TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI BIR MARTALIK ILMIY KENGASH

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

KORABAYEV ELDOR ALIJONOVICH

ELEKTR ENERGETIKA SANOATI KORXONALARINING TASHKILIY-IQTISODIY FAOLIYATINING AXBOROT XAVFSIZLIGI MEXANIZMLARINI RAQAMLASHTIRISH

08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya

Iqtisodiyot fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi AVTOREFERATI

Toshkent – 2024

UDK: 338.2:004.056:621.311

Iqtisodiyot fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата докторской диссертации (PhD) философии по экономическим наукам

Content of the Doctoral (PhD) dissertation abstract

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSC.13/30.12.2019.T.07.02 RAQAMLI BIR MARTALIK ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

KORABAYEV ELDOR ALIJONOVICH

ELEKTR ENERGETIKA SANOATI KORXONALARINING TASHKILIY-IQTISODIY FAOLIYATINING AXBOROT XAVFSIZLIGI MEXANIZMLARINI RAQAMLASHTIRISH

08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya

Iqtisodiyot fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi AVTOREFERATI

Toshkent – 2024

Iqtisodiyot fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy attestatsiya komissiyasida B2024.2.PhD/Iqt4303 raqam bilan ro‘yxatga olingan.

Dissertatsiya Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida bajarilgan.

Dissertatsiya avtoreferati ikki tilda (o‘zbek, rus) Ilmiy kengash veb-sahifasi **(**www.tuit.uz**)** va “ZiyoNet” ta’lim axborot tarmog‘ida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Saitkamolov Muxammadxuja Sobirxo‘ja o‘g‘li** iqtisodiyot fanlari doktori, dotsent
Rasmiy opponentlar:	**Samatov Gaffor Allakulovich** iqtisodiyot fanlari doktori, professor
	Muratova Shoxista Nigmatullayevna iqtisodiyot fanlari doktori, professor
Yetakchi tashkilot:	**Islom Karimov nomidagi Toshkent davlat texnika universiteti**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi ilmiy darajalar beruvchi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 2024 yil “____”_____ soat _____ dagi majlisida bo‘lib o‘tadi (Manzil: 100084, Toshkent shahri, Amir Temur shox ko‘chasi, 108 uy. Tel.: (71) 238-64-15. e-mail: info@tuit.uz.

Dissertatsiya bilan Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari univercitetining Axborot-resurs markazida tanishish mumkin (2870 raqami bilan ro‘yxatga olingan). (Manzil: 100084, Toshkent shahri, Amir Temur shox ko‘chasi, 108 uy. Tel.: (71) 238-64-15. e-mail: info@tuit.uz.

Dissertatsiya avtoreferati 2024 yil “_____”_____ kuni tarqatildi.
(2024 yil “_____”_____ dagi _____ raqamli reestr bayonnomasi).

B.Sh.Maxkamov
Ilmiy darajalar beruvchi ilmiy kengash raisi, i.f.d., prof.

E.Sh.Nazrova
Ilmiy darajalar beruvchi ilmiy kengash kotibi, t.f.d., prof.

Sh.Dj. Irgashxodjayeva
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi ilmiy seminar raisi, i.f.d., prof.

KIRISh (Falsafa doktori dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Globallashuv sharoitida iqtisodiyotni raqamlashtirish darajasining barqaror o‘sishi, ikkinchi tomondan sun’iy intellekt texnologiyalarini izchil rivojlanib borish sharoitida global va milliy darajada sanoat sohalari, jumladan elektr energetika sanoati korxonalarining tashkiliy-iqtisodiy faoliyati axborot xavfsizligini raqamlashtirish mexanizmlarini takomillashtirish muhim ahamiyat kasb etmoqda. “2023-yilda Kanadaning Dit Retro energetika korxonasiga kiberhujum natijasida mamlakat 12,1 foiz YaIMdagi ulushni yo‘qotgan hamda yirik pul hajmida iqtisodiy talofat ko‘rgan”[1]. Bugungi kunda jahon iqtisodiyotini raqamli texnologiyalar asosida maqsadli rivojlantirishning muhim shartidan biri sifatida ishlab chiqarish korxonalarining tashkiliy-iqtisodiy faoliyati axborot xavfsizligini ustuvor darajada tashkil qilish o‘ta dolzarb masala hisoblanmoqda.

Jahonda elektr energetika sanoati korxonalari axborot xavfsiz-ligini ta’minlash bo‘yicha amalga oshirilayotgan tadqiqotlar tarkibida ishlab chiqarishning tashkiliy-iqtisodiy faoliyati axborot xavfsizligini raqamlashtirish mexanizmlarini takomillashtirishga ustuvor darajada qaralmoqda. Bu borada boshqaruvda axborot xavfsizligini ta’minlashning tashkiliy-iqtisodiy mexanizmini to‘laqonli shakllantirish, aqlli energetika tizimlari kiberbardoshliligini oshirishning iqtisodiy asoslarini takomillashtirish, IT texnologiyalar asosida amalga oshiriladigan elektr energiyani boshqarishda sodir bo‘ladigan talofatlarni aniqlash uslubiyotini takomillashtirish, aqlli texnologiyalarga ko‘ra boshqaruvning kibersamaradorligini iqtisodiy qo‘llab-quvvatlash mexanizmlarini takomillashtirish kabi mavzulardagi tadqiqotlar dolzarb bo‘lib qolmoqda.

O‘zbekistonda elektr energetika sanoatini sifat jihatdan rivojlantirish va texnologik darajasini jahon talablariga ko‘ra tashkil qilish bilan bir qatorda boshqaruv samaradorligini oshirish, soha korxonalari tashkiliy-iqtisodiy faoliyatining axborot xavfsizligini to‘laqonli tashkil qilish, issiqlik elektrostansiyalari kiberxavfsizligini ta’minlash, elektr ta’minotini iste’molchilarga to‘g‘ridan-to‘g‘ri yetkazishning kiberhimoyasini oshirish kabilar borasida keng qamrovli chora-tadbirlar amalga oshirilmoqda. “Raqamli O‘zbekiston — 2030” strategiyasi doirasida elektr energiyasi sarfini “onlayn” nazorat qilish, shuningdek avtomatlashtirilgan qurilmalarni o‘rnatish joylarini bosqichma-bosqich raqamlashtirishda kiberiqtisodiy faoliyat rivojlanishini ilgari suradi.[2] Mazkur vazifalarning ilmiy ta’minotini amalga oshirishda, jumladan energetika sanoati korxonalari kiberxavfsizlik darajasining maqbul prametrlarini asoslash, mahsulot iste’moliga qadar elektr energiyasini realizatsiya qilish jarayonlari boshqaruvini takomillashtirish, mahsulot ishlab chiqarish jarayonlari tashkiliy-iqtisodiy kiberxavfsizligining prognoz ko‘rsatkichlarini asoslash bo‘yicha tadqiqotlarni yanada chuqurlashtirish maqsadga muvofiq.

O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasi Prezidentining

[1] Energydata.com

[2] O‘zbekiston Respublikasi Prezidentining 05.10.2020 yildagi PF-6079-sonli “«Raqamli O‘zbekiston — 2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni, II. Axborot tizimlari va dasturiy mahsulotlarni joriy etish bandi

2020-yil 5-noyabrdagi PF-6079-sonli “Raqamli O‘zbekiston–2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni, 2022-yil 22-avgustdagi PQ-357-son “2022-2023 yillarda axborot-kommunikatsiya texnologiyalari sohasini yangi bosqichga olib chiqish chora-tadbirlari to‘g‘risidagi” Qarori va mavzuga oid boshqa me’yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda mazkur dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.[3]

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Dissertatsiya tadqiqoti respublika fan va texnologiyalar rivojlanishining “Demokratik va huquqiy jamiyatni ma’naviy-axloqiy va madaniy rivojlantirish, innovatsion iqtisodiyotni shakllantirish” ustuvor yo‘nalishiga muvofiq bajarilgan.

Muammoning o‘rganilganlik darajasi. Jahon tajribasida energetika korxonalari tashkiliy-iqtisodiy faoliyatida axborot xavfsizligi yuzasidan ishlab chiqarishning iqtisodiy samaradorligini oshirish va turli sohaviy rivojlanishlar borasidagi yondashuvlar hamda amaliy ishlanmalar D.Gaskova, M.Prostoserdov, L.Magomedova, D.Bekbergenova, R.Anderson, G.Lawrense, L.Martin, A.Efe, R.Rutil, R.Ramashandran, E.Serah, S.Grobman[4] kabi xorij iqtisodchi olimlar tomonidan o‘rganilgan.

Mamlakatimizda korxonalarning axborot xavfsizligi va uning iqtisodiy asoslarini tadqiq etish S.Jumanova, I.Alimardonov, A.Anorboyev, A.Rakitskiy, B.Axrorov, T.Shodiyev, M.Saitkamolov, R.Alimjanov, N.Nasrullayev, A.Musayev, K.Kerimov, I.Dustmuhammedov[5] singari olimlarning ilmiy ishlarida yoritilgan.

---

[3] O‘zbekiston Respublikasi Prezidentining Oliy Majlisga Murojaatnomasi.

[4] Гаскова Д.А. Методы, модели и комплекс программ анализа киберситуационной осведомленности энергетических объектов. Автореф. 2021 г, 34 с//Простосеров М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия, авторе дсс. 2016 г, 23 стр//Магомедова Л.Р. 2021 г, 24 ст//Бекбергенова Д.Е. Управление цифровизацией социально-экономического развития региона, 2022 г, 34 стр// Ross Anderson. Why Information Security is Hard – An Economic Perspective.University of Cambridge Computer Laboratory, J.Thomson Avenue, Cambridge CB3 0FD, UK Ross.Anderson@cl.cam.ac.uk, 2000, 64 p// Гордон, Лоуренс А .; Леб, Мартин П. (ноябр 2002 г.). «Экономика инвестиций в информационную безопасност» . Транзакции ACM по информационной и системной безопасности . 5 (4): 438–457. Дои : 10.1145/581271.581274 . S2CID 1500788// Lawrence A. Gordon and Martin P. Loeb. Using Information Security as a Response to Competitor “Analysis Systems”. Communications Of The Acm. September 2001/Vol. 44, No. 9, 71-77// Ахмет Эфе. Организационная кибербезопасност: позиция ИТ-аудита, основанного на экономическом риске, теоретических и практических аспектах кибербезопасности (русское издание). 2023 г, 452 стр// Пунам Патил. Эффективный метод кибербезопасности: Защита данных от киберпреступников (русское издание). Sciencia Scripts. 2022 г, 76 стр// Ravikumar Ramachandran, CISA, CISM, CGEIT, CRISC, CDPSE, OCP-Oracle Cloud Architect, CISSP-ISSAP, SSCP, CAP, PMP, CIA, CRMA, CFE, FCMA, CIMA-Dip.MA, CFA, CEH, ECSA, CHFI, MS (Fin), MBA (IT), COBIT-5 Implementer, Certified COBIT Assessor, ITIL 4 -Managing Professional, togaf 9 Certified, Certified safe5 Agilist, Chennai, India, Date Published: 23 January 2019, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy// Питер Баняш. Различные аспекты кибербезопасности и осведомленности об информационной безопасности (русское издание). Sciencia Scripts 2023 г, 60 стр// Сера Э. Кибербезопасност: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании. Интеллектуалная Литература 2021 г// Капинда Ч. Готовност к кибербезопасности повышают правителство в странах мира (русское издание). Sciencia Scripts 2023 г, 68 стр// Steve Grobman. The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War. Apress. 2016 y, 374 p

[5] Жуманова С. Киберхавфсизлик - рақамли иқтисодиётнинг муҳим шарти. Янги Ўзбекистон. Kolorpak. 2020 й, 330 б// Алимардонов И. Миллий молиявий хатарларнинг олдини олиш шарти. Халқ сўзи, 2022, 336// Анорбоев А.У. Кибержиноятчилик ва киберхавфсизлик бўйича қонун ижодкорлигининг замонавий тенденциялари: миллий, хорижий ва ҳалкаро тажриба монография. Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги, Ўзбекистон Республикаси миллий

Mazkur yo‘nalishda keltirilgan olimlarning tadqiq etilayotgan muammoni hal etish bo‘yicha qo‘shgan hissalarini inobatga olgan holda energetika sanoati korxonalarining axborot xavfisizligini ta’minlash mexanizmlarini takomillashtirish va ularning to‘g‘ri yo‘lga qo‘yilishni baholash yo‘llari kabi masalalar respublikamiz iqtisodiy adabiyotlarida yetarli darajada yoritilmagan. Mazkur dissertatsiya ishida ushbu muammoning yechimi keng yoritib berilgan.

Tadqiqotning dissertatsiya bajarilgan oliy ta’lim muassasasi-ning ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Mazkur dissertatsiya mavzusi Toshkent axborot texnologiyalari universiteti ilmiy-tadqiqot ishlari rejasiga muvofiq №A-2-59 “Raqamli iqtisodiyot sharoitida O‘zbekiston mehnat bozorining adaptiv moslashuvchan transformatsiyasi va ijtimoiy-mehnat munosabatlarini tashkil etish modellari” mavzusidagi amaliy loyiha doirasida bajarilgan.

Tadqiqotning maqsadi elektr energetika sanoati korxonalarining tashkiliy-iqtisodiy faoliyati axborot xavfsizligini raqamlashtirish mexanizmlarini takomillashtirish bo‘yicha taklif va tavsiyalar ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

xorijiy va mahalliy olimlarning nazariy yondashuvlari asosida “kiberxavfsizlik iqtisodiyoti” tushunchasining iqtisodiy mohiyatini energetika sanoatining tashkiliy-iqtisodiy faoliyati uchun asoslash;

issiqlik energetika sanoat korxonalari tashkiliy-iqtisodiy mexanizmlarini takomillashtirishda axborot xavfsizligi rolini izchil tadqiq etish, tashkiliy va iqtisodiy munosabatlarda uning ahamiyati va kibergigiyenaviy salohiyatni aniqlash;

energetika sanoat korxonalarida tashkiliy-iqtisodiy faoliyatning kiberxavfsizligini baholash va ta’sir ko‘rsatuvchi omillar tasnifini shakllantirish;

korxonalar tashkiliy-iqtisodiyot faoliyati mexanizmning tarkibiy komponentlarini ilg‘or xorij tajribasi hamda muallif yondashuviga ko‘ra mamlakatimiz iqtisodiy infratuzilmasiga joriy etish imkoniyatlarini asoslash;

energetika sanoati korxonalarining tashkiliy-iqtisodiy faoliyat mexanizmlarini axborot xavfsizligini rivojlantirishda innovatsion loyihalarni samaradorligini baholash uslubiyotini takomillashtirish;

гвардия ҳарбий техника институти, Мухаммад ал-Хоразмий ном. ТАТУ, 2020 й, 360 б//Ракитский А. Корхонада ахборот хавфсизлиги қандай таъминланади. Korxonani boshqarish. "mtsfer-u Nashriyot uyi" МЧЖ, 2019 й, 334 б//Ахроров Б.А. Иқтисодиёт йўналишидаги бакалаврларни тайёрлашда "Ахборот хавфсизлиги" курсини ўкитиш методикаси. 13.00.02 - Таълим ва тарбия назарияси ва методикаси (информатика): Педагогика фанлари бўйича фалсафа д-ри (phd) дис. Автореф.], 2019 й, 50 б// Шодиев Т. Банк тизимида ахборотларни криптографик услублар ёрдамида ҳимоялашнинг долзарб муаммолари, 2021 й, 312 б// Алимжанов Р. Ахборотни йўқотиш оқибатидаги зарардан компанияни қандай ҳимоя қилиш мумкин. "mtsfer-u Nashriyot uyi" МЧЖ 2020 й, 228 б// Насруллаев Н.Б. Ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш усуллари ва алгоритмлари [Матн] : техника фан. Фалсафа доктори дис.автор, 2019, 54 б// Мусаев А.И. Узлуксиз шифрлашнинг криптобардошли алгоритмлари ва уларнинг самарадорлигини баҳолаш Техника фанлари номзоди. ... Дис. Автореферати, 2011 й, 21 б// Керимов К.Ф. Электрон ресурсларни ахборот ҳавфсизилиги таҳдидларидан ҳимоясини таъминлашнинг мослашувчан моделлари ва усуллари диссертация автореферати, 2020 й, 58 б//Дустимуҳаммедов И.А. Божхона ахборот тизимларида ахборот хавфсизлигини таъминлаш усуллари ва моделлари [Матн] // А. И. Дусмуҳамедов, А. А. Саидов, З. Б. Абдураҳмонов ; Ўзбекистон Республикаси Давлат божхонаси қўмитаси, Божхона институти. Тошкент : Fan va texnologiyalar nashriyot-matbaa uyi, 2022, 204 б//

energetika sanoati korxonalari kiberxavfsizligini oshirishda iqtisodiy risklar va kibergigiyenaviy faoliyatni takomillashtirish choralarini izchilligi bo‘yicha tavsiyalarni asoslash;

elektr energetika sanoati korxonalarining tashkiliy-iqtisodiy faoliyati axborot xavfsizligini raqamlashtirish mexanizmlarini takomillashtirish bo‘yicha taklif va tavsiyalar ishlab chiqish.

Tadqiqotning obyekti sifatida “Toshkent IES”AJ tashkiliy-iqtisodiy faoliyati axborot xavfsizligi tanlangan

Tadqiqotning predmetini energetika sanoati tizimi korxonalari tashkiliy-iqtisodiy faoliyati axborot xavfsizligi mexanizmlarini raqamlashtirishni faollashtirish jarayonida vujudga keladigan iqtisodiy munosabatlar tashkil etadi.

Tadqiqotning usullari. Tadqiqotda analiz va tizimli tahlil, modellashtirish, analogiya, umumlashtirish, abstragatsiya, omilli, modelli va aksiomatik tahlil, ekspert va dasturiy baholash, statistik taqqoslash, iqtisodiy-matematik modellashtirish, algoritmlash va bashoratlash kabi usullardan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

energetika sanoati korxonalari kiberhimoyaviy salohiyati, kiberxavfsizlik va risk darajasiga ko‘ra iqtisodiy kiberxavfsizlik darajasining $0,7 \leq C \leq 0,95$ oralig‘ida bo‘lishi maqsadga muvofiqligi va unga ko‘ra himoya tizimining strategik ta’minoti muvofiqligi asoslangan;

elektr energetika sanoati korxonalari axborot xavfsizligining tashkiliy-iqtisodiy mexanizmini faollashtirish strategiyasi jarayonni maqsadli qiymat o‘lchovlariga ko‘ra baholash, multiseriyaning xronologik ketma-ketligini asoslash, kiberhimoyaviylikni xalqaro va milliy darajalarini qiyoslash kabilarga ko‘ra takomillashtirilgan;

strategik jihatdan ishlab chiqarishning modernizatsiyalash darajasini oshirish, iqlim o‘zgarishlarining ta’siri va arzon xizmatlardan teng foydalanish imkoniyatini kengaytirish kabilarga ko‘ra “Toshkent IES” AJ tashkiliy-iqtisodiy faoliyati kiberxavfsizligini ta’minlanishda 2024-2029 yillarga mo‘ljallangan investitsion loyihalar prognozi asoslangan;

tashkiliy-iqtisodiy faoliyat alternativalari va taklif qilingan multikollakt strategiyani e’tiborga olgan holda “Toshkent IES” AJ elektr energetika komponent jarayonlarining tashkiliy-iqtisodiy kiberxavfsizligining 2023-2028 yillarga bo‘lgan davrdagi ekonometrik ssenariysi prognozi ishlab chiqilgan.

Tadqiqotning amaliy natijalari quyidagilarni o‘z ichiga oladi:

xorijiy va mahalliy olimlarning nazariy yondashuvlari asosida “kiberxavfsizlik iqtisodiyoti” tushunchasining iqtisodiy mohiyatini energetika sanoatining tashkiliy-iqtisodiy faoliyati uchun asoslangan;

issiqlik energetika sanoat korxonalarida tashkiliy-iqtisodiy mexanizmlarini takomillashtirishda axborot xavfsizligining tashkiliy va iqtisodiy munosabatlardagi ahamiyati va kibersalohiyati baholangan;

tashkiliy–iqtisodiy faoliyat mexanizmining tarkibiy komponentlarini xorij tajribasi hamda muallif yondashuviga ko‘ra iqtisodiy infratuzilmasiga joriy etish imkoniyatlari asoslangan;

energetika sanoati korxonalarida tashkiliy-iqtisodiy faoliyat mexanizmini samarali faollashtirishning o‘ziga xos xususiyatlariga ko‘ra samaradorlik oshirish chora-tadbirlari taklif qilingan;

elektr energetika sanoati korxonalarining komponentlarining raqamli texnologiyalarining iqtisodiy xavfsizligi va risk darajasini baholash yuzasidan qarorlar qabul qilishda muallif yondashuviga ko‘ra “qum soati” modeli va uni qo‘llab-quvvatlovchi multikollakt strategiyasi takomillashtirilgan;

axborot xavfsizligini faollashtirish va samaradorligini oshirish bo‘yicha taklif va tavsiyalar ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi tadqiqotda qo‘llanilgan nazariy yondashuv va usullarning maqsadga muvofiqligi, ma’lumotlarning rasmiy manbalardan, jumladan O‘zbekiston Respublikasi Prezidenti huzuridagi Statistika agentligi, “Toshkent IES” AJ va tizim korxonalaridan olingani, tadqiqot jarayonida ishlab chiqilgan xulosa, taklif va tavsiyalar amaliyotga tadbiq etilib, vakolatli davlat organlari tomonidan tasdiqlanganligi bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati ishlab chiqilgan xulosa, taklif va tavsiyalar energetika sanoati korxonalari tashkiliy-iqtisodiy faoliyati axborot xavfsizligi mexanizmi faolligi va samaradorligini oshirishning uslubiy asoslarini takomillashtirishga hamda mazkur mavzuga oid ilmiy tadqiqotlarning ilmiy-uslubiy asoslarini boyitishga xizmat qilishi hamda ishlab chiqilgan taklif va tavsiyalardan respublikada energetika sanoatining yetakchi korxonasi “Toshkent IES” AJ tashkiliy-iqtisodiy faoliyati axborot xavfsizligi mexanizmining kiberhimoyaviy samaradorligini oshirishni ta’minlashga yo‘naltirilgan amaliy chora-tadbirlar tizimini ishlab chiqilgani bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Elektr energetika sanoati korxonalarining tashkiliy-iqtisodiy faoliyati axborot xavfsizligini raqamlashtirish mexanizmlarini takomillashtirish bo‘yicha olingan natijalar asosida:

energetika sanoati korxonalari kiberhimoyaviy salohiyati, kiberxavfsizlik va risk darajasiga ko‘ra iqtisodiy kiberxavfsizlik darajasi $0,7 \leq C \leq 0,95$ oralig‘ida bo‘lishining maqsadga muvofiqligi va unga ko‘ra himoya tizimining strategik ta’minoti muvofiqligi bo‘yicha taklif “Toshkent IES” AJ bo‘yicha 2023-yil 12-apreldagi 284-son buyruq bilan amaliyotga joriy qilingan (O‘zbekiston Respublikasi Energetika vazirligining 2024-yil 3-apreldagi 04-10-2259-sonli ma’lumotnomasi; “Toshkent IES” AJning 2024-yil 27-martdagi 04-10-14/508-sonli ma’lumotnomasi). Natijada jamiyat tashkiliy-iqtisodiy faoliyatining axborot xavfsizligining 0,72 foizga o‘sishi, investitsion salohiyati 0,12 foiz va boshqaruvning tashkiliy-iqtisodiy faoliyatida 229 mln.so‘m tejalishiga muayyan darajada xizmat qilgan;

elektr energetika sanoati korxonalari axborot xavfsizligining tashkiliy-iqtisodiy mexanizmini faollashtirish strategiyasi jarayonni maqsadli qiymat o‘lchovlariga ko‘ra baholash, multiseriyaning xronologik ketma-ketligini asoslash, kiberhimoyaviylikni xalqaro va milliy darajalarini qiyoslash kabilarga ko‘ra takomillashtirilgan yondashuvdan “Toshkent IES” AJ rivojlantirish

strategiyasini ishlab chiqishda foydalanilgan (O‘zbekiston Respublikasi Energetika vazirligining 2024-yil 3-apreldagi 04-10-2259-sonli ma’lumotnomasi; “Toshkent IES” AJning 2024-yil 27-martdagi 04-10-14/508-sonli ma’lumotnomasi). Taklif axborot xavfsizligining tashkiliy-iqtisodiy mexanizmini faollashtirish strategiyasini ishlab chiqish sifatini yanada oshirish, jarayonni miqdoriy baholash aniqligini oshirish asosida maqsadli chora-tadbirlarni qo‘llash imkoniyatini kengaytirishga va samaradorlikni oshirishga muayyan darajada xizmat qilgan;

strategik jihatdan ishlab chiqarishning modernizatsiyalash darajasini oshirish, iqlim o‘zgarishlarining ta’siri va arzon xizmatlardan teng foydalanish imkoniyatini kengaytirish kabilarni e’tiborga olgan holda “Toshkent IES” AJ tashkiliy-iqtisodiy faoliyati kiberxavfsizligini ta’minlanishda 2024-2029 yillarga mo‘ljallangan investitsion loyihalar prognozidan “Toshkent IES” AJ rivojlantirish strategiyasini ishlab chiqishda foydalanilgan (O‘zbekiston Respublikasi Energetika vazirligining 2024-yil 3-apreldagi 04-10-2259-sonli ma’lumotnomasi; “Toshkent IES” AJning 2024-yil 27-martdagi 04-10-14/508-sonli ma’lumotnomasi). Investitsion loyiha kiritilishi foydaning ortishi sharoitida faoliyatning kiberhujumga nisbatan iqtisodiy-texnik bardoshligining ortishiga muayyan darajada xizmat qilgan;

tashkiliy-iqtisodiy faoliyat alternativalari va taklif qilingan multikollakt strategiyani e’tiborga olgan holda “Toshkent IES” AJ elektr energetika komponent jarayonlarining tashkiliy-iqtisodiy kiberxavfsizligining 2023-2028 yillarga bo‘lgan davrdagi ekonometrik ssenariyli prognozi “Toshkent IES” AJ bo‘yicha 2023-yil 12-apreldagi 284-son buyruq bilan amaliyotga joriy qilingan (O‘zbekiston Respublikasi Energetika vazirligining 2024-yil 3-apreldagi 04-10-2259-sonli ma’lumotnomasi; “Toshkent IES” AJning 2024-yil 27-martdagi 04-10-14/508-sonli ma’lumotnomasi). Taklifning joriy qilinish, jumladan 2023-yilda tashkiliy-iqtisodiy chora-tadbirlaring samarali tashkil qilinishiga ko‘ra AJ axborot xavfsizligini 0,7 foizga ortishiga muayyan darajad xizmat qilgan.

Tadqiqot natijalarining aprobatsiyasi. Tadqiqot natijalari 2 ta xalqaro va 2 ta respublika miqyosidagi ilmiy-amaliy anjumanlarda muhokamadan o‘tkazilgan.

Tadqiqot natijalarning e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 10 ta ilmiy ish, jumladan O‘zbekiston Respublikasi Oliy attestatsiya komissiyasi tomonidan tavsiya etgan ilmiy nashrlarda 3 ta va xorijiy jurnallarda 3 ta maqola nashr etilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, uchta bob, xulosa, foydalanilgan adabiyotlar ro‘yxatidan iborat. Dissertatsiyaning hajmi 130 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi va zarurati asoslangan, tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, mavzu bo‘yicha muammoning o‘rganilganlik darajasi keltirilgan, tadqiqot maqsadi, vazifalari, obyekti va predmeti tavsiflangan, tadqiqotning ilmiy yangiligi va amaliy natijalari bayon qilingan, olingan natijalarning nazariy va amaliy ahamiyati izohlab berilgan, tadqiqot natijalarining joriy qilinishi, nashr etilgan ilmiy ishlar va dissertatsiya tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **“Energetika sanoatining tashkiliy-iqtisodiy faoliyati kiberxavfizligi mexanizmlarining ilmiy-nazariy asoslari”** deb nomlangan birinchi bobida elektr energetika sanoat korxonalarida iqtisodiy kiberxavfsizlik, axborot xavfsizligi, axborot risklarining iqtisodiy asoslari, kiberhujumlarning iqtisodiy tahdidlari va talofatlari oqibatlarining ilmiy-nazariy jihatlari yoritilgan.

Bizning fikrimizga ko‘ra, axborot xavfsizligi iqtisodiyoti deganda har bir axborot texnologiyalari foydalanuvchilarining vositalaridan iqtisodiy zarar keltirishini oldini olishga asoslangan iqtisodiyot tushuniladi. Energetika sanoati korxonalarining kiberxavfsizlikka uchrashi boshqa sanoati korxonalariga qaraganda yuqoriroq foizni tashkil etib, unga ta’sir etuvchi omillarni tadqiq etish maqsadga muvofiqdir.

1-jadval

Energetika sanoati korxonalarining kiberhujumga uchrashiga ta’sir etuvchi omillar[6]

T/r	Kiberxujum omillari	Hujum ulushi	Kiberhujum maqsad va oqibatlari
1.	To‘lov varaqalari orqali ma’lumotlarga ega bo‘lish	22%	Elektr energiya to‘lovchilarining moliyaviy rekvizitlarining konfidentsialligi yo‘qoladi
2.	To‘lov kartalaridan pulni o‘marish	19%	To‘lov kartalarida elektr energiya o‘chib qolishiga qarshi pul mablag‘ining shakllantirilganligi
3.	Elektr energiya ta’minoti dispetcherlik xizmati ma’lumotlari o‘chirilishi, “rendom” holati	18%	Asosiy to‘lovchilarning qarzdorliklari uchun sun’iy qora to‘lov bozorining shakllantirishi
4.	Rejalashtirilgan manzilli xonadonni o‘marish	16%	Xonadonni chiroqsiz qoldirgan holda barcha aloqa vositalarini bloklash
5.	“Masaxaraboz xaker” ya’ni xaker mashq qilib ko‘radi, masxara qiladi	10%	Xakerlik faoliyati borasida o‘zining hamkasblari orasida tashrif qog‘ozini shakllantirish

Mazkur jadval “Xalqaro elektraloqa ittifoqi” tashkilotining “Kiberxavfsizlikning global dasturi”ni asoslashda keltirilgan ma’lumot bo‘lib, unda 210 tadan 125 ta mamlakatning statistika asosida shakllantirilgan.

Intellektual texnologiyalar sanoatning asosiy qismida yengillik va mukammallik yaratib berishiga qaramasdan, uning amaliyotga tadbiq etgan intellektual texnologiyalari kiberhujumlarga nisbatan og‘ma xususiyatga ega bo‘lib, o‘ziga xos risklarni keltirib chiqarishi mumkinligi kuzatiladi. Energetika sanoati korxonalariga kiberhujumlardagi asosiy ko‘zlangan nishon moliyaviy manbalar sanalmaydi, aksincha moliyani uzluksiz ta’minlashga ega axborot sanaladi.

[6] https://www.ifap.ru/pr/2008/080908aa.pdf

2-jadval

Kiberjinoyatning egri o‘sishiga ta’sir etuvchi omillar[7]

№	Omillar	Omilning kelib chiqishi	Kiberjinoyatlarning oqibatlari	Kiberjinoyatga qarchi xavfsizlik choralari
1.	Kiberjinoyatni fosh etish murakkabligi.	Internet tarmog’ida shaxsning anonim tarzda faoliyat olib borish imkoniyatining mavjudligi	Moliyaviy talofatlar	Ma'lumotlarni himoya qilish bo'yicha qat'iy qonunlarni amalga oshirish: O‘zbekistonga odamlarning shaxsiy ma'lumotlarining xavfsizligi va maxfiyligini ta'minlaydigan keng qamrovli ma'lumotlarni himoya qilish qonunlari kerak. Ushbu qonunlar tashkilotlarni mijozlar ma'lumotlarini himoya qilish uchun javobgarlikka tortishi va ma'lumotlarning buzilishi va rioya qilmaslik uchun jiddiy jazolarni belgilashi kerak.
2.	Kiberhimoyaviy befarqlik	Korxona va tashkilotlarning kiberhimoyaviy darajasining baholanmasligi va kiberxavfsizlik choralarining yetarlimas	Axborot konfidentsialligini saqlash hamda ma’lumotlar oqimini nazorat qilish	
3.	Transfarmatsion akseliratsiya	Dunyodagi raqamli transformatsion texnologiyalar to‘lqini elektron tijorat, elektron klasterizatsiya, onlayn-banking va raqamli tranzaksiyalarning takomillashuviga turtki bo’ldi.	Ustunlikdan foydalanish. Ilg’or texnologiyalar hayotni yanada qulaylashtirgan bo'lsa-da, kiberjinoyatchilar uchun onlayn platformalardagi zaifliklardan foydalanish, shaxsiy ma'lumotlarni o'g'irlash va moliyaviy firibgarlik.	Hamkorlik va axborot almashish: Davlat organlari, huquqni muhofaza qiluvchi organlar va xalqaro tashkilotlar hamkorligi muhim. Rivojlanayotgan tahdidlar, eng yaxshi amaliyotlar va kiberjinoyat tendentsiyalari ma'lumotlarini almashish kiberjinoyatchilarga qarshi jamoaviy mudofaani yaratishga yordam beradi.
4.	Kiberxafsizlikning qonuniy asosidan voqif bo’lmaslik.	Kiberjinoyatlarning o‘sishiga yordam beradigan asosiy omil - bu kiberxavfsizlikdan xabardorlik va ta'limning etishmasligi. Ko'pgina odamlar va tashkilotlar potentsial tahdidlarni aniqlash yoki tegishli profilaktika choralarini ko'rish uchun zarur bilimga ega emas. Bu bo'shlig'i ularni kiberjinoyatchilar uchun yengil nishonga aylantirdi	Ijtimoiy va psixologik ta'sir. Kiberjinoyat nafaqat shaxslar va tashkilotlarga moliyaviy ta'sir ko'rsatadi, balki chuqur ijtimoiy va psixologik ta'sir ko'rsatadi. Kiberbulling, onlayn ta'qib va kibertalking qurbonlari ko'pincha hissiy iztirob, tashvish va depressiyadan aziyat chekishadi.	Kiberxavfsizlik bo'yicha xabardorlik va ta'lim: Kiberxavfsizlik bo'yicha xabardorlikni oshirish va barcha darajadagi ta'lim shaxslar va tashkilotlarga o'zlarini kiber tahdidlardan himoya qilish imkoniyatlarini kengaytirish uchun juda muhimdir. Konsultatsion kampaniyalarini o'tkazish xavfsiz internet amaliyotlari va kuchli parollarning ahamiyati, dasturiy ta'minotni muntazam yangilash va xavfsiz ko'rish odatlari haqidagi bilimlarni tarqatishga yordam beradi.
5	Sayoz kiberxavfsizlik infratuzilmasi	Kiberjinoyatlardan himoya tizimini qo’llashga investitsiya qilinmasligi va uning nojoiz deb hisoblanilishi natijasida korxona va xizmat ko’rsatish tashkilotlarining moliyaviy talofat ko’rishi	Strategik ahamiyatga ega infratuzilmalarning buzilishi. Elektr tarmoqlari, transport tizimlari va hukumat tarmoqlari kabi muhim infratuzilmaga qaratilgan kiberhujumlar milliy xavfsizlikka jiddiy tahdid soladi.	Kiberxavfsizlik infratuzilmasini mustahkamlash. Mamlakatga kuchli kiberxavfsizlik infratuzilmasiga, tahdidlarni aniqlash tizimlariga, xavfsiz tarmoqlarga va muntazam xavfsizlik auditiga sarmoya kiritishi kerak. Hukumat idoralari, xususiy tashkilotlar va kiberxavfsizlik bo'yicha mutaxassislar o'rtasidagi hamkorlik kiberjinoyatchilardan bir qadam oldinda bo'lish uchun juda muhimdir.

[7] Suhani Dhariwal. Rise of Cybercrime in India: Reasons, Impacts & Safety Measures. https://www.writinglaw.com/rise-of-cybercrime-in-india/

Energetika korxonalarining kibergigiyenasiga olinishi lozim bo‘lgan ma’lumotlar energiya ta’minot, iste’molchilarning konfidentsial ma’lumotlari sanaladi.

Axborot kibergigiyenasini to’g’ri boshqarish uchun energetika sanoati kiberxavfsizlik iqtisodiyoti kaskad samara orqali baholash, ya’ni elektr ta’minoti tizimidagi zanjirlarni kuzatish orqali amalga oshiriladi. Energetika sanoati korxonalarining kiberhujumga uchrashi boshqa sanoati korxonalariga qaraganda yuqoriroq foizni tashkil etib, unga ta’sir etuvchi omillarni tadqiq etish maqsadga muvofiqdir (2-jadval).

Dissertatsiyaning **“Mamlakat iqtisodiyotini raqamli texnologiyalar asosida rivojlantirish sharoitida energetika korxonalari kiberxavfsizligini tashkiliy-iqtisodiy mexanizmlarini baholash”** deb nomlangan ikkinchi bobida “Toshkent IES” AJning kiberxavfsizligining tashkiliy-iqtisodiy mexanizmlarini holatini baholash va uning faoliyatini moliyaviy-iqtisodiy va axborot xavfsizligini ta’minlashning amaldagi holati tahlilini o‘rganish asosida ilmiy takliflar ishlab chiqilgan.

3-jadval

Kiberiqtisodiy hujumlarning kelib chiqish omillari (2016-2023 yy, foizda)[1]

T/r	Kiberiqtisodiy hujum omillari	Hujum ulushi	Baholash usuli	Baholash usulining tarkibi
1	Oylik ish haqi			
1.	Oylik ish haqining pastligi	22%	$M_s = \frac{M_t - M_r}{X}$	M_s-kiberhujumni amalga oshirgan ishchilarning oylik ish haqi; M_t-xakerning tarif bo‘yicha ish haqi; M_r-real vaqt olgan ish haqi; X-kiberhujum qilgan xakerlarning soni.
2.	Oylik ish haqi pastligi bois auditorga buyurtma	4%	$M_{sk} = \frac{M_{td} - M_{sr}}{X}$	Msk-kiberhujumni tadqiq etishda oylik ish haqi inobatga olish; Mtd-ishchilarning tarif bo‘yicha olishi lozim bo‘lgan ish haqi va hisobot qiymati; Mr-real ish haqini soliq bazasidagi qiymatlari; X-kiberhujum qilganlar soni.
2	Iqtisodiy maxinatsiya			
1.	Korxona tomonidan buyurtma asosida	14%	$I_m = \frac{I_t - M_t}{T_t - S_t}$	I_m-iqtisodiy maxinatsiya koeffitsienti; I_t-iqtisodiy to‘lovlar; M_t-moliyaviy operatsiyalar qiymati; T_t-hisobga olingan tovar moddiy boyliklari qiymati; S_t-realizatsion tovar soliq to‘lovlari.
2.	Sug‘urta korxonalaridan pul undirish	15%	$S_m = \frac{I_t - M_t}{B_{tl} - S_{g't}}$	S_m-sug‘urtalash orqali maxinatsiya koeffitsienti; B_{tl}-talofat yetkazilgan TMB; $S_t g'$-sug‘urtalangan obyekt.
3.	Moliyaviy shantaj	7%	-	Kredit operatsiyalarining va xususiy pul mablag‘larining iqtisodiy nofaol tarzda sarflanishi.
3	Tajriba va sinov			
1	Tizimning mustahkamligini sinash	5%	-	Xakerlarning tizimli urinishlari va imkoniyatlarini sinab ko‘rish

Bugungi kunga kelib, mamlakatimizda raqamli iqtisodiyotning izchil rivojlanib borishi axborot iqtisodiyoti, elektron tijorat sohalarida qo‘shimcha qiymatning ortishiga salmoqli ta’sir ko‘rsatmoqda. Shu bilan bir qatorda, eng yirik raqamli iqtisodiyot sanoatning elektroenergetika soha va tarmoqlarining qo‘shilgan qiymat yaratishga to‘g‘ri keladi.

[1] Лахани К. Янсити М. Цифровое преимущество. Исскуство конкурировать в эпоху исскустного интеллекта. Бамбора, М.: 2021 г, 319 стр, Павлюк Ю. Digital всемонущий. 101 инструмент для повышения продаж с помощью цифровых технологий. Эксмо, 2021 г, 208 стр.

4-jadval

Axborot iqtisodiyoti va elektron tijorat sohalarida yaratilgan yalpi qo‘shilgan qiymatining hajmi (*2018-2023 yy, mlrd. so‘m)*[2]

Yillar	2018	2019	2020	2021	2022	2023
Axborot sohasida iqtisodiyot va elektron tijorat	7,934	8,701	11,220	12,109	12,998	13,461
Shundan: Elektr energetika	1,099	2,471	3,729	5,583	5,990	6,780

Elektr energetika sohasida ishtirok etayotgan raqamli texnologiyalarning samaradorligi qo‘shilgan qiymat yarata olish qobiliyatining qiymat ko‘rinishidagi ko‘rsatkichlari oshib borishi sohaga iste’molchilarning iste’molini yaxshilashdan tashqari, uni ishlab chiqarish, taqsimlash, yo‘naltirish hamda uzatish bilan bog‘liq ilg‘or texnologiyalarning innovatsion infratuzilmani butunlay egallab borayatganligini, zamonaviy va aqlli stansiyalarning sonini oshib borayotganligi bilan tavsiflanadi. Texnologik ta’minot o‘sgani sari uning himoya tizimi sustlashuvi va hali hal etilmagan masala ustiga yangi muammolarning qo‘shilishi holatida kiberxavfsizlik ko‘rsatkichlaridagi o‘rni pastlagan.

5-jadval

“Issiqlik elektr stansiyalar” AJ mavjud quvvatlardan foydalanish holati (2023-yil)[3]

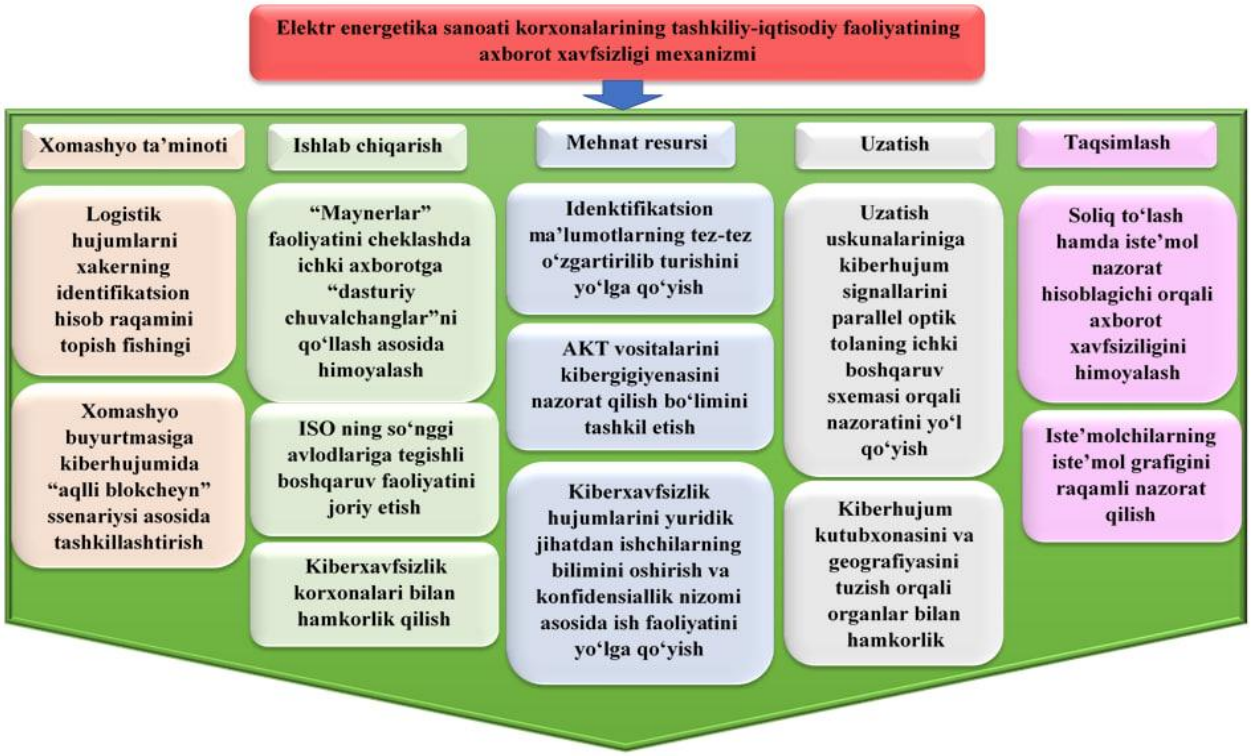
№	IES va IEM nomlari	O‘rnatilgan quvvati, MVt	Amaldagi quvvati, MVt
1.	“Sirdaryo IES” AJ	3 415	3 150
2.	“Toshkent IES” AJ	2 430	2 100
3.	“Navoiy IES” AJ	2 268	1 850
4.	“Taxiatosh IES” AJ	1080	1000
5.	“Farg‘ona IEM” AJ	429	350
6.	“Muborak IEM” AJ	70	60
7.	“Toshkent IEM” AJ	67	60
8.	“Talimarjon IES” AJ	1 760	1 750
9.	“To‘raqo‘rg‘on IES” UK	950	870

Issiqlik elektrostansiyalarning quvvatlarini oshirish yuzasidan tegishli chora-tadbirlarni amalga oshirish natijasida amaldagi quvvatiga nisbatan yuqori quvvatda ishlashi ta’minlangan bo‘lib, tadqiqot ishining obyekti sanalgan “Toshkent IES” AJ quvvati jihatdan ko‘rsatkichlari ikkinchi o‘rinni egallagan. Shunga ko‘ra, “Toshkent IES” AJ yirik ishlab chiqaruvchilar qatoridagi energetika korxonasi deyish mumkin.

Issiqlik energetikasi sohasida mamlakatimizda amalga oshirilayotgan raqamli iqtisodiyot tizimining o‘zgarishlari qanchalik yirik bo‘lmasin, mavjud elektrotexnikalar, ularning qo‘llanishi, ilg‘or texnologik ta’minotning kiberxavfsizligi bilan bog‘liq muammolar o‘z yechimini topa olgani yo‘q. “Toshkent issiqlik elektrstansiyalari” AJ tarkibida 7 ta blok bo‘lsada, barchasi axborot xavfsizligiga nisbatan bardosh bera oladigan texnologiya va dastur bilan ta’minlanmagan.

[2] O‘zbekiston Respublikasi Prezindenti huzuridagi Statistika Agentligi

[3] “Issiqlik elektrstansiyalari” AJ ma’lumotlari



1-rasm. Elektr energetika korxonalari kiberxavfsizligining tashkiliy-iqtisodiy mexanizmi[1]

Bu holatning o‘z holicha qoldirilishi tufayli sohada energiyani o‘marish va uning iste’moli uchun to‘lovni sun’iylashtirish, energiya iste’molini sun’iy bebaholash, to‘lov rekvizitlaridan pul mablag‘larini qisman o‘marish chuvalchanglarini yo‘naltiruvchi dastur yordamida kiberhujumlarning amalga oshirilishi natijasida individual ma’lumotlarning maxfiyligini ta’minlash yuzasidan yirik muammolar keltirib chiqaradi. Shunga ko‘ra, “Toshkent issiqlik elektr stansiyalar” aksiyadorlik jamiyatining tashkiliy-iqtisodiy faoliyatiga kiberxavfsizlik mexanizmlarni ishlab chiqish va uni raqamlashtirish algoritmini qo’llash tavsiya etiladi (1-rasm).

Xomashyo ta’minotini kiberxavfsizligini ta’minlash Logistik hujumlarni xakerning identifikatsion hisob raqamini topish fishingi orqali hujum uyushtiriayotganlarning tajribasini, hujum sxemasini, strategiyasini aniqlash hamda uning manzilini operativ tarzda topish imkonini beradi. Bu tashkiliy-iqtisodiy jihatdan barcha parametrlarning muvaffaqiyatli amalga oshirilishiga qaratilgan tadbir sanaladi.

“Toshkent IES” AJning axborot kompyuterlari texnologiyalaridan foydalanish ta’minoti darajasining funksional qo‘llab-quvvatlash tizimi elektrostansiyalar uchun mo‘ljallangan bo‘lib, aqlli texnologiyani ham qo‘llay oladigan standartiga ega. Uning iqtisodiy samaradorligi 6 ta an’anaviy hamda 3 ta zamonaviylashtirilgan muqobil parametrlarga ega kompyuterni o‘rnini bosa olishi bilan belgilanadi. Korxonaning ishlab chiqarish va xizmat ko‘rsatish faoliyatida raqamli texnologiyalarning tashkiliy-iqtisodiy faoliyatda axborot xavfsizligini ta’minlash mexanizmi va himoya dasturiga ega emas.

[1] Muallif ishlanmasi

6-jadval

“Toshkent IES” AJning axborot kompyuterlari texnologiyalaridan foydalanish ta’minoti darajasi[2]

№	Tashkilotning AKT vositalari, uskunalari dastgohlari				Texnik-iqtisodiy tahlil
	Nomi	Yaroqliligi darajasi (%)	Dona	Ishlab chiqarilgan joyi	
1.	Avtesh Intel Sore i7 6700K	45	34	Tayvan, 2012y	Litsenziyalangana antivirus dasturlari o‘rnatilishi lozim
2.	HP ZBook Studio x360	37	14	AQSh, Kaliforniya	Issiqlik elektrostansiyalari uchun mo‘ljallanmagan
3.	Minelab Equinox 800-metall detektor	100	2	Italiya, 2020 y	-
4.	AWS “Buxgalteriya”	28	4	AQSh, 2001	1S 8.4 ga almashtirish lozim
5.	GPS-treker	15	5	AQSh, 2004	GPS-trekerlarni zamonaviylariga almashtirish va sonini oshirish
6.	Elektrod qozonlar	22	2	Rossiya, 2000	Almashtirish lozim
7.	Xomashyo tozalash qozoni	9	2	Finlandiya, 1994	Ekologik tozalash qozonlariga almashtirish lozim
8.	470 Bl1,7,11 Quvvat bilan ishlash	78	2	Rossiya, 2010	Ekspluatatsiyadan chiqarish lozim
9.	Energobloklar	50	5	Rossiya, 2002	Konservatsiya qilish lozim

Korxona tarkibidagi hech bir AKT kiberhimoyaviy qo‘llab-quvvatlash dasturi, mexanizmiga ega bo‘lmaganligi samaradorlikning barcha ko‘rsatkichlariga aksil ta’sir ko‘rsatgan holda korxonani inqirozga keltirishi mumkin. Bunda himoya tizimini olib borish xalqaro daraja saqlanishi lozimdir. Buning uchun xalqaro stanlartlarga asosan tegishli texnologiyalarni joriy etish hamda ularni qo‘llab-quvvatlovchi dasturlarni muqobillashtirish talab etiladi. Mazkur holat uchun standartizatsion transformatsiya mexanizmini qo‘llash talab etiladi.

Dissertatsiyaning “Elektr energetika sanoati korxonalarining tashkiliy-iqtisodiy faoliyatining axborot xavfsizligi mexanizmlarini raqamlashtirish” deb nomlangan uchinchi bobida korxonalarning axborot xavfsizligi mexanizmlarini raqamlashtirishga oid modellashtirish va uning istiqbollari borasida ma’lumotlar keltirilgan.

Multikollakt modeli ma’lumotlarni tezkor saralash orqali barqaror ma’lumot asosida himoya tizimini shakllantirish sanalib, uni AQSh iqtisodchi olimi Xel Variana tomonidan ishlab chiqilgan. Uning asosiy maqsadi tezkor ma’lumotlarni tasniflash asosida zaruriy qarorlarni qabul qilish uchun tegishli ssenariylarni qo‘llash rejalari majmuasini shakllantirish. Uning model sifatida koeffitsientlarini aniqlash uchun yirik masshtabda tahlil olib borishga hojat bo‘lmay, uning uchun ma’lumotlarning o‘zi yetarli sanaladi. Uning himoya tizimi kiberhujum qilayotgan xakerning taktikasini tahlil qilib, undan nus’ha ko‘chirish evaziga o‘zining tizimiga kirib borishiga yo‘naltirish sanaladi. Natijada, xaker o‘zining tizimiga manzilli kirib ketishiga to‘g‘ri keladi. Uning iqtisodiy asosini iqtisodiy risklarni so‘ndirish hamda

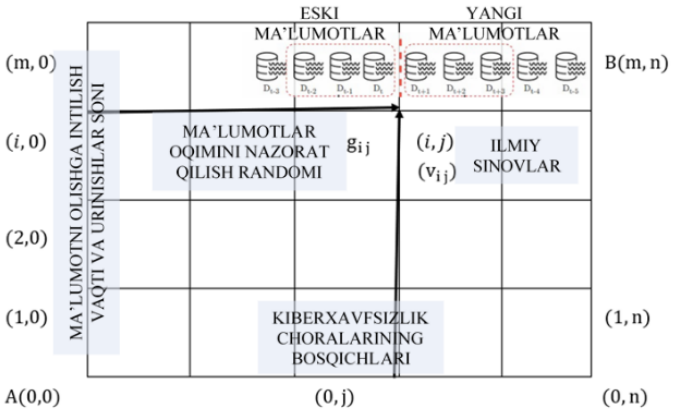
[2] “Toshkent IES” AJ ma’lumotlari

doimiy xarajatlarni himoya qilish sanaladi.Mazkur dissertatsiya ishida ushbu model strategiya darajasiga qadar takomillashtirildi. Unga ko’ra multiswriyaning xronologik ketma-ketligini asoslash, kiberhimoyaviylikni calqaro va milliy darajalarini qiyoslash mumkin (2-rasm).

2-rasm. Elektr energetika korxonalari kiberxavfsizligining tashkiliy-iqtisodiy mexanizmini faollashtirish strategiyasi[3]

Kiberxavfsizlik iqtisodiyotida izlanishlar olib borish davomida monotizimning ilmiy-amaliy hamda kibergigiyenaga amal qilgan holda Kuxning Drift modelidan foydalangan holda issiqlik elektrostansiyalarning axborot xavfsizligining iqtisodiy samaradorligini ta’minlanishini asoslash tavsiya etiladi. Mazkur model aslida raqamli texnologiyalar asosida takomillashtirilgan barcha texnika vositalari uchun mo‘ljallangan bo‘lib, uning asosiy ustunlik jihati iqtisodiy konseptual asosga hamda axborot texnologiyalarining dasturiy tuzilmasi bilan mutanosib hisoblay olish jihatlari sanaladi.

Drift modeli asosida hisob-kitob qilishda raqamli texnologiyalar matritsasini tuzish taqozo etiladi.



3-rasm. Drift modelining raqamli texnologiyalarni optimallashtirish matritsasi[4]

[3] Muallif ishlanmasi

[4] Tashakkori A, C. Teddlie, C. B. Teddlie, Mixed methodology: Combining qualitative and quantitative approaches, volume 46, Sage, 1998

Bu yerda:

m-xom ashyo materiallariga javob beruvchi raqamli texnologiyalarning himoya darajasi; n-ishlab chiqarish jarayonlarining raqamli texnologiyalari himoya darajasi; g-kiberxavfsizlikning iqtisodiy risk darajasi; i-texnologiyalar soni; j-texnologiyalarning qiymati; A-daromadliligi; B-likvidligi.

i dan j ga o‘tishda xarajatlarning gorizontaldan vertikalga o‘zgarishi kiberxavfsizlik risk darajasini aniqlashga yordam beradi. Ya’ni har qanday kiberhujum an’anaviy ishlash tizimini o‘z holiga qo‘yganda ro‘y bermaydi, unda qaysidir element albatta o‘zgartiriladi va matritsaviy o‘zgarish ya’ni antimatritsa qiymatlari kelib chiqadi. Uning o‘zgarishi natijasi v_{ij} ning, ya’ni o‘zgarishlarga (kiberhujumlarga) bardosh bera olish darajasini belgilab beradi. Bu esa kiberhujumlarning iqtisodiy jihatdan himoyalash dasturining standartiga hamda dasturiy tilining ishlab chiqaruvchining o‘rnatgan va bergan dasturiy buyruqlarini ta’minlashning har tomonlama inobatga olinganligiga, shuningdek, iqtisodiy axborot tizimi bloklariga javob bera olishiga bog‘liqdir.

A nuqtada daromadlilik 0 ga teng bo‘lib, bunda iqtisodiy zararning yetkazilmaganligini, iqtisodiy ma’lumotlarning daxlsizligini hamda elektrostansiyadan uzatma panellarinidan elektr energiyasini yo‘naltirishga tegishli o‘zgarish bo‘lmaganligini anglatadi. Bu esa samaradorlikni bir muncha bo‘lsada oshirishga xizmat qiladi, ya’ni V nuqtada xom ashyo va ishlab chiqarish jarayonlaridagi texnologiyalarning himoya darajalarining o‘zaro aloqadorligidan kelib chiqadi.

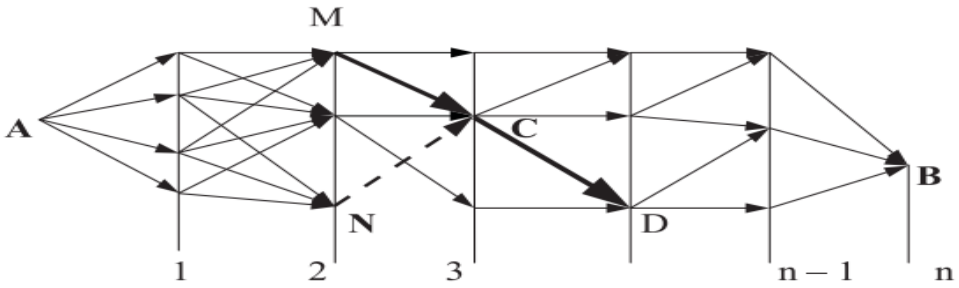
m, n hamda iqtisodiy yo‘qotishlar uchun g_{ij} , v_{ij} (i=0,1,2,...,m; j=0,1,2,..., n) himoya tizimida asosiy komponent himoya dasturlari bilan navbatma-navbat o‘zining vazifasini o‘tashi ko‘zda tutiladi (eskirgan va yangi dastur bo‘lishidan qat’iy nazar). Ularning matematik matritsaviy jihatdan n(m+1) ning ortib borishi natijasida g_{ij} va m(n+1) ning ortishi natijasida v_{ij} dagi o‘zgarishlar mutanosibligini saqlaydi.

O‘zgarishlarning oraliq farqini aniqlashda barcha tanlovlarni qayta tarkiblash usulidan foydalanish A nuqtadan V nuqtagacha jarayonlarning matritsaviy trayektoriyasi qiymatlarini va risk koeffitsiyentlarini aniqlashga xizmat qiladi. Bizning holatimizda himoya tizimlari tanlovlar majmuasidan tegishlisi faollashtirilib, o‘zini biroz ichki dasturlarni algoritmini buzishiga sabab bo‘lishi mumkin. Ularni tizimda yolg‘on qopqon ma’lumotlarni almashinuvi evaziga himoya qilinadi.

$$S = \frac{(m+n)!}{m!n!} (1)$$

Bu yerda S=kiberxavfsizlik himoyasining tanlovlari orasidagi yo‘qotishlari; m=n=10; Bizning holatimizda S=184756 ga teng.

Keyingi hisob-kitob qilish tartibida m=n=1 ga tenglashtirilib, bunda asosiy optimallashtirilishi lozim bo‘lgan tanlov bitta bo‘lishi lozimligini anglatadi. (4-rasm).



4-rasm. Bosqichma-bosqich muqobil tanlovlar algoritmi[5]

Tanlovlarning optimalligi aniqlangach ularni tashkiliy-iqtisodiy faoliyat yuzasidan ekonometrik jihatdan bashoratlaymiz.

v_i, g_j, N_j tanlovlarning chiziq yotqiziqlarida absissa o‘qida approksimatsiyalashgan siniq chiziqlarni x (i=1,2,...n) sifatida olinsa, uning chegarlanishini 10 birlik ichida 3 turga ajratamiz:

1. $v_m \geq A_m$ yoki $v_n \geq A_n$ m va n ba’zi tanlovlarni hisobga olganda;
2. $g_j \leq (v_{j+1} - v_j)/B_{j+1} \leq B_j$;
3. $N_j \leq (v_{j+1} - v_j)/B_{j+1} - (v_{j+1} - v_j)/B_{j+1} \leq D_j(C, M)$.

Bu yerda noma’lum ordinatalar siniq tanlov chiziqlari orasidan muqobilini topishga xizmat qiladi. Ikkinchi turdagi tanlovning chegaralanishi dastlabki hosilani diskret analogli chegarasi sanalib, uning x bilan burchak bilan yasagan tangens burchak og‘ishi approksimativ siniq chiziqqa keltiradi. Uchinchi turdagi tanlov turli elementlarning kombinativ hosilasining natijaviyligi tufayli turli burchaklarga og‘ish xususiyati mavjud emas. Shunga ko‘ra, 3 tanlovni fiksatsiyalashda eng kam og‘ishlarga ega burchak qiyaligiga ega chegaviy chiziqlarning diskret analogiga to‘xtash ma’qul sanaladi. Uning burchak og‘ishi qiymatda 0,001 asosida ma’lumotlarning daxlsizligini saqlashga hamda kiberhujumda hujum manzilini yolg‘on mo‘ljaliga, ya’ni mavjud ahamiyatsiz tanlovga yo‘naltirishga qaratiladi.

Bizda ya’ni bir masala oldimizda ko‘ndalang bo‘ladi, 3 tanlovdan 1 biri o‘zini oqladi. Qolgan ikki tanlovlarni “ishtirokchi afzalligi” orqali kutilayotgan riskni baholash imkoniyati yuzaga keladi. Demak, bizda ikki tanlovdan 50 foizi korxona foydasiga 2 tanlovning xizmat qilishi hamda 1 tanlovning bizga xizmat qilmasligining 50 foizi ehtimoli tursa, biz uni sarhisoblashda matematik kutish (W) formulasidan foydalanamiz (3.2)

$$w = \sum_{i=1}^{N}(B_i \times A_i)(3.2)$$

B_i-tanlovning ijobiy yoki salbiy natija berishi; A_i-tanlovning pul qiymati yoki zarari; N-ehtimolli natijalarning soni.

W=(0,5*2)+(0,5*(-1))=1+(-0,5)=0,5

Endilikda uning yo‘qotishlarini, himoya darajasini va kombinatsion elementlar o‘zgarishini hisoblash talab etiladi.

W=((1/38)*35)+((37/38)*(-1))=(0,02631578947*35)+(0,9736842105*(-1))
=(0,9210526315)+(-0,9736842105)=-0,05263157903.

Birinchi tanlov holatida qolgan ikki tanlovning ham befoyda bo‘lishiga olib keladi, shunga ko‘ra, butunlay 0 ga teng tanlovni aks ettirmagan ma’qul, ya’ni uni

[5] Структченко В.И. Методы оптимизации и прикладных задачах.-М.:МОЛОН-Пресс, 2012-320 с.

ma’lum qiymatga to‘ldirish tavsiya etiladi. Yo‘qsa, korxona o‘rtacha 5,26 foiz iqtisodiy zarar ko‘rish ehtimoli mavjud. Bordiyu, mazkur tanlovlarni sonini 5 taga oshirsa u holda o‘rtacha 26,3 foiz iqtisodiy talofatga uchrashi mumkin. Natijada, korxonaning tashkiliy-iqtisodiy faoliyatining yo‘qotishlari yuzaga keladi:

7-jadval

Drift modeli asosida ekonometrik kuzatishlar[6]

Modelni miqdoriy qiymatlarini yetkazish ko‘rsatkichlari										
Statistik yetkazish	SE	Minimum	Maksimum	Protsentil						
				5	10	25	50	75	90	95
Statsionar R-kvadrat	0,202	0,415	0,908	0,415	0,415	0,541	0,819	0,889	0,908	0,908
R-kvadrat	0,410	-,127	0,917	-,127	-,127	0,155	0,675	0,848	0,917	0,917
KCKO	0,846	0,379	2,609	0,379	0,379	0,577	1,047	1,910	2,609	2,609
COMO	2,874	0,696	7,877	0,696	0,696	0,936	2,485	5,804	7,877	7,877
MOMO	5,510	1,357	15,470	1,357	1,357	2,299	5,169	11,737	15,470	15,470
CMO	0,490	0,241	1,515	0,241	0,241	0,341	0,638	1,183	1,515	1,515
MMO	1,102	,475	3,403	,475	,475	,837	1,292	2,662	3,403	3,403

W=(-0,0526*1)+(-0,0526*10)+(-0,0526*5)=-0,0526-0,526-0,263=-0,8416

Bu holatda korxonaning tashkiliy-iqtisodiy faoliyatining axborot xavfsizligi 84 foiz zarar ko‘rish ehtimoliga uchraydi.

Har bir hujum qilingan elementga ma’lum bir qiymat qo‘yganda korxona 2 foiz kamroq natijaga erishishi mumkin xolos. Yuqoridagi hisob kitoblarga ko‘ra modelning statsionarligini hisoblashda tashkiliy-iqtisodiy faoliyatning elementlarini prognozlashtirib ko‘rish talab etiladi. Yuqorida keltirilgan ekonometrik kuzatishlarni tahlil qilganda, drift modeli asosida prognozlashning Barlett A. testiga ko‘ra statsionarligini tekshirish natijalarining ehtimoli ko‘rsatkichlardan foydalanishimiz mumkin, shuningdek xatoliklar foizi 3,4 foizdan kichik sanaladi. Bu umumholda ijobiy natijaviylikni namoyon etadi.

8-jadval

Drift modeli asosida “Toshkent IES” AJning tashkiliy-iqtisodiy faoliyati kiberxavfsizligini ta’minlanish darajasi (foizda)[7]

Model	2024	2025	2026	2027	2028
Taqsimlash	23,17	25,37	27,57	29,77	31,97
Uzatish	22,17	22,17	22,17	22,17	22,17
Mehnat resurslari	39,00	39,40	39,80	40,20	40,60
Ishlab chiqarish	36,67	37,37	38,07	38,77	39,47
Xomashyo	29,33	30,43	31,53	32,63	33,73

Xomashyo 2025-yilda kiberhimoyaning salkam 30 foizda saqlanib, unga egalik qilmoqchi bo‘lganlarning 19 foizini kamaytirishga erishishi kutiladi. 2026-yilga kelib mazkur ko‘rsatkich deyarli foizlarda o‘zgarishlar namoyon etmasada, barqaror ko‘rsatkichni 2028-yilga qadar saqlay oladi. Ishlab chiqarish jihatdan korxonaning tashkiliy-iqtisodiy faoliyatining kiberhujumga bardoshliligi sezilarli darajada oshib, ishlab chiqarish 2024-yildan boshlab 2028-yilga qadar o‘rtacha 0,9 foizga oshib boradi. Bu esa kibergigiyenani saqlashda 44% samaradorlik namoyon etgan hisoblanadi.

[6] Barlett A. Testiga ko‘ra SPSS Statistis 2.0 dasturida qilindi

[7] Muallif ishlanmasi

Eng zaif va kiberhimoyaga bardosh berishga moyilligi past mehnat resurslarining kiberxavfsizlik jihatdan tashkiliy-iqtisodiy faoliyatdagi darajasi sezilarli ravishda oshib, 2024 yilda 39 foizni tashkil etishi bilan 2028-yilga kelib 10 foiz ortiq natijaviylikni keltirishi kutiladi. Elektr energiyani uzatish tizimida korxonaning tashkiliy-iqtisodiy faoliyatidagi xavfdan holi bo‘lish darajasi barqaror 22,17 foizni tashkil etadi.

Minimal 30 ta tanlovlar orasida Z ni hisoblab ko‘ramiz: $Z = \frac{N*(R-0,5)-X}{\sqrt{\frac{X*(X-N)}{N-1}}}$ (3)

Bu yerda: N-umumiy humumlarning ketma-ketligi; R-huhumga qarshi himoyalangan muvaffaqiyatli urinishlar;

X=2*W*L;

W-umumiy himoyalangan darajasi;L-umu miy yo‘qotishlar darajasi.

R=-3,+2,+7,-4,+1,-1,+6,-1,0,-2,-1 tartibda 2022 yilda qilingan kiberhujumlardan foydalansak, qarshi himoya tanlovlari 7 tani tashkil etadi, umumiy holatda esa N=12 ga teng bo‘ladi. Ya’ni, bizning holatimizda issiqlik elektrostansiyaning tashkiliy-iqtisodiy faoliyatiga qilingan 30 ta kiberhujumga nisbatan 7 ta himoyaviy algoritmlar ish berib, 15 tadan 12 ta ma’lumotlarning xavfsizlik oqimi chegaralanadi. Qolgan 3 himoya tizimidan izdan chiqqan tanlovlarning ichki tarkibi yolg‘on ma’lumotlarni uzatishda bloklanish hosil qiladi.

X=2*6*6=72 %

Demak, korxonaning tashkiliy-iqtisodiy faoliyatiga 30 ta kiberhujumning uyushtirilishi natijasida tizimining himoyalanish darajasi 72 foizni tashkil etadi.

Endilikda, uni tekshirish maqsadida R=8 seriyalar ketma-ketligi faollashtirilib, uning xronologik tizimini aniqlashtiramiz (8-jadval).

Shuni ham ta’kidlash joizki, 0 qiymat neytral oraliq soni sanalsada, uning mazkur holatdagi oraliq pozitsiyasi manfiy qiymatni tashkil etadi. Bu yo‘qotishlarni hisobga olish foizini aniqroq baholash imkonini berishi jihatdan qo‘llanilgan matematik amal sanaladi.

9-jadval

Multiseriyaning xronologik ketma-ketligini asoslash[8]

1	2	3	4	5	6	7	8	8	10	11	12
-3	2	7	-4	1	-1	1	6	-1	0	-2	1
-	+	+	-	+	-	+	+	-	-	-	+
1	2	X	3	4	5	6	X	7	X	X	8

Aqlli elektrostansiyalarning texnik parametrari har tomonlama ustun bo‘lib, ularni kiberxavfsizligini boshqarish operativ himoyalanishi imkoniyati mavjud. Shuningdek, uning amaliyotga tadbiq etilishi natijasida korxonaning ishlab chiqarish imkoniyatlarining ijtimoiy-o‘zgarishlarida dinamik o‘sishga olib kelishi kutiladi (9-jadval).

Ishlab chiqarish xarajatlarining iqtisod qilinishi tabiiyki raqamli texnologiyalarning aniqlikka qaratilgan tizimi hamda avariya, ta’mirlash ishlari,

[8]John Bandler. Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security, 2017, American Bar Association, 416 p

texnik qo‘llab-quvvatlash singari jarayonlarni boshqarishda oldindan ogohlantirish orqali boshqaruv yondoshuvining asosiy qismi ishlab chiqarish xarajatlarining iqtisod qilishga olib keladi.

10-jadval

Aqlli elektrostansiyalarni joriy etishning samaradorligi istiqbollari, (2023-2028 yy, foizda)[9]

Ko‘rsatkichlar	2023	2024	2025	2026	2027	2028
Ishlab chiqarish xarajatlarini iqtisod qilish	6,2	6,5	6,8	7,0	7,0	7,1
Elektr energiyasining tannarxini pasayishi	1,7	1,7	2,0	2,1	2,1	2,1
Qo‘shimcha qiymatning yaratilishi	2,2	2,5	3,0	3,2	2,9	3,0
Daromad	15	17	16	15	18	17
Ishlab chiqarish unumdorligi	3,3	3,3	3,5	3,5	3,4	3,5
Ekologik xavfsizlikning ta’minlanishi	4,9	4,9	5,0	5,0	5,0	4,0

Yuqoridagi taklifni investitsiyani jalb etish orqali amalga oshirish amaliy tadbiq etilishini tezlashtirishi hamda mamlakda salmoqli energetik xizmat qilishni ta’minlashi mumkin. Shunga ko’ra tadqiqotimiz doirasida uning kapital investitsiyaga jalb etilishi holatidagi samaradorligini sarhisob qildik. Mazkur jadvaldan ko’rinib turibdiki, investitsion loyiha kiritilishi natijasida korxona foyda bilan chiqa oladi va uning faoliyatini kiberhujumga nisbatan iqtisodiy va texnik bardosh bera olishi ta’minlanadi.

11-jadval

Drift modeli asosida “Toshkent IES” AJning tashkiliy-iqtisodiy faoliyatining kiberxavfsizligining ta’minlanish uchun investitsion loyiha (ming AQSh dollarida, 2024-2029 yy uchun)[10]

Ko’rsatkichlar	2024	2025	2026	2027	2028	2029
Boshlang’ich investitsion mablag’	1 000					
Pul oqimi		200	200	200	200	200
Natija	1 000	250	250	250	250	250
Diskont foizi	10%					
	>0 – loyiha qabul qilinadi; <0 – rad etiladi					
IRR	7,93%					
tekshiruv:	0	1	2	3	4	5
To’lov qiymati hajmi						
Kredit summasi	1 000					
Kredit bo’yicha foiz	10%					
Yillik to’lov hajmi	**263,797**					
Boshlang’ich ushlanma		1 000	836,203	656,025	457,830	239,816
Quyi ushlanma		836,203	656,025	457,830	239,816	**0**

Bu investitsion loyihani amalga oshirishda quyidagi jihatlar strategik inobatga olingan holda moliyalashtirilishi maqsad qilib belgilanadi:

- iqlim o‘zgarishi - bu barcha mamlakatlarga ta'sir qiladigan potentsial va ekzistensial muammo, jumladan ekstremal ob-havo hodisalari, oziq-ovqat xavfsizligi, inson salomatligiga tahdidlar, mojarolar va boshqalar.

[9] Muallif ishlanmasi
[10] Muallif ishlanmasi

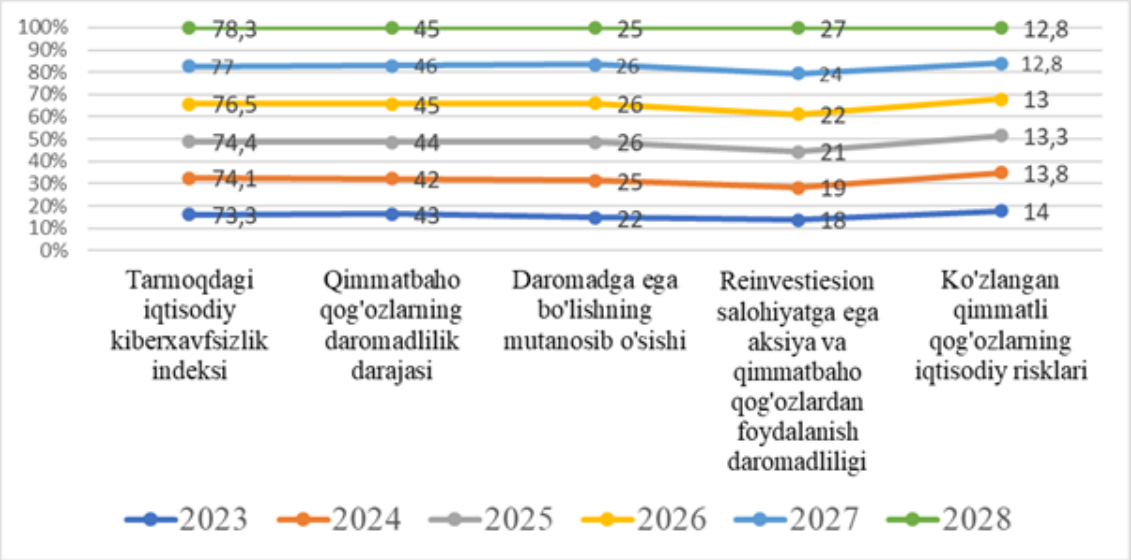
- sog‘liqni saqlash va bolalarni parvarish qilish bo'yicha arzon xizmatlardan teng foydalanish imkoniyatini kengaytirish, uzoq muddatli kasbiy ta'lim va malaka oshirish, yuqori sifatli ta'lim va kadrlar tayyorlash, kasaba uyushmalari va jamoa shartnomasini qo‘llab-quvvatlash, ish o‘rinlari sifatini oshirish va boshqalar.

- sanoatni modernizatsiya qilish, innovatsiyalar va investitsiyalar orqali Shimoliy Atlantika Shartnomasi Tashkiloti (NATO), AQSh-Yevropa Ittifoqi Savdo va Texnologiya Qo'mitasi, alyans orqali xavfsizlik sohasidagi hamkorlikni rivojlantirish;

- jismoniy infratuzilmaga, jumladan transport, keng polosali aloqa, suv va energiyaga sarmoya kiriting, jonlantirish uchun yarimo‘tkazgichlar faniga oid qonunni amalga oshirish;

- yarimo‘tkazgich sanoati, uglerod chiqindilarini 40% ga 30 ga kamaytirish uchun “Inflyatsiyani kamaytirish to‘g‘risidagi qonun”ni qabul qilish orqali kiberhujumlarga chidamlilikni oshirish.

Tadqiqot ishida muallif yondoshuviga ko‘ra iqtisodiy kiberxavfsizlik indeksi asosida dissertatsiyada ko‘zda tutilgan taklif va tavsiyalarni prognozli asoslash natijasida quyidagi natijaviylik kutiladi:



5-rasm. Muallif yondoshuviga ko‘ra iqtisodiy kiberxavfsizlikni baholash prognozi[11]

Tarmoqdagi iqtisodiy kiberxavfsizlik indeksi 76,5 foizga 77 foizga qadar o‘sishiga aqlli texnologiyalarni tadbiq etish orqali erishishdan tashqari, qimmatbaho qog‘ozlarni sotishni kengaytirish va aksiyalarning egaligini unga tegishli risklarini transformatsiyalash orqali aksiyadorlarni sonini oshirish bilan erishish kutiladi. Buning iqtisodiy asosi shundan iboratki, har bir xakerning asosiy manfaati bo‘lishiga qaramasdan turib, aholining zarar ko‘rishiga harakat qilmaydilar. Iqtisodiy kiberxavfsizlikni muallif yondoshuviga ko‘ra me’yorlashtirilishi aksiyalar parokandaligini hamda moliyaviy bozorda korxonaning inqirozini oldini olishga xizmat qilishi mumkin. Shunga ko‘ra, uning oraliq koeffitsiyenti shakllatirildi (11-jadval).

[11] Muallif ishlanmasi

12-jadval

Muallif yondoshuviga ko‘ra energetika korxonasi iqtisodiy kiberxavfsizligi indeksini me’yorlashtirish

Ko’rsatkich nomi	min	maks	Izoh
S_i- iqtisodiy kiberxavfsizlik indeksi;	70	95	Xavfsizlikning pastlashi tarmoqning barcha iqtisodiy parametrlarini zaiflashtiradi
F_i-korxona aksiyalari mutanosib qiymatining;	12	18	Aksiyalarning qiymati qanchalik yuqori bo‘lsa uni himoya qiluvchilar shuncha ko‘p bo‘ladi
E_i-qimmatbaho qog‘ozlarga ega bo‘lganlan soni;	20	200	Egalar soni qancha ko‘p bo‘lsa xakerlik faoliyatiga qarshi kurash yanada avj oladi
P_{Fi}-qimmatbaho qog‘ozlarning o‘rtacha qiymati;	40	55	Qimmatbaho qog‘ozlar o‘rtacha qiymati yuqorilashi risklarni pasaytirishga olib keladi
D_i-qimmatbaho qog‘ozlar va aksiyalarning so‘nggi sotilgan narxlarining o‘rtacha qiymati.	55	65	Qanchalik 50 foizdan ortiq bo‘lsayu 70 foizga qadar chiqmasa, uning kibertahdiddan nari bo‘lishi yuqori bo‘ladi
R_i-ko‘zlangan qimmatli qog‘ozlarning iqtisodiy risklari.	12	22	Risklar qarorlarni qabul qilish hamda investorlar uchun asosiy baholash me’zoni sanaladi

Demak, iqtisodiy kiberxavfsizlikning koeffitsiyentining muvofiqligi 0,7 hamda 0,95 oralig‘ida bo‘lishi tarmoqning xavfsiziligini baholash imkonini va himoya tizimini strategik aniqlashni ta’minlashi mumkin.

XULOSA

1. Bizning fikrimizga ko‘ra, axborot xavfsizligi iqtisodiyoti deganda har bir axborot texnologiyalari foydalanuvchilarining vositalaridan iqtisodiy zarar keltirishini oldini olishga asoslangan iqtisodiyot tushuniladi.
2. Korxonaning tashkiliy-iqtisodiy faoliyatining axborot xavfsizligini ta’minlashning yo‘li sifatida o‘zining samarali ekanligidan kelib chiqqan holda tadbiq etish zarurati mavjud. Mexanizmning taqsimlash tizimi doirasida korxonaning taklif etilgan tashkiliy-iqtisodiy faoliyatni kiberxavfsizligi mexanizmini faollashtirish taqozo etiladi.
3. “Toshkent issiqlik elektr stansiyalar” aksiyadorlik jamiyatining tashkiliy-iqtisodiy faoliyatiga kiberxavfsizlik mexanizmlarni ishlab chiqish va uni raqamlashtirish algoritmini o‘rnatish tavsiya etiladi.
4. Xomashyo ta’minotini kiberxavfsizligini ta’minlash logistik hujumlarni xakerning identifikatsion hisob raqamini topish fishingi orqali hujum uyushtiriayotganlarning tajribasini, hujum sxemasini, strategiyasini aniqlash hamda uning manziligi operativ tarzda topish imkonini beradi.
5. Xomashyo buyurtmasiga kiberhujumida “aqlli blokcheyn” ssenariysi asosida tashkillashtirish eng ko‘p xakerlarning qismi blokcheyn orqali o‘z hujumini uyushtirishga inlitishi tufayli, umumiy texnik-iqtisodiy himoya ssenariysini shakllantirish tavsiya etiladi.
6. Kiberxavfsizlik iqtisodiyotida izlanishlar olib borish davomida monotizimning ilmiy-amaliy hamda kibergigiyenaga amal qilgan holda Kuxning Drift modelidan foydalanish orqali issiqlik elektrostansiyalarning axborot xavfsizligining iqtisodiy samaradorligini ta’minlanishini asoslash zarur.

РАЗОВЫЙ НАУЧНЫЙ СОВЕТ НОМЕР DSc.13/30.12.2019.T.07.02 ПО ПРИДАЧЕ УЧЕНЫХ СТЕПЕНЕЙ В ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КОРАБАЕВ ЭЛДОР АЛИЖОНОВИЧ

ЦИФРОВИЗАЦИЯ МЕХАНИЗМОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИОННО-ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ ЭЛЕКТРОЭНЕРГЕТИКИ

08.00.16 – Цифровая экономика и международная цифровая интеграция

АВТОРЕФЕРАТ ДИССЕРТАТЦИИ ДОКТОРА ФИЛОСОФИИ (PhD) ПО ЭКОНОМИЧЕСКИМ НАУКАМ

Ташкент - 2024

Тема диссертации доктора философии (PhD) по экономическим наукам зарегистрирована Высшей аттестационной комиссией за № B2024.2.PhD/Iqt4303.

Диссертатция выполнена в Ташкентском университете информационных технологий. Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размешен на веб-странице (www.tuit.uz) и на Информационно-образавательном портале «ZiyoNet» (www.ziyonet.uz)

Научный руководитель:	**Саиткамолов Мухаммадхужа Собирхужа угли** доктор экономических наук, доцент
Официальные оппоненты:	**Саматов Гаффор Аллакулович** доктор экономических наук, профессор
	Муратова Шохиста Нигматуллаевна доктор экономических наук, профессор
Ведущая организация:	**Ташкентский государственный технический университет имени Ислама Каримова**

Защита диссертации состоится «_____» _____ 2024 г. в _____ часов на заседании научного совета DSc.13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; e-mail: info@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер № 2870). (Адрес: 100084, г.Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «_____» _____ 2024 года.
(протокол рассылки №____ от «____» _____ 2024 г.).

Б.Ш.Махкамов
Председатель Научного совета по присуждению ученых степеней, доктор экономических наук, проф.

Э.Ш.Назирова
Ученый секретарь Научного совета по присуждению ученых степеней, доктор технический наук, проф.

Ш.Дж.Иргашходжаева
Председатель научного семинара при Научном совете по присуждению ученых степеней, доктор экономических наук, проф.

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В условиях глобализации, а также последовательного развития технологий искусственного интеллекта важное значение приобретают вопросы устойчивого повышения уровня цифровизации экономики, совершенствования механизмов цифровизации информационной безопасности отраслей промышленности на глобальном и государственном уровнях, в частности, в организационно-экономической делятельности предприятий электроэнергетики. «В 2023 году в результате кибератаки на энергетическую компанию Dit Retro (Канада) страна потеряла 12,1% ВВП и понесла большой экономический урон».[1] В настоящее время приоритетная организация информационной безопасности организационно-экономической деятельности производственных предприятий как одно из значимых условий целевого развития мировой экономики на основе цифровых технологий является наиболее актуальной задачей.

В осуществляемых исследованиях по обеспечению информационной безопасности предприятий электроэнергетической промышленности особое внимание уделено совершенствованию механизмов цифровизации информационной безопасности организационно-экономической деятельности производственного сектора. В этом плане актуальными остаются исследования, посвященные всестороннему формированию организационно-экономических механизмов обеспечения информационной безопасности в управлении, совершенствованию экономических основ повышения киберустойчивости «умных» энергетических систем, совершенствования методологии определения урона при управлении системами электроэнергии на основе IT, совершенствования механизмов экономической поддержки киберэффективности управления в соответствии с «умными» технологиями.

В Узбекистане наряду с качественным развитием и технологической организацией электроэнергетической отрасли в соответствии с международными требованиями реализуются широкомасштабные меры по повышению эффективности управления, оптимальной организации информационной безопасности организационно-экономической деятельности предприятий отрасли, обеспечению кибербезопасности тепловых электростанций, осуществлению непосредственной киберзащиты потребителей электросети. В рамках стратегии «Цифровой Узбекистан – 2030» выдвигаются идеи онлайн контроля потребления электроэнергии, развития киберэкономической деятельности при поэтапной цифровизации установок автоматизированных устройств.[2] Для решения этих задач целесообразно углубление исследований по научному обеспечению, в чатсности обоснованию оптимальных параметров кибербезопасности

[1] Energydata.com

[2] Указ Президента Республики Узбекистан от 5 ноября 2020 года № УП-6079 «Об утверждении Стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации», Глава II. Внедрение информационных систем и программных продуктов

предприятий электроэнергетики, совершенствованию управления процессов реализации электроэнергии на этапе, предшествующем потреблению продукции, обоснованию прогностических показателей организационно-экономической кибербезопасности процессов производства продукции.

Закон Республики Узбекистан «О кибербезопасности» №ЗРУ-764 от 15 апреля 2022 года, данное диссертационное исследование в определенной степени служит реализации задач, предусмотренных Указом Президента Республики Узбекистан от 5 ноября 2020 года № УП-6079 «Об утверждении Стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации», Постановлением Президента Республики Узбекистан от 22 августа 2022 года № ПП-357 «О мерах по поднятию на новый уровень сферы информационно-коммуникационных технологий в 2022-2023 годах», а также другими нормативно-правовыми документами, касающимися данной сферы деятельности[3].

Соответствие темы исследования приоритетным направлениям развития науки и технологий республики. Данная диссертация выполнена в соответствии с приоритетным направлением развития науки и технологии республики «Духовно-нравственное и культурное развитие демократического и правового общества, формирование инновационной экономики».

Степень изученности проблемы. Вопросы повышения экономической эффективности производства в рамках информационной безопасности организационно-экономической деятельности энергетических предприятий в контексте мирового опыта, а также различные подходы и практические разработки по развитию отрасли изучались в работах таких зарубежных экономистов как Д.Гаськова, М.Простосердов, Л.Магомедова, Д.Бекбергенова, R.Anderson, G.Lawrence, L.Martin, A.Efe, R.Rutil, R.Ramashandran, E.Serah, S.Grobman[4].

---

[3] Послание Президента Республики Узбекистан Олий Мажлису.

[4] Гаскова Д.А. Методы, модели и комплекс программ анализа киберситуационной осведомленности энергетических объектов. Автореф. 2021 г., 34 с.//Простосеров М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия, авторе дсс. 2016 г., 23 стр.//Магомедова Л.Р. 2021 г., 24 ст.//Бекбергенова Д.Е. Управление цифровизацией социально-экономического развития региона, 2022 г., 34 стр.// Ross Anderson. Why Information Security is Hard – An Economic Perspective.University of Cambridge Computer Laboratory, J.Thomson Avenue, Cambridge CB3 0FD, UK Ross.Anderson@cl.cam.ac.uk, 2000, 64 р// Гордон, Лоуренс А .; Леб, Мартин П. (ноябр 2002 г.). «Экономика инвестиций в информационную безопасность». Транзакции ACM по информационной и системной безопасности. 5 (4): 438–457. doi: 10.1145/581271.581274 . S2CID 1500788// Lawrence A. Gordon and Martin P. Loeb. Using Information Security as a Response to Competitor “ANALYSIS SYSTEMS”. COMMUNICATIONS OF THE ACM. September 2001/Vol. 44, No. 9, 71-77// Ахмет Эфе. Организационная кибербезопасност: позиция ИТ-аудита, основанного на экономическом риске, теоретических и практических аспектах кибербезопасности (русское издание). 2023 г., 452 стр.// Пунам Патил. Эффективный метод кибербезопасности: Защита данных от киберпреступников (русское издание). Sciencia Scripts. 2022 г, 76 стр// Ravikumar Ramachandran, CISA, CISM, CGEIT, CRISC, CDPSE, OCP-Oracle Cloud Architect, CISSP-ISSAP, SSCP, CAP, PMP, CIA, CRMA, CFE, FCMA, CIMA-Dip.MA, CFA, CEH, ECSA, CHFI, MS (Fin), MBA (IT), COBIT-5 Implementer, Certified COBIT Assessor, ITIL 4 -Managing Professional, TOGAF 9 Certified, Certified SAFe5 Agilist, Chennai, India, Date Published: 23 January 2019, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy// Питер Баняш. Различные аспекты кибербезопасности и осведомленности об информационной безопасности (русское издание). Sciencia Scripts 2023 г, 60 стр// Сера Э. Кибербезопасност: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании. Интеллектуальная Литература 2021 г// Капинда Ч. Готовность к кибербезопасности повышают правительство

В нашей стране исследованию информационной безопасности предприятий и ее экономических основ посвящены работы таких ученых как С.Жуманова, И.Алимардонов, А.Анорбоев, А.Ракицкий, Б.Ахроров, Т.Шодиев, М.Саиткамолов, Р.Алимжанов, Н.Насруллаев, А.Мусаев, К.Керимов, И.Дустмухаммедов[5].

В Республике в экономической литературе с учетом вклада приведенных выше ученых в исследуемых вопросов недостаточно освещены такие вопросы как совершенствование механизмов и поиск путей оценки обеспечения информационной безопасности предприятий энергетики. В данной диссертации широко представлены решения этой проблемы.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в соответствии с планом научно-исследовательских работ Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий в рамках прикладного проекта №А-2-59 «Модели адаптивной гибкой трансформации рынка труда Узбекистана в условиях цифровой экономики и организации социально-трудовых отношений» (2023 г.).

Целью исследования является разработка предложений и рекомендаций по совершенствованию механизмов цифровизации информационной безопасности организационно-экономической деятельности предприятий электроэнергетической отрасли.

Задачи исследования:

обоснование экономического содержания понятия «экономика кибербезопасности» для организационно-экономической деятельности энергетической отрасли на основе теоретических подходов зарубежных и отечественных ученых;

в странах мира (русское издание). Sciencia Scripts 2023 г., 68 стр.// Steve Grobman. The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War. Apress. 2016 y., 374 p.

[5] Жуманова С. Киберхавфсизлик - рақамли иқтисодиётнинг муҳим шарти. Янги Ўзбекистон. KOLORPAK. 2020 й, 330 б// Алимардонов И. Миллий молиявий хатарларнинг олдини олиш шарти. Халқ сўзи, 2022, 336.// Анорбоев А.У. Кибержиноятчилик ва киберхавфсизлик бўйича қонун ижодкорлигининг замонавий тенденциялари: миллий, хорижий ва халқаро тажриба монография. Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги, Ўзбекистон Республикаси миллий гвардия ҳарбий техника институти, Мухаммад ал-Хоразмий ном. ТАТУ, 2020 й., 360 б//Ракитский А. Корхонада ахборот хавфсизлиги қандай таъминланади. Korxonani boshqarish. "MTSFER-U Nashriyot uyi" МЧЖ, 2019 й, 334 б//Ахроров Б.А. Иқтисодиёт йўналишидаги бакалаврларни тайёрлашда "Ахборот хавфсизлиги" курсини ўқитиш методикаси. 13.00.02 - Таълим ва тарбия назарияси ва методикаси (информатика): Педагогика фанлари бўйича фалсафа д-ри (PhD) дис. автореф.], 2019 й, 50 б// Шодиев Т. Банк тизимида ахборотларни криптографик услублар ёрдамида ҳимоялашнинг долзарб муаммолари, 2021 й, 312 б// Алимжанов Р. Ахборотни йўқотиш оқибатидаги зарардан компанияни қандай ҳимоя қилиш мумкин. "MTSFER-U Nashriyot uyi" МЧЖ 2020 й., 228 б.// Насруллаев Н.Б. Ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш усуллари ва алгоритмлари [Матн] : техника фан. фалсафа доктори дис.автор, 2019, 54 б// Мусаев А.И. Узлуксиз шифрлашнинг криптобардошли алгоритмлари ва уларнинг самарадорлигини баҳолаш. Техника фанлари номзоди. ... дис. автореферати, 2011 й., 21 б.// Керимов К.Ф. Электрон ресурсларни ахборот хавфсизилиги таҳдидларидан ҳимоясини таъминлашнинг мослашувчан моделлари ва усуллари диссертация автореферати, 2020 й., 58 б.//Дустимуҳаммедов И.А. Божхона ахборот тизимларида ахборот хавфсизлигини таъминлаш усуллари ва моделлари [Матн] / А. И. Дусмуҳамедов, А. А. Саидов, З. Б. Абдураҳмонов; Ўзбекистон Республикаси Давлат божхонаси қўмитаси, Божхона институти. Тошкент : Fan va texnologiyalar nashriyot-matbaa uyi, 2022, 204 б.//

последовательное изучение роли информационной безопасности в совершенствовании организационно-экономических механизмов предприятий тепловой энергетики, определение ее значимости и кибергигиенического потенциала в организационных и экономических отношениях;

формирование классификации факторов оценки и воздействия на кибербезопасность организационно-экономической деятельности предприятий энергетической промышленности;

анализ составляющих компонентов механизмов организационно-экономической деятельности предприятий энергетической отрасли на основе передового зарубежного опыта и авторского подхода, а также обоснование возможностей внедрения их в экономическую инфраструктуру нашей страны;

анализ особенностей эффективной активизации механизмов организационно-экономической деятельности предприятий энергетической отрасли и разработка экономической стратегии повышения ее эффективности;

обоснование рекомендаций по совершенствованию экономической стратегии повышения эффективности предприятий энергетической промышленности в соответствии с особенностями активизации их организационно-экономической деятельности;

совершенствование методологии оценки эффективности инновационных проектов в развитии информационной безопасности механизмов организационно-экономической деятельности предприятий энергетической отрасли;

обоснование рекомендаций по последовательности мер по совершенствованию кибергигиенической деятельности и экономических рисков при повышении киберэффективности предприятий энергетической отрасли;

разработка предложений и рекомендаций по совершенствованию механизмов цифровизации информационной безопасности организационно-экономической деятельности предприятий электроэнергетической промышленности.

Объектом исследования является информационная безопасность организационно-экономической деятельности АО «Toshkent IES».

Предмет исследования – экономические отношения, возникающие в процессе активизации цифровизации механизмов информационной безопасности организационно-экономической деятельности предприятий энергетической промышленности.

Методы исследования. В ходе исследования использованы такие методы как анализ, системный анализ, моделирование, аналогия, обобщение, классификация, абстрагирование, системный, факторный, модельный и аксиоматический анализ, экспертная и программная оценка, статистическое сравнение, математико-экономическое моделирование, алгоритмизация и прогнозирование.

Научная новизна исследования заключается в следующем:

обоснована целесообразность индекса экономической киберббезопасности в пределах $0,7 \leq C \leq 0,95$ на основе киберзащитного потенциала, уровня кибербезопасности и риска предприятий энергетической промышленности, а также соответствие системы защиты стратегическому обеспечению;

усовершенствована стратегия активизации организационно-экономических механизмов информационной безопасности предприятий электроэнергетической отрасли в соответствии с оценкой целевых показателей процесса, обоснованием хронологической последовательности мультисерии, сравнением международного и национального уровней киберзащиты;

обоснован прогноз реализации инвестиционных проектов по обеспечению кибербезопасности организационно-экономической деятельности АО «Toshkent IES» на 2024-2029 годы с учетом стратегического повышения уровня модернизации производства, расширения возможностей равного использования влияния климатических изменений и доступных услуг;

разработан прогноз эконометрического сценария организационно-экономической кибербезопасности процессов электроэнергетических компонентов АО «Toshkent IES» на 2023-2028 годы с учетом альтернатив организационно-экономической деятельности и предложенной мультиколлактной стратегии.

Практические результаты исследования включают в себя:

на основе теоретических подходов зарубежных и отечественных ученых обосновано экономическое содержание понятия «экономика кибербезопасности» для организационно-экономической деятельности энергетической промышленности;

оценены киберпотенциал и значение информационной безопасности организационных и экономических отношений в совершенствовании организационно-экономических механизмов на предприятиях теплоэнергетической промышленности;

обоснованы возможности внедрения компонентов механизмов организационно-экономической деятельности в экономическую структуру на основе зарубежного опыта и авторского подхода;

предложены меры по повышению эффективности механизмов организационно-экономической деятельности предприятий энергетической отрасли в соответствии с особенностями эффективной активизации;

усовершенствованы модель «песочные часы» и поддерживающая ее мультиколлактная стратегия по принятию решений по оценке уровня риска и экономической безопасности цифровых технологий компонентов предприятий электроэнергетической отрасли согласно авторскому подходу;

разработаны предложения и рекомендации по повышению эффективности и активизации информационной безопасности.

Достоверность результатов исследования обоснована целесообразностью примененных в работе теоретических подходов и методов получением статистических данных из официальных и периодических источников, в том числе использованием данных, полученных из официальных источников Агентства статистики при Президенте Республики Узбекистан, АО «Toshkent IES» и его подведомственных структур, внедрением разработанных в ходе исследования выводов, предложений и рекомендаций в практику, а также подтверждением результатов исследования полномочными государственными органами.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования обоснована тем, что разработанные выводы, предложения и рекомендации служат совершенствованию методических основ повышения эффективности и активности механизмов информационной безопасности организационно-экономической деятельности предприятий энергетической отрасли и обогащению научно-методических основ научных исследований по данной теме.

Практическая значимость результатов исследования заключается в использовании предложений и практических рекомендаций в разработке системы практических мер, направленных на обеспечение повышение киберзащитной эффективности механизма информационной безопасности организационно-экономической деятельности АО «Toshkent IES», являющегося ведущим предприятием энергетической отрасли Республики.

Внедрение результатов исследования. На основе полученных результатов по совершенствованию механизмов цифровизации информационной безопасности организационно-экономической деятельности предприятий электроэнергетической промышленности:

предложения по целесообразности уровня экономической безопасности в пределах $0,7 \leq C \leq 0,95$ и соответствия системы защиты стратегическому обеспечению согласно значениям киберзащитного потенциала, кибербезопасности и риска предприятий энергетической отрасли внедрены в практику приказом АО «Toshkent IES» от 12 апреля 2023 года №284 (справка Министерства энергетики Республики Узбекистан от 3 апреля 2024 года №04-10-2259; справка АО «Toshkent IES» от 27 марта 2024 года №04-10-14/508). Результаты послужили повышению уровня информационной безопасности организационно-экономической деятельности общества на 0,72%, повышению инвестиционного потенциала предприятия на 0,12% и снижение расходов в организационно-экономической деятельности управления на 229 млн. сум;

усовершенствованный подход к стратегии активизации организационно-экономических механизмов информационной безопасности предприятий электроэнергетической отрасли в соответствии с оценкой целевых показателей процесса, обоснованием хронологической последовательности мультисерии, сравнением международного и

национального уровней киберзащиты использованы в разработке стратегии развития АО «Toshkent IES» (справка Министерства энергетики Республики Узбекистан от 3 апреля 2024 года №04-10-2259; справка АО «Toshkent IES» от 27 марта 2024 года №04-10-14/508). Предложение в определенной степени послужило дальнейшему повышению качества разработки стратегии активизации организационно-экономических механизмов информационной безопасности, расширению возможностей применения и повышению эффективности целевых мер на основе повышения точности количественной оценки процесса;

прогноз реализации инвестиционных проектов по обеспечению кибербезопасности организационно-экономической деятельности АО «Toshkent IES» на 2024-2029 годы с учетом стратегического повышения уровня модернизации производства, расширения возможностей равного использования влияния климатических изменений и доступных услуг использован в разработке стратегии развития АО «Toshkent IES» (справка Министерства энергетики Республики Узбекистан от 3 апреля 2024 года №04-10-2259; справка АО «Toshkent IES» от 27 марта 2024 года №04-10-14/508). Внедрение инвестиционного проекта в определенной степени послужило повышению технико-экономической устойчивости деятельности предприятия к кибератакам в условиях роста прибыли;

прогноз эконометрического сценария организационно-экономической кибербезопасности процессов электроэнергетических компонентов АО «Toshkent IES» на 2023-2028 годы с учетом альтернатив организационно-экономической деятельности и предложенной мультиколлактной стратегии внедрен в практику АО «Toshkent IES» приказом от 12 апреля 2023 года №284 (справка Министерства энергетики Республики Узбекистан от 3 апреля 2024 года №04-10-2259; справка АО «Toshkent IES» от 27 марта 2024 года №04-10-14/508). Внедрение предложения в определенной мере послужило повышению информационной безопасности АО в 2023 году в соответствии с эффективной организацией организационно-экономических мер.

Апробация результатов исследования. Результаты исследования обсуждены на 2 международных и 2 Республиканских научно-практических конференциях.

Публикация результатов исследования. По теме диссертации опубликовано 10 научных работ, в том числе 3 статьи в Республиканских изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, и 3 статьи в зарубежных журналах.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы. Объем диссертации составляет 130 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обосновываются актуальность и востребованность темы исследования, изложены цель и задачи, объект и предмет диссертации, указано соответствие темы приоритетным направлениям развития науки и технологий республики, изложены научная новизна и практические результаты исследования, раскрыта научная и практическая значимость полученных результатов, приведены сведения о внедрении результатов исследования в практику, об опубликованных работах и структуре диссертации.

В первой главе диссертации «**Научно-теоретические основы механизмов кибербезопасности организационно-экономической деятельности энергетической промышленности**» освещены экономические основы информационных рисков, информационной безопасности, экономической кибербезопасности предприятий электроэнергетической промышленности, научно-теоретические аспекты экономических угроз киберугроз и последствий финансового урона. В соответствии с этим, описаны мировой опыт, экономические исследования и научно-теоретические взгляды зарубежных ученых.

Под экономикой информационной безопасности понимается экономика, основанное на предупреждение экономического урона от средств потребителей информационных технологий. Предприятия энергетической отрасли подвержены кибератакам больше, чем предприятия других секторов промышленности, при этом целесообразно исследование факторов воздействия на кибербезопасность.

Таблица 1

Факторы, оказывающие влияние на киберэкономические атаки на предприятия энергетической отрасли[6]

№	Факторы кибератак	Доля атак	Цели и последствия кибератак
1.	Овладение сведениями посредством платежей	22%	Теряется конфиденциальность финансовых реквизитов потребителей электроэнергии
2.	Кража денег с платежных карт	19%	Формирование денежных средств на платежных картах на случай отключения электроэнергии
3.	Удаление данных диспетчерской службы обеспечения электроэнергией, рандомная ситуация	18%	Формирование искусственного рынка платежей для основных задолжностей потребителей
4.	Спранированное целенаправленное ограбление дома	16%	Блокирование всех средств связи путем оставления дома без электроснабжения и
5.	«Хакер-клоун», т.е. хакер пробует силы, «играет»	10%	Формирование визитной карточки среди коллег по хакерской деятельности

Данная таблица сформирована на основе данных, приведенных в Глобальной программе кибербезопасности Международного союза электросвязи на основе статистических сведений 124 стран из 210.

Несмотря на оптимизацию и совершенствование основной части индустрии интеллектуальных технологий, внедрение их в практику для противодействия киберугрозам носит общий характер и может привести

[6] https://www.ifap.ru/pr/2008/080908aa.pdf

Таблица 2

Факторы, влияющие на кривую роста киберпреступности [7]

№	Факторы	Происхождение факторов	Последствия киберпреступлений	Меры безопасности против киберпреступлений
1.	Сложность раскрытия киберпреступления	Наличие возможностей по анонимному ведению деятельности в Интернете.	Финансовый урон.	Строгое соблюдение законов по защите данных: Необходима широкомасштабная законодательная база, обеспечивающая безопасность и конфиденциальность персональных данных людей. Эти законы должны определить меры наказания за нарушение данных и привлечение к ответственности для защиты данных клиентов организаций.
2.	Киберзащитное равнодушие	Недостаточность мер кибербезопасности и неоценивание уровня киберзащиты предприятий и организаций.	Сохранение конфиденциальности информации и контроль потока данных	
3.	Трансфармационная акселерация	Волна цифровых трансформационных технологий стала толчком для совершенствования электронной кластеризации, онлайн-банкинга и цифровых транзакций.	Использование преимуществ. Хотя передовые технологии улучшают жизнь, тем не менее киберпреступники могут использовать уязвимости в онлайн-платформах, украсть персональные данные и проводить финансовые махинации (мошенничество).	Сотрудничество и обмен информацией: Важно сотрудничество государственных органов, правоохранительных органов и международных организаций. Обмен информацией о развивающихся угрозах, лучших практиках и тенденциях в киберпреступности способствует созданию коллективной безопасности против киберпреступников.
4.	Незнание правовых основ кибербезопасности	Основной фактор, способствующий росту киберпреступности – это неосведомленность о кибербезопасности. Многие люди и организации не обладают необходимыми знаниями по определению потенциальных угроз или принятия соответствующих мер профилактики. Этот пробел используется киберпреступниками.	Социальное и психологическое воздействие. Киберпреступность наносит финансовый урон не только людям и организациям, но и оказывает глубокое социальное и психологическое воздействие. Жертвы кибербуллинга, онлайн-травли и киберсталкинга часто испытывают эмоциональные страдания, тревогу и депрессию.	Образование и информированность в сфере кибербезопасности: Повышение информированности о кибербезопасности и образование в этой сфере на всех уровнях очень важно для защиты от киберугроз людей и организаций. Проведение консультационных кампаний поможет распространить знания о значимости практики безопасного Интернета и надежных паролей, постоянного обновления программного обеспечения и безопасного просмотра данных.
5.	Слабая инфраструктура кибербезопасности	В результате отсутствия и непривлекательности инвестиций в поддержку системы защиты от киберпреступлений наносится финансовый урон.	Разрушение стратегически значимой инфраструктуры. Кибератаки, направленные на значимую инфраструктуру, т.е. сети электроэнергии, транспортные системы и правительственные сети, представляют серьезную угрозу для национальной безопасности.	Укрепление инфраструктуры кибербезопасности. Необходимо вложить инвестиции в надежную инфраструктуру кибербезопасности, систем выявления угроз и постоянного аудита безопасности. Сотрудничество между правительственными ведомствами, частными организациями и специалистами по кибербезопасности является значимым для упреждения действия киберпреступников.

[7] Suhani Dhariwal. Rise of Cybercrime in India: Reasons, Impacts & Safety Measures. https://www.writinglaw.com/rise-of-cybercrime-in-india/

к определенным рискам. Основным объектом кибератак в отношении предприятий отрасли энергетики являются не источники финансирования, а информация, которая служит обеспечению постоянного финансирования. Данные, необходимые для кибергигиены энергетических предприятий, являются конфиденциальными сведениями о потребителях, по обеспечению энергией.

Адекватное управление информационной кибергигиеной осуществляет посредством каскадной эффективной оценки экономики, т.е. наблюдения за цепочкой в системе обеспечения электроэнергией. Предприятия энергетической отрасли подвергаются кибератакам больше, чем предприятия других сфер, целесообразно исследование факторов, которые влияют на на этот процесс (Таблица 2).

Во второй главе диссертации «**Оценка организационно-экономических механизмов кибербезопасности энергетических предприятий в условиях развития экономики страны на основе цифровых технологий**» разработаны научные предложения по оценке состояния организационно-экономических механизмов кибербезопасности АО «Тошкент ИЭС» и изучению текущего состояния обеспечения информационной и финансово-экономической безопасности его деятельности.

Таблица 3

Факторы возникновения киберэкономических атак
(2016-2023 гг., в процентах)[8]

№	Факторы кибер-экономической атаки	Доля в атаки	Способ оценки	Содержание способа оценки
1	Месячная зарботная плата			
1.	Низкий уровень заработной платы	22%	$M_s = \frac{M_t - M_r}{X}$	M_s- месячная заработная плата работников, которые осуществили кибератаку; M_t- значение оплаты необходимых услуг хакера по по тарифу; M_r- заработная плата в реальном времени;X-количество хакеров, осуществивших кибератаки.
2.	Низкий уровень заработной платы, проведение аудиторской кибер-экономической проверки	4%	$M_{sk} = \frac{M_{td} - M_{sr}}{X}$	M_{sk}- учет заработной платы при исследовании кибератак; M_{td}- значение заработной платы работников по тарифу и значение по отчетности; M_{sr}- значения проверки заработной платы в режиме реального времени по налоговой базе; X- количество работников, совершивших кибератаки.
2	Экономические махинации			
3.	На основе заказа собственника предприятия	14%	$I_m = \frac{I_t - M_t}{T_t - S_t}$	I_m- коэффициент экономической махинации; I_t- экономические выплаты; M_t- значения по финансовым операциям; T_t- значение учтенных товаров, материальных ценностей и их прихода-расхода; S_t- налоговые выплаты по реализованным товарам.
4.	Страхование, взыскание с предприятия денежных средств	15%	$S_m = \frac{I_t - M_t}{B_{tl} - S_{g't}}$	S_m- коэффициент махинации путем страхования; B_{tl}- значения товаров, материальных ценностей, которым нанесен урон; $S_{g't}$- объект страхования и процент его компенсирования (по договору).
5.	Финансовый шантаж	7%	-	Пассивный экономический расход кредитных операций и частных денежных средств.
3	Опыт и испытания			
6	Испытание системы на прочность	5%	-	Испытания системных попыток и возможностей хакеров

[8] Лахани К. Янсити М. Цифровое преимущество. Исскуство конкурировать в эпоху исскустного интеллекта. Бамбора, М.: 2021 г, 319 стр, Павлюк Ю. Digital всемонущий. 101 инструмент для повышения продаж с помощью цифровых технологий. Эксмо, 2021 г, 208 стр.

К настоящему времени поступательное развитие цифровой экономики в нашей стране оказывает значительное воздействие на формирование информационной экономики, повышение добавочной стоимости в секторе электронной коммерции. Вместе с тем, электроэнергетика представляет собой крупнейшую отрасль в цифровой экономике, которая создает добавочную стоимость других секторов экономики.

Таблица 4

Объем валовой добавочной стоимости секторов информационной экономики и электронной коммерции (*2018-2023 гг., млрд. сум)*[9]

Годы	2018	2019	2020	2021	2022	2023
Информационная экономика и электронная коммерция	7,934	8,701	11,220	12,109	12,998	13,461
В том числе: электроэнергетика	1,099	2,471	3,729	5,583	5,990	6,780

Эффективность цифровых технологий, принимающих участие в сфере электроэнергетики, повышение показателей в виде значения способности создания добавочной стоимости помимо улучшения положения потребителей характеризуется тем, что передовые технологии, связанные с производством, распределением, направлением и доставкой энергии, полностью овладели инновационной инфраструктурой, увеличивается количество современных и «умных» станций. С возрастанием технологического обеспечения снижается уровень системы защиты и наряду с нерешенными еще проблемами снижаются и показатели кибербезопасности.

Таблица 5

Использование существующих мощностей АО «Тепловые электростанции» (2022 год)[10]

№	Названия ТЭС и ТЭЦ	Установленная мощность, МВт	Текущая мощность, МВт
1.	АО «Сирдарё ИЭС»	3 415	3 150
2.	АО «Тошкент ИЭС»	2 430	2 100
3.	АО «Навоий ИЭС»	2 268	1 850
4.	АО «Тахиатош ИЭС»	1080	1000
5.	АО «Фарғона ИЭМ»	429	350
6.	АО «Муборак ИЭМ»	70	60
7.	АО «Тошкент ИЭМ»	67	60
8.	АО «Талимаржон ИЭС»	1 760	1 750
9.	УП «Тўракўрғон ИЭС»	950	870

В результате принятия соответствующих мер по повышению мощностей тепловых электростанций обеспечено повышение доступных мощностей. С точки зрения мощности АО «Тошкент ИЭС», являющееся объектом исследования, в соответствии с показателями заняло второе место. Таким образом, можно прийти к выводу, что АО «Тошкент ИЭС» входит в число крупнейших энергетических предприятий.

[9] Агентство статистики при Президенте Республики Узбекистан
[10] “Issiqlik elektrstansiyalari” AJ ma’lumotlari

Рис. 1. Организационно-хозяйственный механизм кибербезопасности предприятий электроэнергетики[11]

Несмотря на осуществляемые в системе цифровой энергетике в сфере тепловой энергетики значительные преобразования, не решенными остаются проблемы существующего электрооборудования, его применения, кибербезопасности передового технологического обеспечения. Хотя в АО «Тошкент иссиқлик электрстансиялари» есть 7 блоков, но все они не обеспечены технологиями и программами, которые отвечают требования информационной безопасности. Ввиду этого в отрасли наблюдаются потери энергии и искусственность платежей за ее потребление, искусственные цены за потребление энергии, частичное хищение денежных средств, в результате кибератак с помощью программ-червей, появляются значительные проблемы по обеспечению конфиденциальности индвидуальных данных. В связи с этим, целесообразным представляется разработка механизмов обеспечения кибербезопасности и применение алгоритма их цифровизации в рамках организационно-экономической деятельности акционерного общества «Тошкент иссиқлик электр стансиялар». (рис. 1).

Обеспечение кибербезопасности обеспечения сырьем, фишинг поиска идентификационного расчетного счета хакера, осуществляющего логистических кибератаки, позволяют определить опыт злоумыленников, схему и стратегию атаки, а также оперативно найти их адреса. Это является мерой, направленной на осуществление информационной безопасности по всем параметрам с организационно-хозяйственной точки зрения.

Система функциональной поддержки уровня ИТ-обеспечения АО «Тошкент ИЭС» предназначена для электростанций и имеет стандарт, позволяющий применять умные технологии. Кроме того, их экономическая эффективность характеризуется наличием системы, аналогичной

[11] Авторская разработка

компьютерам с 6 традиционными и 3 современными альтернативными параметрами.

Таблица 6

Уровень обеспеченности технологиями, компьютерами АО «Тошкент ИЭС»[12]

№	Оборудование, средства ИКТ организации				Технико-экономический анализ
	Название	Уровень готовности (%)	Шт.	Место производства	
1.	Avtech Intel Core i7 6700K	45	34	Тайвань, 2012 г.	Необходимо установить лицензированные антивирусные программы
2.	HP ZBook Studio x360	37	14	США, Калифорния	Предназначено для тепловых электростанций
3.	Металлодетектор Minelab Equinox 800	100	2	Италия, 2020 г.	-
4.	«Бухгалтерия»	28	4	США, 2001 г.	Необходимо заменить на 1С 8.4
5.	GPS-трекер	15	5	США, 2004 г.	Заменить ГПС-трекеры на современные и увеличить их количество
6.	Электродные котлы	22	2	Россия, 2000	Необходимо заменить
7.	Котел обработки сырья	9	2	Финляндия, 1994 г.	Необходимо заменить на котлы экологической очистки
8.	470 Bl1,7,11 для работы с мощностью	78	2	Россия, 2010	Необходимо вывести из эксплуатации
9.	Энергоблоки	50	5	Россия, 2002	Необходима консервация

Предприятие в своей производственной и обслуживающей деятельности, в организационно-хозяйственной деятельности не применяет программу защиты и механизма обеспечения информационной безопасности цифровых технологий. Отсутствие в структуре предприятия какой-либо программы поддержки, механизма киберзащиты может оказывать негативное влияние на все параметры эффективности и ведет к кризису. При этом функционирование системы защиты необходимо сохранить на уровне мировых стандартов.

В третьей главе диссертации «**Цифровизация механизмов информационной безопасности организационно-хозяйственной деятельности предприятий электроэнергетики**» приводятся данные по моделированию и перспективам цифровизации механизмов информационной безопасности предприятий.

Мультиколлинеарная модель разработана американским ученым-экономистом Хелом Вэрианом и представляет собой формирование системы защиты на основе устойчивых данных посредством оперативного отбора сведений. Ее основная цель заключается в формирвоании комплекса планом применения соответствующих сценариев для принятия необходимый решений на основе оперативной классификации сведений. Определение коэффициентов в качестве модели не требует анализа в крупных масштабах, достаточны только данные. Ее система защиты анализирует тактику хакеров, осуществляющих кибератаки, ориентирует их

[12] Данные АО “Toshkent IES”

доступ к системе за счет копирования. В результате хакер вынужден искать доступ к системе адресно. В данной диссертационной работе эта модель усовершенствована до уровня стратегии, в которой можно обосновать хронологическую последовательность мультисерии, сравнить международный и национальный уровень киберзащищенности (рис. 2).

В ходе проведения изысканий в сфере экономики кибербезопасности рекомендуется обосновать обеспечение экономической эффективности информационной безопасности тепловых электростанций с использованием дрифт-модели Куха, соблюдая кибергигиену и сохраняя моносистему. Данная модель в действительности усовершенствована на основе цифровых технологий, предназначена для всех технических средств, ее основное преимущество заключается в экономической концептуальной основе и осуществление расчетов в соответствии технологий программной структуре.

Рис. 2. Стратегия активизации организационно-экономических механизмов кибербезопасности предприятий сферы электроэнергетики [13]

При осуществлении вычислений на основе дрифт-модели предполагается составление матрицы цифровых технологий.

Рис. 3. Матрица оптимизации цифровых технологий дрифт-модели[14]

[13] Авторская разработка

[14] Tashakkori A, C. Teddlie, C. B. Teddlie, Mixed methodology: Combining qualitative and quantitative approaches, volume 46, Sage, 1998

где:

м – уровень защиты цифровых технологий, отвечающих за сырье; н – уровень защиты цифровых технологий производственных процессов; г – уровень экономического риска кибербезопасности; и – количество технологий; ж – стоимость технологий; А - прибыльность; Б - ликвидность.

При переходе от и к ж изменение расходов от от горизонтали к вертикали позволяет определить уровень риска нарушения кибербезопасности, т.е. при стандартной работе традиционной системы не происходит кибератак, они проявляются при изменении какого-либо элемента, а именно при матричном преобразовании, т.е. возникают антиматричные значения. В результате таких изменений определяется уровень v_{ij}, т.е. уровень устойчивости к изменениям (кибератакам). Это зависит от стандарта программы защиты от кибератак с экономической точки зрения, предустановленного производителем программного языка, всестороннего учета обеспечения пвыполнения заданных программных команд, а также соответствия блокам экономической информационой системы.

В точке А прибыльность равна 0, что означает ненанесение экономического урона, сохранность экономических данных и отсутствие соответствующих изменений передачи электроэнергии от панелей передачи электростанций. Это в определенной степени служит повышению эффективности, т.е. в точке В налицо взаимосвязь уровеней защиты технологий процессов производства и сырья.

Для м, н ҳ и экономических потерь в системе защиты g_{ij} , v_{ij} (и=0,1,2,...,м; ж=0,1,2,..., н) подразумевается поэтапное выполнение функций основных компонентов с программами защиты в системе защиты (вне зависимости от того, что программа является новой или устаревшей). В результате матричного увеличения н(м+1) сохраняется пропорциональность изменений в v_{ij} в результате увеличения g_{ij} и м(н+1).

Использование метода реструктуризации всех выборок при выявлении промежуточных различий изменений служит определении значений коэффициентов рисков и траектории матрицы процессов от точки А до точки В. В данном случае системы защиты активизирует соответствующий элемент из комплекса выборок, что может быть причиной некоторого нарушения алгоритма встроенных программ. Их защита осуществляет за счет замены данных псевдоловушки.

$$S = \frac{(m+n)!}{m!n!} (1)$$

где: С = потери среди выборок системы кибербезопасности; при этом м=н=10 равна С=184756.

В следующих расчетах м=н=1, при этом основной выборкой, которой необходима оптимизация, может быть одна (рис. 4).

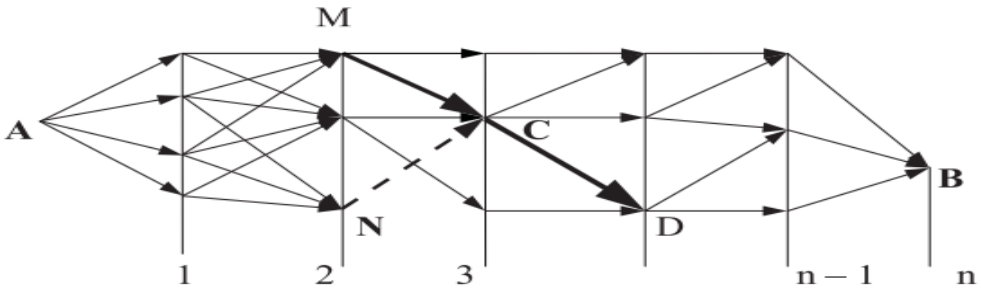


Рис. 4. Алгоритм последовательной альтернативной выборки[15]

После определения оптимальности выборок осуществляется эконометрический прогноз организационно-экономической деятельности.

Если выборки v_i, g_j, N_j брать в качестве кривых линий x (i=1,2,...н), приближенных на оси абсцисс, их ограничение в пределех 10 ед. выделяются в 3 вида:

1. $v_m \geq A_m$ или $v_n \geq A_n$ м и н при учете некоторых выборок;
2. $g_j \leq (v_{j+1} - v_j)/B_{j+1} \leq B_j$;
3. $N_j \leq (v_{j+1} - v_j)/B_{j+1} - (v_{j+1} - v_j)/B_{j+1} \leq D_j(C, M)$.

Здесь неизвестные ординаты служат нахождению альтернативных вариантов среди кривых линий выборки.

Ограничение выборки второго вида является дискретным аналоговым ограничением первичной производной, искажение тангенса угла, построенной углом с x, ведет к приближенной кривой линии. Из-за результативности комбинированной производной разных элементов выборки третьего типа нет искажений в разных углах.

В соответствии с этим, при фиксации 3 вида выборки оптимальным представляется дискретный аналог краевых линий с наиболее низкими показателями искажения угла. На основе значения искажения угла, равной 0,001, направленной на сохранение данных и перенаправление кибератак по ложным адресам, т.е. ориентирования по незначимым выборкам.

Из трех видов выборок 1 вид оправдал себя. Остальные две выборки имеют место быть благодаря возможности оценки ожидаемого риска посредством «преимущества участия». Следовательно, если есть вероятность, что из двух видов выборки 50% служит на пользу предприятию и соответственно 50%, что один из видов выборки не является полезным, при вычислении используется формула математического ожидания (W) (3.2).

$$w = \sum_{i=1}^{N}(B_i \times A_i)(3.2)$$

где: B_i - положительный или отрицательный результат выборки;

A_i - польза или урон при выборке;

N – количество вероятных результатов.

W=(0,5*2)+(0,5*(-1))=1+(-0,5)=0,5

Теперь требуется произвести расчет потерь, уровня защиты и комбинированных элементов.

[15] Струченков В.И. Методы оптимизации и прикладных задачах.-М.:МОЛОН-Пресс, 2012-320 с.

W=((1/38)*35)+((37/38)*(-1))=(0,02631578947*35)+(0,9736842105*(-1))
=(0,9210526315)+(-0,9736842105)=-0,05263157903.

При первой выборке остальные два вида выборки также бесполезны, соответственно целесообразно не отражать полностью выборку, равную 0, т.е. рекомендуется заполнить его некоторыми значениями. Иначе существует вероятность нанесения экономического урона предприятию в среднем на 5,26%. Если же количество видов выборки увеличить до 5, в этом случае возможен экономический урон в среднем на 26,3%.

В результате возникают потери в организационно-хозяйственной деятельности предприятия:

Таблица 7

Эконометрические наблюдения на основе дрифт-модели[16]

Показатели передачи количественных значений модели										
Передатчики статистических данных	CE	Минимум	Максимум	Процентиль						
				5	10	25	50	75	90	95
Стационарный Р-квадрат	0,202	0,415	0,908	0,415	0,415	0,541	0,819	0,889	0,908	0,908
Р-квадрат	0,410	-,127	0,917	-,127	-,127	0,155	0,675	0,848	0,917	0,917
КСКО	0,846	0,379	2,609	0,379	0,379	0,577	1,047	1,910	2,609	2,609
СОМО	2,874	0,696	7,877	0,696	0,696	0,936	2,485	5,804	7,877	7,877
МОМО	5,510	1,357	15,470	1,357	1,357	2,299	5,169	11,737	15,470	15,470
СМО	0,490	0,241	1,515	0,241	0,241	0,341	0,638	1,183	1,515	1,515
ММО	1,102	,475	3,403	,475	,475	,837	1,292	2,662	3,403	3,403

W=(-0,0526*1)+(-0,0526*10)+(-0,0526*5)=-0,0526-0,526-0,263=-0,8416

В этом случае урон информационной безопасности организационно-хозяйственной деятельности предприятия может составлять 84%.

При присвоении каждому элементу, подвергнутому атаке, определенного значения предприятию можно достичь результата всего лишь на 2% меньше. Согласно указанным выше расчетам при вычислении стационарности модели требуется прогнозирование элементов организационно-хозяйственной деятельности. При анализе приведенных эконометрических наблюдений можно использовать вероятностные показатели результатов проверки стационарности в соответствии с тестом прогнозирования Барлетт А. на основе дрифт-модели. Кроме того, процент погрешностей ниже 3,4% считается низким. Это, в целом, демонстрирует положительную результативность.

Ожидается, что в 2025 году киберзащита сырья сохранится почти на уровне 30%, а количество тех, кто хочет овладеть ими, сократится на 19%. Хотя к 2026 году данные показатели практически не изменятся, эта тенденция сохранится до 2028 года. Устойчивость организационно-экономической деятельности предприятия к кибератакам в производственном аспекте значительно повысится, производственные же показатели с 2024 по 2028 годы будут повышаться в среднем на 0,9%. Это демонстрирует эффективность в 44% при сохранении кибергигиены.

[16] Проведение теста Barlett A. осуществлено в программе SPSS Statistis 2.0

Таблица 8

Уровень обеспеченности информационной безопасности организационно-хозяйственной деятельности АО « Тошкент ИЭС» на основе дрифт-модели (в процентах)[17]

Модель	2024	2025	2026	2027	2028
Распределение	23,17	25,37	27,57	29,77	31,97
Передача	22,17	22,17	22,17	22,17	22,17
Трудовые ресурсы	39,00	39,40	39,80	40,20	40,60
Производство	36,67	37,37	38,07	38,77	39,47
Сырье	29,33	30,43	31,53	32,63	33,73

Ожидается, что уровень организационно-экономической активности наиболее слабых и наименее устойчивых к киберзащите трудовых ресурсов значительно повысится, достигнув 39% в 2024 году, что к 2028 составит рост производительности в 10%. Уровень организационно-хозяйственной деятельности предприятия, осуществляемой без рисков, в системе передачи электроэнергии стабильно находится на уровне 22,17%.

Среди минимальных 30 выборок вычисляется З:

$$Z = \frac{N*(R-0{,}5)-X}{\sqrt{\frac{X*(X-N)}{N-1}}} \quad (3)$$

где:

N – общая последовательность атак;

R – успешные попытки защиыт от атак;

$$X=2*W*L$$

где:

W – общий уровень защищенности;

L – общий уровень потерь.

При использовании кибератак, осуществленных в 2022 году, в порядке R=-3,+2,+7,-4,+1,-1,+6,-1,0,-2,-1 выборка мер защитных мер составляет 7, в обще сложности равна N=12, т.е. относительно 30 кибератак на организационно-экономическую деятельность тепловых электростанций успешно применены 7 защитных алгоритмов, из 15 потоков данных 12 ограничены. Внутренняя структура оставшихся 3 выборок, которые не защищены системой защиты, блокируются во избежание передачи некорректных данных.

$$X=2*6*6=72\ \%$$

Таким образом, в результате осуществления 30 кибератак на организационно-хозяйственную деятельность предприятия уровень защиты системы составил 72%.

Затем для проверки этого активируется последовательность серий P=8, определяется его хронологическая система (Таблица 8).

[17] Авторская разработка

Таблица 9

Обоснование хрологической последовательности мультисерии[18]

1	2	3	4	5	6	7	8	8	10	11	12
-3	2	7	-4	1	-1	1	6	-1	0	-2	1
-	+	+	-	+	-	+	+	-	-	-	+
1	2	X	3	4	5	6	X	7	X	X	8

Следует также отметить, что хотя значение 0 рассматривается как нейтральное промежуточное, его позиция в данном случае является отрицательной. Это является математической операцией, позволяющей точнее оценить процент учета потерь.

Технические параметры умных электростанций имеют неопоримое преимущество, а также возможности оперативного управления кибербезопасностью. Кроме того, в результате их внедрения ожидается динамическое повышение производственных мощностей предприятия (таблица 9).

Таблица 10

Перспективы эффективности внедрения умных электростанций, (2023-2028 гг., в процентах)[19]

Показатели	2023	2024	2025	2026	2027	2028
Снижение производственных расходов	6,2	6,5	6,8	7,0	7,0	7,1
Снижение себестоимости электроэнергии	1,7	1,7	2,0	2,1	2,1	2,1
Создание добавочной стоимости	2,2	2,5	3,0	3,2	2,9	3,0
Прибыль	15	17	16	15	18	17
Производительность	3,3	3,3	3,5	3,5	3,4	3,5
Обеспечение экологической безопасности	4,9	4,9	5,0	5,0	5,0	4,0

Снижение производственных расходов, естественно, выражается в системе цифровых технологий, направлененой на точность, походе к управлению посредством предотвращения аварий, связанных с ними ремонтных работ, технической поддержки, что ведет к снижению производственных расходов.

Реализация указанного выше предложения посредством привлечения инвестиций может обеспечить интенсификацию практического внедрения и внести значительный вклад в энергетику страны. В соответствии с этим, в рамках исследования определена эффективность привлечения капитальных инвестиций.

Данная таблица свидетельствует о том, что в результате внедрения инвестиционного проекта предприятие получает прибыль и обеспечивается экономическая и техническая устойчивость его деятельности к кибератакам.

[18]John Bandler. Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security, 2017, American Bar Association, 416 p.

[19] Авторская разработка

Таблица 11

Инвестиционный проект для обеспечения кибербезопасности организационно-экономической деятельности АО «Toshkent IES» на основе дрифт-модели (в тыс. долл. США, для 2024-2029 гг.)[20]

Показатели	2024	2025	2026	2027	2028	2029
Первоначальные инвестиционные средства	1 000					
Денежный поток		200	200	200	200	200
Результат	1 000	250	250	250	250	250
Дисконтный процент	10%					
	>0 – проект принимается; <0 – отвергается					
ВНД(внутренняя норма доходности)	7,93%					
проверка:	0	1	2	3	4	5
Объем платежей						
Сумма кредита	1 000					
Процент по кредиту	10%					
Годовой объем платежей	263,797					
Первоначальное удержание средств		1 000	836,203	656,025	457,830	239,816
Последующее удержание средств		836,203	656,025	457,830	239,816	0

При реализации этого инвестиционного проекта следующие стратегические аспекты определены как цели финансирования:

- изменение климата – это потенциальная и экзистенциальаня проблема, которая оказывает влияние на все страны, в частности, экстремальные погодные явления, продовольственная безопасность, угрозы здоровью человека, конфликты и др.

- расширение возможностей по равному доступу к медицинским услугам и заботе о детях, продолжительное профессиональное обучение и повышение квалификации, качественное образование и подготовка кадров, поддержка профсоюзов и коллективных договоров, повышение качества рабочих мест и др.

- развитие сотрудничества в сфере безопасноси посредством модернизации промышенности, альянса НАТО, Комитета по торговле и технологиями США - ЕС;

- привлечение инвестиций в физическую инфраструктуру, в частности, транспорт, широкополосную связь, водоснабжение и энергетику, соблюдение закона о полупроводниках для активизации;

Для снижения углеродных выбросов с 40% до 30%, индустрии полупроводников необходимо повысить уровень устойчивости к кибератакам посредством принятия закона О снижении инфляции».

В ходе исследования в соответствии с авторским подходом на основе индекса экономической кибербезопасности в результате прогнозного

[20] Авторская разработка

обоснования предложений и рекомендаций, предусмотренных в диссертаций, ожидаются следующие результаты:

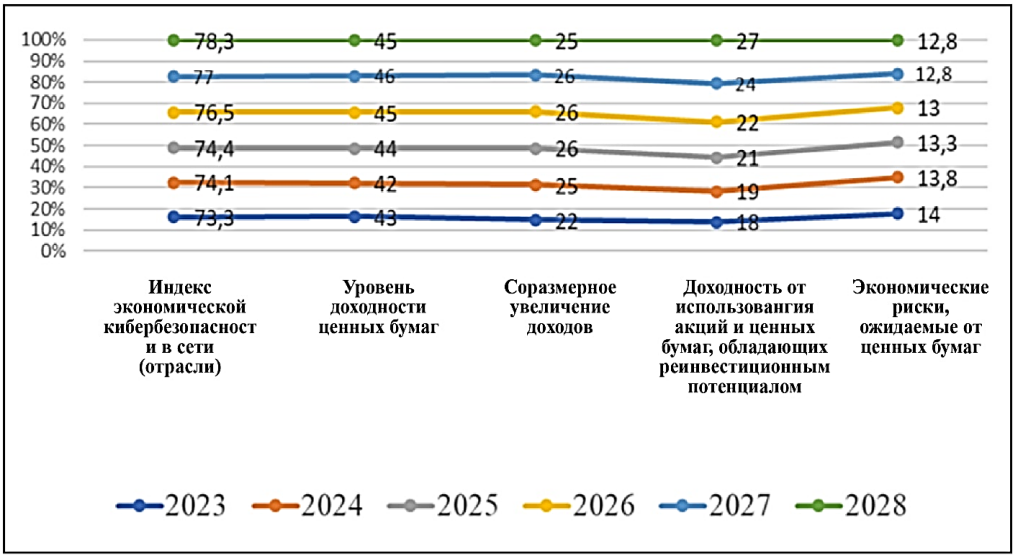


Рис. 5. Прогноз оценки экономической кибербезопасности согласно авторской разработке[21]

Помимо того, что внедрение умных технологий позволяет повысить индекс экономической кибербезопасности отрасли с 76,5% до 77%, ожидается также расширение объемов реализации ценных бумаг и повысить количество акционеров посредством трансформации рисков, связанных с обладанием акциями. Экономической основой является то, что помимо основных интересов у каждого хакера, они не пытаются нанести урон населению. Что согласно авторскому подходу к экономической кибербезопасности, нормирование может служить предотвращению хаоса и кризиса предприятия на финансовом рынке. В соответствии с эим, сформирован его промежуточный коэффициент (Таблица 10).

Таблица 12

Нормирование индекса экономической кибербезопасности предприятий энергетики в соответствии с авторским подходом

Название показателя	мин.	макс.	Примечание
S_i- индекс экономического кибербезопасности;	70	95	Снижение уровня безопасности отрасли снижает экономические параметры
F_i- измерение пропорционального значения существующих акций предприятий;	12	18	Чем выше значение акций, тем больше, кто обеспечивает их защиту
E_i- количество обладателей ценных бумаг;	20	200	Чем больше владельцев ценных бумаг, тем жестче борьба с хакерской деятельностью
P_{Fi}- среднее значение ценных бумаг;	40	55	Высокий уровень средних значений ценных бумаг ведет к снижению рисков и безопасности
D_i- среднее значение цен последних реализованных акций и ценных бумаг.	55	65	Пока показатель превышает 50% и не достигает 70 процентов, скорее всего выходит за рамки киберугрозы.
R_i- экономические риски ценных бумаг.	12	22	Риски являются основным критерием принятия и оценки решений для инвесторов

[21] Muallif ishlanmasi

Таким образом, соответствие коэффициента экономической кибербезопасности в диапазоне 0,7 и 0,95 позволяет оценить безопасность сети и может обеспечить стратегическое определение системы защиты.

ЗАКЛЮЧЕНИЕ

1. По мнению автора, под экономикой информационной безопасности понимается экономика, основанная на предотвращении экономического урона от средств пользователей информационных технологий.
2. Существует необходимость во внедрении способов обеспечения информационной безопасности организационно-экономической деятельности предприятия, исходя из эффективности собственной деятельности. В рамках системы распределения механизмов требуется активировать предложенный механизм кибербезопасности организационно-экономической деятельности.
3. Рекомендуется разработать механизм кибербезопасности организационно-хозяйственной деятельности акционерного общества «Тошкент иссиқлик электр стансиялар», а также установить алгоритм его цифровизации.
4. Обеспечение кибербезопасности обеспечения сырьем, фишинг поиска идентификационного расчетного счета хакера, осуществляющего логистических кибератаки, позволяют определить опыт злоумышленников, схему и стратегию атаки, а также оперативно найти их адреса..
5. Рекомендуется сформировать сценарий общей технико-хозяйственной защиты из-за стремления большинства хакеров к организации атак посредством сценария «умного блокчейна» в кибератака на заказ сырья.
6. В ходе проведения изысканий в сфере экономики кибербезопасности необходимо обосновать обеспечение экономической эффективности информационной безопасности тепловых электростанций с использованием дрифт-модели Куха, соблюдая кибергигиену и сохраняя моносистему.

ONE-TIME SCIENTIFIC COUNCIL NUMBER DSc.13/30.12.2019.T.07.02 ON GRANTING ACADEMIC DEGREES AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

KORABAEV ELDOR ALIJONOVICH

DIGITALIZATION OF INFORMATION SECURITY MECHANISMS OF ORGANIZATIONAL AND ECONOMIC ACTIVITIES OF ELECTRIC POWER INDUSTRY ENTERPRISES

08.00.16 – Digital economy and international digital integration

DISSERTATION ABSTRACT
of Doctor of Philosophy (PhD) on Economic sciences

Tashkent – 2024

The topic of the dissertation for the degree of Doctor of Philosophy (PhD) in Economic Sciences is registered by the Higher Attestation Commission under No. 2024.2.PhD/Iqt4303.

The dissertation was completed at the Tashkent University of Information Technologies. The dissertation abstract in three languages (Uzbek, Russian, English (summary)) is posted on the web page (www.tuit.uz) and on the Information and Educational Portal "ZiyoNet" (www.ziyonet.uz)

Scientific supervisor:	**Saitkamolov Muhammadhuja SobirxujA ugli** Doctor of Economic Sciences, Associate Professor
Official opponents:	**Samatov Gaffor Allakulovich** Doctor of Economic Sciences, Professor
	Muratova Shokhista Nigmatullaevna Doctor of Economic Sciences, Professor
Leading organization:	**Tashkent State Technical University named after Islam Karimov**

The defense of the dissertation will take place on "_____" _____ 2024 at _____ o'clock at the meeting of the scientific council DSc.13/30.12.2019.T.07.02 at the Tashkent University of Information Technologies. (Address: 100084, Tashkent, Amir Temur str., 108.

Tel.:(99871) 238-64-43; e-mail: info@tuit.uz).

The dissertation can be found at the Information Resource Center of the Tashkent University of Information Technologies (registration number No. 2870). (Address: 100084, Tashkent, Amir Temur str., 108. Tel.: (99871) 238-65-44).

The abstract of the dissertation was sent out on "_____" _____ 2024. (mailing protocol No.____ dated "____" _____ 2024).

B.Sh.Maxkamov
Chairman of the scientific council for awarding of scientific degrees, doctor of economic sciences, professor

E.Sh.Nazirova
Scientific secretary of the scientific council for awarding of scientific degrees, doctor of technical sciences, professor

Sh.Dj.Irgashxodjayeva
Chairman of the scientific seminar under the scientific council for awarding of scientific degrees, doctor of economic sciences, professor

INTRODUCTION (abstract of the dissertation for the Doctor of philosophy (PhD) on Economic Sciences)

The purpose of the study is to develop proposals and recommendations for improving the mechanisms of digitalization of information security of organizational and economic activities of enterprises in the electric power industry.

The object of the study is the information security of organizational and economic activities of JSC "Toshkent IES".

The subject of the study is economic relations arising in the process of activating the digitalization of information security mechanisms of organizational and economic activities of enterprises in the energy industry.

The scientific novelty of the study is as follows:

the feasibility of the economic cybersecurity index within $0.7 \leq C \leq 0.95$ based on the cyber defense potential, cybersecurity level and risk of energy industry enterprises, as well as the compliance of the protection system with strategic support has been substantiated;

the strategy for activating organizational and economic mechanisms for information security of enterprises in the electric power industry has been improved in accordance with the assessment of the target indicators of the process, justification of the chronological sequence of the multi-series, comparison of the international and national levels of cyber defense;

the forecast for the implementation of investment projects to ensure cybersecurity of the organizational and economic activities of “Toshkent IES” JSC for 2024-2029 has been substantiated, taking into account the strategic increase in the level of production modernization, expansion of opportunities for equal use of the impact of climate change and available services;

a forecast of the econometric scenario of organizational and economic cybersecurity of the processes of electric power components of “Toshkent IES” JSC for 2023-2028 has been developed, taking into account alternatives to organizational and economic activities and the proposed multi-collective strategy.

Implementation of the research results. Based on the obtained results on improving the mechanisms of digitalization of information security of organizational and economic activities of enterprises in the electric power industry:

proposals on the feasibility of the level of economic security within $0.7 \leq C \leq 0.95$ and the compliance of the protection system with strategic support in accordance with the values of cybersecurity potential, cybersecurity and risk of enterprises in the energy industry were put into practice by the order of JSC “Toshkent IES” dated April 12, 2023 No. 284 (certificate of the Ministry of Energy of the Republic of Uzbekistan dated April 3, 2024 No. 04-10-2259; certificate of JSC “Toshkent IES” dated March 27, 2024 No. 04-10-14/508). The results served to increase the level of information security of the organizational and economic activities of the company by 0.72%, increase the investment potential of the enterprise by 0.12% and reduce expenses in the organizational and economic activities of management by 229 million soums;

an improved approach to the strategy for activating the organizational and economic mechanisms of information security of enterprises in the electric power industry in accordance with the assessment of the target indicators of the process, justification of the chronological sequence of the multi-series, comparison of the international and national levels of cybersecurity were used in the development of the development strategy of JSC “Toshkent IES” (certificate of the Ministry of Energy of the Republic of Uzbekistan dated April 3, 2024 No. 04-10-2259; certificate of JSC “Toshkent IES” dated March 27, 2024 No. 04-10-14/508). The proposal to a certain extent served to further improve the quality of the development of the strategy for activating the organizational and economic mechanisms of information security, expanding the possibilities of application and increasing the effectiveness of target measures based on increasing the accuracy of the quantitative assessment of the process;

the forecast for the implementation of investment projects to ensure cybersecurity of the organizational and economic activities of JSC Toshkent IES for 2024-2029, taking into account the strategic increase in the level of production modernization, expansion of opportunities for equal use of the impact of climate change and available services, was used in the development of the development strategy of JSC “Toshkent IES” (certificate of the Ministry of Energy of the Republic of Uzbekistan dated April 3, 2024 No. 04-10-2259; certificate of JSC “Toshkent IES” dated March 27, 2024 No. 04-10-14/508). The implementation of the investment project to a certain extent served to increase the technical and economic resilience of the enterprise to cyber attacks in the context of profit growth;

the forecast of the econometric scenario of organizational and economic cybersecurity of the processes of electric power components of JSC Toshkent IES for 2023-2028, taking into account alternatives of organizational and economic activities and the proposed multi-collective strategy, was introduced into the practice of JSC “Toshkent IES” by order of April 12, 2023 No. 284 (certificate of the Ministry of Energy of the Republic of Uzbekistan dated April 3, 2024 No. 04-10-2259; certificate of JSC “Toshkent IES” dated March 27, 2024 No. 04-10-14/508). The implementation of the proposal to a certain extent served to improve the information security of JSC in 2023 in accordance with the effective organization of organizational and economic measures.

The structure and volume of the dissertation. The dissertation consists of an introduction, three chapters, a conclusion, a list of references. The volume of the dissertation is 130 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLICATIONS

1. Корабаев Э.А. Жаҳон мамлакатлари энергетика саноати корхоналарининг ташкилий-иқтисодий фаолиятинининг ахборот хавфсизлиги механизмлари/ Хоразм маъмун академияси ахборотномаси, 2024 йил, 2024-1/2 сон, 109-112 б.(08.00.00 №21)
2. Корабаев Э.А. Мамлакатдаги энергетика саноати корхоналарининг энерготизими ахборот хавсизлигининг ташкилий-иқтисодий ҳолати/ Хоразм маъмун академияси ахборотномаси, 2023 йил, 2023-12/5 сон, 45-51 б. (08.00.00 №21)
3. Корабаев Э.А. Энергетика саноати корхоналарининг киберхавфсизлик иқтисодиёти ва унинг муаммолари. Ижтимоий-гуманитар фанларнинг долзарб муаммолари. -№ S/9 (3)-2023. ISSN: 2181-1342 (Online) 44-52 https://scienceproblems.uz (Oliy attestatsiya komissiyasi Rayosatining 2022 yil 30 noyabrdagi 327/5-son qarori)
4. Korabaev E.A. Information security mechanisms of organizational and economic activity of energy industry enterprises of world countries/ Rontline marketing management and economics journal | (ISSN – 2752-700X) | November 09, 2023, VOLUME 03 ISSUE 11 Pages: 1-9. (08.00.00 №4)
https://doi.org/10.37547/marketing-fmmej-03-11-01
5. Korabaev E.A. Organizational and economic situation of energy system information security of energy industry enterprises in Uzbekistan/ Innovative Development in Educational Activities ISSN: 2181-3523 VOLUME 2 | ISSUE 23 | 2023, Pages: 86-94. (08.00.00 №4)
http://sjifactor.com/passport.php?id=22323
6. Korabaev E.A. The economics of cyber security in the energy industry and its assessment methods/ Innovative Development in Educational Activities ISSN: 2181-3523 VOLUME 2 | ISSUE 23 | 2023, Pages:75-85.
http://sjifactor.com/passport.php?id=22323
7. Korabaev E.A. Activity and effectiveness of information security in the mechanisms of organizational and economic activity of enterprises of the energy industry/ «MODELS AND METHODS IN MODERN SCIENCE» named International scientific-online conference, Issue 13, Part 2, December 25, 2023, 195-198 p. https://doi.org/10.5281/zenodo.10430026
8. Korabaev E.A. A brief description of the scientific and theoretical foundations of information security in the organizational and economic activity of the energy industry/ «ACADEMIC INTERNATIONAL CONFERENCE ON MULTI-DISCIPLINARY STUDIES AND EDUCATION» named International Scientific Online Conference:, Issue 22, Part 1, 31th December, 2023, 80-82 p.
https://aidlix.org/index.php/us/article/view/390
9. Корабаев Э.А. Энергетика саноатининг ташкилий-иқтисодий фаолиятида ахборот хавфсизлигининг илмий-назарий асослари/ Pedagogik

islohotlar va ularning yechimlari ilmiy va ilmiy texnik onlayn konferensiya. 2024. -B. 14-16. https://wordlyknowledge.uz/

10. Корабаев Э.А. Электр энергетика саноатида ташкилий-иқтисодий фаолиятининг ахборот хавфсизлигини моделлаштириш истиқболлари/ Ta’lim va innovatsion tadqiqotlar ilmiy va ilmiy texnik onlayn konferensiya. 2023. -B. 57-59. http://conf.sciencebox.uz/

Avtoreferat «_____» jurnali tahririyatida tahrirdan o‘tkazilib, o‘zbek, rus va ingliz tillaridagi matnlar o‘zaro muvofiqlashtirildi.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 3,5. Adadi 100 dona. Buyurtma № 35/24.

Guvohnoma № 851684.
«Tipograff» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko‘chasi, 83-uy.