

GENERATIV SUN'IY INTELLEKT SHAROITIDA TA'LIM TIZIMLARI VA KIBERXAVFSIZLIKNI TRANSFORMATSIYA QILISH, TAHDIDLAR, ISHONCHLILIK MUAMMOLARI VA XAVFSIZ AI ARXITEKTURALARI

Ismoiljonov Tengiz Turdiali o'g'li

Toshkent amaliy fanlar universiteti Iqtisodiyot yo'nalishi 1-bosqich talabasi.

tengizismoiljonov@gmail.com

Qurbonov Shovqi Djurayevich

*Toshkent amaliy fanlar universiteti "Tarmoqlar iqtisodiyoti va buxgalteriyasi" kafedrası (PhD) v.v.b.
dotsenti*

shovqiqurbonov@mail.com

Annotatsiya

Sun'iy intellektning kiberxavfsizlikda qo'llanilishi tashkilotlarning tahdidlarga javob berish usullarini tubdan o'zgartirdi. Sun'iy intellekt katta hajmdagi ma'lumotlarni tez va doimiy ravishda tekshiradi hamda muammolarni oldindan aniqlashga yordam beradi. Aqlli tizimlar xavfsizlikni avtomatik boshqaradi va odamlar bilan birga ishlaganda natija yanada yaxshi chiqadi. Sun'iy intellekt doimiy ravishda foydalanuvchilar nima qilayotganini, tizimda qayerda zaiflik borligini kuzatib boradi.

Sun'iy intellekt, ayniqsa machine learning orqali, avvalgi kiberhujumlarni o'rganib chiqadi va shunga qarab yangi hujumlarni tezroq aniqlashga yordam beradi. Shu sababli tizimlar yanada xavfsizroq bo'lib boradi. Lekin bu texnologiyaning faqat foydasi emas, muammolari ham bor. Masalan, odamlarning ma'lumotlari himoyasi buzilishi mumkin, AI noto'g'ri qaror chiqarsa kim javob berishi noaniq bo'ladi va eng xavflisi kiberjinoyatchilar ham undan foydalanishi mumkin. Shuning uchun AIni ishlatishda doimo inson nazorati bo'lishi va aniq axloqiy qoidalarga amal qilish kerak. Kelajakda esa AI yanada rivojlanib, hujumlarni o'zi mustaqil aniqlaydigan tizimlarga aylanishi, foydalanuvchilarning odatiy xatti-harakatlarini o'rganib, g'alati holatlarni topa olishi va o'z qarorlarini tushuntirib bera oladigan darajaga yetishi kutilmoqda. Masalan, LSTM va Transformer modeli kabi texnologiyalar bu jarayonda muhim rol o'ynaydi. Generativ AI ni Intelligent Transportation Systems ga qo'shish juda katta imkoniyatlar yaratadi, lekin shu bilan birga jiddiy muammolarni ham olib keladi, ayniqsa maxfiylik va kiberxavfsizlik masalalarida. Chunki transport tizimlari tobora ko'proq AIga bog'lanib borayotgan ekan, undagi nozik ma'lumotlarni himoya qilish va yangi turdagi kiberxavflarga qarshi kuchli choralar ko'rish juda muhim bo'lib qoladi. GenAI transport tizimlarini yanada aqlli va samarali qilishi mumkin, lekin undan noto'g'ri foydalanish yoki unga qarshi uyushtirilgan hujumlar ham katta xavf tug'diradi. Ayniqsa, AI asosidagi tizimlarga qarshi maxsus hujumlar ularning ishlashiga jiddiy zarar yetkazishi mumkin. Shu sababli transport infratuzilmasini himoya qilish, hujumlarni tezda aniqlash va foydalanuvchi ma'lumotlarini xavfsiz saqlash juda muhim hisoblanadi. Shuningdek, bu masalalarni hal qilish uchun zamonaviy shifrlash usullaridan foydalanish, tizimlarni real vaqt rejimida kuzatib borish va vaziyatga moslasha oladigan xavfsizlik tizimlarini joriy etish zarurligini unutmasligimiz kerak. Umuman olganda, doimiy ravishda o'zgarib turadigan kiberxavflar transport tizimlariga ta'sir qilishi mumkinligi sababli, ularga qarshi oldindan tayyor turadigan, ya'ni proaktiv xavfsizlik yechimlarini ishlab chiqish kerak degan xulosada bo'lishimiz lozim. Biroq ko'plab muammoli masalalarni sun'iy intellektga yuklab qo'yish ham qaysidir ma'noda noto'g'ri. Chunki, insonlarning o'zlari ham e'tiborli bo'lishi kerak va shaxsiy ma'lumotlarni 3-shaxslarga berishlari noto'g'ri. Salbiy oqibatlardan so'ng tegishli joylarga arz qilib, ulardan kutilgandek natija ola olmay, ularning ham ustidan shikoyat qilish eng katta xatodir, sababi ayrim

muammolarni bartaraf etish yo'llari hamon noaniqdir. Buning uchun televideniyada, radio eshittiruvlarda yoki majlislarda fuqarolarni takror-takror ogohlantirish lozim. Ko'p yangiliklardan aksariyat insonlar bexabar bo'lishiga shubha qilmaymiz, shuning uchun mahalla yettiligi ham o'zlariga qarashli bo'lgan fuqarolarni ogohlantirishga urinishlari lozim.

Kalit so'zlar: Generativ sun'iy intellekt, ta'lim tizimlari, kiberxavfsizlik, sun'iy intellekt xavfsizligi, ma'lumotlar maxfiyligi, model ishonchliligi, xavfsiz AI arxitekturasi, tahdid modellari, kiberfiribgarlik, raqamli transformatsiya.

Abstract

Artificial intelligence has fundamentally transformed how organizations respond to cybersecurity threats. It can rapidly and continuously analyze large volumes of data, helping to detect issues in advance. Intelligent systems automate security management, and when combined with human expertise, they produce even better results. Artificial intelligence continuously monitors user behavior and identifies vulnerabilities within the system.

Artificial intelligence, especially through machine learning, analyzes past cyberattacks and helps detect new attacks more quickly based on learned patterns. As a result, systems become increasingly secure. However, this technology is not only beneficial; it also has its challenges. For example, the protection of personal data may be compromised, it is often unclear who is responsible if AI makes incorrect decisions, and most importantly, cybercriminals can also exploit these technologies. Therefore, when using AI, continuous human oversight and adherence to clear ethical guidelines are essential.

In the future, AI is expected to evolve into systems capable of independently detecting attacks, learning users' normal behavior patterns, identifying anomalies, and even explaining their decisions. Technologies such as LSTM and Transformer models play a significant role in this process. Integrating generative AI into Intelligent Transportation Systems creates vast opportunities, but it also introduces serious challenges, particularly in terms of privacy and cybersecurity. As transportation systems become increasingly dependent on AI, protecting sensitive data and implementing strong measures against emerging cyber threats becomes critically important.

Generative AI can make transportation systems more intelligent and efficient; however, misuse or targeted attacks against such systems can pose significant risks. In particular, specialized attacks on AI-based systems may severely disrupt their functionality. Therefore, protecting transportation infrastructure, rapidly detecting attacks, and ensuring the secure storage of user data are crucial. It is also important to employ modern encryption techniques, monitor systems in real time, and implement adaptive security mechanisms capable of responding to changing conditions. Overall, since constantly evolving cyber threats can impact transportation systems, it is necessary to develop proactive security solutions that anticipate and prevent such risks. However, assigning too many responsibilities to artificial intelligence alone is also misguided. People themselves must remain vigilant and avoid sharing personal data with third parties. Filing complaints after negative consequences and expecting immediate solutions, then expressing dissatisfaction when outcomes fall short, can be counterproductive, as some issues still lack clear resolution mechanisms. To address this, citizens should be regularly informed and warned through television, radio broadcasts, and public meetings. Many people remain unaware of new developments, so local community structures should also take responsibility for educating and warning residents under their jurisdiction.

Keywords: Generative artificial intelligence, learning systems, cybersecurity, artificial intelligence security, data privacy, model reliability, secure AI architecture, threat models, cyber fraud, digital transformation.

Аннотация

Использование искусственного интеллекта в кибербезопасности коренным образом изменило способы реагирования организаций на угрозы. Искусственный интеллект способен быстро и непрерывно анализировать большие объёмы данных, что помогает заранее выявлять проблемы. Интеллектуальные системы автоматически управляют безопасностью, а при совместной работе с людьми достигаются ещё более высокие результаты. Искусственный интеллект постоянно отслеживает действия пользователей и выявляет уязвимости в системе.

Искусственный интеллект, особенно с использованием методов Machine Learning, анализирует предыдущие кибератаки и на этой основе помогает быстрее выявлять новые угрозы. Благодаря этому системы становятся более защищёнными. Однако данная технология имеет не только преимущества, но и ряд проблем. Например, может нарушаться защита персональных данных, остаётся неясным, кто несёт ответственность в случае ошибочных решений ИИ, и, что наиболее опасно, киберпреступники также могут использовать эти технологии в своих целях. Поэтому при использовании ИИ необходимо обеспечивать постоянный человеческий контроль и соблюдать чёткие этические нормы. В будущем ожидается, что ИИ будет развиваться дальше и превратится в системы, способные самостоятельно обнаруживать атаки, изучать типичное поведение пользователей, выявлять аномалии и даже объяснять принятые решения. Такие технологии, как LSTM и Transformer model, играют важную роль в этом процессе. Интеграция генеративного ИИ в Intelligent Transportation Systems открывает большие возможности, но одновременно создаёт серьёзные проблемы, особенно в области конфиденциальности и кибербезопасности. Поскольку транспортные системы всё больше зависят от ИИ, защита чувствительных данных и принятие эффективных мер против новых видов киберугроз становятся крайне важными.

Генеративный ИИ способен сделать транспортные системы более интеллектуальными и эффективными, однако его неправильное использование или целенаправленные атаки могут представлять серьёзную угрозу. В частности, специализированные атаки на системы, основанные на ИИ, могут существенно нарушить их работу. Поэтому защита транспортной инфраструктуры, быстрое выявление атак и обеспечение безопасности пользовательских данных являются ключевыми задачами. Кроме того, важно применять современные методы шифрования, осуществлять мониторинг систем в реальном времени и внедрять адаптивные системы безопасности, способные реагировать на изменяющиеся условия.

В целом, учитывая, что постоянно меняющиеся киберугрозы могут оказывать влияние на транспортные системы, необходимо разрабатывать проактивные решения в области безопасности, направленные на их предотвращение. Вместе с тем, перекладывать слишком много задач исключительно на искусственный интеллект также является ошибочным подходом. Люди сами должны быть внимательными и не передавать личные данные третьим лицам. Обращение с жалобами после негативных последствий и последующее недовольство результатами также может быть неэффективным, поскольку способы решения некоторых проблем всё ещё остаются не до конца определёнными.

В связи с этим необходимо регулярно информировать и предупреждать граждан через телевидение, радиопередачи и общественные собрания. Многие люди остаются неосведомлёнными о новых угрозах, поэтому местные органы самоуправления также должны предпринимать усилия по информированию населения и повышению их осведомлённости.

Ключевые слова: Генеративный искусственный интеллект, системы обучения, кибербезопасность, безопасность искусственного интеллекта, конфиденциальность данных, надежность моделей, безопасная архитектура ИИ, модели угроз, кибермошенничество, цифровая трансформация.

Kirish

So‘nggi yillarda Generativ sun‘iy intellekt texnologiyalarining jadal rivojlanishi global miqyosda barcha sohalarga, xususan ta‘lim tizimiga sezilarli ta‘sir ko‘rsatmoqda. Ushbu texnologiyalar yordamida o‘quv jarayonini individuallashtirish, o‘quv materiallarini avtomatik yaratish, bilimlarni chuqur tahlil qilish va o‘qitish samaradorligini oshirish imkoniyatlari kengaymoqda. Natijada ta‘lim tizimlari an‘anaviy shakldan raqamli va aqlli tizimlarga o‘tmoqda. Biroq, ushbu transformatsiya jarayoni bilan birga kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Sun‘iy intellekt asosidagi tizimlar katta hajmdagi ma‘lumotlarga tayanadi va bu esa ularni turli kiberhujumlar uchun nishonga aylantiradi. Ayniqsa, ma‘lumotlar maxfiyligi, model ishonchliligi va noto‘g‘ri qarorlar qabul qilish xavfi muhim muammolar sifatida namoyon bo‘lmoqda. Ushbu maqolamning asosiy maqsadi - generativ sun‘iy intellekt sharoitida ta‘lim tizimlarining transformatsiyasini o‘rganish, mavjud kiberxavfsizlik tahdidlari va ishonchlilik muammolarini tahlil qilish hamda xavfsiz AI arxitekturalarini ishlab chiqish bo‘yicha ilmiy yondashuvlarni taklif etishdan iborat.

Generativ sun‘iy intellekt va ta‘lim tizimlarining raqamli transformatsiyasi.

Zamonaviy ta‘lim tizimlarida Raqamli transformatsiya jarayoni sun‘iy intellekt bilan chambarchas bog‘liq. Generativ AI texnologiyalari o‘quvchilarning ehtiyojlariga moslashtirilgan kontent yaratish imkonini beradi. Masalan, AI yordamida avtomatik testlar tuzish, referatlar tayyorlash, interaktiv darslar ishlab chiqish mumkin. Bundan tashqari, AI asosidagi tizimlar o‘quvchilarning bilim darajasini real vaqt rejimida baholaydi, shaxsiy o‘quv trajektoriyalarini shakllantiradi va o‘qituvchilar yuklamasini kamaytiradi. Shu bilan birga, generativ AI noto‘g‘ri yoki soxta ma‘lumotlar yaratishi mumkin, bu esa ta‘lim sifati va ishonchliligiga salbiy ta‘sir ko‘rsatadi.

Sun‘iy intellekt asosidagi kiberxavfsizlik tahdidlari va ishonchlilik muammolari.

AI asosidagi tizimlar turli xil kiberxavflarga duch keladi. Ular orasida quyidagilar muhim hisoblanadi: adversarial hujumlar, ma‘lumotlar maxfiyligi buzilishi, modelga hujumlar va ichki tahdidlar. Adversarial hujumlar AI modellarga noto‘g‘ri ma‘lumot berish orqali ularni chalg‘itishga qaratilgan. Bu ayniqsa ta‘lim tizimlarida baholash tizimlarini buzishga olib kelishi mumkin. Ma‘lumotlar maxfiyligi buzilishi foydalanuvchilarning shaxsiy ma‘lumotlari oshkor bo‘lishiga olib keladi. Bu esa huquqiy va axloqiy muammolarni keltirib chiqaradi. Modelni o‘qitish jarayonida zararli ma‘lumotlar kiritilishi mumkin. Bu esa noto‘g‘ri natijalar beruvchi tizimlarga olib keladi. Tizim foydalanuvchilari tomonidan noto‘g‘ri foydalanish ham xavf tug‘diradi.

AI tizimlarining ishonchliligi muhim omillardan biridir. Model ishonchliligi quyidagi muammolar bilan bog‘liq: noto‘g‘ri yoki biasli ma‘lumotlar, modelning tushuntirib bera olmasligi

ya'ni black-box muammosi, qaror qabul qilishdagi noaniqliklar. Shu sababli Explainable AI konsepsiyasi muhim ahamiyat kasb etadi.

Xavfsiz AI arxitekturasini yaratish zamonaviy ilmiy tadqiqotlarning asosiy yo'nalishlaridan biridir. Xavfsiz AI tizimlari quyidagi komponentlardan iborat bo'lishi kerak: ma'lumotlarni himoya qilish mexanizmlari, modelni himoyalash, monitoring va audit tizimlari va foydalanuvchi autentifikatsiyasi. Shuningdek, tahdid modellari orqali tizim zaifliklari oldindan aniqlanishi mumkin.

Sun'iy intellekt texnologiyalari bugungi kunda kelajak taraqqiyotini belgilovchi muhim omillardan biri sifatida e'tirof etilmoqda. McKinsey Global Institute tomonidan olib borilgan tadqiqotlarga ko'ra, 2030-yilga borib sun'iy intellekt jahon yalpi ichki mahsulotiga 13 trillion dollardan ortiq qo'shimcha qiymat keltirishi prognoz qilinmoqda. Bu ko'rsatkich mazkur texnologiyalarning global iqtisodiyotdagi o'rni va ta'siri naqadar sezilarli ekanini yaqqol namoyon etadi. Mamlakatimizda ham raqamli texnologiyalar, xususan sun'iy intellektni rivojlantirish va ta'lim tizimiga keng joriy etish yo'nalishida izchil islohotlar amalga oshirilmoqda.

Xususan, "Raqamli O'zbekiston - 2030" strategiyasini hayotga tatbiq etish doirasida 2021-yil 17-fevralda "Sun'iy intellekt texnologiyalarini tezkor joriy etish uchun zarur shart-sharoitlar yaratish chora-tadbirlari to'g'risida"gi Prezident qarori qabul qilindi. Mazkur hujjat raqamli iqtisodiyotni jadallik bilan rivojlantirish, zamonaviy texnologiyalarni keng qo'llash hamda ushbu yo'nalishda ustuvor vazifalarni samarali amalga oshirishga xizmat qilishi bilan muhim ahamiyat kasb etadi.

Raqamli iqtisodiyot sharoitida ta'lim tizimini rivojlantirish oddiy jarayonlarni raqamlashtirish bilan cheklanmaydi, balki butun ta'lim jarayonining maqsadi, tuzilishi va mazmunini tubdan yangilashni talab etadigan kompleks yondashuvni taqozo etadi. Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va ularning ta'lim jarayoniga integratsiyalashuvi natijasida o'qitish usullari va vositalarida sezilarli o'zgarishlar yuz berdi. Jumladan, turli raqamli platformalar, masofaviy kurslar, simulyatorlar hamda virtual muhitlardan foydalanish kengayib, ta'lim olish imkoniyatlarini yanada kengaytirdi. Shu bilan birga, axborot texnologiyalarining qo'llanilishi o'quv jarayonini individuallashtirishga xizmat qilib, har bir o'quvchining ehtiyoji, qiziqishi va qobiliyatiga moslashtirilgan ta'limni tashkil etishga zamin yaratmoqda. Bundan tashqari, ta'lim jarayoniga interaktiv va o'yin elementlariga asoslangan metodlarning joriy etilishi bilimlarni samarali o'zlashtirishga, o'quvchilarning faolligi va motivatsiyasini oshirishga ijobiy ta'sir ko'rsatmoqda. Ta'lim mazmuni ham tobora amaliyotga yaqinlashib, ayniqsa oliy ta'lim bosqichida startap loyihalar, biznes-rejalar va amaliy tashabbuslar markaziy o'rin egallay boshladi. Mamlakatimizda esa maktabgacha ta'limdan tortib oliy ta'limgacha bo'lgan barcha bosqichlarni rivojlantirish, yangi ta'lim muassasalarini barpo etish va mavjud infratuzilmani modernizatsiya qilishga qaratilgan keng ko'lamli islohotlar amalga oshirilmoqda. Bu sa'y-harakatlar yosh avlodning har tomonlama kamol topishiga xizmat qilmoqda. Shu bilan birga, sun'iy intellekt texnologiyalari jadal rivojlanayotgan sohalardan biri sifatida alohida ahamiyat kasb etib, inson faoliyatiga xos jarayonlarni modellashtirish va turli vazifalarni yuqori aniqlikda bajarishga qodir bo'lgan aqlli tizimlarni yaratishni o'z ichiga oladi.

Machine Learning texnologiyalari kiberxavfsizlikda muhim rol o'ynaydi. Ayniqsa, LSTM vaqt ketma-ketligini tahlil qiladi va transformer model katta hajmdagi ma'lumotlarni samarali qayta ishlaydi. Ushbu modellar tahdidlarni aniqlash va prognoz qilishda keng qo'llaniladi.

Intelligent Transportation Systems bilan generativ AI integratsiyasi yangi imkoniyatlar yaratadi, masalan transport oqimini optimallashtiradi, avtonom boshqaruv tizimlarini amalga

oshiradi va real vaqt monitoringini olib boradi. Biroq bu tizimlar kiberhujumlar uchun zaif bo'lishi mumkin, maxfiy ma'lumotlarga boy bo'lishi shubhasiz va real hayot xavfsizligiga ta'sir qiladi.

Sun'iy intellekt davrida kiberxavfsizlik istiqbollari va xavfsiz AI arxitekturalari.

2023-yil may oyida AQSh Ta'lim vazirligi "Sun'iy intellekt asosida o'qitishda ta'limning kelajagi: tushunchalar va tavsiyalar" nomli hisobotini e'lon qildi. Vazirlik 2022-yilda 700 dan ortiq kishi, jumladan, o'qituvchilar va ota-onalar bilan sun'iy intellekt haqidagi fikrlarini o'rganish uchun tinglash sessiyalarini o'tkazdi. Hisobotda ta'kidlanishicha, "ta'lim texnologiyalarida sun'iy intellektning kutilayotgan o'sishidan oldinroq harakat qilish uchun saylovchilar hozirdanoq harakat qilish kerak deb hisoblaydilar va ular birgalikda ishlashni xohlashadi". Ta'limda sun'iy intellektidan foydalanishning yana bir afzalligi bu uning katta hajmdagi ma'lumotlarni tahlil qilishidir. Bundan tashqari, intellektual tizim talabalarga maqbul bo'lgan qaysi o'qitish usullari eng samarali ekanligini va qaysi mavzularni o'zlashtirish ularga qiyinchiliklar tug'dirishini aniqlay oladi. Bu, o'z navbatida, o'qituvchilarga o'z dasturlarini moslashtirish va ularni talabalar uchun qulayroq qilish imkonini beradi. Shuni ta'kidlash joizki, talabalar fanlar bo'yicha mustaqil ishlarni bajarish jarayonida sun'iy intellekt texnologiyalaridan foydalanishlari muhim ahamiyat kasb etadi. Mustaqil ishlarni bajarish jarayonida katta hajmdagi yangi ma'lumotlarni tahlil qilishlari va ularni o'zlashtirishlari lozim bo'lgan taqdirda intellektual tizimlardan didaktik vosita sifatida foydalanish yaxshi samara beradi. Bundan tashqari, SI algoritmlari ta'lim dasturlari va platformalarida baholash, tarkibni tavsiya qilish va talabalarning fikr-mulohazalarini yaratish kabi vazifalarni avtomatlashtirish uchun amalga oshiriladi. Tabiiy tilni qayta ishlash algoritmlari talabalarning so'rovlari va yozma javoblarini tushunish va ularga javob berishga qodir bo'lgan aqlli repetitorlik tizimlarini rivojlantirishga imkon beradi.

Zamonaviy kiberxavflar sharoitida quyidagi choralar muhim: real vaqt monitoringi, kuchli shifrlash algoritmlari, AI asosidagi xavfsizlik tizimlari va inson nazorati. Proaktiv yondashuv tahdidlarni oldindan aniqlash imkonini beradi. AI texnologiyalaridan foydalanishda axloqiy me'yorlarga rioya qilish zarur, foydalanuvchi ma'lumotlarini himoya qilish shart va jamoatchilikni xabardor qilish muhim hisoblanadi. Aholini ommaviy axborot vositalari orqali ogohlantirish ham muhim ahamiyatga ega. Oddiy misol, Telegram messengerida turli xildagi firibgarlik miqdori tobora oshib bormoqda. Dastlab, notanish accountdan "videodagi sizmi?" – deb APK fayl tashlash urf bo'ldi, keyin esa "Sud qarori" – deb xabarlar kelishni boshladi, hozir esa yaqin isoningni nomidan yozib profil rasmlarini ajratib bo'lmaydigan darajada tayyorlab "qarz berib tur, hozir pul zarur, ertaga qaytib beraman" – degan xabarlar kelmoqda va bular bari firibgarlikning yangi versiyadagi ko'rinishidir. Mana shu yangi accountlardan kelgan xabarlarni ochmaslik yoki tekshirish uchun GenAI bizga samarali yordam bera oladi deb o'ylayman. AI arxitekturalari rivojlanish uchun zarur, ammo inson omili baribir chetda qolmasligi kerak. Moliyaviy korxonalarda, muddatli to'lov tashkilotlarida, jumladan, banklarda ko'plab firibgarliklarni guvohi bo'lganman va bu firibgarliklarning aksariyati online kredit joriy etilgandan so'ng sodir bo'lgan, demak AI va elektron tizimlar ko'paygan sari yangi turdagi firibgarliklar kelib chiqishining ham ehtimoli juda yuqori. Bu muammolarga qarshi kurashish uchun fuqarolarni muntazam ogohlantirish kerak va inson omilini ko'proq qilish joiz. "Xavfsiz AI arxitekturalari" - bu sun'iy intellekt tizimlarini xatolardan, zararli foydalanishdan va nazoratdan chiqib ketishdan himoyalangan holda loyihalash degani. Biz aynan Artificial Intelligence ichidagi AI Safety yo'nalishini chuqur o'rganishimiz lozim. Afsuski, hozirgi vaqtda juda kam sonli mamlakatlarda bu soha o'qitiladi. AQSh, Buyuk Britaniya, Kanada, Germaniya, Fransiya, Singapur, Janubiy Koreya mamlakatlari shular jumlasidandir. Bunday kiber firibgarliklarning aksariyatini yoshi katta

insonlar tashkil etadi. Chunki, yoshi katta insonlar ijtimoiy tarmoqlardan yoki elektron to'lov tizimlaridan to'g'ri foydalanishni bilmasliklari va kerakli yangiliklardan bexabar bo'lishlarining ehtimoli yuqori. Ammo, hozir fuqarolar kredit olishga taqiq qo'ya olishadi va davlatimiz shu kabi yechimlar ustida ishlashni davom etmoqda. Mana shunday xavfsizlik uchun joriy etilgan har bir yangi g'oya kelajakda xalqimizning millionlab qismini firibgarliklardan saqlab qoladi va hatto chetga ham bu uslublarni sotishi mumkin, agar rostdan ham g'oya juda foydali, keng qamrovli va umumiy bo'lsa.

Zamonaviy kiberxavfsizlik vositalari va strategiyalari endi sun'iy intellekt bilan bog'liq komponentlarning kombinatsiyasiga bog'liq. Masalan, Machine Learning muntazamlikni tanib olish va o'tmishdagi voqealardan o'rganish imkonini beradi, ma'lumotlar analizi ya'ni katta ma'lumotlar to'plamidan tahlil qilish imkonini beradi, intellektual tahlil ya'ni tarixiy ma'lumotlarga asoslangan potentsial tahdidlarni bashorat qilish, xatti-harakatlar tahlili esa anomaliyalarni aniqlash uchun foydalanuvchilarning xatti-harakatlarini kuzatish va tahlil qilish, avtomatlashtirilgan qaror qabul qilish esa aniqlangan tahdidlarga tezkor javob berish imkonini beradi. Shuningdek, kiberxavfsizlikda inson omili, ayniqsa murakkab hujumlarni qayta ishlashda eng muhim zaifliklardan biri bo'lib hisoblanadi. Biroq, SI ma'lumotlar hajmi va murakkabligini qayta ishlashda inson tahlilidan ustundir. Ko'pgina tashkilotlarda bilimli kadrlar yetishmasligi tufayli inson tahlili SI bilan raqobatlasha olmaydi. Biroq, kiber mudofaaning kuchayishi bilan bir qatorda, sun'iy intellekt yanada murakkab kiberhujumlarni yaratish vositasiga aylanmoqda. Hujumchilar aqlli va aniqlash qiyin bo'lgan tahdidlarni yaratish uchun mashinani o'rganish ya'ni ML texnologiyalaridan foydalanishlari mumkin. Bu kiberxavfsizlik usullarini doimiy ravishda takomillashtirish va yangi muammolarga moslashish zarurligini ta'kidlaydi. Muhokamaning muhim jihatlaridan biri bu kiberxavfsizlikda sun'iy intellektdan foydalanish bilan bog'liq axloqiy masalalardir. Maxfiylik, qaror qabul qilish uchun javobgarlik va ushbu sohada standartlarni yaratish va tartibga solish masalalari tobora dolzarb bo'lib bormoqda. Bunga parallel ravishda "Dark AI" paydo bo'ldi, u sun'iy intellekt texnologiyalarini, xususan, generativ AI sohasidagi so'nggi yangiliklarni kiberhujumlarni tezlashtirish yoki ta'minlash uchun qo'llaniladi. Shuningdek, u xavfsizlik tizimlarini buzish uchun o'z usullarini o'rganishi va moslashtirishi mumkin.

Shu nuqtai nazardan, davlat boshqaruvi organlari texnologik rivojlanish sur'atlariga moslashishi dolzarb ahamiyat kasb etadi. Ayniqsa, sun'iy intellekt imkoniyatlaridan samarali foydalanish orqali kiberxavfsizlik tizimlarini takomillashtirish muhimdir, zero raqamli makondagi tahdidlar tobora murakkablashib, xilma-xilligi ortib bormoqda. Shu bois, kriptografiya, sun'iy intellekt va ma'lumotlarni himoya qilish yo'nalishlarida ilg'or yechimlar ishlab chiquvchi ilmiy markazlar hamda startap loyihalarni moliyaviy qo'llab-quvvatlash zarur. Bundan tashqari, soha uchun malakali kadrlar tayyorlash maqsadida maxsus ta'lim dasturlari, o'quv kurslari va amaliy treninglarni tashkil etish muhim hisoblanadi.

Shuningdek, kiberxavfsizlik sohasida innovatsion texnologiyalar yaratishga ixtisoslashgan kompaniyalarni rag'batlantirish maqsadida soliq imtiyozlari va grant mexanizmlarini joriy etish maqsadga muvofiqdir.

Microsoft Research tahlilchilarining ma'lumotlariga ko'ra, sun'iy intellekt ta'siriga eng ko'p duchor bo'ladigan kasblar qatoriga tarjimonlar, yozuvchilar, tarixchilar, mijozlarni qo'llab-quvvatlash xizmati xodimlari, sotuvchilar, telefon operatorlari, chipta xizmatlari kassirlari, shuningdek, radio boshlovchilar va dijeylar kiradi.

Biroq ushbu jarayon mutaxassislarning mehnat bozoridan siqib chiqarilishiga emas, balki inson va texnologiya o'rtasidagi hamkorlikning yanada mustahkamlanishiga olib kelishi mumkin. Bu nuqtai nazardan, sun'iy intellekt samaradorlikni oshiruvchi muhim vosita sifatida namoyon bo'ladi. U matn yaratish, ilmiy tadqiqotlarni amalga oshirish hamda kommunikatsiya jarayonlarini qo'llab-quvvatlash kabi turli funksiyalarni bajarish imkoniyatiga ega. Shunga qaramay, ayrim jarayonlarda inson omilini to'liq almashtirish salohiyati hali ham cheklanganligicha qolmoqda. Bundan tashqari, avtomatlashtirish jarayoni jismoniy mehnat talab qiladigan kasblarga nisbatan kamroq ta'sir ko'rsatadi. Jumladan, ishlab chiqarish uskunolari operatorlari, qo'l mehnatiga asoslangan mutaxassislar, tibbiyot xodimlari hamda massaj xizmatlari bilan shug'ullanuvchi kasb egalari ushbu toifaga kiradi.

Masalan, jurnalistikaning asosiy vazifalaridan biri bu - ishonchli, tekshirilgan, muvozanatli axborotni jamiyatga taqdim etishdir. Ammo sun'iy intellekt asosida yaratilgan kontentlar bu tamoyilga doim ham rioya qilmaydi. Algoritmalar ko'pincha inson jurnalistlaridan farqli o'laroq, axborotning ijtimoiy yoki siyosiy kontekstini tushunmaydi, faqat statistik yoki semantik o'xshashliklarga asoslanadi. Natijada, ba'zan noto'g'ri yoki kontekstdan yulib olingan xabarlar tarqaladi. Aynan shu yerda inson omilining o'rni yana bir bor o'z ahamiyatini ko'rsatadi - sun'iy intellekt vositalaridan foydalanganda, ularni inson nazorati bilan uyg'unlashtirish zarur. Boshqa jihatdan qaralganda, sun'iy intellektning rivojlanishi ayrim kasb egalari uchun yangi turdagi xavf-xatarlarni ham keltirib chiqarmoqda. Eng dolzarb muammolardan biri - bu soxta axborotlar hamda dezinformatsiya jarayonlarining sun'iy intellekt yordamida avtomatlashtirilgan holda keng miqyosda tarqatilishidir. Hozirgi davrda "deepfake" texnologiyalari vositasida real ko'rinishga ega bo'lgan, ammo aslida soxta bo'lgan video tasvirlar va audiolar tayyorlanmoqda. Bunday kontent nafaqat oddiy foydalanuvchilarni, balki yirik tashkilotlar va kompaniyalar mutaxassislarni ham chalg'itishi, noto'g'ri qarorlar qabul qilinishiga sabab bo'lishi mumkin. Natijada esa ommaviy axborot vositalariga nisbatan ishonch darajasi pasayib boradi, jamiyatda beqarorlik kuchayadi hamda yolg'on ma'lumotlar orqali jamoatchilik fikrini boshqarish imkoniyatlari kengayadi.

Bot texnologiyalarining tobora rivojlanib, inson intellektiga xos xatti-harakatlarni taqlid qila boshlashi generativ sun'iy intellektidan xavfsizlik sohasida ham keng foydalanishni taqozo etmoqda. Xususan, ilg'or CAPTCHA tizimlari hamda botlarni aniqlash mexanizmlarini ishlab chiqishda sun'iy intellektga asoslangan yondashuvlar muhim ahamiyat kasb etmoqda. Bunday yechimlar inson faoliyati bilan avtomatlashtirilgan jarayonlar o'rtasidagi farqlarni yanada aniqroq ajratish imkonini berib, veb-ilovalar va API tizimlarining himoya darajasini oshiradi. Juda ko'plab zarur ma'lumotlarda CAPTCHA, masalan Mi Cloudda ancha yordam bermoqda. Bank ilovalari va plastic kartalar ya'ni moliyaviy rejalar uchun esa sms kod hamda ikki yoqlama autentifikatsiya tizimlari millionlab firibgarliklarni oldini olishga muvaffaqiyatli yordam bermoqda.

Xulosa.

Xulosa qilib aytganda, generativ sun'iy intellekt ta'lim tizimlarini tubdan o'zgartirmoqda va yangi imkoniyatlar yaratmoqda. Shu bilan birga, u kiberxavfsizlik tahdidlari va ishonchlilik muammolarini ham yuzaga keltirmoqda. Xavfsiz AI arxitekturalarini ishlab chiqish, proaktiv xavfsizlik choralarini joriy etish va inson nazoratini saqlab qolish ushbu muammolarni hal etishda muhim ahamiyatga ega. Kelajakda AI yanada rivojlanib, yanada aqlli va xavfsiz tizimlarga aylanishi kutilmoqda, biroq bu jarayonda texnologik, huquqiy va axloqiy muvozanatni saqlash zarur. Ayniqsa, biz Generativ sun'iy intellekt sharoitida ta'lim tizimlari va kiberxavfsizlikni transformatsiya qilish, tahdidlar, ishonchlilik muammolari va xavfsiz AI arxitekturalari uchun

xorijiy mamlakatlardan yangi tizimlarni, dasturlarni va mutaxassislarni olib kelishimiz kerak, keyin ulardan jarayonlarni o'rganishimiz kerak yoki bilimli yoshlarni moliyaviy jihatdan ta'minlagan holda aynan shu sohadagi bilimlarni qo'lga kiritib kelish uchun horijga tahsil olishga yuborishimiz zarur. Chunki, hozirgi vaqtda bizda bu sohalarida mutaxassislar yetishmaydi, kuchli dasturchilar soni ham kam. Shu bilan birga, sun'iy intellekt modellari parollarni aniqlashga qaratilgan yanada murakkab va samarali algoritmlarni yaratish imkoniyatiga ega bo'lib, bu qo'pol kuch ya'ni brute force hujumlarining samaradorligini oshirishi mumkin. Bunda AI insonning qurilmadagi parollari hamda harakatlarini tahlil qiladi, ehtimoli yuqori parollarni taxmin qilib topadi va firibgarlikka keng qamrovda imkoniyat ochib beradi. Mazkur holat axborot xavfsizligini ta'minlashda kuchli va noyob parollardan foydalanish, shuningdek, ko'p faktorli autentifikatsiya mexanizmlarini joriy etish zaruratini yanada kuchaytiradi.

Sun'iy intellekt asrida kiberxavfsizlik istiqbollari yangi imkoniyatlar bilan bir qatorda murakkab muammolarni ham yuzaga keltirmoqda. Hozirgi kunda zamonaviy AI texnologiyalari tahdidlarni aniqlash va ularning oldini olishda keng qo'llanilayotgan bo'lsa-da, texnologik taraqqiyot jarayoni yangi turdagi xavf-xatarlarning paydo bo'lishiga sabab bo'lmoqda. Xususan, sun'iy intellekt asosida ishlovchi avtonom kiberhujumlar an'anaviy himoya mexanizmlarini chetlab o'tish va ularga moslashish qobiliyatiga ega bo'lib, bu esa mutaxassislardan yanada murakkab, moslashuvchan va tezkor yondashuvlarni talab etadi. Kelajakda ustuvor vazifalardan biri - monitoring va tezkor javob choralarini avtomatlashtirishga asoslangan holda, AI tizimlari va kiberhimoya o'rtasidagi o'zaro integratsiyani samarali hamda xavfsiz yo'lga qo'yishdan iborat. Shu bilan birga, yangi texnologiyalarni ishlab chiqish jarayonida ma'lumotlar maxfiyligi, foydalanuvchi xavfsizligi, shuningdek, axloqiy va huquqiy me'yorlarga rioya etish masalalari alohida e'tibor talab qiladi. Umuman olganda, kiberxavfsizlikning kelajakdagi rivoji sun'iy intellektni himoya tizimlariga chuqur integratsiya qilish bilan birga, undan noqonuniy foydalanish natijasida yuzaga keladigan tahdidlarni minimallashtirish imkoniyatlariga bevosita bog'liqdir. Bu yo'nalishda asosiy e'tibor kadrlar tayyorlash tizimini rivojlantirish, xalqaro hamkorlikni kengaytirish hamda doimiy o'zgarib borayotgan tahdidlarga moslasha oladigan zamonaviy va moslashuvchan xavfsizlik tizimlarini yaratishga qaratilishi lozim. Shunday qilib, sun'iy intellekt davrida kiberxavfsizlikning istiqboli innovatsion texnologiyalarni huquqiy va axloqiy tamoyillar bilan uyg'unlashtirgan kompleks yondashuvni, shuningdek, mutaxassislarning yangi tahdidlarga tezkor va samarali javob berish qobiliyatini talab etadi.

Eng yaxshi yo'l biz AI orqali biror yangilikni kashf qilganimizdan so'ng uzoq vaqt yoki uzoq yillar mobaynida uni sinovdan o'tkazishimiz lozim va o'sha sinovda yo'ldan chiqqan muammolarga yechim topib bo'lganimizdan keyingina o'sha kashfiyotni insonlar bilan ulashsak bo'ladi. Ammo, tavakkalga asoslangan holda yangi loyihani yoki tizimni ommaga tashviq etish ko'plab insonlarning va tashkilotlarning xavfli risklarini kuchaytirib yuborishi shubhasizdir.

Foydalanilgan adabiyotlar ro'yxati

1. National Institute of Standards and Technology (NIST), AI Risk Management Framework, 2023.
2. Finale Doshi-Velez, Been Kim.
3. Towards A Rigorous Science of Interpretable Machine Learning, 2017.
4. European Union Agency for Cybersecurity –
5. Threat Landscape Report, 2023.
6. Sun'iy intellekt davrida kiberxavfsizlikning kelajagi. InfoCOM.UZ, 2025.
7. World Economic Forum –

8. Global Cybersecurity Outlook, 2024.
9. McKinsey & Company –
10. The Future of Work in the Age of AI, 2023.
11. Hasanova Zarina Sodiqovna - SUN'IY INTELEKT VA AXBOROT ISHONCHLILIGI: JURNALISTIKANING KELAJAGI.
12. European Union Agency for Cybersecurity.
13. Threat Landscape: Deepfakes and Information Manipulation, 2023.
14. Digital Identity Guidelines (SP 800-63), 2022.
15. Cybersecurity Threat Landscape, 2023.
16. OECD. (2023). Income-based tax relief for R&D and innovation: An integrated view. OECD Publishing.
17. Russell, S. (2019). Human compatible: Artificial intelligence and the problem of control, Viking.
18. Von Ahn, L., Blum, M., Hopper, N. J., & Langford, J. (2003). CAPTCHA: Using hard AI problems for security. In Advances in Cryptology.
19. UNESCO. (2023). Guidance for generative AI in education and research. UNESCO Publishing.
20. National Institute of Standards and Technology. (2020). Digital Identity Guidelines: Authentication and Lifecycle Management.
21. World Economic Forum. (2024). Global Cybersecurity Outlook 2024.
22. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. (2024). Raqamli O'zbekiston - 2030 strategiyasi.
23. O'zbekiston Respublikasi Vazirlar Mahkamasi. (2020). Kiberxavfsizlik to'g'risida konsepsiya.
24. Karimov, A. A. (2023). Sun'iy intellekt texnologiyalarining ta'lim tizimiga ta'siri. O'zbekiston Axborot Texnologiyalari Jurnal, 15-22.
25. O'zbekiston Respublikasi Prezidentining farmoni (2021). Sun'iy intellekt texnologiyalarini rivojlantirish chora-tadbirlari to'g'risida (PF-4996).