

KIBERXAVFSIZLIKNING REAL SEKTOR KORXONALARI IQTISODIYOTIGA TA'SIRINI ANIQLASH VA BAHOLASH 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 korxonalarining iqtisodiy ko'rsatkichlariga kiberhujumlarning salbiy ta'siri va ularni kamaytirish strategiyalari tahlil qilinadi. Tadqiqotda kiberxavfsizlikka yo'naltirilgan investitsiyalarni xarajat sifatida emas, balki iqtisodiy zararni oldini oluvchi va korxona kapitalizatsiyasini himoya qiluvchi aktiv sifatida ko'rib chiqish masalalari yoritilgan. Iqtisodiy talofatlarni hisoblashda ROI va ALE modellari tahlil qilinib, korxonaning kiber-bardoshlilikini oshirish bo'yicha ilmiy tavsiyalar berilgan.

Kalit so'zlar: kiberxavfsizlik iqtisodiyoti, iqtisodiy talofatlar, xatarlarni boshqarish, moliyaviy barqarorlik, kiber-sug'urta, investitsion salohiyat, ROI, ALE moduli.

Abstract: This article analyzes the negative impact of cyberattacks on the economic performance of enterprises and discusses strategies for their mitigation. The research focuses on re-evaluating cybersecurity investments not merely as operational costs, but as essential assets that prevent economic losses and protect corporate capitalization. In calculating economic damages, ROI (Return on Investment) and ALE (Annual Loss Expectancy) models are analyzed, and scientific recommendations are provided for enhancing the cyber-resilience of enterprises.

Keywords: cybersecurity economics, economic losses, risk management, financial stability, cyber insurance, investment potential, ROI, ALE module.

Аннотация: В данной статье анализируется негативное влияние кибератак на экономические показатели предприятий и рассматриваются стратегии по их минимизации. В исследовании основное внимание уделяется вопросам рассмотрения инвестиций в кибербезопасность не как операционных расходов, а как активов, предотвращающих экономический ущерб и защищающих капитализацию предприятия. При расчете экономического ущерба анализируются модели ROI и ALE, а также даются научные рекомендации по повышению киберустойчивости предприятий.

Ключевые слова: экономика кибербезопасности, экономический ущерб, управление рисками, финансовая устойчивость, киберстрахование, инвестиционный потенциал, ROI, модуль ALE.

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. Cybersecurity Ventures prognozlariga ko'ra, 2025-yilga borib kiberjinoyatchilikdan keladigan yillik global zarar 10.5 trillion dollarni tashkil etishi kutilmogda⁵⁹.

Kiberxavfsizlik va iqtisodiy barqarorlik o'rtasidagi bog'liqlik xalqaro ilmiy doiralarda keng o'rganilayotgan dolzarb yo'nalishlardan biridir. Mavjud ilmiy tadqiqotlarni shartli ravishda uchta asosiy yondashuvga bo'lib tahlil qilish mumkin:

Iqtisodiy zararni modellashtirish yondashuvi: Ushbu yo'nalishning asoschilaridan biri R. Anderson (2001) o'zining fundamental ishlarida kiberjinoyatchilikning iqtisodiy motivlarini tahlil qildi. U himoya tizimidagi kamchiliklar ko'pincha texnik nosozlikdan ko'ra, iqtisodiy rag'batlarning noto'g'ri taqsimlanishi (incentive misalignment) natijasi ekanligini ta'kidlaydi. Shu bilan birga, L. Gordon va M. Loeb (2002) modeli kiberxavfsizlikka investitsiya kiritishning optimal darajasini aniqlashda iqtisodiy "oltin qoida"ni ilgari surdi. Ularning nazariyasiga ko'ra, kiberxavfsizlik xarajatlari kutilayotgan yillik zararining (ALE) taxminan 37 foizdan oshmasligi kerak, aks holda investitsiya iqtisodiy jihatdan o'zini oqlamaydi.

Reputatsion va bilvosita zararlar tahlili: Cashell va boshqalar (2004) kiberhujumdan keyin korxona aksiyalari qiymatining pasayishini o'rganib, ma'lumotlar sizib chiqishi haqidagi xabar e'lon qilingandan so'ng, kompaniya kapitalizatsiyasi o'rtacha 1 foizdan 5 foizgacha yo'qotishga uchrashini isbotlagan. Ponemon Institute (2023) hisobotlari esa kiberhujumlarning o'rtacha qiymati global miqyosda 4.45 million dollarga yetganini ko'rsatib, asosiy urg'uni mijozlarning ommaviy ketishi va brendga bo'lgan ishonchning emirilishi kabi "yashirin xarajatlar"ga qaratadi.

Tizimli risklar va ta'minot zanjiri tahlili: Zamonaviy tadqiqotlarda ta'minot zanjiri hujumlari (Supply Chain Attacks) orqali bitta zaif hamkor korxona butun bir iqtisodiy ekotizimga zarar yetkazishi mumkinligi (masalan, SolarWinds hodisasi) o'rganilmogda. O'zbekistonlik tadqiqotchilar ham raqamli iqtisodiyot sharoitida axborot xavfsizligini ta'minlashning iqtisodiy jihatlariga e'tibor

⁵⁹ Cybersecurity Ventures (2023). 2023 Official Cybercrime Report. [Elektron resurs]. Kirish tartibi: <https://cybersecurityventures.com/cybercrime-report-2023/> (Ma'lumot: 2025-yilga borib 10.5 trillion dollar zarar haqidagi prognoz aynan shu manbaga tegishli).

Morgan, S. (2021). Cyberwarfare in the C-Suite: 2021 Report on Cybercrime. Cybersecurity Ventures. (Raqamli transformatsiya va ekzistensial tahdidlar tahlili).

Statista (2024). Estimated cost of cybercrime worldwide from 2017 to 2028. [Data portal]. Kirish tartibi: <https://www.statista.com/statistics/1280009/global-cybercrime-cost-forecast/>

qaratmoqdalar, biroq real sektor korxonalarida kiber-risklarni iqtisodiy baholashning universal metodologiyasi hali to'liq shakllanmagan.

Yuqoridagi nazariy yondashuvlar va xalqaro statistik ma'lumotlarga tayangan holda, ushbu maqolaning maqsadi O'zbekiston sharoitidagi korxonalar uchun kiberxavfsizlikni iqtisodiy boshqarishning optimal modellarini ishlab chiqish hamda matematik usullar yordamida talofatlarni minimallashtirish strategiyalarini asoslab berishdan iborat.

Tadqiqotning metodologik asosi kiberxavfsizlikka yo'naltirilgan xarajatlarni iqtisodiy optimallashtirish va xatarlarni miqdoriy baholashga qaratilgan kompleks yondashuvdan iborat. Tadqiqot davomida quyidagi usullar qo'llanildi: Iqtisodiy modellashtirish va Gordon-Loeb modeli. Kiberxavfsizlikka investitsiya kiritishning iqtisodiy jihatdan eng maqbul nuqtasini aniqlash uchun Gordon-Loeb (2002) modelidan foydalanildi. Ushbu modelga ko'ra, axborotni himoya qilish uchun sarflanadigan xarajatlar kutilayotgan iqtisodiy zararning ma'lum bir qismini tashkil etishi lozim. Metodning mohiyati shundaki, xavfsizlik darajasi oshgani sayin, har bir keyingi himoya birligining samaradorligi pasayib boradi (kamayib boruvchi samaradorlik qonuni). Model yordamida korxonaning axborot aktivlarining zaiflik darajasi va ularning buzilishidan kelib chiqadigan ehtimoliy zarar o'rtasidagi muvozanat tahlil qilindi. Qiyosiy va sifat tahlili. Tadqiqotda kiberhujumlar natijasida yuzaga keladigan iqtisodiy talofatlar ikki toifaga — bevosita va bilvosita zararlarga ajratilgan holda qiyoslandi. Bevosita zararlarning sifatida pul mablag'larining o'g'rilanishi, texnik infratuzilmani tiklash xarajatlari va jarimalar ko'rib chiqildi. Bilvosita zararlarning tahlilida esa mijozlarning ishonchini yo'qotish, brend qiymatining pasayishi va birja bozorida korxona aksiyalari narxining tushishi kabi faktorlarning uzoq muddatli iqtisodiy ta'siri solishtirildi. Matematik baholash (ROI va ALE). Investitsiyalarning rentabellik darajasini miqdoriy ifodalash uchun ALE (Annual Loss Expectancy) va ROSI (Return on Security Investment) koeffitsiyentlari qo'llanildi. ALE formulasi ($ALE = ARO \times SLE$) orqali yillik kutilayotgan zarar miqdori aniqlandi, bunda ARO — hujumlarning yillik chastotasi, SLE — bitta hujumdan keladigan bir martalik zarar miqdoridir. ROI tahlili esa korxona tomonidan joriylangan kiber-himoya tizimi ALE miqdorini qanchalik kamaytirishi va bu tejamkorlik tizim xarajatlarini qanchalik qoplashini hisoblash imkonini berdi. Tizimli yondashuv: "Zero Trust" va Kiber-sug'urta. Tadqiqotda korxona xavfsizligiga ekotizim sifatida yondashildi. "Zero Trust" (Nol ishonch) arxitekturasining iqtisodiy samaradorligi — insayder hujumlarini kamaytirish va operatsion barqarorlikni saqlash nuqtai nazaridan baholandi. Shuningdek, xatarlarni transfer qilish (o'tkazish) usuli sifatida kiber-sug'urta mexanizmi tahlil qilindi. Bu usul yordamida korxona o'zi ko'tara olmaydigan yirik ("falokatli") moliyaviy risklarni sug'urta kompaniyasi zimmasiga yuklash orqali moliyaviy barqarorlikni ta'minlash modeli taklif etildi.

Tadqiqotning metodologik asosi kiberxavfsizlikka yo'naltirilgan xarajatlarni iqtisodiy optimallashtirish va xatarlarni miqdoriy baholashga qaratilgan kompleks yondashuvdan iborat. Tadqiqot davomida quyidagi usullar qo'llanildi:

IQTISODIY MODELLASHTIRISH VA GORDON-LOEB MODEL

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 qoldirmoqda. 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.

Kiberxavfsizlikka investitsiya kiritishning iqtisodiy jihatdan eng maqbul nuqtasini aniqlash uchun Gordon-Loeb (2002) modelidan foydalanildi. Ushbu modelga ko'ra, axborotni himoya qilish uchun sarflanadigan xarajatlar kutilayotgan iqtisodiy zararining ma'lum bir qismini tashkil etishi lozim. Metodning mohiyati shundaki, xavfsizlik darajasi oshgani sayin, har bir keyingi himoya birligining samaradorligi pasayib boradi (kamayib boruvchi samaradorlik qonuni). Model yordamida korxonaning axborot aktivlarining zaiflik darajasi va ularning buzilishidan kelib chiqadigan ehtimoliy zarar o'rtasidagi muvozanat tahlil qilindi.

Qiyosiy va sifat tahlili. Tadqiqotda kiberhujumlar natijasida yuzaga keladigan iqtisodiy talofatlar ikki toifaga — bevosita va bilvosita zararlarga ajratilgan holda qiyoslandi. Bevosita zararlari sifatida pul mablag'larining o'g'rilanishi, texnik infratuzilmani tiklash xarajatlari va jarimalar ko'rib chiqildi. Bilvosita zararlari tahlilida esa mijozlarning ishonchini yo'qotish, brend qiymatining pasayishi va birja bozorida korxona aksiyalari narxining tushishi kabi faktorlarning uzoq muddatli iqtisodiy ta'siri solishtirildi.

Matematik baholash (*ROI* va *ALE*). Investitsiyalarning rentabellik darajasini miqdoriy ifodalash uchun *ALE* (Annual Loss Expectancy) va *ROSI* (Return on Security Investment) koeffitsiyentlari qo'llanildi. *ALE* quyidagi ifoda orqali aniqlanadi:

$$ALE = ARO * SLE$$

bu yerda:

ALE - yillik kutilayotgan zarar miqdori;

ARO — hujumlarning yillik chastotasi;

SLE — bitta hujumdan keladigan bir martalik zarar miqdoridir.

ROI tahlili esa korxona tomonidan joriylangan kiber-himoya tizimi *ALE* miqdorini qanchalik kamaytirishi va bu tejamkorlik tizim xarajatlarini qanchalik qoplashini hisoblash imkonini berdi.

Tizimli yondashuv: "Zero Trust" va Kiber-sug'urta. Tadqiqotda korxona xavfsizligiga ekotizim sifatida yondashildi. "Zero Trust" (Nol ishonch) arxitekturasining iqtisodiy samaradorligi — insayder

hujumlarini kamaytirish va operatsion barqarorlikni saqlash nuqtai nazaridan baholandi. Shuningdek, xatarlarni transfer qilish (o'tkazish) usuli sifatida kiber-sug'urta mexanizmi tahlil qilindi. Bu usul yordamida korxona o'zi ko'tara olmaydigan yirik ("falokatli") moliyaviy risklarni sug'urta kompaniyasi zimmasiga yuklash orqali moliyaviy barqarorlikni ta'minlash modeli taklif etildi.

Kiberhujumlarning korxona iqtisodiyotiga ta'sirini o'rganishda ularning zararlari tabiatini tizimli tasniflash va miqdoriy-sifat ko'rsatkichlari bo'yicha qiyoslash metodologik jihatdan muhim hisoblanadi. Akademik nuqtai nazardan, kiber-zararlar faqatgina joriy balansdagi yo'qotishlar bilan cheklanmay, korxonaning kelajakdagi pul oqimlari (*future cash flows*) va bozor qiymatiga (*market capitalization*) ta'sir etuvchi strategik omildir.

Quyida bevosita va bilvosita zararlarning akademik tahlili va ularning qiyosiy jadvali keltirilgan.

Bevosita zararlar (Direct Costs): Bular kiberhujum sodir bo'lgan vaqtda yoki undan so'ng darhol yuzaga keladigan, moliyaviy hisobotlarda aniq qayd etiladigan va miqdoriy o'lchanadigan xarajatlardir. Ular asosan korxonaning operatsion aktivlarini tiklash va huquqiy majburiyatlarni bajarish bilan bog'liq.

Bilvosita zararlar (Indirect/Consequential Costs): Bular hujumdan so'ng uzoq muddatli istiqbolda namoyon bo'ladigan, ko'pincha nomoddiy aktivlarning (*intangible assets*) qadrsizlanishi bilan bog'liq bo'lgan yo'qotishlardir. Bilvosita zararlar korxonaning strategik barqarorligiga ko'proq putur yetkazadi va ularni aniq hisoblash murakkab ekonometrik modellarni talab etadi. Quyidagi jadvalda kiberhujumlar natijasida yuzaga keladigan zararlarning strukturaviy qiyoslanishi keltirilgan(1-jadval):

1-jadval.

Kiberhujumlar natijasida yuzaga keladigan iqtisodiy zararlarning strukturaviy-qiyosiy tasnifi

T/r	Zarar toifasi	Bevosita zararlar (Direct)	Bilvosita zararlar (Indirect)
1.	Iqtisodiy tabiati	Moddiy va darhol namoyon bo'luvchi	Nomoddiy va kechikib namoyon bo'luvchi
2.	Asosiy tarkibi	– Bank hisoblaridan o'g'irlangan mablag'lar. – Tizimlarni tiklash va IT-audit xarajatlari. – Ransomware (tovlamachilik) to'lovlari. – Qonuniy jarimalar va sud xarajatlari.	– Brend qiymatining pasayishi (Reputatsiya). – Mijozlarning raqobatchilarga o'tib ketishi (<i>Churn rate</i>). – Intellektual mulkning o'g'irlanishi. – Aksiyalar narxining tushishi.
3.	O'lchov usuli	Buxgalteriya hisobi va tranzaksiya tahlili	Ekonometrik modellashtirish va bozor kapitalizatsiyasi tahlili
4.	Vaqt ko'lami	Qisqa muddatli (0-6 oy)	O'rta va uzoq muddatli (1-5 yil)
5.	Bozorga ta'siri	Operatsion likvidlikning pasayishi	Investitsion jozibadorlikning yo'qolishi

Ushbu jadval kiberhujumlarning korxona iqtisodiyotiga ta'sirini ikki xil fundamental yondashuv — bevosita va bilvosita zararlar kesimida tahlil qiladi. Akademik nuqtai nazardan, bevosita zararlar korxonaning balans hisobotlarida darhol aks etuvchi (masalan, mablag'larning o'g'irlanishi yoki tizimni tiklash xarajatlari) "ko'rinadigan" yo'qotishlardir.

Biroq, jadvaldagi qiyosiy tahlil shuni ko'rsatadiki, bilvosita zararlar (reputatsiya yo'qolishi, aksiyalar narxining tushishi) o'zining ko'lami va uzoq muddatli ta'siri bo'yicha ancha xavfliroqdir. Bu zarar turi korxonaning nomoddiy aktivlarini (brend, intellektual mulk) qadrsizlantiradi. Tadqiqot metodologiyasida ushbu jadval korxona rahbarlariga kiberxavfsizlikka faqat texnik xarajat emas, balki kapitallashuvni saqlash vositasi sifatida qarash zarurligini ilmiy asoslab beradi.

Kiberhujum sodir bo'lganda, korxona "hodisaga javob berish" (*Incident Response*) bosqichida katta miqdorda kutilmagan xarajatlarga duch keladi. Masalan, kiber-ekskavatsiya (dalillarni yig'ish) va raqamli sud ekspertizasi xizmatlari yuqori tariflarda baholanadi. Buning natijasida korxonaning aylanma mablag'lari kamayadi, bu esa qisqa muddatli moliyaviy majburiyatlarni bajarishda qiyinchiliklar tug'dirishi mumkin. 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.

Akademik tadqiqotlar (masalan, *Cashell et al.*) shuni ko'rsatadiki, ma'lumotlar sizib chiqishi haqidagi xabar e'lon qilingan "X" kunida korxona aksiyalari o'rtacha 1.1% dan 3% gacha qiymatini yo'qotadi. Biroq, agar hujum intellektual mulkka (nou-xau) daxl qilgan bo'lsa, uzoq muddatli kapitallashuvning pasayishi 15% gacha yetishi mumkin. Bu investitsion jozibadorlikning strategik eroziyasi hisoblanadi. Korxonaning ishlab chiqarish quvvatlari to'xtab qolishi (Downtime) natijasida keladigan zararlarni quyidagi jadval orqali batafsilroq ko'rish mumkin(2-jadval):

2-jadval.

Operatsion to'xtalishlar (Downtime) natijasida keladigan boy berilgan foyda va samaradorlik ko'rsatkichlari tahlili

T/r	Ko'rsatkich	Ta'sir mexanizmi	Iqtisodiy oqibat
1.	Boy berilgan foyda	Savdo va xizmat ko'rsatishning to'xtashi	Yillik daromadning (Revenue) pasayishi
2.	Mehnat unumdorligi	Xodimlarning IT-tizimlarsiz bekor qolishi	Ish haqi fondining samarasiz sarflanishi
3.	Logistik zanjir	Yetkazib berish shartnomalarining buzilishi	Penya va jarimalar, hamkorlik aloqalarining uzilishi
4.	Qayta tiklash	Ma'lumotlarni rezerv nusxalardan tiklash	Qo'shimcha mehnat va texnik resurslar sarfi

Mazkur jadval kiberhujum natijasida korxona faoliyatining vaqtincha to'xtab qolishi (IT-infratuzilmaning ishdan chiqishi) keltirib chiqaradigan zanjirsimon iqtisodiy oqibatlarni ochib beradi. Jadvalda ta'sir mexanizmlari uchta asosiy yo'nalishga — moliyaviy daromad, inson resurslari samaradorligi va logistik barqarorlikka bo'lingan.

Tahlil natijalari shuni ko'rsatadiki, operatsion to'xtalish faqatgina mahsulot sotilmaganligi uchun boy berilgan foyda bilan cheklanib qolmaydi. U mehnat unumdorligining nolga tushishi (xodimlar IT-tizimsiz ishlay olmasligi) va logistik zanjirdagi uzilishlar sababli yuzaga keladigan jarimalar orqali korxonaning sof foyda marjasini keskin kamaytiradi. Ushbu jadval maqolaning matematik qismidagi ALE (yillik kutilayotgan zarar) ko'rsatkichini hisoblashda empirik asos bo'lib xizmat qiladi.

Tahlil natijalari shuni ko'rsatadiki, bilvosita zararlar ko'pincha bevosita zararlardan 5 dan 10 barobargacha ko'proq bo'lishi mumkin. Shuning uchun korxonalar kiberxavfsizlikka investitsiya kiritishda faqatgina "antivirus sotib olish" (bevosita himoya) emas, balki "biznes barqarorligini boshqarish" (*Business Continuity Management*) tamoyiliga tayanishi lozim.

Korxonalar o'z iqtisodiy xavfsizlik strategiyasida "Kiber-rezerv fondi"ni shakllantirishlari va bu fond miqdorini yuqoridagi jadvalda keltirilgan ALE (yillik kutilayotgan zarar) prognozlari asosida belgilashlari maqsadga muvofiqdir.

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). *Why Information Security is Hard - An Economic Perspective*. University of Cambridge Computer Laboratory.
- [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.
- [3]. Cybersecurity Ventures. (2023). *2023 Official Cybercrime Report*. [Online]. Available: <https://cybersecurityventures.com/cybercrime-report-2023/>
- [4]. Ponemon Institute. (2023). *Cost of a Data Breach Report 2023*. IBM Security.
- [5]. Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *The Economic Impact of Cyber-Attacks*. Congressional Research Service, Library of Congress.
- [6]. Statista. (2024). *Estimated cost of cybercrime worldwide from 2017 to 2028*. [Data portal].
- [7]. Morgan, S. (2021). *Cyberwarfare in the C-Suite: Report on Cybercrime*. Cybersecurity Ventures.
- [8]. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207.
- [9]. Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber insurance? *The Journal of Risk Finance*, 17(5), 474-491.
- [10]. O'zbekiston Respublikasining Qonuni. (2022). *Kiberxavfsizlik to'g'risida* (O'RQ-764-son). Toshkent.