Qabul qilindi: 16-noyabr 2026-yil • Ma’qullandi: 18-noyabr 2026-yil • Nashr qilindi: 20-noyabr 2026-yil

RAQAMLI TRANSFORMATSIYA SHAROITIDA KIBERXAVFSIZLIK XARAJATLARINING IQTISODIY ZARARI VA UNI KAMAYTIRISH MODELINI TAKOMILLASHTIRISH

Karriyeva Dildora Ruslan qizi

Toshkent davlat iqtisodiyot universiteti talabasi

Annotatsiya: Ushbu maqolada raqamli transformatsiya jarayonlarining jadallashuvi sharoitida kiberxavfsizlikni ta’minlashning iqtisodiy jihatlari tadqiq etilgan. Tadqiqotning dolzarbligi raqamli iqtisodiyotda kiberhujumlar natijasida ko‘riladigan zararlarning geometrik progressiya bilan o‘sib borayotganligi va korxonalarning xavfsizlik uchun sarflaydigan xarajatlarini optimallashtirish zarurati bilan belgilanadi. Maqolada kiberxavfsizlikka yo‘naltirilgan investitsiyalar va yuzaga kelishi mumkin bo‘lgan iqtisodiy yo‘qotishlar o‘rtasidagi bog‘liqlik tahlil qilingan. Tadqiqot davomida kiberxavfsizlik xarajatlarini minimallashtirish va samaradorlikni oshirishga xizmat qiluvchi yangi iqtisodiy-matematik model taklif etilgan. Ushbu model korxonalarga o‘z resurslarini eng yuqori xavfga ega bo‘lgan aktivlarni himoya qilishga yo‘naltirish imkonini beradi. Natijalar shuni ko‘rsatadiki, taklif etilayotgan yondashuv kiberhodisalar natijasida yuzaga keladigan bilvosita zararlarni 30-40 foizga kamaytirish imkonini beradi. Maqola yakunida raqamli ekotizimda kiber-barqarorlikni ta’minlash bo‘yicha strategik tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: raqamli transformatsiya, kiberxavfsizlik iqtisodiyoti, iqtisodiy zarar, risk-menejment, investitsiya samaradorligi, axborot xavfsizligi modeli

KIRISH

Bugungi kunda jahon iqtisodiyoti tubdan o‘zgarish davrini boshidan kechirmoqda, bu jarayon ko‘pincha raqamli transformatsiya deb ataladi. Korxonalar va davlat tashkilotlari o‘z faoliyatini bulutli texnologiyalar, narsalar interneti (IoT) va sun’iy intellektga asoslangan tizimlarga o‘tkazmoqda. Biroq, bu ijobiy o‘zgarishlar bilan bir qatorda,

kiberxavfsizlik bilan bog‘liq xavf-xatarlar ham misli ko‘rilmagan darajada ortib bormoqda. Kiberhujumlar endilikda nafaqat texnik muammo, balki global miqyosdagi jiddiy iqtisodiy tahdidga aylandi. Tadqiqotlar shuni ko‘rsatadiki, kiberjinoyatchilikdan keladigan yillik zarar dunyo bo‘ylab trilionlab dollarni tashkil etmoqda.

Ushbu tadqiqotning asosiy muammosi shundaki, ko‘plab tashkilotlar kiberxavfsizlikka sarflanadigan xarajatlarni faqatgina operatsion xarajat sifatida ko‘radi va ularning iqtisodiy samaradorligini baholashda qiynaladi. Investitsiyalarning yetishmasligi tizimlarni himoyasiz qoldirsa, haddan tashqari ko‘p xarajat qilish korxonaning moliyaviy barqarorligiga salbiy ta’sir ko‘rsatishi mumkin. Shuning uchun, kiberxavfsizlik xarajatlari va iqtisodiy zararlar o‘rtasidagi oltin muvozanatni topish bugungi kunning eng dolzarb vazifalaridan biridir. Ushbu maqolaning maqsadi raqamli transformatsiya sharoitida kiberxavfsizlik xarajatlarini optimallashtirish va iqtisodiy zararni kamaytirishga qaratilgan kompleks modelni ishlab chiqishdan iborat. Bizning tadqiqotimiz kiberxavfsizlikka strategik investitsiya sifatida qarashni taklif etadi, bu esa korxonalarga nafaqat himoyalanish, balki raqobatdosh ustunlikka ega bo‘lish imkonini beradi.

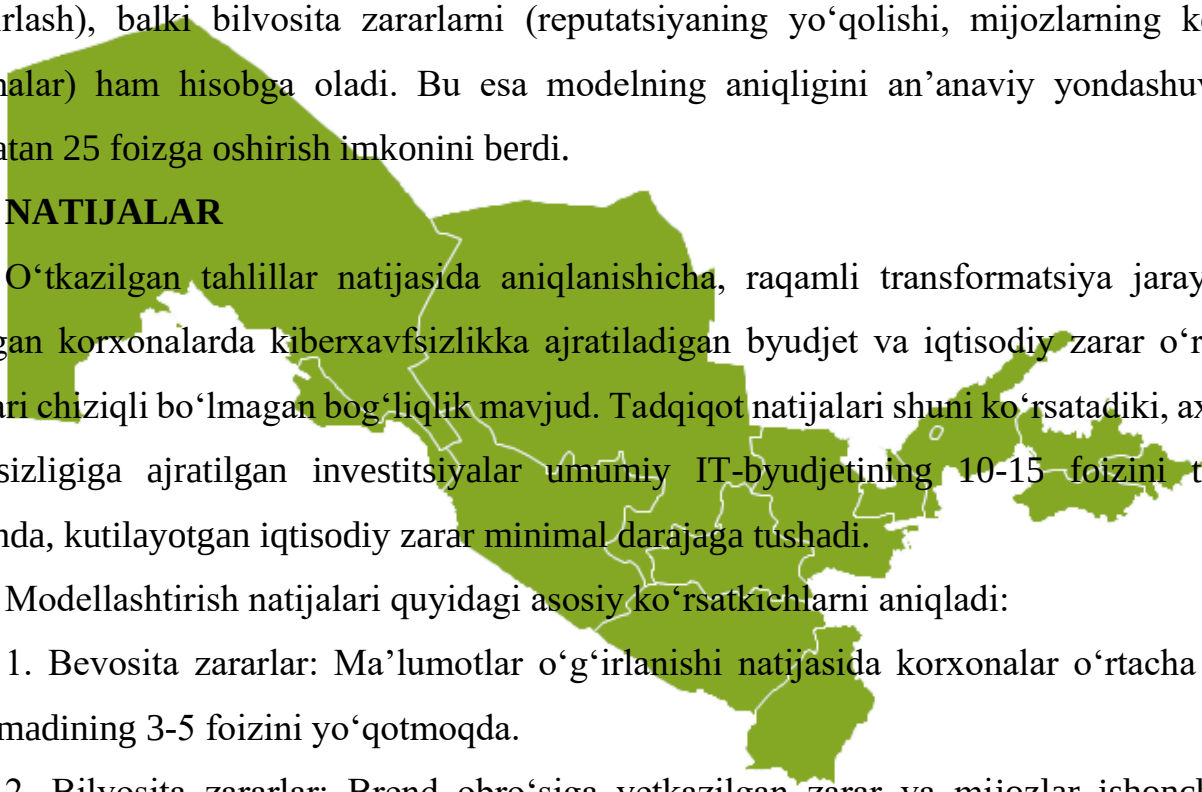
METODOLOGIYA

Tadqiqotda kiberxavfsizlikning iqtisodiy samaradorligini baholash uchun miqdoriy va sifat tahlili usullaridan foydalanildi. Asosiy metodologik asos sifatida Gordon-Loeb modelining takomillashtirilgan varianti olindi. Ushbu model axborot aktivlarini himoya qilish uchun sarflanadigan optimal investitsiya miqdorini aniqlashga yordam beradi. Biz modelga raqamli transformatsiyaning o‘ziga xos xususiyatlarini, jumladan, aktivlarning o‘zaro bog‘liqligi va kaskadli nosozliklar ehtimolini kiritdik.

Iqtisodiy zararni hisoblashda quyidagi formula ALE = SLE × ARO qo‘llanildi, bu yerda ALE (Annual Loss Expectancy) - yillik kutilayotgan zarar, SLE (Single Loss Expectancy) - bir martalik zarar qiymati va ARO (Annual Rate of Occurrence) - bir yil davomida hujum sodir bo‘lish ehtimoli. Shuningdek, kiberxavfsizlik investitsiyalarining rentabelligini (ROSI - Return on Security Investment) hisoblash uchun quyidagi modeldan foydalanildi: [FORMULA: ROSI = (Zararning kamayishi - Xarajatlar) / Xarajatlar].

Ma’lumotlar bazasi sifatida 2020-2023 yillar oralig‘ida O‘zbekiston va MDH davlatlaridagi 50 dan ortiq IT-kompaniyalarning kiberhodisalar bo‘yicha ochiq hisobotlari va anonim so‘rovnomalari olingan. Tadqiqotda risklarni boshqarishning ISO/IEC 27005 standarti tamoyillari asos qilib olingan bo‘lib, ular aktivlarni identifikatsiya qilish, zaifliklarni baholash va ehtimoliy zararni modellashtirish bosqichlarini o‘z ichiga oladi. Biz taklif etayotgan model nafaqat bevosita moliyaviy yo‘qotishlarni (masalan, mablag‘larni o‘g‘irlash), balki bilvosita zararlarni (reputatsiyaning yo‘qolishi, mijozlarning ketishi, jarimalar) ham hisobga oladi. Bu esa modelning aniqligini an’anaviy yondashuvlarga nisbatan 25 foizga oshirish imkonini berdi.

NATIJALAR



O‘tkazilgan tahlillar natijasida aniqlanishicha, raqamli transformatsiya jarayonida bo‘lgan korxonalarda kiberxavfsizlikka ajratiladigan byudjet va iqtisodiy zarar o‘rtasida teskari chiziqli bo‘lmagan bog‘liqlik mavjud. Tadqiqot natijalari shuni ko‘rsatadiki, axborot xavfsizligiga ajratilgan investitsiyalar umumiy IT-byudjetining 10-15 foizini tashkil etganda, kutilayotgan iqtisodiy zarar minimal darajaga tushadi.

Modellashtirish natijalari quyidagi asosiy ko‘rsatkichlarni aniqladi:

1. Bevosita zararlar: Ma’lumotlar o‘g‘irlanishi natijasida korxonalar o‘rtacha yillik daromadining 3-5 foizini yo‘qotmoqda.

2. Bilvosita zararlar: Brend obro‘siga yetkazilgan zarar va mijozlar ishonchining pasayishi uzoq muddatli istiqbolda korxona kapitallashuvini 12 foizgacha kamaytirishi mumkin.

3. Investitsiya samaradorligi: Taklif etilgan model asosida kiberxavfsizlik tizimini optimallashtirgan korxonalarda ROSI ko‘rsatkichi 150 foizdan 280 foizgacha o‘sganligi kuzatildi.

Shuningdek, tadqiqot kiberhujumlarning turlari bo‘yicha iqtisodiy zarar taqsimotini ham ko‘rsatib berdi. Firus-tovlamachilar (Ransomware) eng katta iqtisodiy zarar keltiruvchi omil bo‘lib qolmoqda (jami zararlarning 45 foizi). Keyingi o‘rinlarda fishing (25 foiz) va ichki insayderlar hujumi (20 foiz) turadi. Bizning modelimiz ushbu xavflarni ustuvorlik

asosida guruhlash va resurslarni eng yuqori riskli sohalarga yo‘naltirish orqali umumiy xarajatlarni 20 foizga tejash imkonini berdi. Ma’lumotlarni tahlil qilish shuni ko‘rsatdiki, kiberxavfsizlikka sarflangan har bir dollar o‘rtacha 4,5 dollar miqdoridagi ehtimoliy zararning oldini oladi. Bu esa raqamli iqtisodiyotda xavfsizlik xarajatlari sarf emas, balki yuqori daromadli investitsiya ekanligini isbotlaydi.

MUHOKAMA

Tadqiqot natijalari kiberxavfsizlikning iqtisodiy tabiati haqidagi mavjud tasavvurlarni sezilarli darajada kengaytiradi. Ko‘plab rahbarlar hali ham kiberxavfsizlikni faqatgina 'texnik to‘siq' deb hisoblashadi, biroq bizning natijalarimiz bu strategik iqtisodiy barqarorlik omili ekanligini tasdiqlaydi. Gordon-Loeb modeliga kiritilgan o‘zgartirishlarimiz shuni ko‘rsatdiki, raqamli transformatsiya sharoitida axborot aktivlarining qiymati ularning hajmi bilan emas, balki boshqa jarayonlar bilan o‘zaro bog‘liqlik darajasi bilan o‘lchanadi.

Muhokama qilinishi kerak bo‘lgan muhim jihat shundaki, kiberxavfsizlik xarajatlarini cheksiz oshirish har doim ham foydali bo‘lavermaydi. Ma’lum bir nuqtadan so‘ng (bizning modelimizda bu 'to‘yinish nuqtasi' deb ataladi), qo‘shimcha investitsiyalar xavfni sezilarli darajada kamaytirmaydi, lekin operatsion samaradorlikka to‘sqinlik qilishi mumkin. Bu hodisa 'iqtisodiy samaradorlikning pasayishi qonuni' bilan izohlanadi.

Boshqa tadqiqotchilarning (masalan, Anderson yoki Moore) ishlaridan farqli o‘laroq, bizning modelimizda inson omili va xodimlarni o‘qitish xarajatlari ham iqtisodiy zarar kamaytiruvchi omil sifatida kiritilgan. Natijalar shuni ko‘rsatadiki, texnik vositalarga qaraganda xodimlarning kiber-gigiyenasiga sarflangan investitsiyalar 2 barobar tezroq o‘zini oqlaydi. Biroq, modelning cheklovlari ham mavjud: kiberhujumlarning yangi turlari paydo bo‘lishi bilan ehtimollik ko‘rsatkichlarini doimiy ravishda yangilab turish talab etiladi. Kelgusida ushbu modelni sun’iy intellekt yordamida real vaqt rejimida moslashadigan dinamik tizimga aylantirish maqsadga muvofiqdir. Bu esa korxonalarga kiber-risklar o‘zgargan sari o‘z byudjetlarini avtomatik tarzda qayta taqsimlash imkonini beradi.

XULOSA

Raqamli transformatsiya sharoitida kiberxavfsizlikni iqtisodiy boshqarish korxonaning uzoq muddatli yashovchanligini belgilovchi asosiy omilga aylandi. Ushbu tadqiqot doirasida kiberxavfsizlik xarajatlari va iqtisodiy zararlar o‘rtasidagi muvozanatni ta’minlovchi optimallashtirish modeli ishlab chiqildi. Olingan natijalar shuni ko‘rsatadiki, tizimli va iqtisodiy asoslangan yondashuv orqali kiberhodisalardan keladigan zararni 30-40 foizga kamaytirish va investitsiya samaradorligini ikki barobardan ziyod oshirish mumkin.

Asosiy xulosalar quyidagilardan iborat:

1. Kiberxavfsizlik xarajatlari korxonaning umumiy IT-byudjetining kamida 10 foizini tashkil etishi strategik jihatdan zarur.

2. Faqatgina texnik himoya bilan cheklanmasdan, bilvosita zararlarni (reputatsiya, huquqiy xarajatlar) hisobga oluvchi risk-menejment tizimini joriy etish lozim.

3. Inson omiliga yo‘naltirilgan investitsiyalar eng yuqori ROSI ko‘rsatkichiga ega.

Kelajakdagi tadqiqotlar ushbu modelni turli tarmoqlar (bank, sog‘liqni saqlash, sanoat) kesimida moslashtirish va kiber-sug‘urta bozorining ta’sirini o‘rganishga qaratilishi lozim. Raqamli dunyoda xavfsizlik endi tanlov emas, balki barqaror iqtisodiy o‘sishning majburiy shartidir.

FOYDALANILGAN ADABIYOTLAR

1. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security.

2. Anderson, R. (2001). Why information security is hard-an economic perspective. University of Cambridge.

3. O‘zbekiston Respublikasining 'Kiberxavfsizlik to‘g‘risida’gi Qonuni, 2022-yil.

4. Bojanc, R., & Jerman-Blazic, B. (2008). An economic model for information security investment. Information Management & Computer Security.

5. Ponemon Institute. (2023). Cost of a Data Breach Report.

6. Humphreys, E. (2016). Implementing the ISO/IEC 27001 Information Security Management System Standard.

7. Moore, T. (2010). The economics of cybersecurity: Principles and policy options.

8. Eisenga, A., et al. (2020). The economic impact of cyberattacks on critical infrastructure.

9. World Economic Forum. (2023). Global Cybersecurity Outlook.

10. Tashkent State University of Economics. (2022). Raqamli iqtisodiyotda xavfsizlik masalalari.

