RAQAMLI IQTISODIYOT SHAROITIDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING INNOVATSION MEXANIZMLARINI SUN’IY INTELLEKT TEXNOLOGIYALARI ASOSIDA TAKOMILLASHTIRISH

Ilxamova Yodgora Saidaxmedovna
i.f.n., professor, Toshkent davlat iqtisodiyot universiteti

Annotatsiya. *Maqolada raqamli iqtisodiyotda axborot xavfsizligini ta’minlash mexanizmlarini sun’iy intellekt (SI) texnologiyalari asosida takomillashtirish masalasi ko‘rib chiqilgan. O‘zbekistonda to‘lovlar va davlat xizmatlarining raqamli shaklga o‘tishi bilan kibertahdidlar soni keskin oshdi: milliy segmentdagi resurslarga hujumlar 2022 yildagi qariyb 4,5 mln dan 2023 yilda 11 mln dan oshdi, 2024 yilda esa axborot texnologiyalari yordamida sodir etilgan jinoyatlar umumiy jinoyatlarning 44,4 foizini tashkil qildi. Tadqiqotda ikkilamchi statistik ma’lumotlar tahlili, normativ hujjatlarni qiyosiy o‘rganish va Gordon-Loeb modeli asosida iqtisodiy modellashtirish qo‘llanildi. Tadqiqotning ilmiy yangiligi Gordon-Loeb modelini SI samaradorligi va SI zaifligi parametrlari bilan kengaytirishdan iborat. Ma’lumotlar Kiberxavfsizlik markazi, UZCERT, Ichki ishlar vazirligi, IBM va Jahon iqtisodiy forumining 2022-2026 yillardagi ko‘rsatkichlaridan olindi. Modelga SI samaradorligi koeffitsienti hamda SI tizimining o‘z zaifligini ifodalovchi parametr kiritildi. Shartli tijorat banki misolidagi hisob-kitoblar SI himoyaga sarflangan har bir so‘mning qaytimini oshirib, optimal investitsiyani 17,9 foizga, kutilayotgan zararni esa 36,8 foizga kamaytirishi mumkinligini ko‘rsatdi. SI modellarini boshqarish tizimi bo‘lmasa, umumiy xarajatlarni tejash 18,5 foizdan 13,6 foizgacha pasayadi. Boshqaruvga ketgan xarajat zaiflikning 0,036 dan ortiq o‘sishining oldini olsa, o‘zini qoplaydi. Shu asosda uch darajali mexanizm taklif qilindi. Texnologik daraja anomaliyalarni aniqlash, to‘lovlarni real vaqtda baholash va javob choralarini avtomatlashtirishni o‘z ichiga oladi. Boshqaruv darajasi NIST AI RMF tamoyillari asosida SI modellari reyestri, kirish nazorati va chidamlilik testlarini nazarda tutadi. Iqtisodiy-institutsional daraja xavfga asoslangan byudjetlashtirish, banklar va Kiberxavfsizlik markazi o‘rtasida tahdidlar haqida ma’lumot almashish hamda federativ o‘qitish asosidagi banklararo antifrod modelini qamrab oladi. Natijalardan tijorat banklari, to‘lov tashkilotlari va davlat organlari kiberxavfsizlik xarajatlarini asoslashda hamda 2026-2030 yillarga mo‘ljallangan Kiberxavfsizlik strategiyasini amalga oshirishda foydalanishi mumkin.*

Kalit so‘zlar: *raqamli iqtisodiyot, axborot xavfsizligi, kiberxavfsizlik, sun’iy intellekt, mashinaviy o‘qitish, antifrod monitoring, Gordon-Loeb modeli, kiberxavf, SI boshqaruvi, kiberxavfsizlikka investitsiya.*

KIRISH

Raqamli iqtisodiyotda ishlab chiqarish, savdo va to‘lovlarning katta qismi ma’lumotlarga tayanadi. Bukht va Heeks (2017) uni raqamli texnologiyalar hamda raqamli tovar yoki xizmatlarga asoslangan biznes modellardan olinadigan iqtisodiy natija sifatida ta’riflaydi. Bunday iqtisodiyotda axborot xavfsizligiga sarflangan mablag‘ daromad va mijozlar ishonchi bilan bevosita bog‘liq: bank ilovasidagi bitta zaiflik mijozning puliga ham, bankning obro‘siga ham bir vaqtda zarar yetkazadi.

O‘zbekistonda bu jarayon so‘nggi besh yilda tezlashdi. «Raqamli O‘zbekiston-2030» strategiyasi davlat xizmatlari va to‘lovlarni raqamlashtirishni asosiy yo‘nalishlardan biri qilib belgiladi (O‘zbekiston Respublikasi Prezidenti, 2020). 2024 yilda tasdiqlangan SI strategiyasi esa 2030 yilgacha SI asosidagi dasturiy mahsulotlar va xizmatlar bozorini 1,5 mlrd AQSh dollariga yetkazishni ko‘zda tutadi (O‘zbekiston Respublikasi Prezidenti, 2024). Tahdidlar ham shu sur’atda o‘sdi. Kiberxavfsizlik markazi ma’lumotiga ko‘ra, «.uz» zonasidagi resurslarga hujumlar 2022 yildagi qariyb 4,5 mln dan 2023 yilda 11 mln dan oshgan (Ochilova, 2024). Ichki ishlar vazirligi 2024 yilda axborot texnologiyalari yordamida sodir etilgan jinoyatlar bo‘yicha 58,8 mingta jinoyat ishi qo‘zg‘atilganini ma’lum qilgan (Gazeta.uz, 2025).

2026 yilda tasdiqlangan Kiberxavfsizlik strategiyasi vaziyatni yana bir jihatdan o‘zgartirdi: tijorat banklari va to‘lov tizimlari kiberjinoyat tufayli mijozlar ko‘rgan zarar uchun javobgar bo‘ldi (Gazeta.uz, 2026). Endi kiberhodisa narxi bankning o‘z balansiga tushadi, demak himoyaga qancha va nimaga sarflash masalasi moliyaviy qarorga aylanadi. Xavfsizlik byudjeti ko‘pincha o‘tgan yilgi xarajat yoki yetkazib beruvchining taklifi asosida rejalashtiriladi. SI loyihalarida bunday yondashuv xato berishi mumkin, chunki SI tizimining o‘zi ham nazorat va qo‘shimcha xarajat talab qiladi.

An’anaviy himoya vositalari ko‘pincha ma’lum hujumlarning imzosi (signaturasi) bo‘yicha ishlaydi. Yangi fishing sxemalari, ijtimoiy muhandislik va dipfeyk videolar yordamida qilinadigan firibgarlik bu qoliplarga tushmaydi. Mashinaviy o‘qitish modellari odatiy xatti-harakatdan chetlanishni aniqlay oladi. Banklar va to‘lov tizimlari ularni monitoring va antifrod tizimlariga aynan shu imkoniyat uchun joriy qilmoqda. Biroq sun’iy intellekt ikki tomonga ham xizmat qiladi. U hujumchilarga arzon va moslashuvchan vosita beradi (Brundage va boshq., 2018), SI modelining o‘zi esa yangi hujum obyektiga aylanadi. Masalan, bank SI asosidagi antifrod tizimini sotib olib, uning modellariga kim kirish huquqiga ega ekanini nazorat qilmasa, himoya vositasining o‘zi zaif bo‘g‘inga aylanadi.

Ilmiy muammo shu yerda paydo bo‘ladi. Texnik adabiyotda SI algoritmlarining aniqligi keng o‘rganilgan, rahbar esa boshqa savolga javob izlaydi: SI ga sarflangan har bir so‘m qancha zararning oldini oladi va qanday tashkiliy shartlar bajarilmasa bu samara yo‘qoladi? O‘zbekistonda chop etilgan ishlarda bu savolga miqdoriy javob deyarli uchramaydi.

Tadqiqotning maqsadi raqamli iqtisodiyot subyektlarida axborot xavfsizligini ta’minlash mexanizmlarini SI texnologiyalari asosida takomillashtirish bo‘yicha iqtisodiy jihatdan asoslangan takliflar ishlab chiqishdan iborat. Maqsadga erishish uchun to‘rtta vazifa qo‘yildi: O‘zbekistonda kibertahdidlar dinamikasini tahlil qilish; SI ning himoya samaradorligiga ta’siri haqidagi xalqaro ma’lumotlarni umumlashtirish; Gordon-Loeb modelini SI parametrlari bilan kengaytirib, shartli misolda hisob-kitob qilish; takomillashtirilgan mexanizmni taklif etish.

Tadqiqot obyekti tijorat banklari, to‘lov tashkilotlari va davlat organlarining axborot xavfsizligi tizimidir. Predmeti esa bu tizimlarga SI texnologiyalarini joriy etishda yuzaga keladigan iqtisodiy va tashkiliy munosabatlardir. Ishchi gipoteza quyidagicha: SI himoya xarajatlarining samaradorligini oshiradi, lekin bu samara SI

modellarini boshqarish tizimi mavjud bo‘lgandagina to‘liq namoyon bo‘ladi. Ilmiy yangilik ikki jihatda ko‘rinadi. Birinchidan, Gordon-Loeb modeliga SI samaradorligi koeffitsienti va SI tizimining o‘z zaifligini ifodalovchi parametr kiritildi. Ikkinchidan, PF-38-son Farmon va PQ-358-son qaror talablarini NIST AI RMF tamoyillari bilan bog‘laydigan uch darajali mexanizm taklif qilindi.

ADABIYOTLAR SHARHI

Raqamli iqtisodiyot atamasini keng muomalaga Tapscott (1996) kiritgan. U tarmoq orqali ulangan kompaniyalar va iste’molchilar iqtisodiyotning yangi tuzilishini shakllantirishini ko‘rsatgan edi. Keyinchalik tushuncha aniqlashtirildi va o‘lchanadigan holga keltirildi. Bukht va Heeks (2017) uch qamrovni ajratadi: raqamli sektor, tor ma’nodagi raqamli iqtisodiyot va keng ma’nodagi raqamlashgan iqtisodiyot. Bizning mavzu uchun keyingi ikkisi ahamiyatli, chunki bank, soliq va savdo sohasidagi xavf aynan IT sektoridan tashqarida paydo bo‘ladi. O‘zbekistonlik mualliflar raqamli iqtisodiyotni ko‘proq texnologiyalarni tarmoqlarga joriy etish nuqtayi nazaridan tahlil qiladi (Xurramov, 2024), xavfsizlik esa bunday ishlarda ikkinchi o‘ringa tushib qoladi.

Axborot xavfsizligi iqtisodiyotida ko‘p iqtibos qilinadigan ikki ish bor. Anderson va Moore (2006) xavfsizlik tizimlari ko‘pincha rag‘batlar noto‘g‘ri taqsimlangani sababli ishdan chiqishini ko‘rsatgan: tizimni himoya qiladigan tashkilot muvaffaqiyatsizlikning to‘liq narxini o‘zi to‘lamaydi, zararning bir qismi mijozlar va boshqa ishtirokchilarga o‘tadi. Gordon va Loeb (2002) esa himoyaga optimal investitsiyani aniqlash modelini taklif qilgan. Ularning xulosasiga ko‘ra, buzilish ehtimoli funksiyalarining keng sinfi uchun optimal investitsiya kutilayotgan zararning 1/e qismidan (taxminan 37 foiz) oshmaydi, eng zaif axborot to‘plamiga eng ko‘p mablag‘ sarflash esa har doim ham to‘g‘ri bo‘lmaydi. Model sodda va amaliyotda tez-tez qo‘llaniladi. Ammo unda himoya vositasining o‘zi hujum obyektiga aylanishi hisobga olinmagan. SI uchun bu kamchilik sezilarli, chunki modelni aldash yoki uning o‘quv ma’lumotlarini buzish mumkin.

SI va mashinaviy o‘qitishni kiberxavfsizlikda qo‘llash bo‘yicha adabiyot ancha katta. Buczak va Guven (2016) hujumlarni aniqlash tizimlarida (IDS) ishlatiladigan ma’lumotlarni tahlil qilish va mashinaviy o‘qitish usullarini tizimlashtirib, imzoga va anomaliyaga asoslangan yondashuvlarni solishtirgan. Ularning fikricha, usul tanlash ma’lumotlar turi va hujum xususiyatiga bog‘liq. Ferrag va boshq. (2020) chuqur o‘qitishning yetti modelini CSE-CIC-IDS2018 va Bot-IoT ma’lumotlar to‘plamlarida sinab, ularni aniqlash darajasi va soxta signallar ulushi bo‘yicha taqqoslagan. Mirsky va boshq. (2018) taklif qilgan Kitsune tizimi avtoenkoderlar ansamblidan foydalanib, tarmoq trafigini oldindan belgilangan ma’lumotlarsiz, onlayn rejimda tekshiradi. Belgilangan ma’lumot kam bo‘lgan tashkilotlar uchun bu yondashuv qulay. Sarker va boshq. (2021) SI asosidagi kiberxavfsizlikni mashinaviy o‘qitish, bilimlarni ifodalash va qaror qabul qilishni birlashtirgan «xavfsizlik intellekti» sifatida ko‘rib chiqadi. Kaur va boshq. (2023) 2395 ta ishdan 236 ta birlamchi tadqiqotni ajratib, SI qo‘llanish holatlarini NIST kiberxavfsizlik freymvorki funksiyalari bo‘yicha tasniflagan. Ma’lumotlarni bir joyga to‘plamasdan modelni bir necha tashkilot ishtirokida o‘qitish imkonini beradigan federativ o‘qitish (McMahan va boshq., 2017) maxfiylik

cheklovlari kuchli bo‘lgan moliya sohasida hamkorlik usuli sifatida o‘rganilmoqda. Yuqoridagi sharhlarning ko‘pchiligi aniqlik va to‘liqlik kabi texnik ko‘rsatkichlarga tayanadi, himoyaning iqtisodiy samarasini esa baholamaydi.

Bir qator mualliflar laboratoriya natijalarini amaliyotga ko‘chirishda ehtiyot bo‘lishni talab qiladi. Sommer va Paxson (2010) anomaliyalarni aniqlashda mashinaviy o‘qitish boshqa sohalardagidek yaxshi ishlamasligining sabablarini ko‘rsatgan: xato signalning narxi yuqori, tarmoq trafigi o‘ta xilma-xil, model natijasini tahlilchi tushunadigan ma’noga aylantirish qiyin. Arp va boshq. (2022) yetakchi xavfsizlik konferensiyalarida chop etilgan 30 ta maqolani tekshirib, ma’lumotlarning «sizib ketishi», noto‘g‘ri tanlanma va asossiz taqqoslash bazasi kabi o‘nta keng tarqalgan xatoni aniqlagan. Apruzzese va boshq. (2023) tadqiqot va amaliyot o‘rtasidagi uzilishga e’tibor qaratib, sifatli belgilangan ma’lumotlar yetishmasligi, modelni yangilab turish xarajati va inson nazoratiga bo‘lgan ehtiyojni asosiy cheklovlar qatoriga qo‘yadi. Goodfellow va boshq. (2015) modelga deyarli sezilmaydigan o‘zgartirish kiritilgan ma’lumot berilganda u xato qaror chiqarishini ko‘rsatgan. Brundage va boshq. (2018) esa SI hujumchilar qo‘lida mavjud tahdidlarni kuchaytirib, yangilarini yaratishini ogohlantirgan. Demak, SI samaradorligini sotuvchining va’dasi yoki laboratoriyadagi aniqlik bilan emas, real muhitdagi ko‘rsatkichlar bilan o‘lchash kerak. SHAP kabi tushuntiriladigan SI usullari (Lundberg va Lee, 2017) tahlilchiga model qarorining sababini ko‘rsatib, bunday nazoratni osonlashtiradi.

So‘nggi yillarda e’tibor texnik vositalardan boshqaruvga ko‘chdi. NIST CSF 2.0 freymvorkida avvalgi besh funksiyaga oltinchisi, «boshqarish» (Govern) qo‘shildi (NIST, 2024). NIST AI RMF hujjati SI xavflarini boshqarishni to‘rt funksiya orqali tavsiflaydi: boshqarish, xaritalash, o‘lchash va nazorat qilish (Govern, Map, Measure, Manage) (NIST, 2023). Yevropa Ittifoqining SI to‘g‘risidagi reglamenti yuqori xavfli SI tizimlari uchun aniqlik, barqarorlik va kiberxavfsizlik talablarini qonun darajasida belgiladi (European Parliament and Council, 2024). O‘zbekistonda «Kiberxavfsizlik to‘g‘risida»gi Qonun kiberxavfsizlik subyektlarining huquq va majburiyatlarini belgilab berdi (O‘zbekiston Respublikasi Qonuni, 2022). 2026 yil 10 martdagi PF-38-son Farmon bilan 2026-2030 yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlandi (O‘zbekiston Respublikasi Prezidenti, 2026). Unda milliy SOC standartlarini 2027 yilgacha tasdiqlash, milliy SOC markazlarini 2029 yilgacha to‘liq ishga tushirish, tijorat banklari va to‘lov tizimlarini kiberjinoyat tufayli mijozlar ko‘rgan zarar uchun bevosita javobgar qilish nazarda tutilgan (Gazeta.uz, 2026). Milliy hujjatlarda SI tizimlarining o‘z xavfsizligiga hozircha kamroq e’tibor qaratilgan.

Mahalliy tadqiqotlarda kiberxavfsizlik iqtisodiy, huquqiy va tashkiliy muammo sifatida qaralmoqda. Axmadaliyev (2025) xalqaro tajribaga tayanib, davlat va xususiy sektor hamkorligini kuchaytirish hamda raqamli savodxonlikni oshirishni taklif qiladi. Bunday ishlar yo‘nalishni to‘g‘ri belgilaydi, ammo SI ga investitsiyalar samarasini miqdoriy baholash vositasini bermaydi.

Sharhdan ikki bo‘shliq ko‘rinadi. Birinchidan, SI ning texnik samaradorligi himoyaga investitsiya qarori bilan kam bog‘langan, bog‘langan hollarda ham SI tizimining o‘z zaifligi hisobga olinmaydi. Ikkinchidan, O‘zbekiston ma’lumotlari

asosida bunday baholash deyarli o‘tkazilmagan. Ushbu maqola shu bo‘shliqlarni qisman to‘ldirishga qaratilgan.

METODOLOGIYA

Tadqiqot ikki bosqichda olib borildi. Birinchi bosqichda ikkilamchi ma’lumotlar va normativ hujjatlar tahlil qilindi, ikkinchi bosqichda Gordon-Loeb modeli asosida iqtisodiy-matematik modellashtirish o‘tkazildi. Bunday dizayn tanlanganining sababi shundaki, O‘zbekistonda tashkilotlar kesimidagi kiberincidentlar va ularning xarajatlari bo‘yicha ochiq ma’lumotlar bazasi yo‘q. Shu sababli regressiya kabi ekonometrik usullarni qo‘llashning imkoni bo‘lmadi, model esa mavjud agregat ko‘rsatkichlar bilan ishlashga imkon berdi.

Ma’lumotlar uch guruhga ajratildi. Milliy statistika sifatida Kiberxavfsizlik markazi, UZCERT xizmati va Ichki ishlar vazirligining 2022-2026 yillarda e’lon qilgan ko‘rsatkichlari olindi. Bu idoralar to‘liq hisobotlarini ochiq e’lon qilmagani uchun ko‘rsatkichlar ularning rasmiy chiqishlari asosida tayyorlangan nashrlardan olindi (Ochilova, 2024; Tuxsinov, 2024; Gazeta.uz, 2025, 2026). Xalqaro ko‘rsatkichlar IBM va Ponemon Institutining 2024-2026 yillardagi hisobotlaridan (IBM, 2024, 2025, 2026), Jahon iqtisodiy forumining hisobotidan (WEF, 2025) va Xalqaro elektraloqa ittifoqining Global kiberxavfsizlik indeksidan (ITU, 2021, 2024) olindi. Normativ baza O‘zbekistonning beshta va uchta xalqaro hujjatini qamrab oldi. Hujjatlar rasmiy manbadan olingani, amaldagi tahriri va mavzuga bevosita tegishliligi bo‘yicha tanlandi.

Modellashtirishda Gordon va Loeb (2002) taklif qilgan birinchi turdagi buzilish ehtimoli funksiyasidan foydalanildi:

$$S(z, v) = v / (\alpha z + 1)^{\beta}, \quad (1)$$

bu yerda v deganda himoya choralari bo‘lmagandagi zaiflik, ya’ni buzilish ehtimoli tushuniladi; z himoyaga yo‘naltirilgan investitsiya; $\alpha > 0$ himoya samaradorligi koeffitsienti; $\beta \geq 1$ funksiya shaklini belgilovchi parametr. Tashkilot kutilayotgan sof foydani (ENBIS) maksimallashtiradi:

$$ENBIS(z) = [v - S(z, v)] \cdot L - z, \quad (2)$$

bu yerda L muvaffaqiyatli hujumdagi potensial yo‘qotish. (2) ifodani z bo‘yicha differensiallash optimal investitsiyani beradi:

$$z^* = [(v\alpha\beta L)^{1/(\beta+1)} - 1] / \alpha. \quad (3)$$

Modelga SI bilan bog‘liq ikki o‘zgarish kiritildi. Birinchisi, SI himoya samaradorligi koeffitsientini α_0 dan α_{SI} gacha oshiradi deb faraz qilindi. Ikkinchisi, SI modellari boshqarilmasa (reyestr, kirish nazorati va chidamlilik testlari bo‘lmasa), axborot to‘plamining zaifligi Δv ga ortadi. Bundan tashqari, SI ni joriy etishning qat’iy xarajati F hisobga olindi. Ssenariylarni solishtirish uchun umumiy xarajat ko‘rsatkichi ishlatildi:

$$TC = S(z^*, v) \cdot L + z^* + F. \quad (4)$$

Hisob-kitob shartli o‘rta tijorat banki misolida bajarildi. Parametrlar quyidagicha olindi: L = 100 mlrd so‘m, v = 0,5, $\beta = 1$, $\alpha_0 = 0{,}10$ va $\alpha_{SI} = 0{,}25$ (mlrd so‘mga nisbatan). α_{SI} qiymati kutilayotgan zararning kamayishi IBM (2026) qayd etgan nisbatga yaqin bo‘lishi uchun tanlandi: SI va avtomatlashtirish keng qo‘llangan tashkilotlarda tejalgan

1,93 mln AQSh dollari o‘rtacha zararning (4,99 mln) qariyb 39 foiziga teng. Boshqaruv bo‘lmagan holatdagi zaiflik o‘sishi Δv = 0,10 deb olindi. Bu ekspert baho bo‘lib, IBM (2025) ma’lumotiga tayanadi: SI modellari yoki ilovalari buzilgan tashkilotlarning 97 foizida SI ga kirish nazorati bo‘lmagan. SI ni joriy etish xarajati F = 3 mlrd so‘m, boshqaruv tizimiga qo‘shimcha xarajat 1 mlrd so‘m deb qabul qilindi. Natijalarning parametrlarga bog‘liqligini tekshirish uchun α 0,05 dan 0,40 gacha o‘zgartirilib, sezgirlik tahlili o‘tkazildi, boshqaruv xarajati o‘zini qoplaydigan Δv ning chegaraviy qiymati hisoblandi. Hisob-kitoblar Python 3 dasturlash tilida bajarildi.

TAHLIL VA NATIJALAR

O‘zbekistondagi kibertahdidlar va kiberjinoyatlarning asosiy ko‘rsatkichlari 1-jadvalda jamlangan.

1-jadval

O‘zbekistonda kibertahdidlar va kiberjinoyatlarning asosiy ko‘rsatkichlari

Ko‘rsatkich	Davr	Qiymat	Manba
«uz» zonasidagi resurslarga hujumlar	2022 / 2023	~4,5 mln / 11 mln dan ortiq	Ochilova (2024)
Milliy segmentdagi kiberxavfsizlik incidentlari	2022 / 2023	235 / 158	Ochilova (2024)
Milliy segmentda qayd etilgan hujumlar (UZCERT)	2024 yil I chorak	3,29 mln	Tuxsinov (2024)
IT yordamida sodir etilgan jinoyatlar bo‘yicha qo‘zg‘atilgan jinoyat ishlari	2024	58 800	Gazeta.uz (2025)
Ularning jami jinoyatlardagi ulushi	2024	44,4%	Gazeta.uz (2025)
Fuqarolarga yetkazilgan zarar	2024 / 2021-2024	603 mlrd so‘m / 1,9 trln so‘mdan ortiq	Gazeta.uz (2025)
Bank kartalari bilan bog‘liq kiberjinoyatlar ulushi	2025	98%	Gazeta.uz (2025)
Kiberjinoyatlar soni	so‘nggi 5 yil	62 mingdan ortiq (qariyb 11 barobar o‘sish)	Gazeta.uz (2026)
Antifrod tizimlari to‘xtatgan noqonuniy o‘tkazmalar	2026 yil I yarmi	462 mlrd so‘m	Gazeta.uz (2026)
Global kiberxavfsizlik indeksi balli	2020 / 2024	71,11 / 89,2 (Tier 2)	ITU (2021, 2024)

Jadvaldan ikki holat ko‘rinadi. Birinchisi, hujum urinishlari va muvaffaqiyatli incidentlar teskari yo‘nalishda o‘zgargan: 2023 yilda hujumlar 2,4 barobar ko‘paygan, incidentlar esa 32 foizga kamaygan. Ikkinchisi, zarar asosan to‘lov sohasida to‘planmoqda. IIV ma’lumotiga ko‘ra, kiberjinoyatlarning 60 foizi zararli havola yoki dastur yuborib, bank kartasi yoki mobil qurilmani egallash orqali sodir etilgan, yana 16 foizi SMS-kodni aldov yo‘li bilan olishga to‘g‘ri kelgan. Onlayn kredit olishda mashhur shaxslarning dipfeyk videolaridan foydalanish holatlari ham qayd etilgan (Gazeta.uz, 2025). 2026 yilning birinchi yarmida antifrod tizimlari to‘xtatgan summa 2024 yilda fuqarolarga yetkazilgan yillik zararning qariyb 77 foiziga teng. Davrlar har xil bo‘lgani uchun bu nisbat faqat ko‘lamni tasavvur qilishga yordam beradi. Global kiberxavfsizlik indeksida mamlakat balli 18 balldan ko‘proqqa oshgan.

SI ning himoya samaradorligi va SI bilan bog‘liq xavflarga oid xalqaro ko‘rsatkichlar 2-jadvalda keltirilgan.

2-jadval

SI ning himoya samaradorligi va SI bilan bog‘liq xavflar bo‘yicha xalqaro ko‘rsatkichlar

Ko‘rsatkich	Qiymat	Manba
Ma’lumotlar sizib chiqishi incidentining o‘rtacha global qiymati, mln AQSh dollari (2024 / 2025 / 2026)	4,88 / 4,44 / 4,99	IBM (2024, 2025, 2026)
SI va avtomatlashtirish keng qo‘llanganda incident zararining kamayishi, mln AQSh dollari (2024 / 2025 / 2026)	2,22 / 1,90 / 1,93	IBM (2024, 2025, 2026)
Incidentni aniqlash va bartaraf etishning o‘rtacha davomiyligi, kun (2024 / 2025 / 2026)	258 / 241 / 247	IBM (2025, 2026)
SI keng qo‘llanganda bu davomiylikning qisqarishi, kun (2025 / 2026)	80 / 65	IBM (2025, 2026)
SI modellari yoki ilovalari buzilganini qayd etgan tashkilotlar (2025)	13%; ulardan 97% da SI ga kirish nazorati bo‘lmagan	IBM (2025)
Ruxsatsiz SI vositalari («soya SI») keng tarqalgan tashkilotlarda qo‘shimcha zarar, mln AQSh dollari (2025)	0,67	IBM (2025)
Zararli hujumida SI ishtirok etgan tashkilotlar (2026)	to‘rtdan biridan ko‘p	IBM (2026)
SI ni kiberxavfsizlikka eng katta ta’sir qiluvchi omil deb hisoblovchi tashkilotlar (2025)	66%	WEF (2025)
SI vositalarini joriy etishdan oldin xavfsizligini baholaydigan tashkilotlar (2025)	37%	WEF (2025)

Uch yil davomida SI va avtomatlashtirishni keng qo‘llagan tashkilotlarda bitta incident zarari 1,90-2,22 mln AQSh dollariga kam bo‘lgan, incident hayot sikli esa 65-80 kunga qisqargan. Shu bilan birga, SI ning o‘zi hujum obyekti va vositasiga aylanmoqda. WEF so‘rovida SI ning ta’sirini eng kuchli deb bilganlar bilan SI vositalarining xavfsizligini oldindan baholaydiganlar o‘rtasidagi farq 29 foiz punktni tashkil qilgan.

Modellashtirish natijalari 3-jadvalda keltirilgan.

3-jadval

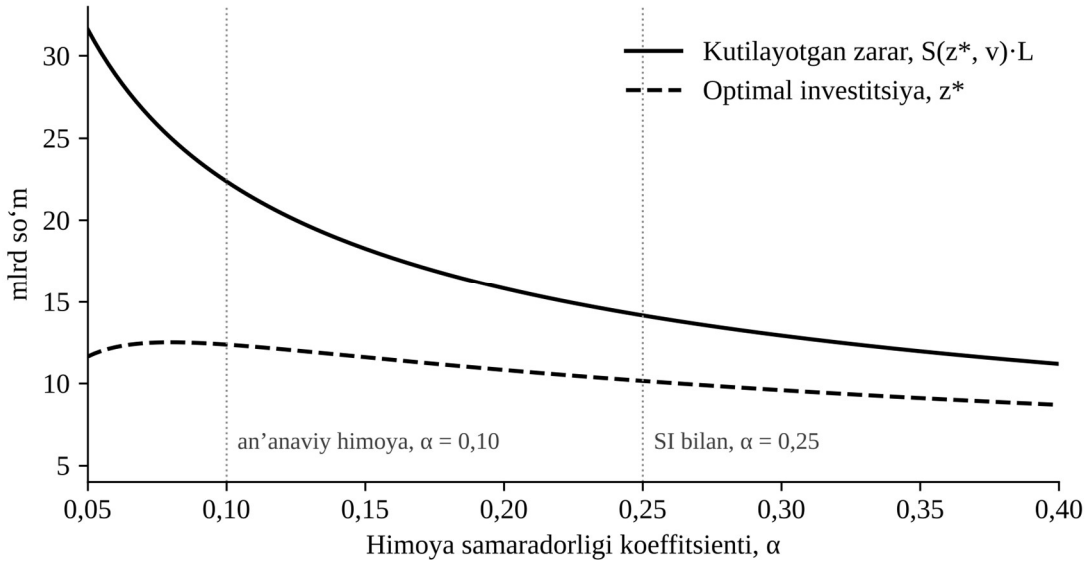
Gordon-Loeb modeli bo‘yicha ssenariylar natijalari (shartli bank, mlrd so‘m)

Ssenariy	v	α	F	z*	S(z*, v)	Kutilayotgan zarar	Umumiy xarajat (TC)
S0. An’anaviy himoya	0,50	0,10	0	12,36	0,224	22,36	34,72
S1. SI, joriy etish xarajatisiz	0,50	0,25	0	10,14	0,141	14,14	24,28
S2. SI, boshqaruv tizimisiz	0,60	0,25	3	11,49	0,155	15,49	29,98
S3. SI va boshqaruv tizimi	0,50	0,25	4	10,14	0,141	14,14	28,28

Izoh: L = 100 mlrd so‘m, β = 1. Manba: muallif hisob-kitoblari.

Faqat samaradorlik oshgan S1 ssenariyda optimal investitsiya 17,9 foizga kamaydi, kutilayotgan zarar 36,8 foizga, umumiy xarajat 30,1 foizga qisqardi. Joriy etish xarajatlarini hisobga olganda S3 ssenariyda umumiy xarajat an’anaviy himoyaga nisbatan 18,5 foiz, boshqaruv tizimi bo‘lmagan S2 ssenariyda esa 13,6 foiz past bo‘ldi. S2 dan S3 ga o‘tish 1 mlrd so‘m qo‘shimcha xarajat talab qiladi, lekin optimal investitsiya va kutilayotgan zararni birgalikda 2,70 mlrd so‘mga kamaytiradi. Boshqaruv xarajati, agar u zaiflikning kamida 0,036 ga ortishining oldini olsa, o‘zini qoplaydi. Barcha ssenariylarda optimal investitsiyaning potensial zararga nisbati (z*/vL) 0,19-0,25 oralig‘ida bo‘lib, 1/e chegarasidan past qoldi.

Sezgirlik tahlili natijalari 1-rasmda ko‘rsatilgan.



1-rasm. Himoya samaradorligi koeffitsienti (α) bilan optimal investitsiya va kutilayotgan zarar o‘rtasidagi bog‘liqlik (v = 0,5; L = 100 mlrd so‘m)

α ortgan sari kutilayotgan zarar kamayadi, lekin kamayish sur’ati pasayadi. α 0,10 dan 0,15 ga oshganda zarar 4,10 mlrd so‘mga, 0,25 dan 0,30 ga oshganda esa atigi 1,23 mlrd so‘mga qisqaradi. Optimal investitsiya chiziqli o‘zgarmaydi: u α = 0,08 da eng yuqori qiymatga (12,5 mlrd so‘m) yetadi, undan keyin kamayib boradi.

Olingan natijalar asosida uch darajali mexanizm ishlab chiqildi (4-jadval). Har bir daraja modeldagi muayyan parametrga ta’sir qiladi: texnologik daraja α ni oshiradi, boshqaruv darajasi Δv ni nolga yaqin ushlab turadi, iqtisodiy-institutsional daraja esa investitsiya hajmini real o‘lchangan ko‘rsatkichlar asosida belgilashga xizmat qiladi.

4-jadval

SI asosida axborot xavfsizligini ta’minlashning uch darajali mexanizmi

Daraja	Asosiy vositalar va mas’ul subyektlar	Modeldagi parametr	Nazorat ko‘rsatkichlari
Texnologik	Tarmoq trafigi hamda foydalanuvchi va qurilmalar xatti-harakatidagi anomaliyalarni aniqlash (avtoenkoderlar, UEBA); to‘lovlarni real vaqtda baholovchi antifrod modellari; fishing	α ni oshirish	Aniqlashning o‘rtacha vaqti (MTTD), javobning o‘rtacha vaqti (MTTR), soxta signallar ulushi, to‘xtatilgan

	havolalari va dipfeyk kontentni aniqlash; javob choralarini avtomatlashtirish (SOAR). Mas’ul: banklar, to‘lov tashkilotlari va davlat organlarining SOC bo‘linmalari.		firibgarlik summasi
Boshqaruv	SI modellari reyestri; modellar va o‘quv ma’lumotlariga kirish nazorati; «soya SI»ni aniqlash; raqib hujumlariga chidamlilik testlari; SHAP yordamida qarorlarni tushuntirish; NIST AI RMF funksiyalari. Mas’ul: rahbariyat, axborot xavfsizligi bo‘limi, ichki audit.	Δv ni nolga yaqin ushlash	Reyestrga kiritilgan, kirish nazorati qo‘llangan va chidamlilik testidan o‘tgan modellar ulushi
Iqtisodiy-institutsional	Gordon-Loeb mezoni asosida xavfga asoslangan byudjetlashtirish; banklar va Kiberxavfsizlik markazi o‘rtasida tahdid indikatorlari almashinuvi; federativ o‘qitish asosidagi banklararo antifrod modeli; kibersug‘urta. Mas’ul: Markaziy bank, Raqamli texnologiyalar vazirligi, Kiberxavfsizlik markazi, tijorat banklari.	z* va F ni asoslash, L ni to‘g‘ri baholash	Xavfsizlik xarajatlarining kutilayotgan zararga nisbati, almashilgan indikatorlar soni, mijozga zararni qoplash muddati

4-jadvalda sun’iy intellekt (SI) asosida axborot xavfsizligini ta’minlashning texnologik, boshqaruv va iqtisodiy-institutsional darajalarini birlashtiruvchi kompleks mexanizm taklif etilgan.

Texnologik daraja kiberxavflar, anomal harakatlar va moliyaviy firibgarlikni aniqlash hamda ularga avtomatlashtirilgan javob qaytarishga qaratilgan. Bu modeldagi α parametrini oshirish orqali xavfsizlik samaradorligini kuchaytiradi. Natijalar MTTD, MTTR, soxta signallar ulushi va oldi olingan moliyaviy zarar bilan baholanadi.

Boshqaruv darajasi SI modellarini ro‘yxatga olish, ulardan foydalanishni nazorat qilish, hujumlarga chidamliligini tekshirish va qarorlarning tushuntirilishini ta’minlashga asoslanadi. Uning vazifasi Δv parametrini nolga yaqin saqlash, ya’ni SI bilan bog‘liq qo‘shimcha zaifliklarni kamaytirishdan iborat.

Iqtisodiy-institutsional daraja Gordon–Loeb modeli asosida xavfsizlik xarajatlarini optimallashtirish, tashkilotlar o‘rtasida tahdid indikatorlarini almashish, federativ o‘qitish va kibersug‘urta mexanizmlarini rivojlantirishni nazarda tutadi. Bunda z*, F va L parametrlarini asosli baholash orqali moliyaviy resurslardan samarali foydalanishga erishish ko‘zda tutiladi.

Shunday qilib, taklif etilgan uch darajali mexanizm texnologik himoya, tashkiliy nazorat va iqtisodiy boshqaruvni yagona tizimga birlashtirib, kiberxavflarni kamaytirish, SI modellarining ishonchliligini oshirish hamda axborot xavfsizligi xarajatlarini optimallashtirishga xizmat qiladi.

MUHOKAMA

Natijalar ishchi gipotezani tasdiqlaydi. SI himoyaga sarflangan har bir so‘mni samaraliroq qiladi, ammo SI modellari boshqarilmasa, bu yutuqning bir qismi yo‘qoladi. S2 va S3 ssenariylari o‘rtasidagi farq aynan shuni ko‘rsatadi. Amaliy jihatdan bundan SI loyihasining byudjetida modellarni boshqarish uchun alohida

modda bo‘lishi kerakligi kelib chiqadi. Busiz loyiha kutilgan iqtisodiy natijani to‘liq bermaydi.

Optimal investitsiyaning kamayishi kutilmagan natija bo‘ldi. Amaliyotda SI ni joriy etish xavfsizlik byudjetini oshiradi deb qaraladi. Gordon va Loeb (2002) modelida esa samaraliroq texnologiya bir xil himoya darajasiga arzonroq yetishga imkon beradi, shuning uchun optimal investitsiya α ning ma’lum qiymatidan keyin kamaya boshlaydi. Bu xulosa SI ga xarajatlarni oshirishdan ko‘ra ularni qayta taqsimlashga asos beradi. Imzolarga asoslangan vositalarni qo‘lda kuzatishga ketadigan mehnat xarajati qisqaradi, bo‘shagan mablag‘ni esa ma’lumotlar sifati va modellar nazoratiga yo‘naltirish mumkin.

Model natijalari yo‘nalish jihatidan IBM (2024, 2025, 2026) ma’lumotlariga mos keladi. Bu moslik qisman parametrlarni kalibrlash usulidan kelib chiqqani uchun uni mustaqil tasdiq deb hisoblab bo‘lmaydi. Sommer va Paxson (2010) hamda Arp va boshq. (2022) ko‘rsatgan muammolar shu yerda o‘zini namoyon qiladi: laboratoriyada yuqori aniqlik ko‘rsatgan model real trafikda α ni kutilgandan kamroq oshirishi mumkin. Sezgirlik tahlili natijasiga ko‘ra, α ning har bir keyingi o‘sishi oldingisiga qaraganda kamroq naf beradi, ya’ni eng qimmat model har doim ham o‘zini oqlamaydi. Mexanizmning texnologik darajasida α aniqlash va javob berish vaqti kabi amaliy ko‘rsatkichlar orqali muntazam o‘lchab boriladi.

Δv bo‘yicha qabul qilingan taxmin ham asossiz emas. WEF (2025) so‘rovidagi 29 foiz punktlik farq tashkilotlarning ko‘pchiligi SI ni joriy etayotganini, lekin uning xavfsizligini oldindan tekshiradiganlar ozchilikda qolayotganini ko‘rsatadi. IBM (2025) qayd etgan «soya SI» bilan bog‘liq qo‘shimcha zarar ham shu yo‘nalishdagi dalil. Boshqacha aytganda, boshqaruvsiz S2 ssenariysi ko‘plab tashkilotlarning hozirgi holatiga yaqin.

Taklif etilgan mexanizmni Kaur va boshq. (2023) tasnifi bilan solishtirish mumkin. Ular SI qo‘llanish holatlarini NIST freymvorkining alohida funksiyalari bo‘yicha guruhlagan. 4-jadvaldagi mexanizm esa aniqlash va javob berish vositalarini boshqaruv va moliyaviy qaror bilan bitta tizimga bog‘laydi. NIST CSF 2.0 da boshqarish funksiyasining alohida ajratilgani (NIST, 2024) xuddi shu yo‘nalishni qo‘llab-quvvatlaydi.

Anderson va Moore (2006) ta’kidlagan rag‘batlar muammosi O‘zbekiston sharoitida yaqqol ko‘rinadi. 2021-2024 yillarda kiberjinoyatlardan ko‘rilgan 1,9 trln so‘mdan ortiq zarar fuqarolarga yetkazilgan zarar sifatida hisobga olingan. PF-38-son Farmon banklar va to‘lov tizimlarini mijoz oldida javobgar qilib, rag‘batni himoyaga sarmoya kiritadigan tomonga ko‘chiradi. Model tilida bu bankning o‘zi uchun L ni oshiradi va (3) formulaga ko‘ra optimal investitsiyani ham ko‘taradi. Bunday sharoitda investitsiya qarorini asoslash vositasi banklar uchun yanada zarur bo‘lib qoladi.

Zararning bank kartalari atrofida to‘plangani ustuvorlikni aniq belgilaydi: SI ni birinchi navbatda to‘lovlarni real vaqtda baholash va fishing havolalarini aniqlashga joriy etish kerak. Bitta bank ko‘radigan firibgarlik namunalari soni cheklangan, banklararo ma’lumot almashish esa «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun talablariga duch keladi (O‘zbekiston Respublikasi Qonuni, 2019). Federativ o‘qitish bu ziddiyatni qisman yechadi: banklar mijozlar ma’lumotlarini uzatmasdan, faqat

model parametrlarini almashib, umumiy antifrod modelini o‘qitadi. Shu tariqa Axmadaliyev (2025) ilgari surgan davlat va xususiy sektor hamkorligi g‘oyasi aniq texnologik shaklga ega bo‘ladi. Dipfeyk videolarning firibgarlikda qo‘llanayotgani Brundage va boshq. (2018) ogohlantirgan xavf amalda ro‘y berayotganini bildiradi. Boshqaruv darajasiga raqib hujumlariga chidamlilik testlari (Goodfellow va boshq., 2015) va qarorlarni tushuntirish vositalari aynan shu sababli kiritildi.

Regulyator uchun ham natijalardan xulosa chiqadi. Agar SI samaradorligi tashkilotlarda muntazam o‘lchanmasa, Markaziy bank banklarning kiberxavfsizlik xarajatlari yetarli yoki yetarli emasligini baholay olmaydi. Aniqlash va javob berish vaqti hamda to‘xtatilgan firibgarlik summasi kabi ko‘rsatkichlarni yagona shaklda yig‘ish modelni kalibrlash uchun ham, nazorat uchun ham asos bo‘ladi.

Tadqiqotning cheklovlari ham bor. Birinchidan, model parametrlari O‘zbekiston banklarining haqiqiy ma’lumotlari bilan emas, xalqaro hisobotlar va ekspert baholari asosida tanlangan. Shuning uchun natijalar aniq qiymatlarni emas, ta’sir yo‘nalishi va tartibini ko‘rsatadi. Ikkinchidan, model statik va bir davrli, hujumchining SI yordamida moslashishi hisobga olinmagan. Uchinchidan, milliy statistika turli idoralar tomonidan turli birliklarda (hujum, incident, jinoyat ishi) yuritiladi va asosan OAV orqali e’lon qilinadi. Bu yillar bo‘yicha to‘g‘ridan-to‘g‘ri solishtirishni qiyinlashtiradi. IBM ma’lumotlari esa ko‘proq yirik va rivojlangan mamlakatlardagi tashkilotlarga tegishli, ularni O‘zbekistonga ko‘chirishda ehtiyot bo‘lish kerak.

XULOSA

Tahlil O‘zbekistonda kibertahdidlar keskin o‘sganini va zarar asosan to‘lov sohasida to‘planayotganini ko‘rsatdi. Bunday sharoitda sun’iy intellekt axborot xavfsizligini ta’minlashning samarali vositasiga aylanishi mumkin, lekin bitta shart bilan: SI modellarining o‘zi boshqarilishi va himoyalanishi kerak.

Kengaytirilgan Gordon-Loeb modeli shartli bank misolida SI himoya samaradorligini oshirib, optimal investitsiyani 17,9 foizga, kutilayotgan zararni 36,8 foizga kamaytirishini ko‘rsatdi. Boshqaruv tizimi bo‘lmasa, umumiy xarajatlarni tejash 18,5 foizdan 13,6 foizgacha tushadi. Boshqaruvga ajratilgan mablag‘ zaiflikning nisbatan kichik o‘sishini oldini olganda ham o‘zini qoplaydi.

Amaliy takliflar quyidagilardan iborat. Tijorat banklari va to‘lov tashkilotlari SI loyihalarini Gordon-Loeb mezoni asosida baholashi va byudjetda SI modellarini boshqarish uchun alohida moddani nazarda tutishi lozim. Markaziy bank va Kiberxavfsizlik markazi 2027 yilgacha tasdiqlanadigan milliy SOC standartlariga SI modellari reyestri, kirish nazorati va chidamlilik testlariga oid talablarni kiritishi maqsadga muvofiq. Banklararo antifrod modelini federativ o‘qitish asosida yaratish shaxsiy ma’lumotlarni uzatmasdan firibgarlikni aniqlash darajasini oshirishga imkon beradi. Kiberincidentlar va ularning xarajatlari bo‘yicha yagona statistik hisobot shaklini joriy etish esa bunday modellarni haqiqiy ma’lumotlar bilan kalibrlash uchun zarur.

Kelgusi tadqiqotlarda modelni O‘zbekiston banklarining incidentlar ma’lumotlari asosida kalibrlash hamda hujumchi va himoyachi o‘rtasidagi o‘zaro ta’sirni o‘yinlar nazariyasi yordamida ko‘p davrli modelda tahlil qilish rejalashtirilgan.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992
2. Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), Article 8. https://doi.org/10.1145/3545574
3. Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., & Rieck, K. (2022). Dos and don’ts of machine learning in computer security. In Proceedings of the 31st USENIX Security Symposium (pp. 3971-3988). USENIX Association.
4. Axmadaliyev, M. E. (2025). Raqamli iqtisodiyotda kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari. Oriental Renaissance: Innovative, Educational, Natural and Social Sciences, 5(9), 64-75.
5. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv. https://doi.org/10.48550/arXiv.1802.07228
6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
7. Bukht, R., & Heeks, R. (2017). Defining, conceptualising and measuring the digital economy (Development Informatics Working Paper No. 68). Centre for Development Informatics, University of Manchester.
8. European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.
9. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419
10. Gazeta.uz. (2025, 5 noyabr). O‘zbekistonda kiberjinoyatlar umumiy jinoyatlarning salkam yarmini tashkil qilyapti. IIV ularning sodir etilish usullarini ochiqladi. https://www.gazeta.uz/oz/2025/11/05/cybercrime/
11. Gazeta.uz. (2026, 30 sentabr). Mansabdorlar uchun javobgarlik, maktablarda kibergigiyena darslari, milliy SOC markazlari. O‘zbekiston kiberxavfsizlik sohasida o‘z oldiga qanday vazifalar qo‘ymoqda? https://www.gazeta.uz/oz/2026/09/30/cybersecurity/
12. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. In International Conference on Learning Representations (ICLR 2015). https://doi.org/10.48550/arXiv.1412.6572
13. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457.

https://doi.org/10.1145/581271.581274
14. IBM. (2024). Cost of a data breach report 2024. IBM Security; Ponemon Institute. https://www.ibm.com/reports/data-breach
15. IBM. (2025). Cost of a data breach report 2025. IBM Security; Ponemon Institute. https://www.ibm.com/reports/data-breach
16. IBM. (2026). Cost of a data breach report 2026. IBM Security; Ponemon Institute. https://www.ibm.com/reports/data-breach
17. ITU. (2021). Global cybersecurity index 2020. International Telecommunication Union.
18. ITU. (2024). Global cybersecurity index 2024 (5th ed.). International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
19. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
20. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In Advances in Neural Information Processing Systems 30 (pp. 4765-4774).
21. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (PMLR 54, pp. 1273-1282).
22. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In Network and Distributed System Security Symposium (NDSS 2018). https://doi.org/10.14722/ndss.2018.23204
23. NIST. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1
24. NIST. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
25. O‘zbekiston Respublikasi Prezidenti. (2020). «Raqamli O‘zbekiston-2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida: 2020 yil 5 oktabrdagi PF-6079-son Farmon. https://lex.uz
26. O‘zbekiston Respublikasi Prezidenti. (2024). 2030 yilgacha sun’iy intellekt texnologiyalarini rivojlantirish strategiyasini tasdiqlash to‘g‘risida: 2024 yil 14 oktabrdagi PQ-358-son qaror. https://lex.uz/uz/docs/7159258
27. O‘zbekiston Respublikasi Prezidenti. (2026). O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida: 2026 yil 10 martdagi PF-38-son Farmon. https://lex.uz/docs/8079286
28. O‘zbekiston Respublikasi Qonuni. (2019). Shaxsga doir ma’lumotlar to‘g‘risida: 2019 yil 2 iyuldagi O‘RQ-547-son. https://lex.uz

29. O‘zbekiston Respublikasi Qonuni. (2022). Kiberxavfsizlik to‘g‘risida: 2022 yil 15 apreldagi O‘RQ-764-son. https://lex.uz/uz/docs/5960604
30. Ochilova, M. (2024, 29 mart). O‘zbekistondagi axborot resurslariga kiberhujumlar 2,4 barobarga oshdi. Kun.uz. https://kun.uz/news/2024/03/29/ozbekistondagi-axborot-resurslariga-kiberhujumlar-24-barobarga-oshdi
31. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173. https://doi.org/10.1007/s42979-021-00557-0
32. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305-316). https://doi.org/10.1109/SP.2010.25
33. Tapscott, D. (1996). The digital economy: Promise and peril in the age of networked intelligence. McGraw-Hill.
34. Tuxsinov, D. (2024, 6 aprel). Uzbekistan reports over 3 million cyberattacks for Q1 2024. Kun.uz. https://kun.uz/en/news/2024/04/06/uzbekistan-reports-over-3-million-cyberattacks-for-q1-2024
35. WEF. (2025). Global cybersecurity outlook 2025. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
36. Xurramov, A. (2024). Raqamli iqtisodiyot va axborot texnologiyalarining o‘rni va roli. Aktuar moliya va buxgalteriya hisobi ilmiy jurnali, 4(06), 38-42.