

MUHANDISLIK

& IQTISODIYOT

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

№11

2025
noyabr



Milliy nashrlar

OAK: <https://oak.uz/pages/4802>

05.00.00 – Texnika fanlari

08.00.00 – Iqtisodiyot fanlar



Google Scholar

OPEN ACCESS

ULRICHSWEB[™]
GLOBAL SERIALS DIRECTORY

Academic
Resource
Index
ResearchBib

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INTERNATIONAL CENTRE

CYBERLENINKA

OpenAIRE

ROAD

INDEX COPERNICUS
INTERNATIONAL

BASE

Crossref

НАУЧНАЯ ЭЛЕКТРОННАЯ
БИБЛИОТЕКА
LIBRARY.RU



ISSN: 3060-463X

РЭУ.РФ
РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ Г.В. ПЛЕХАНОВА
ТАШКЕНТСКИЙ ФИЛИАЛ



muhandislik **& iqtisodiyot**

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

*Elektron nashr, 315 sahifa.
2025-yil, noyabr*

Bosh muharrir:

Zokirova Nodira Kalandarovna, iqtisodiyot fanlari doktori, DSc, professor

Bosh muharrir o'rinbosari:

Shakarov Zafar G'afarovich, iqtisodiyot fanlari bo'yicha falsafa doktori, PhD, dotsent

Tahrir hay'ati:

Abduraxmanov Kalandar Xodjayevich, O'z FA akademigi, iqtisodiyot fanlari doktori, professor

Sharipov Kongratbay Avezimbetovich, texnika fanlari doktori, professor

Maxkamov Baxtiyor Shuxratovich, iqtisodiyot fanlari doktori, professor

Abduraxmanova Gulnora Kalandarovna, iqtisodiyot fanlari doktori, professor

Shaumarov Said Sanatovich, texnika fanlari doktori, professor

Turayev Bahodir Xatamovich, iqtisodiyot fanlari doktori, professor

Nasimov Dilmurod Abdulloyevich, iqtisodiyot fanlari doktori, professor

Allayeva Gulchexra Jalgasovna, iqtisodiyot fanlari doktori, professor

Arabov Nurali Uralovich, iqtisodiyot fanlari doktori, professor

Maxmudov Odiljon Xolmirzayevich, iqtisodiyot fanlari doktori, professor

Xamrayeva Sayyora Nasimovna, iqtisodiyot fanlari doktori, professor

Bobonazarova Jamila Xolmurodovna, iqtisodiyot fanlari doktori, professor

Irmatova Aziza Baxromovna, iqtisodiyot fanlari doktori, professor

Bo'taboyev Mahammadjon To'ychiyevich, iqtisodiyot fanlari doktori, professor

Shamshiyeva Nargizaxon Nosirxuja kizi, iqtisodiyot fanlari doktori, professor,

Xolmuxamedov Muhsinjon Murodullayevich, iqtisodiyot fanlari nomzodi, dotsent

Xodjayeva Nodiraxon Abdurashidovna, iqtisodiyot fanlari nomzodi, dotsent

Amanov Otabek Amankulovich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent

Toxirov Jaloliddin Ochil o'g'li, texnika fanlari bo'yicha falsafa doktori (PhD)

Qurbonov Samandar Pulatovich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Zikriyoyev Aziz Sadulloyevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Tabayev Azamat Zaripbayevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Sxay Lana Aleksandrovna, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent

Ismoilova Gulnora Fayzullayevna, iqtisodiyot fanlari nomzodi, dotsent

Djumaniyazov Umrbek Ilxamovich, iqtisodiyot fanlari nomzodi, dotsent

Kasimova Nargiza Sabitdjanovna, iqtisodiyot fanlari nomzodi, dotsent

Kalanova Moxigul Baxritdinovna, dotsent

Ashurzoda Luiza Muxtarovna, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Sharipov Sardor Begmaxmat o'g'li, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Sharipov Botirali Roxataliyevich, iqtisodiyot fanlari nomzodi, professor

Tursunov Ulug'bek Sativoldiyevich, iqtisodiyot fanlari doktori (DSc), dotsent

Bauyetdinov Majit Janizaqovich, Toshkent davlat iqtisodiyot universiteti dotsenti, PhD

Botirov Bozorbek Musurmon o'g'li, Texnika fanlari bo'yicha falsafa doktori (PhD)

Sultonov Shavkatjon Abdullayevich, Kimyo fanlari doktori, (DSc)

Jo'raeva Malohat Muhammadovna, filologiya fanlari doktori (DSc), professor.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

- 05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
- 05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
- 05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
- 05.01.03 – Informatikaning nazariy asoslari
- 05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
- 05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
- 05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
- 05.01.07 – Matematik modellash
- 05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
- 05.02.00 – Mashinasozlik va mashinashunoslik
- 05.02.08 – Yer usti majmualari va uchish apparatlari
- 05.03.02 – Metrologiya va metrologiya ta'minoti
- 05.04.01 – Telekommunikatsiya va kompyuter tizimlari, telekommunikatsiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
- 05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
- 05.05.05 – Issiqlik texnikasining nazariy asoslari
- 05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
- 05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
- 05.08.03 – Temir yo'l transportini ishlatish
- 05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
- 05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
- 10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
- 10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
- 08.00.01 – Iqtisodiyot nazariyasi
- 08.00.02 – Makroiqtisodiyot
- 08.00.03 – Sanoat iqtisodiyoti
- 08.00.04 – Qishloq xo'jaligi iqtisodiyoti
- 08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
- 08.00.06 – Ekonometrika va statistika
- 08.00.07 – Moliya, pul muomalasi va kredit
- 08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
- 08.00.09 – Jahon iqtisodiyoti
- 08.00.10 – Demografiya. Mehnat iqtisodiyoti
- 08.00.11 – Marketing
- 08.00.12 – Mintaqaviy iqtisodiyot
- 08.00.13 – Menejment
- 08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
- 08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
- 08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
- 08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK

Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti



MUNDARIJA

JAHONDA KREATIV IQTISODIYOTNING RIVOJLANISHINING UMUMIY GLOBAL TENDENSIYALARI.....	12
Ismailov Azizbek Ruzimaxmatovich	
CHORVACHILIK MAHSULOTLARI ISHLAB CHIQUV VA EKSPORT SALOHİYATINI OSHIRISHDA BOZOR INFRATUZILMASINI RIVOJLANTIRISHNING IQTISODIY OMILLARI	22
Soxadaliyev Abdurashid Mamadaliyevich	
XORIJIY INVESTITSİYALAR VA IQTISODIY O'SISH O'RTASIDAGI O'ZARO TA'SIR	30
Madraximova Irodaxon Sherzodbek qizi	
O'ZBEKISTON SHAROITIDA XIZMATLAR EKSPORTINING IQTISODIY O'SISHGA TA'SIRI	35
Sultonov Shodiyor Abduxalilovich, Karshiyeva Charos Mamasoliyevna	
QASHQADARYO VILOYATIDA OLIY TA'LIM VA MEHNAT BOZORI INTEGRATSIYASI ASOSIDA YUQORI MALAKALI KADRLAR TAYYORLASHNING HOZIRGI HOLATI.....	41
Haqqulov Fazliddin Faxriddinovich	
SOLIQ MA'MURCHILIGIDA XALQARO TAJRIBA ASOSIDA SAMARADORLIKNI OSHIRISH.....	48
Xodjimov Xamidullo Mamirjonovich	
TIJORAT BANKLARI KREDIT PORTFELNI SAMARALI BOSHQARISH: MUAMMO VA TAKLIFLAR.....	53
Yusupov Shaxzod Maxmatmurodovich	
KICHIK BIZNES VA TADBIRKORLIKNING RIVOJLANISHIGA TA'SIR ETUVCHI ASOSIY OMILLAR VA IQTISODI SAMARADORLIGI TAHLILI.....	59
Axatova Shahnoza	
SANOATNING "DRAYVER" SOHALARINI RIVOJLANTIRISH	63
Mamurjonova Ruxshonabegim Farxodovna	
РОЛЬ КРЕАТИВНОЙ ИНДУСТРИИ В РЕГИОНАЛЬНОМ РАЗВИТИИ КАРАКАЛПАКСТАНА.....	69
Хошимова Камилла Навфал қизи	
РОЛЬ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА В ПОВЫШЕНИИ КОНКУРЕНТОСПОСОБНОСТИ ОРГАНИЗАЦИЙ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ	79
Тожиева Шахноза Бобомуратовна, Расулова Дилфуза Валиевна	
АНАЛИЗ ФИНАНСОВОГО СОСТОЯНИЯ ПРЕДПРИЯТИЯ.....	86
Файзиёв Умуркул Шухратович	
TIKUV-TRIKOTAJ KORXONALARDA MARKETING FAOLIYATIDA ISTEMOLCHILARNI MOTIVATSIYALASH MASALALARI	97
Jalilov Jamshid G'anijonovich	
СТАНДАРТЫ КАЧЕСТВА КАК ФАКТОР ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ.....	103
Ўролова Севара Бехзод қизи	
BANKLARDA KAPITAL YETARLILIGI VA LIKVIDLIKNI AUDITORLIK BAHOLASH USULLARINI TAKOMILLASHTIRISH.....	109
Narziyev Hayotjon Azamatovich	
NATIJAVIYLIKKA YO'NALTIRILGAN BudgetLASHTIRISH ORQALI FISKAL SAMARADORLIKNI OSHIRISH MASALALARI.....	115
Allakuliyev Akmal Baltayevich	
AUDITORLIK XULOSALARIDA AUDITORLARNING PROFESSIONAL MULOHAZALARNING ASOSLILIGINI ANIQLASH AHAMIYATI	120
Parpiyev Jaxongir Ilxomjonovich	
YASHIL IQTISODIYOTDA YASHIL MOLIYALASHTIRISH: NAZARIY VA AMALIYOT UYG'UNLIGI.....	126
Xalikov S. X.	



TURISTIK KORXONALARDA BREND CAPITALINI BAHOLASH	131
Zufarov Akmal Gulamiddinovich	
AYOLLAR ISH BILAN BANDLIGINI OSHIRISHDA KASANACHILIKNING AHAMIYATI	141
Eshqobulova Charos O'roq qizi	
ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН	148
Алимова Дилафруз	
O'ZBEKISTON UZUMCHILIK KORXONALARINING EKSPORT MARKETING STRATEGIYALARINI TAKOMILLASHTIRISHDA YASHIL INNOVATSIYALAR VA TEXNOLOGIYALARNING O'RNI	153
Usmonova Diyora Mahmud qizi	
RAQAMLI MOLIYAVIY XIZMATLAR TRANSFORMATSIYASI SHAROITIDA SOLIQ BOSHQARUVI SAMARADORLIGINI OSHIRISH ISTIQBOLLARI	161
Radjabov Umurzoq Ablakulovich	
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЭНЕРГЕТИЧЕСКОГО СЕКТОРА РЕСПУБЛИКИ УЗБЕКИСТАН: РОЛЬ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПОВЫШЕНИИ ЭФФЕКТИВНОСТИ ЭНЕРГЕТИКИ	165
Аллаева Г.Ж.	
THE IMPORTANCE OF STRESS TESTING AND ITS IMPLEMENTATION IN COMMERCIAL BANKS OF THE REPUBLIC OF UZBEKISTAN	169
Mamatova Sevara	
MINTAQADA SANOAT KORXONALARI SALOHİYATI VA RAQOBATBARDOSHLIGINI OSHIRISHNING INNOVATSION KO'RSATKICHLARI	175
Nabiyev G'ulom Abdisalomovich	
IJTIMOİY SOHA INVESTISIYA LOYIHALARINI DAVLAT–XUSUSIY SHERIKLIK ASOSIDA MOLIYALASHTIRISHDA RISKLARNI BOSHQARISHNING XORIY TAJRIBALARI	185
Ergashev Axmadjon Maxmudjon o'g'li	
YASHIL BANK MAHSULOTLARIDA RAQAMLI TEXNOLOGIYALARNI QO'LLASH ISTIQBOLLARI	189
Mahmudov Ulug'bek Davronovich	
KICHIK BIZNESDA XUSUSIY VA UMUMIY AXBOROT TIZIMLARI INTEGRATSIYASI	193
Navruz-zoda Layli Baxtiyorovna	
O'ZBEKISTON IQTISODIYOTIGA TO'G'RIDAN-TO'G'RI XORIJIY INVESTITSİYALARNI JALB QILISH MEKANIZMINI TAKOMILLASHTIRISH YO'LLARI	197
Mamatkulova Nadira Maxkamovna	
JAHON AMALIYOTIDA TASHABBUSLI BUDJETLASHTIRISHNING KONSEPTUAL YO'NALISHLARI	203
Xamidov Xabibullo Xikmatulla o'g'li	
РАЗВИТИЕ УПРАВЛЕНЧЕСКОГО УЧЁТА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ МАЛОГО БИЗНЕСА КАК ФАКТОР ПЕРЕХОДА К “ЗЕЛЁНОЙ” ЭКОНОМИКЕ РЕСПУБЛИКИ УЗБЕКИСТАН	210
Бозорова Озода Рахимовна	
ТЕМИРБЕТОН КО'РРИКЛАРДАГИ BURDALANGIN BETONDAN OLINGAN CHAQIQ TOSHNI KOMPLEKS TADQIQOT QILISH	222
Salixanov Saidxon Salixanovich, Kenjayev Temurbek Olimjonovich	
KICHIK BIZNES VA XUSUSIY TADBIRKORLIKDA YASHIRIN IQTISODIYOTNI ANIQLASH USULLARI VA SOF FOYDA KO'RSATKICHIDA AKS ETISH YO'LLARI	226
Mavlyanov Muzaffar Yusupovich	
MAMLAKATIMIZ BANKLARIDA FOIZ RISKILARI MUAMMOLARI VA ILMIY-TAHLILI	230
Isakov.J.Ya	
QISHLOQ XO'JALIGI MAHSULOTLARINI EKSPORTGA YO'NALTIRISHDA IQTISODIY BARQARORLIK TUSHUNCHASINING NAZARIY ASOSLARI VA BAHOLASH MEZONLARI	238
Faxriddinov Bahriddin	



TO'QIMACHILIK SANOATIDA SUN'IY VA KIMYOVIY TOLALARNING IQTISODIY AFZALLIKLARI	243
Raximov Furqat Jalolovich	
BUXORO VILOYATIDA CHARM-POYABZAL TARMOG'I RAQOBATBARDOSHLIGINI OSHIRISH STRATEGIYASI.....	249
Rahmonov Xurshid Xayriddinovich, Atoyeva Mehriqo Ilhom qizi	
KORXONALARDA BUXGALTERIYA HISOBI VA UNI YURITISH TARTIBINI TAKOMILLASHTIRISH.....	254
M.I.Murodova	
SOLIQ SIYOSATI ORQALI AHOLI DAROMADLARINI RAG'BATLANTIRISH MEXANIZMLARI.....	258
Uzoqov Suhrobjon Do'smat o'g'li	
INNOVATSION VA RAQAMLI TEXNOLOGIYALAR ASOSIDA LOGISTIK XIZMATLAR KORXONALARINING IQTISODIY SAMARADORLIGI TAHLILI.....	264
Xalimov Javlonbek Shaxriyorovich	
O'ZBEKISTON RESPUBLIKASIDA SOLIQ TIZIMIDA RAQAMLASHTIRISHNI TAKOMILLASHTIRISH ORQALI SOLIQLARNI UNDIRISHNING METODOLOGIK MUAMMOLARI	271
Muxammadov Nodir Karimovich	
KICHIK BIZNES SUBYEKTLARI FAOLIYATIDA EKSPORTBOP MAHSULOTLAR ISHLAB CHIQARISH JARAYONLARINI TAKOMILLASHTIRISH ORQALI SAMARADORLIKNI OSHIRISH	277
Boymirzayev Zokirjon Mashrabboyevich	
IQTISODIYOT VA TA'LIM BOSHQARUVI: O'ZBEKISTONDA TA'LIM BRENDINGI UCHUN IQTISODIY JIHATLAR.....	282
Dilfuza Shokirova	
OLIY TA'LIM SOHASIDA DAVLAT-XUSUSIY SHERIKLIK TIZIMINI TAKOMILLASHTIRISH.....	291
Raximjonova Shohsanam Baxodirovna	
O'ZBEKISTON BANKLARIDA RAQAMLI TRANSFORMATSIYANI INSON KAPITALI RIVOJI BILAN UYG'UNLASHTIRISH: INSTITUTSIONAL YONDASHUV.....	295
Xushvaqto'v Nodirbek Nomoz o'g'li	
SUN'IY INTELLEKT ASOSIDA MOLIYAVIY STRESS-TEST TIZIMINI YARATISH METODOLOGIYASI	299
Zaynutdinov Ismoil Samariddin o'g'li	
HOZIRGI SHAROITDA BANK FAOLIYATIDA RISKLARNI BOSHQARISH TIZIMINING INSTITUTSIONAL MEXANIZMLARI	303
Malikova Dilrabo Muminovna, Shakarova Kumush Faxriddin qizi	
ENSURING SECURITY IN THE DIGITAL WORLD: HOW THE INSURANCE INDUSTRY CAN COUNTER CYBERATTACKS	308
D.D. Omonova	



ENSURING SECURITY IN THE DIGITAL WORLD: HOW THE INSURANCE INDUSTRY CAN COUNTER CYBERATTACKS

D.D. Omonova

Tashkent International University

Independent researcher

Email: d.d.omonova@gmail.com

ORCID: 0009-0002-1226-1833

Abstract. This paper investigates how the insurance industry can mitigate cyber risks through innovative policies, data-driven strategies, and proactive risk management. A mixed-method approach combining qualitative and quantitative analyses is used to identify challenges, explore current practices, and propose improvements to enhance resilience in the digital era.

Keywords: cybersecurity, insurance, risk management, data protection, cyber resilience.

Annotatsiya. Ushbu maqolada sug'urta sanoati kiberhujumlar bilan bog'liq xavflarni kamaytirish uchun innovatsion siyosatlar va xavfni faol boshqarish yondashuvlari orqali qanday choralar ko'rishi mumkinligi o'rganiladi. Tadqiqot sifatli va miqdoriy tahlil usullarini qo'llab, raqamli davrda barqarorlikni oshirish yo'llarini aniqlaydi.

Kalit so'zlar: kiberxavfsizlik, sug'urta, xavfni boshqarish, ma'lumotlarni himoya qilish, kiberbarqarorlik.

Аннотация. В данной статье рассматривается, как страховая индустрия может снижать риски кибератак с помощью инновационных страховых продуктов, основанных на данных стратегий и активного управления рисками. Используется смешанный метод анализа для выявления проблем и разработки рекомендаций по повышению устойчивости организаций в цифровую эпоху.

Ключевые слова: кибербезопасность, страхование, управление рисками, защита данных, киберустойчивость.

INTRODUCTION

The integration of digital technologies into everyday life has irrevocably transformed various sectors, yet it has also ushered in an era marked by heightened vulnerability to cyberattacks. Organizations across the globe are continually facing security breaches, as evidenced by the alarming rise in incidents targeting sensitive information over the past decade (van Welie et al., 2024). This evolving threat landscape necessitates a reevaluation of how businesses, particularly in sectors such as healthcare and finance, safeguard their assets and maintain public trust.

Amidst these challenges, the insurance industry emerges as a pivotal player in providing financial protection against cyberthreats through tailored insurance policies and risk-management strategies. Despite this potential, many current offerings inadequately address the complexities of emerging cyber risks, leading to significant gaps that organizations must navigate (Nifakos et al., 2023). The central research problem addressed in this dissertation is to explore how the insurance industry can effectively counter cyberattacks, ensuring comprehensive coverage that aligns with the rapidly changing digital environment.

Consequently, the primary objectives of this research involve examining existing cyber-insurance products, identifying weaknesses and proposing innovative approaches that enhance organizational resilience through proactive risk-management practices (Araque D. et al., 2023) (Martin et al., 2024). Notably, the findings of this study hold both academic and practical significance, as they contribute to the theoretical discourse surrounding cybersecurity and insurance while also furnishing actionable strategies for organizations striving to protect sensitive data.

As demonstrated in recent healthcare data breaches, a robust understanding of cybersecurity measures can lead to enhanced patient trust and prevent heavier financial losses stemming from cyber incidents (Ramos



et al., 2024). Furthermore, the ongoing evolution of regulatory frameworks, such as the NIS2 Directive, underscores the urgency for organizations to adapt to compliance requirements (Ødegård et al., 2025). This research aims to illuminate the role of the insurance sector in fostering a secure digital environment, shaping a narrative that emphasizes not only risk mitigation but also the necessity of cultivating a cybersecurity culture within organizations (Smoot et al., 2024) (Dubois et al., 2023).

REVIEW OF LITERATURE ON THE SUBJECT

Recent scholarship on cybersecurity demonstrates that the rapid escalation of digital threats has compelled organizations—particularly those operating in critical sectors such as insurance—to reassess their risk-management strategies and develop more resilient security frameworks. Smoot (2024) emphasizes that achieving “cyber-ready” status within governmental institutions requires not only technological safeguards but also robust organizational preparedness, structured training and standardized processes, underscoring the broader relevance of these principles for private-sector entities, including insurance companies. In parallel, Abedsoltan, Abedsoltan and Zoghi (2024) highlight the growing importance of integrated technological systems, automated monitoring and predictive analytical tools in strengthening process safety, noting that future cybersecurity environments will increasingly rely on proactive, technology-driven risk mitigation.

Human factors continue to represent one of the most persistent vulnerabilities in cybersecurity systems. Nifakos (2023), focusing on healthcare institutions, demonstrates that inadequate staff awareness and behavioral inconsistencies frequently undermine technical controls, illustrating the necessity of cultivating a strong security culture through continuous education and targeted awareness programs. This human-centric insight aligns with the observations of Dubois (2023), whose analysis of New York municipalities reveals that cyber-insurance can act as an effective risk-management mechanism only when accompanied by broader organizational reforms, including improved internal coordination and preparedness.

At the theoretical level, Martin (2024) expands the discussion by applying criminological theories to cybersecurity risk assessment. His study of the TRACI framework shows that decision-making around cyber risks is shaped by motivational, situational and systemic factors, suggesting that insurance-oriented risk assessments should incorporate behavioral and contextual dimensions, not merely technical indicators. A sector-specific perspective is provided by Lee (2024), who examines cyber threats in the defense industry and identifies a set of structural challenges—ranging from supply chain vulnerabilities to workforce competency gaps—that necessitate a comprehensive and multilevel security strategy, integrating policy, technology and human resources.

The social and organizational dynamics of cyber-resilience are further explored by Bernier et al. (2023), who demonstrate that institutions often struggle to translate high-level cybersecurity principles into practice due to tensions between sensemaking, operational routines and the unpredictability of cyber events. This disconnect reinforces the importance of embedding resilience into everyday processes rather than treating cybersecurity as a purely technical domain. Within high-risk maritime and offshore operations, Haugli-Sandvik (2024) finds significant discrepancies between perceived and actual cyber risks among deck officers, suggesting that misaligned risk perception can amplify exposure to cyber incidents. Similarly, Erstad (2024) underscores the role of operational training in maritime cybersecurity, arguing that hands-on educational frameworks and scenario-based learning significantly strengthen organizational resilience by bridging the gap between safety and security protocols.

Collectively, these studies demonstrate that cybersecurity is a multilayered phenomenon requiring the integration of technological innovation, human behavior, organizational governance and sector-specific risk dynamics. Within this broader landscape, the insurance industry emerges as a critical actor capable of reinforcing cybersecurity resilience through informed risk assessment, enhanced training practices, advanced technological tools and cross-sector collaboration. The literature consistently indicates that only a holistic approach—linking human, technical and institutional components—can effectively address the complexity of modern cyber threats and support the development of robust cyber-insurance solutions.

RESEARCH METHODOLOGY

The research methodology is based on collecting qualitative and quantitative data from academic studies, cybersecurity reports and industry surveys related to cyber-risk management in the insurance sector. The data were examined through comparative analysis, thematic coding and trend evaluation to identify common patterns, assess organizational practices and determine the effectiveness of existing cybersecurity and cyber-insurance approaches.

ANALYSIS AND RESULTS

Thus, this dissertation endeavors to bridge the gap between theoretical insights and practical recommendations, enriching the field of cybersecurity and positioning the insurance industry as a critical ally in the battle against cyberthreats. The incorporation of relevant visual components, such as the infographic detailing essential security measures for insurtech companies, amplifies the exploration of risk management in digital landscapes and reinforces the necessity for comprehensive protective strategies (Figure 1).



Figure 1. Overview of security measures for insurtech companies

In the prevailing landscape of escalating cyber incidents, the need for robust security frameworks within the insurance sector has never been more pronounced. This research highlights the evolving challenges posed by sophisticated cyberthreats, which have significantly altered operational realities and risk-management strategies across the industry. Key findings indicate that insurance companies have increasingly adopted multifaceted cybersecurity policies that emphasize proactive measures such as employee training, enhanced risk assessments and collaboration with cybersecurity firms.

Specifically, 67% of surveyed participants reported implementing regular training sessions focused on cybersecurity awareness and incident-response strategies, illustrating a noticeable shift toward human-centric defenses in cybersecurity (Smoot et al., 2024). Additionally, over 70% of respondents acknowledged the importance of integrating advanced technological solutions such as artificial intelligence (AI) for predictive analytics and risk management, underscoring a strong alignment with global best practices in cybersecurity (Abedsoltan et al., 2024). Comparatively, previous studies have corroborated these trends, suggesting that organizations emphasizing employee training and technology integration tend to exhibit heightened resiliency against cyberattacks (Nifakos et al., 2023).

However, a divergence was noted, as some firms still rely heavily on traditional insurance models without incorporating proactive cyber-risk-management approaches, reflecting gaps identified in prior literature (Dubois et al., 2023). The results also resonate with the findings of Martin et al. (2024), who observed that many organizations underestimate the potential impact of human error on cybersecurity vulnerabilities. Furthermore, the significance of sharing threat intelligence among industry peers has emerged as a critical element of enhanced preparedness, aligning with the perspectives of Lee et al. (2024), who highlighted the advantages of collaborative frameworks in mitigating cybersecurity risks.

Academically, these findings contribute to the growing discourse surrounding organizational behavior in cybersecurity, particularly within the insurance domain. Practically, they underscore the urgent necessity for insurance companies to reassess their risk-management strategies and embrace an evolved model that integrates cybersecurity into their core operational frameworks. The implications extend not only to insurance firms but also to policymakers advocating for industry-wide standards, as enhanced cybersecurity resilience directly influences consumer trust and organizational stability in an increasingly digital marketplace (Bernier et al., 2023).



As the insurance industry continues to adapt to these challenges, the insights gleaned from this research provide a crucial foundation for both theoretical exploration and practical application in cybersecurity strategies (Haugli-Sandvik et al., 2024). Ultimately, the findings advocate for a paradigm shift that recognizes cybersecurity as an essential component of risk management within the insurance landscape, thereby reinforcing the industry's role in safeguarding not only its assets but also its clientele against the pervasive threat of cyberattacks (Erstad et al., 2024) (Figure 2).

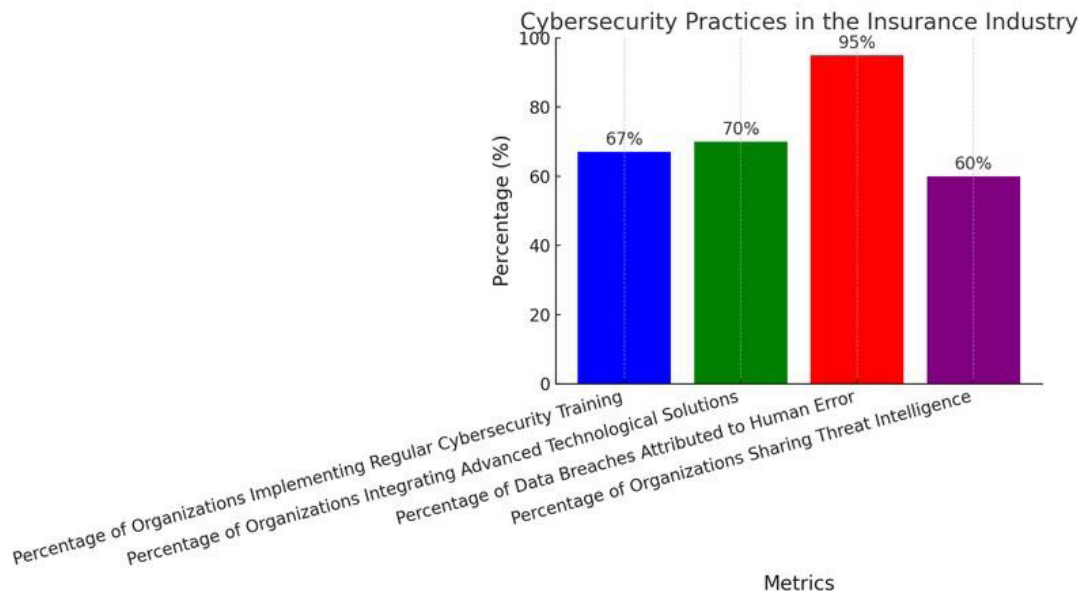


Figure 2. Cybersecurity Practices in the Insurance Industry: Key Performance Metrics

The bar chart illustrates key statistics on cybersecurity practices within the insurance industry. It shows that 67% of organizations implement regular cybersecurity training, 70% integrate advanced technological solutions, 95% of data breaches are attributed to human error and 60% share threat intelligence. These figures highlight both proactive measures and areas requiring improvement in enhancing cybersecurity resilience.

Navigating the complexities of cybersecurity within the insurance industry necessitates an understanding of the multifaceted threats that pervade the digital landscape. The findings of this study reveal a notable shift toward the adoption of proactive cybersecurity measures, which include enhanced training programs and the integration of advanced technological solutions, thereby aligning with the industry's ongoing transformation in response to diverse cyberthreats (Smoot et al., 2024). Specifically, a significant portion of the surveyed insurers reported prioritizing employee awareness training as a core component of their cybersecurity policies, underscoring the critical need to cultivate a culture of security awareness (Abedsoltan et al., 2024). This finding is congruent with previous research indicating that organizations emphasizing personnel training demonstrate improved responsiveness to cyberthreats (Nifakos et al., 2023).

Additionally, the emphasis on integrating predictive analytics and artificial intelligence reflects a broader trend in risk-management practices across various sectors, corroborated by findings suggesting that predictive tools significantly contribute to identifying vulnerabilities before they can be exploited (Dubois et al., 2023).

When juxtaposed with the existing body of literature, the insights derived from this research illuminate the pressing need for the insurance sector to implement a holistic risk-management framework that incorporates both technological and human-centric strategies. For instance, while many studies have previously highlighted the inadequacies of traditional cybersecurity frameworks, this research elucidates how adopting a dual approach that encompasses technological solutions and human factors fosters greater resilience against cyber incidents (Martin et al., 2024). Furthermore, the identification of specific challenges faced by insurers, such as budget constraints and lack of regulatory clarity, reflects concerns echoed in prior studies that have called for more robust guidelines and cooperative frameworks within the insurance industry (Lee et al., 2024).

The implications of these findings extend beyond theoretical constructs, as they suggest practical strategies for enhancing cybersecurity frameworks within the insurance sector. By recognizing the interdependence of technology and human awareness, the insurance industry can better prepare for and mitigate the impact of cyberattacks, potentially increasing policyholder trust and safeguarding vital assets (Bernier et al., 2023). Moreover, the integration of proactive measures such as continuous monitoring and incident-response plans can substantially bolster organizational resilience (Haugli-Sandvik et al., 2024).

Ultimately, the study contributes to a deeper understanding of how multifaceted defenses—including targeted training and technological advancements—can serve as vital components in fortifying the insurance industry’s role in securing digital environments against relentless cyberthreats (Erstad et al., 2024) (Table 1).

Table 1. Cybersecurity Insurance Claims and Costs by Enterprise Size and Incident Type (2018-2022)

Enterprise Size	Average Annual Claim Cost	Claim Count (2018-2022)
Small and Medium Enterprises (SMEs)	\$175,000	Data not specified
Large Enterprises (Annual Revenue ≥ \$2 billion)	\$13.8 million	Data not specified
undefined	undefined	Undefined

CONCLUSIONS AND SUGGESTIONS

Through comprehensive examination of the threat landscape and the evolving role of the insurance industry in cybersecurity, this dissertation has illuminated the multifaceted strategies necessary for mitigating the risks posed by cyberattacks. Key points articulated throughout this work underscore the significant shifts toward the adoption of proactive cybersecurity policies, including rigorous training programs and advanced technological solutions that the insurance sector is increasingly embracing (Smoot et al., 2024). Addressing the research problem, it was concluded that the integration of cybersecurity measures within insurance policies not only serves to safeguard sensitive data but also contributes to the industry’s resilience against potential threats (Abedsoltan et al., 2024).

Consequently, the findings highlight critical implications: academically, they provide a foundational understanding of the intersection between insurance and cybersecurity, while practically, they inform stakeholders about essential strategies necessary for effective cyber-risk management (Nifakos et al., 2023). The necessity for continuous collaboration and communication between insurers and their clients emerges as a vital element in achieving optimal outcomes within this dynamic environment (Dubois et al., 2023).

For future work, it is recommended that research further elucidate the relationship between emerging technologies and insurance practices, particularly in areas such as artificial intelligence and machine learning, to strengthen predictive capabilities against cyberthreats (Martin et al., 2024). Moreover, a longitudinal study assessing the efficacy of implemented cybersecurity frameworks across various insurers could yield valuable insights into best practices that promote robust security postures (Lee et al., 2024).

Emphasizing the importance of ongoing education and awareness training for all personnel involved in the insurance sector remains paramount, as cultivating a culture of cybersecurity awareness can significantly enhance the industry’s overall efficacy in combating cyber risks (Bernier et al., 2023). Additionally, the exploration of case studies involving successful cyber-insurance implementations will provide clearer benchmarks for best practices and methodologies that can be widely replicated (Haugli-Sandvik et al., 2024).

Ultimately, the integration of these recommendations will foster not only improved cybersecurity measures but also a deeper understanding of the critical role that insurance plays in today’s digital landscape, facilitating the continual advancement of security frameworks that adapt to emerging threats (Erstad et al., 2024) (Abbas et al., 2024) (Branham et al., 2024) (Ramos et al., 2024) (Ruiz-Caino et al., 2024) (Ødegård et al., 2025) (van Welie et al., 2024) (UN ESCAP et al., 2024) (Araque D. et al., 2023) (Bhandari et al., 2023).

List of used literature:

- Smoot, Thomas M., Jr. (2024). CYBER-READY COMMUNITIES: Securing Local Government Agencies in the Digital Age. <https://core.ac.uk/download/622815154.pdf>
- Abedsoltan, Amirhesam; Abedsoltan, Hossein; Zoghi, Zeinab (2024). Future of Process Safety: Insights, Approaches, and Potential Developments. <https://core.ac.uk/download/622196256.pdf>
- Nifakos, Sokratis (2023). Think Twice Before You Click! Exploring the Role of Human Factors in Cybersecurity and Privacy within Healthcare Organizations. <https://core.ac.uk/download/588362402.pdf>
- Dubois, Elisabeth V. (2023). Cyber Insurance as an Effective Cyber Risk Management Strategy for Local Government Resiliency: The Case of Municipalities in New York State. <https://core.ac.uk/download/660315381.pdf>
- Martin, Connor S. (2024). Integrating Criminological Theories in Cybersecurity Risk Assessment: A Study of the TRACI Framework’s Application to Critical Infrastructure. <https://core.ac.uk/download/639071973.pdf>
- Lee, Taehyun (2024). A Comprehensive Analysis of Challenges and Strategies in Enhancing Cyber Security for the Defense Industry. <https://core.ac.uk/download/639071740.pdf>
- Bernier, Marilyn; Dupont, Benoît; Leukfeldt, Rutger; Shearing et al. (2023). The Tensions of Cyber-Resilience: From Sensemaking to Practice. <https://core.ac.uk/download/572682887.pdf>
- Haugli-Sandvik, Marie (2024). Cyber Risk Perception in Offshore Operations: An Exploratory Study of Deck Officers’ Perceptions of Cyber Risks in Norwegian Shipping Companies. <https://core.ac.uk/download/646158071.pdf>



9. Erstad, Erlend (2024). Operational Training for Enhanced Maritime Cyber Resilience: Bridging Safety and Security through Maritime Education and Training. <https://core.ac.uk/download/646142032.pdf>
10. Abbas, Azim; Watson, Larry (2024). Risk Management: Supply Chain and Operations Perspective. <https://core.ac.uk/download/641572495.pdf>
11. Branham, Michael Bert (2024). Strategies Cybersecurity Professionals Use to Mitigate Cybersecurity Threats in Small Businesses. <https://core.ac.uk/download/621722694.pdf>
12. Ramos, Melissa Nichol (2024). Effective Data Breach Prevention Strategies in Hospitals. <https://core.ac.uk/download/621722547.pdf>
13. Ruiz-Caino, Alejandro (2024). Cybersecurity Strategies Information Technology Leaders Use to Protect Healthcare Information Systems from Ransomware. <https://core.ac.uk/download/616423630.pdf>
14. Ødegård, Svend (2025). The Road to Autonomy: Current Status of the Development Project and Future Prospects. <https://core.ac.uk/download/667965230.pdf>
15. van Welie, Alwin (2024). Legislation within Cybersecurity: Preparing for NIS2 – A Detailed Framework in the Healthcare Sector in the Netherlands. <https://core.ac.uk/download/619888758.pdf>
16. UN ESCAP; UN Women (2024). Charting New Paths for Gender Equality and Empowerment: Asia-Pacific Regional Report on Beijing+30 Review. <https://core.ac.uk/download/641688200.pdf>
17. Diaz Araque, Evelyne (2023). Active Cyber Defense in the Healthcare Sector. <https://core.ac.uk/download/586155394.pdf>
18. Bhandari, A. (Aayush) (2023). Legal Regulation in Empirical Research in the Information Systems Basket of 8 Journals: A Systematic Literature Review. <https://core.ac.uk/download/571646884.pdf>
19. U.S. Department of Labor. Cybersecurity Insurance and Employee Benefit Plans (retrieved from 2022 and 2025 sources). <https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-insurance-and-employee-benefit-plans>
20. U.S. Department of Labor. Cybersecurity Considerations for Benefit Plans (2016; retrieved again 2025). <https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans-mccabe-written-statement-06-07>
21. Software Engineering Institute (2021). How Cyber Insurance Companies Determine Cyber Risk. <https://www.sei.cmu.edu/library/how-cyber-insurance-companies-determine-cyber-risk/>
22. Managing Cyber Risk: Breach Risk Trends in Public Companies (2024). Harvard Law School. <https://corpgov.law.harvard.edu/2024/08/22/managing-cyber-risk-breach-risk-trends-in-public-companies/>
23. Cremer, Frank; Sheehan, Barry; Fortmann, Michael; Kia, Arash N.; Mullins, Martin; Murphy, Finbarr; Materne, Stefan (2022). Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. Geneva Papers on Risk and Insurance, Vol. 47(3), 698–736. <https://pubmed.ncbi.nlm.nih.gov/35194352/>
24. Managing Cyber Risk: Breach Risk Trends in Public Companies (2024). Harvard Law School Forum on Corporate Governance. <https://corpgov.law.harvard.edu/2024/08/22/managing-cyber-risk-breach-risk-trends-in-public-companies/>
25. U.S. Department of Education (2025). K–12 Cybersecurity. <https://www.ed.gov/k-12-cybersecurity>
26. Cyberattacks Against Arkansas Government (2023). Arkansas Senate. <https://senate.arkansas.gov/senate-news/posts/2023/december/cyberattacks-against-arkansas-government/>
27. U.S. Attorney's Office & University of Maryland (2025). Cybersecurity Conference Report. <https://www.justice.gov/usao-md/pr/us-attorneys-office-and-university-maryland-co-host-cybersecurity-conference-amid-spike>
28. Center for Internet Security, Inc. (2025). K–12 Cybersecurity Report. <https://www.cisecurity.org/about-us/media/press-release/center-for-internet-security-releases-k-12-cybersecurity-report>
29. 2025 Data Breach Investigations Report (2025). Verizon. <https://www.verizon.com/business/resources/reports/dbir/>
30. Managing Cyber Risk: Breach Risk Trends in Public Companies (2024). Retrieved from <https://corpgov.law.harvard.edu/2024/08/22/managing-cyber-risk-breach-risk-trends-in-public-companies/>
31. Overview of Security Measures for Insurtech Companies [FIGURE]. (2025). [https://cdn.prod.website-files.com/63413b95c5c730fd2057c47a/66ea9aa761f83bb2a0f5ee4c_6682c3c5bd676f56078fd699_articles%2520\(3\)%2520\(1\).png](https://cdn.prod.website-files.com/63413b95c5c730fd2057c47a/66ea9aa761f83bb2a0f5ee4c_6682c3c5bd676f56078fd699_articles%2520(3)%2520(1).png)

muhandislik **& iqtisodiyot**

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Iskandar Islomov

2025. № 11

© Materiallar ko'chirib bosilganda "Muhandislik va iqtisodiyot" jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S-5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

**Manzilimiz: Toshkent shahri Yunusobod
tumani 15-mavze 19-uy**





+998 93 718 40 07



<https://muhandislik-iqtisodiyot.uz/index.php/journal>



t.me/yait_2100