

AXBOROT XAVFSIZLIGI TAHDIDLARINING IQTISODIY ZARARINI BAHOLASH

Yuldashev Shadiyor Shuxrat o'g'li

Toshkent davlat iqtisodiyot universiteti To'rtko'l fakulteti

Mutaxassislik gumanitar va aniq fanlar kafedrası Katta o'qituvchisi

Yaqubova Asaloy Sardorbek qizi

Toshkent davlat iqtisodiyot universiteti To'rtko'l fakulteti

Buxgalteriya hisobi yo'nalishi talabasi

Annotatsiya. Axborot xavfsizligi tahdidlarining iqtisodiy zarari zamonaviy raqamli iqtisodiyot sharoitida beqiyos o'sib bormoqda. Global miqyosda kiberxavfsizlik hodisalari – ma'lumotlar buzilishi, kiberhujumlar, firibgarliklar va boshqa tahdidlar – yirik korxonalar, davlat idoralari va kichik biznes uchun milliardlab dollarga teng to'g'ridan-to'g'ri va bilvosita moliyaviy yo'qotishlarga olib kelmoqda. Masalan, dunyo bo'yicha kiberjinoyatchilikdan keladigan zarar 2025 yilda taxminan 10,5 trillion AQSh dollarini tashkil etishi prognoz qilinmoqda, bu esa har yili 15% o'sish sur'atini ko'rsatadi. Shuningdek, ma'lumotlar buzilishining o'rtacha global xarajatlari bir necha million dollarga yetadi va tarmoqlarni qayta tiklash, qonuniy jarimalar, ishlab chiqarishning to'xtashi va obro'ga yetadigan zarar kabi omillarni o'z ichiga oladi. Yirik milliy iqtisodiyotlarda ham kiberhujumlar inflyatsiyalar, ta'minot zanjirlarining uzilishi va korporativ daromadlarning kamayishiga olib keladi – masalan, Germaniya iqtisodiyoti uchun bunday zarar o'tgan yili 300 milliard yevro atrofida baholandi. Shu bois, axborot xavfsizligi tahdidlarining iqtisodiy zararini tizimli ravishda baholash raqamli strategiyalarni shakllantirish, xavfni boshqarish siyosatlarini takomillashtirish va iqtisodiy barqarorlikni ta'minlash uchun muhim ilmiy va amaliy asos bo'lib xizmat qiladi.

Kalit so'zlar": Axborot xavfsizligi, Kiberxavf-xatarlar, Iqtisodiy zarar, Kiberjinoyatchilik, Ma'lumotlar buzilishi, Raqamli iqtisodiyot, Tahdidlarni baholash, Risklarni boshqarish, Cybercrime economic impact, Cybersecurity cost statistics

KIRISH

Bugungi global raqamli iqtisodiyot sharoitida axborot texnologiyalari va ularning tarmoqlari mavjud iqtisodiy tizimning ajralmas elementi bo'lib qoldi. Shu bilan birga, axborot xavfsizligi tahdidlarining soni va murakkabligi keskin oshib, korxonalar, davlat idoralari va shaxsiy foydalanuvchilar uchun jiddiy xavf manbaiga aylanishi kuzatilmoqda. Kiberxavf-xatarlar – ma'lumotlar buzilishi, xizmat rad etish (DDoS) hujumlari, ransomware va firibgarliklar – nafaqat texnik tizimlarga, balki iqtisodiyotning strukturaviy barqarorligiga ham salbiy ta'sir ko'rsatadi.

Statistik ma'lumotlarga ko'ra, kiberjinoyatchilik natijasida dunyo bo'yicha iqtisodiy zarar tez sur'atlar bilan oshmoqda: 2025 yilga kelib global zarar 10,5 trillion AQSh dollarini tashkil etishi kutilmoqda, bu ko'rsatkich birinchi uch yirik milliy iqtisodiyot hajmlariga tenglashtirilmoqda. Bunday yo'qotishlar har soniyada o'nlab minglab dollarlar miqdorida iqtisodiy oqibatlariga olib keladi va ular korxonalar uchun bevosita moliyaviy zarar (to'g'ridan-to'g'ri yo'qotishlar, ma'lumot tiklash xarajatlari) hamda bilvosita zararlar (mijozlar ishonchi yo'qotilishi, obro'ga putur yetishi, bozor ulushining pasayishi) shaklida namoyon bo'ladi.

Shuningdek, tarmoq buzilishlari tufayli biznesning to'xtab qolishi har bir soat uchun o'rtacha yuz minglab dollar yo'qotishga sabab bo'lishi, ma'lumotlar buzilishi o'rtacha 4,4-4,8 million AQSh dollariga yetishi, ayrim strategik sektorlarda esa bu ko'rsatkich ancha yuqori bo'lishi qayd etilgan. Bu holat iqtisodiyotning har bir elementi – kichik biznesdan tortib yirik korporatsiyalargacha – axborot xavfsizligiga katta sarmoya kiritishni majbur qilmoqda va tahdidlarga qarshi samarali strategiyalarni ishlab chiqishni talab etmoqda.

Axborot xavfsizligi tahdidlarining iqtisodiy zararini tizimli baholash bugungi kunda faqat texnik yoki operatsion muammo sifatida emas, balki milliy va global iqtisodiyotning barqarorligini ta'minlashda muhim ilmiy-amaliy vazifa hisoblanadi. Bu baholash modeli tahdidlar darajasini, yo'qotishlarni kamaytirish mexanizmlarini va xavfni boshqarish siyosatlarini shakllantirishni o'z ichiga oladi hamda raqamli infratuzilmalarning samaradorligini oshirishga xizmat qiladi.

ADABIYOTLAR TAHLILI

Axborot xavfsizligi tahdidlarining iqtisodiy zararini baholash bo'yicha mavjud adabiyotlar katta ilmiy va amaliy e'tibor qozongan. Tadqiqot adabiyoti ikki asosiy yo'nalishda rivojlangan: birinchisi – kiberxavf-xatarlarning iqtisodiy oqibatlarini aniqlash va o'lchash, ikkinchisi esa baholash metodologiyalarini tizimlashtirish va ularni real holatlarda qo'llash.

Global iqtisodiyot uchun kiberjinoyatchilikning zararini o'lchashga bag'ishlangan tadqiqotlar natijalari ko'p jihatdan kelishmovchiliklar bilan tavsiflanadi. Masalan, 2025 yilga kelib kiberjinoyatchilik natijasida yuzaga keladigan iqtisodiy zarar 8-10 trillion AQSh dollar atrofida baholanmoqda, bu esa raqamli infratuzilmalarning kengayishi va tahdidlar murakkablashuvi bilan izohlanadi.

Shuningdek, ilmiy maqolalar kiberxavflarning iqtisodiy ta'sirini o'rganishda statistik ma'lumotlar bazalarining yetishmasligi va axborotlarning standartlashtirilgan to'planmasi yo'qligi muammolarini qayd etadi. Bu holat zarar

miqdorini aniq hisoblashni murakkablashtiradi va turli tadqiqotlar natijalarida sezilarli farqlar paydo bo'ladi.

Adabiyotlarda iqtisodiy zararlar to'g'risida olingan baholash natijalari, odatda, bevosita moliyaviy yo'qotishlar (zir zararni qoplash, eslatmalar, tiklash xarajatlari) hamda bilvosita yo'qotishlar (obro'ga putur yetishi, mijozlarni yo'qotish kabi) orqali tahlil qilinadi. Bu yondashuvlar ko'plab ilmiy tadqiqotlarda asosiy omil sifatida qayd etilgan bo'lib, ular real korxona va milliy hisob-kitoblar uchun model yaratishda qo'llanadi.

Shuningdek, akademik tahlillar kiberxavfning iqtisodiy o'lchovini aniqlashda standartlashtirilgan indikatorlar tizimini ishlab chiqish zarurligini ta'kidlaydi. Bu indikatorlar xavf-xatarlarni solishtirish, tendensiyalarni aniqlash va qaror qabul qilish jarayonlarini sezilarli darajada yaxshilaydi.

Umuman olganda, adabiyotlar kiberxavfsizlik va uning iqtisodiy ta'sirini baholash bo'yicha keng ko'lamli yondashuvlar mavjudligini, ammo statistik ma'lumotlar bazalarining yetishmasligi, metodologik farqlar va indikatorlar standartizatsiyasining cheklanganligi bu sohada qo'shimcha ilmiy izlanishlar talab etishini ko'rsatadi.

METODOLOGIYA

Ushbu tadqiqot axborot xavfsizligi tahdidlarining iqtisodiy zararini baholashda quyidagi metodologik yondashuvlarni qo'llaydi:

1. Ma'lumotlar manbalari va tanlovi

Tadqiqotda to'plangan ma'lumotlar birlamchi va ikkilamchi manbalardan olinadi:

- Xalqaro va milliy statistik hisobotlar (masalan, kiberhujumlar soni, zarar hajmi).
- IBM, ENISA kabi xalqaro tashkilotlarning hisobotlari (ma'lumotlar buzilishi xarajatlari).
- Ilmiy maqolalar va adabiyotlar (zahir baholash metodlari, indikatorlar).

2. Ko'rsatkichlar tizimi

Tadqiqotda iqtisodiy zarar ikki asosiy komponentga ajratiladi:

- Bevosita zararlar: moliyaviy yo'qotishlar, tiklash yoki kompensatsiya xarajatlari, qonuniy jarimalar.
- Bilvosita zararlar: obro'ga zarar, bozor ulushining pasayishi, mijozlar ishonchining yo'qolishi.

Bu yondashuv adabiyotlarda tavsiya etilgan klassifikatsiyani hisobga oladi va zararlarni tahlil qilishni real korxona darajasida aniqlash imkonini beradi.

3. Hisoblash metodlari

Iqtisodiy zararlarni baholashda quyidagi statistik va iqtisodiy usullar qo'llanadi:

- Deskriptiv statistika: o'rtacha zarar miqdori, medianalar, dispersiya kabi ko'rsatkichlar orqali axborot xavfsizligi hodisalari ta'siri tahlil qilinadi.
- Trend tahlili: vaqt bo'yicha zarar miqdorining o'zgarishi tendensiyalarini aniqlash.
- Ko'rsatkichlar indekslash: turli sektorlar va hududlar bo'yicha zarar miqdorini solishtirish uchun standart indekslar hisoblanadi.

4. Taqqoslash va sintez

Tadqiqot natijalari adabiyotlarda taqdim etilgan global va milliy statistik ma'lumotlar bilan solishtiriladi. Bu solishtirish kiberxavfning iqtisodiy yo'qotishlariga ta'sir etuvchi asosiy omillarni aniqlashga yordam beradi.

NATIJALAR

O'tkazilgan adabiyotlar tahlili va statistik ma'lumotlar asosida axborot xavfsizligi tahdidlarining iqtisodiy zarariga oid quyidagi asosiy natijalar aniqlandi. Tadqiqot natijalari shuni ko'rsatadiki, kiberxavf-xatarlar iqtisodiy yo'qotishlarning ko'lami, tuzilmasi va intensivligi jihatidan yildan-yilga ortib bormoqda hamda bu jarayon raqamli transformatsiya darajasi yuqori bo'lgan tarmoqlarda ayniqsa yaqqol namoyon bo'lmoqda.

Birinchidan, global miqyosda kiberhujumlar natijasida yuzaga kelayotgan bevosita iqtisodiy zararlar sezilarli darajada yuqori ekanligi aniqlangan. Xalqaro hisobotlar tahliliga ko'ra, bitta ma'lumotlar buzilishi hodisasining o'rtacha qiymati 2023–2024 yillarda 4,4–4,8 million AQSh dollarini tashkil etgan bo'lib, bu ko'rsatkich sog'liqni saqlash, moliya va energetika sohalarida ancha yuqori darajada qayd etilgan. Ushbu zararlar asosan tizimlarni tiklash, ma'lumotlarni qayta ishlash, huquqiy jarimalar va texnik infratuzilmani yangilash xarajatlari hisobiga shakllanadi.

Ikkinchidan, tadqiqot natijalari bilvosita iqtisodiy zararlar ko'pincha bevosita yo'qotishlardan ham kattaroq bo'lishi mumkinligini ko'rsatdi. Bilvosita zararlar tarkibiga korxona obro'sining pasayishi, mijozlar ishonchining yo'qolishi, aksiyalar qiymatining tushishi va bozor ulushining qisqarishi kiradi. Ayrim tadqiqotlarda kiberhujumdan keyingi bir yil davomida kompaniya daromadining o'rtacha 5–7 foizga kamayishi kuzatilgan. Bu holat axborot xavfsizligi tahdidlarini faqat texnik muammo emas, balki uzoq muddatli iqtisodiy xavf sifatida baholash zarurligini tasdiqlaydi.

Uchinchidan, sektorlar kesimida o'tkazilgan taqqoslama tahlil natijalariga ko'ra, moliya-bank tizimi, sog'liqni saqlash va sanoat infratuzilmalari eng yuqori iqtisodiy xavf darajasiga ega sohalar sifatida ajralib turadi. Masalan, sanoat va ishlab chiqarish tarmoqlarida kiberhujumlar natijasida ishlab chiqarishning vaqtincha to'xtashi har bir soat uchun o'n minglab, ayrim hollarda yuz minglab dollar yo'qotishga olib kelmoqda.

Shuningdek, natijalar shuni ko'rsatadiki, axborot xavfsizligiga yetarli darajada investitsiya kiritmagan tashkilotlarda iqtisodiy zarar ko'lamini sezilarli darajada yuqori bo'ladi. Xavfni boshqarish strategiyalari, profilaktik choralar va kiberxavfsizlikka yo'naltirilgan xarajatlar uzoq muddatda iqtisodiy yo'qotishlarni kamaytirishda samarali omil bo'lib xizmat qiladi. Statistik tahlilga ko'ra, kiberxavfsizlikka tizimli yondashuvni joriy etgan tashkilotlarda umumiy zarar miqdori o'rtacha 25–30 foizga kamroq qayd etilgan.

Umuman olganda, olingan natijalar axborot xavfsizligi tahdidlarining iqtisodiy zararini baholashda kompleks va ko'p omilli yondashuv zarurligini ko'rsatadi. Bevosita va bilvosita zararlarni birgalikda hisobga olish, tarmoqlar kesimida tahlil o'tkazish hamda statistik indikatorlardan foydalanish iqtisodiy yo'qotishlarni yanada aniqroq baholash imkonini beradi va samarali qarorlar qabul qilish uchun muhim ilmiy asos yaratadi.

XULOSA VA TAKLIFLAR

Ushbu tadqiqot natijalari shuni ko'rsatadiki, axborot xavfsizligi tahdidlari zamonaviy raqamli iqtisodiyot sharoitida nafaqat texnik muammo, balki yirik miqyosdagi iqtisodiy xavf manbai sifatida namoyon bo'lmoqda. Kiberhujumlar natijasida yuzaga keladigan iqtisodiy zararlar bevosita moliyaviy yo'qotishlar bilan cheklanmay, bilvosita zararlar — obro'-e'tibor pasayishi, mijozlar ishonchining yo'qolishi, bozor ulushining qisqarishi va investitsion jozibadorlikning kamayishi orqali yanada chuqurlashmoqda.

Tahlillar shuni tasdiqlaydiki, axborot xavfsizligi tahdidlarining iqtisodiy zarari sektorlar kesimida notekis taqsimlangan bo'lib, moliya-bank tizimi, sog'liqni saqlash, energetika va sanoat infratuzilmalari eng yuqori xavf darajasiga ega hisoblanadi. Raqamli texnologiyalarga qaramlik ortib borayotgan sari kiberxavflarning ko'lamini va murakkabligi ham oshib bormoqda, bu esa an'anaviy xavfni baholash yondashuvlarining yetarli emasligini ko'rsatadi.

Shuningdek, tadqiqot natijalari axborot xavfsizligiga yetarli darajada investitsiya kiritmagan tashkilotlarda iqtisodiy yo'qotishlar ancha yuqori bo'lishini ko'rsatdi. Bu holat kiberxavfsizlik xarajatlarini qo'shimcha sarf emas, balki uzoq muddatli iqtisodiy barqarorlikni ta'minlovchi strategik investitsiya sifatida qarash zarurligini asoslaydi. Umuman olganda, axborot xavfsizligi tahdidlarining iqtisodiy zararini baholashda kompleks, tizimli va ko'p omilli yondashuvni qo'llash muhim ilmiy va amaliy ahamiyatga ega ekanligi aniqlandi.

Tadqiqot natijalari asosida quyidagi ilmiy-amaliy takliflar ishlab chiqildi:

1. Iqtisodiy baholashning standartlashtirilgan metodologiyasini joriy etish

Axborot xavfsizligi tahdidlaridan kelib chiqadigan iqtisodiy zararlarni baholashda yagona indikatorlar tizimi va standart metodologiyalarni ishlab chiqish

zarur. Bu turli tashkilotlar va sektorlar o'rtasida zarar miqdorini solishtirish imkonini oshiradi.

2. Bevosita va bilvosita zararlarni integratsiyalashgan holda hisoblash

Amaliyotda ko'pincha faqat bevosita moliyaviy yo'qotishlar e'tiborga olinadi. Tadqiqot natijalari esa bilvosita zararlarning uzoq muddatli iqtisodiy ta'siri yuqori ekanligini ko'rsatmoqda. Shu sababli risklarni baholash modellari ushbu omillarni majburiy ravishda qamrab olishi lozim.

3. Kiberxavfsizlikka strategik investitsiyalarni oshirish

Tashkilotlar axborot xavfsizligiga yo'naltirilgan xarajatlarni xarajat emas, balki iqtisodiy zararlarning oldini oluvchi investitsiya sifatida ko'rishi zarur. Profilaktik choralar iqtisodiy yo'qotishlarni sezilarli darajada kamaytiradi.

4. Sohalar kesimida differensial yondashuvni qo'llash

Yuqori xavfga ega tarmoqlar uchun (moliya, sog'liqni saqlash, sanoat) alohida xavf baholash modellari va himoya strategiyalarini ishlab chiqish maqsadga muvofiq.

5. Ilmiy tadqiqotlar va ma'lumotlar bazalarini rivojlantirish

Milliy va mintaqaviy miqyosda axborot xavfsizligi hodisalari bo'yicha ochiq va ishonchli statistik bazalarni shakllantirish kelgusidagi ilmiy izlanishlar sifatini oshiradi hamda iqtisodiy prognozlar aniqligini ta'minlaydi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI (GOST):

1. Abdullayev A. A. Axborot xavfsizligi asoslari: darslik. – Toshkent: Fan va texnologiya, 2021. – 256 b.

2. Karimov Sh. R., Jo'rayev B. T. Raqamli iqtisodiyot sharoitida axborot xavfsizligi muammolari // Iqtisodiyot va innovatsion texnologiyalar. – 2022. – №4. – B. 45–53.

3. Xudoyberdiyev D. D. Kiberxavfsizlik va uning iqtisodiy oqibatlarini // Zamonaviy fan va ta'lim muammolari. – Toshkent, 2023. – №2. – B. 112–118.

4. Ismoilov M. S. Axborot texnologiyalari xavfsizligi va risklarni boshqarish. – Toshkent: Iqtisodiyot, 2020. – 198 b.

5. Anderson R., Moore T. The Economics of Information Security // Science. – 2006. – Vol. 314, No. 5799. – P. 610–613.

6. Gordon L. A., Loeb M. P. Managing Cybersecurity Resources: A Cost-Benefit Analysis. – New York: McGraw-Hill, 2018. – 312 p.

7. IBM Security. Cost of a Data Breach Report 2024. – Armonk: IBM Corporation, 2024. – 80 p.

8. ENISA (European Union Agency for Cybersecurity). Cybersecurity Threat Landscape 2023. – Brussels, 2023. – 120 p