RAQAMLI IQTISODIYOT SHAROITIDA KIBER SUG‘URTA TIZIMINI RIVOJLANTIRISH: XALQARO TAJRIBA, QIYOSIY TAHLIL VA O‘ZBEKISTON UCHUN INNOVATSION MODEL

Fahriddinova Dilhumor Botirjon qizi
Xalq Sug‘urta kompaniyasining Toshkent
shahar filiali yetakchi mutaxassisi
https://doi.org/10.5281/zenodo.23240241

Annotatsiya. Ushbu maqolada raqamli iqtisodiyot sharoitida kiber sug‘urta tizimining iqtisodiy va institutsional ahamiyati, uning xalqaro rivojlanish tendensiyalari hamda O‘zbekiston sharoitida shakllantirish imkoniyatlari tadqiq etiladi. Raqamli bank xizmatlari, elektron tijorat, bulutli texnologiyalar, sun’iy intellekt va boshqa raqamli infratuzilmalarning kengayishi tashkilotlarning texnologik bog‘liqligini kuchaytirib, kiberhujumlar natijasida yuzaga keladigan moliyaviy yo‘qotishlar ehtimolini oshirmoqda. Shu sharoitda kiber sug‘urta nafaqat zararlarni qoplash, balki kiberxatarlarni aniqlash, risklarni kamaytirish va tashkilotlarning kiberbarqarorligini oshirishga xizmat qiluvchi moliyaviy mexanizm sifatida qaralmoqda.

Tadqiqotda tizimli adabiyotlar sharhi, qiyosiy tahlil, kontent tahlili va institutsional-tizimli yondashuvdan foydalanildi. AQSh, Yevropa Ittifoqi, Singapur va Yaponiya tajribasi bozor rivojlanishi, davlatning roli, risklarni baholash, underwriting, kiberxavfsizlik standartlari va sug‘urta mahsulotlari nuqtayi nazaridan taqqoslandi. Tadqiqot natijasida kiber sug‘urta bozorining asosiy muammolari sifatida tarixiy ma’lumotlarning yetishmasligi, kiber risklarning o‘zaro bog‘liqligi, sistemik risk, axborot assimetriyasi va standartlashtirilgan underwriting ma’lumotlarining cheklanganligi aniqlandi.

O‘zbekiston sharoitida kiber sug‘urta bozorining rivojlanishi uchun mavjud sug‘urta va kiberxavfsizlik infratuzilmasini o‘zaro integratsiya qilish zarur. Shu maqsadda maqolada Risk–Data–Insurance–Resilience (RDIR) konseptual modeli taklif etiladi. Model kiberxatarlarni identifikatsiya qilish, risklarni raqamli baholash, risklarni segmentatsiya qilish, dinamik underwriting, sug‘urta qoplamasi, zararlarni boshqarish va feedback asosida risk modelini takomillashtirish bosqichlarini birlashtiradi. Taklif etilayotgan model kiberxavfsizlik darajasini sug‘urta mukofoti bilan bog‘lash, ma’lumotlarga asoslangan tariflashni joriy etish va davlat-xususiy risk-sharing mexanizmlarini shakllantirish imkonini beradi.

Kalit so‘zlar: kiber sug‘urta, raqamli iqtisodiyot, kiberxavfsizlik, kiber risk, cyber resilience, underwriting, risk management, sun’iy intellekt, data-driven insurance, raqamli transformatsiya

Kirish. Raqamli transformatsiya iqtisodiy faoliyatning deyarli barcha yo‘nalishlarini o‘zgartirmoqda. Bank-moliya sektori, elektron tijorat, davlat xizmatlari, logistika, telekommunikatsiya va ishlab chiqarish jarayonlarining raqamli platformalarga ko‘chishi iqtisodiy samaradorlikni oshirayotgan bo‘lsa-da, ayni vaqtda tashkilotlarning axborot-kommunikatsiya texnologiyalariga bog‘liqligini kuchaytirmoqda.

Natijada kiberxavfsizlik masalasi faqat texnik muammo bo‘lib qolmasdan, korxonaning moliyaviy barqarorligi va biznesning uzluksiz faoliyatini ta’minlash bilan bog‘liq iqtisodiy muammoga aylanmoqda.

2026-yilgi World Economic Forum Global Cybersecurity Outlook hisobotida sun’iy intellekt kiberxavfsizlik muhitini o‘zgartirayotgan asosiy omillardan biri sifatida baholangan. Bu holat kiberxatarlarning nafaqat soni, balki ularning murakkabligi va iqtisodiy oqibatlari ham o‘zgarayotganini ko‘rsatadi.

Shu nuqtayi nazardan, kiber sug‘urta tashkilotlarning kiberhodisalar natijasida yuzaga keladigan moliyaviy zararlarini transfer qilish mexanizmi sifatida alohida ahamiyat kasb etadi. OECD kiber sug‘urtani kiberxavfsizlik investitsiyalarining o‘rnini bosuvchi vosita emas, balki risklarni boshqarishni to‘ldiruvchi mexanizm sifatida ko‘rsatadi. Sug‘urta tashkilotlarning kiberxatarlar to‘g‘risidagi xabardorligini oshirish, risklarni kamaytirishga investitsiyalarni rag‘batlantirish va hodisadan keyingi tiklanish jarayonini qo‘llab-quvvatlashi mumkin.

Kiber sug‘urta bozorining global iqtisodiy ahamiyati ham ortib bormoqda. Munich Re (**Munich Re — Germaniyada tashkil topgan, dunyodagi eng yirik qayta sug‘urtalash (reinsurance) kompaniyalaridan biri. Kompaniya 1880-yilda tashkil etilgan va bosh qarorgohi Myunxenda joylashgan**.) ma’lumotlariga ko‘ra, global kiber sug‘urta bozori 2025-yilda qariyb 15 mlrd AQSh dollarini tashkil etgan va 2030-yilga kelib 28 mlrd dollarga yaqinlashishi kutilmoqda.

Biroq kiber sug‘urta an’anaviy sug‘urta turlaridan sezilarli darajada farq qiladi. Kiber risklar tez o‘zgaradi, texnologik tizimlar o‘zaro bog‘langan va bitta hujum bir vaqtning o‘zida ko‘plab sug‘urtalanuvchilarga zarar yetkazishi mumkin. ENISA (**ENISA — Yevropa Ittifoqining Kiberxavfsizlik agentligi European Union Agency for Cybersecurity**) ham kiber sug‘urta uchun individual riskdan tashqari portfolio darajasidagi o‘zaro bog‘liqliklarni hisobga olish zarurligini ta’kidlaydi.

O‘zbekistonda raqamli iqtisodiyotning rivojlanishi bilan ushbu muammo tobora dolzarb bo‘lmoqda. Mamlakatda “Kiberxavfsizlik to‘g‘risida”gi Qonun, “Sug‘urta faoliyati to‘g‘risida”gi Qonun va 2026–2030-yillarga mo‘ljallangan kiberxavfsizlik siyosati doirasidagi mexanizmlar shakllanmoqda.

Shu sababli mazkur tadqiqotning asosiy maqsadi xalqaro tajribani qiyosiy o‘rganish, kiber sug‘urta bozorining institutsional muammolarini aniqlash va O‘zbekiston sharoitiga mos keluvchi innovatsion kiber sug‘urta modelini ishlab chiqishdan iborat.

Tadqiqotning asosiy savoli quyidagicha shakllantiriladi:

O‘zbekistonda raqamli iqtisodiyotning rivojlanishi sharoitida kiber sug‘urta bozorini qanday institutsional va texnologik model asosida shakllantirish mumkin?

Adabiyotlar sharhi. Kiber sug‘urta bo‘yicha ilmiy adabiyotlarni shartli ravishda to‘rt yo‘nalishga ajratish mumkin: kiber risklarning sug‘urtalanish imkoniyati, iqtisodiy zararlarni baholash, data-driven underwriting va cyber resilience.

Biener, Eling va Wirfs (2015) kiber risklarning sug‘urtalanish imkoniyatini empirik jihatdan o‘rgangan. Tadqiqotda 994 ta real kiber zarar holati tahlil qilingan bo‘lib, ma’lumotlarning yetishmasligi, risklarning o‘zaro bog‘liqligi va noaniqlik kiber sug‘urta bozorining asosiy muammolari sifatida ko‘rsatilgan.

Romanosky (2016) kiber hodisalarning sabablari va iqtisodiy oqibatlarini tahlil qilib, kiber xavfsizlikni boshqarishda iqtisodiy rag‘batlarning ahamiyatini ko‘rsatgan.

Nurse tadqiqotlari kiber sug‘urta underwriting va claim jarayonlarida ma’lumotlarning muhim rolini ochib beradi. Ularning tadqiqotlari kiber sug‘urta bozorida ma’lumotlarni yig‘ish va standartlashtirish muammosi mavjudligini ko‘rsatadi.

OECD (2017) kiber sug‘urtani kiberxavfsizlik ekotizimining bir qismi sifatida ko‘radi. Tashkilotga ko‘ra, sug‘urta risklarni faqat transfer qilish emas, balki risklarni aniqlash va kamaytirishga investitsiyalarni rag‘batlantirish vositasi bo‘lishi mumkin.

ENISAning 2024-yilgi tadqiqoti kiber sug‘urta modellarida statistik usullar, machine learning va AI imkoniyatlaridan foydalanishni alohida ko‘rib chiqadi. Hisobotda sug‘urtalovchilar uchun loss frequency, loss severity, individual risk va portfolio riskini birgalikda baholash zarurligi ko‘rsatiladi.

Shuningdek, zamonaviy tadqiqotlarda cyber resilience tushunchasining ahamiyati ortmoqda. Bunda tashkilotning asosiy maqsadi hujum ehtimolini mutlaq nolga tushirish emas, balki hujumning oldini olish, unga tezkor javob berish va faoliyatni imkon qadar tez tiklashdan iborat.

Adabiyotlar tahlili shuni ko‘rsatadiki, mavjud tadqiqotlarda kiber sug‘urta bozorining alohida elementlari chuqur o‘rganilgan bo‘lsa-da, rivojlanayotgan davlatlar uchun **risk baholash + ma’lumotlar + sug‘urta + cyber resilience + davlat regulyatsiyasi** elementlarini yagona konseptual modelga birlashtirish masalasi yetarlicha ishlab chiqilmagan.

Mazkur tadqiqot aynan ushbu ilmiy bo‘shliqni to‘ldirishga qaratilgan

Tadqiqot metodologiyasi. Tadqiqotning metodologik asosini tizimli adabiyotlar sharhi, qiyosiy tahlil, kontent tahlili va institutsional-tizimli yondashuv tashkil etadi.

3.1. Tizimli adabiyotlar sharhi

Kiber sug‘urta, kiber risk, cyber resilience, underwriting, risk modelling va data-driven insurance bo‘yicha ilmiy tadqiqotlar hamda OECD, ENISA, Munich Re kabi xalqaro tashkilotlarning materiallari tahlil qilindi.

3.2. Qiyosiy tahlil

AQSh, Yevropa Ittifoqi, Singapur va Yaponiya quyidagi mezonlar asosida taqqoslandi:

- bozor rivojlanish darajasi;
- davlatning roli;
- risk baholash mexanizmlari;
- kiberxavfsizlik standartlari;
- underwriting;
- SME segmentining ahamiyati;
- ma’lumotlar infratuzilmasi;
- risk-sharing mexanizmlari.

3.3. Institutsional tahlil

O‘zbekistonning kiberxavfsizlik va sug‘urta faoliyatiga oid normativ-huquqiy bazasi o‘rganildi.

3.4. Konseptual modellashtirish

Xalqaro tajribadan aniqlangan samarali elementlar asosida O‘zbekiston uchun RDIR modeli ishlab chiqildi.

4. XALQARO TAJRIBA

4.1. AQSh

AQSh global kiber sug‘urta bozorining eng yirik segmentiga ega. Munich Re 2025 tahliliga ko‘ra, Shimoliy Amerika 2024-yilda 10,6 mlrd AQSh dollari miqdoridagi kiber sug‘urta mukofotlarini shakllantirib, global bozorning 69 foizini tashkil etgan.

AQSh modelining asosiy xususiyatlari:

- xususiy sektorning yetakchi roli;
- rivojlangan brokerlik infratuzilmasi;
- risk analytics;
- threat intelligence;
- rivojlangan qayta sug‘urtalash;
- individual underwriting.

Shu bilan birga, sistemik risk, ransomware va uchinchi tomon texnologik provayderlariga bog‘liqlik bozor uchun muhim muammo bo‘lib qolmoqda.

4.2. Yevropa

Yevropa modelida huquqiy va regulyativ talablar katta rol o‘ynaydi. Ma’lumotlarni himoya qilish, kiberxavfsizlik va tashkilotlarning javobgarligi sug‘urta mahsulotlarining shakllanishiga ta’sir qiladi.

2024-yilgi ENISA tadqiqoti kiber sug‘urta modellarida AI va ilg‘or statistik usullardan foydalanish imkoniyatlarini ko‘rib chiqadi.

Yevropa tajribasining O‘zbekiston uchun asosiy sabog‘i — kiber sug‘urta bozorini rivojlantirishdan oldin risklarni tasniflash va minimal kiberxavfsizlik talablarini standartlashtirish zarurligidir.

4.3. Singapur

Singapur tajribasi davlat siyosati va sug‘urta rag‘batlarini integratsiya qilish nuqtayi nazaridan muhimdir.

Ushbu modelda kiberxavfsizlik standartlariga javob beradigan tashkilotlar uchun sug‘urta shartlari yaxshilanishi mumkin. Bu yondashuvdan O‘zbekiston uchun **“yuqori kiberxavfsizlik = pastroq sug‘urta riski = qulayroq tarif”** tamoyilini ishlab chiqish mumkin.

4.4. Yaponiya

Yaponiya tajribasi SME segmentiga e’tibor qaratishi bilan ajralib turadi. Bu O‘zbekiston uchun ham muhim, chunki kichik biznes subyektlarining ko‘pchiligida alohida kiberxavfsizlik bo‘limi yoki professional cyber-risk manager bo‘lmasligi mumkin.

Shu sababli kiber sug‘urta mahsuloti mustaqil polis sifatida emas, balki:

Cybersecurity audit + Monitoring + Incident Response + Insurance kompleksi sifatida taklif qilinishi mumkin.

5. QIYOSIY TAHLIL

Ko‘rsatkich	AQSh	Yevropa	Singapur/Yaponiya	O‘zbekiston
Bozor	Yetuk	Rivojlangan	Rivojlanayotgan	Shakllanish bosqichi
Davlat roli	O‘rtacha	Yuqori	Yuqori	Rivojlanmoqda
Underwriting	Juda rivojlangan	Rivojlangan	Rivojlanayotgan	Boshlang‘ich
AI/Data analytics	Yuqori	Yuqori	O‘sayotgan	Istiqbolli
SME segmenti	Muhim	Muhim	Markaziy	Juda muhim
Risk ma’lumotlari	Keng	Nisbatan keng	Rivojlanmoqda	Cheklangan
Cybersecurity integration	Yuqori	Juda yuqori	Juda yuqori	Rivojlantirish zarur
Asosiy muammo	Systemic risk	Compliance/protection gap	Standartlashuv	Data va infratuzilma

2024-yil bozor hajmi bo‘yicha Shimoliy Amerika 69 foiz, Yevropa 21 foiz ulushga ega bo‘lgan; Asia/Oceania ulushi esa 2027-yilga kelib 8 foizga yetishi prognoz qilingan. Shu sababli ushbu ko‘rsatkichlarni bir xil yilga tegishli global ulushlar sifatida talqin qilish noto‘g‘ri bo‘ladi.

6. O‘ZBEKISTONDA KIBER SUG‘URTANI RIVOJLANTIRISH MUAMMOLARI

O‘zbekistonda kiber sug‘urta bozorining rivojlanishini cheklashi mumkin bo‘lgan asosiy omillar quyidagilardan iborat:

6.1. Ma’lumotlar bazasining yetarli emasligi

Kiber sug‘urta tariflarini ilmiy asosda hisoblash uchun:

- hodisalar soni;
- zarar miqdori;
- hujum turi;
- tiklanish vaqti;
- tashkilotning himoya darajasi

kabi ma’lumotlar kerak.

6.2. Risklarni standartlashtirish muammosi

Sug‘urta kompaniyalari turli tashkilotlarning kiberxavfsizlik darajasini bir xil mezon bilan baholashi zarur.

6.3. SME uchun mahsulotlarning murakkabligi

Kichik korxonalarga yirik korporatsiyalar uchun ishlab chiqilgan murakkab polislarni taklif qilish iqtisodiy jihatdan samarali bo‘lmasligi mumkin.

6.4. Sistemik risk

Bir cloud platforma, dasturiy ta’minot yoki texnologik provayderga qilingan hujum ko‘plab sug‘urtalanuvchilarga bir vaqtning o‘zida zarar yetkazishi mumkin.

6.5. Sug‘urta va kiberxavfsizlikning ajratilganligi

Kelajakda sug‘urta kompaniyasi faqat polis sotuvchi tashkilot emas, balki kiberxavfsizlik ekotizimining faol ishtirokchisiga aylanishi kerak.

7. O‘ZBEKISTON UCHUN RDIR INNOVATSION MODELI

Mazkur tadqiqotning asosiy ilmiy natijasi sifatida **Risk–Data–Insurance–Resilience (RDIR)** modeli taklif etiladi.

Model quyidagi siklni ifodalaydi:

Kiber aktivlar → Risk identifikatsiyasi → Risk baholash → Risk klassifikatsiyasi → Dynamic underwriting → Sug‘urta → Incident/Claim → Feedback → Yangilangan risk modeli

7.1. Risk identifikatsiyasi

Tashkilotning raqamli aktivlari aniqlanadi.

Baholanadigan elementlar:

- serverlar;
- cloud infrastructure;
- ma’lumotlar;
- internetga ulangan qurilmalar;
- xodimlar;
- uchinchi tomon provayderlari;
- muhim axborot infratuzilmasi.

7.2. Cyber Risk Index

Tadqiqotda quyidagi konseptual indeks taklif qilinadi:

CRI = 0.20V + 0.20E + 0.20D + 0.15T + 0.15R + 0.10C

Bu yerda:

- **V** — vulnerability;
- **E** — exposure;
- **D** — data sensitivity;
- **T** — technological dependence;
- **R** — resilience;

- **C** — compliance.

Koeffitsiyentlar dastlab ekspert baholashiga asoslangan konseptual qiymatlar bo‘lib, real ma’lumotlar yig‘ilgandan keyin statistik yoki machine-learning usullari orqali kalibrlanishi kerak.

Bu jihat modelning ilmiy muhim tomonidir: **maqolada ushbu koeffitsiyentlar empirik haqiqat sifatida emas, kelajakdagi empirik tadqiqot uchun boshlang‘ich parametrlar sifatida talqin qilinadi.**

7.3. Risk segmentatsiyasi

CRI	Risk	Tavsiya
0–0.33	Past	Standart polis, chegirma
0.34–0.66	O‘rta	Qo‘shimcha xavfsizlik talablari
0.67–1.00	Yuqori	Yuqori premium, limit yoki majburiy security improvement

7.4. Dynamic underwriting

Sug‘urta mukofoti quyidagicha konseptual shaklda ifodalanadi:

$$P = B \times CRF \times EF \times IF \times SF$$

Bu yerda:

- **P** — sug‘urta mukofoti;
- **B** — base premium;
- **CRF** — cyber risk factor;
- **EF** — exposure factor;
- **IF** — industry factor;
- **SF** — security factor.

Tashkilotning kiberxavfsizlik darajasi yaxshilanganda **SF** kamayishi va natijada sug‘urta mukofoti pasayishi mumkin.

Shunday qilib, sug‘urta kompaniyasi korxonani xavfsizlikka investitsiya qilishga iqtisodiy jihatdan rag‘batlantiradi.

8. RDIR MODELINING ILMIY YANGILIGI

Taklif etilayotgan modelning ilmiy yangiligi quyidagi besh elementning integratsiyasida ifodalanadi:

1. **Risk-based insurance** — sug‘urta mukofoti risk darajasiga bog‘lanadi.
2. **Data-driven underwriting** — qarorlar real ma’lumotlarga asoslanadi.
3. **Cybersecurity incentive** — xavfsizlik darajasi yaxshilanganda tarif pasayishi mumkin.
4. **Cyber resilience** — sug‘urta hujumdan keyingi tiklanish qobiliyatini ham hisobga oladi.
5. **Feedback mechanism** — har bir yangi incident kelajakdagi risk modelini takomillashtirish uchun ma’lumot yaratadi.

Mazkur yondashuv ENISAning cyber insurance modelling va AI bo‘yicha tadqiqotlari bilan metodologik jihatdan mos keladi. ENISA sug‘urta kompaniyalari uchun individual risk

bilan bir qatorda portfolio risk, loss frequency, loss severity va texnologik o‘zaro bog‘liqliklarni hisobga olish zarurligini ko‘rsatadi.

9. MODELNI O‘ZBEKISTONDA BOSQICHMA-BOSQICH JORIY ETISH

Modelni birdaniga butun iqtisodiyotga joriy etish o‘rniga uch bosqichli strategiya taklif etiladi.

I bosqich — 2026–2027-yillar

Pilot bosqich

- yirik banklar;
- fintech kompaniyalari;
- telekommunikatsiya;
- elektron tijorat;
- muhim axborot infratuzilmasi.

Ushbu bosqichda kiber risk indikatorlari va standart polislar ishlab chiqiladi.

II bosqich — 2028–2029-yillar

Bozorni kengaytirish

- SME segmenti;
- cloud xizmatlari;
- logistika;
- ishlab chiqarish;
- davlat pudratchilari.

Ushbu bosqichda risk ma’lumotlar bazasi shakllantiriladi.

III bosqich — 2030-yildan

Data-driven milliy model

- AI-assisted underwriting;
- real-time risk monitoring;
- predictive analytics;
- automated claims;
- xalqaro qayta sug‘urtalash;
- davlat-xususiy risk-sharing.

10. KUTILAYOTGAN IQTISODIY SAMARALAR

RDIR modelini joriy etish quyidagi iqtisodiy natijalarni berishi mumkin:

Birinchidan,

kiberhujumlardan keladigan to‘g‘ridan-to‘g‘ri moliyaviy zararlarni qoplash imkoniyati oshadi.

Ikkinchidan,

korxonalar kiberxavfsizlikka investitsiya qilishga iqtisodiy rag‘bat oladi.

Uchinchidan,

sug‘urta kompaniyalari uchun yangi bozor segmenti shakllanadi.

To‘rtinchidan,

kiberhodisalar bo‘yicha milliy statistik ma’lumotlar bazasi vujudga keladi.

Beshinchidan,

davlatning yirik kiberhodisalarga javob berishdagi moliyaviy yuklamasi kamayishi mumkin.

Oltinchidan,

O‘zbekistonning raqamli iqtisodiyoti uchun umumiy cyber resilience darajasi oshadi.

11. MUHOKAMA

Tadqiqot natijalari kiber sug‘urtani faqat moliyaviy kompensatsiya vositasi sifatida ko‘rish yetarli emasligini ko‘rsatadi.

An’anaviy sug‘urta modelida asosiy jarayon:

Risk → Insurance → Loss → Compensation

ko‘rinishida bo‘lsa, zamonaviy kiber sug‘urta modelida:

Risk identification → Risk reduction → Insurance → Incident response → Compensation → Learning

sikli shakllanishi kerak.

Bu farq kiber sug‘urtaning o‘ziga xosligini belgilaydi.

OECD sug‘urtaning kiberxavfsizlikka investitsiyalarni rag‘batlantirishi mumkinligini qayd etadi. OECD ENISA esa AI va machine learning yordamida kiber risklarni baholash imkoniyatlari rivojlanayotganini ko‘rsatadi.

Shu sababli O‘zbekiston uchun optimal model AQShning sof bozor modelini yoki Yevropaning qat’iy regulyativ modelini to‘liq ko‘chirish emas. O‘zbekiston uchun **gibrid model** maqsadga muvofiq:

Davlat regulyatsiyasi + xususiy sug‘urta + kiberxavfsizlik standartlari + data analytics + qayta sug‘urtalash.

12. XULOSA

Tadqiqot natijalari raqamli iqtisodiyotning rivojlanishi bilan kiber risklarning iqtisodiy ahamiyati ortib borayotganini ko‘rsatdi. Kiber sug‘urta ushbu sharoitda tashkilotlarning moliyaviy barqarorligini ta’minlash, zararlarni transfer qilish va kiberxavfsizlikka investitsiyalarni rag‘batlantirishning muhim vositasiga aylanmoqda.

Global kiber sug‘urta bozori 2025-yilda qariyb 15 mlrd AQSh dollarini tashkil etgan va Munich Re 2030-yilga borib bozor hajmini 28 mlrd dollar atrofida baholamoqda.

Xalqaro tajriba uch xil asosiy yondashuvni ko‘rsatdi. AQShda bozor xususiy sektor va rivojlangan risk analytics asosida rivojlangan. Yevropada huquqiy va regulyativ mexanizmlar muhim rol o‘ynaydi. Singapur va Yaponiya tajribasi esa davlat qo‘llab-quvvatlashi, standartlashtirish va SME segmentiga e’tibor berishning samarali jihatlarini ko‘rsatadi.

Tadqiqotning asosiy ilmiy natijasi sifatida O‘zbekiston uchun **Risk–Data–Insurance–Resilience (RDIR)** modeli taklif qilindi. Model kiberxatarlarni identifikatsiya qilish, Cyber Risk Index orqali baholash, risklarni segmentatsiya qilish, dynamic underwriting, sug‘urta qoplamasi, claim management va feedback mexanizmlarini yagona tizimga birlashtiradi.

Modelning muhim jihati shundaki, sug‘urta mukofoti tashkilotning kiberxavfsizlik holati bilan bog‘lanadi. Natijada korxona kiberxavfsizlikka investitsiya qilgan sari uning risk profili yaxshilanadi va kelgusida sug‘urta xarajatlarini kamaytirish imkoniyati paydo bo‘ladi.

O‘zbekiston uchun kiber sug‘urta bozorini shakllantirishning asosiy shartlari quyidagilardan iborat:

- milliy kiber risk ma’lumotlar bazasini yaratish;
- kiber risklarni baholash standartlarini ishlab chiqish;
- SME uchun soddalashtirilgan sug‘urta mahsulotlarini joriy etish;
- kiberxavfsizlik sertifikatsiyasini sug‘urta tariflari bilan bog‘lash;
- AI-assisted underwriting tizimini bosqichma-bosqich joriy etish;
- qayta sug‘urtalash imkoniyatlarini kengaytirish;
- davlat-xususiy risk-sharing mexanizmlarini shakllantirish.

Shunday qilib, O‘zbekistonda kiber sug‘urta bozorining rivojlanishi faqat yangi sug‘urta mahsulotlarini yaratish masalasi emas. U raqamli iqtisodiyot, kiberxavfsizlik, ma’lumotlar boshqaruvi, sug‘urta texnologiyalari va davlat regulyatsiyasini birlashtiruvchi kompleks institutsional tizim sifatida qaralishi lozim.

Tadqiqotning keyingi bosqichi sifatida taklif etilayotgan RDIR modelini real korxonalar ma’lumotlari asosida empirik sinovdan o‘tkazish, Cyber Risk Index koeffitsiyentlarini statistik usullar bilan kalibrlash va O‘zbekiston korxonalari uchun optimal sug‘urta mukofotini hisoblash metodikasini ishlab chiqish maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance – Issues and Practice, 40(1), 131–158. https://doi.org/10.1057/gpp.2014.19
2. European Union Agency for Cybersecurity. (2024). Cyber insurance – Models and methods and the use of AI. ENISA.
3. Munich Re. (2025). Cyber insurance: Risks and trends 2025. Munich Re.
4. Munich Re. (2026). Global cyber risk and insurance survey 2026. Munich Re
5. Munich Re. (2026). Cyber insurance: Risks and trends 2026. Munich Re.
6. Nurse, J. R. C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). The data that drives cyber insurance: A study into the underwriting and claims processes. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE.
7. OECD. (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. https://doi.org/10.1787/9789264282148-en.
8. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001
9. Swiss Re Institute. (2022). Cyber insurance: Strengthening resilience for the digital transformation. Swiss Re Institute.
10. World Economic Forum. (2026). Global cybersecurity outlook 2026. World Economic Forum.
11. O‘zbekiston Respublikasi. (2021). Sug‘urta faoliyati to‘g‘risida: O‘RQ-730-son Qonun.
12. O‘zbekiston Respublikasi. (2022). Kiberxavfsizlik to‘g‘risida: O‘RQ-764-son Qonun.