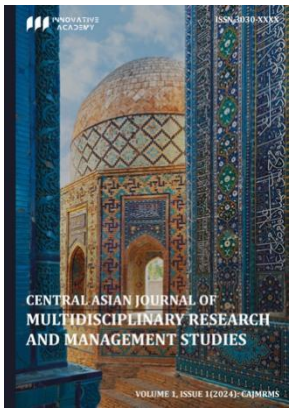


KIBERXAVFSIZLIK XAVFLARINI MOLIYALASHTIRISH (CYBER RISK TRANSFER) VA SUG'URTA QOPLAMALARINI BOSHQARISH.

Uralov Baxtiyor Maxmudovich
"CYBER UNIVERSITY" Davlat universiteti
Ijtimoiy fanlar kafedrasi assistant-o'qituvchisi
uralovbaxtiyor20@gmail.com, +99899-591-54-68
Ochilova Sadoqat Qodir qizi
Huquq va biznes fakulteti MNG 101-guruh talabasi
sadoqatochilova966@gmail.com +998771183550
https://doi.org/10.5281/zenodo.18333349

ARTICLE INFO

Received: 31st December 2025
Accepted: 11th January 2026
Published: 22nd January 2026

KEYWORDS

Kiberxavfsizlik, kiberxavflarni moliyalashtirish, Cyber Risk Transfer, kiber sug'urta, risklarni boshqarish, kiber tahdidlar, ma'lumotlar buzilishi, ransomware, kiber javobgarlik, biznesning uzluksizligi, raqamli xavfsizlik, kiber hodisalar, sug'urta qoplamalari, riskni o'tkazish, kiber barqarorlik.

ABSTRACT

Ushbu maqolada kiberxavfsizlik xavflarini moliyalashtirish (Cyber Risk Transfer) hamda kiber sug'urta qoplamalarini boshqarishning nazariy va amaliy jihatlari yoritiladi. Raqamli transformatsiya jarayonida korxonalar duch kelayotgan kiber tahdidlar ko'lami kengayib borayotgani, ularning moliyaviy oqibatlari chuqurlashayotgani tahlil qilinadi. Kiberxavflarni moliyaviy boshqarish mexanizmlari — xususan, kiber sug'urta instrumentlari — biznes barqarorligini ta'minlashda muhim vosita sifatida ko'rib chiqiladi. Tashkilotlarning kiberhujumlar oqibatida yuzaga kelishi mumkin bo'lgan zararlarni kamaytirish va boshqarish bo'yicha samarali yondashuvlar taklif etiladi.

KIRISH

Raqamli iqtisodiyotning jadal rivojlanishi moliya sohasi uchun yangi imkoniyatlar yaratgani kabi, o'sib borayotgan kiberxavflarni ham yuzaga keltirmoqda. Bugungi kunda tashkilotlar axborot tizimlari, moliyaviy operatsiyalar, mijozlar ma'lumotlari va biznes jarayonlarining katta qismini raqamlashtirar ekan, kiberhujumlar tufayli yuzaga kelishi mumkin bo'lgan zararlar ham keskin ortib bormoqda. Aynan shuning uchun kiberxavfszlik xavflarni moliyalashtirish (Cyber Risk Transfer) mexanizmlari va kiber sug'urta qoplamalarini samarali boshqarish strategiyalari zamonaviy korxonalar barqarorligini ta'minlashda muhim ahamiyat kasb etadi.

Ushbu maqolada kiberxavflarni moliyalashtirishning mohiyati, kiber sug'urta turlari, qoplama shartlari, risklarni baholash tamoyillari hamda sug'urta qoplamalarini samarali boshqarish mexanizmlari ilmiy-amaliy nuqtai nazardan tahlil qilinadi. Mazkur yo'nalish korxonalar uchun strategik ustuvorlikka aylanib borar ekan, to'g'ri yondashuv biznesning raqobatbardoshligi va barqaror rivojlanishini ta'minlashda hal qiluvchi omil bo'lib qolmoqda.

MAVZUGA OID ADABIYOTLAR TAHLILI

Kiberxavfsizlik risklarini moliyalashtirish va sug'urta qoplamalari mavzusi so'nggi yillarda ilmiy adabiyotlarda keng yoritilmoqda. Xalqaro tadqiqotlar (masalan, Aon, Allianz, Munich Re kabi tashkilotlar hisobotlari) kiber sug'urta bozorining jadal rivojlanishi, risklarni baholashda sun'iy intellektning ahamiyati, va davlat-xususiy hamkorlikning ro'lini o'rgangan.

O‘zbekiston kontekstida esa maxsus kiber sug‘urta mahsulotlarining hali keng tarqalmaganligi, qonuniy bazaning rivojlanayotgan holati va milliy kiberxavfsizlik tizimlarining (masalan, UZCERT) mavjudligi haqida ma’lumotlar mavjud. Shuningdek, Sci-P va Cyber Law kabi manbalar O‘zbekistonda raqamlashtirish va sug‘urta bozoridagi yangi yo‘nalishlar haqida ma’lumot beradi.

Adabiyotlar tahlili shuni ko‘rsatadiki, global tajriba kiber risklarni o‘tkazish va sug‘urta qoplamalarini boshqarishda ancha rivojlangan bo‘lsa, O‘zbekistonda bu yo‘nalishda hali ko‘p ishlar qilinishi kerak.

TADQIQOT METODOLOGIYASI

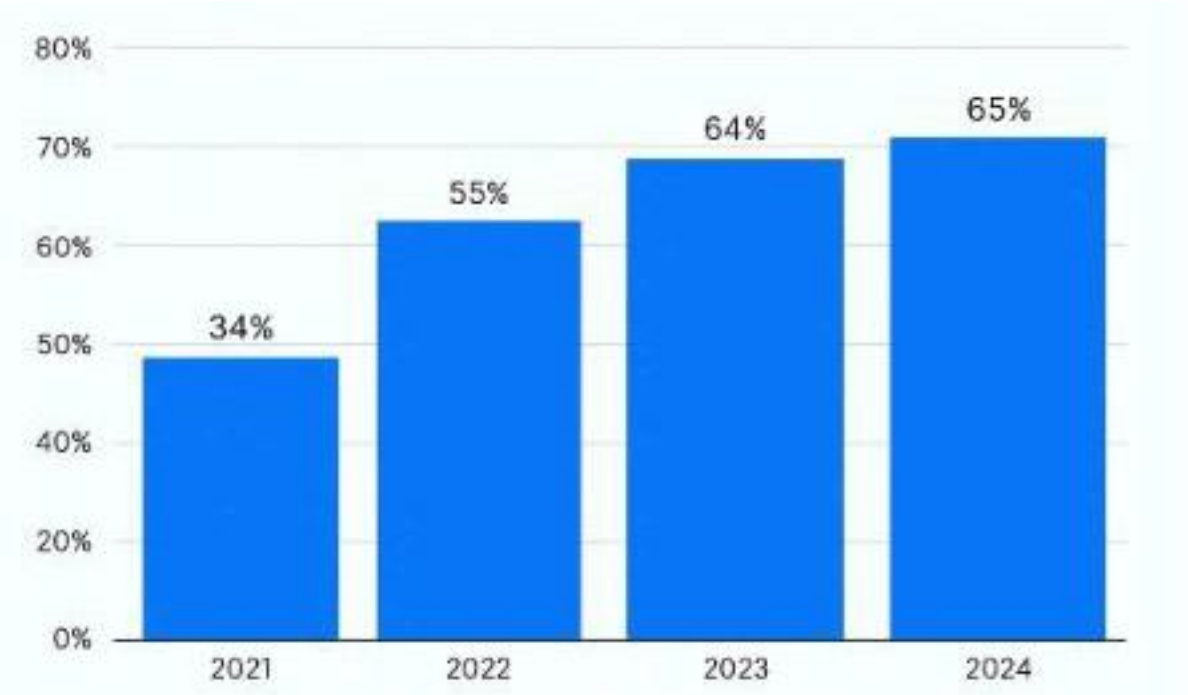
Kiberxavfsizlik xavflarini moliyalashtirish (cyber risk transfer) va sug'urta qoplamalarini boshqarishda Tadqiqot quyidagi metodlardan foydalangan holda olib borildi birinchidan tahliliy-metodologik yondashuv bu orqali biz kiber risklarni moliyalashtirishning nazariy asoslari va turlari tahlil qilindi. Ikkinchidan qiyosiy tahlil qilish orqali O‘zbekiston va xorijiy davlatlar tajribalari jadval shaklida solishtirildi. Uchinchidan statistik tahlilinib 2021–2024 yillar davomida moliyaviy tashkilotlarga qilingan ransomware hujumlari dinamikasi grafik orqali tahli qilindi. To‘rtinchidan maslahat va takliflar ishlab chiqishda muammolar asosida amaliy yechimlar taklif qilindi.

TAHLIL VA NATIJALAR MUHOKAMASI

Kiberxavfsizlik bu - kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati[1] hisoblanadi. Shu bilan birga , kiberxavflarni moliyalashtirish — bu tashkilot kiberhujumlar oqibatida ko‘rishi mumkin bo‘lgan moliyaviy zararni kamaytirishning iqtisodiy instrumentlari majmuasidir. Kiber sug‘urta esa ushbu jarayonning asosiy yo‘nalishlaridan biri bo‘lib, u kiberhodisalar tufayli yuzaga keladigan to‘xtab qolishlar, ma’lumotlar buzilishi, firibgarlik, tizim ishdan chiqishi kabi holatlarda zararlarni qoplashga xizmat qiladi. Zamonaviy boshqaruvda bu mexanizmlar nafaqat moliyaviy himoya, balki risklarni strategik boshqarish, ichki xavfsizlik siyosatini mustahkamlash va hujumlarga tayyorgarlikni oshirish vositasi sifatida ham ko‘riladi.

Xalqaro Valyuta Jamg‘armasining Global Moliyaviy Barqarorlik Hisobotiga ko‘ra, banklar kiberhujumlar uchun eng ko‘p nishon bo‘lmoqda. Bu yo‘qotishlarga bilvosita zararlar va obro‘ga salbiy ta’sirlar ham qo‘shilsa, real ko‘rsatkichlar yanada yuqori bo‘lishi mumkin.[2]

[1] Источник: LEX.UZ. https://share.google/hMGUuTJqgVfvZLSes
[2] Источник: TDIU. https://share.google/cfYgZdPEOZ9RHQGnO



1-rasm. 2021-yildan 2024-yilgacha dunyo bo‘yicha moliyaviy tashkilotlarga qilingan ransomware (ma'lumotlarni garovga oluvchi) hujumlar ulushi.[3]

Yuqoridagi rasmda 2021–2024 yillar davomida dunyo bo‘yicha moliyaviy tashkilotlarga qilingan ransomware hujumlari ulushi dinamikasi tasvirlangan.Shunindek ushbu grafikni tahlil qiladigan bo’lsak, 2021–2024 yillar oralig‘ida moliyaviy tashkilotlarga nisbatan ransomware hujumlari deyarli ikki baravar oshgan (34% dan 65% gacha). Bu moliya sektori global miqyosda kiberjinoyatchilar uchun eng daromadli va zaif nishonlardan biriga aylanganini ko‘rsatadi.

2021 → 2022: 34% dan 55% ga oshgan, bu degani 21% o‘sish. Bu davrda hujumlar sonining keskin oshishiga pandemiyadan keyingi raqamlashtirish, masofaviy ish modeli va moliyaviy xizmatlarning onlayn ko‘payishi sabab bo‘lgan.

2022 → 2023: 55% dan 64% ga ko’rsatkich o’sgan , bu oraliqda 9% o‘sishni tashkil etgan. Bu esa moliyaviy tizimni nishonga oluvchi professional kiber guruhlar sonining ko‘paygani anglatadi.

2023 → 2024: 64% dan 65% ga yetgan, bu atigi 1% o‘sishdir.Shuningdek, bu o‘sish sekinlashganini ko’rsatadi, bu esa ikki omilga ishora qiladi:

1. tashkilotlarda himoya kuchaygan,

2. hujumlar allaqachon yuqori darajaga yetib bo‘lgan.

Eng yaxshi sa’y-harakatlarga qaramay, doimiy ravishda qoldiq (residual) kiber xavf mavjud bo‘ladi. Bu xavflar uchinchi tomon oldidagi kiber majburiyatlarga, ish samaradorligining pasayishiga, savdo yo‘qotilishiga va yetkazib berish zanjiridagi uzilishlarga olib kelishi mumkin. Shu xavfni yaxshiroq boshqarish uchun tashkilotlar kiberxavfsizlik xavfini moliyalashtirish strategiyasini qabul qilishi kerak.

Kiberxavfsizlik xavfini moliyalashtirish strategiyasi — bu kiberxavfsizlik sohasidagi mumkin bo‘lgan zararlar uchun moliyaviy javobgarlikni boshqa tomonga, odatda sug‘urta polislar yoki

[3] Источник: TDIU. https://share.google/cfYgZdPEOZ9RHQGnO

shartnoma kelishuvlari orqali, o‘tkazish strategik jarayonidir. Risklarni oldini olish yoki yumshatish xavf-xatarlarning sodir bo‘lishining oldini olishga qaratilgan bo‘lsa,buni moliyalashtirish ba’zi tahdidlarning oldini olishning imkonsizligini tan oladi va tashkilotni ularning moliyaviy oqibatlarini boshqarishga tayyorlaydi.

Kiberxavfsizlik xavfni moliyalashtirishning asosiy tushunchalari:

1. Riskdan qochish (Risk Avoidance):

Ma’lum kiber xavflardan to‘liq qochish choralarini ko‘rish. Masalan, yuqori xavfli faoliyat yoki kiber hodisaga olib kelishi mumkin bo‘lgan muhitlardan uzoq turish.

2. Xavfni kamaytirish (Risk Mitigation):

Kiber xavflarning ehtimoli yoki ta’sirini qattiq xavfsizlik choralari orqali kamaytirish. Bunga muntazam dasturiy ta’minot yangilanishi, xodimlarni o‘qitish va ilg‘or kiberxavfsizlik texnologiyalarini joriy etish kiradi.

3. Xavfni qabul qilish (Risk Acceptance):

Ba’zi kiber xavflarni biznesning tabiiy qismi sifatida qabul qilish. Bu odatda ta’siri yoki ehtimoli past bo‘lgan xavflar uchun qo‘llanadi, ular oldini olish yoki kamaytirishga sarflanadigan xarajatlarni oqlamaydi.Redditdagi bir kiberxavfsizlik mutaxassisi shunday yozgan edi: «Hamma risklardan qochib bo‘lmaydi, shuning uchun biz ba’zi risklarni qabul qilishimizga to‘g‘ri keladi»[4]. Bu fikr risklarni uzatish zamonaviy kiberxavfsizlik tizimlarida nima uchun muhim ekanligini aniq aks ettiradi.

4. Xavfni o‘tkazish (Risk Transference):

Kiber xavflarning moliyaviy ta’sirini boshqa tashkilotga o‘tkazish, ko‘pincha kiber sug‘urta orqali amalga oshiriladi. Bu yondashuv orqali tashkilot kiber hodisalar bilan bog‘liq xarajatlar uchun yolg‘iz javobgar bo‘lmaydi.[5]

Zamonaviy murakkab tahdidlar tizimida tashkilotlar bir qator muammolarga duch keladi:

1. Ba’zi tahdidlarning oldini olishning imkonsizligi: barcha sa’y-harakatlarga qaramay, ayrim risklar sizdan mustaqil omillar sababli oldini olish mumkin emas.

2. Moliyaviy himoya: Katta kiberhodisa millionlab dollarlik xarajatlarga, sud xarajatlariga va obro‘ga zarar yetkazishi mumkin, bu esa tashkilotning mavjudligiga xavf tug‘diradi.

3. Resurslarni optimallashtirish: Ba’zi risklarni boshqa tomonlarga uzatish orqali siz cheklangan resurslaringizni bevosita nazorat qila oladigan tahdidlarga qarshi kurashishga qaratishingiz mumkin.

4. Normativ talablar bilan moslik: Ko‘plab sohalarda tashkilotlardan risklarni boshqarish strategiyalarini, shu jumladan risklarni uzatish variantlarini taqdim etish talab etiladi.

So‘nggi tadqiqotlarga ko‘ra, 2023 yilda ma’lumotlar tarqalishi o‘rtacha 4,45 million dollarni tashkil qilgan, bu esa moliyaviy himoya mexanizmlarining, jumladan risklarni uzatishning zarurligini yana bir bor ko‘rsatadi.[6]

[4] https://share.google/R4gCKvV7n7CUwZOIj
[5] Источник: LinkedIn. https://share.google/eGawy3DEh1FyOic1n
[6] https://share.google/R4gCKvV7n7CUwZOIj

Kiberxavfsizlik xavfini moliyalashtirishning asosiy usuli shuki, kiberxavfsizlik sug‘urtasi, bu eng keng tarqalgan moliyalashtirish shakli maxsus kiberxavfsizlik sug‘urta polislaridir. Bu polislar ma’lumotlarning tarqalishi, ransomware (dastur-vymogateli) hujumlari, biznes faoliyatining uzilishi va boshqa kiberhodisalar natijasida yuzaga keladigan moliyaviy zararlarni qoplashga mo‘ljallangan.[7] Lekin kiber sug‘urta bozoriga chiqishdan oldin tashkilotning kiber tayyorgarligini baholash va maslahat berish, zarur ma’lumotlarni aniqlash va qayta ishlash orqali sifatli risk o‘tkazish yechimlarini ta’minlash kerak bo’ladi. Aonning risklarni boshqarish modeli, ya’ni aniqlash, baholash, yumshatish, o‘tkazish va tiklash, har qanday bosqichda kiber barqarorlikni ta’minlash, sug‘urta shartlarini yaxshilash va biznesning uzluksizligini ta’minlash uchun qo‘llanilishi mumkin.[8]

Sug‘urta turlariga keladigan bo’lsak, bular:

- ✓ Shaxsiy zararlar sug‘urtasi: Tashkilotni to‘g‘ridan-to‘g‘ri zararlaridan himoya qiladi.
- ✓ Ma’lumotlar oqib chiqishi va xabardor qilish xarajatlari
- ✓ Biznes faoliyatining uzilishidan kelib chiqqan zararlar
- ✓ Raqamli aktivlarni tiklash
- ✓ Kiber-vymogateli to‘lovlari
- ✓ Uchinchi tomon oldidagi javobgarlik sug‘urtasi: Uchinchi tomonning da’volaridan himoya qiladi.
- ✓ Maxfiylikni buzganlik uchun javobgarlik
- ✓ Tarmoq xavfsizligi bo‘yicha javobgarlik
- ✓ OAV bilan bog‘liq javobgarlik
- ✓ Regulyator organlar oldidagi himoya xarajatlar

Biroq, ko‘plab tashkilotlar sug‘urta da’volarini amalga oshirishda qiyinchiliklarga duch keladi. Redditdagi bir IT-mutaxassis shunday yozgan edi: «Mening bir nechta mijozlarim kiberxavfsizlik sug‘urtasiga ega edi, xavfsizligi yetarlicha bo‘lmagan tizim natijasida zarar uchun da’vo qilganlar, lekin menga qarshi tavsiyalarga qaramay, polising yangilanishi rad etildi». Bu sug‘urta siyosatining talablarini tushunish va belgilangan xavfsizlik choralarini qo‘llashning muhimligini ko‘rsatadi.[9]

Hukumat shuningdek, kompaniyalarni kiber-xavfsizlik va kiber-xavfsizlikni sug'urtalashga sarmoya kiritishga da'vat etadi. O`zbekiston va xorijiy davlatlar tajribasini koradigan bolsak

Tajriba jihat	**Xorijiy tajriba (Global)**	**O‘zbekiston tajribasi**
Kiberxavf transferi tushunchasi	Kiberxavflarni sug‘urta asosida moliyaviy transfer qilish risklarni qisman sug‘urta kompaniyasiga o‘tkazishdir — bu birinchi va uchinchi tomon yo‘qotishlarini qamrab oladi. munichre.com+1	O‘zbekiston bozorida hozircha **maxsus kibersug‘urta mahsulotlari** keng taklif qilinayotgani haqida rasmiy ma’lumotlar cheklangan. Sug‘urta bozorida umumiy raqamlashtirish yo‘nalishlari rivojlanmoqda, ammo kiberxavf sug‘urtasi o‘ziga xos mahsulot sifatida hali keng tatbiq etilgan emas. Sci-P
Asosiy qoplama	➢ **First-party coverage**: ma’lumot yo‘qolishi, biznes	Maxsus kibersug‘urta mahsulotlari shakllanmagan, shuning uchun

[7] Источник: TechTarget. https://share.google/EAjumSj5zy5cd9gKo
[8] https://share.google/ZL3WRqTmo3HNVeBwB
[9] https://share.google/R4gCKvV7n7CUwZOIj

turlari	to‘xtashi, tiklash xarajatlari. Allianz Commercial ➢ **Third-party liability**: uchinchi tomon da’volari, qonuniy jarimalar. Silverfort	hozircha bank va korxonalarda kiberxavfsizlik uchun sug‘urta qoplamalari an’anaviy sug‘urta shakllari doirasida integratsiya qilinayotgan bo‘lishi mumkin (masalan, mulk, operatsion sug‘urta). Ayni mahsulotlar bo‘yicha ochiq statistik axborot cheklangan. Sci-P
Bozor holati va penetratsiya	Kiber sug‘urta bozori jadal o‘smoqda; global sug‘urta mukofotlari milliardlab dollarni tashkil etadi va talab ortmoqda, lekin bozor penetratsiyasi past bo‘lib, katta yo‘qotishlar uchun davlat-xususiy sherikliklar taklif qilinmoqda. S&P Global+1	O‘zbek sug‘urta bozorida raqamlashtirish, sug‘urta xizmatlari sichqoncha, kredit sug‘urtasi kabi mahsulotlar mavjud, kibersug‘urta — yangi yo‘nalish. Bozor ishlab chiqilishi davom etmoqda va InsurTech/RegTech integratsiyasi bosqichlaridan o‘tmoqda. Cyber Law
Risk baholash va anderrayting	Anderrayting jarayonlari texnologik risklar, qarshi choralar, IT infratuzilma holati asosida amalga oshiriladi; AI va katta ma’lumotlar tahlili keng qo‘llanadi. ENISA	O‘zbekiston rasmiy statistika bo‘yicha kiber risklar bo‘yicha maxsus anderrayting platformalari faol ishlayotgani haqida ochiq ma’lumot yo‘q, shu bois risklarni baholash ko‘proq korxona darajasida ichki tahlil orqali amalga oshiriladi va davlat sug‘urta tartiblari sug‘urta kompaniyalari bilan muvofiq.
Ishchi mexanizmlar (Detekt/ Response)	Ko‘p sug‘urtachilar pre-breach xizmatlari (IT forensics, hodisaga javob, risk maslahatlari) bilan birga taklif etadi. Allianz Commercial	O‘zbekistonda **UZCERT** kabi milliy kibertahdidlarga chora ko‘rish markazi mavjud bo‘lib, hodisalarni aniqlash va sohalararo tajriba almashadi, lekin sug‘urta bilan to‘g‘ridan-to‘g‘ri integratsiya hujjatlashtirilgani mavjud emas. UZCERT xizmati
Regulyativ muhit va standartlar	Xalqaro standartlar va qonunchilik orqali kiberxavfsizlik hamda sug‘urta talablarida barqaror yondashuvlar mavjud (masalan, IAIS tavsiyalari). IAIS	O‘zbekiston “Sug’urta faoliyati to‘g‘risida”gi qonunga ega, lekin kibersug‘urta bo‘yicha maxsus me’yorlar hali to‘liq shakllanmayapti; milliy cyber security qonunchiligi ham rivojlanmoqda. Cyber Law
Davlat roli va hamkorlik	Ba’zi davlatlar kiberxavflarni sug‘urtalash bo‘yicha davlat-xususiy sherikliklar yaratmoqda (masalan, ekstremal voqealar uchun shtat kafolati). Financial Times	O‘zbekiston xalqaro kibermaydon hamkorligi va standartlarga moslashish bo‘yicha faol ishtirok etmoqda, lekin davlat tomonidan maxsus kiber sug‘urta mahsuloti qo‘llab-quvvatlanayotgani to‘g‘risida rasmiy ma’lumot kam. CBU

Kiberxavfsizlik xavflarini moliyalashtirish (Cyber Risk Transfer) va sug'urta qoplamalarini boshqarishda ayrim muammolarni ko'rishimiz mumkin:

1. Kiberxavflarni aniq baholashdagi qiyinchiliklar

Tashkilotlar kiber tahdidlarning real ehtimoli va potentsial moliyaviy zararini aniqlashda qiyinchilikka duch keladi. Chunki kiberhujumlar doimiy o‘zgarib boradi va zarar hajmini oldindan prognoz qilish juda murakkab.

2. Kiber sug‘urta polislarining murakkabligi va cheklovlari

Sug‘urta qoplamalari ko‘pincha murakkab bo‘ladi, shartlar ko‘p, istisnolar keng. Natijada ko‘plab tashkilotlar voqea sodir bo‘lganda da’vo qila olmay qoladi yoki sug‘urta kompaniyalari talab bilan bog‘liq rad javobini beradi.

3. Tashkilotlarning yetarli kiber tayyorgarlikka ega emasligi

Kiber sug‘urta kompaniyalari qoplama berishdan oldin kuchli xavfsizlik siyosatini talab qiladi. Ko‘plab tashkilotlarda esa minimal xavfsizlik protokollari mavjud bo‘lib, bu sug‘urtadan foydalanishni qiyinlashtiradi.

4. Kiber sug‘urta bozoridagi narxlarning oshib borishi

Kiberhujumlar, ayniqsa ransomware hujumlari soni ortgani sababli sug‘urta mukofotlari yildan yilga oshmoqda. Bu kichik va o‘rta bizneslar uchun kiber sug‘urtani moliyaviy jihatdan qiyinlashtiradi.

5. Kiber hodisalar zanjirining murakkabligi va javobgarlik masalalari

Hujumlar ko‘pincha uchinchi tomon xizmatlari, yetkazib beruvchilar yoki bulut platformalari orqali sodir bo‘ladi. Bu esa kim javobgar ekani, zarar kim zimmasiga tushishini aniqlashda katta huquqiy muammolarni keltirib chiqaradi.

Muammolarni bartaraf etish uchun quyidagi takliflarni berishim mumkin:

1. Sun’iy intellekt asosida kiberxavf baholash tizimini joriy etish

Sun’iy intellekt va mashinaviy o‘rganish algoritmlaridan foydalanish orqali kiber tahdidlarni avtomatik tahlil qilish, anomaliyalarni real vaqt rejimida aniqlash va xavf ehtimolini aniq prognozlash mumkin bo‘ladi. Bu usul an’anaviy baholashdan farqli o‘laroq, o‘zgaruvchan kiber tahdidlar sharoitida aniqlikni oshiradi.

2. Kiber sug‘urta polislarini standartlashtirish bo‘yicha me’yoriy bazani yaratish

Kiber sug‘urta shartnomalaridagi terminlar, qamrov doiralari va istisnolarni yagona standartga solish sug‘urta jarayonida aniqlik, shaffoflik va barqarorlikni ta’minlaydi. Bu korxonalarga qaysi risklar qoplanishini yaxshi tushunishga, sug‘urtalovchilarga esa riskni to‘g‘ri baholashga yordam beradi.

3. Tashkilotlarda Zero-Trust Architecture (ZTA) va kiber gigiyena standartlarini joriy etish

Zero-Trust modeli har qanday foydalanuvchi yoki qurilmani ishonchsiz deb hisoblagan holda doimiy tekshiruvni talab qiladi. Bu tizimni muntazam audit, xodimlar uchun majburiy kiber treninglar va ma’lumotlarni zaxiralash bilan birga qo‘llash kompaniyalarning xavfsizlik darajasini sezilarli oshiradi va sug‘urta talablari bilan moslashishini ta’minlaydi.

4. Kiber xavf kafolat fondini (Cyber Risk Guarantee Fund) tashkil etish

Davlat va xususiy sektor hamkorligida yaratiladigan bunday fond sug‘urta kompaniyalariga katta kiber hodisalar bo‘lganda qayta moliyalashtirish imkonini beradi. Natijada sug‘urta mukofotlarining keskin oshib borishining oldi olinadi, bozor barqarorligi ta’minlanadi va kichik bizneslar uchun ham sug‘urta yanada arzonlashadi.

5. Ko‘p tomonlama javobgarlik mexanizmini ishlab chiqish

Kiber hodisalarda ko‘pincha bir nechta subyekt — xizmat ko‘rsatuvchilar, bulut provayderlari, yetkazib beruvchilar, ichki xodimlar ishtirok etadi. Shu sababli huquqiy tartibotlarda ushbu subyektlar javobgarligini aniq taqsimlaydigan, zararni qaysi tomon qoplashini belgilaydigan ko‘p tomonlama mexanizm ishlab chiqish zararlarni tez va adolatli qoplashga imkon beradi.

Shularning barchasidan kelib chiqqan holda quyidagi xulosani berishimiz mumkinki:

Kiberxavfsizlik tahdidlari bizneslar uchun katta moliyaviy va operatsion xavf tug‘diradi. Kiber risklarni moliyalashtirish va o‘tkazish (Cyber Risk Transfer) strategiyalari bu xavflarni tashqi tomonga, ko‘pincha kiber sug‘urta vositalari orqali o‘tkazishga imkon beradi. Sug‘urta qoplamalari esa quyidagilarni ta’minlaydi:

- ✓ kiber hodisalar natijasidagi moliyaviy zararlarni qoplash,
- ✓ biznesning uzluksiz faoliyatini ta’minlash,
- ✓ ma’lumotlar buzilishi, ransomware yoki boshqa kiber hodisalardan keladigan operatsion va reputatsion xavflarni kamaytirish,
- ✓ regulatorlar va qonunchilik talablariga rioya qilish orqali jarimalar va moliyaviy yo‘qotishlardan himoya qilish.

Shuningdek, kiber risklarni o‘tkazish strategiyasi tashkilotlarga xavfni baholash, tayyorgarlikni oshirish, alternativ risk transfer vositalarini qo‘llash va global kapital resurslariga kirish imkonini beradi. Shu tarzda, kiber risklarni moliyalashtirish va sug‘urta qoplamalarini boshqarish tashkilotlarni moliyaviy va operatsion jihatdan barqaror qilishning muhim vositasi hisoblanadi.

XULOSA

Kiberxavfsizlik xavflarini moliyalashtirish va sug‘urta qoplamalarini boshqarish zamonaviy biznes uchun strategik ahamiyatga ega. Kiber risklarni o‘tkazish (Cyber Risk Transfer) tashkilotlarga moliyaviy yo‘qotishlarni kamaytirish, biznesning uzluksizligini ta’minlash va qonuniy talablarga moslashish imkonini beradi.

Global tajriba kiber sug‘urta bozorining rivojlanganligini ko‘rsatsa, O‘zbekistonda bu soha hali bosqichma-bosqich rivojlanmoqda. Muammolarni hal qilish uchun quyidagi choralar samarali bo‘lishi mumkin:

1. Sun’iy intellekt asosida risk baholash tizimlarini joriy etish.

2. Kiber sug‘urta polislarini standartlashtirish.

3. Zero-Trust Architecture va kiber gigiyena standartlarini keng joriy etish.

4. Kiber xavf kafolat fondini tashkil etish.

5. Ko‘p tomonlama javobgarlik mexanizmlari ishlab chiqish.

Kiber risklarni moliyalashtirish nafaqat himoya vositasi, balki tashkilotlarning raqobatbardoshligi va barqaror rivojlanishini ta’minlovchi strategik instrument sifatida qaralishi lozim.

FOYDALANILGAN ADABIYOTLAR:

1.Kiber-xavfsizlikni sug'urtalash: ortiqcha hashamdorlik yo'q

https://share.google/pYrQ30vrOI0RiJrLi

2.Источник: TechTarget. https://share.google/EAjumSj5zy5cd9gKo

3.Transfer Cyber Risks - Cyber Loop - Aon

https://share.google/ZL3WRqTmo3HNVeBwB

4.Источник: LinkedIn. https://share.google/eGawy3DEh1FyOic1n

5. Uralov, B. (2024). Soliq imtiyozlarini nazariy asoslash va huquqiy tartibga solish. YASHIL IQTISODIYOT VA TARAQQIYOT, 2(1).

6.Источник: 6clicks. https://share.google/Ha08CwC8YWrOgDxwY

7.Источник: Cyber Sierra. https://share.google/R4gCKvV7n7CUwZOIj

Ilyos, A., & Uralov, B. Investment Strategy as a Factor of Innovation in Uzbekistan. JournalNX, 453-456.

8.Источник: LEX.UZ. https://share.google/hMGUuTJqgVfvZLSes

9. Жавманов, Ж. А., Уралов, Б. М., Очилова, М. Т., & Файзуллаев, У. Х. (2024). Налогообложение индивидуальных предпринимателей как форма государственного регулирования самозанятости. So ‘ngi ilmiy tadqiqotlar nazariyasi, 7(1), 369-378.