiradigan tizimlarni qurish bilan boshlandi. Bu vaqtga kelib, zararli fayllar namunalari soni shunchalik ko‘payib ketdiki, qo‘lda yoki oddiy avtomatlashtirilgan tahlil endi etarli emas edi. Bular zararli koddagi naqshlarni (o‘xshashlikni) aniqlagan va hech bo‘lmaganda minimal atributga ruxsat beruvchi tizimlar edi. Ya'ni, ular teskari mutaxassislar va virus tahlilchilariga ma'lum ma'lumotlarni taqdim etdilar, bu esa u yoki bu zararli dasturlarni ma'lum bir guruh yoki sinfga tayinlash imkonini berdi. Aslida, bu klasterlash va katta ma'lumotlar bilan ishlash edi. [3]

Axborot xavfsizligini ta’minlashda sun’iy intellektdan foydalanish, quyidagi ikki omilga asoslanadi: kiber voqea sodir bo‘lgan taqdirda tezkor choralar ko‘rish zarurati va kibermudofaa bo‘yicha malakali mutaxassislarning etishmasligi. Darhaqiqat, zamonaviy voqelikda xodimlar ro‘yxatini zarur tajribaga ega bo‘lgan malakali axborot xavfsizligi mutaxassislari bilan to‘ldirish juda qiyin va keng ko‘lamli axborot xavfsizligi hodisalari tez rivojlanishi mumkin: daqiqalar ko‘pincha hisoblanadi. Agar kompaniyada axborot xavfsizligi bo‘yicha tahlilchilarning kechayu kunduz navbatchilik smetasi bo‘lmasa, u holda kiber hodisalarga tezkor avtonom javob berish tizimisiz ish vaqtidan tashqarida yuqori sifatli himoyani ta'minlash qiyin bo‘ladi. Bundan tashqari, tahdidni amalga oshiruvchilar o‘z hujumlaridan oldin chalg'itishni amalga oshirishi mumkin - masalan, DDoS hujumini boshlash yoki tarmoqni faol skanerlash. Bunday vaziyatlarda sun'iy intellektga asoslangan kiber hodisalarga javob berish tizimi yordam beradi, bu bir vaqtning o‘zida ko‘p sonli axborot xavfsizligi hodisalarini qayta ishlash, axborot xavfsizligi bo‘yicha tahlilchilarning muntazam harakatlarini avtomatlashtirish va inson aralashuvisiz hodisalarga tezkor javob berish imkonini beradi. [5]

Bugungi kunga kelib SIning axborot xavfsizligini ta'minlash doirasi ancha keng. Internetda yangi tahdidlarni ko‘rsatishi yoki oldindan bashorat qilishi mumkin bo‘lgan katta hajmdagi ma'lumotlarni tahlil qiladigan global kompaniyalar mavjud. Ushbu kompaniyalarda ma'lumotlar to‘plamlarini to‘playdigan, SI-sinf texnologiyasidan foydalangan holda ularni tahlil qiladigan, klaster ma'lumotlarini aniqlaydigan va tahdidlarni bashorat qiladigan tizimlar mavjud. Ushbu texnologiyalarsiz bunday hajmdagi ma'lumotlarni qayta ishlash deyarli mumkin emas. Bu yerda, albatta, neyron tarmoqlar ham, klasterlash ham juda keng qo‘llaniladi. SI tizimlari tahdidlarni kuzatish uchun ham qo‘llaniladi, ya’ni ochiq va yopiq manbalardan to‘plangan ma'lumotlar asosida axborot xavfsizligi tahdidlarini bashorat qilish uchun foydalaniladi. Shunday qilib, so‘nggi yigirma yil ichida axborot xavfsizligi sohasida sun'iy intellektni qo‘llash vazifalari ko‘lami sezilarli darajada o‘sdi.

Bugungi kunga kelib sun'iy intellekt endi qandaydir sehr emas, balki kiber tahdidlardan himoya qilishda samarali yordamchidir.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni. 2022-yil 25-fevral
2. O’zR Prezidentining «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to’g’risida»gi qarori. PQ-4996-son. 17.02.2021y.
3. *А.Фишман. Искусственный интеллект: возможности и угрозы. ИТ Безопасность (it-world.ru). Журнал IT Manager. 01.06.2021*
4. **David Poole Alan Mackworth Artificial Intelligence: Foundations of Computational Agents, Cambridge University Press, 2010**
5. Руслан Рахметов Искусственный интеллект в информационной безопасности/ www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti/