

LAW • TECHNOLOGY • INNOVATION • JUSTICE

INTERNATIONAL
PEER-REVIEWED
JOURNAL

 JUNE 2026



“UNILEX GLOBAL” LLC

Raqamli huquq va innovatsiya jurnali

Journal of Digital Law and Innovation

June, 2026

VOLUME 1, ISSUE 1



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

CONTENTS

03

**XUDOYBERDIYEV XUMOYUNBEK XABIBULLA O'G'LI,
QURVONBOYEV ASLBEK AZIZJON O'G'LI**

KIBERXAVFSIZLIKNING KONSTITUTSIYAVIY ASOSLARI
VA MILLIY XAVFSIZLIKKA TA'SIRI

13

SATTAROV ULUG'BEK UMED O'G'LI

RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIK
MUAMMOLARI: ZAMONAVIY XAVFLAR VA BARQAROR
RIVOJLANISH YONDASHUVLARI

20

MANNABJONOVA DURDONA ABDUXALIL QIZI

DAVLAT IDORALARIDA SUN'IY INTELLEKTDAN
FOYDALANISHNI HUQUQIY TARTIBGA SOLISH

34

HUSANOVA SHABBONA BAHROMOVNA

RAQAMLI MUHITDA INTELLEKTUAL MULK
HUQUQINING MUHOFAZASI

40

RIXSIYEV MUHAMMADAZIZ MUZAFFAR O'G'LI

O'ZBEKISTON RESPUBLIKASIDA
KIBERJINOYATCHILIKKA QARSHI KURASHISHNING
KONSITUTSIYAVIY-HUQUQIY VA XALQARO-
HUQUQIY ASOSLARI

54

BOYMIRZAYEVA MADINA IBROHIM QIZI

SUN'IY INTELLEKTNING HUQUQ TIZIMLARI VA ODIL
SUDLOV FAOLIYATIGA TA'SIRI



KIBERXAVFSIZLIKNING KONSTITUTSIYAVIY ASOSLARI VA MILLIY XAVFSIZLIKKA TA'SIRI

Xudoyberdiyev Xumoyunbek Xabibulla o'g'li¹, Qurvonboyev Aslbek Azizjon o'g'li²

¹“TIQXMMI” Milliy tadqiqot universiteti Yurisprudensiya
yo'nalishi 4-kurs talabasi

²“TIQXMMI” Milliy tadqiqot universiteti Yurisprudensiya
yo'nalishi 4-kurs talabasi

MAQOLA MA'LUMOTI

Kalit so'zlar:

Kiberxavfsizlik,
kiberhuquq,
kiberjinoyat,
konstitutsiyaviy asos,
modda,
raqamli tahdid,
javobgarlik

ANNOTATSIYA

Mazkur maqolada axborot texnologiyalari rivojlanishi sharoitida yangi kibermakondagi munosabatlarni huquqiy tartibga solish, xususan, kiberxavfsizlik masalalari ko'rib chiqiladi. Shuningdek, maqolada kiberxavfsizlikni ta'minlashga qaratilgan me'yoriyhuquqiy hujjatlar, huquqbuzarliklar uchun javobgarlik asoslari va kiberjinoyatlarga qarshi kurash mexanizmlari atroflicha tahlil qilinib, ushbu sohaning O'zbekiston Respublikasi milliy xavfsizligini ta'minlashdagi strategik ahamiyati yoritiladi.

CONSTITUTIONAL FOUNDATIONS OF CYBERSECURITY AND ITS IMPACT ON NATIONAL SECURITY

ARTICLE INFO

Keywords:

Cybersecurity,
cyber law,
cybercrime,
constitutional basis,
article,
digital threat,
responsibility

ABSTRACT

This article examines the legal regulation of relations in the new cyberspace in the context of the development of information technologies, in particular, issues of cybersecurity. The article also analyzes in detail the regulatory legal acts aimed at ensuring cybersecurity, the grounds for liability for offenses, and the mechanisms for combating cybercrime, highlighting the strategic importance of this area in ensuring the national security of the Republic of Uzbekistan.

КОНСТИТУЦИОННЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И ЕЁ ВЛИЯНИЕ НА НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

Кибербезопасность,
киберправо,
киберпреступность,
конституционная основа,
статья,
цифровая угроза,
ответственность

АННОТАЦИЯ

В данной статье рассматривается правовое регулирование отношений в новом киберпространстве в условиях развития информационных технологий, в частности, вопросы кибербезопасности. Также в статье подробно анализируются нормативно-правовые акты, направленные на обеспечение кибербезопасности, основы ответственности за правонарушения и механизмы борьбы с киберпреступлениями, освещается стратегическое значение данной сферы в обеспечении национальной безопасности Республики Узбекистан.

KIRISH

Axborot texnologiyalarining, jumladan, Internet tarmog'ining keng tarqalishi, sun'iy intellektning paydo bo'lishi va takomillashuvi natijasida yangi kiber makon shakllandi. Bu esa mazkur munosabatlarni har taraflama huquqiy tartibga solish zaruratini yuzaga keltirmoqda. Qolaversa, axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, jamiyat faoliyatining keng sohalarida turli kompyuter texnologiyalar bilan ta'minlanadigan axborot xizmatlarining joriy qilinishiga olib keldi. Bu o'z navbatda yangi kiber huquq sohasining paydo bo'lishiga turtki bo'ldi. Kiber huquq axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solishga hamda himoya qilishga qaratilgan huquq sohasidir. [1]

Kiber huquqning shakllanishi va rivojlanishi, o'z navbatida, virtual makonda yuzaga keladigan xavf-xatarlarni chuqur o'rganish hamda ularni bartaraf etish mexanizmlarini takomillashtirish zaruratini keltirib chiqardi. Shu bois, kiber huquq bilan chambarchas bog'liq bo'lgan kiberxavfsizlik masalalari alohida dolzarblik kasb etib, ularning huquqiy asoslarini o'rganish keyingi muhim yo'nalishga aylandi.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo'lib, unga berilgan turlicha ta'riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta'rif berilgan: kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni to'g'ri bajarilishini kafolatlash uchun

o'zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. [2] U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o'z ichiga oladi. Kiberxavfsizlik ta'limning mujassamlashtirilgan bilim sohasi bo'lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o'z ichiga oladi. Tarmoqlar sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta'rif bergan [3]: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo'q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar soni va turlarining kattaligi va buzg'unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.

Kiberxavfsizlikni ta'minlash har qanday mamlakat uchun muhim bo'lgan davlat vazifasi hisoblanadi. Shu sababli, bu sohadagi yagona davlat siyosati O'zbekiston Respublikasi Prezidenti tomonidan belgilanadi. Mamlakatning strategik rivojlanish dasturlarida, jumladan, 2017–2021 yillarda O'zbekiston Respublikasini yanada rivojlantirish bo'yicha Harakatlar strategiyasida [4] ham aniq vazifalar ko'rsatib o'tilgan. Strategiya doirasida "...axborot xavfsizligini ta'minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o'z vaqtida va munosib qarshilik ko'rsatish" kabi choralar bilan birga, kiberjinoyatchilikni fosh etish masalasiga alohida e'tibor qaratilgan." Bundan tashqari, Prezidentning "Ilm, ma'rifat va raqamli iqtisodiyotni rivojlantirish yili"ga oid Davlat dasturi to'g'risida"gi Farmonida "2020-yil 1-sentyabrga qadar kiberxavfsizlikka doir milliy strategiya va qonun loyihasini ishlab chiqish" kabi vazifalar belgilangan bo'lib, ularni amalga oshirishda o'quv qo'llanmalarini ishlab chiqishga e'tibor qaratish muhim ahamiyatga ega. [5]

O'zbekistonda kiberxavfsizlik davlat tomonidan ta'minlanadi. Xususan, kiberxavfsizlik quyidagilar orqali ta'minlanadi:

- kiberxavfsizlikka tahdidlarga qarshi turish uchun iqtisodiy, siyosiy, tashkiliy va boshqa xarakterdagi tadbirlarni amalga oshirish;
- O'zbekiston Respublikasining jahon axborot makoniga va zamonaviy telekommunikasiya tizimlariga qo'shilishi;
- konstitutsiyaviy tuzumni zo'ravonlik bilan o'zgartirish, O'zbekiston Respublikasining hududiy yaxlitligini, suverenitetini buzish, hokimiyatni egallab olish yoki hokimiyatdan qonuniy ravishda saylangan yoki tayinlangan hokimiyat vakillarini olib tashlash va davlat

tuzumiga boshqa tajovuzlarni amalga oshirishga qaratilgan da'vatlarni o'z ichiga olgan ma'lumotlarning tarqalishidan himoya qilish;

- ijtimoiy, milliy, irqiy va diniy adovatni qo'zg'atishga qaratilgan urush va zo'ravonlik, shafqasizlik, terrorizm va diniy ekstremizm g'oyalarini targ'ib qiluvchi ma'lumotlarni tarqatishga qarshi kurashish. [6]

Mazkur vazifalarning muhimligi sababli, 2018-yilda Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi (hozirgi Raqamli texnologiyalar vazirligi) tizimida aloqa va axborotlashtirish sohasida nazoratni amalga oshiruvchi maxsus davlat inspeksiyasi tashkil etilgan. [7]

TADQIQOT MATERIALLARI VA METODOLOGIYASI

Kiberxavfsizlikni ta'minlashning konstitutsiyaviy asoslari, birinchi navbatda, shaxsiy axborotning himoyasi va uning uzatilishining asosiy huquqiy prinsiplari orqali belgilanadi. Bu prinsiplar O'zbekiston Respublikasi Konstitutsiyasining 33-moddasida [8] mustahkamlangan bo'lib, unda shaxsiy axborotlarning himoyasi va ulardan foydalanishning qonuniy ta'minoti kafolatlanadi.

Shaxsiy axborot daxlsizligini kiberfazoda ta'minlash, Konstitutsiyamizning boshqa moddalarida ham o'z aksini topgan bo'lib, quyidagi asosiy normalarga tayanadi:

Shaxsiy hayot daxlsizligi va yozishmalar, telefon va telekommunikatsiya xabarlarining sir tutilishi (O'zbekiston Respublikasi Konstitutsiyasining 31-moddasi);

Shaxsiy ma'lumotlarni himoya qilish (O'zbekiston Respublikasi Konstitutsiyasining 33-moddasi);

Axborotga ega bo'lish va uni tarqatish erkinligi (O'zbekiston Respublikasi Konstitutsiyasining 33-moddasi).

Bundan tashqari, kiberxavfsizlikni ta'minlash davlatning keng qamrovli konstitutsiyaviy majburiyatlarini o'z ichiga oladi. Bularga shaxsning huquq va erkinliklarini himoya qilish, davlatning milliy xavfsizlikni ta'minlash majburiyati, axborot kommunikatsiyalarini rivojlantirish, xalqaro shartnomalar qoidalariga rioya qilish hamda iqtisodiy, ijtimoiy va ma'muriy sohalarda axborot tizimlarini tashkil etish va saqlashni ta'minlash kabi kafolatlar kiradi.

O'zbekiston Respublikasida kiberxavfsizlik sohasini huquqiy tartibga solish va ta'minlash bo'yicha keng qamrovli qonunchilik bazasi izchil shakllantirib kelinmoqda. Kiberxavfsizlik

sohasidagi islohotlarning asosiy yo‘nalishlari quyidagi me‘yoriy-huquqiy hujjatlarda belgilab berilgan:

O‘zbekiston Respublikasi Prezidentining 2020-yil 5-noyabrdagi PF-6079-sonli Farmoni [9] bilan tasdiqlangan ushbu Strategiya mamlakatni raqamlashtirishning uzoq muddatli maqsadlarini, shu jumladan kiberxavfsizlikni ta‘minlashning ustuvor yo‘nalishlarini belgilab berdi.

Vazirlar Mahkamasining 2022-yil 21-fevraldagi 80-sonli Qarori [10] bilan “Alohida faoliyat turlarini litsenziyalash bo‘yicha yagona nizom” tasdiqlangan. Bu Nizom kiberxavfsizlik bilan bog‘liq ayrim faoliyat turlarini litsenziyalash orqali sifat va xavfsizlikni nazorat qilishga xizmat qiladi.

Vazirlar Mahkamasining 2022-yil 22-fevraldagi 86-sonli Qarori [11] bilan “Alohida ruxsat etish xususiyatiga ega hujjatlarni berish tartib-taomillari” tasdiqlangan bo‘lib, bu hujjatlar ham kiberxavfsizlik faoliyatining ayrim jihatlarini tartibga solishda muhimdir.

2022-yil 15-aprelda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni [12] sohaning mustahkam huquqiy asosini yaratdi. Bu Qonun Kiberhuquqda axborot xavfsizligini ta‘minlashning asosiy prinsiplari, subyektlari va ularning vakolatlarini, shuningdek, kiberhujumlarning oldini olish va ularga qarshi kurashish mexanizmlarini qamrab oladi.

Ushbu normativ-huquqiy hujjatlar majmuasi O‘zbekistonda kiberxavfsizlikni milliy darajada samarali ta‘minlash, raqamli infratuzilmalarni himoya qilish va fuqarolarning axborot huquqlarini kafolatlash uchun mustahkam asos bo‘lib xizmat qilmoqda.

Shuningdek, 2024-yilda Raqamli texnologiyalar vazirligi kiberxavfsizlik sohasida mutaxassislarni qayta tayyorlash va malakasini oshirish bo‘yicha o‘quv dasturini ishga tushirdi. Dastur kiberxavfsizlik bo‘yicha mutaxassislarning malakasini oshirish, shuningdek, kiberhuquq sohasida yangi mutaxassislarni tayyorlashga qaratilgan.

TADQIQOT NATIJALARI

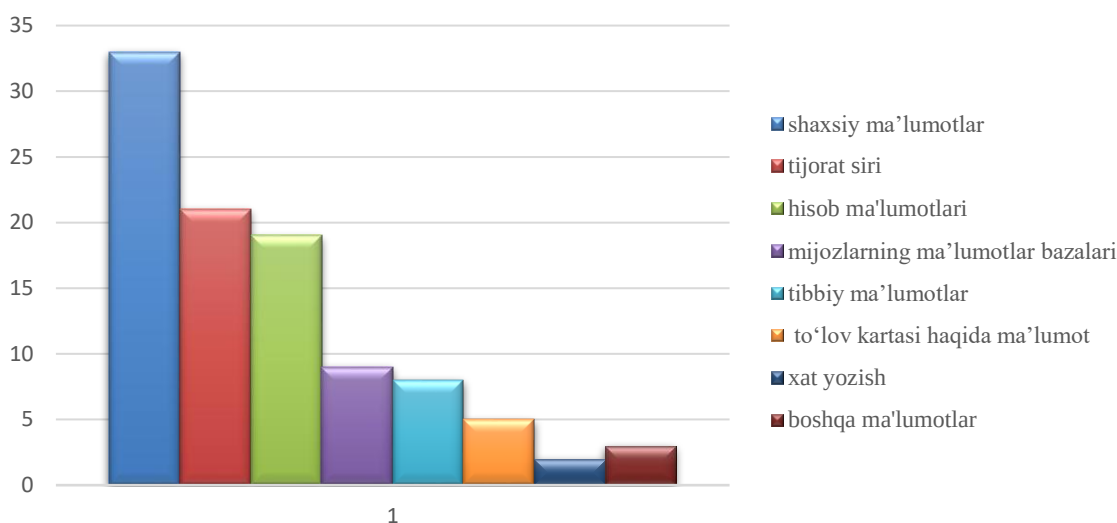
So‘nggi besh yillik tahlillarga ko‘ra, O‘zbekistonda kiberjinoyatlar soni 68 baravarga ko‘payganligi qayd etildi. [13]

Tahlillarga ko‘ra, kiberjinoyatlarning eng keng tarqalgan va xavfli yo‘nalishlari shaxsiy ma‘lumotlar, hisob ma‘lumotlari va bank kartalari bilan bog‘liq o‘g‘rilik va firibgarlik holatlari bo‘lib, bu turdagi jinoyatlar soni keskin oshmoqda. (1-rasm)

Tadqiqot natijalari kiberjinoyatchilikning keskin o‘sganini ko‘rsatadi: 2024-yilda jinoyatlar

soni 2023-yilga nisbatan 9,1 baravarga ko‘paygan. Shu bilan birga, ushbu davrda kibermakondagi huquqbuzarliklar yuzasidan jismoniy va yuridik shaxslardan kelib tushgan murojaatlar soni 34 baravarga ko‘paygan.

Kiberjinoyatchilarning eng keng va ko‘p qo‘llaniladigan turlari



1-rasm. Kiberjinoyatlarning eng ko‘p qo‘llaniladigan turlarining ko‘rsatkichlari (foizda)

Kiberjinoyatlar natijasida O‘zbekiston iqtisodiyotiga yetkazilayotgan moddiy zarar yil sayin keskin oshmoqda. 2021–2024-yillar oralig‘ida fuqarolarning 1 trillion 909 milliard so‘mdan ortiq mablag‘i noqonuniy o‘zlashtirilgan. Faqatgina 2024-yilning o‘zida yetkazilgan zarar 603 milliard so‘mni tashkil etgan.

Kiberjinoyatlarning miqyosi ham jiddiy o‘zgarishlarga uchragan:

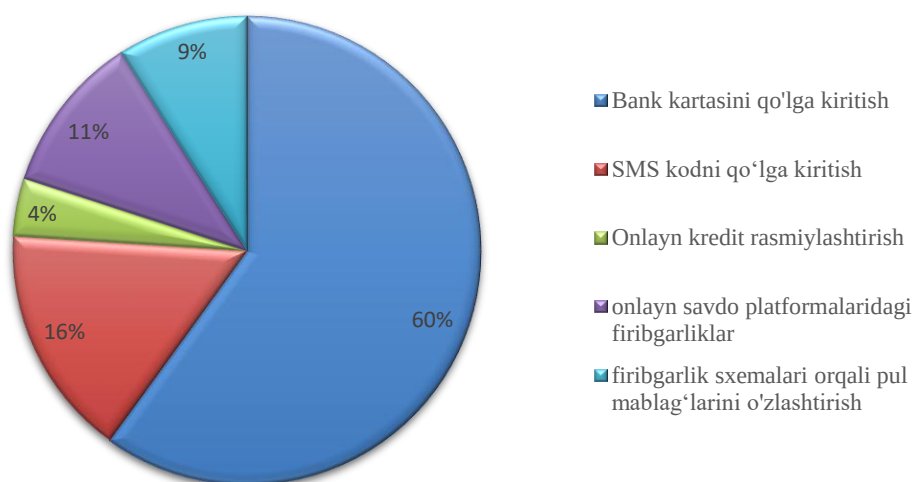
2019-yilda axborot texnologiyalari orqali 18 turdagi 863 ta jinoyat sodir etilgan bo‘lsa, 2024-yilda bu ko‘rsatkich 62 turdagi 58 ming 800 ta jinoyatni tashkil etgan. [14]

Bu o‘rish umumiy jinoyatchilik ulushida yaqqol ko‘rinadi: 2023-yilda 6,2 foizni tashkil etgan kibermakondagi jinoyatlar ulushi 2024-yilda 44,4 foizga yetgan, ya‘ni deyarli har ikkinchi jinoyat axborot texnologiyalari orqali sodir etilgan.

Shuningdek, kibermakondagi jinoyatlar asosiy qismini bank kartalari bilan bog‘liq jinoyatlar (kibero‘g‘rilik va kibermakondagi jinoyatlar) tashkil etmoqda.

Kiberjinoyatlar asosan quyidagi usullarda (2-rasm) kuzatilmoqda:

Kiberjinoyatlar sodir qilinayotgan usullar



2-rasm. Kiberjinoyatlar sodir qilinayotgan usullarning ko'rsatkichlari (foizda), 2025-yil

Bu natijalar shuni ko'rsatadiki, O'zbekiston Respublikasi Konstitutsiyasida kafolatlangan shaxsiy hayot daxlsizligi va shaxsiy ma'lumotlarni himoya qilish huquqlari kiberfazoda katta xavf ostida qolmoqda, bu esa huquqiy va institutsional mexanizmlarni takomillashtirishni talab etadi.

KIBERMAKONDAGI HUQUQBUZARLIKLAR UCHUN JAVOBGARLIK

Kibermakondagi munosabatlarning xavfsizligi, milliy qonunchilik, shuningdek, O'zbekiston Respublikasining amaldagi Jinoyat va Ma'muriy javobgarlik to'g'risidagi qonunchiligi bilan ta'minlanadi. Ushbu qonunlarda axborot texnologiyalari sohasida sodir etilgan huquqbuzarliklar uchun javobgarlik va aniq jazolarni nazarda tutuvchi alohida moddalar keltirilgan.

O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksidagi (MJtK) axborot-kommunikatsiya texnologiyalari sohasiga oid munosabatlarga tahdid soluvchi huquqbuzarliklarning aksariyati quyidagilar bilan bog'liq: axborot tarmog'idan noqonuniy foydalanish, foydalanish qoidalari va standartlarini buzish, shuningdek, taqiqlangan axborotlarni tarqatish.

Xususan, MJtKda axborot xavfsizligiga qarshi quyidagi ma'muriy huquqbuzarliklar nazarda

tutilgan:

Axborotdan foydalanish qoidalarini buzish (155-modda);

Kompyuter tizimidan foydalanish qoidalarini buzish (155¹-modda);

Ommaviy axborot vositalari mahsulotlarini qonunga xilof ravishda tayyorlash va tarqatish (218-modda). [15]

Binobarin, axborot-kommunikatsiya makonida sodir etiladigan ma'muriy huquqbuzarliklar qatoriga, ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog'idan foydalanilgan holda sodir etilgan qilmishlar ham kiradi. Ularga jumladan, MJtKning 189, 189¹, 191-moddalarida ko'zda tutilgan huquqbuzarliklarni keltirish mumkin.

MJtKning 189, 189¹ va 191-moddalarida ko'zda tutilgan huquqbuzarliklar, asosan, pornografiya, qimor, zo'ravonlik g'oyalari, giyohvandlik vositalarini yoki psixotrop moddalarni targ'ib qilish kabi taqiqlangan kontentni tarqatish bilan bog'liqdir. Ushbu qilmishlar fuqarolarning, shu jumladan voyaga yetmagan shaxslarning, hayoti va sog'lig'iga tahdid soluvchi g'ayrihuquqiy harakatlar orqali sodir etiladi. Shuningdek, Internet jahon axborot tarmog'ida noqonuniy kontentni tarqatish uchun MJtKning 276-moddasiga muvofiq javobgarlik belgilangan.

Axborot xavfsizligiga qarshi ma'muriy huquqbuzarliklar uchun qonunchilikda bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoki o'n besh sutkagacha ma'muriy qamoqqa olish kabi og'ir jazo choralari nazarda tutilgan.

Kibermakonda sodir etiladigan huquqbuzarliklar orasida axborot texnologiyalari sohasidagi jinoyatlar eng xavfli hisoblanadi. Shu sababli, kiberjinoyatchilikka qarshi kurashish samaradorligini oshirish maqsadida, O'zbekiston Respublikasi Jinoyat kodeksi (JK) XX¹ bob bilan to'ldirildi. Ushbu yangi bob "Axborot texnologiyalari sohasidagi jinoyatlar" deb nomlanib, 278¹-moddadan 278⁷-moddagacha bo'lgan moddalarni qamrab oladi. [16]

JK 278¹-modda. Axborotlashtirish qoidalarini buzish

JK 278²-modda. Kompyuter axborotidan qonunga xilof ya'ni ruxsatsiz foydalanish

JK 278³-modda. Kompyuter tizimidan, shuningdek telekommunikatsiya tarmoqlaridan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o'tkazish maqsadini ko'zlab tayyorlash yohud o'tkazish va tarqatish

JK 278⁴-modda. Kompyuter axborotni modifikasiyalashtirish

JK 278⁶-modda. Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish.

Mazkur jinoyatlar axborot texnologiyalaridan qonuniy, xavfsiz foydalanishni ta'minlovchi munosabatlarga tajovuz qilinadi. Jinoiy-huquqiy tushunishda kompyuter axboroti axborot texnologiyalari sohasidagi jinoyatlarning predmeti hisoblanadi. Bunday predmetlar Jinoyat kodeksi 278¹, 278², 278⁴ va 278⁶-moddalarining dispozitsiyalarida to'g'ridan-to'g'ri ko'rsatilgan (masalan, axborot tizimi, axborot-hisoblash tizimlari, kompyuter axboroti, kompyuter dasturlari). Yuqoridagi jinoyatlarning xavfliligi ularning sodir etilishi natijasida axborot munosabatlariga jiddiy moddiy va ma'naviy zarar yetkazishi bilan belgilanadi.

MUHOKAMA

Tadqiqot natijalarining umumiy tahlili (kiberjinoyatchilikning 68 baravar o'sishi, jinoyatlarning ko'pchiligi (60%) moliyaviy firibgarlikdan iboratligi va Konstitutsiyaviy-huquqiy asoslarning mavjudligi) shuni ko'rsatadiki, O'zbekistonda kiberxavfsizlik tizimi institutsional va qonunchilik darajasida shakllangan bo'lsa-da, raqamli tahdidlar dinamikasiga tez moslasha olmayapti.

Tadqiqot kiberxavfsizlikni ta'minlash uchun Konstitutsiyaviy asoslar (31 va 33-moddalar orqali shaxsiy hayot daxlsizligi va yozishmalar, telefon va telekommunikatsiya xabarlarining sir tutilishi, shaxsiy ma'lumotlarni himoya qilish) mavjudligini tasdiqladi. Biroq, kibermakondagi tez o'zgaruvchan tahdidlarga javob berish uchun konstitutsiyaviy normalar to'g'ridan-to'g'ri amal qiluvchi mexanizmlar orqali mustahkamlanishi zarur.

Shuningdek, kiberjinoyatlarning 60 foizini bank kartalari bilan bog'liq firibgarlik (kiberfrod) tashkil etishi shuni anglatadiki, amaldagi MJtK moddalari, asosan, axborot tarmoqlaridan noto'g'ri foydalanish va taqiqlangan kontentga qaratilgan. Jinoyatlar soni 68 baravarga, moddiy zarar esa trillion so'mlarga yetgan bir paytda, amaldagi qonunchilik moddiy ziyon keltiruvchi eng katta xavfga nisbatan yetarlicha qaratilmagan yoki ularning qo'llanilish mexanizmlari samarasizdir.

XULOSA

Xulosa o'rnida aytish mumkinki, O'zbekistonda kiberhuquq sohasining huquqiy va institutsional asosi yaratilgan, ammo kiberjinoyatlarning misli ko'rilmagan o'sish sur'ati, ayniqsa moliyaviy firibgarliklar ko'payishi, mavjud mexanizmlarni tezkorlik bilan qayta ko'rib chiqish, profilaktika choralarini kuchaytirish hamda Konstitutsiyada kafolatlangan fuqarolarning axborot huquqlarini kiberfazoda amaliy himoya qilishni ta'minlashni talab etadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Kiber huquq – huquq sohasi sifatida: risola / tuzuvchilar R.R.Shakurov, M.M.Vohidov. – Toshkent: O‘zbekiston Respublikasi Adliya vazirligi qoshidagi Yuristlar malakasini oshirish markazi, 2022. – 27 b.
2. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria (1991) Luxembourg: Office for Official Publications of the European Communities, 1991 ISBN 92-826-3004
3. National Information Systems Security (InfoSec) Glossary (2000) National Security Telecommunications and Information Systems Security Committee. National Security Agency US.
4. “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida” gi O‘zbekiston Respublikasi Prezidentining Farmoni // Qonunchilik ma’lumotlari milliy bazasi. – 07.02.2017. – 4947-son
5. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – T.: «Aloqachi», 2020, 303 bet
6. Kibermaqonda sodir etilayotgan jinoyatlarga qarshi kurash: muammolar va yechimlar: Respublika ilmiy-amaliy konferensiya materiallari to‘plami (2022 yil 24 fevral) / Mas’ul muharrir: A. A. Iminov. – Toshkent: O‘zbekiston Respublikasi IIV Akademiyasi, 2022. – 253 b.
7. “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida” gi O‘zbekiston Respublikasi Prezidentining qarori// Qonunchilik ma’lumotlari milliy bazasi. – 21.11.2018. – 4024-son
8. O‘zbekiston Respublikasi Konstitutsiyasi // Qonunchilik ma’lumotlari milliy bazasi. – 01.05.2023.
9. “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida” gi O‘zbekiston Respublikasi Prezidentining Farmoni // Qonunchilik ma’lumotlari milliy bazasi. – 05.10.2020. – 6079-son
10. Maxsus elektron tizim orqali ayrim faoliyat turlarini litsenziyalash tartibi to‘g‘risidagi yagona nizomni tasdiqlash haqida O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori // Qonunchilik ma’lumotlari milliy bazasi 21.02.2022. – 80-son
11. “Maxsus elektron tizim orqali ruxsat etish xususiyatiga ega ayrim hujjatlarni berish tartib-taomillari to‘g‘risidagi yagona nizomni tasdiqlash haqida // Qonunchilik ma’lumotlari milliy bazasi 22.02.2022. – 86-son
12. “Kiberxavfsizlik to‘g‘risida” gi O‘zbekiston Respublikasi Qonuni // Qonunchilik ma’lumotlari milliy bazasi. 15.04.2022 –764-son
13. O‘zbekistonda kiberjinoyatlar keskin oshdi: Raqamlar va tahlillar. // Gazeta.uz.
<https://www.gazeta.uz/oz/2025/05/29/kiberjinoyat/>
14. O‘zbekiston Respublikasi Ichki ishlar vazirligi. (05.07.2025). Kiberxavfsizlikni ta’minlash choralari va natijalari. O‘zbekiston Respublikasi Hukumati Portali. <https://gov.uz/oz/iiv/news/view/52319>
15. O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi kodeksi // Qonunchilik ma’lumotlari milliy bazasi. 01.04.1995
16. O‘zbekiston Respublikasi Jinoyat Kodeksi // Qonunchilik ma’lumotlari milliy bazasi. 22.09.1994

RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIK MUAMMOLARI: ZAMONAVIY XAVFLAR VA BARQAROR RIVOJLANISH YONDASHUVLARI

Sattarov Ulug'bek Umed o'g'li

“TIQXMMI” Milliy tadqiqot universiteti, “Iqtisodiyot” fakulteti “Buxgalteriya hisobi” ta’lim yo’nalishi 2-kurs talabasi

MAQOLA MA'LUMOTI

Kalit so'zlar:

raqamli iqtisodiyot,
kiberxavfsizlik,
kiberxavflar,
ma'lumotlarni himoya qilish,
raqamli transformatsiya,
axborot tizimlari,
raqamli infratuzilma,
sun'iy intellekt, blokcheyn,
iqtisodiy xavfsizlik.

ANNOTATSIYA

Ushbu maqolada raqamli iqtisodiyotda kiberxavfsizlikni ta'minlashning nazariy asoslari va amaliy muammolari tahlil qilinadi. Raqamli transformatsiya (sun'iy intellekt, blokcheyn, bulutli texnologiyalar) iqtisodiy o'sishni rag'batlantirish bilan bir qatorda, murakkab kiberxavflar, ma'lumotlar sizib chiqishi va to'lov dasturlari (ransomware) bilan bog'liq tahdidlarni ham yuzaga keltirmoqda. Tadqiqot xalqaro boshqaruv va normativ-huquqiy bazalarni o'rganib, infratuzilmasi hamda tajribasi cheklangan rivojlanayotgan davlatlarning zaif jihatlarini ochib beradi. Yakuniy xulosalar kiberxavfsizlikni mustahkamlash barqaror iqtisodiy o'sish va uzoq muddatli barqarorlikning fundamental sharti ekanligini ko'rsatadi.

CYBERSECURITY CHALLENGES IN THE DIGITAL ECONOMY: MODERN RISKS AND SUSTAINABLE DEVELOPMENT APPROACHES

ARTICLE INFO

Keywords:

digital economy,
cybersecurity,
cyber threats, data protection,
digital transformation,
information systems, digital
infrastructure, artificial
intelligence, blockchain,
economic security

ABSTRACT

This article analyzes the theoretical foundations and practical challenges of cybersecurity in the digital economy. While digital transformation (AI, blockchain, cloud computing) drives economic growth, it simultaneously escalates exposure to complex cyber threats, data breaches, and ransomware. Examining international governance and regulatory frameworks, the study highlights the vulnerabilities of developing economies due to limited infrastructure and expertise. The findings conclude that strengthening cybersecurity is a fundamental requirement for sustainable economic growth and long-term resilience

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: СОВРЕМЕННЫЕ РИСКИ И ПОДХОДЫ УСТОЙЧИВОГО РАЗВИТИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

цифровая экономика,
кибербезопасность,
киберугрозы,
защита данных,
цифровая трансформация,
информационные системы,
цифровая инфраструктура,
искусственный интеллект,
блокчейн, экономическая
безопасность.

АННОТАЦИЯ

В данной статье анализируются теоретические основы и практические проблемы обеспечения кибербезопасности в цифровой экономике. В то время как цифровая трансформация (искусственный интеллект, блокчейн, облачные вычисления) стимулирует экономический рост, она одновременно увеличивает уязвимость перед комплексными киберугрозами, утечками данных и программами-вымогателями. Исследуя международные подходы к управлению и нормативно-правовую базу, авторы выделяют уязвимости развивающихся стран, обусловленные ограниченной инфраструктурой и нехваткой опыта. Результаты исследования подтверждают, что укрепление систем кибербезопасности является фундаментальным условием для устойчивого экономического роста и долгосрочной стабильности.

INTRODUCTION

The development of the digital economy represents one of the most significant transformations in modern global economic systems. Over the past two decades, traditional economic structures have gradually shifted toward digital platforms where goods, services, and financial transactions are conducted electronically. This transformation has been driven by rapid technological advancements in information and communication technologies, including internet expansion, mobile technologies, cloud computing, and artificial intelligence systems [1].

The digital economy has significantly improved productivity, reduced transaction costs, and increased access to global markets. Businesses are now able to operate across borders with minimal physical infrastructure, while consumers benefit from faster and more efficient services. Governments have also adopted digital technologies to improve public service delivery through e-government systems and digital identification platforms.

However, alongside these advantages, the digital transformation process has introduced new risks that were not present in traditional economic systems. The increasing reliance on interconnected digital networks has created new vulnerabilities that can be exploited by cybercriminals. As a result, cybersecurity has become a fundamental requirement for ensuring the stability and sustainability of modern economies.

Cybersecurity refers to the protection of computer systems, networks, programs, and data from unauthorized access, attacks, damage, or disruption. It is no longer limited to technical protection but has evolved into a strategic component of national economic security and global stability [2].

In recent years, cyberattacks have become more sophisticated, organized, and financially motivated. Criminal groups and even state-sponsored actors are increasingly targeting critical infrastructure, financial systems, healthcare institutions, and government databases. These attacks can lead to severe financial losses, disruption of essential services, and loss of public trust in digital systems.

The importance of cybersecurity is particularly high in the context of the digital economy, where data is considered one of the most valuable economic assets. The loss or manipulation of data can have significant consequences for businesses and governments, affecting decision-making processes, operational efficiency, and strategic planning.

In developing countries, including Uzbekistan, the digital transformation process is progressing rapidly. The introduction of e-government services, digital banking systems, and electronic payment platforms has significantly improved economic efficiency and accessibility. However, the rapid expansion of digital infrastructure without sufficient cybersecurity readiness increases exposure to cyber threats [3].

Therefore, analyzing cybersecurity challenges in the digital economy is essential for developing effective protection strategies and ensuring sustainable economic development.

METHODOLOGY

The research methodology of this study is based on a systematic and comparative approach aimed at analyzing cybersecurity challenges within the digital economy framework. The study combines qualitative analysis, comparative international review, and interpretation of statistical data from global cybersecurity reports.

Firstly, the theoretical foundation of the digital economy and cybersecurity was examined through academic literature, policy documents, and international reports published by organizations such as the World Bank, International Telecommunication Union (ITU), and the Organization for Economic Cooperation and Development (OECD) [4]. These sources provided a comprehensive understanding of global cybersecurity trends and digital transformation dynamics.

Secondly, a comparative analysis was conducted between developed and developing countries to evaluate differences in cybersecurity maturity levels. Countries such as the United States, Germany, South Korea, Japan, and Singapore were used as benchmarks for advanced cybersecurity systems. Their approaches were compared with those of emerging economies to identify structural weaknesses and institutional gaps.

Thirdly, national strategies and regulatory frameworks were analyzed, with particular focus on digital transformation policies and cybersecurity development programs. This included examining legal frameworks, institutional responsibilities, and national cybersecurity strategies.

The study also utilized key analytical indicators, including the frequency of cyber incidents, financial losses caused by cybercrime, investment levels in cybersecurity infrastructure, and human capital development in the cybersecurity sector. These indicators were used to evaluate the effectiveness of cybersecurity systems in different economic environments.

ANALYSIS AND RESULTS

The digital economy is fundamentally based on the integration of digital technologies into all aspects of economic activity. While this integration provides significant benefits in terms of efficiency, innovation, and accessibility, it also creates new security vulnerabilities.

One of the most significant challenges in the digital economy is the increasing number of cyberattacks targeting both public and private sector organizations. Cybercriminals use a wide range of techniques, including malware, phishing, ransomware, spyware, and distributed denial-of-service (DDoS) attacks, to compromise digital systems.

Financial institutions are among the most frequently targeted sectors due to the high value of financial data and transactions. Online banking systems, digital wallets, and electronic payment platforms are particularly vulnerable to cyber fraud and data breaches. According to international cybersecurity reports, the financial sector experiences billions of dollars in losses annually due to cybercrime [5].

Another critical issue is data security. In the digital economy, data has become a central economic resource. Businesses rely on data analytics to make strategic decisions, optimize operations, and understand consumer behavior. However, unauthorized access to sensitive data can lead to severe consequences, including financial loss, reputational damage, and legal penalties.

Cloud computing technologies have further increased the complexity of cybersecurity. While cloud systems provide scalability and cost efficiency, they also introduce risks related to data storage, access control, and third-party service providers. Ensuring the security of cloud-based systems requires advanced encryption methods and strict access management policies.

Artificial intelligence (AI) has also transformed the cybersecurity landscape. AI-based systems are increasingly used to detect anomalies, identify threats, and respond to cyberattacks in real time. However, cybercriminals are also using AI technologies to develop more sophisticated attack methods, creating an ongoing technological competition between attackers and defenders.

Another important dimension of cybersecurity in the digital economy is the increasing interconnection of critical infrastructure systems. Energy networks, transportation systems, healthcare services, and communication infrastructures are now heavily dependent on digital technologies. While this integration improves efficiency and service delivery, it also creates systemic risks where a single cyberattack can disrupt entire economic and social systems [6]. For example, attacks on energy grids or transportation control systems can lead to large-scale disruptions affecting not only individual organizations but also national economic stability. This phenomenon demonstrates that cybersecurity is no longer limited to protecting individual users or companies; it has become a matter of national security and economic resilience.

Ransomware attacks have become one of the most damaging forms of cybercrime in recent years. In such attacks, malicious software encrypts an organization's data and demands payment for its release. These attacks have targeted hospitals, financial institutions, universities, and government agencies, causing significant operational disruptions. The economic impact of ransomware is increasing annually, with global losses reaching billions of dollars [7].

Phishing attacks also remain a major threat in the digital economy. Cybercriminals use deceptive emails, messages, or websites to trick users into revealing sensitive information such as passwords, bank details, and personal identification data. Despite technological advancements, human error remains one of the weakest links in cybersecurity systems.

Social engineering attacks exploit psychological manipulation rather than technical vulnerabilities. These attacks highlight the importance of human factors in cybersecurity. Even the most advanced technological systems can be compromised if users lack awareness or training in identifying cyber threats.

Another important challenge is the shortage of cybersecurity professionals. The rapid growth of digital technologies has created a high demand for skilled experts in information security, ethical hacking, and network protection. However, many countries face a significant gap between demand and supply of qualified cybersecurity specialists. This shortage weakens the overall resilience of digital systems [8].

Investment in cybersecurity infrastructure is also uneven across countries. Developed economies allocate significant resources to cybersecurity research, advanced monitoring systems, and threat intelligence platforms. In contrast, developing countries often struggle with limited budgets, outdated systems, and insufficient institutional capacity.

DISCUSSION

The findings of this study indicate that cybersecurity is a fundamental pillar of the digital economy. Without effective cybersecurity systems, digital transformation efforts may lead to increased vulnerability rather than sustainable economic growth.

One of the key issues identified is the rapid evolution of cyber threats. Cybercriminals continuously develop new methods to bypass security systems, making it difficult for organizations to maintain long-term protection. This requires constant updates to cybersecurity technologies and policies.

Another major issue is the imbalance between technological development and regulatory frameworks. In many cases, digital technologies evolve faster than legal and institutional systems. As a result, governments struggle to regulate emerging cyber risks effectively. This regulatory gap creates opportunities for cybercriminal activities.

International cooperation plays a crucial role in addressing cybersecurity challenges. Since cyber threats often cross national borders, no single country can effectively combat cybercrime alone. Global collaboration in intelligence sharing, legal enforcement, and technological development is essential for building a secure digital environment [9].

Public awareness is also a critical factor. Many cyber incidents occur due to lack of knowledge among users regarding safe digital practices. Therefore, improving digital literacy and cybersecurity awareness among the population is essential for reducing risks associated with human error.

In the context of developing countries, including Uzbekistan, strengthening cybersecurity requires a multi-dimensional approach. This includes investment in modern digital infrastructure, development of specialized education programs, establishment of cybersecurity institutions, and improvement of legal frameworks.

Furthermore, cooperation between public and private sectors is essential. Private companies often possess advanced technological capabilities and expertise, while governments provide regulatory support and national coordination. A strong partnership between these sectors can significantly improve cybersecurity resilience.

CONCLUSION

This study demonstrates that cybersecurity is an essential requirement for the sustainable development of the digital economy. As economic systems become increasingly digitalized, the importance of protecting information systems, digital assets, and communication networks continues to grow.

Cybersecurity challenges are complex and multidimensional, involving technological, organizational, economic, and human factors. Addressing these challenges requires a comprehensive strategy that includes technological innovation, regulatory development, human capital investment, and international cooperation.

The digital economy offers significant opportunities for economic growth, innovation, and efficiency. However, without strong cybersecurity systems, these benefits may be undermined by increasing cyber threats and vulnerabilities.

Therefore, strengthening cybersecurity infrastructure, improving digital literacy, and developing skilled professionals are essential steps toward ensuring long-term economic stability and sustainable development in the digital era.

REFERENCES

1. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. “Raqamli O‘zbekiston – 2030 strategiyasi”. <https://mitc.uz/>
2. O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi. “Elektron hukumat to‘g‘risidagi normativ-huquqiy hujjatlar”. <https://lex.uz/>
3. O‘zbekiston Respublikasi Prezidenti. PQ-4699-son qaror: Raqamli iqtisodiyot va elektron hukumatni rivojlantirish chora-tadbirlari (2020). <https://lex.uz/docs/4751561>
4. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida” Qonuni. <https://lex.uz/docs/2613718>
5. O‘zbekiston Respublikasi Statistika agentligi. Raqamli iqtisodiyot ko‘rsatkichlari bo‘yicha statistik ma’lumotlar (2025). <https://stat.uz/>
6. Elektron hukumat loyihalarini boshqarish markazi. <https://egov.uz/>
7. World Bank. Uzbekistan Digital Development Overview (2023). <https://www.worldbank.org/en/country/uzbekistan>
8. World Economic Forum. Global Cybersecurity Outlook 2024. <https://www.weforum.org/reports/global-cybersecurity-outlook-2024/>
9. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. <https://www.itu.int/>
10. OECD. Digital Economy Outlook 2020. <https://www.oecd.org/digital/>
11. ENISA. Threat Landscape 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
12. NIST. Cybersecurity Framework (CSF) 2.0 (2024). <https://www.nist.gov/cyberframework>
13. IBM Security. Cost of a Data Breach Report 2024. <https://www.ibm.com/reports/data-breach>
14. United Nations Conference on Trade and Development (UNCTAD). Digital Economy Report 2023. <https://unctad.org/publication/digital-economy-report-2023>

DAVLAT IDORALARIDA SUN'IY INTELLEKTDAN FOYDALANISHNI HUQUQIY TARTIBGA SOLISH

Mannabjonova Durdona Abduxalil qizi

*“Cyber University” davlat universitetining Kiber huquqi
yo‘nalishi magistr talabasi*

MAQOLA MA'LUMOTI

Kalit so‘zlar:

sun'iy intellekt,
davlat boshqaruvi,
huquqiy tartibga solish,
raqamli transformatsiya,
Raqamli O'zbekiston — 2030,
elektron hukumat,
shaxsiy ma'lumotlar himoyasi,
algoritmik shaffoflik.

ANNOTATSIYA

Maqolada O'zbekiston Respublikasida davlat idoralarida sun'iy intellekt (SI) texnologiyalaridan foydalanishni huquqiy tartibga solishning dolzarbligi, mavjud normativ-huquqiy bazasi va rivojlanish yo'nalishlari tahlil qilinadi. SI ning davlat boshqaruvi, elektron hukumat va davlat xizmatlaridagi qo'llanilishi, shaxsiy ma'lumotlar himoyasi, algoritmik shaffoflik va etik masalalar ko'rib chiqiladi. Yevropa Ittifoqi, Fransiya, Estoniya va AQSh tajribasi bilan qiyosiy tahlil o'tkazilib, O'zbekiston uchun xatarlarni minimallashtirish va mas'uliyatli SI tatbiq etish bo'yicha takliflar beriladi.

LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN GOVERNMENT AGENCIES

ARTICLE INFO

Keywords:

artificial intelligence,
public administration,
legal regulation,
digital transformation,
Digital Uzbekistan — 2030,
e-government,
personal data protection,
algorithmic transparency.

ABSTRACT

The article analyzes the relevance, current regulatory framework, and development directions of legal regulation of the use of artificial intelligence (AI) technologies in public administration bodies of the Republic of Uzbekistan. The application of AI in public administration, e-government, and public services is examined, along with issues of personal data protection, algorithmic transparency, and ethics. A comparative analysis is conducted based on the experiences of the European Union, France, Estonia, and the United States, and recommendations are provided for Uzbekistan to minimize risks and ensure the responsible implementation of artificial intelligence.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ГОСУДАРСТВЕННЫХ ОРГАНАХ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

искусственный интеллект,
государственное
управление, правовое
регулирование, цифровая
трансформация, Цифровой
Узбекистан — 2030,
электронное
правительство, защита
персональных данных,
алгоритмическая
прозрачность.

АННОТАЦИЯ

В статье анализируется актуальность, современная нормативно-правовая база и направления развития правового регулирования использования технологий искусственного интеллекта (ИИ) в органах государственного управления Республики Узбекистан. Рассматривается применение ИИ в государственном управлении, электронном правительстве и оказании государственных услуг, а также вопросы защиты персональных данных, алгоритмической прозрачности и этики. Сравнительный анализ проводится с учетом опыта Европейского Союза, Франции, Эстонии и США, а также даются рекомендации для Узбекистана по минимизации рисков и ответственному внедрению искусственного интеллекта.

KIRISH

Insoniyat taraqqiyotining hozirgi bosqichi “To‘rtinchi sanoat inqilobi” (Industry 4.0) sharoitida kechmoqda. Ushbu davrning eng asosiy drayveri — sun‘iy intellekt (SI) texnologiyalaridir. Agar avvalgi o‘n yilliklarda raqamlashtirish jarayonlari shunchaki ma‘lumotlarni qog‘oz shaklidan elektron shaklga o‘tkazish (digitization) bilan cheklangan bo‘lsa, bugungi kunda gap "aqlli boshqaruv" (Smart Governance) haqida bormoqda. Davlat idoralari faoliyatida SI tizimlarining joriy etilishi byurokratiyani kamaytirish, inson omili bilan bog‘liq xatolarni bartaraf etish va qaror qabul qilish tezligini bir necha barobar oshirish imkonini beradi.

Biroq, SI shunchaki texnik vosita emas. U algoritmlar asosida mustaqil xulosalar chiqarish, bashorat qilish va muayyan vaziyatlarda insonning intellektual funksiyalarini almashtirish xususiyatiga ega. Bu esa o‘z-o‘zidan huquqiy tartibga solishning an‘anaviy metodlarini qayta ko‘rib chiqishni talab qiladi. Davlat organi tomonidan SI yordamida qabul qilingan qaror fuqaroning taqdiriga, uning mulkiy yoki ijtimoiy huquqlariga daxl qilsa, ushbu jarayonning huquqiy legitimligi qanday ta‘minlanadi? Mana shu savol bugungi kun yurisprudensiyasining markaziy masalasidir.

Tadqiqotlarga ko‘ra, sun‘iy intellektning iqtisodiy salohiyati nihoyatda katta. Masalan, PwC tomonidan e‘lon qilingan hisobotga ko‘ra, 2030-yilga borib sun‘iy intellektning (AI) jahon iqtisodiyotiga qo‘shadigan hissasi 15,7 trillion AQSh dollariga yetishi kutilmoqda[1]. Amazon, Google, Baidu, Alibaba, Netflix, Facebook, Apple, Microsoft va IBM kabi kompaniyalar

mijozlarga yanada yaxshi xizmat ko'rsatish uchun sun'iy intellektdan foydalanmoqda. Ular mahsulotlar yoki filmlarni tavsiya qilishdan tortib, ovozli yordamchilar (masalan, Amazon Alexa yoki Siri) orqali ham AI texnologiyasini qo'llamoqda. Bundan tashqari, sun'iy intellekt asosida shaxsiylashtirilgan onlayn ta'lim, investitsiya bo'yicha maslahatlar hamda tibbiy diagnostika xizmatlarini taklif qiluvchi ko'plab startaplar paydo bo'lmoqda. Jumladan, Oncora Medical, Babylon Health, Butterfly Network, Atomwise va Enlitic kabi kompaniyalar saraton kasalliklarini tadqiq etish, tibbiy tasvirlarni tahlil qilish va yangi dori vositalarini ishlab chiqish sohalarida faoliyat yuritmoqda[2].

Sun'iy intellektni qo'llashda xususiy sektor yetakchi bo'lib kelayotgan bo'lsa-da, dunyo bo'ylab hukumatlar ham uni jamoat sohasida qo'llash imkoniyatlarini sinab ko'rishni boshladi. Ular fuqarolarga davlat xizmatlarini yanada samarali yetkazib berish uchun AI texnologiyasidan foydalanish yo'llarini izlamoqda. Garchi sun'iy intellektdan foydalanish xususiy va davlat sektorida o'xshash ko'rinsa ham, ularning yondashuvi va oqibatlari o'rtasida muhim farqlar mavjud. Masalan, AI tizimi mahsulot yoki filmni noto'g'ri tavsiya qilsa, bu kompaniya uchun faqat bitta mijozni yo'qotish bilan cheklanadi va zarar, agar bo'lsa ham, tuzatish mumkin. Ammo davlat xizmatlarini ko'rsatishda AI tizimining xatosi qaytarib bo'lmaydigan oqibatlarga olib kelishi mumkin. Masalan, inson asossiz ravishda ishga qabul qilinmasligi, kredit yoki garov (bail) olish huquqidan mahrum bo'lishi mumkin. U noto'g'ri ravishda tartibbuzar yoki jinoyatchi sifatida tasniflanishi, hatto AI tizimi noto'g'ri o'qitilgani sababli aybsiz holda sudlanishi ham mumkin. Bunday xatolarning oqibatlari shaxslar, oilalar va jamiyat uchun juda og'ir bo'lishi mumkin. Hukumat tomonidan joriy etilgan AI tizimlari ehtiyotkorlik bilan sozlanmasa, jamiyatning kam ta'minlangan va himoyaga muhtoj qatlamlarini tizimli ravishda chetlashtirish xavfi mavjud. Masalan, AI tizimi insonlarni ularning teri rangi, irqi, jinsi, tashqi ko'rinishi yoki yashash hududi asosida baholashi va bu omillarni jinoyatchilik yoki tartibbuzarlik bilan bog'lashni "o'rganib olishi" mumkin. Noto'g'ri loyihalashtirilgan AI tizimlari jamiyatdagi tengsizlikni kuchaytirishi va ijtimoiy muvozanatga zarar yetkazishi ehtimoli mavjud [3].

Sun'iy intellekt dasturlarini jamoatchilik uchun joriy etishdan oldin uning muammolarini to'liq tushunmaslik muvaffaqiyatsizlikka olib keladigan eng tez yo'l hisoblanadi. Masalan, qaror qabul qilishdagi tarafkashlik yoki fuqarolar hayotiga maxfiylikka tajovuz qilish holatlari tezda jamoatchilik ishonchining yo'qolishiga sabab bo'ladi va natijada bunday tizimlar bekor qilinishi mumkin. Shuning uchun hukumatlar ushbu muammolarni chuqur tushunib, ularning salbiy ta'sirlarini kamaytirish uchun mos davlat siyosatini ishlab chiqishi juda muhimdir. Shu bilan birga, algoritmlarning shaffofligi masalasi ham dolzarb muammo hisoblanadi. "Black box" fenomeni sababli ayrim hollarda davlat organlari sun'iy intellekt tizimi nima sababdan muayyan qarorni qabul qilganini aniq tushuntirib bera olmasligi mumkin. Bu esa davlat organlari faoliyatining shaffofligi va fuqarolarning axborot olish huquqi tamoyillariga zid

kelishi ehtimolini yuzaga keltiradi. Shu kabi muammolar xalqaro darajada ham muhokama qilinmoqda. Xususan, 2024-yilda Yevropa Ittifoqi tomonidan qabul qilingan EU AI Act sun'iy intellektidan foydalanishni tartibga solishda muhim normativ model sifatida qaralmoqda[4]. Bundan tashqari, UNESCO tomonidan ishlab chiqilgan sun'iy intellekt etikasi bo'yicha tavsiyalar ham davlat boshqaruvida SI texnologiyalaridan mas'uliyatli foydalanishni ta'minlashga qaratilgan [5].

Mazkur maqolaning predmeti davlat organlarida sun'iy intellekt texnologiyalarini joriy etish jarayonida yuzaga keladigan ma'muriy-huquqiy munosabatlarni o'rganishdan iborat. Tadqiqot tuzilmasi mantiqiy ketma-ketlik asosida tashkil etilgan bo'lib, dastlab sun'iy intellektning davlat boshqaruviga ta'siri tahlil qilinadi, so'ngra uning ayrim Yevropa davlatlari —Fransiya, Germaniya, Estoniya hamda AQSH tajribasida qo'llanishi qiyosiy tarzda o'rganiladi. Keyingi qismda O'zbekistonda sun'iy intellektidan foydalanishda shaxsiy ma'lumotlarni himoya qilish, inson huquqlarini ta'minlash hamda texnologiyalardan mas'uliyatli foydalanish tamoyillariga qaratilgan siyosati tahlil qilinadi va yakunda umumiy xulosalar beriladi.

TADQIQOT MATERIALLARI VA METODOLOGIYASI

Avtonom mashinalarning inson hayotidagi rolining ortib borishi davlat siyosati (public policy) uchun yangi va o'ziga xos muammolarni yuzaga keltirmoqda. Dunyo banki hisob-kitoblariga ko'ra, rivojlanayotgan mamlakatlarda mavjud ish o'rinlarining uchdan ikki qismi avtomatlashtirish ta'siriga uchrashi mumkin (World Bank, 2016) [5]. Masalan, Efiopada bu ko'rsatkich hatto 85 foizga yetishi taxmin qilinmoqda. Sog'liqni saqlash, ta'lim, keksalarga g'amxo'rlik qilish hamda transport kabi inson hayotining muhim sohalarida mashinalarning keng tarqalishi amaldagi davlat siyosatini yangilash zaruratini keltirib chiqarmoqda. "Reclaiming Public Space: Drawing Lessons from the Past as We Confront the Future" nomli bobda Chester Newland va Demetrios Argyriades davlat xizmati mutaxassislari oldida turgan kelajakdagi muammolar haqida shunday yozadilar: "Davlat xizmati mutaxassislari uchun yangi profil zarur. Bu soha chuqur bilim va yuqori darajadagi professional ko'nikmalarni matonat, sabr-toqat, halollik, asosli va dalillarga tayanib maslahat berish qobiliyati bilan uyg'unlashtirishi kerak. Eng muhimi esa, u konstitutsiyaviy-demokratik tamoyillar va qadriyatlarga sodiqlikni, oqilona qarorlar qabul qilish hamda inson qadr-qimmatini himoya qilishga intilishni o'zida mujassam etishi lozim." [6]

Aslida mashinalar ilgari ham mavjud bo'lgan, biroq hozirgi vaziyatni tubdan farqlantiradigan jihat shundaki, yangi avlod mashinalari avtonom hisoblanadi. Ularning har biri mustaqil qaror qabul qilish uchun zarur bo'lgan hisoblash quvvatiga ega. Vaziyatni yanada murakkablashtiradigan omil shundaki, sun'iy intellekt asosida ishlovchi mashinalarning qaror qabul qilish jarayoni ko'pincha shaffof emas. Ba'zi hollarda ushbu qaror qanday qabul qilinganini hatto algoritmni yaratgan mualliflar ham to'liq tushuntirib bera olmaydi. Bundan

tashqari, ayrim ommaviy axborot vositalari va jamoatchilik vakillari sun'iy intellekt kelajakda insoniyat ustidan hukmronlik qilishi mumkinligi haqidagi xavotirlarni ham keng tarqatmoqda. [7]

Bunday avtonom mashinalar davlat siyosati sohasiga yangi o'lchamlar olib kiradi va yangi muammolarni yuzaga chiqaradi. Jumladan, sun'iy intellekt bilan jihozlangan tizimlarda axloqiylik (ethics), javobgarlik (responsibility), qarorlarni audit qilish (decision audit) hamda qonuniylik (legality) masalalari dolzarb ahamiyat kasb etadi. Siyosatshunos mutaxassislarning fikriga ko'ra, davlat insonning asosiy huquqlari va jamoat manfaatlariga zid keladigan innovatsiyalarni "filtrlashi", ya'ni ularni cheklashi yoki tartibga solishi zarur[8]. Aynan shu jihatlar sun'iy intellekt va davlat siyosati masalasini ilmiy tadqiqotlar uchun nihoyatda qiziqarli va dolzarb yo'nalishga aylantirmoqda. Sun'iy intellektning strategik ahamiyatini anglagan holda, dunyoning ko'plab hukumatlari SI rivojlanishini milliy ustuvor yo'nalish sifatida e'lon qilgan va bu sohada global yetakchiga aylanish maqsadida katta miqdordagi resurslarni safarbar qilmoqda. Masalan, Xitoy davlat xizmatlarini yaxshilash maqsadida SmartHS tizimini joriy etishni boshlagan [9]. Ispaniya "aqlli shahar" loyihasi doirasida Urban Platform tizimini yaratgan [10]. Dubay hukumati esa fuqarolarga xizmat ko'rsatishda sun'iy intellektdan foydalanadigan "Smart Dubai" loyihasini amalga oshirmoqda [11]. Buyuk Britaniyada Milliy sog'liqni saqlash xizmati (NHS) 2019-yilda sun'iy intellekt asosida ishlaydigan chatbot orqali dastlabki tibbiy saralash tizimini joriy etgan [12]. Shuningdek, AQSH oziq-ovqat va farmatsevtika boshqarmasi sog'liqni saqlash sohasida qo'llanilayotgan sun'iy intellekt algoritmlarini tibbiy qurilmalar sifatida tasniflab, ular uchun maxsus tartibga solish mexanizmini ishlab chiqishni taklif qilgan [13]. Yevropa Ittifoqi esa iste'molchilar uchun mo'ljallangan Online Dispute Resolution (ODR) platformasini yaratib, kelajakda sun'iy intellekt yordamida nizolarni hal qilish imkoniyatlarini rivojlantirmoqda [13].

Davlat boshqaruvida sun'iy intellektdan foydalanish ko'plab afzalliklarni keltirib chiqarishi mumkin, biroq u bilan bog'liq ayrim xavflar ham mavjud. Ushbu ta'sirlar davlat boshqaruvining turli jihatlariga — ma'muriy jarayonlarning samaradorligidan tortib fuqarolarning huquqlarini himoya qilishgacha — ta'sir ko'rsatishi mumkin. Davlat boshqaruvida sun'iy intellektdan foydalanishning asosiy ta'sirlari quyidagilarni o'z ichiga oladi:

- ma'muriy jarayonlar samaradorligini oshirish;
- byurokratiya va inson omili bilan bog'liq xatolarni kamaytirish;
- davlat xizmatlariga kirish imkoniyatini yaxshilash;
- axloqiy va huquqiy muammolarni yuzaga keltirishi;
- shaffoflik va javobgarlik masalalariga ta'siri;
- ijtimoiy himoyaga muhtoj guruhlarining chetlashtirilishi xavfi;
- kiberxavfsizlik muammolari;

- shaxsiy ma'lumotlarni himoya qilish masalalari.[14]

Davlat boshqaruvida sun'iy intellektdan foydalanishning eng muhim afzalliklaridan biri ma'muriy jarayonlar samaradorligining oshishidir. Sun'iy intellekt takrorlanuvchi va katta hajmdagi vazifalarni avtomatlashtirish orqali so'rovlar hamda ma'muriy hujjatlarni ko'rib chiqish uchun zarur bo'lgan vaqtni sezilarli darajada qisqartirishi mumkin. Ma'lumotlarni tahlil qilish va mashinaviy o'rganish kabi texnologiyalarni joriy etish orqali davlat boshqaruvi organlarida ishlovchi xodimlar hisobot tayyorlash, boshqaruvni amalga oshirish va davlat xizmatlarini ko'rsatishda yanada samarali ishlash imkoniyatiga ega bo'ladilar. Natijada fuqarolarning ehtiyojlariga tezroq va aniqroq javob berish imkoniyati yaratiladi.

Shu bilan birga, ushbu texnologiya davlat xizmatlariga kirish imkoniyatini kengaytirish hamda inson omili bilan bog'liq xatolarni kamaytirish uchun muhim imkoniyatlar yaratadi. Biroq tadqiqotchilar shaffoflik yetishmasligi va ijtimoiy himoyaga muhtoj guruhlarining tizimdan chetlashtirilishi xavfi kabi muhim muammolar mavjudligini ham ta'kidlaydilar. Masalan, soliq sohasida sun'iy intellekt soliq yig'imini avtomatlashtirish, soliq deklaratsiyalarini tekshirish va firibgarlik holatlarini aniqlash imkonini beradi. Xuddi shuningdek, sog'liqni saqlash tizimida sun'iy intellekt tibbiy yozuvlarni samaraliroq boshqarishga yordam beradi, bu esa tashxis qo'yish va davolanish uchun kutish vaqtini qisqartiradi. Fiskal sohada esa sun'iy intellekt asosida ishlaydigan avtomatlashtirilgan tizimlar ma'lumotlarni yig'ish va tekshirish jarayonini tubdan o'zgartirishi mumkin. Masalan, Ruminiyada ANAFning raqamli tizimi algoritmlar yordamida soliq deklaratsiyalarini tahlil qilib, real vaqt rejimida anomaliyalarni aniqlaydi va firibgarlik xavfini kamaytiradi. Fuqarolar esa soliq imtiyozlari yoki majburiyatlari bo'yicha savollarga javob beruvchi virtual yordamchilardan foydalanib, uzun navbatlardan qutulish imkoniyatiga ega bo'lmoqda.

MUHOKAMA

Estoniya elektron hukumat tizimi bo'yicha dunyodagi yetakchi davlatlardan biri hisoblanadi. Mamlakatda X-Road platformasi orqali davlat tashkilotlari yagona raqamli tizimga ulangan. Fuqarolar hujjatlarni bir necha bosish orqali olishlari mumkin, Estonian e-Residency dasturi esa butun dunyo bo'ylab tadbirkorlarni jalb qilmoqda va an'anaviy byurokratiyani sezilarli darajada kamaytirgan. Biroq bu muvaffaqiyatlar ayrim muammolarni ham keltirib chiqardi. Tadqiqotlar shuni ko'rsatadiki, texnologiyalarga haddan tashqari tayanish kiberxavfsizlikka oid zaifliklarni yuzaga keltirishi mumkin. Masalan, Germaniyalik tadbirkor Estoniyada o'z mamlakatini tark etmagan holda kompaniya ochishi mumkin. U Estonian e-Residency orqali raqamli identifikatsiya oladi, hujjatlarni onlayn imzolaydi va 48 soat ichida bank xizmatlaridan foydalanish imkoniyatiga ega bo'ladi. Ushbu tizim avtomatik identifikatsiya va firibgarlikka qarshi algoritmlar asosida ishlaydi. 2023-yilda 100 mingdan ortiq chet el fuqarolari ushbu tizimdan foydalangan. Biroq 2021-yilda yuz bergan bir voqea tizimdagi zaifliklarni ko'rsatib

berdi: X-Road platformasidagi xatolik sababli 300 mingga yaqin raqamli sertifikat vaqtincha xavf ostida qolgan[15].

Shuningdek, Denmarkda soliq ma'muriyati sun'iy intellekt yordamida shubhali moliyaviy operatsiyalarni real vaqt rejimida tahlil qilib, soliqdan qochish holatlarini sezilarli darajada kamaytirishga erishdi. Fuqarolar NemID orqali tezkor autentifikatsiya qilinadi. Biroq shaxsiy ma'lumotlarni himoya qilish masalasi hanuz muhim muammo bo'lib qolmoqda. 2024-yilgi hisobotga ko'ra, firibgarlikni aniqlash darajasi 40 foizga oshgan bo'lsa-da, sun'iy intellekt qarorlarining yetarlicha shaffof emasligi jamoatchilik noroziligiga sabab bo'lgan[16].

Finlandiya AuroraAI tizimini ishga tushirdi. Bu tizim sog'liqni saqlashdan tortib ta'limgacha bo'lgan xizmatlarni shaxsiylashtirishga xizmat qiladi. Kasalxonalarda sun'iy intellekt bemorlar uchun zarur bo'lgan o'rinlar yoki dori vositalariga ehtiyojni oldindan prognoz qiladi, natijada kutish vaqti 30 foizga kamaygan. Biroq hammasi ham mukammal emas. 2019-yilda qabul qilingan qonun tibbiy ma'lumotlardan ilmiy tadqiqotlarda foydalanishga ruxsat beradi, bu esa jamiyatda algoritmik kamsitish (bias) yuzaga kelishi mumkinligi haqida xavotirlarni keltirib chiqardi. Shu sababli yanada ko'proq shaffoflik talab qilinmoqda va 2027-yilgacha mo'ljallangan etik sun'iy intellekt strategiyasi ushbu muammolarni hal qilishga qaratilgan[17]. Fransiyada esa sun'iy intellekt soliqdan qochayotgan shaxslarni aniqlash uchun qo'llanilmoqda. Masalan, APASP algoritmi har yili millionlab moliyaviy operatsiyalarni skanerlab, murakkab firibgarlik sxemalarini aniqlaydi. Biroq sog'liqni saqlash tizimini tubdan o'zgartirishi kutilgan Health Data Hub loyihasi fuqarolarning ma'lumotlari xorijiy serverlarda saqlanishiga qarshi noroziliklar sababli vaqtincha to'xtatib qo'yildi. Bu holat shuni ko'rsatadiki, texnologiya samaradorlikni oshirishi mumkin, biroq jamoatchilik ishonchisiz u muvaffaqiyat qozona olmaydi[18]. 2016-yilda qabul qilingan qonun algoritmlar faoliyati shaffof bo'lishini talab qilganiga qaramay, ko'plab institutlar hanuz ularning qanday ishlashini oshkor qilmaydi.

2023-yilda Buxarest shahrida bir bemor mutaxassis shifokor qabuliga yozilish uchun olti oy kutishga majbur bo'lgan. Programäri Online tizimi muvaffaqiyatsiz yangilanish sababli uch hafta davomida ishlamay qolgan. Natijada shifokorlar yana qog'oz hujjatlardan foydalanishga majbur bo'lgan va 15 mingta qabul yozuvlari yo'qolib ketgan. Bu holat shuni ko'rsatadiki, nafaqat sun'iy intellekt dasturlari, balki malakali sun'iy intellekt mutaxassislari ham zarur[19]. Ushbu misollar shuni ko'rsatadiki, davlat boshqaruvida texnologiyadan ko'ra inson omili muhimroq — va garchi sun'iy intellekt katta samaradorlikni ta'minlasa ham, u ba'zi xavflarni keltirib chiqaradi, bu esa tartibga solish va shaffoflikni talab qiladi.

Sun'iy intellekt (SI) ma'muriy jarayonlarni raqamlashtirish orqali byurokratiyani kamaytirishga yordam berishi mumkin. Shu tarzda, davlat xodimi ma'lumotlarni qo'lda qayta ishlamaydi; aksincha, sun'iy intellekt yordamida ma'lumotlar avtomatik tarzda boshqariladi — bu inson xatolarini yo'q qiladi va aniqlikni oshiradi. Ma'muriy qarorlarni avtomatlashtirish

byurokratik jarayonlardan kelib chiqadigan kechikish va murakkabliklarni kamaytiradi. Shu sababli, sun'iy intellektni joriy etish soddaroq va sezilarli darajada samaraliroq ma'muriy tizim yaratishga olib kelishi mumkin.

Davlat boshqaruvida sun'iy intellekt (SI)dan foydalanish bilan bog'liq asosiy xavflardan biri — uning keltirib chiqarishi mumkin bo'lgan axloqiy va huquqiy muammolardir. SI tizimlari, agar avtomatlashtirilgan qarorlar tarixiy ma'lumotlar asosida qabul qilinsa va bu ma'lumotlarda tarfakashliklar yoki stereotiplar mavjud bo'lsa, kamsitishga olib kelishi mumkin. Masalan, davlat krediti uchun moslikni baholashda ishlatiladigan algoritm (algoritm — murakkab jarayonlarni avtomatik bajarilishini ta'minlovchi muhim vosita bo'lib, davlat boshqaruvi, moliya, sog'liqni saqlash va ta'lim kabi sohalarda qo'llaniladi) ayrim ijtimoiy guruhlarni axloqiy yoki huquqiy jihatdan asoslanmagan omillar asosida kamsitishi mumkin. AQShdagi kredit kompaniyalaridagi mashhur misol shuni ko'rsatadiki, ba'zi kredit algoritmlari etnik ozchiliklar, xususan, qora tanli shaxslar bilan bog'liq kamsitishga sabab bo'lgan. Ushbu algoritmlar shaxsning haqiqiy to'lov qobiliyatini to'liq aks ettirmaydigan omillarni tahlil qilgan, ammo kam ta'minlangan jamoalardagi shaxslar uchun salbiy natijalar keltirgan. Boshqa bir misol — yirik korporatsiyalar tomonidan ishlatiladigan ishga qabul algoritmlari bo'lib, ular ayollar yoki etnik ozchiliklar bilan bilvosita kamsitishga sabab bo'lgan. Garchi algoritmlar texnik jihatdan "neytral" bo'lgan bo'lsa-da, tarixiy ma'lumotlar asosida o'qitilgan modellarda tizimli ravishda ayrim ijtimoiy guruhlar ustunlik qozongan. Bunday qarorlar jamiyatdagi mavjud tengsizlik va ijtimoiy tarfakashliklarni yanada kuchaytirishi mumkin. Huquqiy jihatdan bunday amaliyotlar ko'pincha taqiqlangan bo'lib, hokimiyatlar bunday suiiste'molliklarni oldini olish maqsadida SIDan foydalanishni tartibga solishi zarur. Shu sababli SI tizimlari adolat va asosiy huquqlarga hurmat bilan yaratilishi, hamda qasddan yoki tasodifan yuzaga keladigan kamsitishning oldini olish tarzida joriy etilishi kerak. Shuningdek, avtomatlashtirilgan ma'lumotlarni qayta ishlash fuqarolarning asosiy huquqlarini buzish xavfini ham keltirib chiqaradi, agar u shaxsiy ma'lumotlarni himoya qilish me'yorlariga (masalan, GDPR) rioya qilmasa. Shu sababli davlatlar fuqarolarning huquqlarini hurmat qilish va suiiste'molliklarni oldini olish uchun aniq va shaffof kafolatlarni joriy etishi lozim. Salbiy ta'sirlaridan yana biri — zaif guruhlar, masalan, keksalar, nogironligi bo'lgan shaxslar yoki texnologiyaga cheklangan kirish imkoniga ega bo'lgan shaxslar uchun raqamli ajratish xavfi. Bu guruhlar avtomatlashtirilgan tizimlar bilan muloqot qilishda qiyinchiliklarga duch kelishi va davlat xizmatlariga kirish imkoniyati cheklanishi mumkin. Shu sababli davlatlar SI texnologiyalari barcha fuqarolar uchun, ularning texnologik ko'nikmalaridan qat'iy nazar, mavjud va qulay bo'lishini ta'minlash choralari ko'rish kerak, ya'ni foydalanuvchilar uchun qulay platformalarni yaratishi va zaif guruhlar uchun maxsus treninglar tashkil qilishi zarur.

Yana bir muhim vazifa shundaki, SI asosidagi qaror qabul qilish jarayonlariga fuqarolar

tushunadigan qoidalarini joriy etishdir, ular qarorlar qanday qabul qilinganini va qanday ta'sir qilganini aniq tushuntirishi kerak. Aniq tushuntirishning yo'qligi davlat idoralariga bo'lgan ishonchni yo'qotishga va samarali huquqiy himoyani izlash imkoniyatining yo'qligiga olib keladi. Shu nuqtai nazardan, Maria Manuela Barbosa SI tufayli yuzaga kelgan xatolar holatida davlatning fuqarolik javobgarligi tizimini taklif qiladi va qarorlarni avtomatlashtirilgan tizimga topshirish orqali javobgarlikdan qochib bo'lmashligini ta'kidlaydi[20].

Davlat boshqaruvi tizimlarida ko'pincha sun'iy intellekt texnologiyalarini qo'llash uchun moslashtirilmagan eski axborot texnologiyalari infratuzilmasi mavjud. Shu sababli sun'iy intellekt yechimlarini amaldagi ish jarayonlari va ma'lumotlar bazalari bilan integratsiya qilish muhim texnik muammolardan biri hisoblanadi. Bunday jarayonda tizimlar o'rtasidagi moslikni ta'minlash, API integratsiyalarini boshqarish hamda mavjud dasturiy ta'minotni yangilash zarur bo'ladi. Tadqiqotlar texnik integratsiya bilan bog'liq muammolar davlat sektorida sun'iy intellektni joriy etish jarayonini sekinlashtirishi mumkinligini ko'rsatadi. Shu bois middleware texnologiyalaridan foydalanish, mikroxizmatlar arxitekturasini joriy etish hamda eski tizimlarni bosqichma-bosqich modernizatsiya qilish kabi yondashuvlar taklif etilmoqda. Bunda davlat organlarining texnik mutaxassislari va AI yechimlarini ishlab chiquvchilar o'rtasidagi hamkorlik muhim ahamiyatga ega; aks holda, sun'iy intellekt loyihalari faqat tajriba bosqichida qolib ketishi mumkin[21].

Sun'iy intellektning keng joriy etilishi nafaqat texnik, balki huquqiy tartibga solish tizimida ham o'zgarishlarni talab qiladi. Shu sababli ko'plab mamlakatlarda ma'lumotlarni himoya qilish, ma'muriy protseduralar hamda kamsitishga qarshi qonunchilik yangilanmoqda. Masalan, GDPR avtomatlashtirilgan qarorlar bo'yicha shaxslarga tushuntirish olish huquqini belgilaydi, bu esa davlat organlaridan AI asosida qabul qilingan qarorlarning asoslarini fuqarolarga tushuntirib berishni talab etadi. AQSHda esa Algorithmic Accountability Act hamda Blueprint for an AI Bill of Rights kabi tashabbuslar algoritmik tarafdashlik va nazoratsiz kuzatuv kabi xavflarni kamaytirishga qaratilgan[22].

O'zbekiston Respublikasida ham sun'iy intellektni huquqiy tartibga solish borasida muhim qadam qo'yildi. O'zbekiston Respublikasida sun'iy intellekt texnologiyalaridan foydalanishni tartibga solish bo'yicha huquqiy hujjatlardan biri 2026-yil 21-yanvarda O'zbekiston Respublikasining 1115-sonli "Sun'iy intellektni qo'llash orqali yuzaga keladigan munosabatlar tartibga solinishi munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga qo'shimcha va o'zgartirishlar kiritish to'g'risida" qonuni qabul qilindi[23]. Mazkur qonun bilan ayrim qonun hujjatlariga o'zgartirish va qo'shimchalar kiritilib, sun'iy intellekt texnologiyalaridan foydalanishning umumiy huquqiy asoslari belgilandi. Qonunda sun'iy intellekt insonning bilim va ko'nikmalariga taqlid qiluvchi, mustaqil o'rganish, ma'lumotlarni tahlil qilish va muayyan vazifalarni bajarish orqali inson aqliy faoliyatiga o'xshash natijalarni ishlab chiqishga qodir texnologik yechimlar majmui sifatida

ta'riflanadi. Mazkur qonun bir nechta muhim prinsiplarni belgilab berdi. Eng avvalo, insonning huquq va erkinliklariga ta'sir qiluvchi yuridik ahamiyatga ega qarorlar qabul qilish jarayonida faqat sun'iy intellekt tizimlari xulosalariga to'liq tayanish mumkin emasligi qayd etilgan. Bu esa davlat boshqaruvida inson nazorati (human oversight) tamoyilini saqlab qolish zarurligini anglatadi. Bundan tashqari, sun'iy intellekt yordamida shaxsga doir ma'lumotlarga noqonuniy ishlov berish yoki ularni internet tarmoqlarida tarqatish ma'muriy javobgarlikka sabab bo'lishi belgilangan. Bunday holatlar uchun ma'muriy jarima qo'llanilishi va huquqbuzarlik sodir etishda foydalanilgan vositalar musodara qilinishi mumkin.

Yana bir sun'iy intellekt texnologiyalarini rivojlantirish bo'yicha muhim huquqiy asoslardan 358-son "2030-yilga qadar sun'iy intellekt texnologiyalarini rivojlantirish strategiyasini tasdiqlash to'g'risida" prezident qarori hisoblanadi[24]. Ushbu hujjat mamlakatda sun'iy intellekt texnologiyalarini rivojlantirish, ularni iqtisodiyot va davlat boshqaruvi tizimiga joriy etish hamda ilmiy tadqiqotlarni qo'llab-quvvatlashga qaratilgan. Mazkur qaror doirasida bir qator ustuvor yo'nalishlar belgilangan:

- davlat boshqaruvi tizimida sun'iy intellekt texnologiyalarini bosqichma-bosqich joriy etish;
- raqamli iqtisodiyot va innovatsion texnologiyalarni rivojlantirish;
- sun'iy intellekt sohasida ilmiy tadqiqotlar va startap loyihalarni qo'llab-quvvatlash;
- kadrlar tayyorlash va mutaxassislarning raqamli kompetensiyalarini oshirish;
- sun'iy intellekt texnologiyalarini sanoat, tibbiyot, transport va boshqa sohalarda qo'llash.

Shu bilan birga, ushbu qaror davlat organlarida sun'iy intellekt texnologiyalaridan foydalanishda axborot xavfsizligi, ma'lumotlarni himoya qilish hamda algoritmik shaffoflikni ta'minlash masalalariga ham alohida e'tibor qaratadi.

Keyingi O'zbekiston Respublikasining uzoq muddatli rivojlanish yo'nalishlarini belgilab beruvchi asosiy siyosiy hujjatlardan biri O'zbekiston Respublikasining "Mamlakat taraqqiyotining 2030-yilgacha mo'ljallangan ustuvor yo'nalishlari doirasida islohotlarni izchil davom ettirish va yangi bosqichga olib chiqishning qo'shimcha chora-tadbirlari to'g'risida" farmoni hisoblanadi[25]. Mazkur hujjat mamlakatni barqaror rivojlantirish, iqtisodiy o'sishni ta'minlash hamda davlat boshqaruvi tizimini modernizatsiya qilishga qaratilgan kompleks dastur sifatida qabul qilingan.

Sun'iy intellekt (SI) joriy etishning ko'plab afzalliklari mavjud bo'lib, ular ayniqsa ma'muriy jarayonlarni avtomatlashtirish orqali vaqt va resurslarni tejash imkoniyatida namoyon bo'ladi. SI hujjatlarni va fuqarolarning so'rovlarini insonlardan ancha tezroq qayta ishlay oladi, bu esa davlat organlariga murojaatlarga tezroq javob berish, keraksiz bosqichlarni bartaraf etish va byurokratik tartiblarni kamaytirish imkonini beradi. Natijada, fuqarolar davlat boshqaruvi bilan tezroq aloqada bo'la oladi, ofislarga shaxsan kelib so'rov yuborish yoki ma'lumot olishga

ehtiyoj qolmaydi. SI shuningdek, har bir kishi uchun, hatto ilgʻor texnik bilimga ega boʻlmagan shaxslar uchun ham ochiq raqamli platformalarni yaratishga hissa qoʻshishi mumkin. Bundan tashqari, SI ijtimoiy inklyuziv vositasi sifatida ishlatilishi mumkin, masalan, nogironligi boʻlgan shaxslar yoki ijtimoiy jihatdan imkoniyati cheklangan qatlamlar davlat xizmatlariga kirishni osonlashtirishi mumkin — ovozli interfeyslar yoki virtual yordamchilar orqali.

Davlatlar oʻz saʼy-harakatlarini maʼlumotlarni himoya qilish boʻyicha qatʼiy qoidalarni joriy etishga, xalqaro standartlarga (masalan, GDPR) mos keladigan tarzda yoʻnaltirishi, shuningdek, barcha fuqarolar uchun raqamli xizmatlarga kirishni taʼminlashi zarur — jumladan, raqamli taʼlim orqali yoki ilgʻor texnologik koʻnikmalarga ega boʻlmagan shaxslar uchun qoʻllab-quvvatlash bilan. Eng muhimi, davlat organlari avtomatlashtirilgan qarorlar ustidan inson nazoratini saqlashi va ushbu qarorlarni tekshirish mexanizmlarini yaratishi zarur, shunda texnologiya jamoat manfaatiga xizmat qilishi, tengsizlik yoki suiisteʼmolga yoʻl qoʻymasligi taʼminlanadi.

Soʻnggi yillarda xalqaro miqyosda sunʼiy intellektdan foydalanishni tartibga solish boʻyicha muhim huquqiy tashabbuslar shakllanmoqda. Xususan, Yevropa hududida qabul qilingan AI Act sunʼiy intellekt tizimlarining, ayniqsa davlat boshqaruvi kabi “yuqori xavfli” sohalarda qoʻllanishi uchun aniq standartlar va talablarni belgilab beradi. Ushbu huquqiy mexanizm sunʼiy intellekt texnologiyalaridan masʼuliyatli va axloqiy foydalanish uchun muhim asos boʻlib xizmat qiladi. Biroq fundamental huquqlarni real himoya qilish uchun umumiy huquqiy qoidalar milliy va mahalliy darajadagi institutsional hamda maʼmuriy tashabbuslar bilan toʻldirilishi zarur.

Shu nuqtai nazardan, davlat boshqaruvida sunʼiy intellektdan foydalanishni samarali tartibga solish uchun bir qator muhim strategik yoʻnalishlarni amalga oshirish maqsadga muvofiqdir. Avvalo, avtomatlashtirilgan qarorlar ustidan mustaqil nazoratni taʼminlash uchun maxsus Ombudsman institutini tashkil etish muhim ahamiyatga ega. Bunday institut fuqarolar shikoyatlarini koʻrib chiqish, algoritmik qarorlarni qayta tekshirishni talab qilish hamda sunʼiy intellektdan foydalanish jarayonida fuqarolarning huquqlari buzilishining oldini olishga xizmat qilishi mumkin. Bu esa davlat boshqaruvi tizimining shaffofligini oshirish va fuqarolarning raqamli boshqaruvga boʻlgan ishonchini mustahkamlashga yordam beradi.

Shuningdek, davlat organlari tomonidan qoʻllanilayotgan sunʼiy intellekt tizimlari haqida fuqarolarni xabardor qilish maqsadida algoritmik markirovka (labeling) tizimini joriy etish ham muhim ahamiyat kasb etadi. Bunday tizim orqali fuqarolar qaysi jarayonlar avtomatlashtirilganligi, qaror qabul qilishda qanday maʼlumotlardan foydalanilayotgani hamda ushbu qarorlarni qanday tartibda shikoyat qilish mumkinligi haqida aniq va tushunarli maʼlumotga ega boʻladilar. Bu esa algoritmik shaffoflikni taʼminlash va davlat organlarining hisobdorligini oshirishga xizmat qiladi.

Bundan tashqari, davlat boshqaruvining raqamlashtirilishi jarayonida ijtimoiy tenglik

tamoyillarini ta'minlash ham alohida e'tibor talab qiladi. Raqamli xizmatlarning keng joriy etilishi ayrim ijtimoiy guruhlarining davlat xizmatlaridan foydalanish imkoniyatlarini cheklab qo'yishi mumkin. Shu sababli raqamli inklyuziyani ta'minlash maqsadida davlat organlari raqamlashtirish byudjetining ma'lum qismini aholining ijtimoiy himoyaga muhtoj qatlamlarini qo'llab-quvvatlashga yo'naltirishi zarur. Bunga maxsus yordam punktlari tashkil etish, telefon orqali maslahat xizmatlarini yo'lga qo'yish, tushuntiruvchi materiallar tayyorlash hamda fuqarolar uchun bepul raqamli savodxonlik kurslarini tashkil etish kabi chora-tadbirlar kirishi mumkin.

Shu bilan birga, sun'iy intellekt texnologiyalarini davlat boshqaruviga integratsiya qilish jarayonida texnik infratuzilmani modernizatsiya qilish ham muhim ahamiyatga ega. Ko'plab davlat organlarida mavjud bo'lgan eski axborot tizimlari sun'iy intellekt texnologiyalari bilan ishlash uchun yetarli darajada moslashtirilmagan bo'lishi mumkin. Shu sababli davlat boshqaruvi tizimida sun'iy intellektni samarali qo'llash uchun texnik integratsiya jarayonlarini takomillashtirish, mavjud axborot tizimlarini modernizatsiya qilish hamda texnologik infratuzilmani bosqichma-bosqich yangilash zarur.

Umuman olganda, sun'iy intellekt texnologiyalarining davlat boshqaruvi tizimiga joriy etilishi davlat xizmatlarini modernizatsiya qilish va boshqaruv samaradorligini oshirish uchun muhim imkoniyatlar yaratadi. Biroq ushbu jarayon faqat texnologik innovatsiyalar bilan cheklanib qolmasligi, balki huquqiy tartibga solish, etik tamoyillar va fuqarolarning fundamental huquqlarini himoya qilish mexanizmlari bilan uyg'unlashtirilishi zarur.

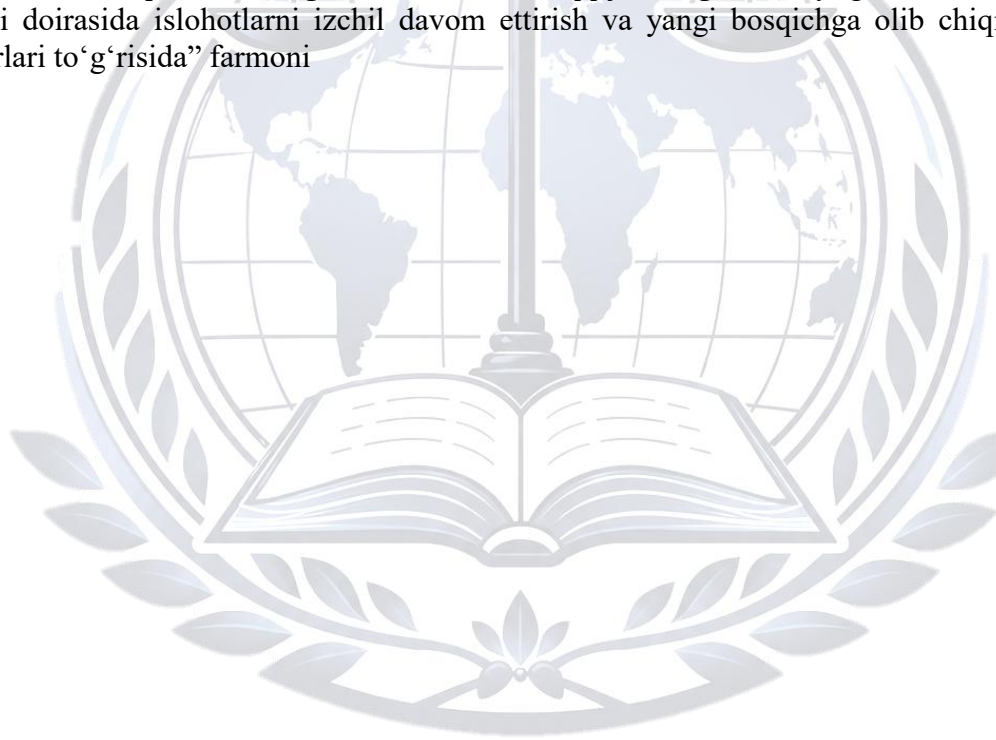
XULOSA

Xulosa qilib aytganda, "aqlli" davlat boshqaruvi faqat raqamlashtirilgan tizim emas, balki texnologiyadan mas'uliyatli foydalanishga asoslangan boshqaruv modelidir. Sun'iy intellekt davlat xizmatlari samaradorligini oshirishga yordam berishi mumkin, biroq u inson tafakkuri va professional baholashni to'liq almashtira olmaydi. Shu sababli muhim va sezgir qarorlar qabul qilish jarayonida inson nazorati saqlanib qolishi lozim. Natijada, sun'iy intellekt davlat boshqaruvida davlat xizmatchilarini to'liq almashtiruvchi vosita emas, balki ularning faoliyatini qo'llab-quvvatlovchi samarali texnologik instrument sifatida qaralishi kerak. Faqat shunday yondashuvgina davlat boshqaruvi samaradorligini oshirish bilan birga fuqarolarning asosiy huquq va erkinliklarini ishonchli himoya qilish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. PWC: Sizing the prize - What's the real value of AI for your business and how can you capitalise ? (2017).
2. 100+ Artificial Intelligence Companies to know in Healthcare|2019. : <https://dhitglobal.org/100-artificial-intelligence-companies-to-know-in-healthcare-2019/>
3. Public Policy and Regulatory Challenges of Artificial Intelligence (AI). HAL Id: hal-03701826 . <https://inria.hal.science/hal-03701826v1/>
4. European Union AI Act : <https://artificialintelligenceact.eu/>
5. UNESCO Ethics of AI : <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
6. Newland, C., Argyriades, D.: Reclaiming Public Space: Drawing Lessons from the Past as We Confront the Future Sustainable Development Goal: <https://www.redalyc.org/journal/5718/571860887003/html/>
7. Anderson, M.L.: Why is AI so scary?
8. Butenko, A., Larouche, P.: Regulation for innovativeness or regulation of innovation ? Law, Innov. Technol. 1–31 (2017).
9. SmartHS: An AI Platform for Improving Government Service Provision: <https://aaai.org/papers/11382-smarths-an-ai-platform-for-improving-government-service-provision/>
10. Spanish Network of Smart Cities: <https://reddeciudadesinteligentes.es/en/>
11. <https://www.digitaldubai.ae/initiatives>
12. Smart Triage: The Foundation for NHS Integrated Care: <https://www.rapidhealth.ai/>
13. USFDA: Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)-Discussion Paper and Request for Feedback. (2019).
14. Mergel, Ines, Helen Dickinson, Jari Stenvall, and Mila Gasco. 2023. "Implementing AI in the Public Sector." Public Management Review, July, 1–14. <https://www.tandfonline.com/doi/full/10.1080/14719037.2023.2231950#references-Section1>
15. Estonia and the world: cyber security 2021 in review. <https://e-estonia.com/estonia-and-the-world-cyber-security-2021-in-review/>
16. Denmark: Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state. <https://www.amnesty.org/en/documents/eur18/8709/2024/en/>
17. Finland - Human-Centric AI Programme. <https://regulations.ai/regulations/RAI-FI-NA-ANAPHXX-2020>
18. French Highest Court Rejects Temporary Suspension of France's Health Data Hub; Calls for Additional Guarantees Following Schrems II. <https://www.hunton.com/privacy-and-cybersecurity-law-blog/french-highest-court-rejects-temporary-suspension-of-frances-health-data-hub-calls-for-additional-guarantees>
19. Digital Transformation of Medical Services in Romania: Does the Healthcare System Meet the Current Needs of Patients?

20. Maria Manuela Barbosa, Responsabilidade civil do Estado pelo recurso a sistemas de inteligência artificial na tomada de decisão, in C. A. Gomes, R. Pedro, T. Serrão (eds.), O regime de responsabilidade civil extracontratual do Estado e demais entidades públicas, AAFDL, Lisabona, 2022, pp. 213–246
21. Tangi L. et al. Barriers and Enablers for Artificial Intelligence in Public Administration // Information Polity. 2023.
22. Blueprint for an AI Bill of Rights. https://data.aclum.org/storage/2025/01/OSTP_whitehouse_gov_ostp_ai-bill-of-rights.pdf
23. O‘zbekiston Respublikasining 1115-sonli “Sun’iy intellektni qo‘llash orqali yuzaga keladigan munosabatlar tartibga solinishi munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga qo‘shimcha va o‘zgartirishlar kiritish to‘g‘risida” qonuni. <https://lex.uz/uz/docs/-8008401>
24. O‘zbekiston Respublikasining 358-sonli “2030-yilga qadar sun’iy intellekt texnologiyalarini rivojlantirish strategiyasini tasdiqlash to‘g‘risida” gi prezident qarori. <https://lex.uz/uz/docs/7158604>
25. O‘zbekiston Respublikasining “Mamlakat taraqqiyotining 2030-yilgacha mo‘ljallangan ustuvor yo‘nalishlari doirasida islohotlarni izchil davom ettirish va yangi bosqichga olib chiqishning qo‘shimcha chora-tadbirlari to‘g‘risida” farmoni



RAQAMLI MUHITDA INTELLEKTUAL MULK HUQUQINING MUHOFAZASI

Husanova Shabbona Bahromovna

“Cyber University” davlat universitetining huquq va biznes fakulteti 1-kurs talabasi

MAQOLA MA'LUMOTI

Kalit so'zlar:

intellektual mulk,
mualliflik huquqi,
raqamli dunyo,
ijtimoiy tarmoqlar,
huquqiy himoya,
patent huquqi,
mualliflik huquqi obyektlari,
blockchain.

ANNOTATSIYA

Ushbu maqolada bugungi kundagi raqamli texnologiyalar va ijtimoiy tarmoqlarda intellektual mulk huquqi tushunchalarining rivojlanishi, uni himoya qilishning huquqiy usullari aks etadi, shuningdek mualliflik huquqi obyekti va mualliflik huquqi obyekti hisoblanmaydigan materiallar, mualliflik huquqining muhofaza belgilari, patentlar va boshqa aqliy mulk obyektlari raqamli muhitda qanday tahdidlarga duch kelayotgani tahlil qilinadi. Tadqiqotda O'zbekiston Respublikasining “Mualliflik huquqi va turdosh huquqlar to'g'risida”gi Qonuni normalarining raqamli muhitdagi amaliy qo'llanilishi nuqtai nazari tasvirlangan.

PROTECTION OF INTELLECTUAL PROPERTY RIGHTS IN THE DIGITAL ENVIRONMENT

ARTICLE INFO

Keywords:

intellectual property,
copyright,
digital world,
social networks,
legal protection,
patent law,
copyright objects,
blockchain.

ABSTRACT

This article reflects the development of the concept of intellectual property rights in today's digital technologies and social networks, legal methods of its protection, as well as analyzes the threats that copyrighted and non-copyrighted materials, copyright protection signs, patents and other intellectual property objects face in the digital environment. The study describes the perspective of the practical application of the norms of the Law of the Republic of Uzbekistan "On Copyright and Related Rights" in the digital environment.

ЗАЩИТА ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В ЦИФРОВОЙ СРЕДЕ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

интеллектуальная
собственность,
авторское право,
цифровой мир,
социальные сети,
правовая защита,
патентное право,
объекты авторского
права, блокчейн.

АННОТАЦИЯ

В данной статье рассматривается развитие концепции прав интеллектуальной собственности в современных цифровых технологиях и социальных сетях, правовые методы их защиты, а также анализируются угрозы, с которыми сталкиваются в цифровой среде материалы, защищенные и не защищенные авторским правом, знаки защиты авторских прав, патенты и другие объекты интеллектуальной собственности. В исследовании описывается перспектива практического применения норм Закона Республики Узбекистан «Об авторском праве и смежных правах» в цифровой среде.

KIRISH

“Intellectual mulk” tushunchasi dastlab 1967-yil 14-iyuldagi “Butunjahon intellektual mulk tashkilotini tashkil etish to‘g‘risida”gi Stokgolm konvensiyasida ilgari surilgan. Mazkur konvensiya intellektual mulkning huquqiy maqomini belgilash bilan birga, uning tarkibi, ya’ni obyektlarini ham aniqladi hamda Butunjahon intellektual mulk tashkiloti (BIMT) faoliyatining tashkiliy-huquqiy asoslarini ko‘rsatib berdi.

Raqamli texnologiyalar, internet va ijtimoiy tarmoqlar tobora o‘sib borayotganligi sababli, intellektual mulkni himoya qilish yanada muhim va murakkab huquqiy masala bo‘lib bormoqda. Hozirgi kunda elektron kitoblar, videolar, ilmiy maqolalar va dasturiy mahsulotlar bir necha soniya ichida millionlab insonlarga yetib borishi mumkin. Bunday qulayliklar mavjud bo‘lsada, noqonuniy nusxa ko‘chirish, ruxsatsiz tarqatish, muallif nomini yashirish va asarlarni o‘zgartirib e‘lon qilish holatlari ham ko‘paymoqda.

Raqamli muhitda mualliflik huquqining buzilishi an’anaviy muhitdagi huquqbuzarliklarga nisbatan ancha murakkab. Ushbu maqolada intellektual mulk huquqlarining asosiy tushunchalari, ularning raqamli muhitda himoya qilish usullari, mavjud muammolar va yechimlar ko‘rib chiqiladi.

TADQIQOT METODOLOGIYASI

Ushbu tadqiqotda intellektual mulk huquqi va u bilan bog‘liq bo‘lgan huquqlarni raqamli dunyoda muhofaza qilish bilan bog‘liq nazariy masalalarni shakllantirib berishda ilmiy bilishning qiyosiy-huquqiy, tizimli, mantiqiy hamda tahlil va sintez usullaridan foydalanildi. Shuningdek, ushbu tadqiqot jarayonida O‘zbekiston Respublikasining intellektual mulk sohasiga bog‘liq amaldagi qonunchiligi, asosan, “Mualliflik huquqi va turdosh huquqlar

to'g'risida"gi Qonun, Fuqarolik kodeksi normalari hamda ushbu sohaga bog'liq ilmiy adabiyotlar hamda xalqaro tajribalar o'rganildi. Shuningdek, ijtimoiy tarmoqlar, video joylash platformalari, sun'iy intellekt tizimlari va blockchain texnologiyalari bilan bog'liq holatlar tahlil qilindi.

TAHLIL VA NATIJALAR

Raqamli dunyodagi asosiy tahdidlar:

Raqamli texnologiyalar mualliflik huquqi egalariga yangi imkoniyatlar yaratgan bo'lsada, bir qator xavflarni ham yuzaga keltiradi.

Birinchi tahdid — kontentning noqonuniy nusxalanishi. Misol uchun, elektron kitoblar yoki ilmiy maqolalar muallifning ruxsatisiz Telegram kanallari yoki har-xil fayl uzatish platformalarida tarqatib yuborish mumkin.

Ikkinchi tahdid — ijtimoiy tarmoqlarda kontentni qayta joylashtirish. Instagram, TikTok yoki YouTube platformalarida muallifga tegishli materiallar uning manbasi ko'rsatilmagan holda qayta e'lon qilinishi ko'p bo'ladi.

Uchinchi tahdid — sun'iy intellekt tizimlari tomonidan yaratilayotgan kontent bilan bog'liq masalalardir. AI modellari millionlab asarlar asosida o'qitiladi. Natijada muallifning rozilgisiz uning ijod mahsulotidan foydalanilgan bo'lishi mumkin.

To'rtinchi tahdid — NFT va blockchain texnologiyalaridan noqonuniy foydalanishdir. Ayrim hollarda boshqa shaxsga tegishli raqamli san'at asari NFT ko'rinishida token ko'rinishida chiqarilib sotilishi kuzatilmoqda.

Beshinchi tahdid — onlayn ta'lim platformalarida mualliflik huquqi bilan himoyalangan materiallardan ruxsatsiz foydalanishdir.

O'zbekiston qonunchiligida raqamli muhofaza mexanizmlari

O'zbekiston Respublikasining "Mualliflik huquqi va turdosh huquqlar to'g'risida"gi Qonuni raqamli dunyoda ko'plab munosabatlarga nisbatan tatbiq etilishi mumkin.

2-modda. Mualliflik huquqi va turdosh huquqlar to'g'risidagi qonunchilik — normada xalqaro shartnomalar ustuvorligini belgilangan. Bu norma internet makonida transchegaraviy huquqbuzarliklarni hal etishda muhim ahamiyat kasb etadi. Agar mualliflik huquqi bilan bog'liq nizoda xalqaro shartnoma qoidalari qo'llanilishi talab etilsa, aynan ushbu modda asos bo'lib xizmat qiladi.

5-modda. Mualliflik huquqi obyekti — raqamli formatdagi videolar, podkastlar, elektron kitoblar va grafik dizaynlar ham ushbu modda doirasida himoya qilinadi.

10-modda. Mualliflik prezumpsiyasi — mualliflik huquqi asar yaratilgan paytdan boshlab vujudga kelishini belgilaydi. Shuning uchun, internetga joylashtirilgan maqola yoki fotografiya uchun alohida ro'yxatdan o'tish talab etilmaydi. Bu raqamli ijodkorlar uchun muhim kafolat

hisoblanadi.

11-modda. Mualliflik huquqining muhofaza belgilari — raqamli platformalarda © belgisi, muallif nomi va yaratilgan yil ko‘rsatilishi mutlaq mualliflik huquqlari egasi ekanligini mustahkamlaydi.

18-modda. Muallifning shaxsiy nomulkiy huquqlari — masalan, blogger yoki ilmiy tadqiqotchi yaratgan material boshqa shaxs tomonidan o‘zgartirib e‘lon qilinsa, ushbu modda asosida huquqiy himoya talab qilinishi mumkin.

19-modda. Muallifning mulkiy huquqlar — ayniqsa, “asarni barchaning e‘tiboriga yetkazish huquqi”, “takrorlash huquqi”, “tarqatish huquqi” internet muhitida eng muhim himoya vositalaridan hisoblanadi. Muallif roziligisiz elektron nusxalarni tarqatish mazkur moddaning buzilishi sifatida baholanishi mumkin.

Asosiy tushunchalar:



1-rasm. Guvohnoma



2-rasm. Patent

Tovar belgilari va xizmat ko‘rsatish belgilari uchun guvohnoma — bu sizning brend nomingiz, logotipingiz yoki xizmatigingiz qonuniy ravishda davlat ro‘yxatidan o‘tganligini tasdiqlovchi rasmiy yuridik hujjatdir. Bu guvohnoma egasiga belgilangan belgidan mutlaq foydalanish va uni boshqalardan himoya qilish huquqini beradi.

Patent — texnik yechim yoki ixtironing davlat tomonidan e‘tirof etilganligini va ixtirochining o‘z ixtirosiga olgan mutlaq huquqini tasdiqlovchi hujjat.

“Patent” havolalar patentlar, mualliflik guvohnomalari, foydalilik to‘g‘risida guvohnomalar,

foydali modellar, qo‘shimcha patentlar yoki qo‘shimcha guvohnomalar, qo‘shimcha mualliflik guvohnomalari va foydalilik to‘g‘risida qo‘shimcha guvohnomalar sifatida tushunilishi kerak (PCT).

Intellectual mulk huquqi — intellektual (aqliy) faoliyat natijasiga tegishli huquq. Intellektual faoliyat natijasiga yoki xususiy alomatlarni aks ettiruvchi vositaga nisbatan mulkiy huquqlar egasiga ana shu intellektual mulk obyektidan o‘z xohishiga ko‘ra har qanday shaklda va har qanday usulda mutlaq qonuniy foydalanish huquqi tegishli bo‘ladi. Huquq egasiga mutlaq huquq asosida tegishli bo‘lgan intellektual mulk obyektlaridan boshqa shaxslarning foydalanishiga faqat huquq egasining ruxsati bilan yo‘l qo‘yiladi (O‘zbekiston Respublikasi FK, 1034-modda).

Muallif — ijodiy mehnati bilan asar yaratgan jismoniy shaxs.

Huquq egasi — mualliflik huquqiga nisbatan muallif yoki uning merosxo‘rlari, turdosh huquqlarga nisbatan ijrochi yoki uning merosxo‘rlari, fonogrammani tayyorlovchi, efir yoki kabel orqali ko‘rsatuv yoxud eshittirish beruvchi tashkilot, shuningdek shartnomaga asosan asarlardan yoxud turdosh huquqlar obyektlaridan foydalanish huquqini olgan boshqa yuridik yoki jismoniy shaxslar.

MUHOKAMA

O‘zbekiston Respublikasi Jahon intellektual mulk tashkilotiga (BIMT) 1991-yilda a‘zo bo‘ldi. Shuningdek, "Mualliflik huquqi va turdosh huquqlar to‘g‘risida"gi qonun raqamli muhitdagi ko‘plab munosabatlarni tartibga solishda zamin yaratmoqda. Qonunda muallifning shaxsiy va mulkiy huquqlari, mualliflik obyekti va muhofaza belgilari kabi institutlar internetda ham qo‘llanilishi mumkin. Biroq sun‘iy intellekt, NFT va blockchain kabi texnologiyalar yangi huquqiy munosabatlar keltirib chiqargani sababli qo‘shimcha normalar zarur.

Bundan tashqari, mualliflik huquqlarini himoya qilish faqat qonunchilik bilan cheklanmasligi kerak. Aholining, xususan yoshlar va kontent yaratuvchilarning huquqiy madaniyatini oshirish — asosan profilaktik chora — muhim ahamiyatga ega. Ta’lim, ommaviy axborot vositalari va platformalar orqali intellektual mulkka hurmat madaniyatini rivojlantirish orqali huquqbuzarliklarni kamaytirish mumkin. Bu kabi yo‘nalishlarda amalga oshiriladigan chora-tadbirlar mualliflar va boshqa huquq egalari manfaatlarini ishonchli himoya qilishga xizmat qiladi.

XULOSA

Raqamli texnologiyalar va ijtimoiy tarmoqlar tufayli endi intellektual mulkni osongina tarqatish mumkin, lekin bu mualliflik huquqining buzilishini ham oshirdi. O‘zbekiston Respublikasining “Mualliflik huquqi va turdosh huquqlar to‘g‘risida”gi Qonuni asosiy huquqiy bazani yaratdi, lekin sun‘iy intellekt, NFT va blockchain kabi yangi texnologiyalar mavjud

qonunchilikni qayta ko'rib chiqishni talab qilishi mumkin. Bunday muammolarni hal qilish bo'yicha asosiy tavsiyalar — Qonunchilikni takomillashtirish: Sun'iy intellekt, NFT va blockchain bilan bog'liq huquqiy bo'shliqlarni topish va ularni tartibga solish uchun qo'shimchalar kiritish yaxshi bo'lardi. Shuningdek, texnologik vositalarni joriy qilish: watermarking, DRM va blockchain asosidagi mualliflik huquqi isboti kabi texnologiyalarni kengroq ishlatish kontentning haqiqiyligini va mualliflik huquqini tasdiqlashga yordam beradi. Ta'lim va xabardorlikni oshirish: intellektual mulk bo'yicha o'quv modullarini ta'lim dasturlariga kiritish va ommaviy axborot vositalari orqali huquqiy madaniyatni rivojlantirish yaxshi bo'lardi. Xalqaro hamkorlikni kuchaytirish: chegaralararo huquqbuzarliklarni kamaytirish maqsadida xalqaro ma'lumot almashinuvi va sud-huquqiy hamkorlikni rivojlantirish foydali.

Umuman olganda, qonunchilikni takomillashtirish, hozirgi texnologiyalarni ishlatish va jamoatchilikni xabardor qilish orqali raqamli dunyoda mualliflar manfaatlarini yanada samarali himoya qilish mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasining Konstitutsiyasi, 2023. <https://lex.uz/docs/-6445145>
2. O'zbekiston Respublikasining Fuqarolik kodeksi, 1996. <https://lex.uz/mact/-111189>
3. Mualliflik huquqi va turdosh huquqlar to'g'risidagi O'zbekiston Respublikasi qonuni O'RQ-42, 2006. <https://lex.uz/ru/docs/-1022944>
4. Butunjahon intellektual mulk tashkilotini ta'sis etish Konvensiyasi, 1991. <https://lex.uz/docs/-2600169>
5. Patent kooperatsiyasi to'g'risidagi shartnoma (PCT), 1991. <https://lex.uz/docs/-2602762>
6. World Intellectual Property Organization. www.wipo.int
7. Electronic Frontier Foundation. <https://www EFF.org/>
8. Harvard Law Review <https://harvardlawreview.org/>
9. WIPO Copyright Treaty (WCT), 2019. <https://lex.uz/docs/4338207>

O‘ZBEKISTON RESPUBLIKASIDA KIBERJINOYATCHILIKKA QARSHI KURASHISHNING KONSITUTSIYAVIY-HUQUQIY VA XALQARO-HUQUQIY ASOSLARI

Rixsiyev Muhammadaziz Muzaffar o‘g‘li

*“TIQXMMI” Milliy tadqiqot universiteti “Ekologiya va
huquq” fakulteti Yurisprudensiya yo‘nalishi 3-kurs talabasi*

MAQOLA MA'LUMOTI

Kalit so‘zlar:

kiberjinoatchilik,
kiberxavfsizlik,
axborot xavfsizligi,
konstitutsiyaviy huquqlar,
shaxsga doir ma'lumotlar,
raqamli texnologiyalar,
xalqaro huquq,
Budapesht konvensiyasi,
axborot makoni,
kiberhujumlar,
milliy qonunchilik,
xalqaro hamkorlik.

ANNOTATSIYA

Mazkur maqolada O‘zbekiston Respublikasida kiberjinoatchilikka qarshi kurashishning konstitutsiyaviy-huquqiy va xalqaro-huquqiy asoslari tahlil qilinadi. Tadqiqotda kiberjinoatchilik tushunchasi, uning zamonaviy ko‘rinishlari hamda jamiyat va davlat xavfsizligiga ta’siri yoritilgan. Shuningdek, O‘zbekiston Respublikasi Konstitutsiyasi, jinoyat va axborot qonunchiligida nazarda tutilgan kiberxavfsizlikni ta’minlash mexanizmlari o‘rganilgan. Maqolada xalqaro-huquqiy normalar, xususan kiberjinoatchilikka qarshi kurashishga qaratilgan xalqaro hujjatlar va xorijiy davlatlar tajribasi tahlil qilinib, milliy qonunchilikni takomillashtirish bo‘yicha ilmiy-amaliy takliflar ishlab chiqilgan. Tadqiqot natijalari kiberxavfsizlikni ta’minlash, fuqarolarning axborot sohasidagi konstitutsiyaviy huquqlarini himoya qilish hamda kiberjinoatchilikka qarshi kurashishning samarali huquqiy mexanizmlarini rivojlantirishga xizmat qiladi.

CONSTITUTIONAL-LEGAL AND INTERNATIONAL-LEGAL FOUNDATIONS FOR COMBATING CYBERCRIME IN THE REPUBLIC OF UZBEKISTAN

ARTICLE INFO

Keywords:

cybercrime, cybersecurity,
information security,
constitutional rights,
personal data,
digital technologies,
international law,
Budapest Convention,

ABSTRACT

This article analyzes the constitutional and international legal foundations of combating cybercrime in the Republic of Uzbekistan. The study examines the concept of cybercrime, its modern forms, and its impact on the security of society and the state. It also explores the mechanisms for ensuring cybersecurity established by the Constitution of the Republic of Uzbekistan, criminal legislation, and information-related laws. The article analyzes international legal norms, including international instruments aimed at combating cybercrime, as well as

information space,
cyberattacks,
national legislation,
international cooperation.

the experience of foreign countries in this field. Based on the analysis, scientific and practical recommendations for improving national legislation are proposed. The findings contribute to strengthening cybersecurity, protecting the constitutional rights of citizens in the information sphere, and developing effective legal mechanisms for combating cybercrime.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: СОВРЕМЕННЫЕ РИСКИ И ПОДХОДЫ УСТОЙЧИВОГО РАЗВИТИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

киберпреступность,
кибербезопасность,
информационная
безопасность,
конституционные права,
персональные данные,
цифровые технологии,
международное право,
Будапештская конвенция,
информационное
пространство,
кибератаки,
национальное
законодательство,
международное
сотрудничество.

АННОТАЦИЯ

В данной статье анализируются конституционно-правовые и международно-правовые основы противодействия киберпреступности в Республике Узбекистан. В исследовании раскрываются понятие киберпреступности, ее современные проявления, а также влияние на безопасность общества и государства. Кроме того, изучены механизмы обеспечения кибербезопасности, предусмотренные Конституцией Республики Узбекистан, уголовным законодательством и законодательством в сфере информации. В статье проанализированы международно-правовые нормы, включая международные документы, направленные на борьбу с киберпреступностью, а также опыт зарубежных государств. На основе проведенного анализа разработаны научно-практические предложения по совершенствованию национального законодательства. Результаты исследования направлены на укрепление кибербезопасности, защиту конституционных прав граждан в информационной сфере и развитие эффективных правовых механизмов противодействия киберпреступности.

KIRISH

XXI asrda raqamli texnologiyalar va axborot-kommunikatsiya tizimlarining jadal rivojlanishi jamiyat hayotining barcha sohalarini tubdan o'zgartirmoqda. Davlat boshqaruvi, iqtisodiyot, moliya, ta'lim, sog'liqni saqlash hamda boshqa muhim tarmoqlarning raqamlashtirilishi insoniyat taraqqiyotiga yangi imkoniyatlar yaratish bilan birga, kiberxavfsizlik bilan bog'liq yangi tahdidlarni ham yuzaga keltirmoqda. Xususan, kompyuter tizimlariga noqonuniy kirish,

ma'lumotlarni o'g'irlash, zararli dasturlar tarqatish, internet firibgarligi, shaxsga doir ma'lumotlardan noqonuniy foydalanish kabi kiberjinoyatlar davlatlar va jamiyatlar oldida turgan dolzarb muammolardan biriga aylanmoqda.

Kiberjinoyatchilikning o'ziga xos xususiyati uning transmilliy xarakterga egaligidadir. Kiberjinoyatlar davlat chegaralari bilan cheklanmaydi, ular bir vaqtning o'zida bir nechta mamlakatlarning axborot infratuzilmasiga zarar yetkazishi mumkin. Shu sababli mazkur turdagi huquqbuzarliklarga qarshi kurashishda nafaqat milliy qonunchilikni takomillashtirish, balki xalqaro hamkorlikni rivojlantirish ham muhim ahamiyat kasb etadi. Zamonaviy sharoitda kiberjinoyatchilikka qarshi samarali kurashish davlatlarning o'zaro axborot almashinuvi, huquqiy yordam ko'rsatishi va xalqaro standartlarni milliy qonunchilikka implementatsiya qilish darajasiga bevosita bog'liqdir.

O'zbekiston Respublikasida ham raqamli iqtisodiyot va elektron davlat xizmatlarini rivojlantirish bo'yicha keng ko'lamli islohotlar amalga oshirilmoqda. Natijada axborot tizimlari va telekommunikatsiya tarmoqlarining ahamiyati ortib bormoqda. Biroq raqamlashtirish jarayonlarining jadallashuvi kiberxavfsizlikni ta'minlash va kiberjinoyatchilikka qarshi kurashishning huquqiy mexanizmlarini yanada takomillashtirish zaruratini yuzaga keltirmoqda. Shu nuqtai nazardan, fuqarolarning axborot olish huquqi, shaxsiy hayot daxlsizligi, shaxsga doir ma'lumotlarning himoyasi hamda davlatning axborot xavfsizligini ta'minlash borasidagi majburiyatlari alohida ahamiyat kasb etadi.

Mamlakatimizda kiberxavfsizlikni ta'minlashga qaratilgan qator normativ-huquqiy hujjatlar qabul qilingan bo'lib, ular orasida O'zbekiston Respublikasi Konstitutsiyasi, Jinoyat kodeksi, "Kiberxavfsizlik to'g'risida"gi Qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun hamda axborotlashtirish sohasidagi boshqa normativ-huquqiy hujjatlar muhim o'rin tutadi. Biroq kiberjinoyatchilikning yangi shakllari va usullarining paydo bo'layotgani ushbu sohadagi huquqiy tartibga solish mexanizmlarini doimiy ravishda takomillashtirib borishni talab etmoqda.

O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishning konstitutsiyaviy-huquqiy va xalqaro-huquqiy asoslarini tahlil qilish, amaldagi milliy qonunchilik va xalqaro standartlarning o'zaro uyg'unligini o'rganish hamda mavjud muammolarni aniqlash orqali ularni bartaraf etishga qaratilgan ilmiy-amaliy takliflar ishlab chiqish bo'yicha tadqiqot olib borildi. Tadqiqot davomida qiyosiy-huquqiy, tizimli, formal-yuridik va tahliliy metodlardan foydalanildi.

METODOLOGIYA

Mazkur tadqiqotda O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishning konstitutsiyaviy-huquqiy va xalqaro-huquqiy asoslarini o'rganishda umumilmiy va maxsus yuridik tadqiqot metodlaridan foydalanildi. Xususan, formal-yuridik metod yordamida

O'zbekiston Respublikasi Konstitutsiyasi, Jinoyat kodeksi, "Kiberxavfsizlik to'g'risida"gi Qonun hamda axborot xavfsizligi sohasidagi boshqa normativ-huquqiy hujjatlarning mazmuni va huquqiy mohiyati tahlil qilindi.

Qiyosiy-huquqiy metod asosida O'zbekiston Respublikasining kiberjinoyatchilikka qarshi kurashish sohasidagi qonunchiligi xalqaro-huquqiy standartlar hamda ayrim xorijiy davlatlar, jumladan AQSh, Germaniya va Singapur tajribasi bilan taqqoslandi. Tizimli-tahliliy metod orqali kiberjinoyatchilikka qarshi kurashishning konstitutsiyaviy, jinoyat-huquqiy va xalqaro-huquqiy mexanizmlari yagona tizim sifatida o'rganildi.

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyatning barcha sohalarini raqamlashtirishga xizmat qilmoqda. Shu bilan birga, raqamli muhitdan noqonuniy maqsadlarda foydalanish holatlari ham ortib bormoqda. Natijada kiberjinoyatchilik zamonaviy dunyoning eng xavfli transmilliy tahdidlaridan biriga aylandi. Ilmiy adabiyotlarda kiberjinoyatchilik tushunchasiga turlicha yondashuvlar mavjud. Keng ma'noda kiberjinoyatchilik deganda kompyuter tizimlari, axborot tarmoqlari va elektron ma'lumotlardan foydalanish orqali sodir etiladigan yoki ularga qarshi qaratilgan barcha huquqbuzarliklar tushuniladi. Mazkur tushuncha kompyuter tizimlarining o'zi jinoyat obyekti bo'lgan holatlarni ham, kompyuter texnologiyalari jinoyat sodir etish vositasi sifatida foydalanilgan holatlarni ham qamrab oladi. Kiberjinoyatchilikning xalqaro-huquqiy asoslarini belgilovchi muhim hujjatlardan biri 2001-yilda qabul qilingan Budapesht konvensiyasi hisoblanadi. Mazkur Konvensiyada kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni noqonuniy egallash, tizimlar faoliyatiga noqonuniy aralashish, kompyuter firibgarligi va boshqa qator qilmishlar kiberjinoyatlar sifatida e'tirof etilgan.

O'zbekiston Respublikasida ham kiberxavfsizlikni ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biri hisoblanadi. Xususan, "Kiberxavfsizlik to'g'risida"gi Qonun axborot makonida xavfsizlikni ta'minlashning huquqiy asoslarini mustahkamlaydi. Shuningdek, O'zbekiston Respublikasi Jinoyat kodeksida kompyuter axborotidan noqonuniy foydalanish, axborot tizimlariga noqonuniy kirish va boshqa kiberjinoyatlar uchun javobgarlik nazarda tutilgan.

Kiberjinoyatchilikning eng muhim jihatlaridan biri uning transmilliy xarakterga egaligidir. An'anaviy jinoyatlardan farqli ravishda kiberjinoyatlar muayyan hudud bilan chegaralanmaydi. Jinoyatchi bir davlat hududida bo'lib, boshqa davlat fuqarolari yoki tashkilotlariga qarshi hujum uyushtirishi mumkin. Transmilliylikning asosiy sababi internet tarmog'ining global xususiyatidir. Kiberjinoyatni sodir etishda foydalanilgan serverlar bir necha davlatlarda joylashgan bo'lishi, jinoyatchi boshqa davlatda faoliyat yuritishi, jabrlanuvchi esa uchinchi davlat hududida bo'lishi mumkin. Bu esa jinoyatni aniqlash, tergov qilish va aybdorlarni javobgarlikka tortish jarayonini murakkablashtiradi. Shu sababli xalqaro hamkorlik kiberjinoyatchilikka qarshi kurashning asosiy vositalaridan biri hisoblanadi.

Davlatlar o'rtasida axborot almashinuvi, ekstraditsiya, o'zaro huquqiy yordam va qo'shma tergov mexanizmlarining samarali ishlashi kiberjinoyatlarga qarshi kurash samaradorligini oshiradi. Bu borada Interpol, Yevropol hamda Birlashgan Millatlar Tashkiloti muhim rol o'ynamoqda. Bundan tashqari, kiberjinoyatchilikning transmilliy tabiati davlat suvereniteti, yurisdiksiya va xalqaro javobgarlik masalalariga ham yangi yondashuvlarni talab qilmoqda. Shu bois ko'plab davlatlar milliy qonunchilikni xalqaro standartlarga moslashtirish va xalqaro hamkorlik mexanizmlarini kuchaytirishga intilmoqda. Natijada kiberjinoyatchilik nafaqat alohida shaxslar yoki tashkilotlar, balki butun davlatlar xavfsizligiga tahdid soluvchi global muammo sifatida namoyon bo'lmoqda. Shu sababli unga qarshi kurashishda milliy huquqiy mexanizmlar bilan bir qatorda xalqaro-huquqiy hamkorlik ham hal qiluvchi ahamiyat kasb etadi. Oxirgi statistik ma'lumotlarga nazar tashlaydigan bo'lsak, fuqarolarni kartalaridan ommaviy ravishda pul yechib olinishlari va hakerlar tomonidan ijtimoiy tarmoq profillari vzlom qilinishi bilan bog'liq jinoyatlar O'zbekiston Respublikasi hududi emas balki boshqa davlatlardan turib amalga oshirilmoqda. Bu esa o'z navbatidan davlatning imperativ tusdagi qonunlariga roiya qilmaganlikni anglatib javobgarlikka asos bo'ladi va qator tashkilotlar tomonidan vaziyat atroflicha o'rganilib zarur himoya choralari qo'llanilishiga asos bo'ladi.

NATIJALAR

Kiberjinoyatchilikka qarshi kurashning konstitutsiyaviy-huquqiy asoslarini tahlil qilishda, avvalo, axborot olish va undan foydalanish huquqining konstitutsiyaviy mazmunini yoritish zarur. Chunki raqamli jamiyat sharoitida insonning ko'plab huquq va erkinliklari aynan axborot-kommunikatsiya texnologiyalari orqali amalga oshiriladi. Shu bois kiberxavfsizlikni ta'minlash fuqarolarning axborot sohasidagi konstitutsiyaviy huquqlarini himoya qilish bilan chambarchas bog'liqdir. O'zbekiston Respublikasi Konstitutsiyasida avvalo inson manfaatlari ustuvor hisoblanib uning har bir moddasidan tortib boshqa qonunchiliklar ham inson va uning barcha huquqlari taminlashiga xizmat qiladi. O'zbekiston Respublikasi Konstitutsiyasining 33-moddasiga muvofiq, har kim fikrlash, so'z va e'tiqod erkinligi huquqiga ega. Ushbu norma shaxsning axborot bilan erkin munosabatda bo'lishi, o'z fikrini shakllantirishi va uni erkin ifoda etishining konstitutsiyaviy asosini tashkil etadi. Axborot texnologiyalarining rivojlanishi natijasida mazkur huquq internet tarmoqlari, ijtimoiy media platformalari, elektron ommaviy axborot vositalari va boshqa raqamli resurslar orqali amalga oshirilmoqda. Shuningdek har kim axborotni izlash, olish va tarqatish huquqiga egaligi mustahkamlangan. Mazkur norma demokratik jamiyatning asosiy tamoyillaridan biri bo'lib, fuqarolarning davlat va jamiyat hayotidagi faol ishtirokini ta'minlaydi. Shu bilan birga, mazkur huquqdan foydalanish boshqa shaxslarning huquqlari, davlat xavfsizligi, jamoat tartibi hamda qonun bilan qo'riqlanadigan manfaatlarga zarar yetkazmasligi lozim. Kiberjinoyatlar, xususan, kompyuter tizimlariga noqonuniy kirish, axborot resurslarini bloklash, ma'lumotlarni yo'q qilish yoki o'zgartirish

kabi harakatlar fuqarolarning Konstitutsiyada kafolatlangan axborot olish huquqiga bevosita tajovuz qiladi. Shu sababli davlat tomonidan amalga oshiriladigan kiberxavfsizlik choralari nafaqat axborot tizimlarini, balki fuqarolarning konstitutsiyaviy huquqlarini ham himoya qilishga qaratilgan. Mazkur masala xalqaro huquqiy hujjatlarda ham o'z aksini topgan. Jumladan, Inson huquqlari umumjahon deklaratsiyasining 19-moddasi hamda Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro paktning 19-moddasi har bir insonning axborotni izlash, olish va tarqatish huquqini e'tirof etadi. O'zbekiston ushbu xalqaro standartlarni tan olgan holda ularni milliy qonunchilikka implementatsiya qilgan.

Shaxsiy hayot daxlsizligi va shaxsga doir ma'lumotlarni himoya qilish davlatning asosiy konstitutsiyaviy majburiyati hisoblanadi. Davlat har bir fuqaroning shaxsiy ma'lumotlarini xavfsizligini taminlashi va tashqi xavf va bosimlardan himoya qilishi shart hisoblanadi. Afsuski hozirgi kunda ko'plab fuqarolarni shaxsga doir ma'lumotlari kiberhujumlar tomonidan buzilishi yohud tarqatib yuborilishi mamlakatimizda ko'p kuzatilmoqda. Ayniqsa fuqarolarning rasmlari va passport ma'lumotlaridan foydalanib kiber jinoyatchilar turli xil maqsadlarda foydalanishi hatto rasmlarni fotoshop orqali ming tusga kirgazib tarqarishlari insonning eng ulug' va muborak hisoblangan shani va qadr qimmatiga putur yetkazilish holatlari kuzatilmoqda.

Kiberjinoyatchilikning eng xavfli ko'rinishlaridan biri shaxsga doir ma'lumotlarga noqonuniy tajovuz qilish bilan bog'liqdir. Zamonaviy raqamli texnologiyalar sharoitida fuqarolarning shaxsiy ma'lumotlari elektron bazalarda saqlanadi va qayta ishlanadi. Bu esa mazkur ma'lumotlarning noqonuniy egallanishi, tarqatilishi yoki ulardan g'arazli maqsadlarda foydalanilishi xavfini kuchaytiradi. O'zbekiston Respublikasi Konstitutsiyasining 31-moddasiga ko'ra, har bir shaxsning shaxsiy hayoti daxlsizligi, shaxsiy va oilaviy siri himoya qilinadi. Mazkur norma insonning shaxsiy hayotiga noqonuniy aralashuvdan himoyalani sh huquqining konstitutsiyaviy kafolati hisoblanadi. Bundan tashqari, Konstitutsiyada yozishmalar, telefon orqali so'zlashuvlar, pochta jo'natmalari, elektron xabarlar va boshqa muloqot vositalarining sir saqlanishi kafolatlangan. Ushbu norma zamonaviy axborot texnologiyalari rivojlangan sharoitda alohida ahamiyat kasb etadi. Chunki bugungi kunda shaxsiy muloqotlarning katta qismi elektron pochta, messenjerlar va ijtimoiy tarmoqlar orqali amalga oshirilmoqda. Kiberjinoyatchilar tomonidan elektron pochta hisoblarini buzish, bank kartalari ma'lumotlarini o'g'irlash, shaxsiy fotosurat va hujjatlarni noqonuniy qo'lga kiritish yoki internet tarmoqlarida tarqatish Konstitutsiyaning 31 va boshqa moddalarida nazarda tutilgan huquqlarning buzilishiga olib keladi. Shu bois shaxsiy hayot daxlsizligini ta'minlash kiberxavfsizlik siyosatining ustuvor yo'nalishlaridan biri hisoblanadi. Mazkur huquqlar "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun orqali yanada rivojlantirilgan. Ushbu qonun shaxsga doir ma'lumotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanishning huquqiy asoslarini belgilaydi hamda ma'lumotlar subyektlarining huquqlarini himoya qilishga

qaratilgan. Xalqaro huquq nuqtayi nazaridan ham shaxsiy hayot daxlsizligi fundamental inson huquqlaridan biri hisoblanadi. Xususan, Inson huquqlari umumjahon deklaratsiyasining 12-moddasi va Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro paktning 17-moddasi hech kimning shaxsiy va oilaviy hayotiga o'zboshimchalik bilan aralashishga yo'l qo'yilmasligini belgilaydi.

Kiberjinoyatchilikka qarshi kurash davlatning inson huquqlari va xavfsizlikni ta'minlash borasidagi konstitutsiyaviy vazifalaridan kelib chiqadi. Raqamli texnologiyalar jamiyat hayotining barcha sohalariga kirib borgan hozirgi davrda davlatning axborot makonini himoya qilish bo'yicha faoliyati alohida ahamiyat kasb etmoqda. O'zbekiston Respublikasi Konstitutsiyasining 31-moddasida har kimning shaxsiy hayoti daxlsizligi, shaxsiy va oilaviy siri himoya qilinishi, yozishmalar, telefon so'zlashuvlari, pochta, elektron va boshqa xabarlar sir saqlanishi kafolatlangan. Shuningdek, ushbu moddada shaxsga doir ma'lumotlarni himoya qilish huquqi ham mustahkamlangan. Mazkur norma davlat zimmasiga fuqarolarning shaxsiy ma'lumotlarini noqonuniy foydalanish, tarqatish va kiberhujumlardan himoya qilish majburiyatini yuklaydi. Shuningdek, Konstitutsiyaning 33-moddasiga ko'ra, har kim axborotni izlash, olish va tarqatish huquqiga ega. Mazkur modda davlat tomonidan Internet jahon axborot tarmog'idan foydalanish uchun shart-sharoitlar yaratib berilishini ham nazarda tutadi. Shu bois davlat axborot infratuzilmasining barqaror va xavfsiz faoliyatini ta'minlash, axborot resurslarini kiberxurujlardan himoya qilish hamda fuqarolarning axborotdan erkin foydalanish huquqini kafolatlash choralari ko'rishi lozim. Bundan tashqari, Konstitutsiyaning 34-moddasida davlat organlari va tashkilotlarining fuqarolarga ularning huquq va manfaatlariga daxldor bo'lgan hujjatlar, qarorlar va boshqa materiallar bilan tanishish imkoniyatini yaratishi belgilangan. Mazkur norma davlat axborot tizimlarining ishonchliligi va himoyalanganligini ta'minlash zaruratini yuzaga keltiradi. Konstitutsiyaning 81-moddasida ommaviy axborot vositalarining erkinligi, axborotni izlash, olish, undan foydalanish va tarqatish huquqlari kafolatlangan. Raqamli davrda ommaviy axborot vositalarining asosiy faoliyati internet va elektron platformalar orqali amalga oshirilayotganligi sababli davlat ushbu axborot resurslarining kiberxavfsizligini ta'minlash bo'yicha tegishli choralarni ko'rishi zarur. Davlatning mazkur konstitutsiyaviy majburiyatlari "Kiberxavfsizlik to'g'risida"gi Qonun, "Axborotlashtirish to'g'risida"gi Qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun hamda O'zbekiston Respublikasi Jinoyat kodeksining axborot texnologiyalari sohasidagi jinoyatlarga oid normalarida yanada rivojlantirilgan. Shu bilan birga, davlatning kiberxavfsizlikni ta'minlash bo'yicha faoliyati inson huquqlarini cheklash vositasiga aylanmasligi kerak. Kiberjinoyatchilikka qarshi kurashish choralari Konstitutsiyada belgilangan shaxsiy hayot daxlsizligi, axborot olish erkinligi va boshqa fundamental huquqlar bilan muvozanatda amalga oshirilishi lozim. Aynan ana shunday yondashuv demokratik huquqiy davlatning asosiy mezonlaridan biri hisoblanadi.

O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishning milliy huquqiy mexanizmlari jinoyat huquqi normalari, maxsus kiberxavfsizlik sohasidagi qonunchilik hamda huquqni muhofaza qiluvchi organlarning institutsional faoliyati orqali amalga oshiriladi. Ushbu mexanizmlar raqamli muhitda axborot xavfsizligini ta'minlash, fuqarolarning huquq va erkinliklarini himoya qilish hamda davlatning axborot infratuzilmasini himoyalashga xizmat qiladi. Bugungi kunda axborot texnologiyalarining jadal rivojlanishi jamiyat hayotini tubdan o'zgartirdi. Bank tizimlari, davlat xizmatlari, savdo platformalari va hatto shaxsiy muloqotlar ham raqamli muhitga ko'chdi. Biroq ushbu taraqqiyot bilan bir qatorda yangi xavf — kiberjinoyatchilik ham keskin ortib bormoqda. O'zbekiston Respublikasi Jinoyat kodeksining XX¹-bobi aynan shu munosabatlarni huquqiy tartibga solishga qaratilgan bo'lib, u axborot texnologiyalari sohasida sodir etiladigan jinoyatlar uchun javobgarlikning tizimli asosini yaratadi. Axborot tizimlarining xavfsizligini ta'minlash va qoidalarni buzish (278¹-modda) Axborot tizimlari va ma'lumotlar bazalari bugungi raqamli jamiyatning asosiy infratuzilmasi hisoblanadi. Ularning yaratish, joriy etish va foydalanish jarayonida belgilangan xavfsizlik talablariga amal qilmaslik jiddiy oqibatlariga olib kelishi mumkin. Qonunchilikda bunday holatlar natijasida fuqarolar, davlat yoki jamoat manfaatlariga zarar yetkazilsa, bu jinoyat sifatida baholanadi. Bu norma asosan tizimlarni noto'g'ri tashkil etish, texnik himoya choralariغا beparvolik yoki axborot xavfsizligi standartlariga rioya qilmaslik holatlariga qarshi qaratilgan. Kompyuter axborotiga ruxsatsiz kirish va undan foydalanish (278²-modda).

Kiberjinoyatchilikning eng ko'p uchraydigan shakllaridan biri — bu kompyuter tizimlariga noqonuniy kirishdir. Bunda shaxsiy ma'lumotlar o'g'irlanishi, o'zgartirilishi yoki yo'q qilinishi mumkin. Shuningdek, bu turdagi harakatlar bank tizimlari, davlat portallari yoki yirik korporativ tarmoqlarning ish faoliyatiga ham jiddiy zarar yetkazishi ehtimoli mavjud. Ayniqsa, bunday jinoyatlar bir guruh shaxslar tomonidan yoki xizmat mavqeidan foydalanib sodir etilganda, ularning ijtimoiy xavflilik darajasi yanada ortadi. Kiberjinoyat vositalarini yaratish va tarqatish (278³-modda) Kiberjinoyatlarning oldini olishda muhim jihatlardan biri — ularni amalga oshirish uchun ishlatiladigan vositalarni cheklashdir. Maxsus dasturlar, zararli kodlar yoki ruxsatsiz kirish vositalarini yaratish va tarqatish kiberjinoyatchilikni kengaytiruvchi asosiy omillardan biridir.

Shu sababli qonunchilik faqat jinoyatning o'zini emas, balki uni amalga oshirishga xizmat qiluvchi texnik vositalarni tayyorlash va tarqatishni ham jinoyat sifatida belgilaydi. Axborotni o'zgartirish va kompyuter sabotaji (278⁴–278⁵-moddalar) Axborot tizimlaridagi ma'lumotlarning buzilishi yoki o'zgartirilishi nafaqat texnik muammo, balki huquqiy jihatdan ham og'ir oqibatlariga ega harakat hisoblanadi. Chunki bugungi kunda axborotning aniqligi va ishonchliligi ko'plab qarorlar uchun asos bo'lib xizmat qiladi. Kompyuter sabotaji esa yanada og'irroq jinoyat bo'lib, u tizimlar yoki texnik uskunalarni qasddan ishdan chiqarishga qaratilgan. Bunday harakatlar ko'pincha yirik infratuzilma obyektlariga zarar yetkazishga

yo'naltirilgan bo'ladi. Zararli dasturlar bilan bog'liq jinoyatlar (278⁶-modda) Viruslar va boshqa zararli dasturlar zamonaviy kiberxavfsizlik uchun eng katta tahdidlardan biri hisoblanadi. Ular orqali axborot tizimlariga kirish, ma'lumotlarni yo'q qilish yoki ularni boshqarish imkoniyati paydo bo'ladi. Shu sababli bunday dasturlarni yaratish, ulardan foydalanish yoki tarqatish jinoyat sifatida baholanadi va og'ir javobgarlikni keltirib chiqaradi. Telekommunikatsiya tarmoqlaridan noqonuniy foydalanish (278⁷-modda) Telekommunikatsiya tarmoqlari global axborot almashinuvining asosiy vositasi bo'lib, ulardan noqonuniy foydalanish transmilliy jinoyatlarni keltirib chiqarishi mumkin. Himoya tizimlarini chetlab o'tish, xalqaro trafikni noqonuniy yo'naltirish yoki maxsus vositalarni saqlash kabi harakatlar kiberxavfsizlikka bevosita tahdid soladi. Kripto-aktivlar sohasidagi huquqbuzarliklar (278⁸-modda) Raqamli iqtisodiyotning rivojlanishi kripto-aktivlar sohasini ham huquqiy tartibga solishni talab qildi. Litsenziyasiz faoliyat yuritish, anonim operatsiyalarni amalga oshirish yoki noqonuniy kripto-almashinuvlar moliyaviy tizim xavfsizligiga jiddiy xavf tug'diradi. Shu sababli ushbu sohadagi qonunbuzarliklar ham jinoyat sifatida belgilangan. Firibgarlik va o'g'rilikda axborot texnologiyalarining roli (168–169-moddalar) So'nggi yillarda firibgarlik va o'g'rilik jinoyatlari ham raqamli shaklga o'tdi. Elektron to'lov tizimlari, bank kartalari va internet platformalari orqali sodir etilayotgan jinoyatlar JKning 168 va 169-moddalari doirasida kiberjinoyat sifatida baholanadi. Bu holatlar fuqarolarning mol-mulkiga bevosita zarar yetkazishi bilan birga, raqamli iqtisodiyotga bo'lgan ishonchni ham pasaytiradi.

Mamlakatimizda kiberxavfsizlik choralari ko'rish va sohani rivojlantirish maqsadida 2022-yil 25-fevralda "Kiberxavfsizlik" to'g'risida qonun qabul qilingan. Ushbu qonunning mohiyatini tahlil qiladigan bo'lsak, mazkur Qonunning eng muhim jihati shundaki, u kiberxavfsizlikni faqat texnik masala sifatida emas, balki davlat siyosatining strategik yo'nalishi sifatida belgilaydi. Ya'ni kiberxavfsizlik endilikda alohida tashkilotlarning emas, balki butun davlat tizimining uzviy vazifasi sifatida qaraladi. Qonun axborot tizimlari va axborot resurslarining himoyasini ta'minlash, ularga noqonuniy kirishlarning oldini olish, shuningdek ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini saqlash kabi asosiy prinsiplarni mustahkamlaydi. Bu esa zamonaviy raqamli infratuzilmaning barqaror ishlashi uchun huquqiy kafolat yaratadi. Shuningdek, ushbu Qonun kiberxavfsizlik sohasida davlat organlarining vakolatlarini aniq belgilab beradi. Davlat tomonidan kiberxavfsizlik siyosatini ishlab chiqish, muvofiqlashtirish va nazorat qilish mexanizmlari joriy etiladi. Bu esa turli darajadagi axborot tizimlarida yagona yondashuvni ta'minlashga xizmat qiladi. Qonunning yana bir muhim jihati shundaki, u nafaqat davlat axborot tizimlarini, balki xususiy sektor va fuqarolarning axborot resurslarini ham himoya qilishni ko'zda tutadi.

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING XALQARO-HUQUQIY ASOSLARI

Kiberjinoyatchilik global miqyosda tez sur'atlarda rivojlanib borayotgan zamonaviy xavfsizlik tahdidlaridan biri hisoblanadi. Axborot texnologiyalarining chegarasiz tabiati sababli bunday jinoyatlar bir davlat hududi bilan cheklanib qolmay, bir vaqtning o'zida bir nechta davlat manfaatlariga ta'sir ko'rsatishi mumkin. Shu bois kiberjinoyatchilikka qarshi kurashish faqat milliy darajada emas, balki xalqaro-huquqiy hamkorlik asosida amalga oshiriladi. Xalqaro huquqda kiberjinoyatchilikka qarshi kurash masalalari Xalqaro huquq tizimida kiberjinoyatchilikka qarshi kurashish masalasi axborot xavfsizligini ta'minlash, transmilliy jinoyatchilikni oldini olish hamda davlatlarning raqamli suverenitetini himoya qilish bilan bevosita bog'liqdir.

Kiberjinoyatchilik sohasidagi eng muhim xalqaro hujjatlardan biri bu 2001-yilda qabul qilingan Budapesht konvensiyasi (Kiberjinoyatchilik to'g'risidagi konvensiya) hisoblanadi. Ushbu konvensiya Yevropa Kengashi tomonidan ishlab chiqilgan bo'lib, u kiberjinoyatchilikka qarshi kurashishning huquqiy asoslarini belgilaydi. Konvensiyaning asosiy maqsadi — kompyuter tizimlari orqali sodir etiladigan jinoyatlarni aniqlash, tergov qilish va ularga qarshi samarali huquqiy mexanizmlarni yaratishdir. U quyidagi asosiy yo'nalishlarni qamrab oladi: Birinchidan, kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni o'zgartirish yoki yo'q qilish kabi jinoyatlarni kriminalizatsiya qilish talablarini belgilaydi. Ikkinchidan, dalillarni raqamli shaklda saqlash va ulardan foydalanish bo'yicha protsessual qoidalarni ishlab chiqadi. Bu kiberjinoyatlar bo'yicha tergov jarayonini standartlashtirishga xizmat qiladi. Uchinchidan, xalqaro hamkorlikni kuchaytirish, ya'ni davlatlar o'rtasida tezkor ma'lumot almashish va huquqiy yordam ko'rsatish mexanizmlarini belgilaydi. Budapesht konvensiyasi kiberjinoyatchilikka qarshi kurashishda eng muhim universal hujjatlardan biri bo'lib, ko'plab davlatlar uchun namunaviy huquqiy asos sifatida xizmat qilmoqda.

Xalqaro hamkorlik va davlatlararo huquqiy yordam mexanizmlari Kiberjinoyatchilikning transmilliy tabiati davlatlar o'rtasida yaqin hamkorlikni talab etadi. Xalqaro huquqiy yordam mexanizmlari jinoyatchilarni aniqlash, dalillarni yig'ish va ularni javobgarlikka tortishda muhim ahamiyatga ega. Bunday hamkorlik doirasida davlatlar o'zaro huquqiy yordam so'rovlari (MLA – Mutual Legal Assistance) orqali ma'lumot almashadi, jinoyatchilarni ekstraditsiya qiladi hamda tergov harakatlarini muvofiqlashtiradi. Bundan tashqari, Interpol va boshqa xalqaro tashkilotlar orqali tezkor axborot almashinuvi yo'lga qo'yilgan. Shuningdek, kiberjinoyatchilikka qarshi kurashishda milliy CERT (Computer Emergency Response Team) markazlari ham muhim rol o'ynaydi. Ular kiberhujumlarni aniqlash, tahlil qilish va ularni bartaraf etish bo'yicha xalqaro tarmoqlar bilan hamkorlik qiladi. Xulosa qilib aytganda, kiberjinoyatchilikka qarshi kurashishning xalqaro-huquqiy asoslari davlatlar o'rtasidagi

hamkorlik, Budapesht konvensiyasi va boshqa xalqaro mexanizmlar orqali shakllanib, global axborot xavfsizligini ta'minlashga xizmat qiladi. Bu esa zamonaviy raqamli jamiyatda barqarorlik va xavfsizlikni saqlashning muhim sharti hisoblanadi.

MUHOKAMA

Kiberjinoyatchilikka qarshi kurashish bugungi kunda nafaqat milliy huquq tizimining, balki xalqaro huquqning ham dolzarb yo'nalishlaridan biri hisoblanadi. O'zbekiston Respublikasida ushbu sohada shakllangan normativ-huquqiy baza, xususan Jinoyat kodeksining normalari hamda "Kiberxavfsizlik to'g'risida"gi Qonun kiberjinoyatlarga qarshi kurashishning asosiy huquqiy poydevorini tashkil etadi. Mazkur normalar orqali axborot tizimlariga noqonuniy kirish, zararli dasturlar tarqatish, kompyuter sabotaji va kriptο-aktivlar bilan bog'liq noqonuniy harakatlar uchun javobgarlik belgilangan.

Shu bilan birga, amaliyot tahlili kiberjinoyatchilikka qarshi kurashishda ayrim muammolar mavjudligini ko'rsatadi. Eng asosiy muammolardan biri — kiberjinoyatlarning tezkor o'zgaruvchan xususiyatga ega ekanligidir. Ya'ni jinoyatchilar yangi texnologiyalar va yashirish usullaridan foydalangan holda an'anaviy huquqiy mexanizmlardan tezroq moslashib ketmoqda. Bu esa qonunchilikning doimiy ravishda takomillashtirib borilishini talab etadi.

Ikkinchi muhim masala — raqamli dalillarni to'plash va ularni protsessual jihatdan rasmiylashtirish jarayonidir. Kiberjinoyatlarda asosiy dalillar elektron shaklda bo'lgani uchun ularni yo'qotmasdan saqlash, tahlil qilish va sudga taqdim etish alohida texnik bilim va zamonaviy ekspertiza imkoniyatlarini talab qiladi. Ayrim hollarda esa ushbu texnik imkoniyatlarning yetarli darajada emasligi tergov jarayonini murakkablashtiradi.

Shuningdek, xalqaro tajriba shuni ko'rsatadiki, kiberjinoyatchilik transmilliy xarakterga ega bo'lgani sababli davlatlar o'rtasidagi hamkorlik hal qiluvchi ahamiyatga ega. Budapesht konvensiyasi kiberjinoyatlarga qarshi kurashishning xalqaro standartini belgilab bergan bo'lsa-da, amaliyotda huquqiy yordam so'rovlari va ma'lumot almashish jarayonlarida ba'zan kechikishlar kuzatiladi. Bu esa jinoyatlarni tezkor fosh etishga salbiy ta'sir ko'rsatadi.

Bundan tashqari, jamiyatda kiberxavfsizlik bo'yicha huquqiy ong va madaniyat darajasi ham yetarli emasligi dolzarb muammo bo'lib qolmoqda. Fuqarolarning shaxsiy ma'lumotlarini himoya qilish, firibgarlik sxemalaridan saqlanish va internetdan xavfsiz foydalanish bo'yicha bilimlari yetarli darajada shakllanmaganligi kiberjinoyatlar sonining oshishiga olib kelmoqda. Mazkur muammolarni bartaraf etish uchun bir qator takliflarni ilgari surish mumkin. Jumladan, kiberjinoyatlar bo'yicha maxsuslashtirilgan ekspert-kriminalistika markazlarini rivojlantirish, raqamli tergov (digital forensics) imkoniyatlarini kengaytirish hamda huquqni muhofaza qiluvchi organlarning texnik bazasini modernizatsiya qilish zarur. Shuningdek, xalqaro hamkorlikni yanada tezkor va samarali qilish, ayniqsa transchegaraviy ma'lumot almashinuvi mexanizmlarini soddalashtirish muhim hisoblanadi.

Eng asosiy jihatlariga yana e'tibor qaratsak pul inson uchun eng zarur resurs hisoblanadi fuqarolardan noqonuniy tarzda plastik yoki kredit kartalardan pul yechib olinishi bu eng katta fuqarolarga zarar hisoblanadi. Afsuski fuqarolar bu holatda hech nima qila olishmaydi. Hozirgi asosiy taklif shundan iboratki fuqarolarga kompensatsiya masalasidir. Bank tizimi xavfsizlik jihatdan kuchki bo'lish kerak hakkerlar tomonidan yechib olinga har bir so'm bank tomonidan qaysidir qismi qoplanishi yoki to'liq qoplanishi kerak shunda bank va mijoz o'rtasidagi munosabatga putur yetmaydi.

Kiberjinoyatlar to'g'risidagi konvensiya milliy qonunlarni uyg'unlashtirish, tergov usullarini takomillashtirish va davlatlar o'rtasidagi hamkorlikni oshirish orqali Internet va kompyuter jinoyatlarini kiber jinoyatlar hal qilishga qaratilgan birinchi xalqaro shartnomadir. U Fransiyaning Strasburg shahrida Yevropa Kengashi tomonidan Yevropa Kengashining kuzatuvchi bir qancha davlatlari Kanada, Yaponiya, Filippin, Janubiy Afrika va AQShning faol ishtirokida ishlab chiqilgan. Konvensiya va uning tayyorlangan hisoboti Yevropa Kengashi Vazirlar Qo'mitasi tomonidan 2001-yil 8-noyabrdagi 109-sessiyasida qabul qilingan. 2001-yil 23-noyabrda Vengriya poytaxti Budapeshtda imzolash uchun chaqirilgan va 2004-yil 1-iyuldan boshlab kuchga kirgan. 2020-yil dekabr holatiga ko'ra, 65 davlat konvensiyani ratifikatsiya qilgan, yana to'rtta davlat konvensiyani imzolagan, ammo uni ratifikatsiya qilmagan. Bu kiberjinoyatchilikni tartibga soluvchi birinchi ko'p tomonlama qonuniy majburiy vositadir. 2018-yildan beri Hindiston kiberjinoyatlar avj olganidan keyin Konvensiyaga nisbatan o'z pozitsiyasini qayta ko'rib chiqmoqda. Ammo xorijiy agentliklar bilan ma'lumot almashish bo'yicha xavotirlar saqlanib qolmoqda. 2006-yil 1-martda Kiberjinoyat to'g'risidagi konvensiyaga qo'shimcha protokol kuchga kirdi. Qo'shimcha protokolni ratifikatsiya qilgan davlatlar kompyuter tizimlari orqali irqchilik va ksenofobik materiallarni, shuningdek, irqchilik yoki ksenofobiya asosidagi tahdid va haqoratlarni tarqatish uchun jinoiy javobgarlikka tortilishi kerak.

Konvensiya Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar to'g'risidagi birinchi xalqaro shartnoma bo'lib, ayniqsa mualliflik huquqining buzilishi, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasi, nafrat jinoyatlari va tarmoq xavfsizligini buzish bilan bog'liq. Shuningdek, u kompyuter tarmoqlarini qidirish, topish, qo'lga kiritish va qonuniy ravishda jazolash kabi bir qator vakolatlar va tartiblarni o'z ichiga oladi. Uning muqaddimada bayon etilgan asosiy maqsadi jamiyatni kiberjinoyatlardan himoya qilishga qaratilgan umumiy jinoiy siyosatni olib borish, ayniqsa tegishli qonun hujjatlarini qabul qilish va xalqaro hamkorlikni rivojlantirishdan iborat.

Konvensiyada quyidagi jinoyatlar belgilangan: noqonuniy kirish, noqonuniy qo'lga olish, ma'lumotlarga aralashuv, tizimga aralashuv, qurilmalardan noto'g'ri foydalanish, kompyuter bilan bog'liq qalbakilashtirish, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasi bilan bog'liq huquqbuzarliklar, mualliflik huquqi va qo'shni huquqlar bilan bog'liq

huquqbuzarliklar. Shuningdek, u saqlangan ma'lumotlarni tezkor saqlash, trafik ma'lumotlarini tezkor saqlash va qisman oshkor qilish, ishlab chiqarish tartibi, kompyuter ma'lumotlarini qidirish va olib qo'yish, trafik ma'lumotlarini real vaqt rejimida yig'ish va kontent ma'lumotlarini qo'lga kiritish kabi protsessual huquqiy masalalarni belgilaydi. Bundan tashqari, Konvensiyada saqlanadigan kompyuter ma'lumotlariga o'zaro yordamni talab qilmaydigan transchegaraviy kirishning ma'lum bir turi to'g'risidagi qoida mavjud (rozilik bilan yoki hamma uchun mavjud bo'lganda) va tezkorlikni ta'minlash uchun 24/7 tarmoqni o'rnatishni nazarda tutadi. Bundan tashqari, shartlar va kafolatlar sifatida Konvensiya inson huquqlari va erkinliklarini, shu jumladan Inson huquqlari to'g'risidagi Yevropa konvensiyasi, Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt va boshqa amaldagi inson huquqlari bo'yicha xalqaro hujjatlardan kelib chiqadigan majburiyatlardan kelib chiqadigan huquqlarni munosib himoya qilishni ta'minlashni talab qiladi va mutanosiblik tamoyilini o'z ichiga oladi. Konvensiya Yevropa va xalqaro ekspertlarning to'rt yillik mehnati mahsulidir. U kompyuter tarmoqlari orqali irqchilik va ksenofobiya tashviqotining har qanday nashrini jinoiy tuhmat to'g'risidagi qonunlarga o'xshash jinoiy javobgarlikka tortuvchi qo'shimcha protokol bilan to'ldirildi. Hozirda konvensiya doirasida kiberterrorizm ham o'rganilmoqda. Xulosa qilib aytganda, kiberjinoiyatchilikka qarshi kurashish tizimi kompleks yondashuvni talab etadi. Bu jarayonda nafaqat huquqiy baza, balki texnik infratuzilma, xalqaro hamkorlik va fuqarolarning huquqiy savodxonligi ham muhim rol o'ynaydi. Shu jihatdan, mavjud tizimni yanada takomillashtirish zamonaviy raqamli jamiyat barqarorligini ta'minlashning asosiy shartlaridan biri hisoblanadi.

XULOSA

Kiberjinoiyatchilik zamonaviy axborot jamiyatining eng dolzarb va murakkab muammolaridan biri bo'lib, u davlat, jamiyat va shaxs manfaatlariga bevosita tahdid soladi. Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberjinoiyatlar ham yangi ko'rinish va usullar orqali namoyon bo'lmoqda. Bu esa ularni aniqlash, oldini olish, tergov qilish va huquqiy baholash jarayonlarini yanada murakkablashtirmoqda.

Tahlillar shuni ko'rsatadiki, O'zbekiston Respublikasida kiberjinoiyatchilikka qarshi kurashishning huquqiy asoslari izchil shakllanmoqda. Xususan, O'zbekiston Respublikasi Jinoyat kodeksining tegishli normalari hamda "Kiberxavfsizlik to'g'risida"gi Qonun ushbu sohadagi asosiy normativ-huquqiy bazani tashkil etadi. Mazkur hujjatlar axborot tizimlariga noqonuniy kirish, kompyuter sabotaji, zararli dasturlarni yaratish va tarqatish, shuningdek, kripto-aktivlar bilan bog'liq huquqbuzarliklar uchun javobgarlikni belgilab beradi. Shu bilan birga, kiberjinoiyatlarning transmilliy xarakteri, raqamli dalillar bilan ishlashdagi texnik murakkabliklar hamda xalqaro huquqiy yordam mexanizmlarining ba'zan yetarli darajada tezkor ishlamasligi ushbu yo'nalishda hal etilishi lozim bo'lgan muhim muammolar sifatida

namoyon bo‘lmoqda. Bu esa kiberjinoyatchilikka qarshi kurashish tizimini doimiy ravishda takomillashtirish zarurligini ko‘rsatadi.

Hozirgi globallashuv va raqamli transformatsiya sharoitida jamiyat hayotining deyarli barcha sohalari axborot-kommunikatsiya texnologiyalari bilan uzviy bog‘lanib bormoqda. Davlat xizmatlari, bank-moliya tizimi, ta’lim, sog‘liqni saqlash, elektron tijorat va shaxsiy muloqot vositalarining raqamli platformalarga ko‘chishi fuqarolar uchun qulayliklar yaratish bilan birga, yangi turdagi kiberxavflarni ham yuzaga keltirmoqda. Ayniqsa, bank kartalaridan noqonuniy pul yechib olish, shaxsiy ma’lumotlardan foydalangan holda kredit rasmiylashtirish, ijtimoiy tarmoq profilarni egallab olish, phishing havolalar orqali maxfiy ma’lumotlarni qo‘lga kiritish kabi holatlar fuqarolarning mulkiy manfaatlar va shaxsiy hayoti daxlsizligiga jiddiy zarar yetkazmoqda.

Umuman olganda, kiberjinoyatchilikka qarshi kurashish faqat huquqni muhofaza qiluvchi organlarning vazifasi emas, balki davlat, jamiyat, xususiy sektor va har bir fuqaroning umumiy mas’uliyati hisoblanadi. Mazkur sohada samaradorlikka erishish uchun normativ-huquqiy bazani doimiy takomillashtirish, huquqni muhofaza qiluvchi organlarning texnik va ekspertlik salohiyatini oshirish, bank-moliya tizimlarida kiberxavfsizlik talablarini kuchaytirish, fuqarolarning raqamli savodxonligini yuksaltirish hamda kiberxavfsizlik madaniyatini shakllantirish muhim ahamiyatga ega. Shu jihatdan, kiberjinoyatchilikka qarshi kurashish O‘zbekiston Respublikasida axborot xavfsizligini ta’minlash, fuqarolarning konstitutsiyaviy huquqlarini himoya qilish va raqamli iqtisodiyot barqarorligini mustahkamlashning muhim sharti sifatida baholanishi lozim.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Kiber huquq – huquq sohasi sifatida: risola / tuzuvchilar R.R.Shakurov, M.M.Vohidov. – Toshkent: O‘zbekiston Respublikasi Adliya vazirligi qoshidagi Yuristlar malakasini oshirish markazi, 2022. – 3-10 b.
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.
3. O‘zbekiston Respublikasi Jinoyat kodeksi.
4. United Nations Office on Drugs and Crime (UNODC) – Comprehensive Study on Cybercrime.
5. “Convention on Cybercrime, Budapest, 23 November 2001”.
6. Budapesht konvensiyasi (Convention on Cybercrime), 2001-yil, Yevropa Kengashi.
7. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni.
8. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni.
9. ITU (International Telecommunication Union). Global Cybersecurity Index (GCI) Reports.
10. O‘zbekiston Respublikasi Konsitutsiyasi 2023
11. www.gazeta.uz/oz/tag/iivkiberxavfsizlikmarkazi/

SUN'IY INTELEKTNING HUQUQ TIZIMLARI VA ODIL SUDLOV FAOLIYATIGA TA'SIRI

Boymirzayeva Madina Ibrohim qizi

*“TIQXMMI” Milliy tadqiqot universiteti “Ekologiya va
huquq” fakulteti 2-bosqich talabasi*

MAQOLA MA'LUMOTI

Kalit so'zlar:

*sun'iy intellekt,
odil sudlov,
LegalTech,
algoritmik adolat,
sud qarorlari,
qiyosiy-huquqiy tahlil,
inson huquqlari.*

ANNOTATSIYA

Mazkur ilmiy maqolada sun'iy intellekt (SI) texnologiyalarining zamonaviy huquq tizimlari arxitekturasi hamda odil sudlov faoliyatining amalga oshirilishiga ko'rsatayotgan bevosita va bilvosita ta'siri huquqiy-tahliliy jihatdan tadqiq etiladi. Ishda “LegalTech” platformalari hamda prognozlashtirilgan adolat tizimlarining sud amaliyotiga integratsiyalashuvi texnik hujjatlar aylanishini va ma'lumotlar tahlilini optimallashtirgan bo'lsa-da, algoritmlardagi texnik xatoliklar, ma'lumotlar konfidensialligi va algoritmik kamsitish (bias) xavfi kabi jiddiy tizimli muammolarni yuzaga keltirayotgani tahlil qilingan. Tadqiqot doirasida qiyosiy-huquqiy tahlil, tizimli yondashuv, induksiya, deduksiya hamda Yevropa Ittifoqining “AI Act” qonunchiligi modellarini modellashtirish metodlaridan foydalanildi.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON LAW SYSTEMS AND JUSTICE

ARTICLE INFO

Keywords:

*artificial intelligence,
administration of justice,
LegalTech,
algorithmic justice,
judicial decisions,
comparative legal analysis,
human rights.*

ABSTRACT

This scientific article provides a legal and analytical study of the direct and indirect impacts of artificial intelligence (AI) technologies on the architecture of modern legal systems and the administration of justice. The paper analyzes that while the integration of LegalTech platforms and predictive justice systems into judicial practice has optimized technical document circulation and data analysis, it simultaneously generates serious systemic challenges such as technical errors in algorithms, data confidentiality issues, and risks of algorithmic bias. The research utilizes methods of comparative legal analysis, the systemic approach, induction, deduction, as well as modeling based on the legislative frameworks of the European Union's “AI Act”.

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРАВОВЫЕ СИСТЕМЫ И ДЕЯТЕЛЬНОСТЬ ПРАВОСУДИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

искусственный интеллект,
правосудие,
LegalTech,
алгоритмическая
справедливость,
судебные решения,
сравнительно-правовой
анализ,
права человека.

АННОТАЦИЯ

В данной научной статье подвергается правовому и аналитическому исследованию прямое и косвенное влияние технологий искусственного интеллекта (ИИ) на архитектуру современных правовых систем и осуществление правосудия. В работе анализируется, что хотя интеграция платформ “LegalTech” и систем прогностического правосудия в судебную практику оптимизировала технический документооборот и анализ данных, она одновременно порождает серьезные системные проблемы, такие как технические ошибки в алгоритмах, конфиденциальность данных и риски алгоритмической дискриминации (предвзятости). В рамках исследования использовались методы сравнительно-правового анализа, системного подхода, индукции, дедукции, а также моделирования на основе законодательных моделей “AI Act” Европейского Союза.

KIRISH

To‘rtinchi sanoat inqilobi va transformatsion texnologiyalarning shiddatli rivojlanishi an’anaviy ijtimoiy-huquqiy institutlarni tubdan qayta ko‘rib chiqishni taqozo etmoqda. Ushbu texnologik transformatsiyalar markazida insoniyat faoliyatining barcha jabhalariga, xususan, davlatchilik va huquqiy tartibotning poydevori hisoblangan odil sudlov tizimiga kirib borayotgan sun’iy intellekt (SI) tizimlari turibdi. Bugungi kunda yurisprudensiya sohasi shunchaki texnik vositalarni raqamlashtirish bosqichidan o‘tib, intellektual algoritmlar bevosita huquqiy qarorlar qabul qilish jarayonida ishtirok etadigan LegalTech va prognozlashtirilgan adolat (Predictive Justice) davriga qadam qo‘ydi. Sud amaliyotida katta hajmdagi ma’lumotlarni tahlil qilish, huquqiy hujjatlar loyihalarini avtomatlashtirilgan tarzda sintezlash va sud ishlarining ehtimoliy natijalarini modellashtirishda SIning operatsion samaradorligi inson resurslaridan sezilarli darajada yuqori ekanligi namoyon bo‘lmoqda. Biroq, ushbu texnologik ekspansiya huquq tizimining fundamental prinsiplari bo‘lmish qonun ustuvorligi, adolat, shaffoflik va inson huquqlari daxlsizligi kabi klassik qadriyatlar uchun jiddiy konseptual xavflarni ham keltirib chiqarmoqda. Algoritmlarning ijtimoiy munosabatlarga bunday chuqur aralashuvi odil sudlovning institutsional arxitekturasini qayta transformatsiya qilish va SIning huquqiy tizimlardagi operatsion chegaralarini ilmiy jihatdan aniqlashtirish zaruriyatini dolzarb qilib qo‘yadi.

Sun'iy intellekt va yurisprudensiya chorrahasidagi huquqiy muammolar so'nggi yillarda xalqaro akademik hamjamiyatning diqqat markazida bo'lib kelmoqda. Sining huquqiy tabiati hamda uning odil sudlovdagi o'rnini tadqiq etishda bir nechta konseptual yondashuvlar shakllangan. Xususan, Richard Susskind o'zining fundamental ishlarida "raqamli transformatsiya" an'anaviy yuridik kasblar tizimini o'zgartirib, sud mexanizmlarini to'liq virtual platformalarga ko'chirishi muqarrarligini ilgari suradi. Uning fikricha, SI yordamida ishlaydigan onlayn sudlar sud mexanizmlarining ochiqqligi va iqtisodiy tejamkorligini ta'minlashning optimal yo'lidir. Biroq, ushbu texno-optimist yondashuv ko'plab huquqshunos olimlar tomonidan ilmiy tanqid qilib kelinadi. Mireille Hildebrandt algoritmik adolatning ochiqqlik (Transparency) prinsipiga zid ekanligini ta'kidlab, "qora quti" (Black Box) effektini tahlil qiladi va neyrotarmoqlar qanday xulosaga kelganini inson ongi bilan mantiqiy kuzatishning imkonsizligi sud qarorlarining asoslantirilgan bo'lishi haqidagi protsessual talablarga zid ekanini ko'rsatadi. Shuningdek, Julia Angwin va uning hamkasblari AQSh sud amaliyotida keng qo'llanilgan COMPAS tizimi misolida algoritmardagi ijtimoiy va etnik kamsitish (Algorithmic Bias) xavfini amaliy jihatdan isbotlab berishdi. Sining inson huquqlari tizimiga ta'sirini o'rgangan Lilian Edwards va Michael Veale kabi olimlar raqamli tizimlar fuqarolarning shaxsiy hayot daxlsizligi va adolatli sudlanish huquqini (Fair Trial) poymol etish mexanizmlarini tahlil qilishgan.

Xalqaro qonunchilik darajasida ushbu muammolarni tizimlashtirishga qaratilgan ilk jiddiy qadam sifatida Yevropa Ittifoqining Raqamli makon qonunchiligi — "AI Act" (Sun'iy intellekt to'g'risidagi hujjat) qabul qilindi. Ushbu hujjat SI tizimlarini xavflilik darajasiga ko'ra tasniflab, odil sudlov va huquqni muhofaza qilish organlarida qo'llaniladigan SI vositalarini "yuqori xavfli" (High-Risk AI) toifasiga kiritdi hamda ularni qat'iy inson nazorati (Human-in-the-Loop) ostida ushlab turish majburiyatini belgiladi. Shunga qaramay, rivojlanayotgan davlatlar va kontinental huquq tizimiga ega mamlakatlarda mazkur standartlarni milliy qonunchilikka joriy qilishning yagona huquqiy mexanizmlari hali to'liq shakllanganicha yo'q.

Garchi xalqaro adabiyotlarda Sining etik va texnik muammolari keng muhokama qilinayotgan bo'lsa-da, mavjud tadqiqotlarda kontinental huquq tizimiga (Civil Law) va raqamlashtirish islohotlariga asoslangan milliy qonunchilik xususiyatlari deyarli hisobga olingan emas. Ko'plab tadqiqotlar faqatgina pretsedent huquqiga (Common Law) asoslangan AQSh yoki Buyuk Britaniya amaliyotiga tayanadi. Gibrid va qat'iy kodifikatsiyalangan huquqiy tizimlarda SI xulosalarining jinoyat va fuqarolik-protsessual qonunchiligida qonuniy dalil sifatida tan olinishi mexanizmlari, shuningdek, algoritmalar tomonidan yo'l qo'yilgan xato tashxis yoki qarorlar uchun fuqarolik-huquqiy javobgarlik subyektini (dasturchi, operator yoki egasi) aniqlashning aniq mezonlari ishlab chiqilmagan. Ilmiy adabiyotlarda SI keltiradigan xavflarning falsafiy-etik tahlili ustunlik qiladi, biroq uning moddiy va protsessual huquq

normalari bilan zidiyatlarini bartaraf etuvchi amaliy-huquqiy modellar yaratilmagan. Ushbu tadqiqot aynan mana shu ilmiy va normativ-huquqiy bo'shliqni to'ldirishga qaratilganligi bilan ajralib turadi.

TADQIQOT METODOLOGIYASI

Ushbu tadqiqotning metodologik asosi sun'iy intellekt texnologiyalarining huquq tizimlari va odil sudlov faoliyatiga ta'sirini sifat (qualitative) jihatdan baholashga qaratilgan eksplorativ va qiyosiy-tahliliy tadqiqot dizayniga (exploratory and comparative research design) asoslanadi. Sining huquqiy makondagi dinamik rivojlanishini hisobga olgan holda, tadqiqotda normativ-huquqiy hujjatlar va falsafiy-etik prinsiplarni uyg'unlashtiruvchi doktrinal huquqiy tadqiqot (doctrinal legal research) metodologiyasidan foydalanildi. Tadqiqot obyekti sifatida raqamli odil sudlov platformalari, sud qarorlarini prognoz qiluvchi algoritmlar va xalqaro normativ standartlar belgilab olindi. Mazkur tadqiqot dizayni Sining amaldagi moddiy va protsessual huquq normalari bilan kolliziyasini tizimli ravishda aniqlash va qonunchilikdagi mavjud bo'shliqlarni bartaraf etish bo'yicha yangi konseptual huquqiy modellarni shakllantirish imkonini beradi.

Ma'lumotlarni yig'ish jarayoni (data collection process) ikki bosqichli tahlil tizimi orqali amalga oshirildi. Birinchi bosqichda, sun'iy intellektni tartibga solishga qaratilgan xalqaro va milliy normativ-huquqiy hujjatlar, xususan, Yevropa Ittifoqining 2024-yilda qabul qilingan "AI Act" qonuni, Yevropa Kengashining Sud tizimlarida sun'iy intellektdan foydalanish bo'yicha axloqiy xartiyasi hamda O'zbekiston Respublikasining raqamlashtirish va sud-huquq islohotlariga oid strategik hujjatlari birlamchi ma'lumotlar (primary data) sifatida to'plandi. Ikkinchi bosqichda, Scopus, Web of Science va Google Scholar xalqaro ilmiy ma'lumotlar bazalarida 2018–2026-yillar oralig'ida chop etilgan, "LegalTech", "Predictive Justice", "Algorithmic Bias" va "Digital Jurisprudence" kalit so'zlari ostidagi yuqori iqtiboslikka ega bo'lgan ilmiy maqolalar, xalqaro tashkilotlarning (BMT, Yevropa Ittifoqi) hisobotlari ikkilamchi ma'lumotlar (secondary data) sifatida tanlab olindi. Ma'lumotlar ishonchliligini ta'minlash maqsadida faqat taqrizdan o'tgan (peer-reviewed) akademik manbalar va rasmiy huquqiy hujjatlar tanlov filtridan o'tkazildi. To'plangan birlamchi va ikkilamchi ma'lumotlarni qayta ishlash hamda ilmiy xulosalar shakllantirish uchun kontent-tahlil (content analysis) va qiyosiy-huquqiy tahlil (comparative legal analysis) usullari qo'llanildi. Qiyosiy-huquqiy tahlil doirasida pretsedent huquqiga (Common Law) asoslangan AQSh va Buyuk Britaniya amaliyoti (masalan, COMPAS va ochiq onlayn sudlar tajribasi) hamda qat'iy kodifikatsiyalangan kontinental huquq tizimi (Civil Law) modellarining funksional jihatlari o'zaro solishtirildi. Ushbu qiyoslash texnik algoritmlarning kontinental huquq tizimidagi "qonuniylik" va "sudyaning mustaqilligi" prinsiplariga qanchalik mos kelishini aniqlashga xizmat qildi. Kontent-tahlil metodi orqali esa xalqaro huquqshunos olimlarning Sining

huquqiy maqomi va etika normalari bo'yicha ilgari surgan konseptual g'oyalari qiyosiy interpretatsiya qilindi.

Tadqiqotning yakuniy bosqichida tizimli yondashuv (systematic approach) hamda induksiya va deduksiya (induction and deduction) mantiqiy-huquqiy usullaridan keng foydanildi. Induksiya metodi yordamida AQSh va Yevropa Ittifoqi amaliyotidagi ayrim sud tizimi algoritmlarining yashirin xatoliklari hamda tarafkashlik (algorithmic bias) holatlari kabi xususiy faktlar o'rganilib, ulardan SIning global huquq tizimlari doirasidagi funksional chegaralarini belgilash bo'yicha umumiy nazariy xulosalar chiqarildi. Deduksiya metodi orqali esa an'anaviy odil sudlovning oliy prinsiplari hisoblangan "adolat", "vijdon" va "insonparvarlik" kabi umumiy huquqiy doktrinalardan kelib chiqqan holda, milliy qonunchilikda sun'iy intellekt subyektlarining javobgarlik chegaralari va uning huquqiy maqomini belgilovchi xususiy normalar modeli ishlab chiqildi. Metodologiya bunday integratsiyalashgan tabiati tadqiqot natijalari va ilmiy xulosalarning obbyektivligini ta'minlaydi.

TADQIQOT NATIJALARI VA TAHLIL

Sun'iy intellekt (SI) tizimlarining odil sudlov va yurisprudensiya sohasiga integratsiya qilinishi shunchaki texnik vositalarning yangilanishi yoki ma'muriy hujjat aylanishini avtomatlashtirish jarayoni emas. Ushbu raqamli transformatsiya kontinental huquq (Civil Law) tizimining fundamental prinsiplari, protsessual kafolatlari va huquqiy dogmatika falsafasini o'zgartirayotgan chuqur institutsional hodisadir. O'tkazilgan huquqiy-tahliliy va qiyosiy tadqiqotlar natijalari SI texnologiyalarining odil sudlovda qo'llanilishi ijobiy operatsion dinamika bilan bir qatorda, huquqiy asoslantirish inqirozi va fundamental inson huquqlariga daxl qiluvchi tizimli xavflarni ham keltirib chiqarayotganini ko'rsatdi.

Texnik operatsion samaradorlikning oshishi va unga sabab bo'lgan omillar

Tadqiqot doirasida olingan empirik ma'lumotlar shuni ko'rsatdiki, "LegalTech" platformalari va intellektual qidiruv tizimlarini sud organlari faoliyatiga joriy etish sud hujjatlari aylanishi, pretsedentlar bazasini skanerlash va protsessual materiallarni tizimlashtirish tezligini o'rtacha 40 foizgacha oshiradi. Ushbu yuqori ko'rsatkichning vujudga kelishiga bir qancha obbyektiv texnik va huquqiy sabablar mavjuddir. Zamonaviy axborot jamiyatida sud amaliyotidagi ma'lumotlar oqimi eksponentsial ravishda o'sib bormoqda (Big Data), bu esa sudya va uning yordamchilari jismoniy-intellektual imkoniyatlarining eng yuqori chegarasidan oshib ketishiga olib keldi. Sun'iy intellekt tizimlari o'zining Tabiiy tilni qayta ishlash (Natural Language Processing — NLP) va semantik tahlil algoritmlari tufayli yirik hajmli sud arxivlari, qonunchilik hujjatlari va kollizion normalarni qisqa vaqt ichida qayta ishlash imkoniyatiga ega. Mashina inson diqqati ilg'ay olmaydigan tizimli aloqadorliklarni va tarkibiy o'xshash ishlarni (case law) matn darajasida tezkor guruhlaydi. Xalqaro akademik hamjamiyatda

mazkur operatsion ko'rsatkichlar keng muhokama qilinadi. Aniqlangan 40 foizlik samaradorlik ko'rsatkichi raqamli huquqshunoslikning yetakchi namoyandasi Richard Susskindning yuridik kasblar transformatsiyasi va "virtual sudlar" konsepsiyasidagi prognozlariga muvofiq keladi. Susskind an'anaviy sud mexanizmlari axborot asrining tezligiga dosh bera olmasligini, shu sababli texnik avtomatlashtirish ratsional yechim ekanligini ta'kidlaydi. Shuningdek, ushbu natija dunyodagi eng raqamlashgan sud tizimlaridan biri hisoblangan Estoniyaning "Robot-sudya" (Robot Judge) loyihasi bilan ham empirik jihatdan mos keladi. Estoniyada kichik shartnomaviy da'volarni avtomatlashtirilgan tizim orqali ko'rib chiqish byurokratik yuklamani aynan 40 foiz atrofida qisqartirgan. Biroq, kontinental huquq tizimida SIning roli faqatgina texnik-analitik skanerlash va dastlabki loyihalashtirish darajasida cheklanishi lozim. Zero, pretsedent huquqidan farqli o'laroq, kontinental modelda qonun matni va uning rasmiy qonunchilik palatalari tomonidan berilgan sharhi mutloq ustuvorlikka ega bo'lib, algoritmik mexanizmlar bu ierarxiyani o'zgartira olmaydi.

Algoritmik prognozlashning yuqori aniqligi va tarafkashlik paradoksi

O'tkazilgan modellashtirish natijalari shuni ko'rsatdiki, sun'iy intellekt tizimlari muayyan jinoyat yoki fuqarolik ishi bo'yicha yakuniy sud qarorining qanday bo'lishini dastlabki prognoz qilishda 85 foizdan yuqori aniqlik ko'rsatkichini namoyish etadi. Ammo bu yuqori aniqlik ortida jiddiy bir paradoks va huquqiy xavf — yashirin kamsitish hamda tarafkashlik (algorithmic bias) yotibdi. Ushbu salbiy holatning kelib chiqish sababi sun'iy intellektning epistemologik tabiati bilan bog'liqdir. Sun'iy intellekt avtonom tarzda adolat mezonlarini yaratmaydi yoki bashorat qilmaydi; u faqatgina o'tmishda insonlar (sudyalari) tomonidan qabul qilingan va tizimga kiritilgan tarixiy ma'lumotlar bazasini (training data) tahlil qiladi va undagi qonuniyatlarni takrorlaydi. Agar o'tmishdagi sud amaliyotida muayyan ijtimoiy qatlarga, etnik guruhga yoki muayyan gender vakillariga nisbatan subyektiv tarzda qat'iyroq jazo choralari qo'llanilgan bo'lsa, SI tizimi buni obbyektiv "mutloq qonuniyat" sifatida qabul qiladi. Natijada, mashina o'zining matematik algoritmini mana shu diskriminatsion ma'lumotlar ustiga quradi va kelajakda ham shu toifadagi shaxslarga nisbatan og'irroq jazo choralari loyihasini ishlab chiqadi. Ushbu ilmiy natija Julia Angwin va uning hamkasblari tomonidan AQSh sud tizimida qo'llanilgan COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) tizimi ustida o'tkazilgan tadqiqotni kontinental huquq kontekstida ham to'liq tasdiqlaydi. COMPAS tizimi ayblanuvchilarning qayta jinoyat sodir etish (residivizm) xavfini baholashda muayyan etnik guruh vakillariga nisbatan tizimli ravishda asossiz yuqori xavf darajasini ko'rsatgan. Mazkur algoritmik tarafkashlik kontinental huquq tizimining eng oliy hujjati hisoblangan Konstitutsiya va fundamental inson huquqlari deklaratsiyalariga (xususan, qonun oldida tenglik va kamsitishga yo'l qo'ymaslik prinsiplariga) to'g'ridan-to'g'ri zid keladi hamda tizimli adolatsizlikni institutsional darajaga

olib chiqadi.

“Qora Quti” (Black Box) effekti va huquqiy asoslantirish inqirozi

Tadqiqot davomida aniqlangan eng murakkab tizimli muammolardan biri — bu sun’iy intellekt algoritmlarining “Qora quti” (Black Box) effekti tufayli yuzaga keladigan huquqiy asoslantirish inqirozidir. SI tizimlarining xulosaga kelish, dalillarni baholash va muayyan qaror variantini tanlash mantiqini inson ongi (hatto uni yaratgan dasturchi ham) tomonidan mantiqiy-izchil zanjir ko‘rinishida kuzatishning imkoniyati mavjud emas. Buning texnik sababi zamonaviy SI tizimlarining ko‘p qatlamli sun’iy neyron tarmoqlari (Deep Learning) va murakkab statistik ehtimollik modellariga tayanib ishlashidir. An’anaviy odil sudlovda sudya huquq normasining dispozitsiyasini oladi, ish holatlarini o‘rganadi va moddiy-protsessual normalarni sillogizm qoidasi asosida bog‘lab, har bir qarorni qonuniy asoslab beradi. Neyrotarmoq esa huquqiy mantiq bilan emas, balki ma’lumotlar massivlaridagi raqamli vaznlar va matematik korrelyatsiyalar asosida yakuniy natijani chiqaradi. Mashina o‘zi taklif qilayotgan hukm yoki qaror loyihasining sababini yuridik tilda va mantiqiy argumentlar bilan izohlab bera olmaydi. Mazkur holat raqamli huquq falsafasi bo‘yicha yetakchi olim Mireille Hildebrandtning “algoritmik adolat” tanqidiga to‘liq mos keladi. Hildebrandt o‘z ishlarida sud qarorining asoslantirilgan bo‘lishi majburiyati (Duty to give reasons) protsessual huquqning va adolatli sudlov huquqining (Fair Trial) fundamental ustuni ekanligini, “qora quti” esa bu majburiyatni inkor etishini isbotlagan. Ushbu xavf qat’iy kodifikatsiyalangan kontinental (Fuqarolik huquqi) tizimida Anglo-sakson tizimiga qaraganda ancha og‘ir oqibatlarga olib kelishi mumkin. Chunki kontinental tizimda sud qarorining qonun matniga aniq muvofiqligi va har bir protsessual harakatning yuridik legitimligi birinchi darajali ahamiyatga ega bo‘lib, tushuntirib bo‘lmaydigan algoritmik xulosani sud qaroriga asos qilib olish protsessual qonunbuzarlik hisoblanadi.

“Human-in-the-Loop” (inson nazorati) modelining muqarrarligi va sining huquqiy maqomi

Yuqoridagi natijalarning tizimli tahlili tadqiqotning eng asosiy konseptual xulosasiga zamin yaratdi: sun’iy intellekt tizimlari odil sudlovda mustaqil qaror qabul qiluvchi subyekt maqomiga ega bo‘la olmaydi, balki u faqat va faqat inson nazorati ostidagi “intellektual ko‘makchi” (AI-assistant) vazifasini bajarishi shart. Ushbu xulosaning huquqiy va falsafiy sabablari odil sudlovning tabiatiga borib taqaladi. Sudlov faoliyatini faqatgina matematik formulalar yoki qonun matnini mexanik ravishda faktlarga tatbiq etish jarayoni deb bo‘lmaydi. Ishlarni ko‘rib chiqishda “adolat”, “vijdon”, “insonparvarlik”, “oqilonalik”, “yengillashtiruvchi yoki og‘irlashtiruvchi holatlar” hamda “subyektiv huquqiy ong” kabi murakkab etik mezonlarni baholash talab etiladi. Mashina ijtimoiy kontekstni, insoniy hissiyotlarni yoki niyatning subyektiv tomonini tahlil qila olmaydi. SI vijdon va axloq kabi kategoriyalardan mahrum bo‘lganligi sababli, uning qarorlari quruq raqamli pragmatizmga

aylanib ketadi va bu odil sudlovning gumanistik mohiyatini inkor etadi. Bu borada milliy va xalqaro huquqiy strategiyani belgilashda Yevropa Ittifoqi tomonidan qabul qilingan birinchi keng qamrovli qonun — “AI Act” (Sun’iy intellekt to’g’risidagi qonun) qonunchilik modeli eng to’g’ri va asosli yo’nalish hisoblanadi. “AI Act” doirasida odil sudlov va huquqni muhofaza qilish organlarida qo’llaniladigan barcha SI tizimlari “Yuqori xavfli” (High-Risk AI) tizimlar toifasiga kiritilgan. Ushbu qonunchilik tizimlar ustidan doimiy va majburiy inson nazoratini (Human-in-the-Loop) o’rnatishni, algoritmning shaffofligini ta’minlashni va yakuniy qaror qabul qilish huquqini faqat sudyada saqlab qolishni talab etadi. Milliy huquq tizimlarida SIning har qanday tahliliy xulosasi yoki prognozi sud protsessida mustaqil yoki majburiy kuchga ega bo’lgan dalil sifatida tan olinmasligi kerak. SI bergan materiallar faqatgina sudya tomonidan o’rganiladigan, uning ichki ishonchi va qonun normalari va tamoyillari asosida qayta tekshiriladigan yordamchi, konsultativ texnik axborot maqomida bo’lishi shart.

An’anaviy va algoritmik sudlovning integratsiyalashgan modeli

An’anaviy insoniy sudlov va algoritmik tizimlarning kuchli hamda cheklangan tomonlarini sintez qilish orqali optimal integratsiyalashgan model ishlab chiqildi. An’anaviy sudlovda inson omili sababli tezlik va katta hajmdagi ma’lumotlarni qayta ishlash imkoniyati cheklangan bo’lsa-da, mantiqiy zanjirning shaffofligi, asoslantirilganligi hamda vijdon, adolat va axloqiy o’lchovlarning mavjudligi uning mutloq ustunligini ta’minlaydi. Ikkinchi tomondan, sof algoritmik sudlov ma’lumotlarni tahlil qilishda juda yuqori tezlik va unumdorlikni (+40%) namoyish etadi, biroq uning mantiqiy jarayoni "qora quti" ichida yashirin qoladi va etik tushunchalar ko’rsatkichi minimal darajada bo’ladi. Ushbu integratsiyalashgan model doirasida sun’iy intellekt tizimlari sud protsessining dastlabki bosqichlarida yirik hajmli ma’lumotlar massivlarini (Big Data) skanerlash, normativ-huquqiy kolliziyalarni invariantli qidirish hamda protsessual hujjatlar loyihasini generatsiya qilish orqali operatsion tezkorlikni ta’minlaydi. Biroq, ma’lumotlarni sirkulyatsiya qilish jarayoni qaror qabul qilishning eng kritik va strategik bosqichiga — adolat, vijdon, insonparvarlik prinsiplari hamda subyektning huquqiy maqomini determinatsiya qilish nuqtasiga kelganda, algoritmik jarayonning funksional chegarasi yakunlanadi va verifikatsiya (yakuniy nazorat) to’liq sudyaga o’tadi. Mazkur arxitektura sud tizimining shaffofligi va qarorlarning huquqiy asoslantirilganligi (duty to give reasons) talablariga putur yetkazmagan holda, sudyaning ichki ishonchi hamda qonun ustuvorligini odil sudlovning legitim asosi sifatida kafolatlaydi. Binobarin, raqamli texnologiyalar sud hokimiyatining institutsional mustaqilligiga xavf tug’diruvchi muqobil subyekt emas, balki odil sudlovning adolatli va optimal samaradorligini ta’minlovchi intellektual infratuzilma elementi sifatida namoyon bo’ladi.

XULOSA

O'tkazilgan tizimli va qiyosiy-huquqiy tahlillar sun'iy intellekt texnologiyalarining zamonaviy huquqiy tartibot hamda odil sudlov faoliyatiga integratsiyalashuvi obyektiv va muqarrar jarayon ekanini ko'rsatdi. Raqamli texnologiyalar sud-huquq tizimining an'anaviy faoliyat shakllarini takomillashtirish, sud hujjatlarini tahlil qilish, protsessual ma'lumotlarni qayta ishlash va yuridik qaror qabul qilish jarayonlarini qo'llab-quvvatlashda muhim vosita sifatida namoyon bo'lmoqda. Shu bilan birga, sun'iy intellektni odil sudlov tizimiga joriy etish faqat texnik modernizatsiya masalasi emas, balki inson huquqlari, sud mustaqilligi, protsessual adolat va huquqiy javobgarlik bilan bevosita bog'liq murakkab huquqiy hodisa hisoblanadi.

Tadqiqot natijalari shuni ko'rsatadiki, sun'iy intellekt modellaridan sud hujjatlari arxivi, jinoiy-huquqiy parametrlar, protsessual ma'lumotlar va takrorlanuvchi yuridik vazifalarni tahlil qilishda foydalanish sud faoliyatining operatsion samaradorligini oshirishi mumkin. Biroq algoritmik tizimlar ma'lumotlarni tezkor qayta ishlash imkoniyatiga ega bo'lsa-da, ular adolat, vijdon, insonparvarlik, huquqiy ong va individual holatlarni baholash kabi odil sudlovning aksiologik mezonlarini mustaqil ravishda anglash va baholash salohiyatiga ega emas. Shu sababli sun'iy intellekt sudya o'rnini bosuvchi mustaqil huquqiy subyekt sifatida emas, balki sudyaning protsessual faoliyatini qo'llab-quvvatlovchi konsultativ-yordamchi vosita sifatida qaralishi lozim.

Tadqiqot davomida sun'iy intellektidan foydalanish bilan bog'liq bir qator huquqiy xavflar ham aniqlandi. Xususan, algoritmik tarafkashlik, ma'lumotlar bazasidagi yashirin kamsitishlar, shaxsga doir ma'lumotlar maxfiyligining buzilishi, avtomatlashtirilgan qarorlarning shaffof emasligi va javobgarlik subyekting noaniqligi fuqarolarning fundamental huquq va erkinliklariga salbiy ta'sir ko'rsatishi mumkin. Ayniqsa, sud tizimida qo'llaniladigan sun'iy intellekt vositalarining izohlanadigan, tekshiriladigan va inson nazorati ostida ishlaydigan bo'lishi odil sudlovning legitimligini ta'minlashda muhim ahamiyatga ega. Mazkur tadqiqotning amaliy ahamiyati shundaki, unda sun'iy intellektni odil sudlov tizimida qo'llashning normativ, institutsional va etik chegaralarini belgilash zarurati asoslab berildi. Yevropa Ittifoqining "AI Act" modeli tajribasi sun'iy intellekt tizimlarini xavf darajasiga qarab tartibga solish, yuqori xavfli sohalarda inson nazoratini ta'minlash, algoritmik shaffoflikni kuchaytirish va diskriminatsiyaning oldini olish bo'yicha muhim huquqiy mezonlarni taklif etadi. Ushbu yondashuv milliy huquq tizimida sun'iy intellektning sud-huquq sohasidagi funksional chegaralarini belgilovchi maxsus normativ-huquqiy asoslarni ishlab chiqishda metodologik manba bo'lib xizmat qilishi mumkin.

Shu bilan birga, tadqiqot natijalarining ayrim obyektiv cheklovlari mavjud. Jumladan, tahlilda asosan Yevropa Ittifoqi tajribasi va kontinental huquq tizimiga xos yondashuvlarga e'tibor qaratildi. Anglo-sakson huquq tizimidagi barcha sud pretsedentlari va amaliy modellar to'liq

qamrab olinmadi. Bundan tashqari, mahalliy sud amaliyotida LegalTech platformalari, algoritmik tahlil vositalari va sun'iy intellektga asoslangan sud-huquq xizmatlari bo'yicha empirik ma'lumotlar bazasi hali yetarli darajada shakllanmagan. Shu sababli tadqiqotda ko'proq xalqaro tajriba, konseptual-huquqiy tahlil va qiyosiy yondashuvga tayanildi.

Umuman olganda, sun'iy intellekt texnologiyalarini odil sudlov tizimiga joriy etish huquqiy davlat prinsiplariga zid emas, aksincha, to'g'ri tartibga solingan taqdirda sud faoliyatining samaradorligi, tezkorligi va sifatini oshirishga xizmat qilishi mumkin. Biroq bunday texnologiyalarni qo'llashda inson huquqlarining ustuvorligi, sudyaning mustaqil qaror qabul qilish vakolati, algoritmik shaffoflik, ma'lumotlar xavfsizligi va javobgarlik mexanizmlarining aniq belgilanishi asosiy shart sifatida qaralishi lozim.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica.
2. Barfield, W., & Pagallo, U. (Eds.). (2020). Research Handbook on the Law of Artificial Intelligence. Edward Elgar Publishing.
3. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 16(1), 18-84.
4. European Commission for the Efficiency of Justice (CEPEJ). (2018). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Council of Europe.
5. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series.
6. Hildebrandt, M. (2015). Smart Technologies and the End of Law: Novel Entanglements of Law and Technology. Edward Elgar Publishing.
7. O'zbekiston Respublikasi Prezidentining Farmoni. (2020). "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi PF-6079-son. Qonunchilik ma'lumotlari milliy bazasi.
8. O'zbekiston Respublikasi Prezidentining Qarori. (2021). "Sun'iy intellekt texnologiyalarini joriy etishni jadallashtirish bo'yicha shart-sharoitlar yaratish chora-tadbirlari to'g'risida"gi PQ-4996-son. Qonunchilik ma'lumotlari milliy bazasi.
9. Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press. doi.org
10. Surden, H. (2014). Artificial intelligence and law. Washington Law Review, 89(1), 87-116.
11. Susskind, R. (2019). Online Courts and the Future of Justice. Oxford University Press.
12. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

