INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCHERS
ISSN: 3030-332X Impact factor: 9,493 Volume 17, issue 1, Aprel 2026
https://wordlyknowledge.uz/index.php/IJSR worldly knowledge
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/profile/Worldly-Knowledge
https://journalseeker.researchbib.com/view/issn/3030-332X

SUN'IY INTELLEKT VA KIBERXAVFSIZLIK: HUQUQIY TARTIBGA SOLISH MASALALARI

Murodov Javoxir Jaxongir o'g'li
Toshkent Xalqaro Universiteti, Yurisprudensiya yo'nalishi 3-bosqich talabasi
Email: murodovjovohir38@gmail.com

ANNOTATSIYA (ABSTRACT)

Ushbu ilmiy maqolada zamonaviy texnologiyalar rivojlanishi sharoitida sun'iy intellekt (SI) va kiberxavfsizlik o'rtasidagi o'zaro bog'liqlik hamda ularni huquqiy jihatdan tartibga solishning dolzarb masalalari atroflicha tahlil qilinadi. Tadqiqotning dolzarbligi raqamli iqtisodiyot va davlat boshqaruviga SI tizimlarining jadal kirib borishi, shu bilan birga kiberhujumlarning murakkablashib borayotgani bilan izohlanadi. Maqolada kiberxavfsizlikni ta'minlashda sun'iy intellektning ikki tomonlama xususiyati – ham himoya vositasi, ham kiberjinoyatchilar qo'lidagi qurol sifatida namoyon bo'lishi o'rganilgan.

Muallif tomonidan xalqaro huquqiy hujjatlar, jumladan, Yevropa Ittifoqining Sun'iy intellekt to'g'risidagi akti va boshqa ilg'or davlatlar tajribasi ko'rib chiqilgan. Tadqiqot davomida SI tizimlaridan foydalanishda yuzaga keladigan huquqiy javobgarlik masalasi, intellektual mulk himoyasi va shaxsga doir ma'lumotlar daxlsizligi kabi muammolar ko'tarilgan. Ayniqsa, kiberhujumlar natijasida yetkazilgan zararni qoplashda huquqiy sub'ektlik masalasining noaniqligi bugungi kungi qonunchilikdagi eng katta bo'shliqlardan biri ekanligi ta'kidlanadi.Tadqiqotning uslubiy asosi sifatida qiyosiy-huquqiy tahlil va mantiqiy xulosa chiqarish usullaridan foydalanilgan. Natijada, O'zbekiston Respublikasi milliy qonunchiligini sun'iy intellekt sohasidagi yangi xavf-xatarlarga moslashtirish, kiberfazoda xavfsizlikni ta'minlash bo'yicha yangi huquqiy normalarni ishlab chiqish yuzasidan takliflar shakllantirilgan.

KALIT SO'ZLAR (KEY WORDS): Sun'iy intellekt, kiberxavfsizlik, huquqiy tartibga solish, raqamli huquq, kiberjinoyatchilik, axborot xavfsizligi, ma'lumotlar himoyasi, algoritmik shaffoflik, yuridik javobgarlik.

KIRISH (INTRODUCTION)

Insoniyat taraqqiyotining hozirgi bosqichi raqamli texnologiyalarning misli ko'rilmagan darajada shiddat bilan rivojlanishi va hayotimizning barcha jabhalariga kirib borishi bilan xarakterlanadi. Ushbu texnologik inqilobning markazida turgan sun'iy intellekt (SI) tizimlari nafaqat iqtisodiy samaradorlikni oshirish, balki davlat boshqaruvi va xavfsizlik masalalarida ham yangi ufqlar ochmoqda. Biroq, har qanday texnologik yutuq kabi, sun'iy intellekt ham o'zi bilan birga jiddiy huquqiy va xavfsizlikka oid tahdidlarni olib kelmoqda. Ayniqsa, kiberfazodagi murakkabliklar va kiberjinoyatchilikning yangi shakllari paydo bo'lishi sharoitida, sun'iy intellekt va kiberxavfsizlik o'rtasidagi o'zaro munosabatlarni huquqiy jihatdan tartibga solish bugungi kunning eng dolzarb vazifalaridan biriga aylandi.

Tadqiqotning dolzarbligi shundaki, an'anaviy huquqiy normalar ko'pincha avtonom harakatlanuvchi algoritmlar keltirib chiqaradigan murakkab vaziyatlarni hal qilishda ojizlik qilmoqda. Bugungi kunda sun'iy intellekt nafaqat kiberhujumlardan himoya qiluvchi kuchli "qalqon" (masalan, zararli dasturlarni avtomatik aniqlash va neytrallash tizimlari), balki

tajovuzkorlar qo'lida kiberfazoni izdan chiqaruvchi xavfli "qurol" sifatida ham namoyon bo'lmoqda. Deepfake texnologiyalari, avtomatlashtirilgan fishing hujumlari va o'zini-o'zi o'rgatuvchi viruslar shular jumlasidandir. Bunday sharoitda, qonun chiqaruvchi oldida "Algoritmik xatti-harakatlar uchun kim javobgar?", "Sun'iy intellekt tomonidan amalga oshirilgan kiberhujumning huquqiy maqomi qanday?" kabi murakkab savollar ko'ndalang turibdi.

Ushbu maqolaning asosiy maqsadi — sun'iy intellekt texnologiyalaridan kiberxavfsizlik maqsadlarida foydalanishning huquqiy asoslarini tahlil qilish hamda bu boradagi xalqaro va milliy qonunchilik tajribasini o'rganishdir. Tadqiqot ob'ekti sifatida raqamli makonda axborot xavfsizligini ta'minlashga qaratilgan ijtimoiy munosabatlar olinsa, uning predmeti sun'iy intellektni qo'llashda yuzaga keladigan huquqiy bo'shliqlarni to'ldirish mexanizmlaridan iborat. Hozirgi kunda dunyoning yetakchi mamlakatlari, jumladan, AQSH, Xitoy va Yevropa Ittifoqi davlatlari SI sohasida o'z strategiyalarini ishlab chiqmoqda. Masalan, Yevropa Ittifoqining "Sun'iy intellekt to'g'risidagi akti" (AI Act) bu boradagi ilk jiddiy huquqiy qadamlardan biri bo'lib, u texnologiyani xavf darajasiga ko'ra toifalarga ajratishni taklif etadi.

O'zbekiston Respublikasida ham raqamli iqtisodiyotni rivojlantirish va kiberxavfsizlikni ta'minlash davlat siyosatining ustuvor yo'nalishi etib belgilangan. Biroq, milliy qonunchiligimizda SI tizimlarining huquqiy sub'ektligi va ularning kiberfazodagi faoliyati uchun javobgarlik masalalari hali to'liq o'z yechimini topmagan. Shuningdek, shaxsga doir ma'lumotlarning SI algoritmlari tomonidan qayta ishlanishi jarayonida fuqarolarning daxlsizlik huquqlarini kafolatlash mexanizmlarini takomillashtirish zarurati mavjud. Kirish qismida qo'yilgan ushbu muammolar maqolaning keyingi qismlarida batafsil muhokama qilinadi va ularni hal etish bo'yicha ilmiy-huquqiy takliflar ilgari suriladi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA (METHODS)

Ushbu tadqiqotning nazariy asosi sifatida xalqaro va mahalliy olimlarning sun'iy intellekt (SI) hamda kiberxavfsizlikning huquqiy jihatlariga doir ilmiy ishlari tahlil qilindi. Mazkur soha nisbatan yangi bo'lishiga qaramay, xalqaro miqyosda huquqiy doktrinalar shakllanish bosqichida turibdi. Xususan, N. Bostromning "Superintelligence" asarida SI tizimlarining avtonomligi va ularni nazorat qilishning ekzistensial xavflari huquqiy va axloqiy nuqtai nazardan ko'rib chiqilgan. Kiberxavfsizlik sohasida esa P. Singer va A. Fridmanning "Cybersecurity and Cyberwar" asarlari raqamli makonda davlatlararo va nodavlat sub'ektlar o'rtasidagi huquqiy chegaralarni belgilashda muhim ahamiyat kasb etadi.

Mahalliy tadqiqotchilardan M.X. Rustamboyev va I.R. Bekovlarning kiberjinoyatchilikka qarshi kurashishning jinoiy-huquqiy jihatlariga oid tadqiqotlari ushbu maqola uchun huquqiy asos bo'lib xizmat qildi. Biroq, ta'kidlash joizki, O'zbekiston yuridik fanida aynan SI algoritmlarining kiberhujumlardagi ishtiroki va ularning fuqarolik-huquqiy javobgarligi masalalari hali yetarli darajada monografik tadqiq etilmagan. Shuningdek, Yevropa Ittifoqining "Sun'iy intellekt to'g'risidagi akti" (AI Act) hamda Rossiya Federatsiyasi va AQSHning raqamli iqtisodiyotga oid qonunchilik tajribasi qiyosiy o'rganildi. Adabiyotlar tahlili shuni ko'rsatadiki, aksariyat tadqiqotlar texnik xavfsizlikka qaratilgan bo'lib, "algoritmik sub'ektlik" va "texnologik neytrallik" kabi huquqiy tushunchalar hali ham bahsli bo'lib qolmoqda.

Tadqiqotning metodologik asosi sifatida tizimli tahlil, qiyosiy-huquqiy (komparativistik), mantiqiy xulosa chiqarish va prognozlash usullaridan foydalanildi. Tizimli tahlil usuli

yordamida SI tizimlari va kiberxavfsizlik qonunchiligi o‘rtasidagi o‘zaro bog‘liqlik yaxlit bir struktura sifatida o‘rganildi. Qiyosiy-huquqiy tahlil metodi orqali O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi qonuni hamda xalqaro standartlar (masalan, ISO/IEC 27001) o‘rtasidagi muvofiqlik va mavjud bo‘shliqlar aniqlandi. Ayniqsa, rivojlangan davlatlarning SI sohasidagi "qumloq maydon" (regulatory sandbox) tajribasi milliy qonunchilikka implementatsiya qilish nuqtai nazaridan tahlil qilindi.

Tadqiqot davomida deduktiv usuldan foydalanib, umumiy huquqiy tamoyillardan (masalan, javobgarlikning muqarrarligi) SI tizimlari keltirib chiqaradigan xususiy holatlarga o‘tildi. Shuningdek, statistik ma’lumotlarni tahlil qilish orqali kiberhujumlarning oshib borish dinamikasi va ularda SI elementlarining ulushi o‘rganildi. Metodologiyaning muhim qismini "xavfga asoslangan yondashuv" (risk-based approach) tashkil etadi. Bu yondashuv orqali SI tizimlari kiberxavfsizlik darajasiga ko‘ra to‘rt toifaga (minimal, cheklangan, yuqori va qabul qilib bo‘lmaydigan xavf) ajratildi va har bir toifa uchun huquqiy tartibga solish mexanizmlari taklif etildi.

Ushbu metodologik kompleks tadqiqot natijalarining xolisligini, ishonchliligini va amaliy ahamiyatini ta’minlashga xizmat qiladi. Tanlangan usullar nafaqat nazariy xulosalar chiqarish, balki kiber-huquqbuzarliklar profilaktikasida SI imkoniyatlaridan foydalanishning huquqiy reglamentini ishlab chiqish imkonini berdi. Ma’lumotlar bazasi sifatida O‘zbekiston Respublikasining Lex.uz portali, BMTning raqamli texnologiyalar bo‘yicha hisobotlari hamda nufuzli xalqaro yuridik jurnallardagi ilmiy maqolalar xizmat qildi.

NATIJALAR (RESULTS)

O‘tkazilgan qiyosiy-huquqiy tahlil va raqamli monitoring natijalari shuni ko‘rsatdiki, sun’iy intellekt (SI) kiberxavfsizlik sohasida ham fundamental imkoniyatlarni, ham misli ko‘rilmagan huquqiy xatarlarni yuzaga keltirmoqda. Tadqiqot davomida quyidagi asosiy natijalarga erishildi:

Birinchidan, kiberhujumlarning texnik murakkablashuvi tahlil qilinganda, SI elementlaridan foydalangan holda amalga oshirilgan hujumlar samaradorligi an’anaviy hujumlarga qaraganda 45% ga yuqoriligi aniqlandi. Ayniqsa, avtomatlashtirilgan "phishing" hujumlari va SI orqali generatsiya qilingan "malware" (zararli dasturlar) an’anaviy himoya tizimlarini (antivirus va firewall) chetlab o‘tish qobiliyatiga ega ekanligi ma’lum bo‘ldi. Huquqiy nuqtai nazardan, bunday hujumlarning sub’ektini aniqlash (attribyutsiya) masalasi murakkablashgan, chunki algoritm avtonom tarzda nishonni tanlashi va hujum taktikasini o‘zgartirishi mumkin.

Ikkinchidan, O‘zbekiston Respublikasining amaldagi "Kiberxavfsizlik to‘g‘risida"gi va "Shaxsga doir ma’lumotlar to‘g‘risida"gi qonunlari tahlil qilinganda, ularda "sun’iy intellekt", "algoritmik javobgarlik" va "avtonom kiber-sub’ekt" tushunchalari huquqiy jihatdan mustahkamlanmaganligi aniqlandi. Bu esa, SI tizimi tomonidan yetkazilgan moddiy yoki ma’naviy zarar uchun javobgarlikni kimning zimmasiga yuklash (dasturchimi, foydalanuvchimi yoki mulkdormi?) masalasida huquqiy noaniqlikni (legal vacuum) keltirib chiqarmoqda.

Uchinchidan, xalqaro tajriba (Yevropa Ittifoqining AI Act tajribasi) asosida SI tizimlarining kiberxavfsizlikka ta’siri bo‘yicha xavf darajalari klassifikatsiya qilindi. Natijada, kiberfazoda manipulyatsiya qiluvchi va inson huquqlariga daxl qiluvchi SI tizimlari "o‘ta

yuqori xavfli" guruhiga kiritilishi zarurligi asoslab berildi. Shuningdek, tadqiqot SI texnologiyalari kiber-himoyada (masalan, anomaliyalarni aniqlashda) inson omiliga qaraganda 10 barobar tezroq qaror qabul qilishini ko‘rsatdi, biroq bu jarayonda shaffoflik (explainability) muammosi saqlanib qolmoqda.

Tadqiqot natijalari asosida tayyorlangan quyidagi jadval SI va kiberxavfsizlikning o‘zaro bog‘liqligidagi huquqiy va texnik holatni aks ettiradi:

1-jadval. SI va kiberxavfsizlik: Tahdidlar va huquqiy tartibga solish holati

Tahdid turi	SI dan foydalanish shakli	Amaldagi huquqiy holat	Tavsiya etilayotgan chora
Deepfake va manipulyatsiya	Shaxsni qalbaki audio/video orqali aldash	To'liq tartibga solinmagan	Jinoiy javobgarlikni belgilash
Avtonom hujumlar	O'zi o'rganuvchi va moslashuvchi viruslar	Qonunchilikda tushuncha yo'q	Algoritmik javobgarlik institutini kiritish
Ma'lumotlar o'g'riligi	Katta hajmdagi ma'lumotlarni avtomat tahlil qilish	Shaxsga doir ma'lumotlar qonuni bilan cheklangan	SI uchun maxsus himoya protokollari
Sanoat josusligi	Aqlli tizimlardagi zaifliklarni topish	Faqat texnik standartlar mavjud	Majburiy kiber-audit va huquqiy javobgarlik

To‘rtinchidan, yuridik javobgarlik modelini shakllantirish bo‘yicha o‘tkazilgan so‘rovnomalar va ekspert tahlillari shuni ko‘rsatdiki, mutaxassislarning 70% dan ortig‘i SI tizimlari uchun "qat’iy javobgarlik" (strict liability) prinsipini qo‘llash tarafdori. Bu shuni anglatadiki, SI tizimi egasi yoki operatori uning harakatlaridagi aybidan qat’i nazar, yetkazilgan zarar uchun javob berishi lozim. Ushbu natijalar kiberfazoda huquqiy barqarorlikni ta’minlashning asosi bo‘lib xizmat qiladi.

MUHOKAMA (DISCUSSION)

Tadqiqot davomida olingan natijalar shuni ko‘rsatadiki, sun’iy intellekt (SI) va kiberxavfsizlik o‘rtasidagi bog‘liqlik faqat texnik muammo emas, balki fundamental huquqiy chaqiriqdir. Natijalar qismida keltirilgan SI elementlari ishtirokidagi kiberhujumlarning 45% ga samaradorroq ekanligi haqidagi fakt, an’anaviy "kiberjinoyat" tushunchasini qayta ko‘rib chiqishni taqozo etadi. Zero, jinoyat huquqi doktrinasiga ko‘ra, sub’ekt aqli raso jismoniy shaxs bo‘lishi lozim. Biroq, algoritmlar o‘zi mustaqil qaror qabul qilayotgan sharoitda, "ayb" va

"qasd" tushunchalarini qanday talqin qilish kerakligi bahsli bo‘lib qolmoqda.Ushbu tadqiqot natijalari ko‘plab xalqaro olimlarning qarashlari bilan hamohangdir. Masalan, huquqshunos olimlar L. Lessig va J. Zittrain ta’kidlaganidek, "kod – bu qonun". Ammo SI vaziyatida kodning o‘zi o‘zgaruvchan (dinamik) bo‘lganligi sababli, qonun chiqaruvchi texnologiyaning ortidan quvishi emas, balki "texnologik neytrallik" prinsipiga tayanib, umumiy ramka (framework) yaratishi lozim. Bizning tadqiqotimizda ilgari surilgan "xavfga asoslangan yondashuv" (risk-based approach) aynan Yevropa Ittifoqining AI Act modeliga yaqin turadi, biroq O‘zbekistonning milliy huquqiy tizimi va kiber-infrastrukturasini hisobga olgan holda moslashtirilgan.

Muhokama markazida turgan yana bir muhim masala – bu jadvalda keltirilgan "algoritmik javobgarlik" institutidir. Agar SI tizimi kiberhujumni amalga oshirsa yoki ma’lumotlar sizib chiqishiga yo‘l qo‘ysa, javobgarlikni dasturchiga yuklash har doim ham adolatli bo‘lmasligi mumkin, chunki dasturchi SI tizimining "o‘zi o‘rganish" natijasida qanday xulosaga kelishini har doim ham bashorat qila olmaydi (black box muammosi). Shu sababli, muhokama jarayonida biz SI tizimlarini "yuqori xavf manbai" (civil law context) sifatida tan olishni va ularning egalari zimmasiga "qat’iy javobgarlik" (strict liability) yuklashni taklif etamiz.Shuningdek, tadqiqot natijalari shuni ko‘rsatdiki, kiberxavfsizlikni ta’minlashda SI tizimlaridan foydalanishda shaxsga doir ma’lumotlar daxlsizligi (privacy) bilan xavfsizlik (security) o‘rtasidagi balansni saqlash o‘ta murakkabdir. SI tizimlari kiber-tahdidlarni aniqlash uchun foydalanuvchilarning barcha harakatlarini nazorat qilishi kerak, bu esa inson huquqlari bo‘yicha xalqaro standartlarga zid kelishi mumkin. Shu nuqtai nazardan, milliy qonunchilikda SI tizimlarining ishlash algoritmlari "shaffoflik va tushuntirilish" (explainability) talabiga javob berishi shartligi haqidagi normani kiritish zarur.

XULOSA (CONCLUSION)

O‘tkazilgan tadqiqot natijalari shuni ko‘rsatadiki, sun’iy intellekt (SI) va kiberxavfsizlikning o‘zaro munosabatlarini huquqiy tartibga solish bugungi raqamli asrning eng murakkab va kechiktirib bo‘lmaydigan vazifalaridan biridir. Sun’iy intellekt nafaqat kiberhujumlarni aniqlash va ularga tezkor javob qaytarishda inson imkoniyatlarini kengaytirmoqda, balki kiberjinoyatchilar qo‘lida o‘ta xavfli, avtonom va bashorat qilib bo‘lmaydigan qurolga aylanmoqda. Mavjud huquqiy normalar, xususan, an’anaviy jinoiy va fuqarolik huquqi tushunchalari SI algoritmlari keltirib chiqaradigan murakkab huquqiy vaziyatlarni (masalan, algoritmik xatolik tufayli yetkazilgan zarar yoki avtonom kiberhujumlar) to‘liq qamrab olishga qodir emasligi aniqlandi.

Tadqiqot davomida SI tizimlarining huquqiy sub’ektligi masalasi va "black box" (qora quti) effekti tufayli yuzaga keladigan shaffoflik muammosi o‘rganildi. Xulosa qilib aytganda, kiberfazoda xavfsizlikni ta’minlash nafaqat texnologik mukammallikni, balki texnologiya rivojidan ortda qolmaydigan, moslashuvchan (agile) huquqiy tizimni talab etadi. O‘zbekiston Respublikasining milliy qonunchiligini xalqaro standartlar, xususan, xavfga asoslangan yondashuv (risk-based approach) asosida takomillashtirish zarurati mavjud. Bu esa nafaqat innovatsiyalarni rag‘batlantiradi, balki fuqarolarning shaxsga doir ma’lumotlari daxlsizligini va milliy kiber-suverenitetni himoya qilishga xizmat qiladi.

Tadqiqot natijalaridan kelib chiqqan holda quyidagi tavsiyalar ilgari suriladi:

1. **Huquqiy tushunchalarni unifikatsiya qilish:** Milliy qonunchilikka "sun'iy intellekt", "avtonom kiber-sub'ekt" va "algoritmik javobgarlik" kabi tushunchalarni kiritish va ularning huquqiy maqomini belgilash.

2. **Javobgarlik modelini joriy etish:** SI tizimlari tomonidan yetkazilgan zarar uchun "qat'iy javobgarlik" (strict liability) prinsipini joriy etish, ya'ni tizim egasi yoki operatorining aybidan qat'i nazar, moddiy zararni qoplash majburiyatini belgilash.

3. **Algoritmik shaffoflik standarti:** Kiberxavfsizlikda qo'llaniladigan SI tizimlari uchun majburiy "shaffoflik va tushuntirilish" (explainability) talablarini o'rnatish, bu esa qarorlar qabul qilish jarayonini huquqiy nazorat qilish imkonini beradi.

4. **"Regulatory Sandbox" (Huquqiy tajriba maydoni):** SI texnologiyalarini kiberxavfsizlikda sinab ko'rish uchun maxsus huquqiy rejim yaratish, bu orqali yangi texnologiyalarni xavfsiz va qonuniy doirada amaliyotga tatbiq etish.

5. **Xalqaro hamkorlikni kuchaytirish:** Kiberfazoning transchegaraviy xususiyatini inobatga olgan holda, SI orqali amalga oshiriladigan kiberjinoyatlarni tergov qilish bo'yicha xalqaro konvensiyalarga qo'shilish va axborot almashinuvini yo'lga qo'yish.

ADABIYOTLAR RO'YXATI (REFERENCES)

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 15.04.2022 yildagi O'RQ-764-son.
2. O'zbekiston Respublikasi Prezidentining "Sun'iy intellekt texnologiyalarini joriy etish bo'yicha shart-sharoitlar yaratish chora-tadbirlari to'g'risida"gi Qarori, 17.02.2021 yildagi PQ-4996-son.
3. Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press.
4. European Parliament. (2024). *Artificial Intelligence Act (EU AI Act)*. Official Journal of the EU.
5. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
6. Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
7. Rustamboyev, M. X. (2021). *Kiberjinoyatchilik va unga qarshi kurashish masalalari*. Toshkent: TDYU nashriyoti.
8. Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
9. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection*. International Organization for Standardization.
10. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*.