KIBERXAVFSIZLIK, SUN'IY INTELLEKT VA KATTA HAJMDAGI MA'LUMOTLAR (BIG DATA)

Salomova Zaynab Jamol qizi
Buxoro soliq texnikumi o'qituvchisi

Annotatsiya: *Ushbu maqolada kiberxavfsizlik, sun'iy intellekt (AI) va katta hajmdagi ma'lumotlar (Big Data) o'rtasidagi o'zaro bog'liqlik hamda ularning zamonaviy axborot texnologiyalari tizimidagi o'rni ilmiy tahlil qilinadi. Raqamli transformatsiya sharoitida axborot resurslarining xavfsizligi, ma'lumotlarni himoya qilish, shuningdek, sun'iy intellekt vositalaridan foydalangan holda kiber tahdidlarga qarshi kurashish masalalari dolzarb ahamiyat kasb etmoqda. Maqolada Big Data tahlil texnologiyalari, mashinaviy o'qitish algoritmlari va neyron tarmoqlar yordamida xavfsizlik tizimlarini avtomatlashtirishning samaradorligi yoritilgan. Shu bilan birga, kiberxavfsizlikning huquqiy, texnik va axloqiy jihatlari, ma'lumotlar maxfiyligini saqlash va intellektual tizimlarning xavfsiz integratsiyasi bo'yicha ilmiy yondashuvlar tahlil etiladi.*

Kalit so'zlar: *kiberxavfsizlik, sun'iy intellekt, Big Data, mashinaviy o'qitish, ma'lumotlar tahlili, raqamli xavfsizlik, axborot tizimlari, texnologik xavf.*

Аннотация: *В статье рассматриваются взаимосвязь и роль кибербезопасности, искусственного интеллекта (AI) и больших данных (Big Data) в современных информационно-технологических системах. В условиях цифровой трансформации особое значение приобретают вопросы защиты информации, обеспечения конфиденциальности данных и применения интеллектуальных технологий для противодействия киберугрозам. В работе анализируется эффективность автоматизации систем безопасности с использованием методов машинного обучения, нейронных сетей и технологий анализа больших данных. Кроме того, рассматриваются правовые, технические и этические аспекты кибербезопасности, а также подходы к безопасной интеграции интеллектуальных систем.*

Ключевые слова: *кибербезопасность, искусственный интеллект, Big Data, машинное обучение, анализ данных, цифровая безопасность, информационные системы, технологические риски.*

Abstract: *This article explores the interconnection and role of cybersecurity, artificial intelligence (AI), and big data in modern information technology systems. In the era of digital transformation, ensuring data security, privacy protection, and the use of intelligent technologies to counter cyber threats have become critical issues. The study highlights the effectiveness of automating security systems through machine learning algorithms, neural networks, and big data analytics. Furthermore, it analyzes the legal, technical, and ethical aspects of cybersecurity, emphasizing secure integration of AI-based systems and protection of sensitive information.*

Keywords: *cybersecurity, artificial intelligence, Big Data, machine learning, data analytics, digital security, information systems, technological risk.*

KIRISH

XXI asrda raqamli texnologiyalar insoniyat hayotining barcha sohalarini tubdan o‘zgartirdi. Axborot texnologiyalarining jadal rivojlanishi natijasida sun’iy intellekt (AI), katta hajmdagi ma’lumotlar (Big Data) va kiberxavfsizlik masalalari global miqyosda strategik ahamiyat kasb etmoqda. Ushbu uch yo‘nalish bir-biri bilan uzviy bog‘liq bo‘lib, zamonaviy axborot jamiyatining asosiy tayanch ustunlariga aylanmoqda. Har bir sohada — davlat boshqaruvi, moliya, ta’lim, tibbiyot, transport, sanoat va mudofaa tizimlarida — sun’iy intellekt algoritmlari va Big Data tahlili yordamida katta hajmdagi ma’lumotlar qayta ishlanmoqda. Shu bilan birga, raqamli infratuzilmaning kengayishi va ma’lumotlarning markazlashuvi bilan bog‘liq kiberxavf tahdidlari ham ortib bormoqda.

Bugungi global axborot makonida kiberxavfsizlik masalasi milliy xavfsizlik darajasidagi muhim strategik vazifalardan biriga aylangan. Chunki har kuni milliardlab ma’lumotlar internet orqali almashinmoqda, ularning aksariyati shaxsiy, tijorat yoki davlat sirlariga tegishli. Shunday sharoitda sun’iy intellekt texnologiyalarini kiberxavfsizlik tizimlariga tatbiq etish, ya’ni intellektual xavfsizlik algoritmlarini yaratish, avtomatik aniqlash va bashorat qilish modellarini ishlab chiqish dolzarb ehtiyoj sifatida yuzaga chiqmoqda.

Sun’iy intellekt yordamida kiberxavfsizlikni ta’minlashning afzalliklaridan biri — u inson omiliga nisbatan tezkorroq, aniqroq va barqaror ishlashidir. AI tizimlari real vaqt rejimida tarmoqdagi g‘ayrioddiy faoliyatni aniqlay oladi, xakerlik urinishlarini prognozlaydi va avtomatik tarzda qarshi choralar ko‘radi. Shu jarayonda Big Data tahlil texnologiyalari hal qiluvchi ahamiyatga ega bo‘ladi, chunki xavfsizlik tizimlari son-sanoqsiz loglar, signallar va tranzaktsiyalarni qayta tahlil qilib, xavfga oid “patronlarni” aniqlaydi.

Katta hajmdagi ma’lumotlar (Big Data) konsepsiyasi o‘z mohiyatiga ko‘ra ma’lumotlarning hajmi, tezligi va xilma-xilligiga asoslanadi (“3V” modeli — Volume, Velocity, Variety). Bu ma’lumotlar ichida foydali va xavfli signallarni ajratish, kiberxavfsizlikka tahdid soluvchi xatti-harakatlarni aniqlash uchun sun’iy intellekt algoritmlaridan — xususan, mashinaviy o‘qitish (machine learning), chuqur o‘rganish (deep learning) va neyron tarmoqlar (neural networks) texnologiyalaridan foydalanish zarur bo‘ladi.

Ammo kiberxavfsizlik va sun’iy intellekt o‘rtasidagi o‘zaro integratsiya nafaqat texnik, balki axloqiy, huquqiy va falsafiy masalalarni ham kun tartibiga olib chiqmoqda. Masalan, intellektual tizimlarning qaror qabul qilish jarayonidagi shaffoflik, inson huquqlarini himoya qilish, maxfiylik va ma’lumotlarni noqonuniy qayta ishlash muammolari hozirgi kunda eng dolzarb mavzulardan biridir. AI tizimlari inson qarorlarini avtomatlashtirgan sari, axborot xavfsizligi bilan bog‘liq mas’uliyat va ishonch muammolari yanada murakkablashmoqda.

Shuningdek, “raqamli suverenitet” va “axborot mustaqilligi” tushunchalari bugungi global raqobat davrida kiberxavfsizlikning geosiyosiy o‘lchamiga e’tibor qaratishni taqozo etmoqda. Dunyoda kiberxavfsizlik infratuzilmasini AI va Big Data asosida mustahkamlashga oid siyosiy strategiyalar shakllanmoqda. Masalan, Yevropa Ittifoqining “Cyber Resilience Act” qonuni, AQShning “AI Cyber Defense Initiative” dasturi va Xitoyning “Data Security Law” siyosati bu yo‘nalishda yirik davlatlarning manfaatlarini ifodalaydi.

O‘zbekiston Respublikasi ham raqamli xavfsizlik masalalarini ustuvor yo‘nalish sifatida belgilagan. “Raqamli O‘zbekiston – 2030” strategiyasi, “Axborot xavfsizligi to‘g‘risida”gi Qonun hamda kiberxavfsizlikni ta’minlash bo‘yicha milliy konsepsiyalar ushbu yo‘nalishda tizimli yondashuvni shakllantirmoqda. Bu jarayonda milliy sun’iy intellekt tizimlarini rivojlantirish, katta ma’lumotlarni qayta ishlash markazlarini tashkil etish va ularni kiberxavfsizlik standartlari asosida himoyalash dolzarb vazifa sifatida e’tirof etilmoqda.

Xulosa qilib aytganda, kiberxavfsizlik, sun’iy intellekt va katta hajmdagi ma’lumotlar o‘rtasidagi integratsiya — bu nafaqat texnologik yangilik, balki global axborot jamiyatining yangi sivilizatsion bosqichidir. U insoniyatning raqamli xavfsizligi, iqtisodiy barqarorligi va ilmiy taraqqiyoti uchun asosiy tayanchlardan biriga aylanmoqda. Shu sababli ushbu maqolada kiberxavfsizlik va sun’iy intellekt o‘zaro ta’sirining ilmiy asoslari, Big Data tahlilining ahamiyati, ularning qo‘shma qo‘llanishi natijasida yuzaga kelayotgan yangi imkoniyatlar va xavf-xatarlar keng ilmiy nuqtayi nazardan tahlil qilinadi.

ASOSIY QISM

Raqamli davrda kiberxavfsizlik nafaqat texnik muammo, balki global ijtimoiy-iqtisodiy, siyosiy va axloqiy masalaga aylangan. Internet tarmoqlarining kengayishi, “Internet of Things” (IoT) texnologiyalarining rivojlanishi va raqamli xizmatlarning ko‘payishi natijasida ma’lumotlar hajmi keskin oshdi, shu bilan birga kiberjinoyatlar, xakerlik hujumlari va ma’lumotlar o‘g‘irlanishi holatlari ham ortmoqda.

Kiberxavfsizlik tizimining asosiy maqsadi — axborot resurslarini himoya qilish, ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdir (CIA triadasi: Confidentiality, Integrity, Availability). Biroq, an’anaviy xavfsizlik yondashuvlari zamonaviy kiber tahdidlar hajmi va murakkabligiga qarshi yetarli emas. Shu sababli so‘nggi yillarda kiberxavfsizlik sohasida sun’iy intellekt va katta ma’lumotlar tahlili (Big Data Analytics) texnologiyalarini qo‘llash zarurati paydo bo‘ldi.

Sun’iy intellekt kiberxavfsizlikda “proaktiv himoya” konsepsiyasini joriy etadi. Bu degani — tizimlar nafaqat mavjud tahdidlarga javob beradi, balki ularni oldindan aniqlash va bashorat qilish imkoniyatiga ega bo‘ladi.

AI asosidagi xavfsizlik algoritmlari quyidagi yo‘nalishlarda samarali qo‘llanmoqda:

 Intrusion Detection Systems (IDS) va Anomaly Detection texnologiyalari orqali tarmoqdagi g‘ayritabiiy xatti-harakatlarni real vaqt rejimida aniqlash;

 Mashinaviy o‘qitish (Machine Learning) yordamida phishing, spam va zararli dasturlarni avtomatik aniqlash;

 Neyron tarmoqlar (Neural Networks) asosida foydalanuvchi xulq-atvori (User Behavior Analytics – UBA) ni kuzatish va xavfli naqshlarni (pattern) tahlil qilish;

 Natural Language Processing (NLP) yordamida kiberhujum ssenariylarini matnli ma’lumotlardan avtomatik aniqlash.

Sun’iy intellekt asosida ishlovchi xavfsizlik tizimlari inson omilini kamaytiradi, tezkor javob choralarini avtomatlashtiradi hamda kiberhujumlarning ilgari noma’lum turlarini aniqlash imkonini beradi.

Katta hajmdagi ma’lumotlar (Big Data) kiberxavfsizlik uchun asosiy “yoqilg‘i” hisoblanadi. Har kuni milliardlab log fayllar, tranzaktsiyalar, tarmoq signallari va foydalanuvchi harakatlari haqidagi ma’lumotlar to‘planadi. Ushbu ma’lumotlarning tahlili quyidagi imkoniyatlarni yaratadi:

 Xavfli tendensiyalarni erta aniqlash va ularga nisbatan profilaktik choralar ko‘rish;

 Xakerlik hujumlarining statistik naqshlarini aniqlash;

 Real vaqt rejimida tahdidlarni kuzatish va javob berish mexanizmlarini ishlab chiqish;

 Ma’lumotlarning buzilishi, soxtalashtirilishi yoki noqonuniy tarqalishini tezda aniqlash.

Big Data tahlilida Hadoop, Spark, TensorFlow, Elasticsearch kabi texnologiyalar keng qo‘llanmoqda. Ular AI tizimlariga tarmoqlardagi millionlab ma’lumotlarni bir zumda qayta tahlil qilish imkonini beradi.

Kiberxavfsizlikda sun’iy intellekt va Big Data integratsiyasi yangi avlod intellektual xavfsizlik tizimlarini (Intelligent Security Systems) yaratish imkonini berdi. Bunday tizimlarda AI algoritmlari Big Data oqimlaridan o‘z-o‘zidan o‘rganadi, xatti-harakat naqshlarini tahlil qiladi va o‘zini yangilab boradi.

Masalan, “Darktrace”, “Cylance”, “CrowdStrike” kabi tizimlar real vaqt rejimida o‘z-o‘zidan o‘rganish asosida xavfli faoliyatni aniqlaydi.

Shuningdek, “Predictive Cyber Defense” konsepsiyasi — ya’ni xavfsizlik tahdidlarini bashorat qilish texnologiyasi — bugungi kunda ilg‘or davlatlarda keng joriy etilmoqda. Bu yondashuvda AI tizimi har bir tahdidga moslashuvchan qaror qabul qiladi, xavfsizlik siyosatini dinamik ravishda yangilaydi.

AI va Big Data texnologiyalarini kiberxavfsizlikda qo‘llash bilan bir qatorda, yangi muammolar ham yuzaga kelmoqda. Jumladan:

 Maxfiylik (Privacy) – katta hajmdagi ma’lumotlarni tahlil qilish jarayonida shaxsiy axborotlar sir saqlanishi kafolatlanishi lozim;

 Mas’uliyat (Accountability) – sun’iy intellekt noto‘g‘ri qaror qabul qilganda, buning uchun kim javobgar bo‘lishi masalasi hali to‘liq hal etilmagan;

 Axloqiy me’yorlar (Ethical AI) – kiberxavfsizlikda ishlatilayotgan algoritmlar diskriminatsiya, manipulyatsiya yoki siyosiy nazorat vositasiga aylanmasligi zarur;

 Huquqiy moslik (Legal Compliance) – xalqaro huquq me’yorlari (masalan, GDPR) asosida ma’lumotlarni qayta ishlash va himoya qilish normalariga amal qilinishi shart.

Bu masalalar ilmiy jamoatchilik va xalqaro tashkilotlar tomonidan chuqur muhokama qilinmoqda. UNESCO, ITU, va OECD kabi tashkilotlar sun’iy intellektdan mas’uliyatli foydalanish bo‘yicha global standartlarni ishlab chiqmoqda.

O‘zbekiston Respublikasi so‘nggi yillarda raqamli xavfsizlik sohasida tizimli islohotlarni amalga oshirmoqda. “Raqamli O‘zbekiston – 2030” strategiyasi, “Axborot xavfsizligi to‘g‘risida”gi Qonun, shuningdek, “Sun’iy intellektni rivojlantirish konsepsiyasi” bu yo‘nalishdagi muhim qadamdir.

Davlat organlari, bank tizimi, telekommunikatsiya, ta’lim va sog‘liqni saqlash tarmoqlarida axborot xavfsizligini ta’minlash uchun AI asosidagi monitoring tizimlari joriy etilmoqda. “UZCERT”, “Cyber Security Center” va boshqa milliy tashkilotlar Big Data tahliliga asoslangan xavfsizlik arxitekturalarini ishlab chiqmoqda.

Kelgusida quyidagi yo‘nalishlar O‘zbekiston uchun ustuvor bo‘lishi mumkin:

- Milliy sun’iy intellekt asosidagi kiberxavfsizlik platformasini yaratish;
- Katta ma’lumotlar markazlarida (Data Center) xavfsizlik siyosatini kuchaytirish;
- Raqamli ma’lumotlarni himoya qilish bo‘yicha xalqaro sertifikatlash tizimlarini joriy etish;
- Axloqiy AI va “Explainable AI” (tushuntiriladigan sun’iy intellekt) tamoyillarini amaliyotga tatbiq etish.

Kiberxavfsizlik, sun’iy intellekt va Big Data texnologiyalarining integratsiyasi axborot xavfsizligini ta’minlashda yangi davrni boshlab berdi. Bu yondashuv texnik jihatdan murakkab bo‘lsa-da, u insoniyatning raqamli makondagi barqarorligiga xizmat qiladi. AI tizimlari yordamida tarmoqdagi tahdidlarni erta aniqlash, Big Data orqali ularni statistik tahlil qilish va avtomatik javob choralarini ishlab chiqish kiberxavfsizlikni sifat jihatdan yangi bosqichga olib chiqmoqda.

Ammo texnologik imkoniyatlar bilan bir qatorda, bu sohada axloqiy va huquqiy me’yorlarni takomillashtirish, ma’lumotlar suverenitetini ta’minlash va inson huquqlarini himoya qilish ham muhim ahamiyat kasb etadi.

XULOSA

Sun’iy intellekt (AI), katta hajmdagi ma’lumotlar (Big Data) va kiberxavfsizlik o‘zaro chambarchas bog‘liq uch yo‘nalish bo‘lib, ularning integratsiyasi raqamli davrning eng muhim strategik vazifasiga aylandi. XXI asr texnologik inqilobining asosi hisoblangan bu konsepsiyalar axborot jamiyatining barqaror rivojlanishi, milliy xavfsizlikni ta’minlash, iqtisodiyotning raqamli sektorlari va inson faoliyatining deyarli barcha sohalarida tub o‘zgarishlar yasamoqda.

Ilmiy tahlillar shuni ko‘rsatadiki, an’anaviy kiberxavfsizlik yondashuvlari endi zamonaviy raqamli tahdidlar oldida yetarli emas. Sun’iy intellekt algoritmlari va Big Data tahlil texnologiyalari asosida qurilgan xavfsizlik tizimlari esa axborot muhitini proaktiv tarzda himoya qilishga, ya’ni kiberxavflarni oldindan aniqlash va bashorat qilishga imkon beradi. Bunday tizimlar inson omilining xatoliklarini kamaytiradi, tarmoqdagi g‘ayritabiiy xatti-harakatlarni tezkorlik bilan aniqlaydi hamda avtomatik qaror qabul

qilish imkoniyatiga ega. Bu jihatdan AI va Big Data kiberxavfsizlikni yangi darajaga — intellektual xavfsizlik bosqichiga olib chiqmoqda.

Big Data texnologiyalari orqali kiberxavfsizlik tizimlari son-sanoqsiz ma’lumotlarni (log fayllar, trafik oqimlari, foydalanuvchi harakatlari) tahlil qilib, tahdidlar naqshini aniqlay oladi. Bu, o‘z navbatida, mashinaviy o‘qitish va chuqur o‘rganish (deep learning) modellarini samarali ishlatish uchun zamin yaratadi. Demak, katta ma’lumotlar tahlili kiberxavfsizlikni sun’iy intellekt bilan birgalikda “avtonom himoya tizimlari” bosqichiga olib chiqmoqda.

Biroq bu integratsiya bilan bir qatorda yangi axloqiy, huquqiy va ijtimoiy muammolar ham yuzaga chiqmoqda. Eng avvalo, ma’lumotlar maxfiyligi, AI qarorlarining shaffofligi va javobgarlik (accountability) masalalari dolzarbdir. Katta hajmdagi ma’lumotlarni qayta ishlashda shaxsiy ma’lumotlarning sir saqlanishi, algoritmik diskriminatsiyaning oldini olish, intellektual tizimlar ustidan insoniy nazoratni saqlab qolish kiberxavfsizlikning yangi axloqiy o‘lchamlarini belgilab bermoqda.

Kiberxavfsizlikda sun’iy intellektdan foydalanish texnik imkoniyatlar bilan cheklanmaydi; bu, avvalo, axborot suvereniteti va milliy raqamli xavfsizlikni ta’minlashga xizmat qiluvchi siyosiy-ijtimoiy masaladir. Dunyodagi ilg‘or davlatlar — AQSh, Xitoy, Yaponiya, Janubiy Koreya va Yevropa Ittifoqi — o‘z milliy AI-kiberxavfsizlik platformalarini yaratib, global raqamli hukmronlik uchun raqobat olib bormoqda. O‘zbekiston uchun ham ushbu yo‘nalishda mustaqil intellektual himoya tizimlarini shakllantirish, mahalliy ma’lumotlar bazalarini milliy himoya standartlari asosida boshqarish dolzarb strategik zaruratdir.

Kiberxavfsizlik, AI va Big Data integratsiyasining amaliy samaradorligi quyidagilarda namoyon bo‘ladi:

1. Xavfsizlik tizimlarining reaktsiya tezligi va aniqlik darajasi ortadi;
2. Tarmoqdagi tahdidlarni real vaqt rejimida bashorat qilish imkoniyati yaratiladi;
3. Ma’lumotlar oqimidan foydali naqshlarni ajratish orqali xavf profilaktikasi kuchayadi;
4. Avtomatlashtirilgan xavfsizlik siyosati inson ishtirokisiz yangilanadi;
5. Kiberhujumlarning iqtisodiy va texnik zararini kamaytirish imkoniyati yaratiladi.

Sun’iy intellekt va Big Data kiberxavfsizlikni avtomatlashtirish bilan birga, uni moslashuvchan (adaptive), bashoratchi (predictive) va mustahkam (resilient) tizimga aylantiradi. Shu bilan birga, insonning intellektual ishtiroki, etik me’yorlar va milliy qonunchilik talablarini muvozanatda saqlash ham muhim ahamiyatga ega.

O‘zbekiston sharoitida bu integratsiyani rivojlantirish uchun quyidagi ilmiy-amaliy chora-tadbirlar zarur:

- Sun’iy intellekt asosidagi milliy kiberxavfsizlik platformalarini ishlab chiqish;
- Katta ma’lumotlar markazlarida ma’lumotlarni saqlash va himoyalashning texnik standartlarini joriy etish;
- Axborot xavfsizligi bo‘yicha AI mutaxassislarini tayyorlash tizimini kuchaytirish;
- AI qarorlarining axloqiy nazorat mexanizmlarini ishlab chiqish;

 Raqamli qonunchilikni xalqaro standartlarga moslashtirish.

Xulosa qilib aytganda, AI, Big Data va kiberxavfsizlik integratsiyasi raqamli jamiyatning barqaror rivojlanishini ta’minlovchi strategik yo‘nalishdir. Bu integratsiya orqali axborot xavfsizligi inson intellektiga tayanadigan himoya tizimidan sun’iy intellekt asosidagi avtonom, o‘zini o‘rganadigan tizimga aylanmoqda. Biroq, bu jarayon faqat texnologik yutuqlar emas, balki ilmiy yondashuv, etik mas’uliyat va global hamkorlikni talab etadi.

Shunday ekan, raqamli asrning muvaffaqiyati kiberxavfsizlikni sun’iy intellekt bilan uyg‘unlashtirish darajasiga bevosita bog‘liqdir — bu esa insoniyatning raqamli kelajagini xavfsiz, barqaror va adolatli shaklda qurishning asosiy kafolatidir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Abdullayev, I. (2023). Sun’iy intellekt texnologiyalarining kiberxavfsizlik tizimidagi qo‘llanilishi. – Toshkent: Fan va taraqqiyot nashriyoti.
2. Ahmedova, D. (2022). Big Data tahlil texnologiyalari va ularning axborot xavfsizligidagi roli. – Samarqand: SamDU nashriyoti.
3. Alimov, Sh. (2021). Axborot xavfsizligi asoslari. – Toshkent: O‘zbekiston Milliy universiteti nashriyoti.
4. Chuvakin, A., Schmidt, C., & Phillips, D. (2020). Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. – Burlington: Syngress Publishing.
5. G‘anieva, M. (2023). Raqamli xavfsizlik va axborot tizimlarini himoyalash strategiyalari. – Toshkent: TDATU nashriyoti.
6. Kaspersky, E. (2022). Global Cybersecurity Trends: Artificial Intelligence and Automation. – London: Routledge.
7. Karimov, A. (2021). Sun’iy intellekt, mashinaviy o‘qitish va axborot tizimlari xavfsizligi. – Toshkent: Ilm ziyo nashriyoti.
8. Nishonov, Z. (2020). Axborot xavfsizligini ta’minlashda zamonaviy texnologiyalar. – Buxoro: BDU nashriyoti.
9. Reimann, M. (2022). AI in Cyber Defense: Machine Learning for Threat Detection and Prevention. – New York: Springer.
10. Yuldashev, S. (2023). Raqamli iqtisodiyot sharoitida kiberxavfsizlik siyosatini shakllantirish muammolari va yechimlari. – Toshkent: TDIU nashriyoti.