ZAMONAVIY IQTISODIYOT VA INTELLEKTUAL TEXNOLOGIYALAR
Ilmiy-uslubiy elektron jurnali — Sharq universiteti
ISSN: 3093-9062 Vol. 1 No. 1 (2026)

RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIKNI TA'MINLASH: AXBOROTNI HIMOYALASH MUAMMOLARI, TAHDIDLARI VA AMALIY YECHIMLAR

Elmurodov Dovud Abdilatif o'g'li,
Kiberxavfsizlik injiniringi yo'nalishi talabasi,
Farg'ona davlat texnika universiteti,
EMAIL: elmurodovdovud2@gmail.com
DOI: https://doi.org/10.66493/h6q7vc94

Annotatsiya: Ushbu maqolada raqamli iqtisodiyotning jadal rivojlanishi sharoitida kiberxavfsizlikni ta'minlash muammolari, zamonaviy tahdidlar va ularni kamaytirishga xizmat qiluvchi amaliy yechimlar tahlil qilinadi. Tadqiqotning maqsadi - axborot resurslari, shaxsiy ma'lumotlar, moliyaviy tranzaksiyalar va raqamli xizmatlar xavfsizligiga ta'sir qilayotgan asosiy omillarni tizimlashtirish hamda ularni boshqarish bo'yicha kompleks yondashuvni taklif etishdir. Maqolada qiyosiy tahlil, tizimli yondashuv, statistik kuzatish natijalarini umumlashtirish va ilmiy adabiyotlarni sharhlash usullaridan foydalanildi. Tahlil natijalari shuni ko'rsatadiki, phishing, ransomware, DDoS, ma'lumotlar sizib chiqishi va IoT muhitidagi zaifliklar iqtisodiy faoliyatning uzluksizligiga, korxonalarning raqobatbardoshligiga hamda fuqarolarning ishonchiga jiddiy zarar yetkazadi. Tadqiqotning ilmiy yangiligi kiberxavfsizlikni faqat texnik masala sifatida emas, balki iqtisodiy barqarorlik, boshqaruv sifati va inson kapitali bilan uzviy bog'liq tizimli omil sifatida talqin etilishidadir. Amaliy ahamiyati sifatida zero trust arxitekturasi, ko'p bosqichli autentifikatsiya, xodimlarni o'qitish, audit, normativ-huquqiy muvofiqlik va riskga asoslangan boshqaruvni birlashtiruvchi model taklif qilinadi.

Аннотация: В статье анализируются проблемы обеспечения кибербезопасности, современные угрозы и практические решения в условиях стремительного развития цифровой экономики. Цель исследования заключается в

© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

систематизации факторов, влияющих на безопасность информационных ресурсов, персональных данных, финансовых транзакций и цифровых сервисов, а также в разработке комплексного подхода к управлению этими рисками. В работе использованы методы сравнительного анализа, системного подхода, обобщения статистических наблюдений и обзора научной литературы. Результаты показывают, что фишинг, ransomware, DDoS-атаки, утечки данных и уязвимости в среде IoT наносят серьёзный ущерб непрерывности хозяйственной деятельности, конкурентоспособности организаций и доверию пользователей. Научная новизна исследования состоит в рассмотрении кибербезопасности не только как технической задачи, но и как системного фактора, тесно связанного с экономической устойчивостью, качеством управления и развитием человеческого капитала. Практическая значимость статьи заключается в предложении модели, объединяющей архитектуру zero trust, многофакторную аутентификацию, обучение персонала, регулярный аудит, нормативно-правовое соответствие и риск-ориентированное управление.

Abstract: This article examines cybersecurity challenges, contemporary threats, and practical countermeasures in the context of the rapid expansion of the digital economy. The purpose of the study is to systematize the main factors affecting the security of information resources, personal data, financial transactions, and digital services, and to propose a comprehensive approach to managing these risks. The research applies comparative analysis, a systems approach, generalization of statistical observations, and a review of scholarly literature. The findings demonstrate that phishing, ransomware, DDoS attacks, data breaches, and vulnerabilities in IoT environments significantly damage business continuity, organizational competitiveness, and public trust. The scientific novelty of the paper lies in interpreting cybersecurity not merely as a technical issue, but as a systemic factor closely related to economic resilience, governance quality, and human capital development. The practical contribution of the

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

study is a model that integrates zero trust architecture, multi-factor authentication, employee awareness training, regular security audits, legal compliance, and risk-based governance.

Kalit so‘zlar: kiberxavfsizlik, raqamli iqtisodiyot, axborot xavfsizligi, kibertahdidlar, phishing, ransomware, DDoS, IoT xavfsizligi, zero trust, ma’lumotlar himoyasi, risklarni boshqarish, raqamli infratuzilma.

Ключевые слова: кибербезопасность, цифровая экономика, информационная безопасность, киберугрозы, фишинг, ransomware, DDoS, безопасность IoT, zero trust, защита данных, управление рисками, цифровая инфраструктура.

Keywords: cybersecurity, digital economy, information security, cyber threats, phishing, ransomware, DDoS, IoT security, zero trust, data protection, risk management, digital infrastructure.

Kirish

Raqamli iqtisodiyotning kengayishi bilan iqtisodiy jarayonlar, boshqaruv tizimlari, bank-moliya xizmatlari, ta’lim, sog‘liqni saqlash va davlat xizmatlari tobora ko‘proq elektron platformalarga ko‘chmoqda. Bu holat samaradorlikni oshirayotgan bo‘lsa-da, axborot xavfsizligini ta’minlash masalasini strategik darajaga olib chiqmoqda. Chunki raqamli infratuzilmadagi har qanday uzilish korxona faoliyati, moliyaviy barqarorlik, iste’molchilar ishonchi va milliy manfaatlarga bevosita ta’sir ko‘rsatadi [1; 2].

Bugungi sharoitda kiberxavfsizlik faqat IT bo‘limining vazifasi emas. U boshqaruv, iqtisod, huquq, kadrlar siyosati va risk-menejment bilan uzviy bog‘liq kompleks yo‘nalishga aylandi. Ayniqsa, masofaviy ish shakllari, bulutli xizmatlar, mobil ilovalar va Internet of Things texnologiyalari faol qo‘llanayotgan tashkilotlarda tahdidlar soni ham, ularning murakkabligi ham ortib bormoqda [3].

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Ushbu maqolaning obyekti raqamli jamiyat va undagi axborot almashinuvi tizimlari hisoblanadi. Tadqiqot predmeti esa ushbu tizimlarda yuzaga kelayotgan kibertahdidlar, ularning iqtisodiy va tashkiliy oqibatlari hamda ularni kamaytirish mexanizmlaridir. Tadqiqotning maqsadi zamonaviy kiberxavfsizlik muammolarini tahlil qilish, asosiy tahdidlarni tizimlashtirish va ularning oldini olish bo‘yicha amaliy takliflar ishlab chiqishdan iborat.

Maqola tuzilishi quyidagicha tashkil etildi: avval adabiyotlar tahlili orqali mavzuning ilmiy asoslari ko‘rib chiqiladi, so‘ng tadqiqot metodologiyasi yoritiladi, keyin tahlil va natijalar bo‘limida muammolar, tahdidlar va himoya yechimlari bir tizimga solinadi, yakunda esa xulosa va takliflar beriladi.

Adabiyotlar tahlili

Zamonaviy ilmiy manbalarda kiberxavfsizlik ko‘proq uch yo‘nalishda o‘rganiladi: texnologik himoya vositalari, inson omili va institutsional boshqaruv. Smith [1] global axborot xavfsizligi tendensiyalarini tahlil qilib, raqamli iqtisodiyotning o‘sishi bilan tahdidlar ssenariylari ham ko‘payayotganini ko‘rsatadi. Johnson va Lee [2] kiberhujumlar evolutsiyasini o‘rganib, oddiy zararli dasturlardan murakkab, maqsadli va iqtisodiy manfaatga yo‘naltirilgan hujumlarga o‘tish jarayonini izohlaydi.

Ahmed [3] va Chen [4] tadqiqotlarida zararli dasturlar hamda IoT muhitidagi zaifliklar asosiy xavf omillari sifatida talqin qilingan. Ularning fikricha, ko‘plab qurilmalar ishlab chiqarish bosqichidayoq yetarli himoya mexanizmlariga ega emasligi sababli butun tarmoqni xavf ostida qoldiradi. Garcia [5] inson omilining markaziy rolini asoslab, xodimlarning xatolari aksariyat kiberhodisalarning boshlang‘ich nuqtasiga aylanishini ta’kidlaydi.

Williams [6], Kim [7] va Thompson [8] ishlarida esa kiberhujumlarning iqtisodiy oqibatlari ochib berilgan. Ular ma’lumotlar sizib chiqishi, to‘xtab qolgan biznes jarayonlari, tiklash xarajatlari va reputatsion yo‘qotishlarni tashkilotlar uchun eng og‘ir

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

zarar manbalari sifatida ko‘rsatadi. Petrov [9] milliy kiberxavfsizlik strategiyalarini, Morgan [10] esa sun’iy intellekt va avtomatlashtirilgan himoya tizimlarining istiqbollarini yoritadi.

Ko‘rib chiqilgan adabiyotlar shuni ko‘rsatadiki, kiberxavfsizlik bo‘yicha alohida texnik yechimlar ko‘p bo‘lsa-da, ularni iqtisodiy boshqaruv, tashkiliy siyosat va xodimlar savodxonligi bilan birlashtiruvchi yondashuv hali ham dolzarb bo‘lib qolmoqda. Mazkur maqolada aynan shu integratsiyalashgan nuqtai nazar ilgari suriladi.

Tadqiqot metodologiyasi

Tadqiqotda tizimli yondashuv asosiy metodologik poydevor sifatida qo‘llanildi. Mazkur yondashuv kiberxavfsizlikni alohida texnik jarayon sifatida emas, balki bir-biriga bog‘liq bo‘lgan texnologik, tashkiliy, iqtisodiy va huquqiy omillar tizimi sifatida o‘rganish imkonini berdi.

Shuningdek, qiyosiy tahlil usulidan foydalanilib, phishing, ransomware, DDoS, ma’lumotlar sizib chiqishi va IoT hujumlari kabi tahdidlar o‘zaro taqqoslandi. Ilmiy adabiyotlar sharhi orqali mahalliy va xorijiy manbalardagi nazariy qarashlar umumlashtirildi. Statistik tavsiflash usuli yordamida ochiq manbalarda keltirilgan raqamlar va tendensiyalar asosida kiberxavfsizlikning iqtisodiy ahamiyati baholandi [6; 8].

Tadqiqotning amaliy tomoni sifatida kiberxavfsizlik bo‘yicha samarali boshqaruv modelini ishlab chiqish maqsad qilindi. Bunda himoya vositalari to‘rtta blokka - profilaktika, aniqlash, javob qaytarish va tiklash bosqichlariga ajratildi. Ushbu metodologiya tashkilot miqyosida qaror qabul qilishga mos, sodda va amaliy tavsiyalar ishlab chiqishga xizmat qildi.

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Tahlil va natijalar

Raqamli iqtisodiyotda kiberxavfsizlikka tahdid soluvchi omillar bir nechta darajada namoyon bo‘ladi. Birinchi daraja - texnologik zaifliklar. Eskirgan dasturiy ta’minot, noto‘g‘ri sozlangan tarmoqlar, patch management jarayonining sustligi va autentifikatsiya mexanizmlarining kuchsizligi hujumchilar uchun qulay sharoit yaratadi. Ikkinchi daraja - tashkiliy kamchiliklar. Ko‘plab muassasalarda xavfsizlik siyosati qog‘ozda mavjud bo‘lsa-da, amaliyotda unga rioya etilmaydi. Uchinchi daraja esa inson omili bo‘lib, aynan shu qatlam aksariyat hodisalarda boshlang‘ich nuqta vazifasini bajaradi [5].

Kiberxavfsizlik tahdidlarining iqtisodiy oqibatlari bevosita va bilvosita shaklda namoyon bo‘ladi. Bevosita yo‘qotishlarga moliyaviy zarar, tizimlarni tiklash xarajatlari, xizmatlarning to‘xtashi va jarimalar kiradi. Bilvosita yo‘qotishlar esa mijozlar ishonchining pasayishi, brend obro‘siga putur yetishi, hamkorlar bilan aloqalarning susayishi va bozor ulushining qisqarishida ko‘rinadi. Shu sababli kiberxavfsizlik xarajatlari ko‘pincha qo‘shimcha xarajat emas, balki biznesning uzluksizligi va raqobatbardoshligini ta’minlovchi investitsiya sifatida qaralishi zarur.

Quyidagi jadvalda keng tarqalgan kibertahdidlar, ularning asosiy nishonlari, mumkin bo‘lgan oqibatlari va ustuvor himoya choralarining umumlashgan ko‘rinishi keltirilgan.

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Jadval 1. Zamonaviy kibertahdidlar va ularga qarshi ustuvor choralar

Tahdid turi	Asosiy nishon	Ehtimoliy oqibat	Ustuvor himoya choralari
Phishing	Foydalanuvchi hisoblari, e-mail, to‘lov ma’lumotlari	Hisoblar egallanishi, maxfiy ma’lumotlarning oshkor bo‘lishi	Xodimlarni o‘qitish, MFA, e-mail filtrlash
Ransomware	Fayl serverlari, ishchi stansiyalar, zaxira tizimlari	Ish jarayonining to‘xtashi, to‘lov talabi, ma’lumot yo‘qotilishi	Zaxira nusxa, segmentatsiya, EDR, patch management
DDoS	Veb-servislar, davlat va tijorat portallari	Xizmat uzilishi, mijozlar noroziligi, daromad yo‘qotish	Trafik filtrlash, CDN, anti-DDoS xizmatlari
Ma’lumotlar sizib chiqishi	Mijoz bazasi, moliyaviy va shaxsiy ma’lumotlar	Jarimalar, reputatsion zarar, huquqiy risk	Ma’lumotlarni shifrlash, kirishni cheklash, audit
IoT hujumlari	Aqlli qurilmalar, sensorlar, sanoat tizimlari	Tarmoq orqali keng tarqaluvchi buzilishlar, boshqaruvning izdan chiqishi	Standart sozlamalarni almashtirish, firmware yangilash, monitoring

Manba: muallif ishlanmasi, ilmiy manbalar asosida umumlashtirilgan [1-10].

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Jadval ma’lumotlari ko‘rsatadiki, tahdidlar turlicha ko‘rinishda bo‘lsa-da, ularning aksariyati identifikatsiya va kirishni boshqarish, monitoring, zaxira nusxalash va xodimlar savodxonligini oshirish orqali sezilarli darajada kamaytirilishi mumkin. Bu esa texnik choralarni tashkiliy intizom bilan birlashtirish zarurligini anglatadi.

Keyingi muhim natija shundan iboratki, zamonaviy himoya modeli bir martalik vositalar to‘plami emas, balki uzluksiz jarayon sifatida tashkil etilishi kerak. Zero trust yondashuvi ushbu fikrni kuchaytiradi: tarmoq ichidagi har bir foydalanuvchi, qurilma va so‘rov ishonchli deb qabul qilinmaydi, balki alohida tekshiriladi. Bunday model masofaviy ish, bulutli xizmatlar va ko‘p platformali infratuzilmalar sharoitida ayniqsa muhim hisoblanadi.

Shuningdek, tadqiqot davomida kiberxavfsizlikni boshqarishda to‘rtta ustuvor yo‘nalish aniqlandi: birinchisi - aktivlarni inventarizatsiya qilish va tasniflash; ikkinchisi - risklarni baholash va ustuvorlashtirish; uchinchisi - texnik himoya vositalarini joriy etish; to‘rtinchisi - xodimlar ishtirokini oshirish. Ushbu ketma-ketlik tashkilotlarga cheklangan resurslar sharoitida ham xavfsizlik darajasini bosqichma-bosqich mustahkamlash imkonini beradi.

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Jadval 2. Tashkilotlarda kiberxavfsizlikni boshqarishning tavsiya etilgan bosqichlari

Bosqich	Mazmuni	Kutiladigan natija
1	Axborot aktivlarini aniqlash, kritik tizimlar va ma’lumotlarni tasniflash	Himoya resurslari eng muhim obyektlarga yo‘naltiriladi
2	Risklarni baholash, ehtimol va zarar darajasini aniqlash	Ustuvor tahdidlar bo‘yicha aniq reja shakllanadi
3	MFA, segmentatsiya, EDR, zaxira nusxalash va shifrlashni joriy etish	Texnik barqarorlik va aniqlash imkoniyati ortadi
4	Xodimlar uchun doimiy trening va phishing simulyatsiyalarini o‘tkazish	Inson omilidan kelib chiqadigan xatolar kamayadi
5	Audit, monitoring, insidentlarga javob va tiklash rejasini yangilab borish	Xavfsizlik tizimi uzluksiz takomillashadi

Manba: muallif ishlanmasi.

Jadval 2 da keltirilgan bosqichlar amaliy jihatdan tashkilotlarga kiberxavfsizlikni tartibli boshqarish imkonini beradi. Ayniqsa, kichik va o‘rta biznes subyektlari uchun resurslarni to‘g‘ri taqsimlash, qaysi himoya choralarini qaysi ketma-ketlikda joriy etish masalasi juda muhimdir. Shu nuqtai nazardan, riskga asoslangan yondashuv eng maqbul yechimlardan biri hisoblanadi.

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Natijalarni ilmiy adabiyotlar bilan qiyoslash shuni ko‘rsatadiki, texnik vositalar qanchalik kuchli bo‘lmasin, xodimlar savodxonligi va boshqaruv intizomi sust bo‘lsa, umumiy himoya darajasi kutilgan natijani bermaydi. Demak, kiberxavfsizlik samaradorligini oshirish uchun texnologiya, boshqaruv va ta’lim bir-birini to‘ldiruvchi uch tayanch omil sifatida qaralishi zarur.

Xulosa va takliflar

Tadqiqot natijalari shuni ko‘rsatdiki, raqamli iqtisodiyot sharoitida kiberxavfsizlikni ta’minlash iqtisodiy barqarorlik, institutsional ishonch va raqamli xizmatlarning uzluksiz ishlashi uchun asosiy shartlardan biridir. Phishing, ransomware, DDoS, ma’lumotlar sizib chiqishi va IoT hujumlari eng dolzarb tahdidlar sifatida ajralib turadi. Ularning har biri alohida texnik vosita bilan emas, balki kompleks boshqaruv modeli orqali samarali jilovlanadi.

Maqolada ishlab chiqilgan yondashuvning amaliy qiymati shundaki, u kiberxavfsizlikni to‘rtta ketma-ket yo‘nalishda tashkil etishni tavsiya etadi: aktivlarni aniqlash, risklarni baholash, texnik himoyani kuchaytirish va inson omiliga ta’sir ko‘rsatish. Ushbu model tashkilotlarning o‘z resurslaridan oqilona foydalanishiga, zararni kamaytirishiga va biznes uzluksizligini ta’minlashiga yordam beradi.

Tadqiqot asosida quyidagi takliflar ilgari suriladi: birinchidan, barcha tashkilotlarda zero trust tamoyillariga mos kirishni boshqarish tizimlari bosqichma-bosqich joriy etilishi lozim; ikkinchidan, xodimlar uchun muntazam o‘quv mashg‘ulotlari va phishingga qarshi amaliy treninglar tashkil etilishi zarur; uchinchidan, ma’lumotlarni zaxiralash, shifrlash va audit qilish mexanizmlari yagona siyosatga birlashtirilishi kerak; to‘rtinchidan, davlat va xususiy sektor o‘rtasida axborot almashinuvi hamda normativ-huquqiy uyg‘unlik kuchaytirilishi maqsadga muvofiq.

Kelgusida ushbu yo‘nalishda tarmoq monitoringi, sun’iy intellektga asoslangan aniqlash tizimlari, O‘zbekiston sharoitida kiberxavfsizlikning iqtisodiy

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

samaradorligini baholash va sohaviy kesimdagi taqqoslama tadqiqotlar olib borish ilmiy hamda amaliy jihatdan muhim natijalar berishi mumkin.

Foydalanilgan adabiyotlar

[1] Smith J. Global Information Security Trends 2025. Cybersecurity Journal, 2024, pp. 15-28.

[2] Johnson M., Lee S. The Evolution of Cyber Threats in Digital Era. International Security Review, 2023, pp. 5-19.

[3] Ahmed R. Malware Development and Protection Strategies. Tech Security Publications, 2024, pp. 20-35.

[4] Chen X. IoT Security Challenges and Solutions. Network Security Quarterly, 2023, pp. 40-55.

[5] Garcia P. Human Factor in Cybersecurity Incidents. Behavioral Security Studies, 2024, pp. 30-45.

[6] Williams T. Economic Impact of Ransomware Attacks. Financial Security Review, 2023, pp. 15-25.

[7] Kim Y. Data Breaches in Modern Enterprises. Data Protection Journal, 2024, pp. 25-38.

[8] Thompson L. Cost Analysis of Cyber Incidents. Business Security Analytics, 2023, pp. 10-22.

[9] Petrov A. National Cybersecurity Strategies in Digital Age. Government Technology Review, 2024, pp. 30-45.

[10] Morgan S. Future of Cybersecurity: AI and Beyond. Innovation Security Report, 2024, pp. 40-55.

DOI: https://doi.org/10.66493/h6q7vc94
© Sharq universiteti, 2026