

# KORXONALARDA KIBER XAVFSIZLIKNI TA'MINLASH ORQALI IQTISODIY TALOFATLARNI KAMAYTIRISH USULLARI

**Meliquziyev Murodbek Shuxratjon o'g'li**

*O'zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Biznes va tadbirkorlikoliy maktabi  
doktoranti*

*e-mail: murodjon.1996@gmail.com*

**Annotatsiya:** Ushbu maqolada korxonalarning iqtisodiy ko'rsatkichlariga kiberhujumlarning salbiy ta'siri va ularni kamaytirish strategiyalari tahlil qilinadi. Maqolada kiber xavfsizlikka yo'naltirilgan investitsiyalarni xarajat sifatida emas, balki iqtisodiy zararni oldini oluvchi vosita sifatida ko'rib chiqish masalalari yoritilgan.

**Kalit so'zlar:** kiber xavfsizlik iqtisodiyoti, iqtisodiy talofatlar, xatarlarni boshqarish, moliyaviy barqarorlik, kiber sug'urta, investitsion salohiyat, raqamli transformatsiya, samaradorlik tahlili.

**Abstract:** This article analyzes the negative impact of cyberattacks on the economic performance of enterprises and discusses strategies for their mitigation. The paper focuses on re-evaluating cybersecurity investments not as mere costs, but as essential tools for preventing significant economic losses and ensuring long-term financial stability.

**Keywords:** cybersecurity economics, economic losses, risk management, financial stability, cyber insurance, investment potential, digital transformation, cost-benefit analysis.

**Аннотация:** В данной статье анализируется негативное влияние кибератак на экономические показатели предприятий и рассматриваются стратегии по минимизации их последствий. Основное внимание уделяется вопросам рассмотрения инвестиций в кибербезопасность не как операционных расходов, а как инструмента предотвращения экономического ущерба и обеспечения финансовой устойчивости.

**Ключевые слова:** экономика кибербезопасности, экономический ущерб, управление рисками, финансовая устойчивость, киберстрахование, инвестиционный потенциал, цифровая трансформация, анализ эффективности.

## KIRISH

Bugungi global iqtisodiyotda raqamli transformatsiya korxonalar uchun ixtiyoriy tanlovdan strategik zaruriyatga aylandi. Ishlab chiqarish, logistika va moliya jarayonlarining bulutli texnologiyalar (Cloud Computing) va narsalar interneti (IoT) platformalariga ko'chishi operatsion

samaradorlikni oshirgan bo'lsa-da, korxonalarning kiber makondagi "hujum maydoni"ni (attack surface) misli ko'rilmagan darajada kengaytirdi. Endilikda kiberhujumlar shunchaki texnik nosozlik emas, balki korxonaning bozordagi mavjudligini xavf ostiga qo'yuvchi ekzistensial iqtisodiy tahdid sifatida ko'rilmogda.

Raqamli transformatsiya jarayonida korxonalarning barcha moliyaviy va operatsion ma'lumotlari bulutli texnologiyalar va tarmoqlarga ko'chishi kiber jinoyatchilar uchun yangi imkoniyatlar yaratib, korxonalarni katta iqtisodiy xavf ostida qoldirmogda. Bugungi global iqtisodiyotda kiber xavfsizlik va iqtisodiy barqarorlik o'rtasidagi bog'liqlik xalqaro ilmiy doiralarda keng o'rganilayotgan dolzarb yo'nalishlardan biridir. Ilmiy tadqiqotlarni bu borada shartli ravishda uchta asosiy maktabga bo'lib tahlil qilish mumkin.

Birinchidan, iqtisodiy zararni modellashtirish yondashuvi doirasida Anderson (2001) o'zining fundamental ishlarida kiber jinoyatchilikning iqtisodiy motivlarini tahlil qildi. U himoya tizimidagi kamchiliklar ko'pincha texnik nosozlikdan ko'ra, iqtisodiy rag'batlarning noto'g'ri taqsimlanishi, ya'ni "incentive misalignment" natijasi ekanligini ta'kidlaydi. Shu bilan birga, Gordon va Loeb (2002) modeli kiber xavfsizlikka investitsiya kiritishning optimal darajasini aniqlashda iqtisodiy "oltin qoida"ni ilgari surdi. Ularning nazariyasiga ko'ra, kiber xavfsizlik xarajatlari kutilayotgan yillik zararning (ALE) taxminan 37 foizidan oshmasligi kerak, aks holda kiritilgan investitsiya iqtisodiy jihatdan o'zini oqlamaydi va samarasiz hisoblanadi.

Ikkinchi yo'nalish bo'lgan reputatsion va bilvosita zararlar tahliliga ko'ra, Cashell va boshqa tadqiqotchilar (2004) kiberhujumdan keyin korxona aksiyalari qiymatining pasayishini o'rganishgan. Ularning xulosasiga ko'ra, ma'lumotlar sizib chiqishi haqidagi xabar e'lon qilingandan so'ng, kompaniya kapitalizatsiyasi o'rtacha 1 foizdan 5 foizgacha yo'qotishga uchraydi. Bu ko'rsatkich bevosita moliyaviy o'g'rilikdan ko'ra bir necha barobar ko'proq zarar keltirishi bilan xavflidir.

Uchinchi maktab — tizimli risklar va zamonaviy tendensiyalarni o'rganuvchi tadqiqotlardir. Masalan, Ponemon Institute (2023) hisobotlari kiberhujumlarning o'rtacha qiymati global miqyosda 4.45 million dollarga yetganini ko'rsatmogda. Bu tadqiqotlarda asosiy urg'u mijozlarning ommaviy ketishi va brendga bo'lgan ishonchning emirilishi kabi "bilvosita xarajatlar"ga qaratilgan. Global statistika va iqtisodiy prognozlarga ko'ra, kiberhujumlarning iqtisodiy oqibatlari faqatgina ransomware kabi bir martalik to'lovlar bilan cheklanmaydi. Cybersecurity Ventures prognozlariga ko'ra, 2025-yilga borib kiber jinoyatchilikdan keladigan yillik global zarar 10.5 trillion dollarni tashkil etishi kutilmogda<sup>1</sup>.

Ushbu iqtisodiy xavf bir necha omillar bilan yanada chuqurlashmogda. Xususan, ta'minot zanjiri hujumlari (Supply Chain Attacks) orqali bitta zaif hamkor korxona butun bir iqtisodiy ekotizimga zarar yetkazishi mumkin, bunga SolarWinds hodisasi yorqin misol bo'la oladi.

---

<sup>1</sup> SolarWinds Cyberattack Study. (2021). The Economic Fallout of Supply Chain Attacks. [Online resource].

Shuningdek, intellektual mulk o'g'riligi texnologik korxonalarning ko'p yillik tadqiqot natijalarini raqobatchilar qo'lga o'tkazib, uzoq muddatli iqtisodiy tanazzulga sabab bo'ladi<sup>2</sup>.

Mazkur tadqiqotning maqsadi yuqoridagi nazariy yondashuvlar va xalqaro statistik ma'lumotlarga tayangan holda, O'zbekiston sharoitidagi korxonalar uchun kiber xavfsizlikni iqtisodiy boshqarishning optimal modellarini ishlab chiqish hamda talofatlarni minimallashtirishning amaliy usullarini ko'rsatib berishdan

## **KIBERHUJUMLAR NATIJASIDA KELIB CHIQADIGAN IQTISODIY ZARARLAR TAHLILI**

Kiber xavfsizlik tizimidagi mavjud bo'shliqlar korxona iqtisodiyotiga nafaqat texnik nosozlik, balki ko'p qirrali moliyaviy inqiroz sifatida ta'sir ko'rsatadi. Ushbu talofatlar o'z tabiatiga ko'ra bevosita va bilvosita iqtisodiy yo'qotishlarga bo'linib, korxonaning umumiy rentabelligini pasaytiradi. Birinchi navbatda, to'g'ridan-to'g'ri moliyaviy yo'qotishlar kiberhujumlarning eng ko'zga ko'ringan oqibati hisoblanadi. Bu jarayonda korxonaning bank hisob raqamlaridan mablag'larning noqonuniy o'zlashtirilishi, to'lov tizimlarining bloklanishi yoki tranzaksiyalarning buzilishi natijasida real pul oqimlari to'xtab qoladi. Ayniqsa, moliyaviy texnologiyalar sektorida bu turdagi zarar korxonaning likvidlik darajasiga keskin zarba beradi.

Shu bilan birga, operatsion to'xtalishlar natijasida yuzaga keladigan boy berilgan foyda kiberhujumlarning eng og'ir iqtisodiy yuklaridan biridir. Ishlab chiqarish jarayonlarini boshqaradigan IT-tizimlarining (masalan, ERP yoki SCADA tizimlari) ishdan chiqishi korxonaning asosiy faoliyatini to'xtatib qo'yadi. Har bir soatlik to'xtalish mahsulot yetkazib berish hajmining kamayishiga va shartnomaviy majburiyatlarning bajarilmasligiga olib keladi, bu esa o'z navbatida korxonaning yillik daromad ko'rsatkichlariga salbiy ta'sir ko'rsatadi.

Bilvosita zararlar doirasida reputatsion zarar masalasi alohida strategik ahamiyatga ega. Korxonaning kiberhujumga uchrashi va mijozlarga tegishli maxfiy ma'lumotlarning sizib chiqishi bozorda brendga bo'lgan ishonchning emirilishiga sabab bo'ladi. Iqtisodiy nuqtai nazardan, bu holat mijozlarning ommaviy ravishda raqobatchilarga o'tib ketishi (churn rate) va bozor ulushining sezilarli darajada kamayishi bilan xarakterlanadi. Brend reputatsiyasini qayta tiklash uchun sarflanadigan marketing va PR xarajatlari ko'pincha kiber xavfsizlik tizimini modernizatsiya qilish xarajatlaridan bir necha barobar yuqori bo'ladi.

Nihoyat, kiberhujumlar yuridik va tartibga soluvchi xarajatlarning oshishiga olib keladi. Zamonaviy qonunchilik talablariga ko'ra, ma'lumotlar xavfsizligini ta'minlamagan korxonalar davlat organlari tomonidan katta miqdordagi jarimalarga tortilishi mumkin. Bundan tashqari, zarar ko'rgan mijozlar tomonidan beriladigan jamoaviy da'volar bo'yicha sud xarajatlari va tovon pullari

---

<sup>2</sup> Statista. (2024). Average cost of cybercrime worldwide from 2017 to 2028. [Data portal].

korxonaning zaxira fondlarini sarflashga majbur qiladi. Xulosa qilib aytganda, kiber xavfsizlikdagi kamchiliklar korxonaning barcha iqtisodiy bo'g'inlarida zanjirsimon reaksiya beruvchi talofatlarni yuzaga keltiradi.

Maqolaning uchinchi qismini ilmiy standartlarga mos ravishda, bandlarga bo'lmisdan, tahliliy matn ko'rinishida quyidagicha bayon etish mumkin:

### **IQTISODIY TALOFATLARNI KAMAYTIRISHNING STRATEGIK USULLARI VA ULARNING SAMARADORLIGI**

Korxonalarda kiber xavfsizlikni boshqarish jarayoni shunchaki texnik himoya emas, balki iqtisodiy resurslarni optimallashtirishga yo'naltirilgan kompleks strategiya sifatida ko'rilishi lozim. Bu borada talofatlarni minimallashtirishning eng ustuvor usullaridan biri — xatarlarni baholash va aktivlarni prioritetlash (Risk Assessment) hisoblanadi. Iqtisodiy nuqtai nazardan, korxonaning barcha ma'lumotlar segmentini bir xil darajada himoyalash byudjet samaradorligini pasaytiradi. Shu sababli, eng muhim aktivlarni — moliya oqimlari, intellektual mulk va mijozlar bazasini aniqlash hamda asosiy investitsiyalarni aynan shu nuqtalarga yo'naltirish kutilayotgan zararining (ALE) oldini olishda yuqori iqtisodiy rentabellikni ta'minlaydi.

Zamonaviy kiber-ekotizimda "Zero Trust" (Nol ishonch) modelini joriylash korxonaning ichki xarajatlarini nazorat qilishda muhim o'rin tutadi. Ushbu yondashuv tarmoq ichidagi hech bir subyektga avtomatik ishonch bildirmaslik tamoyiliga tayanadi. Iqtisodiy tahlillar shuni ko'rsatadiki, ichki xodimlar yoki hamkorlar orqali keladigan "insayder xavflari" ko'pincha tashqi hujumlardan ko'ra qimmatroqqa tushadi. "Nol ishonch" modeli ruxsatsiz kirish imkoniyatlarini cheklash orqali, inson omili bilan bog'liq iqtisodiy yo'qotishlarni sezilarli darajada qisqartiradi va tarmoq xavfsizligini ta'minlashda operatsion barqarorlikni oshiradi.

Hujumlardan keyingi tiklanish davrida iqtisodiy talofatlarni kamaytirishning eng samarali vositasi — ma'lumotlarni avtomatlashtirilgan rezervlash (Backup) tizimidir. Ayniqsa, ransomware (tovlamachi-viruslar) hujumlari sharoitida korxonalar uchun ma'lumotlarni qayta sotib olish yoki ularni tiklash uchun yirik to'lovlarni amalga oshirish xavfi yuqori. Rezervlash tizimining mavjudligi korxonaga kiber jinoyatchilar bilan muzokaraga kirmaslik va tizimni minimal vaqt ichida qayta ishga tushirish imkonini beradi. Bu esa operatsion to'xtalishlar natijasida yuzaga keladigan boy berilgan foyda hajmini 70-80 foizgacha qisqartirib, korxonaning moliyaviy barqarorligini saqlab qoladi. Xulosa qilib aytganda, ushbu usullar kompleks qo'llanilganda kiber xavfsizlik xarajatlarini "sug'urta" xususiyatiga ega aktivga aylantiradi.

Maqolaning yakuniy tahliliy va xulosa qismlarini, shuningdek, matematik modelning iqtisodiy talqinini quyidagi yaxlit matn shaklida bayon etish mumkin:

## KIBER SUG'URTA MEXANIZMI VA IQTISODIY SAMARADORLIKNI MATEMATIK BAHOLASH

Korxonalarda kiber xavfsizlik strategiyasining ajralmas qismi sifatida kiber sug'urta (Cyber Insurance) mexanizmi tobora muhim ahamiyat kasb etmoqda. Iqtisodiy nuqtai nazardan, kiber sug'urta — bu kutilmagan va o'ta yuqori miqdordagi moliyaviy zararlarni (residual risk) korxona balansidan sug'urta kompaniyasi zimmasiga o'tkazish usulidir. Ushbu mexanizm korxonalarga kiberhujum oqibatida yuzaga keladigan yirik talofatlar sharoitida ham moliyaviy likvidlikni saqlab qolish va operatsion faoliyatni tezkor tiklash imkonini beradi. Ayniqsa, o'rta va kichik biznes subyektlari uchun kiber sug'urta falokatli iqtisodiy inqirozlarning oldini oluvchi barqarorlashtiruvchi vosita bo'lib xizmat qiladi.

Kiber xavfsizlik choralariga yo'naltirilgan investitsiyalarning iqtisodiy maqsadga muvofiqligini baholash uchun ilmiy asoslangan matematik modellardan foydalaniladi. Xususan, xavfsizlik choralarining rentabellik koeffitsiyenti (ROI - Return on Investment) quyidagi formula orqali hisoblanadi:

$$ROI_{security} = \frac{(ALE_{without} - ALE_{with}) - Cost_{mitigation}}{Cost_{mitigation}}$$

Ushbu modelda yillik kutilayotgan zarar miqdori (ALE) tushunchasi markaziy o'rin tutadi. Bunda  $ALE_{without}$  — xavfsizlik choralari ko'rilmagan holatdagi ehtimoliy zarar,  $ALE_{with}$  esa himoya tizimi joriylanganidan keyingi zarar darajasini ifodalaydi.  $Cost_{mitigation}$  ko'rsatkichi esa ushbu himoya tizimini yaratish va saqlash xarajatlarini anglatadi. Agar hisoblash natijasida olingan koeffitsiyent musbat qiymatga ega bo'lsa, demak, kiber xavfsizlikka yo'naltirilgan investitsiya iqtisodiy jihatdan samarali va o'zini oqlaydigan loyiha hisoblanadi.

Tadqiqot natijalari shuni ko'rsatadiki, zamonaviy sharoitda kiber xavfsizlik shunchaki texnik ehtiyoj emas, balki korxonaning iqtisodiy barqarorligini ta'minlovchi fundamental omildir. Kiberhujumlarning to'g'ridan-to'g'ri va bilvosita zararlari korxona kapitalizatsiyasiga jiddiy putur yetkazishi mumkinligini inobatga olgan holda, tizimli himoya usullarini qo'llash strategik zaruriyatdir. "Zero Trust" modelini joriylash, aktivlarni risklar asosida prioritetlash va kiber sug'urta mexanizmlaridan foydalanish orqali korxonalar ehtimoliy iqtisodiy talofatlarni minimal darajaga tushirishlari mumkin. Matematik modellar orqali investitsiyalarni optimallashtirish esa kiber xavfsizlik byudjetini xarajat emas, balki korxonaning kelajakdagi daromadlarini himoya qiluvchi samarali aktiv sifatida boshqarish imkonini beradi.

## XULOSA

Tadqiqot natijalari shuni ko'rsatdiki, zamonaviy ishlab chiqarish korxonalarining iqtisodiy salohiyati raqamli muhit bilan uzviy bog'liq bo'lgan murakkab, ko'p omilli va dinamik tizim sifatida

namoyon bo'ladi. Mazkur salohiyat korxonaning moddiy, moliyaviy va texnologik resurslaridan samarali foydalanishi bilan bir qatorda, ushbu resurslarning kiber tahdidlardan himoyalanganlik darajasiga ham bevosita bog'liqdir. Shu sababli, iqtisodiy salohiyatni baholashda faqat an'anaviy moliyaviy ko'rsatkichlar emas, balki kiber xavfsizlik xatarlarini ham hisobga oluvchi kompleks yondashuvdan foydalanish muhim ilmiy-amaliy ahamiyat kasb etadi. Tadqiqot davomida ishlab chiqilgan integrallashgan baholash algoritmi korxonalarning kiber xavfsizlik darajasini iqtisodiy imkoniyatlar bilan tizimli ravishda bog'lash, kutilayotgan ehtimoliy talofatlarni aniqlash va ichki resurslarni himoyalangan holda safarbar etish imkonini berdi. Mazkur algoritm asosida ishlab chiqarish quvvatlari, moliyaviy barqarorlik va innovatsion faollik bilan bir qatorda, "axborot aktivlarining daxlsizligi" va "kiber-risklarga chidamlilik" kabi muhim omillar yagona baholash tizimida birlashtirildi. Natijada korxona faoliyatining real holatini va kiberhujumlar natijasida yuzaga kelishi mumkin bo'lgan iqtisodiy inqirozlarni bashorat qiluvchi integral ko'rsatkich shakllantirildi.

Tahlillar shuni ko'rsatdiki, iqtisodiy salohiyatni baholash jarayonida kiber xavfsizlik ko'rsatkichlarining vazn koeffitsiyentlarini ilmiy asosda belgilash alohida ahamiyatga ega. Chunki kiber makondagi bitta zaiflik korxona aksiyalari qiymatiga yoki operatsion foydasiga turlicha ta'sir ko'rsatadi. Shu bois, ekspert baholash, statistik tahlil hamda ekonometrik modellashtirish (ROI va ALE formulalari) usullaridan foydalanish baholash natijalarining aniqligi va ishonchliligini oshiradi. Shuningdek, korxonalarda iqtisodiy salohiyatni himoya qilish jarayoniga zamonaviy axborot texnologiyalarini joriy etish, jumladan, ERP platformalari, Zero Trust modellari va sun'iy intellekt asosidagi kiber-himoya vositalaridan foydalanish korxonaning umumiy samaradorligini sezilarli darajada kuchaytiradi. Bu esa ma'lumotlarni tezkor qayta ishlash bilan birga, kiberhujumlar natijasida kelib chiqadigan operatsion to'xtalishlarning oldini olish va boshqaruv qarorlarini iqtisodiy xavf-xatarlarni inobatga olgan holda qabul qilish imkonini beradi..

#### **FOYDALANILGAN ADABIYOTLAR RO'YXATI**

- [1]. Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons. (Kiber jinoyatchilikning iqtisodiy motivlari va rag'batlar tahlili bo'yicha).
- [2]. Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457. (Kiber xavfsizlik investitsiyalarining 37% lik "oltin qoidasi" modeli).
- [3]. Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. *Congressional Research Service Report for Congress*. (Kiberhujumlarning aksiyadorlik qiymatiga va kapitalizatsiyaga ta'siri tahlili).
- [4]. Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International*

*Journal of Critical Infrastructure Protection*, 3(3-4), 103-117.

- [5]. Eide, E. R., & Showalter, M. H. (2011). Estimating the Economic Cost of Cybercrime. *Journal of Financial Crime*, 18(4).
- [6]. Ponemon Institute. (2023). *Cost of a Data Breach Report 2023*. IBM Security. (Global miqyosdagi kiberhujumlar qiymati – 4.45 mln dollar statistikasi bo'yicha).
- [7]. Cybersecurity Ventures. (2023). *2025 Official Cybercrime Report*. (2025-yilga borib kiber jinoyatchilik zarari 10.5 trillion dollarga yetishi haqidagi prognoz).
- [8]. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. (Tizimli risklar va ta'minot zanjiri hujumlari tahlili).
- [9]. SolarWinds Cyberattack Study. (2021). *The Economic Fallout of Supply Chain Attacks*. [Online resource].
- [10]. Statista. (2024). *Average cost of cybercrime worldwide from 2017 to 2028*. [Data portal].