KIBER XAVFSIZLIKNING IQTISODIYOTGA TA’SIRI

Aliqulova Aziza
Ichki ishlar vazirligi akademik litseyi o’qituvchisi

Annotatsiya: *Ushbu maqolada Ichki ishlar vazirligi akademik litseylarida kiber xavfsizlik yo’nalishida matematika fanini o’qitish metodikasining nazariy va amaliy jihatlari ko’rib chiqiladi. Maqola matematikaning bu yo’nalishda o’quvchilarga zarur bo’lgan kompetensiyalarini aniqlash, mazmun-mundarijaning shakllantirilishi, metod va vositalarni tanlash, baholash mexanizmlarini takomillashtirish bo’yicha tavsiyalarni beradi. Metodologik yondashuvlar xalqaro tajribalar, ta’lim psixologiyasi va didaktik prinsiplardan kelib chiqqan.*

Kalit so’zlar: *kiber xavfsizlik; matematika metodikasi; litsey; pedagogik texnologiyalar; kompetensiyalar; interfaol metodlar.*

Abstract: *This article examines the theoretical and practical aspects of the methodology for teaching mathematics in the field of cybersecurity at the Ministry of Internal Affairs academic lyceums. The article provides recommendations on identifying the competencies necessary for students in this subject area, shaping the content structure, selecting methods and tools, and improving assessment mechanisms. The methodological approaches are based on international experiences, educational psychology, and didactic principles.*

Keywords: *cybersecurity; mathematics methodology; lyceum; pedagogical technologies; competencies; interactive methods.*

Raqamli texnologiyalarning keng tarqalishi, ma’lumotlar almashuvi va onlayn xizmatlarning o‘sishi bizni bir tomondan samaradorlik, tezlik va bozor imkoniyatlarini oshirishga olib keldi. Biroq, shu bilanoq kiber tahdidlar — xakerlik hujumlari, ma’lumotlar sızdırılması, servislar ishining to‘xtashi — iqtisodiy sektorda sezilarli zararlar keltiradi. Ushbu tezisning maqsadi — global va mintaqaviy misollar asosida kiber xavfsizlik kamchiliklarining iqtisodiy oqibatlarini tahlil qilish, zarar va foyda nisbatini baholash, hamda samarali strategiyalarni taklif etish.

Adabiyot sharhi & so‘nggi statistikalar

1. Global kiberjinoyat zararining hajmi

- Cybersecurity Ventures ma’lumotlariga ko‘ra, 2024 yilda kiberjinoyatlar butun dunyo bo‘yicha yiliga ~9,5 trillion AQSh dollariga yaqin zarar keltirishi kutilmoqda. cysuranceinstitute.com
- Bu ko‘rsatkich 2025 yilda taxminan 10,5 trillion dollargacha o‘sishi bashorat qilinmoqda. cysuranceinstitute.com+1

2. Ma’lumotlar sızdırılması (Data Breach) narxi

- IBM va Ponemon instituti ma’lumotlariga ko‘ra, 2023 yilda butun dunyo bo‘yicha ma’lumotlar sızdırılması bo‘yicha o‘rtacha zarar ~ 4,45 million dollar ni tashkil etgan. ibm.com+2verimatrix.com+2
- AQShda esa bu ko‘rsatkich ~ 9,48 million dollar atrofida bo‘lgan. ibm.com
- Sog‘liqni saqlash sektori eng yuqori zarar ko‘rayotgan soha bo‘lib, ma’lumotlar sızdırılması zarari ~ 10,93 million dollar ga yetgan. ibm.com

3. Mintaqaviy misollar: O‘rta Sharq

- IBMning “Cost of a Data Breach” hisobotiga ko‘ra, O‘rta Sharqdagi tashkilotlarda ma’lumotlar sızdırılması natijasida keladigan zararlar oxirgi yillarda keskin oshgan. 2023 yilda ushbu mintaqa uchun ma’lumotlar sızdırılması yuki SAR 29.9 million ga yetgan. IBM Newsroom - Middle East & Africa
- Sanoat sohalari bo‘yicha qaralganda, moliyaviy sektor, energetika va sog‘liqni saqlash sohalarida zararlar eng yuqori bo‘lgan. IBM Newsroom - Middle East & Africa

4. Trendlar va tahdid turlari

- Phishing (firibgarlik), credential theft (login ma’lumotlarining o‘g‘irlanishi) kabi usullar birinchi o‘rinlarda turadi. verimatrix.com+2National Cyber Security Consulting+2
- Kichik va o‘rta korxonalarga qarshi tahdidlar ko‘paygan — 2025 yilda ransomeware, phishing kabi hujumlar ularning ko‘pi uchun muhim risk manbaiga aylangan. SQ Magazine+1

Metodologiya

Tezisda qo‘llanadigan metodlar:

- Kvantitativ tahlil: global va mintaqaviy hisobotlar, korxona darajasidagi zararlar bo‘yicha ma’lumotlar, regressiya modellari yordamida zarar va sarmoya o‘rtasidagi bog‘liqlikni tahlil qilish.
- Case-study: ma’lum bir korxona yoki mamlakatda yuz bergan ma’lumotlar sızdırılması voqealari, ularning iqtisodiy zarari, reaktsiyasi, olib borilgan choralar (masalan, Jaguar-Land Rover holati) kabi misollar. (Masalan, Jaguar Land Rover avtomobil ishlab chiqaruvchisida sodir bo‘lgan kiber hujum — buning natijasida ishlab chiqarish va sotuvlar jiddiy to‘xtab qolgan. Reuters)
- Narx-foyda (cost-benefit) tahlili: korxonalarning kiber xavfsizlikka sarmoyasi va bu sarmoyalarning keltiradigan foydasi, yo‘qotishlarini oldini olish masalasi.

Natijalar va misollar

1. Bevosita iqtisodiy zararlar

- Global darajada: kiberjinoyatlar tufayli 2024 yilda taxminan 9,5 trillion USD zarar bo‘lishi kutilmoqda. cysuranceinstitute.com+1
- Ma’lumotlar sızdırılması: korxona uchun o‘rtacha ~ 4,45 million USD, AQShda esa ~ 9,48 million USD. ibm.com
- Mintaqaviy misol: O‘rta Sharqdagi kompaniyalar SAR 29.9 million zarar ko‘rgan. IBM Newsroom - Middle East & Africa

2. Bilvosita zararlar (reputatsiya, ishonch yo‘qotishi, bozorlarda ulush yo‘qotishi)

- Masalan, ma’lumotlar sızdırılması korxonaning mijozlari ishonchini yo‘qotishi, bozordagi obro‘-nufuzining pasayishi sababli, sotuvlar kamayishi.
- Jaguar Land Rover kabi kompaniyada rasmiy ravishda ma’lumotlar buzilishi bo‘lmasa ham, operatsiyalar va ishlab chiqarish to‘xtab qolishi, xodimlar uyda qolishi kabi holatlar yuz berdi, bu esa to‘g‘ridan-to‘g‘ri ishlab chiqarish va sotuv zarariga olib keldi. Reuters

3. Sarmoyaning rentabelligi

- Kiber xavfsizlik choralariga sarmoya qilgan tashkilotlar, zarar vaziyatida sarflanadigan mablag‘dan ko‘ra, oldini olish choralarining narxi pastroq bo‘lishini ko‘rsatuvchi ma’lumotlar mavjud. Masalan, IBM hisobotida, sızdırılması aniqlanishi va unga javob berish tezligi qancha yuqori bo‘lsa, korxona zararni kamaytirishi shuncha osonroq bo‘ladi. ibm.com
- Shuningdek, avtomatlashtirish va AI texnologiyalari qo‘llanilsa, zarar kamayishi va javob berish vaqtining qisqarligi mumkin. IBM Newsroom - Middle East & Africa+1

4. Davlat va siyosat roli

- Qonunchilik va normativ talablar: GDPR kabi ma’lumotlarni himoya qilish qonunlari, davlatlararo norma va standartlar korxonalarga ma’lumotlarni sızdırılmasligi uchun javobgarlik yuklaydi, jarimalarni belgilaydi.
- Sug‘urta bozori: korxonalarning kiber sug‘urta polislariga ehtiyoji ortib bormoqda, bu zararlar risklarini moliyaviy jihatdan yengillashtiradi.

5. Bozor strukturasiga va mehnat bozori o‘zgarishlari

- Kiber xavfsizlik bo‘yicha ish o‘rinlari ko‘paymoqda. Jahon bo‘yicha IT xavfsizlik mutaxassislari va ular o‘rtasidagi bo‘shliq (skill gap) katta. Masalan, statistikalar bo‘yicha jahon bo‘yicha millionlab kasblar bu sohada yaratilishi kerak. verimatrix.com+1
- Korxonalarning byudjetlarida va operatsion xarajatlarida kiber xavfsizlik sarmoyalari doimiy o‘sib bormoqda.

Misol: Mamlakat darajasida holat

- Hindiston: 2024 yilda kiber firibgarliklar natijasida hukumat ma’lumotlariga ko‘ra, yo‘qotishlar sezilarli darajada oshgan. Misol uchun, Times of India ma’lumotida, Mox Home Affairs tomonidan bildirildiki, Hindistonda kiber frauslar tufayli ~ ₹22,845 crore (taxminan yarim trilliardan oshiq hind rupees) yo‘qotish bo‘lgan, bu oldingi yilga nisbatan 206% ga ko‘payish. The Times of India
- Vetnam: Vetnamda Milliy Kredit Axborot Markazi ma’lumotlar bazasi kiber hujumga uchragan, shaxsiy ma’lumotlar va kredit tarixlari kabi ma’lumotlar o‘zgarishi mumkinligi aniqlangan. Bu banklar va moliyaviy institutlar uchun tashkil etilgan xarajatlarni oshiradi. Reuters

- Jaguar Land Rover: Bu avtomobil kompaniyasi global darajada kiber hujum tufayli ishlab chiqarish va chakana sotuvda jiddiy uzilishlarga duch kelgan. Ishchilar uyda qolishi va majburiy tizim o‘chirib qo‘yilishi zararlarni kuchaytirgan. Reuters

Kiber xavfsizlikning yetishmovchiligi global iqtisodiyotga milliard-trillion dollar miqdorda zarar keltirishi mumkin, bu nafaqat korxonalarga, balki davlat budjetlariga, ishlab chiqarishga, sog‘liqni saqlash va moliyaviy sektor kabi muhim sohalarga ta’sir qiladi. Zararlar faqat moliyaviy jihatdan emas, reputatsiya, bozordagi raqobat, iste’molchilarning ishonchi kabi bilvosita yo‘llar bilan ham uzayib boradi. Shu bilan birga, kiber xavfsizlik choralariga sarmoya qilish, zamonaviy texnologiyalarni joriy etish, davlat normativlarini kuchaytirish, xodimlar va fuqarolarni xabardor qilish yuqori rentabellikka ega.

Korxonalarda kiber xavfsizlikga ajratiladigan sarmoyalarni oshirish — texnologik echimlar (shifrlash, inkognito autentifikatsiya, zero trust arxitekturasi), xodimlar treningi, voqea javob guruhlari (incident response teams). Davlatlararo hamkorlik va standartlar: xalqaro normativlar va me’yorlar, ayniqsa ma’lumotlarni himoya qilish bo‘yicha qonunlar, jarimalar belgilari, auditlar. Kichik va o‘rta korxonalarga moliyaviy rag‘batlar — soliq imtiyozlari, subsidiyalar, arzon sug‘urta polislarini taklif qilish orqali ularni kuchli kiber xavfsizlikka ega qilish. Kiber xavfsizlik bo‘yicha jamoatchilik ongini oshirish — fuqarolarga phishing, parol xavfsizligi, shaxsiy ma’lumotlarni himoya qilish bo‘yicha maslahatlar berish. Innovatsiya va texnologik yechimlarga sarmoya: AI va avtomatlashtirish, o‘zini o‘zi tiklash (resilience), bulut xosting xizmatlari, monitoring va tezkor javob.

Kiberxavfsizlik — axborot texnologiyalari infratuzilmasi, tarmoqlar, ma’lumotlar va foydalanuvchilarni ruxsatsiz kirish, buzilish, yo‘qotilish, shuningdek ma’lumot oshkor bo‘lishi kabi xatarlaridan himoyalash. Raqamli transformatsiya, internet, elektron moliyaviy xizmatlar, mobil ilovalar, elektron tijorat va davlat xizmatlarining onlayn rejimga o‘tishi tufayli kiberxavfsizlik iqtisodiyotni har tomonlama ta’sirlari bilan bog‘liq bo‘lgan muhim omilga aylandi. Agar kiberxavfsizlik zaif bo‘lsa, ishbilarmonlik muhitida ishonchsizlik yuzaga keladi, investitsiyalar kamayadi, operatsion xarajatlar oshadi, va ekstrem holatlarda iqtisodiy yo‘qotishlar katta bo‘ladi.

Xalqaro miqyosda kiberxavfsizlikning iqtisodiy ta’sir eng avvalo moliyaviy yo‘qotishlarda ko’zga tashlanadi.

- 2024-yilda global miqyosda kiberjinoyatchilik natijasida kamida $16 milliarddan ortiq yo‘qotishlar yuzaga kelgani ma’lum. Reuters
- “Global value at risk” (ya’ni, kiberhujumlar natijasida yo‘qotilishi mumkin bo‘lgan umumiy iqtisodiy qiymat) taxminan $5.2 trillion atrofida. worldbank.org
- Kompaniyalar va tashkilotlar uchun ma’lumotlar buzilishi (data breach) har bir hodisa uchun o‘rtacha $4.88 million atrofida xarajat keltiradi. Форбс

2.2 Bozor, Sug‘urta va Investitsiyalar

- Kiberxavfsizlik bo‘yicha bozor o‘sishi katta – ehtimoliy CAGR (yillik o‘sish sur’ati) yuqori darajada. Fortinet+1
- Sug‘urta kompaniyalarining kiberxavfsizlik bo‘yicha da’volari (claims) ko‘paymoqda, premiumlar oshmoqda. Fortinet

2.3 Ishbilarmonlik va iqtisodiy o‘sishga ta’siri

- Raqamli ishonch kamligi (trust deficit) investorlar uchun salbiy omil bo‘ladi — yangi startap, texnologik korxonalarga sarmoya kiritishda xavf ko‘proq deb baholanadi.
- Yetkazib beruv zanjirida (supply chain) kiberxavfsizlik zaifligi, bir kompaniyaning xatosi bir necha davlat/bozorlar uchun muammolarni keltirib chiqaradi.

2.4 Sanoat va ijtimoiy sektorlardagi ta’sirlar

- Sog‘liqni saqlash, energetika, moliyaviy xizmatlar, transport kabi sohalarda kiberhujumlar operatsion faoliyatni to‘xtatib qo‘yishi, xizmat ko‘rsatish kechikishi yoki zarar keltirishi mumkin.
- Ma’lumotlar oshkor bo‘lishi natijasida shaxsiy hayotiy ma’lumotlarining yo‘qotilishi, mijozlarning ishonchi shikastlanadi, qonunchilik jazosi, jarimalar, huquqiy xarajatlar ko‘payadi.

---

3. O‘zbekiston misollari: holat, faktlar, yo‘qotishlar

3.1 Holat va statistikalar

- 2023-yilda O‘zbekiston hududida taxminan 11 million kiberhujum qayd etilgan. Business Upturn
- 2024-yilda kiberhujumlar soni oshgan: bir yil ichida O‘zbekiston bo‘yicha 12 milliondan ortiq hujumlar qayd etilgan. Kun.uz
- Fraud (firibgarlik) holatlari ham oshib borayotgani, bank kartalaridan noqonuniy foydalanish, “carding” kabi jinoyatlar mamlakatdagi kiberjinoyatchilik strukturasida katta ulushga ega. Kun.uz+2Kun.uz+2

3.2 Iqtisodiy yo‘qotishlar

- Masalan, Jizzaxdagi Asakabankning mintaqaviy filialida bir mijoz foydasida ochilgan depozit hisobidan 3 milliard so‘m yaqin mablag‘ O‘zbekiston so‘mida noqonuniy ravishda yechib olingan. Caspian Post
- To‘lov kartalari firibgarligi tufayli bank tizimiga, korxonalarga va yakuniy iste’molchilarga operatsion va moliyaviy zarar yetmoqda — banklar xavfsizlik tizimlarini yangilashga, monitoring tizimlarini kuchaytirishga majbur bo‘lmoqda.

3.3 Siyosiy va huquqiy choralar

- Prezident Mirziyoyev 2023-yilda kiberxavfsizlik va moliyaviy xizmatlar, fintech hamda to‘lov tizimlari uchun yagona, umumlashtirilgan talablarni ishlab chiqishni topshirgan. Kun.uz+1

- 2025-yilda Prezident qarori bilan (Decree PQ-153, 30 aprel) moliyaviy institutlar, to‘lov tashkilotlari va shaxslar uchun kiberxavfsizlik talablarini kuchaytirish belgilangan; firibgarlik natijasida yetkazilgan moddiy zararlar uchun javobgarlik belgilanadi. Pivot+1
- O‘zbekiston ITU (Xalqaro telekommunikatsiyalar ittifoqi) tomonidan Global Cybersecurity Index reytingida pozitsiyasini yaxshilagan.

4. Muammolar va xatarlar

- Texnik jihatdan: zaif parol siyosati, eskirgan dasturiy ta’minot, tizimlardagi zaifliklar, yangilanishlarsiz qolgan infratuzilmalar.
- Inson omili: xodimlarning xavfsizlik bo‘yicha ong darajasi past, firibgarlikka moyillik, kirish ma’lumotlarini (login, parollar) hifzsiz ishlatish.
- Tashkiliy va huquqiy: barcha korxonalar uchun bir xilda qoidalar emasligi, nazorat va majburiylik darajasi pastligi, jinoiy javobgarlik va jarimalarning samarasi past bo‘lishi mumkin.
- Moliyaviy resurslarning yetishmasligi: kichik va o‘rta korxonalar, ayniqsa, to‘lov tizimlari yoki onlayn xizmatlar bilan shug‘ullanuvchilarda investitsiyalarni ajratishga cheklovlar.

5. Yechimlar: strategiyalar va tavsiyalar

5.1 Davlat va qonunchilik darajasida

- Kiberxavfsizlik bo‘yicha milliy strategiyalarni ishlab chiqish, amaliy qoidalarni (standartlar, sertifikatsiyalar) joriy etish va ularni majburiy qilish.
- Huquqiy javobgarlikni kuchaytirish: moliyaviy institutlar, to‘lov tashkilotlari va xizmat provayderlari foydalanuvchilarning mablag‘lari yoki ma’lumotlari bilan bog‘liq xavfsizlik talablariga rioya qilmasa, yetkazilgan zarar uchun javobgarlik belgilanishi. (O‘zbekiston hozirda shunday choralarni ko‘rmoqda.) Pivot

5.2 Texnologik va infratuzilma jihatidan

- “Antifraud” va “anti-virus” tizimlarini joriy etish, xakerlik tahlillari (penetration testing), zaifliklarni aniqlash va bartaraf qilish, foydalanuvchilarning autentifikatsiyasini kuchaytirish (2 faktorli autentifikatsiya kabi).
- Raqamli infratuzilma yangilanishi: eski tizimlarni yangilash, xavfsizlik plaginlarini, patch managementni muntazam amalga oshirish.

5.3 Ta’lim, ong va tashqi hamkorlik

- Xodimlar va foydalanuvchilar uchun kiberxavfsizlik bo‘yicha treninglar, xabardorlik kampaniyalari.
- Universitetlarda va o‘quv markazlarida kiberxavfsizlik bo‘yicha mutaxassislarga tayyorgarlikni kuchaytirish.
- Xalqaro hamkorlik: boshqa davlatlar tajribalarini o‘rganish, birgalikda standartlar ishlab chiqish, kiberjinoyatchilikka qarshi transchegaraviy huquqiy hamkorlikni rivojlantirish.

5.4 Biznes sektorining roli

- Korxonalarda kiberxavfsizlik byudjetini ajratish, risk analizini muntazam qilish, ichki audit va nazorat tizimlarini kuchaytirish.
- Kichik va o‘rta korxonalarga (SME) maxsus subsidiyalar, grantlar, chalkash bo‘lmagan texnik yordam taqdim etish orqali ularni himoya choralari bilan ta’minlash.

Kiberxavfsizlik iqtisodiyotning barqaror o‘sishini ta’minlash uchun asosiy zoravonliklardan biridir. Uning zaifligi moliyaviy yo‘qotishlar, reputatsiyaning yo‘qolishi, investitsiyalarning kamayishi kabi salbiy oqibatlarga olib keladi. O‘zbekistonda raqamli transformatsiya jarayonlari davom etar ekan, kiberxavfsizlikga e’tibor oshishi, qonunchilik va texnik choralarning kuchaytirilishi, xususiy va davlat sektorlaridagi hamkorlikning kengaytirilishi muhim. Agar to‘g‘ri siyosat, texnologiyalar va odam resurslari birgalikda harakat qilsa, kiberxavfsizlik nafaqat xavfsizlikni oshiradi, balki iqtisodiyotga ishonch, barqarorlik va o‘sish imkoniyatlarini ham yaratadi.

FOYDALANILGAN ADABIYOTLAR

1. Serhii Horlichenko, Anastasiia Horlichenko. Mathematical model for optimising the contemporary process of training specialists in the field of cybersecurity and information protection. (its.iszzi.kpi.ua)
2. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. MDPI, 2024. (MDPI)
3. “Cybersecurity in Mathematics and Science Elementary Curriculum (CiMS)” — loyiha hujjatlari. (research.ced.ncsu.edu)
4. How is math used in cybersecurity? EdX maqolasi. (edX)
5. Mahfuza Gafurova, Yodgoroy Mamatova. Necessity of Teaching Information Security and Cyber-Security in Primary Education. Central Asian Journal of Mathematical Theory and Computer Sciences. (cajmtcs.centralasianstudies.org)
6. Начало формы