

**FINTECH KOMPANIYALARI VA RAQAMLI BANK XIZMATLARIDA
KIBERXAVFSIZLIK TAVAKKALINI BAHOLASHNING STATISTIK-HUQUQIY
ASOSLARI**

Shakirova Nigora Axralovna

Tashkent State University of Economics PhD, Associate Professor

Department of Economic statistics

E-mail: shakirova0130@gmail.com

Orcid: [0009-0006-5025-4764](https://orcid.org/0009-0006-5025-4764)

Tugalov Elshod Zafar o'g'li

Toshkent davlat iqtisodiyot universiteti Moliya fakulteti 2-kurs talabasi

E-mail: elshodbekt7@gmail.com

ORCID: 0009-0001-1658-4165

Annotatsiya

Ushbu maqolada fintech-kompaniyalari va raqamli bank xizmatlarida yuzaga keladigan kiberxavfsizlik tavakkalini baholashning statistik-huquqiy asoslari tahlil qilinadi. Kiberhodisalarning chastotasi va zarar hajmini baholovchi statistik ko'rsatkichlar, ekstremal qiymatlar nazariyasi (Extreme Value Theory) asosidagi modellar, operatsion tavakkal doirasidagi zarar taqsimoti yondashuvi (Loss Distribution Approach) hamda kiberxavfsizlik bo'yicha tavakkal ostidagi qiymat (CyVaR) tushunchasining nazariy mohiyati yoritilgan. Shuningdek, xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework, PCI DSS, Bazil operatsion tavakkal talablari) va O'zbekiston milliy qonunchiligi (kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilish to'g'risidagi qonunlar) o'rtasidagi uzviy bog'liqlik ko'rib chiqilgan. Tadqiqot natijalariga ko'ra, statistik-miqdoriy baholash usullari bilan huquqiy tartibga solish mexanizmlarini birgalikda qo'llash moliya sektorida kiberxavfsizlik darajasini oshirishning eng samarali yo'li hisoblanadi.

Kalit so'zlar: kiberxavfsizlik, fintech, raqamli bank xizmatlari, operatsion tavakkal, statistik indikatorlar, tavakkal ostidagi qiymat (CyVaR), zarar taqsimoti yondashuvi, ISO/IEC 27001, shaxsiy ma'lumotlar himoyasi.

**СТАТИСТИКО-ПРАВОВЫЕ ОСНОВЫ ОЦЕНКИ РИСКА
КИБЕРБЕЗОПАСНОСТИ В FINTECH-КОМПАНИЯХ И ЦИФРОВЫХ
БАНКОВСКИХ УСЛУГАХ**

Аннотация

В данной статье анализируются статистико-правовые основы оценки риска кибербезопасности, возникающего в деятельности финтех-компаний и цифровых банковских услуг. Рассмотрены статистические показатели частоты и величины ущерба от киберинцидентов, модели на основе теории экстремальных значений (Extreme Value Theory), подход распределения убытков (Loss Distribution Approach) в рамках операционного риска, а также теоретическая сущность понятия стоимости под риском кибербезопасности (CyVaR). Также рассмотрена взаимосвязь между международными стандартами (ISO/IEC 27001, NIST Cybersecurity Framework, PCI DSS, требования Базельского комитета к операционному риску) и национальным законодательством Узбекистана в сфере кибербезопасности и защиты персональных данных. Результаты исследования показывают, что совместное применение статистико-количественных методов оценки и механизмов правового регулирования является наиболее эффективным путём повышения уровня кибербезопасности в финансовом секторе.

Ключевые слова: кибербезопасность, финтех, цифровые банковские услуги, операционный риск, статистические индикаторы, стоимость под риском (CyVaR), подход распределения убытков, ISO/IEC 27001, защита персональных данных.

**STATISTICAL AND LEGAL FOUNDATIONS FOR ASSESSING
CYBERSECURITY RISK IN FINTECH COMPANIES AND DIGITAL BANKING
SERVICES**

Abstract

This article analyzes the statistical and legal foundations for assessing cybersecurity risk arising in the activities of fintech companies and digital banking services. It examines statistical indicators of the frequency and severity of cyber incidents, models based on Extreme Value Theory, the Loss Distribution Approach within the framework of operational risk, and the theoretical essence of the concept of Cyber Value-at-Risk (CyVaR). The article also considers the close relationship between international standards (ISO/IEC 27001, the NIST Cybersecurity Framework, PCI DSS, and the Basel Committee's operational risk requirements) and Uzbekistan's national legislation on cybersecurity and personal data protection. The findings indicate that the combined application of statistical-quantitative assessment methods and legal regulatory mechanisms is the most effective way to strengthen the level of cybersecurity in the financial sector.

Keywords: *cybersecurity, fintech, digital banking services, operational risk, statistical indicators, Cyber Value-at-Risk (CyVaR), loss distribution approach, ISO/IEC 27001, personal data protection.*

Kirish

Moliya sektorining raqamlashtirilishi mobil bank ilovalari, internet-banking tizimlari, fintech-platformalar va bulutli hisoblash texnologiyalarining keng tarqalishiga olib kelmoqda. Ushbu jarayon moliyaviy xizmatlarga kirish imkoniyatlarini kengaytirish va operatsion xarajatlarni kamaytirish bilan bir qatorda, yangi turdagi tavakkalchilik — kiberxavfsizlik tavakkalini ham keskin kuchaytirmoqda. Kiberhujumlar, ma'lumotlar sizib chiqishi, to'lov tizimlaridagi firibgarlik va xizmat ko'rsatishni rad etish (DDoS) hujumlari nafaqat alohida moliya institutiga, balki butun moliya tizimining barqarorligiga tahdid solishi mumkin.

Kiberxavfsizlik tavakkalining o'ziga xos xususiyati shundaki, u boshqa moliyaviy tavakkal turlaridan farqli o'laroq, statistik jihatdan yuqori darajadagi noaniqlik va "og'ir dum" (heavy-tail) xususiyatiga ega taqsimotlar bilan tavsiflanadi: ko'pchilik hodisalar nisbatan kichik zarar keltiradi, ammo kamdan-kam uchraydigan yirik kiberhujumlar favqulodda katta moliyaviy va obro' yo'qotishlarga olib kelishi mumkin. Shu sababli an'anaviy statistik usullar bilan bir qatorda, ekstremal hodisalarni baholashga ixtisoslashgan maxsus statistik-matematik vositalarni qo'llash zarurati yuzaga keladi.

Bundan tashqari, kiberxavfsizlik tavakkali faqat texnik yoki statistik muammo bo'lib qolmasdan, chuqur huquqiy tartibga solishni ham talab qiladi. Shaxsiy ma'lumotlarni himoya qilish, axborot xavfsizligi insidentlari to'g'risida xabar berish majburiyati, operatsion barqarorlikka qo'yiladigan me'yoriy talablar kabi masalalar statistik baholash tizimi bilan uzviy bog'liq holda rivojlanishi lozim. Xalqaro amaliyotda ISO/IEC 27001, NIST Cybersecurity Framework kabi standartlar hamda Bazel qo'mitasining operatsion barqarorlik bo'yicha tamoyillari aynan shu ikki yo'nalishning — statistik baholash va huquqiy tartibga solishning — uyg'unlashuviga asoslangan.

O'zbekistonda so'nggi yillarda "Kiberxavfsizlik to'g'risida"gi va "Shaxsiy ma'lumotlar to'g'risida"gi qonunlarning qabul qilinishi, shuningdek Markaziy bank tomonidan axborot xavfsizligiga qo'yiladigan talablarning kuchaytirilishi ushbu sohada institutsional islohotlarning boshlanganidan dalolat beradi. Biroq kiberxavfsizlik tavakkalini miqdoriy baholashning yagona milliy metodologiyasi va statistik ma'lumotlar bazasi hali to'liq shakllanmagan, bu esa mazkur tadqiqot mavzusining dolzarbligini belgilaydi.

Tadqiqotning maqsadi — fintech-kompaniyalari va raqamli bank xizmatlarida kiberxavfsizlik tavakkalini baholashda qo'llaniladigan asosiy statistik indikatorlar va

modellarning nazariy mohiyatini ochib berish, ularni xalqaro huquqiy-me'yoriy talablar bilan bog'lagan holda tahlil qilish hamda O'zbekiston moliya bozori uchun statistik-huquqiy baholash tizimini takomillashtirish bo'yicha ilmiy asoslangan takliflar ishlab chiqishdan iborat.

Adabiyotlar sharhi

Kiberxavfsizlik tavakkalini iqtisodiy-statistik jihatdan baholash muammosi so'nggi o'n-o'n besh yil ichida xorijiy ilmiy adabiyotda faol o'rganilmoqda. M. Eling va J. Wirfs o'zlarining tadqiqotlarida kiberhodisalar natijasida yuzaga keladigan real moliyaviy zararlarni empirik tahlil qilib, kiberyo'qotishlar taqsimoti an'anaviy operatsion tavakkal hodisalariga nisbatan sezilarli darajada "og'ir dum"ga ega ekanligini, ya'ni ekstremal yirik zararlar ehtimoli yuqoriroq bo'lishini isbotlaganlar [1].

C. Biener, M. Eling va J.H. Wirfs kiberxavfsizlik tavakkalining sug'urtalanish imkoniyatlarini o'rganib, ushbu tavakkal turining klassik sug'urta nazariyasi talablariga (statistik mustaqillik, ma'lumotlarning yetarliligi) to'liq javob bermasligini, shu sababli maxsus aktuar-statistik yondashuvlar zarurligini asoslab berganlar [2].

Amerika Qo'shma Shtatlarining Milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan Kiberxavfsizlik asosiy tizimi (Cybersecurity Framework) tashkilotlarda kiberxavfsizlikni boshqarishning besh bosqichli (aniqlash, himoya qilish, aniqlash, javob berish, tiklash) uslubiy modelini taklif etadi, bu model kiberxavfsizlik indikatorlarini tizimli tarzda shakllantirish uchun keng qo'llaniladigan asos hisoblanadi [3].

Xalqaro standartlashtirish tashkiloti tomonidan ishlab chiqilgan ISO/IEC 27001 standarti axborot xavfsizligini boshqarish tizimiga qo'yiladigan talablarni belgilab, tashkilotlarda tavakkalni baholash, nazorat mexanizmlarini joriy etish va doimiy monitoring olib borish tartib-qoidalarini tavsiya etadi [4]. Bazel bank nazorati qo'mitasi esa operatsion barqarorlik bo'yicha tamoyillarida banklarning kiberxavfsizlik tavakkalini operatsion tavakkal tarkibiy qismi sifatida baholashi va tegishli kapital zaxiralarini shakllantirishi zarurligini belgilagan [5].

O'zbekistonda kiberxavfsizlik va raqamli moliyaviy xizmatlar mavzusi R. Rahimov [6] va N. Tosheva [7] kabi mahalliy tadqiqotchilar tomonidan qisman o'rganilgan bo'lib, ularning ishlarida asosan huquqiy tartibga solish va shaxsiy ma'lumotlarni himoya qilish masalalariga urg'u berilgan. Biroq kiberxavfsizlik tavakkalini statistik-miqdoriy baholash, xususan ekstremal qiymatlar nazariyasi va zarar taqsimoti yondashuvini milliy moliya bozori ma'lumotlari asosida qo'llash masalalari hozirgacha yetarli darajada ilmiy tadqiq etilmagan, bu esa mazkur tadqiqotning ilmiy yangiligini belgilaydi.

Tadqiqot metodologiyasi

Tadqiqot jarayonida ilmiy bilishning umumnazariy va maxsus usullaridan kompleks tarzda foydalanildi. Mavzuga oid xorijiy va mahalliy ilmiy adabiyotlarni tizimlashtirish uchun mantiqiy tahlil va sintez usuli qo‘llanildi. Kiberxavfsizlik tavakkalini statistik baholash usullarining matematik mohiyatini ochib berishda statistik-matematik modellashtirish usulidan foydalanildi, jumladan hodisalar chastotasi va zarar hajmini modellashtirish (frequency-severity), ekstremal qiymatlar nazariyasi hamda tavakkal ostidagi qiymat (VaR/CyVaR) hisoblash yondashuvlari qiyosiy tarzda yoritildi. Xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework, Bazel operatsion barqarorlik tamoyillari) hamda O‘zbekiston Respublikasining kiberxavfsizlik va shaxsiy ma’lumotlarni himoya qilish sohasidagi qonunchiligi tahlili asosida normativ-huquqiy tahlil metodidan foydalanildi. Tadqiqot yakunida xalqaro tajribadan kelib chiqqan holda induktiv-deduktiv mantiqiy xulosalash usuli orqali milliy moliya bozori uchun amaliy tavsiyalar shakllantirildi.

Tahlil va natijalar muhokamasi

Fintech-kompaniyalari va raqamli bank xizmatlarida kiberxavfsizlik tavakkalini baholashda qo‘llaniladigan statistik indikatorlarni ularning vazifasiga ko‘ra shartli ravishda to‘rt guruhga ajratish mumkin: hodisalar chastotasi ko‘rsatkichlari, zarar hajmi (severity) ko‘rsatkichlari, agregatlangan tavakkal ko‘rsatkichlari va nazorat yetukligi (maturity) ko‘rsatkichlari.

1-jadval.

Kiberxavfsizlik tavakkalini baholashning asosiy statistik indikatorlari [3]

Indikator guruhi	Asosiy ko‘rsatkichlar	Vazifasi	Qo‘llanish sohasi
Chastota ko‘rsatkichlari	Yiliga ro‘y beradigan insidentlar soni, hujum turlari bo‘yicha taqsimot	Kiberhodisalarning yuzaga kelish ehtimolini baholaydi	Tavakkal xaritasini shakllantirish
Zarar hajmi ko‘rsatkichlari	O‘rtacha va median zarar, zararining standart og‘ishi	Har bir hodisadan kelib chiqadigan moliyaviy yo‘qotish miqyosini o‘lchaydi	Sug‘urta va zaxira kapitalini rejalashtirish
Agregatlangan tavakkal ko‘rsatkichlari	Kiberxavfsizlik bo‘yicha tavakkal ostidagi qiymat (CyVaR), kutilgan yo‘qotish	Belgilangan ishonch darajasida umumiy mumkin bo‘lgan zararni baholaydi	Kapital yetarliligini va limitlarni belgilash

Indikator guruhi	Asosiy ko‘rsatkichlar	Vazifasi	Qo‘llanish sohasi
Nazorat yetukligi ko‘rsatkichlari	Xavfsizlik nazorati indeksi, insidentga javob berish vaqti (MTTR)	Tashkilotning kiberxavfsizlik tayyorligini baholaydi	Ichki audit va tartibga solish nazorati

Chastota ko‘rsatkichlari kiberhodisalarning vaqt birligida necha marta ro‘y berishini statistik jihatdan tavsiflab, ular ko‘pincha Puasson yoki manfiy binomial taqsimot asosida modellashiriladi. Zarar hajmi ko‘rsatkichlari esa har bir alohida hodisadan kelib chiqadigan moliyaviy yo‘qotish miqdorini tavsiflaydi va, yuqorida qayd etilganidek, odatda log-normal yoki umumlashtirilgan Pareto kabi “og‘ir dum”li taqsimotlarga yaqinroq bo‘ladi. Ushbu ikki tavsifni birlashtirish orqali kiberxavfsizlik tavakkalini kompleks baholashning asosiy uslubiy yondashuvi — zarar taqsimoti yondashuvi (Loss Distribution Approach, LDA) shakllanadi.

Zarar taqsimoti yondashuviga ko‘ra, ma’lum davr (masalan, bir yil) mobaynidagi umumiy kiberzarar tasodifiy sondagi hodisalar zararlarining yig‘indisi sifatida modellashiriladi: hodisalar soni chastota taqsimoti orqali, har bir hodisaning zarar hajmi esa alohida severity taqsimoti orqali ifodalanadi, so‘ngra ikkala taqsimot Monte-Karlo simulyatsiyasi yordamida birlashtiriladi. Natijada olingan umumiy zarar taqsimoti asosida kiberxavfsizlik bo‘yicha tavakkal ostidagi qiymat (CyVaR) — belgilangan ishonch darajasida (masalan, 99%) yil davomida yuzaga kelishi mumkin bo‘lgan maksimal zarar miqdori — hisoblab chiqiladi.

2-jadval.

Zarar taqsimoti yondashuvi (Loss Distribution Approach) tarkibiy qismlari [2]

Tarkibiy qism	Qisqacha tavsifi	Odatiy qo‘llaniladigan modellar
Chastota modeli	Ma’lum davrda ro‘y beradigan kiberhodisalar sonini tavsiflaydi	Puasson taqsimoti, manfiy binomial taqsimot
Zarar hajmi (severity) modeli	Har bir alohida hodisadan kelib chiqadigan moliyaviy yo‘qotishni tavsiflaydi	Log-normal taqsimot, umumlashtirilgan Pareto taqsimoti (Extreme Value Theory)
Agregatlash bosqichi	Chastota va zarar hajmi modellarini birlashtirib, umumiy	Monte-Karlo simulyatsiyasi, Fast Fourier Transform usuli

Tarkibiy qism	Qisqacha tavsifi	Odatiy qo‘llaniladigan modellar
	yillik zarar taqsimotini shakllantiradi	

Ekstremal qiymatlar nazariyasi (Extreme Value Theory, EVT) kiberxavfsizlik tavakkalini baholashda alohida ahamiyatga ega, chunki u aynan taqsimotning “dum” qismidagi, ya’ni kamdan-kam uchraydigan, ammo favqulodda katta zararli hodisalarni statistik jihatdan aniqroq tavsiflash imkonini beradi. Umumlashtirilgan Pareto taqsimoti yordamida ma’lum chegara qiymatidan yuqori zararlarning ehtimoliy xususiyatlari alohida modellashtiriladi, bu esa an’anaviy normal taqsimotga asoslangan usullarga nisbatan yirik kiberhujumlar xavfini yanada real baholash imkonini yaratadi.

Statistik baholash tizimi o‘z-o‘zidan yetarli emas — u xalqaro va milliy huquqiy-me’yoriy talablar bilan uzviy bog‘langan holdagina samarali natija beradi. Quyidagi jadvalda kiberxavfsizlik sohasidagi asosiy xalqaro standartlar va ularning statistik-miqdoriy talablarga bog‘liqligi umumlashtirilgan.

3-jadval.

Kiberxavfsizlik sohasidagi xalqaro standartlarning statistik-huquqiy talablari [5]

Standart / hujjat	Asosiy yo‘nalishi	Statistik-miqdoriy talabi
ISO/IEC 27001	Axborot xavfsizligini boshqarish tizimi	Tavakkalni baholash reestri, insidentlar statistikasini yuritish
NIST Cybersecurity Framework	Kiberxavfsizlikni boshqarishning besh bosqichli modeli	Nazorat yetukligi indeksleri, javob berish vaqti ko‘rsatkichlari
PCI DSS	To‘lov kartalari ma’lumotlarini himoya qilish	Firibgarlik operatsiyalari chastotasi va zarar hajmi monitoringi
Bazel operatsion barqarorlik tamoyillari	Bank operatsion tavakkalini boshqarish	Zarar taqsimoti yondashuvi (LDA) asosida kapital zaxirasini hisoblash

Jadvaldan ko‘rinib turibdiki, xalqaro standartlarning barchasi, u yoki bu darajada, kiberxavfsizlik holatini statistik ko‘rsatkichlar orqali muntazam o‘lchab borishni talab qiladi. Bu, o‘z navbatida, milliy darajada yagona insidentlar reestri va statistik hisobot tizimini yaratish zaruriyatini keltirib chiqaradi. O‘zbekistonda “Kiberxavfsizlik to‘g‘risida”gi qonun

[8] va shaxsiy ma’lumotlarni himoya qilish to‘g‘risidagi qonunchilik [9] kiberhodisalar to‘g‘risida xabar berish majburiyatini umumiy tarzda belgilagan bo‘lsa-da, insidentlarni yagona statistik bazada tizimli to‘plash va tahlil qilish mexanizmi hali to‘liq shakllanmagan.

4-jadval.

Kiberxavfsizlik tavakkalini statistik-huquqiy baholash tizimini O‘zbekistonda joriy etishning institutsional shartlari [10]

Shart-sharoit	Hozirgi holat	Yaxshilash yo‘nalishi
Insidentlar bo‘yicha yagona statistik baza	Kiberhodisalar to‘g‘risidagi ma’lumotlar tarqoq holda, tizimlashtirilmagan	Markaziy bank yoki kiberxavfsizlik agentligi huzurida yagona insidentlar reestrini yaratish
Majburiy hisobot berish me‘yorlari	Xabar berish majburiyati umumiy tarzda belgilangan, ammo statistik shakl va muddatlar aniq emas	Insidentlar to‘g‘risida standartlashtirilgan statistik hisobot shakllarini joriy etish
Kadrlar salohiyati	Kiber-tavakkalni aktuar-statistik baholay oladigan mutaxassislar yetishmovchiligi	Oliy ta’lim muassasalarida kiber-risk analitikasi yo‘nalishini rivojlantirish
Huquqiy-me‘yoriy uyg‘unlik	Milliy qonunchilik xalqaro standartlar (ISO, NIST) bilan qisman uyg‘unlashtirilgan	Milliy me‘yoriy hujjatlarni ISO/IEC 27001 va Bazel talablariga muvofiqlashtirish

Yuqoridagi tahlildan ko‘rinib turibdiki, O‘zbekiston moliya bozorida kiberxavfsizlik tavakkalini statistik-huquqiy baholash tizimini rivojlantirishning asosiy sharti — bu faqat texnik vositalarni joriy etish emas, balki insidentlar to‘g‘risidagi ma’lumotlarni tizimli to‘plash, ularni yagona statistik metodologiya asosida tahlil qilish va bu jarayonni aniq huquqiy normalar bilan mustahkamlashdir. Bunday kompleks yondashuvsiz statistik modellarning (jumladan CyVaR va zarar taqsimoti yondashuvining) amaliy qo‘llanilishi ma’lumotlar yetishmovchiligi sababli cheklangan bo‘lib qoladi.

Xulosa

O‘tkazilgan tadqiqot fintech-kompaniyalari va raqamli bank xizmatlarida kiberxavfsizlik tavakkalini baholashda statistik-huquqiy yondashuvning uyg‘unlashuvi nafaqat nazariy, balki amaliy jihatdan ham muhim ekanligini ko‘rsatdi. Olingan natijalar asosida quyidagi yakuniy xulosalar shakllantirildi.

Birinchidan, kiberxavfsizlik tavakkali o‘zining “og‘ir dum” xususiyati bilan boshqa moliyaviy tavakkal turlaridan farqlanadi, shu sababli uni baholashda an‘anaviy statistik usullar bilan bir qatorda ekstremal qiymatlar nazariyasi va zarar taqsimoti yondashuvi kabi maxsus vositalarni qo‘llash zarur.

Ikkinchidan, kiberxavfsizlik bo‘yicha tavakkal ostidagi qiymat (CyVaR) ko‘rsatkichi bank va fintech institutlari uchun kapital zaxirasini va tavakkal limitlarini belgilashning istiqbolli vositasi hisoblanadi, biroq uning ishonchliligi hodisalar chastotasi va zarar hajmi bo‘yicha yetarli statistik ma‘lumotlar mavjudligiga bevosita bog‘liq.

Uchinchidan, xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework, Bazel operatsion barqarorlik tamoyillari) statistik baholash va huquqiy tartibga solishning uzviy bog‘liqligiga asoslangan bo‘lib, O‘zbekiston milliy amaliyotini ushbu standartlarga muvofiqlashtirish maqsadga muvofiqdir.

To‘rtinchidan, O‘zbekistonda kiberxavfsizlik tavakkalini statistik-huquqiy baholash tizimini rivojlantirish uchun, birinchi navbatda, insidentlar bo‘yicha yagona statistik baza yaratish, standartlashtirilgan hisobot shakllarini joriy etish va kiber-risk analitikasi bo‘yicha malakali kadrlar tayyorlashni yo‘lga qo‘yish zarur.

Yakuniy xulosa sifatida aytish mumkinki, statistik-miqdoriy baholash usullari bilan huquqiy tartibga solish mexanizmlarini birgalikda rivojlantirish O‘zbekiston moliya sektorida kiberxavfsizlik darajasini oshirish, fintech-ekotizimga bo‘lgan ishonchni mustahkamlash hamda raqamli moliyaviy barqarorlikni ta‘minlashning strategik ahamiyatga ega yo‘nalishlaridan biri bo‘lib qolmoqda.

Foydalanilgan adabiyotlar

1. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109–1119.
2. 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.
3. NIST (National Institute of Standards and Technology). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce (Gaithersburg, AQSH). <https://www.nist.gov/cyberframework>
4. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization (Geneva, Shveysariya).
5. Basel Committee on Banking Supervision. (2021). Principles for Operational Resilience. Bank for International Settlements (Bazel, Shveysariya). <https://www.bis.org>

6. Rahimov, R.O. (2023). O‘zbekiston bank tizimida kiberxavfsizlikni ta’minlashning huquqiy asoslari. O‘zbekiston yuridik jurnali.

7. Tosheva, N.B. (2024). Raqamli moliyaviy xizmatlarda shaxsiy ma’lumotlarni himoya qilish muammolari. Toshkent.

8. O‘zbekiston Respublikasi qonuni. (2022). “Kiberxavfsizlik to‘g‘risida”. O‘zbekiston qonunchilik bazasi (Toshkent). <https://lex.uz/uz/search/nat>

9. O‘zbekiston Respublikasi qonuni. (2019). “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonunga o‘zgartish va qo‘shimchalar kiritish haqida. O‘zbekiston qonunchilik bazasi (Toshkent). <https://lex.uz/uz/search/nat>

10. ENISA (European Union Agency for Cybersecurity). (2025). ENISA Threat Landscape Report. ENISA Publications (Afina, Gretsiya). <https://www.enisa.europa.eu>