KIBER HUJUMLARDA SUN'IY INTELLEKTNING O'RNI: XAKERLAR VA HIMOYACHILAR POYGASI

Mualliflar: ***Tuychiyeva Setorabonu Nodir qizi***
Saydullayeva Gulsevar Alisher qizi
O'qituvchi: ***Ulasheva Shakhlo Tagayevna***

ANNOTATSIYA: *Ushbu maqolada kiberxavfsizlik olamidagi eng dolzarb transformatsiya — sun'iy intellektning (AI) hujumkor va mudofaa vositasiga aylanishi tahlil qilinadi. Maqolada xakerlar tomonidan AIning fishing, deepfake va polimorfik viruslarni yaratishda qo'llanilishi, shuningdek, kiber-himoyachilarning anomaliyalarni bashorat qilish va ularga avtomatik javob qaytarishda ushbu texnologiyadan foydalanish usullari yoritilgan. Asosiy e'tibor "algoritmlar jangi" davrida inson omilining o'rni va kiber-poyganing kelajakdagi rivojlanish tendensiyalariga qaratilgan. Maqola kiberxavfsizlik mutaxassislari, IT-talabalar va raqamli dunyoda o'z xavfsizligiga befarq bo'lmagan keng ommaga mo'ljallangan.*

Kalit so'zlar: *Kiberxavfsizlik, sun'iy intellekt, mashinali o'rganish,kebrhujum, depfake, aqlli fishing, Cyber Resilience, Adversarial AI, Automated Defense, Cyber Resilience* Vishing va smishing,SOAR tizimlari,endpoint himoyasi, Ma'lumotlar zaxarlanishi.

Kirish

Bugungi kunda biz kiberolamning tub burilish nuqtasida turibmiz. Agar o'tgan o'n yillikda kiberhujumlar asosan insonlar tomonidan yozilgan viruslar va statik kodlarga tayangan bo'lsa, 2026-yilga kelib vaziyat butunlay o'zgardi. Endi raqamli barrikadalarning har ikki tomonida — xakerlar safida ham, tizim himoyachilari orasida ham — eng qudratli qurol sifatida **Sun'iy Intellekt (AI)** namoyon bo'lmoqda.Kiberhujumlarning yangi to'lqini shunchaki ma'lumot o'g'irlash emas, balki "algoritmlar jangi"ga aylandi. Xakerlar AI yordamida soniyalar ichida millionlab parollarni tekshirish, inson ovozini mukammal taqlid

qilish (deepfake) va o‘z-o‘zini o‘zgartiruvchi zararli kodlarni yaratish imkoniyatiga ega bo‘ldilar. Ushbu texnologiya xavf-xatarlarni shunchalik masshtablashtirdiki, an’anaviy mudofaa tizimlari ularning tezligiga dosh bera olmay qoldi. Biroq, bu poygada faqat hujumkor tomon ustunlikka ega emas. Kiber-himoyachilar ham "mashinali o‘rganish" (Machine Learning) algoritmlari orqali xavfni u hali sodir bo‘lmasdan bashorat qilishni o‘rganmoqdalar. Mazkur maqolada biz sun’iy intellektning kiberolamda qanday qilib ham eng katta tahdid, ham eng kuchli qalqon bo‘lib xizmat qilayotganini, xakerlar va himoyachilar o‘rtasidagi ushbu intellektual poyga qayerga yetaklashini tahlil qilamiz.

Biroq, bu poygada faqat hujumkor tomon ustunlikka ega emas. Kiber-himoyachilar ham "mashinali o‘rganish" (Machine Learning) algoritmlari orqali xavfni u hali sodir bo‘lmasdan bashorat qilishni o‘rganmoqdalar. Mazkur maqolada biz sun’iy intellektning kiberolamda qanday qilib ham eng katta tahdid, ham eng kuchli qalqon bo‘lib xizmat qilayotganini, xakerlar va himoyachilar o‘rtasidagi ushbu intellektual poyga qayerga yetaklashini tahlil qilamiz.

ASOSIY QISM

Xakerlar LLMlardan dasturiy kodlardagi mantiqiy xatolarni (logic flaws) topishda foydalanmoqda. Inson ko‘zi bilan ko‘rish qiyin bo‘lgan "teshik"lar AI tomonidan soniyalarda skanerlanadi. Himoyachilar esa, aksincha, o‘z dasturlarini yozish jarayonidayoq AI yordamida tekshirib, xavfsiz kod (secure coding) yozishni avtomatlashtirdilar. AI tufayli hatto yuqori texnik bilimga ega bo‘lmagan shaxslar ham murakkab viruslarni yaratish imkoniyatiga ega bo‘ldi. Bu kiberjinoyatchilikning "demokratlashuviga" olib keldi. Kiber-poyga endi shunchaki shaxsiy xakerlar ishi emas.

Kiber-armiyalar: Davlatlar o‘zlarining AI-ga asoslangan kiber-qurollarini yaratmoqdalar. Bu qurollar dushman davlatning energetika tizimi, bank tarmog‘i yoki transport infratuzilmasini bir necha daqiqada falaj qilib qo‘yishi mumkin.

Raqamli suverenitet: Ma’lumotlarni o‘z hududida saqlash va milliy AI mudofaa tizimlarini yaratish davlat xavfsizligining ustuvor yo‘nalishiga aylandi.

Poyganing eng murakkab nuqtasi shundaki, xakerlar endi tizimning o‘zini emas, balki uni himoya qilayotgan **AI modelini** nishonga olmoqda. Ular mudofaa algoritmlarini chalg‘ituvchi "zaharlangan" ma’lumotlarni kiritish orqali AIni ko‘r qilib qo‘yishga urinmoqdalar. Bu esa kiberxavfsizlikni sof texnik sohadan yuqori intellektual strategiyalar maydoniga aylantirdi.

2026-yilda “AI Security Auditor” (AI xavfsizligi auditori) kabi yangi kasblar yuzaga keldi. Ularning vazifasi — kompaniya foydalanayotgan AI modellari xavfsiz ekanligini nazorat qilishdir. Davlatlar o‘zlarining AI-ga asoslangan kiber-qurollarini yaratmoqdalar. Bu qurollar dushman davlatning energetika tizimi, bank tarmog‘i yoki transport infratuzilmasini bir necha daqiqada falaj qilib qo‘yishi mumkin.Bugungi kunda g‘olibni algoritmlarning **tezligi va aniqligi** belgilamoqda. Agar ilgari kiberhujumlar haftalab tayyorlangan bo‘lsa, hozirda SI buni bir necha daqiqada amalga oshirishi mumkin. Himoyachilar esa qarshi turish uchun faqatgina “reaktiv” (hujumdan keyin chora ko‘rish) emas, balki **“proaktiv”** (hujumni kutish va oldini olish) strategiyasiga o‘tishga majbur.

XULOSA

Raqamli texnologiyalar jadal rivojlanayotgan hozirgi davrda kiberhujumlar shakli va ko‘lami tubdan o‘zgarib bormoqda. Sun’iy intellektning bu jarayonga kirib kelishi kiberxavfsizlik sohasida yangi bosqichni boshlab berdi. Endilikda xakerlar hujumlarni avtomatlashtirish, nishonlarni aniq tanlash, tizim zaifliklarini tezkor aniqlash va inson sezmaydigan darajada murakkab usullarni qo‘llash imkoniyatiga ega bo‘lmoqda. Shu bilan birga, himoya tomoni ham sun’iy intellekt yordamida tahdidlarni oldindan bashorat qilish, noodatiy xatti-harakatlarni aniqlash va real vaqt rejimida qarshi choralar ko‘rish imkoniyatlarini kengaytirmoqda.

Bu holat kiber makonda oddiy raqobat emas, balki doimiy intellektual poyga yuzaga kelayotganini ko‘rsatadi. Har bir yangi hujum usuli yangi himoya mexanizmlarini talab qilsa, har bir kuchli himoya tizimi xakerlarni yanada murakkab va moslashuvchan strategiyalar ishlab chiqishga undaydi. Sun’iy intellekt bu poygada asosiy qurolga aylangan bo‘lib, u faqat tezlik va aniqlikni emas, balki

mustaqil o‘rganish va qaror qabul qilish qobiliyatini ham ta’minlamoqda. Natijada kiberxavfsizlik statik himoya choralaridan dinamik va o‘zgaruvchan tizimlarga o‘tmoqda.

Shuningdek, sun’iy intellektdan foydalanish bilan bog‘liq axloqiy va huquqiy masalalar ham tobora dolzarb bo‘lib bormoqda. Avtomatlashtirilgan hujumlar va himoya tizimlari inson nazoratidan chiqib ketmasligi, noto‘g‘ri qarorlar qabul qilmasligi va oddiy foydalanuvchilarga zarar yetkazmasligi muhim ahamiyat kasb etadi. Shu sababli kiberxavfsizlikni ta’minlash faqat texnik mutaxassislar zimmasidagi vazifa bo‘lib qolmay, balki qonunchilar, ta’lim sohasi vakillari va jamiyatning barcha qatlamlari uchun umumiy mas’uliyatga aylanmoqda.

Xulosa qilib aytganda, kiberhujumlarda sun’iy intellektning o‘rni ikki qirrali bo‘lib, u bir vaqtning o‘zida ham tahdid, ham himoya vositasi sifatida namoyon bo‘lmoqda. Bu poygada ustunlik faqat ilg‘or texnologiyalarga emas, balki bilimli kadrlar, to‘g‘ri strategiya va mas’uliyatli yondashuvga bog‘liq. Kelajakda kiber makon xavfsizligi sun’iy intellektning imkoniyatlaridan qanday maqsadda va qay darajada foydalanilishiga qarab belgilanadi.

FOYDALANILGAN ADABIYOTLAR

1.**Stallings, W.** *Network Security Essentials: Applications and Standards.* — Kiberxavfsizlik asoslari va tahdidlar haqida.

2. **Goodfellow, I., Bengio, Y., Courville, A.** *Deep Learning.* — Sun’iy intellekt va mashinaviy o‘rganish asoslari.

3. **Russell, S., Norvig, P.** *Artificial Intelligence: A Modern Approach.* — Sun’iy intellektning umumiy nazariyasi va qo‘llanilishi.

4. **Bishop, M.** *Computer Security: Art and Science.* — Hujum va himoya modellari bo‘yicha ilmiy yondashuv.