

KIBERXAVFSIZLIKNING 21-ASRDAGI O'RNI

THE ROLE OF CYBERSECURITY IN THE 21ST CENTURY

Mo'minov Haydar Muhiddinovich

"Realsoft Academy" MChJ direktori (Ilmiy rahbar)

univorarsa@gmail.com

Ochilboyev Nurillo Nodirjon o'g'li

Toshkent amaliy fanlar universiteti, Axborot xavfsizligi yo'nalishi

ORCID: 0009-0004-7032-6740

nurilloochilboyev@gmail.com

Hamroqulov Behruz Baxtiyor o'g'li

Toshkent amaliy fanlar universiteti, Axborot xavfsizligi yo'nalishi

ORCID: 0009-0009-0056-6956

hamroqulovbehruz41@gmail.com

Annotatsiya: 21-asrda kiberxavfsizlik muhim infratuzilmalar, shaxsiy ma'lu'motlar va milliy xavfsizlikni himoya qilishning asosiy omili sifatida tobora katta ahamiyat kasb etmoqda. Raqamli texnologiyalarning jamiyatning barcha jabhalariga — sog'liqni saqlashdan tortib moliyagacha, davlat boshqaruvidan tortib shaxsiy turmush tarziga — jadal integratsiyalashuvi potentsial kiber tahdidlar manzarasini sezilarli darajada kengaytirdi. Ushbu maqolada texnologik innovatsiyalar va kiberdushmanlarning doimiy murakkablashishi o'rtasidagi dinamik munosabatga e'tibor qaratilgan holda, kiberxavfsizlik muammolarining rivojlanayotgan tabiati o'rganilgan. Tadqiqotda mustahkam mudofaa strategiyalarini ishlab chiqish, xalqaro hamkorlikni kuchaytirish hamda ma'lu'motlar o'g'irlanishi, tizimlar buzilishi va raqamli urushlardan himoyalash uchun ilg'or texnologiyalarga sarmoya kiritishning ahamiyati ta'kidlangan. Joriy tendentsiyalar, amaliy tadqiqotlar va me'yoriy-huquqiy bazalar tahlili asosida kiberxavfsizlik choralarining raqamli asrning murakkab talablariga qanday moslashayotgani ko'rsatilgan va kelajakdagi tadqiqot va siyosat yo'nalishlari belgilangan.

Kalit so'zlar: kiberxavfsizlik, kibertahdidlar, axborot xavfsizligi, raqamli mudofaa, ma'lu'motlarni himoya qilish, kiberbardoshlik, kiberurush, normativ-huquqiy asoslar, texnologik innovatsiyalar, global kiberstrategiya.

Abstract: In the 21st century, cybersecurity has emerged as a fundamental pillar in safeguarding critical infrastructure, personal data, and national security. The rapid integration of digital technologies into all spheres of society — from healthcare to finance, from government operations to individual lifestyles — has substantially expanded the landscape of potential cyber threats. This article examines the evolving nature of cybersecurity challenges, with particular emphasis on the dynamic interplay between technological innovation and the continuously increasing sophistication of cyber adversaries. The study underscores the importance of developing robust defense strategies, fostering international cooperation, and investing in advanced technologies to protect against data breaches, system compromises, and digital warfare. By analyzing current trends, case studies, and regulatory frameworks, the article provides a comprehensive overview of how cybersecurity measures are adapting to the complex demands of the digital era, and identifies future directions for research and policy development.

Keywords: cybersecurity, cyber threats, information security, digital defense, data protection, cyber resilience, cyber warfare, regulatory frameworks, technological innovation, global cyber strategy.

1. Kirish

Kiberxavfsizlik endilikda har bir raqamli tizimning ajralmas tarkibiy qismi bo'lib, zamonaviy aloqa, savdo va infratuzilmaning xavfsizligi va ishonchligini ta'minlashda hal qiluvchi rol o'ynaydi. Raqamli transformatsiya jadallashgani va internetning global miqyosda keng tarqalishi tufayli o'zaro bog'langan tizimlar va infratuzilmalardagi zaifliklar sezilarli darajada oshdi (Singer & Friedman, 2014).

Zamonaviy axborot-kommunikatsiya texnologiyalari va internetning ommalashuvi global miqyosda shaxsiy hayot, iqtisodiyot va milliy xavfsizlik sohalarida tub o'zgarishlarni yuzaga keltirdi. Kiberjinoyatlar — ma'lu'motlar buzilishidan tortib murakkab xakerlik hujumlarigacha — shaxsiy hayot, korporativ faoliyat va davlat xavfsizligiga jiddiy zarar yetkazishi mumkin (Von Solms & Van Niekerk, 2013).

Ushbu maqolaning asosiy maqsadi zamonaviy kiberxavfsizlikka oid dolzarb muammolarni tahlil etish, qo'llanilayotgan metodlarni baholash, real hayotdagi qo'llanilish tajribalarini o'rganish va kelajak istiqbollarini aniqlashdir. Tadqiqot kiberxavfsizlikning 21-asrda texnik, tashkiliy va me'yoriy-huquqiy jihatlarini kompleks tarzda yoritadi.

2. Adabiyotlar sharhi va nazariy asos

Kiberxavfsizlik sohasidagi ilmiy adabiyotlar so'nggi yigirma yilda jadal sur'atda rivojlandi. Von Solms va Van Niekerk (2013) axborot xavfsizligidan kiberxavfsizlikka o'tish jarayonini nazariy jihatdan asoslagan. Kello (2013) kiberinqilob va davlatchilikka oid tahdidlarni xalqaro xavfsizlik nuqtai nazaridan tahlil etgan.

Clarke va Knake (2010) kiberurush muammosini strategik va siyosiy nuqtai nazardan ko'rib chiqqan. Nye (2011) yadroviy xavfsizlikdan kiberxavfsizlikka ko'chirish mumkin bo'lgan saboqlarni o'rgangan. Libicki (2009) kiberto'xtatish va kiberurush nazariyasini tahlil qilib, davlatlar va nodavlat aktoryalarning strategik xatti-harakatlarini o'rgangan.

O'zbekiston kontekstida Jumaev, Normuminov va Primbetov (2023) zamonaviy kiberxavfsizlik usullarini o'rganib, milliy darajadagi xavfsizlik muammolari va yechimlarini tahlil qilgan. Sotvoldiyev, Isaxonov va Siddiqov (2023) axborot aktivlarining kiberxavfsizlikni ta'minlashdagi rolini baholagan. Jabborov va Jabborova (2024) O'zbekistonda axborot xavfsizligi va kiberxurujlarning oldini olishga doir davlat siyosatini o'rganishgan.

3. Tadqiqot metodologiyasi

Ushbu tadqiqot kiberxavfsizlikning 21-asrdagi o'rnini tahlil etish uchun sifatli tahliliy yondashuvga asoslanadi. Tadqiqot dizayni quyidagi elementlarni o'z ichiga oladi:

- Manba bazasi: Ilmiy jurnallar (IEEE, Computers & Security, International Security), sanoat hisobotlari, davlat nashrlari hamda BMT va Jahon Iqtisodiy Forumi kabi xalqaro tashkilotlarning ma'lu'motlari.
- Davr chegarasi: 2000-yildan 2024-yilgacha bo'lgan muddat, 2018-yildan keyingi nashrlar ustuvor hisoblanadi.
- Tahlil usullari: Adabiyotlar sharhi, qiyosiy tahlil, amaliy tadqiqotlarni (case study) o'rganish va tizimli umumlashtirish.
- Etik e'tirof: Tadqiqotda barcha manbalar tegishli ravishda ko'rsatilgan. Shaxslarni aniqlashga imkon beruvchi ma'lu'motlar ishlatilmagan.

4. Natijalar va muhokama

4.1. Kiberxavfsizlikning 21-asrdagi evolyutsiyasi

Kiberxavfsizlikning zamonaviy rivojlanishi 21-asr boshlaridan boshlab jadal sur'atlarda kechdi. Dastlabki yillarda parol asosidagi autentifikatsiya va oddiy xavfsizlik devorlari asosiy

himoya vositasi bo'lgan. Biroq murakkab kiberhujumlarning paydo bo'lishi yangi yondashuvlarni zarur qildi. Sun'iy intellekt va mashinali o'qitish texnologiyalarining joriy etilishi kiberxavfsizlik sohasida tub o'zgarishlarga olib keldi (Jumaev et al., 2023).

1-jadval. Kiberxavfsizlik usullarining samaradorligi taqqoslash

Usul	Samaradorlik darajasi	Asosiy kuchli tomonlari	Asosiy cheklavlari
Parol asosidagi autentifikatsiya	Past	Soddaligi, oson joriy etish	Phishing va brute-force hujumlariga zaif
Xavfsizlik devori (Firewall)	O'rtacha	Tarmoq trafikini nazorat qilish	Bulutli tizimlar va IoT uchun yetarli emas
Ko'p faktorli autentifikatsiya (MFA)	Yuqori	Ruxsatsiz kirishni sezilarli kamaytiradi	Foydalanuvchiga qo'shimcha qadamlar kerak
Mashinali o'qitish modellari	Yuqori	Anomal xatti-harakatlarni avtomatik aniqlash	Katta ma'lu'mot to'plamlari talab qilinadi
Zero-Trust arxitekturasida	Juda yuqori	Ichki xavf-xatarlarni kamaytirish	Murakkab va qimmat joriy etish

4.2. Sun'iy intellektning kiberxavfsizlikdagi o'rni

21-asrning eng muhim yutuqlaridan biri kiberxavfsizlikda sun'iy intellekt va chuqur o'qitish texnologiyalarining joriy etilishidir. Mashinali o'qitish modellari kiberhujumlarni aniqlashda anomal xatti-harakatlarni avtomatik tarzda sezadi va tezkor choralar ko'rishga imkon beradi. Neyron tarmoqlar yordamida potentsial xavf-xatarlarni bashorat qilish va ularga qarshi proaktiv choralar ko'rish imkoniyati yaratilgan (Mustaffaqulov et al., 2024).

Chuqur o'qitish algoritmlari deepfake va ransomware kabi murakkab tahdidlarni aniqlashda yuqori samaradorlik ko'rsatmoqda. Tadqiqotlar shuni ko'rsatadiki, sun'iy intellekt asosidagi tizimlar an'anaviy usullarga nisbatan kiberhujumlarni aniqlashda 40–60% yuqori aniqlik bilan ishlaydi (Jumaev et al., 2023).

4.3. Kiberxavfsizlikning real hayotdagi qo'llanilishi

Kiberxavfsizlik texnologiyalari turli sohalarda amaliy qo'llanilish topmoqda:

- Korxona xavfsizligi: Yirik kompaniyalar ma'lu'motlar bazalarini himoyalash va ichki tarmoqlarga ruxsatsiz kirishning oldini olish uchun bulutli shifrlash va Zero-Trust arxitekturasidan keng foydalanmoqda.
- Davlat idoralari: Muhim infratuzilmalarni — elektr tarmoqlari, suv ta'minoti, moliyaviy tizimlar — kiberhujumlardan himoyalash milliy xavfsizlikning ustuvor yo'nalishiga aylandi (Clarke & Knake, 2010).
- Shaxsiy xavfsizlik: Smartfonlar va moliyaviy ilovalarda biometrik autentifikatsiya (yuzni aniqlash, barmoq izi) shaxsiy ma'lu'motlarni himoyalashning ishonchli usuli sifatida keng tarqaldi.

4.4. Axloqiy va maxfiylik masalalari

Kiberxavfsizlikning rivojlanishi bilan bir qatorda bir qator axloqiy va huquqiy muammolar ham paydo bo'ldi. Sun'iy intellekt tizimlari ba'zan noto'g'ri ma'lumotlar to'plamlariga asoslanib, noto'g'ri qarorlar qabul qilishi mumkin. Bundan tashqari, doimiy monitoring shaxsiy maxfiylikka tahdid solishi va turli mamlakatlar qonunchiligiga moslashish zarurati qo'shimcha murakkabliklarni yuzaga keltiradi (Jabborov & Jabborova, 2024).

5. Cheklovlar

Ushbu tadqiqotning asosiy cheklovlari quyidagilardan iborat. Birinchidan, tadqiqot asosan sifatli yondashuvga asoslanib, miqdoriy tahlil (keng ko'lamli so'rovnoma yoki eksperiment) qo'llanmagan. Shu sababli natijalar umumlashtirishda ehtiyotkorlik talab etiladi. Ikkinchidan, kiberxavfsizlik sohasidagi texnologiyalar juda tez o'zgarib turishi sababli ushbu maqoladagi ayrim xulosalar keyingi yillarda yangi tadqiqotlar bilan to'ldirilishi zarur. Uchinchidan, O'zbekiston va rivojlanayotgan mamlakatlar kontekstidagi ma'lumotlar bazasi rivojlangan davlatlar bilan solishtirganda hali nisbatan cheklangan bo'lib qolmoqda. Kelajakdagi tadqiqotlarda empirik ma'lumotlar to'plash va mintaqaviy tahlilni chuqurlashtirish tavsiya etiladi.

6. Xulosa va takliflar

Kiberxavfsizlik 21-asrda raqamli dunyoning barqarorligi va xavfsizligini ta'minlovchi muhim omil sifatida o'z o'rnini mustahkamladi. Tadqiqot natijalari shuni ko'rsatadiki, dastlabki himoya usullari zamonaviy murakkab kiberhujumlarga qarshi yetarli darajada samarali emasligini isbotladi. Sun'iy intellekt va mashinali o'qitish texnologiyalari kiberxavfsizlik sohasida muhim yutuqlarga erishish imkonini berdi.

Biroq soha rivojlanishida bir qator to'siqlar ham mavjud: malakali mutaxassislar yetishmasligi, yuqori texnologik xarajatlar va doimiy o'zgarib turadigan kiber tahdidlar. Ushbu muammolarni hal etish uchun quyidagi takliflar tavsiya etiladi:

- Sun'iy intellekt, blokcheyn va kvantga chidamli kriptografik texnologiyalarga investitsiyalarni oshirish orqali kiberxavfsizlik infratuzilmasini mustahkamlash.
- Ta'lim tizimida kiberxavfsizlik yo'nalishini kengaytirish va amaliy ko'nikmalarni rivojlantiruvchi o'quv dasturlarini joriy etish.
- Xalqaro hamkorlikni kuchaytirish va bir-birining tajribasidan foydalanish orqali global kibertahdidlarga nisbatan muvofiqlashtirilgan javob mexanizmlarini ishlab chiqish.
- Shaxsiy maxfiylik va ma'lumotlar xavfsizligini ta'minlash maqsadida normativ-huquqiy bazani takomillashtirish va algoritmik adolatlilik tamoyillarini belgilash.

Kiberxavfsizlik doimiy rivojlanish va moslashishni talab qiladi. Kiber tahdidlar tobora murakkablashib borar ekan, ularga qarshi kurash ham yangi innovatsion yondashuvlarni taqozo etadi.

Adabiyotlar ro'yxati

- [1] Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.
- [2] Jabborov, Z. B., & Jabborova, N. B. (2024). O'zbekistonda axborot xavfsizligi va kiberxurujlarning oldini olishga doir davlat siyosati. *Ilm-fan va innovatsiya*, 2(30), 120–122.
- [3] Jumaev, G., Normuminov, A., & Primbetov, A. (2023). Safeguarding the digital frontier: Exploring modern cybersecurity methods. *Journal of Multidisciplinary Bulletin*, 6(4). <https://sirpublishers.org/index.php/jomb/article/view/156>
- [4] Jumaniyazova, T. A. (2024). Oliy ta'lim muassasalarida kiberxavfsizlik madaniyatini oshirish. *Journal of Academic Research and Trends in Educational Sciences*.

- [5] Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138
- [6] Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.
- [7] Mamatqulov, M. M. (2024). Kiber xavfsizlik muammolari va yechimlari. *Ilmiy Xabarlar*, 2(8).
- [8] Mustaffaqulov, M. A., Eshturdiyeva, Z. S., & Abduraximova, R. B. (2024). Ta’im jarayonida kiberxavfsizlikni ta’minlash. *Journal of Academic Research and Trends in Educational Sciences*.
- [9] Muxammadjonov, X. Z. (2024). Madaniyatshunoslik yondashuvi asosida o’smirlarda kiberxavfsizlik tushunchalarini rivojlantirish mexanizmlari. *Universal xalqaro ilmiy jurnal*, 1(5).
- [10] Normo’minov, A. A., Kendjaeva, D. X., & Primbetov, A. M. (2024). Kiberxavfsizlikning ta’im jarayonidagi roli. *Yevroosiyo akademik tadqiqotlar jurnali*, 4(12).
- [11] Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly*, 5(4), 18–38.
- [12] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- [13] Sotvoldiyev, A. A., Isaxonov, X. M., & Siddiqov, M. Y. (2023). Kiberxavfsizlikni ta’minlashda axborot aktiv qiymatining o’rni. *Yangi O‘zbekiston taraqqiyotida tadqiqotlarni o’rni va rivojlanish omillari*, 2(2).
- [14] To’xtasinov, A. R. (2023). O‘zbekiston kiberxavfsizlik taraqqiyoti. *PEDAGOGS jurnali*, 43(1), 180–185.
- [15] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>