IJIS INTERNATIONAL JOURNAL OF INTEGRATED SCIENCES

SUN'IY INTELLEKT DAVRIDA KIBERXAVFSIZLIK: AI TIZIMLARINI HIMOYA QILISH UCHUN YANGI MUAMMOLAR VA YECHIMLAR

Toshpo‘latova Dilfo‘za Komiljon qizi
Toshkent axborot texnologiyari unevirsiteti Samarqand filiali 3-bosqich talabasi

Annotatsiya*: Ushbu maqolada kiberxavfsizlik va sun’iy intellect raqamli hayotimizga nechog’lik ta’sir ko’rsatishi va raqamli hayotimini himoya qilishdagi o‘rni muammolar va yechimlar haqida so‘z boradi.*

Kalit so‘zlar: *AI modellari, kiberxavfsizlik, xavfsizlik tahlili, monitoring, axloqiy mulohazalar, fishing, tarmoq xavfsizligi.*

Kiberxavfsizlik: raqamli dunyomizni himoya qilish.

Kiberxavfsizlik tobora raqamli hayotimizning muhim jihati hisoblanadi. U bizning onlayn ma'lumotlarimiz, tizimlarimiz va qurilmalarimizni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish yoki yo'q qilishdan himoya qilish uchun mo'ljallangan amaliyot va texnologiyalarni o'z ichiga oladi.

Bu yerda asosiy jihatlarning taqsimoti:

Tahdidlar va zaifliklar:

* Zararli dastur: viruslar, qurtlar, troyanlar, to'lov dasturlari va tizimlarga zarar etkazishi, ma'lumotlarni o'g'irlashi yoki operatsiyalarni buzishi mumkin bo'lgan boshqa zararli dasturlar.

* Fishing: Aldamchi elektron pochta xabarlari, xabarlar yoki veb-saytlar foydalanuvchilarni aldab, parollar yoki moliyaviy tafsilotlar kabi nozik ma’lumotlarni oshkor qiladi.

* Ijtimoiy muhandislik: maxfiy ma'lumotlarni oshkor qilish yoki psixologik taktikalar orqali tizimlarga kirish uchun shaxslarni manipulyatsiya qilish.

* Xizmatni rad etish (DoS) hujumlari: tizimni qonuniy foydalanuvchilar uchun mavjud bo'lmasligi uchun trafik bilan ortiqcha yuklash.

* Ma'lumotlarning buzilishi: maxfiy ma'lumotlarga ruxsatsiz kirish, ko'pincha moliyaviy daromad yoki josuslik uchun tashkilotlar va shaxslarni nishonga oladi.

Asosiy himoya sohalari:

* Tarmoq xavfsizligi: kompyuter tarmoqlari va infratuzilmasini ruxsatsiz kirishdan himoya qilish, shu jumladan xavfsizlik devorlari, bosqinlarni aniqlash tizimlari (IDS) va kirishni oldini olish tizimlari (IPS).

* Endpoint Security: Noutbuklar, smartfonlar va serverlar kabi individual qurilmalarni antivirus dasturlari, so'nggi nuqtani aniqlash va javob berish (EDR) va ma'lumotlarni shifrlash orqali himoya qilish.

* Ma'lumotlar xavfsizligi: shifrlash, kirishni boshqarish va ma'lumotlar yo'qotilishining oldini olish (DLP) mexanizmlari orqali nozik ma'lumotlarni himoya qilish.

* Ilova xavfsizligi: Xavfsiz kodlash amaliyotlari, zaifliklarni skanerlash va kirish testi orqali dasturiy ta'minot ilovalari va veb-xizmatlarini himoya qilish.

* Identity and Access Management (IAM): Rollar va ruxsatlar asosida tizimlar va resurslarga foydalanuvchi kirishini nazorat qilish, shu jumladan ko‘p faktorli autentifikatsiya (MFA).

* Xavfsizlik bo'yicha trening: foydalanuvchilarni kiberxavfsizlikning eng yaxshi amaliyotlari, keng tarqalgan tahdidlar va fishing urinishlarini qanday aniqlash va oldini olish haqida o'rgatish.

Sun'iy intellekt davrida kiberxavfsizlik: yangi chegaraga o'tish

Sun'iy intellekt (AI) va kiberxavfsizlikning yaqinlashuvi misli ko'rilmagan imkoniyatlarni ham, dahshatli muammolarni ham taqdim etadi. Sun'iy intellektning o'zgartiruvchi kuchi yangi imkoniyatlarni ochish bilan birga, yangi xavfsizlik strategiyalarini talab qiladigan zaifliklarni ham keltirib chiqaradi. Bu yerda AI tizimlarini himoya qilish bo'yicha asosiy muammolar va yechimlarning taqsimoti keltirilgan:

Qiyinchiliklar:

* Sun'iy intellektga asoslangan hujumlar: dushmanlar fishing, zararli dasturlarni yaratish va ijtimoiy muhandislik kabi zararli harakatlarni avtomatlashtirish va yaxshilash uchun AIdan tobora ko'proq foydalanmoqda. Bu aniqlash va javob berishni murakkablashtiradi.

* Ma'lumotlardan zaharlanish: AI tizimlari ma'lumotlar zaharlanishiga moyil bo'lib, bu erda zararli aktyorlar o'quv ma'lumotlar to'plamini ularning aniqligini buzish va noto'g'ri qarashlarni kiritish uchun manipulyatsiya qiladi.

* Modelni o'g'irlash va manipulyatsiya qilish: AI modellari, ayniqsa xususiy algoritmlar bilan ishlab chiqilganlar qimmatli intellektual mulkdir. Ular o'g'irlanishi yoki noto'g'ri natijalarni yaratish yoki nozik ma'lumotlarni sizib chiqarish uchun manipulyatsiya qilinishi mumkin.

* Sun'iy intellektga asoslangan kuzatuv va maxfiylik: yuzni aniqlash, xatti-harakatlarni tahlil qilish va boshqa kuzatuv ilovalari uchun sun'iy intellektdan keng foydalanish maxfiylikka oid jiddiy muammolarni keltirib chiqaradi va mustahkam xavfsizlik choralarini talab qiladi.

* AI qora qutisi muammosi: Murakkab AI modellarining noaniqligi ularning qaror qabul qilish jarayonlarini tushunishni qiyinlashtiradi, bu xavfsizlik tahlili va zaifliklarni aniqlashga xalaqit beradi.

Yechimlar:

* Sun'iy intellektga asoslangan mudofaa: anomaliyalarni aniqlash, tahdidlar haqida razvedka va avtomatlashtirilgan hodisalarga javob berish kabi sun'iy

intellektga asoslangan xavfsizlik echimlaridan foydalanish tahdidlarni aniqlik va tezlikni oshirish bilan aniqlash va yumshatishga yordam beradi.

* Ma'lumotlar yaxlitligi va tekshiruvi: Ma'lumotlarni tekshirishning ishonchli usullarini, ma'lumotlarning kelib chiqishini kuzatish va xavfsiz ma'lumotlarni saqlash mexanizmlarini joriy qilish ma'lumotlar zaharlanishining oldini olish va ma'lumotlar yaxlitligini ta'minlash uchun zarurdir.

* Model xavfsizligi va tushuntirish mumkinligi: AI modellari uchun xavfsiz ishlab chiqish amaliyotlarini ishlab chiqish, jumladan kodni chalkashtirish, modelni qattiqlashtirish va modelning tushuntirilishini oshirish usullari, bu ularning qaror qabul qilish jarayonlarini yaxshiroq tushunish imkonini beradi.

* Maxfiylikni yaxshilaydigan texnologiyalar: AI modelini o'rgatish va qo'llash paytida nozik ma'lumotlarni himoya qilish uchun federativ o'rganish, differentsial maxfiylik va gomomorfik shifrlash kabi maxfiylikni saqlaydigan AI usullarini joriy qiling.

* Inson va AI hamkorligi: AI xavfsizlikni kuchaytirishi mumkin bo'lsa-da, inson tajribasi muhim qarorlar qabul qilish, axloqiy mulohazalar va AI kurashishi mumkin bo'lgan murakkab vaziyatlarni hal qilish uchun juda muhimdir.

Asosiy fikrlar:

* Doimiy monitoring va moslashish: AI tahdidlarining o'zgaruvchan tabiati doimiy monitoringni, tahdidlar haqida ma'lumotni yangilashni va dushmanlardan oldinda bo'lish uchun moslashtirilgan xavfsizlik choralarini talab qiladi.

* Hamkorlik va almashish: sanoat hamkorligi, ma’lumot almashish va ochiq manbali xavfsizlik vositalari sun’iy intellekt tahdidlariga qarshi samarali mudofaa vositalarini birgalikda ishlab chiqish uchun juda muhimdir.

* Axloqiy mulohazalar: kiberxavfsizlikda sun’iy intellektdan foydalanish tarafkashlik, adolat va mas’uliyat bilan bog‘liq axloqiy mulohazalarni oshiradi. Shaffoflik va mas'uliyatli rivojlanish amaliyotini ta'minlash muhim ahamiyatga ega.

Xulosa:

AI tizimlarini himoya qilish ko'p qatlamli yondashuvni talab qiladigan doimiy muammodir. Sun’iy intellektga asoslangan himoya vositalarini qo‘llash, ma’lumotlar yaxlitligini birinchi o‘ringa qo‘yish, model xavfsizligini ta’minlash va inson va sun’iy intellekt hamkorligini rag‘batlantirish orqali biz sun’iy intellekt asrida rivojlanayotgan kiberxavfsizlik landshaftini yo‘lga qo‘yishimiz va yanada mustahkam raqamli kelajakni qurishimiz mumkin.

ADABIYOTLAR:

1. Shogan VV, Storozhakova EV. Methodology of teaching history at school. Textbook. - M.: Yurayt publishing house, 2019.

2. Tursunov F. G'. Improving the theory and methodology of legal education in non-legal higher education institutions (in the example of the educational direction "National idea, spiritual foundations and legal education"): Doctor of Pedagogical Sciences (PhD) ... dis. - Tashkent, 2020.

3. Akbarov D., Abdukadirov A., Umarov S. Research of general mathematical characteristics of logical operations and table replacements in cryptographic transformations //AIP Conference Proceedings. – AIP Publishing LLC, 2022. – T. 2432.

4. Umarov S. A. Research on General Mathematical Characteristics of Boolean Functions' Models and Their Logical Operations and Table Replacement in Cryptographic Transformations //Journal of Optoelectronics Laser. – 2022.