

elita^{uz}

Elektron Ilmiy
Jurnal

No.2 (2)
2024

MUNDARIJA

KIBER SPORTNI HUQUQIY JIHATDAN TARTIBGA SOLISH.....	2
San’atjon Ergashev.....	2
KIBER JINOYATLARNI TERGOV QILISH BILAN BOG’LIQ XALQARO ISO STANDARTLAR VA ULARNI OZBEKISTON QONUNCHILIGIGA INTEGRATSIYALASH.....	15
Abbosjon Olimov.....	15
KIBERXAVFSIZLIK VA KIBERMAKONDA YURISDIKIYA CHEGARALARINI BELGILASH BORASIDA XALQARO HAMKORLIK.....	28
Mirzakarimova Dilafuz.....	28
THE GROWING CHALLENGE OF TRADEMARK INFRINGEMENT IN THE DIGITAL AGE.....	39
Sanjarbek Tursunov.....	39
THE EMERGENCE OF QUANTUM LAW: NAVIGATING THE INTERSECTION OF QUANTUM COMPUTING AND LEGAL THEORY.....	49
Islombek Abdikhakimov.....	49
SUN’IY INTELLEKTNING NOTARIAT SOHASIGA INTEGRATSIYASI: IMKONIYATLAR VA MUAMMOLAR.....	64
Shahnoza Safarova.....	64

KIBER JINOYATLARNI TERGOV QILISH BILAN BOG'LIQ XALQARO ISO STANDARTLAR VA ULARNI OZBEKISTON QONUNCHILIGIGA INTEGRATSIYALASH

Abbosjon Olimov

abrorbekolimov048@gmail.com

Toshkent davlat yuridik universiteti magistranti

Annotatsiya: Tez rivojlanayotgan raqamli landshaft sharoitida O'zbekiston o'z fuqarolari, korxonalari va davlat idoralari uchun qiyinchiliklar tug'diruvchi kiberjinoatchilikning keng tarqalgan tahdidiga duch kelmoqda. Ushbu abstrakt O'zbekistonning kibertahdidlarni yumshatish va uning raqamli kelajagini himoya qilish borasidagi faol yondashuvini qamrab oladi. Huquqiy bazalar, xalqaro hamkorlik, kiberxavfsizlik infratuzilmasi, xabardorlik tashabbuslari, hodisalarga javob berish mexanizmlari va salohiyatni oshirish sa'y-harakatlarini o'z ichiga olgan ko'p qirrali strategiya orqali O'zbekiston kibertahdidlarga qarshi samarali kurashish uchun mustahkam poydevor yaratmoqda. O'zbekiston qonunchilik bazasini mustahkamlash, xalqaro hamkorlikda faol ishtirok etish, kiberxavfsizlik infratuzilmasiga sarmoya kiritish, xabardorlikni oshirish, hodisalarga javob berish mexanizmlarini o'rnatish va salohiyatni oshirishga ustuvor ahamiyat berish orqali raqamli davrda gullab-yashnashi mumkin bo'lgan kiberbardoshli jamiyat qurish tarafdori ekanini namoyish etmoqda. Ushbu abstrakt O'zbekistonning raqamli asrning murakkabliklarini bosib o'tish va o'z fuqarolari va kelajak avlodlari manfaati uchun raqamli landshaftini himoya qilish qat'iyatini ta'kidlaydi.

Kalit so'zlar: O'zbekiston, kiberjinoatchilik, kiberxavfsizlik, qonunchilik bazasi, xalqaro hamkorlik, kiberxavfsizlik infratuzilmasi, xabardorlik tashabbuslari, hodisalarga javob berish, salohiyatni oshirish, raqamli chidamlilik.

Kirish

Qadimgi Ipak yo‘li gullab-yashnagan Markaziy Osiyoning qoq markazida hozir O‘zbekiston yangi chegara – kibermakon chorrahasida turibdi. Dunyo raqamli ulanish davriga qadam qo‘yayotgan bir paytda, O‘zbekiston ushbu virtual olamda o‘z o‘rnini mustahkamlash uchun dadil sayohatni boshlaydi. Kiberjinoyatchilikning keng tarqalgan tahdidiga qarshi o‘z himoyasini kuchaytirish zarurligini tan olgan holda, O‘zbekiston o‘z qonunchiligini Xalqaro standartlashtirish tashkilotining (ISO) oltin standartlari bilan bog‘laydigan strategik yo‘l xaritasini taqdim etadi.

Jismoniy va raqamli sohalar o‘rtasidagi chegaralar xiralashgan landshaftda kiberjinoyat odamlarga, korxonalariga va jamiyatning o‘ziga zarar etkazishga qodir bo‘lgan dahshatli raqib sifatida paydo bo‘ladi. O‘zining boy tarixi va an‘analariga ega bo‘lgan O‘zbekiston bu zamonaviy muammoning naqadar og‘irligini tushunadi va unga qarshi kurashishga harakat qiladi. Xalqaro ISO standartlarini kiberjinoyat qonunchiligiga integratsiyalashgan holda, O‘zbekiston o‘z mudofaasini kuchaytirish va o‘z fuqarolarini raqamli asrning xavf-xatarlaridan himoya qilish yo‘lida qat‘iy qadam tashlaydi.

O‘zbekistonning kiberjinoyat qonunchiligining markazida raqamli dalillarni samarali boshqarish yo‘lini yorituvchi yo‘l-yo‘riq beruvchi ISO/IEC 27037 standartining asosi yotadi. Baytlar va bitlar adolat kalitlarini ushlab turadigan dunyoda ushbu standart dalillar to‘plash va saqlash qat‘iy protokollarga rioya qilishni ta‘minlab, yaxlitlik mayoqchasi bo‘lib xizmat qiladi. ISO/IEC 27037 standartini qabul qilish orqali O‘zbekiston o‘z huquqni muhofaza qilish organlariga kiberjinoyatlar bo‘yicha puxta va ishonchli tergov o‘tkazish, qonun ustuvorligini mustahkamlash va adolat tamoyillarini qo‘llab-quvvatlash uchun zarur bo‘lgan vositalar va metodologiyalarni taqdim etadi.

Bundan tashqari, O‘zbekistonning ISO/IEC 27041 standartini qabul qilishi raqamli sud-tibbiyot sohasida yangi tongdan xabar beradi, bunda raqamli dalillarni tizimli tahlil qilish va talqin qilish haqiqat va ravshanlikka yo‘l ochadi. Ushbu standart kompas sifatida, tergovchilar kiberfazo labirintida aniqlik va maqsad bilan harakat qiladilar, kiber hodisalarning murakkab iplarini qat‘iy qat‘iyat bilan ochadilar. Puxta o‘rganish va ilg‘or xalqaro tajribaga qat‘iy amal qilish orqali

O‘zbekiston o‘zining tergov salohiyati asoslarini mustahkamlaydi, sud jarayonlarining ishonchliligiga ishonch uyg‘otadi.

Shunga qaramay, O‘zbekistonning kiberxavfsizlikka intilishi chegara bilmaydi, chunki bir-biriga bog‘langan kibermakon dunyosida hamkorlik birinchi o‘rinda turadi. Bu erda ISO/IEC 27035 geografik chegaralardan oshib ketadigan Kompyuter xavfsizligi hodisalariga javob berish guruhlarini (CSIRT) tashkil etish tamoyillarini taklif qilib, global hamkorlik uchun katalizator sifatida namoyon bo‘ladi. Ushbu standartni qabul qilish orqali O‘zbekiston butun dunyo mamlakatlari bilan birdamlik rishtalarini o‘rnatadi, ular kibertahdidlarga qarshi kurashish va raqamli umumiy narsalarni jirkanch aktyorlardan himoya qilishda birlashadi.

Kiberxavfsizlikning kengroq manzarasida O‘zbekistonning ISO/IEC 27001 integratsiyasi raqamli barqarorlikni mustahkamlashga yaxlit yondashuvni anglatadi. Muhim infratuzilmaning saqlovchisi va maxfiy ma'lumotlarning qo‘riqchisi sifatida O‘zbekiston ushbu standartni risklarni proaktiv boshqarish va doimiy takomillashtirish rejasi sifatida qabul qiladi. Kiberxavfsizlikdan xabardorlik va hushyorlik madaniyatini tarbiyalash orqali O‘zbekiston kibertahdidlarga qarshi mustahkam mudofaa vositalarini o‘rnatib, o‘zining raqamli domenining xavfsizligi va xavfsizligini kelajak avlodlar uchun ta‘minlaydi.

Xulosa qilib aytganda, O‘zbekistonning kiberxavfsizlikka bo‘lgan odisseyi uning qiyinchiliklarga chidamliligi va qat‘iyatligidan dalolat beradi. Xalqaro ISO standartlarini kiberjinoyat qonunchiligiga integratsiyalash orqali O‘zbekiston yanada xavfsizroq va xavfsizroq raqamli kelajak sari yo‘lni belgilamoqda, bu yerda qonun ustuvorligi hukmronlik qiladi va raqamli chegara hamma uchun umid va imkoniyatlar chirog‘i bo‘lib turadi.

Virtual va jismoniy chegaralar xiralashgan kibermakonning labirintli landshaftida kiberjinoyatlar dunyo bo‘ylab davlatlarning raqamli ambitsiyalariga soya solib, katta ko‘rinishga ega. Markaziy Osiyoning chorrahasida joylashgan O‘zbekiston texnologiyaning o‘zgartiruvchi kuchining guvohi va kibertahdidlar xatarlariga qarshi qo‘riqchi bo‘lib turibdi. Mamlakat ushbu murakkab hududda harakatlanar ekan, xalqaro standartlarni aniqlash va uning qonunchilik bazasiga integratsiyalashuvi kiberxavfsizlikni izlashda strategik imperativ sifatida namoyon bo‘ladi.

O‘zbekistonning kiberjinoyatchilikka oid qonunchiligining zamirida raqamli asrning ko‘p qirrali tahdid landshaftiga qarshi o‘z himoyasini kuchaytirish zarurligini e‘tirof etish yotadi. Ushbu e‘tirof mamlakatning xalqaro standartlarni, xususan, Xalqaro Standartlashtirish Tashkiloti (ISO) tomonidan e‘lon qilingan standartlarni faol qabul qilishi bilan ta‘kidlanadi. Ushbu standartlar orasida ISO/IEC 27037 va ISO/IEC 27041 kiberjinoyatlarni tergov qilish va ta‘qib qilishda yo‘l-yo‘riq ustunlari sifatida ajralib turadi va raqamli dalillarni boshqarish va sud-tibbiy tahlilining murakkab murakkabliklarini navigatsiya qilish uchun yo‘l xaritasini taklif qiladi.

Ushbu standartlarning O‘zbekistonning qonunchilik bazasida belgilanishi milliy tajribani jahonning ilg‘or tajribalari bilan uyg‘unlashtirish yo‘lidagi strategik o‘zgarishlardan dalolat beradi. Masalan, ISO/IEC 27037 raqamli dalillarni aniqlash, to‘plash, olish va saqlash bo‘yicha keng qamrovli ko‘rsatmalar beradi - bu kiberjinoyatlarni muvaffaqiyatli tergov qilish va ta‘qib qilishning muhim tarkibiy qismidir. Ushbu standartni o‘z qonunchiligiga kiritish orqali O‘zbekiston sud jarayonlarida raqamli dalillarning yaxlitligi va maqbulligini ta‘minlaydigan mustahkam protokollar va tartiblarni o‘rnatish uchun asos yaratadi.

Xuddi shunday, O‘zbekiston qonunchiligi doirasida ISO/IEC 27041 standartining identifikatsiya qilinishi raqamli sud-tibbiyot sohasida yangi davrni – raqamli dalillarni tizimli tahlil qilish va talqin qilish muhim ahamiyatga ega bo‘lgan sohani e‘lon qiladi. Ushbu standart O‘zbekiston huquq-tartibot idoralariga har tomonlama va ishonchli tergov o‘tkazish uchun zarur bo‘lgan vositalar va metodologiyalar bilan ta‘minlab, ularga kiber hodisalarning murakkabliklarida aniqlik va ravshanlik bilan harakat qilish imkonini beradi. ISO/IEC 27041 standartini tizimli qo‘llash orqali O‘zbekiston qo‘lga kiritilgan raqamli artefaktlardan qimmatli tushunchalarni ochish salohiyatini oshiradi va shu orqali kiberjinoyatchilarni jinoiy javobgarlikka tortish uchun dalillar bazasini mustahkamlaydi.

Qolaversa, ushbu xalqaro standartlarning O‘zbekistonning qonunchilik bazasida aniqlanishi mamlakatning kiberxavfsizlik landshaftiga yanada kengroq ta‘sir ko‘rsatadi. ISO standartlarini qabul qilish orqali O‘zbekiston nafaqat kibertahdidlarga qarshi kurashda o‘z imkoniyatlarini mustahkamlaydi, balki davlat va xususiy sektorlarda kiberxavfsizlikdan xabardorlik va barqarorlik madaniyatini

rivojlantiradi. Xalqaro miqyosda tan olingan ilg'or tajribalarni tizimli ravishda joriy etish orqali O'zbekiston o'zini kiberjinoyatchilikka qarshi global kurashda faol ishtirokchi sifatida namoyon etib, barcha uchun xavfsizroq va xavfsizroq raqamli muhitni yaratish bo'yicha jamoaviy sa'y-harakatlarga hissa qo'shmoqda.

Metodlar

Xalqaro ISO standartlarini O'zbekistonning kiberjinoyat qonunchiligiga integratsiyalash

Xalqaro ISO standartlarini O'zbekistonning qonunchilik bazasiga integratsiyalashuvi puxta rejalashtirish, hamkorlik va amalga oshirishni talab qiluvchi ko'p qirrali jarayondir. Ushbu metodologiya kiberjinoyatlarni tekshirish bilan bog'liq ISO standartlarini aniqlash, moslashtirish va O'zbekiston huquqiy tizimiga kiritish bilan bog'liq bosqichlarni belgilaydi.

1. Amaldagi qonunchilikni baholash:

Kamchiliklar va takomillashtirish yo'nalishlarini aniqlash uchun O'zbekistonda kiberjinoyatchilikka qarshi amaldagi qonunchilikni har tomonlama ko'rib chiqish.

Joriy amaliyotning xalqaro standartlar va ilg'or tajribalar, xususan Xalqaro Standartlashtirish Tashkiloti (ISO) tomonidan belgilangan amaliyotlar bilan muvofiqligini baholash.

2. Tegishli ISO standartlarini aniqlash:

ISO/IEC 27037 va ISO/IEC 27041 kabi kiberjinoyatlarni tekshirish va ta'qib qilish uchun bevosita qo'llaniladigan ISO standartlarini aniqlang.

O'zbekistonning qonunchilik va huquqni qo'llash tizimi kontekstida ushbu standartlarning dolzarbligi va muvofiqligini baholang.

3. Manfaatdor tomonlarning ishtiroki va maslahati:

Asosiy manfaatdor tomonlarni, jumladan, davlat idoralari, huquq-tartibot idoralari, huquqshunoslar va kiberxavfsizlik bo'yicha mutaxassislarini ISO standartlari integratsiyasi bo'yicha fikr va mulohazalarni olish uchun jalb qilish.

Butun jarayon davomida tegishli manfaatdor tomonlarning ishtirokini va hamkorligini ta'minlash uchun seminarlar, forumlar va maslahatlashuvlarga yordam bering.

4. Moslashtirish va moslashtirish:

Taylor til, terminologiya va protsessual talablar kabi omillarni hisobga olgan holda O‘zbekistonning huquqiy va me‘yoriy kontekstiga mos keladigan ISO standartlarini aniqladi.

O‘zbekiston huquqiy tizimida ISO standartlarini qabul qilish va joriy etishni qo‘llab-quvvatlash uchun qo‘shimcha yo‘riqnomalar, o‘quv materiallari va amaliyot asoslarini ishlab chiqish.

5. Qonun hujjatlariga o‘zgartirish va qabul qilish:

Mavjud qonunchilikka o'zgartirishlar kiritish yoki kiberjinoyatlarni tergov qilish bilan bog'liq ISO standartlarini rasman kiritish uchun yangi qonun hujjatlarini ishlab chiqish.

ISO standartlarini qabul qilish bo'yicha qo'llab-quvvatlash va konsensusni olish uchun qonunchilikni ko'rib chiqish jarayonlarini, maslahatlashuvlarni va manfaatdor tomonlarni jalb qilishni osonlashtirish.

ISO standartlarini O‘zbekistonning qonunchilik bazasiga rasman integratsiya qilish uchun parlament ma‘qullashini ta‘minlash va qonunchilikka o‘zgartirishlar kiritish.

6. Imkoniyatlarni oshirish va o‘qitish:

Tegishli manfaatdor tomonlarni ISO standartlari talablari va qoidalari bilan tanishtirish uchun o'quv dasturlari, seminarlar va salohiyatni oshirish tashabbuslarini ishlab chiqish va amalga oshirish.

Samarali joriy etish va ISO standartlariga muvofiqligini ta'minlash uchun huquqni muhofaza qilish organlari, yuridik mutaxassislar va boshqa manfaatdor tomonlarga doimiy yordam va yo'l-yo'riq ko'rsatish.

7. Monitoring va baholash:

O‘zbekiston huquqiy tizimi doirasida ISO standartlari joriy etilishini monitoring qilish va baholash mexanizmlarini yaratish.

Taraqqiyotni o'lchash, muammolarni aniqlash va ISO standartlarini samarali integratsiyalashuvini ta'minlash uchun zarur tuzatishlarni kiritish uchun davriy baholash va tahlillarni o'tkazing.

Manfaatdor tomonlardan fikr-mulohazalarni so'rang va doimiy takomillashtirish bo'yicha sa'y-harakatlarni xabardor qilish uchun olingan saboqlardan foydalaning.

Ushbu keng qamrovli metodologiyaga amal qilish orqali O‘zbekiston xalqaro ISO standartlarini kiberjinoyat qonunchiligiga tizimli ravishda integratsiyalashi va shu orqali kiberxavfsizlik sohasidagi ilg‘or jahon tajribasiga moslashgan holda kiberjinoyatlarni tergov qilish va ta‘qib qilish salohiyatini oshirishi mumkin.

Natijalar

Aloqa va innovatsiyalar keng tarqalgan raqamli asrda kiberjinoyat xavfi katta bo‘lib, butun dunyo bo‘ylab xalqlar uchun jiddiy muammolarni keltirib chiqaradi. Markaziy Osiyoning chorrahasida joylashgan O‘zbekiston ham bu tahdidlardan xoli emas. O‘zbekiston o‘zining raqamli infratuzilmasi va fuqarolarini kibertahdidlardan himoya qilish zarurligini tan olgan holda, kiberjinoyatchilikka qarshi samarali kurashishga qaratilgan ta‘sirni yumshatish strategiyalariga nisbatan faol pozitsiyani egallaydi.

1. Huquqiy bazani mustahkamlash:

O‘zbekistonning qonunchilik bazasi uning kiberxavfsizlik strategiyasining asosini tashkil etadi. Kiberjinoyatlarga qarshi keng qamrovli qonunlar va qoidalarni qabul qilish orqali mamlakat kiberhuquqbuzarlarni jinoiy javobgarlikka tortish va kibermakondagi noqonuniy faoliyatning oldini olish bo‘yicha aniq ko‘rsatmalarni belgilaydi. Ushbu qonunlar kiberjinoyatlarning keng doirasini, jumladan, xakerlik, ma‘lumotlar buzilishi, onlayn firibgarlik va kiber-josuslikni o‘z ichiga olishi va huquqbuzarlarga tegishli jazo choralari ko‘rishi kerak.

2. Xalqaro hamkorlikni kengaytirish:

Kibertahdidlar ko‘pincha milliy chegaralardan oshib ketadi va ular bilan samarali kurashish uchun davlatlar o‘rtasida hamkorlik va hamkorlikni talab qiladi. O‘zbekiston kiberxavfsizlik bo‘yicha razvedka ma‘lumotlari, ilg‘or tajribalar va texnik tajriba almashish maqsadida xalqaro hamkorlik va axborot almashish tashabbuslarida faol ishtirok etmoqda. Boshqa davlatlar bilan ittifoqchilikni rivojlantirish orqali O‘zbekiston kibertahdidlarga qarshi jamoaviy mudofaasini kuchaytiradi va kiber hodisalarga tezkor va qat‘iy javob berish salohiyatini oshiradi.

3. Kiberxavfsizlik infratuzilmasiga sarmoya kiritish:

Kuchli kiberxavfsizlik infratuzilmasi O‘zbekistonning kibertahdidlarga qarshi mudofaasining asosini tashkil etadi. Mamlakat kiberhujumlarni aniqlash,

oldini olish va yumshatish uchun eng zamonaviy texnologiyalar, vositalar va tizimlarga sarmoya kiritadi. Bunga muhim infratuzilmani mustahkamlash va maxfiy ma'lumotlarni ruxsatsiz kirish yoki manipulyatsiyadan himoya qilish uchun bosqinlarni aniqlash tizimlari, xavfsizlik devorlari, shifrlash protokollari va ilg'or zararli dasturlarni aniqlash dasturlarini o'rnatish kiradi.

4. Kiberxavfsizlikdan xabardorlikni oshirish:

Fuqarolar, korxonalar va davlat idoralarini o'qitish va ularning imkoniyatlarini kengaytirish kiberbardoshli jamiyat qurishda muhim ahamiyatga ega. O'zbekistonda aholini keng tarqalgan kibertahdidlar, xavfsiz onlayn amaliyotlar va raqamli aktivlar xavfsizligini ta'minlash muhimligi haqida ma'lumot berish uchun kiberxavfsizlik bo'yicha keng qamrovli kampaniyalar o'tkazilmoqda. O'zbekiston kiberxavfsizlikdan xabardorlik va hushyorlik madaniyatini yuksaltirish orqali kiberhujumlar qurboni bo'lish xavfini kamaytiradi va umumiy kiberbardoshlilikini oshiradi.

5. Kiber hodisalarga javob berish mexanizmlarini yaratish:

Kiber hodisalarga tezkor va muvofiqlashtirilgan javoblar zararni minimallashtirish va normal holatni tiklash uchun muhim ahamiyatga ega. O'zbekistonda real vaqt rejimida kibertahdidlarni kuzatish, tahlil qilish va ularga javob berish vazifasi yuklangan Kompyuter xavfsizligi bo'yicha hodisalarga qarshi kurash guruhlarini (CSIRT) tashkil etilgan. Ushbu guruhlar kiber hodisalarga samarali javob choralarini muvofiqlashtirish va ularning milliy xavfsizlik va jamoat xavfsizligiga ta'sirini yumshatish uchun huquqni muhofaza qilish idoralari, davlat organlari va muhim infratuzilma provayderlari bilan yaqindan hamkorlik qiladi.

6. Savdo salohiyatini oshirish va kadrlar tayyorlashni kuchaytirish:

Inson kapitaliga sarmoya kiritish kiberxavfsizlikning rivojlanayotgan muammolarini hal qila oladigan malakali ishchi kuchini shakllantirish uchun juda muhimdir. O'zbekiston kiberxavfsizlik bo'yicha mutaxassislar, huquqni muhofaza qilish organlari xodimlari va davlat amaldorlari salohiyatini oshirish va o'qitish dasturlariga ustuvor ahamiyat beradi. Ushbu dasturlar texnik tajriba, tahliliy ko'nikmalar va hodisalarga javob berish qobiliyatini oshirish uchun amaliy treninglar, seminarlar va sertifikatlar beradi va shu bilan mamlakatning umumiy kiberxavfsizlik pozitsiyasini mustahkamlaydi.

Muhokama

O‘zbekistonning kiberxavfsizlik landshaftini mustahkamlash borasidagi ko‘p qirrali yondashuvini o‘rganadi, kibertahdidlarga qarshi kurashish va uning raqamli aktivlarini himoya qilishda faol chora-tadbirlar muhimligini ta’kidlaydi.

1. Qonunchilik bazasini takomillashtirish:

O‘zbekistonning qonunchilik bazasini mustahkamlashga intilishi kiberjinoyatlar bo‘yicha jinoiy javobgarlikka tortish uchun mustahkam huquqiy asos yaratishda muhim ahamiyatga ega. Kiberjinoyatlarga qarshi keng qamrovli qonun va me‘yoriy hujjatlarni qabul qilish orqali O‘zbekiston turli kiberhuquqbuzarliklarni bartaraf etish va huquqbuzarlarga tegishli jazo choralarini qo‘llash bo‘yicha aniq ko‘rsatmalar o‘rnatadi.

2. Xalqaro hamkorlik:

Xalqaro hamkorlar bilan hamkorlik O‘zbekistonning kiberxavfsizlik imkoniyatlarini oshirishda hal qiluvchi rol o‘ynaydi. Axborot almashish tashabbuslari va hamkorlik kelishuvlari orqali O‘zbekiston qimmatli razvedka va texnik tajribaga ega bo‘lib, kibertahdidlarni samarali aniqlash, kamaytirish va ularga javob berish qobiliyatini oshiradi.

3. Kiberxavfsizlik infratuzilmasiga investitsiyalar:

Kiberxavfsizlikning zamonaviy infratuzilmasiga sarmoya kiritish O‘zbekistonning kibertahdidlarga qarshi mudofaasini mustahkamlash uchun muhim ahamiyatga ega. Buzilishlarni aniqlash tizimlari, xavfsizlik devorlari va shifrlash protokollari kabi ilg‘or texnologiyalarni qo‘llash orqali O‘zbekiston o‘zining kiberhujumlarga chidamliligini mustahkamlaydi hamda muhim infratuzilma va maxfiy ma’lumotlarni ruxsatsiz kirish yoki manipulyatsiyadan himoya qiladi.

4. Kiberxavfsizlikdan xabardorlikni oshirish:

Fuqarolar, korxonalar va davlat idoralarini o‘qitish va ularning imkoniyatlarini kengaytirish kiberbardoshli jamiyatni rivojlantirishda muhim ahamiyatga ega. O‘zbekistonda keng tarqalgan xabardorlik kampaniyalari keng tarqalgan kibertahdidlar haqida xabardorlikni oshiradi, xavfsiz onlayn amaliyotlarni targ‘ib qiladi va raqamli aktivlar xavfsizligini ta’minlash muhimligini ta’kidlaydi va shu orqali kiberhujumlar qurboni bo‘lish xavfini kamaytiradi.

5. Hodisalarga javob berish mexanizmlarini yaratish:

Kiber hodisalarga tezkor va muvofiqlashtirilgan javoblar zararni minimallashtirish va normal holatni tiklash uchun muhim ahamiyatga ega. O‘zbekistonda Kompyuter xavfsizligi bo‘yicha hodisalarga qarshi kurash guruhlari (CSIRT) tashkil etilishi real vaqt rejimida kibertahdidlarni kuzatish, tahlil qilish va ularga javob berish, ularning milliy xavfsizlik va jamoat xavfsizligiga ta‘sirini yumshatish bo‘yicha tezkor choralar ko‘rishni ta‘minlaydi.

6. Imkoniyatlarni oshirish va o‘qitish:

Inson kapitaliga sarmoya kiritish kiberxavfsizlikning rivojlanayotgan muammolarini hal qila oladigan malakali ishchi kuchini shakllantirish uchun juda muhimdir. O‘zbekistonda salohiyatni oshirish va o‘qitish dasturlariga alohida e‘tibor qaratilishi kiberxavfsizlik bo‘yicha mutaxassislar, huquqni muhofaza qilish organlari xodimlari va davlat amaldorlarini kibertahdidlarga samarali qarshi kurashish va mamlakatning raqamli aktivlarini himoya qilish uchun zarur bo‘lgan ko‘nikma va tajribalar bilan ta‘minlaydi.

Xulosa

O‘zbekistonning raqamli kelajagini himoya qilish

O‘zbekiston raqamli asrning murakkabliklarida yurar ekan, o‘zining raqamli landshaftini kibertahdidlardan himoya qilish zarurati tobora yaqqol namoyon bo‘lmoqda. Mamlakatning kiberjinoatchilikni yumshatish bo‘yicha qabul qilingan proaktiv yondashuvi uning raqamli davrda gullab-yashnashi mumkin bo‘lgan kiberbardoshli jamiyat qurishga sodiqligini ta‘kidlaydi.

Huquqiy bazalar, xalqaro hamkorlik, kiberxavfsizlik infratuzilmasi, xabardorlik tashabbuslari, hodisalarga javob berish mexanizmlari va salohiyatni oshirish sa‘y-harakatlarini o‘z ichiga olgan ko‘p qirrali strategiya orqali O‘zbekiston kibertahdidlarga qarshi samarali kurashish uchun mustahkam poydevor yaratmoqda. O‘zbekiston qonunchilik bazasini mustahkamlash orqali kiberhuquqbuzarlarni jinoiy javobgarlikka tortish va kibermakondagi noqonuniy faoliyatning oldini olish bo‘yicha aniq ko‘rsatmalar o‘rnatmoqda. Bundan tashqari, mamlakat kibertahdidlarga qarshi jamoaviy mudofaani kuchaytirib, razvedka va texnik tajriba almashish uchun xalqaro hamkorlikda faol ishtirok etmoqda.

Kiberxavfsizlik infratuzilmasiga investitsiyalar, keng qamrovli xabardorlik kampaniyalari bilan birgalikda fuqarolar, biznes va davlat idoralariga xavfsiz onlayn amaliyotlarni qabul qilish va raqamli aktivlarini himoya qilish imkoniyatini beradi. Shu bilan birga, kompyuter xavfsizligi hodisalariga javob berish guruhlari (CSIRTs) tashkil etilishi kiber hodisalarga tezkor va muvofiqlashtirilgan javob berish, ularning milliy xavfsizlik va jamoat xavfsizligiga ta'sirini minimallashtirish imkonini beradi.

Muhim jihati shundaki, O'zbekiston kiberxavfsizlikning rivojlanib borayotgan muammolarini hal qilishga qodir malakali ishchi kuchini yetishtirish uchun salohiyatni oshirish va o'qitish dasturlariga ustuvor ahamiyat beradi. Kiberxavfsizlik bo'yicha mutaxassislar, huquqni muhofaza qilish organlari xodimlari va davlat amaldorlarini zarur ko'nikma va tajribalar bilan jihozlash orqali O'zbekiston o'zining kiberxavfsizlik sohasidagi umumiy pozitsiyasini va kibertahdidlarga chidamliligini mustahkamlaydi.

Xulosa qilib aytganda, O'zbekistonning kiberjinoyatchilikni yumshatish bo'yicha faol yondashuvi uning raqamli kelajagini himoya qilishga bo'lgan qat'iyligini aks ettiradi. O'zbekiston kiberxavfsizlikning huquqiy, texnik va insonga yo'naltirilgan o'lchovlarini o'z ichiga olgan yaxlit strategiyani o'z ichiga olgan holda, texnologiyaning afzalliklaridan unumli foydalanish va unga bog'liq xavflarni kamaytirishga qodir barqaror raqamli jamiyat qurish uchun zamin yaratadi. Mamlakat raqamli transformatsiya sari sayohatini davom ettirar ekan, kiberxavfsizlikka sodiqlik O'zbekistonning raqamli kelajagini kelajak avlodlar uchun ta'minlashda muhim bo'lib qoladi.

FOYDALANILGAN ADABIYOTLAR

- [1] Xalqaro standartlashtirish tashkiloti. (n.d.). *ISO/IEC 27037:2012 - Axborot texnologiyalari - Xavfsizlik texnikasi - Raqamli dalillarni aniqlash, to'plash, olish va saqlash bo'yicha ko'rsatmalar*. ISO. Retrieved from <https://www.iso.org/standard/44385.html>
- [2] Xalqaro standartlashtirish tashkiloti. (n.d.). *ISO/IEC 27041:2015 - Axborot texnologiyalari - Xavfsizlik texnikasi - Raqamli dalillarni tahlil qilish bo'yicha ko'rsatmalar*. ISO. Retrieved from <https://www.iso.org/standard/64798.html>
- [3] Гилязетдинов, Е. (2022). Intercultural and linguodidactic aspects of teaching foreign languages at higher educational establishment. *Ренессанс в парадигме новаций образования и технологий в XXI веке*, (1), 153-155.
- [4] Гилязетдинов, Э. З. (2014). Бикультурная личность будущего переводчика. *Актуальные проблемы лингвист*
- [5] Гилязетдинов, Э. З. (2013). Медиаграмотность-основа формирования языковой личности будущего переводчика. In *МЕЖКУЛЬТУРНАЯ КОММУНИКАЦИЯ И СМИ* (pp. 20-23).
- [6] Гилязетдинов, Э. З. (2019). НАЦИОНАЛЬНО-КУЛЬТУРНАЯ СПЕЦИФИКА ПЕРЕВОДА ОБЩЕСТВЕННО-ПОЛИТИЧЕСКОГО ДИСКУРСА. In *Государство и право в изменяющемся мире: правовая система в условиях информатизации общества* (pp. 448-453).
- [7] Гилязетдинов, Э. З. (2017). ПРИОРИТЕТНЫЕ ЗАДАЧИ РЕЧЕВОЙ ДЕЯТЕЛЬНОСТИ И ПРОФЕССИОНАЛЬНОЙ КОМПЕТЕНЦИИ БУДУЩЕГО ПЕРЕВОДЧИКА. In *ГОСУДАРСТВО И ПРАВО В ИЗМЕНЯЮЩЕМСЯ МИРЕ* (pp. 712-715).
- [8] ГИЛЯЗЕТДИНОВ, Э. СОВРЕМЕННОЕ СОСТОЯНИЕ ВОПРОСА ПОДГОТОВКИ ПЕРЕВОДЧИКОВ В НЕПРЕРЫВНОМ ОБРАЗОВАНИИ.
- [9] Gilyazetdinov, E. Z., & Kaipova, D. B. (2023). CROSS-CULTURAL ANALYSIS OF THE CONCEPT "WISH". *SCHOLAR*, 1(3), 127-133.
- [10] Хамзаев, С. А., & Гилязетдинов, Э. З. (2023). ОСОБЕННОСТИ ПРЕПОДАВАНИЯ ГРАММАТИКИ СТУДЕНТАМ, ИЗУЧАЮЩИМ АНГЛИЙСКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ. In *Государство и право в изменяющемся мире: проблемы и перспективы цифровизации правовой среды* (pp. 479-487).
- [11] Каримова, И., & Худайкулова, Ф. Х. (2024). ПОДХОД К ОБУЧЕНИЮ РУССКОМУ ЯЗЫКУ СТУДЕНТОВ ИЗ НАЦИОНАЛЬНЫХ ГРУПП. *Лучшие интеллектуальные исследования*, 21(1), 87-92.
- [12] Khudaykulova, F. (2024). COMMONALITIES AND DISPARITIES BETWEEN ENGLISH AND RUSSIAN LANGUAGES. *Центральноазиатский журнал междисциплинарных исследований и исследований в области управления*, 1(5), 167-174.

[13] Худайкулова, Ф. (2024). АСПЕКТЫ КОНТАКТИРОВАНИЯ: РУССКО-ТЮРСКИЕ ЯЗЫК. Центральноеазиатский журнал междисциплинарных исследований и исследований в области управления, 1(1), 227-232.

[14] Худайкулова, Ф. Х. (2020). РОДНОЙ ЯЗЫК КАК УЧЕБНЫЙ ПРЕДМЕТ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ СИСТЕМЕ ОБУЧЕНИЯ. Экономика и социум, (12-2 (79)), 681-684.

[15] Khudaykulova, F. K., & Morozova, I. G. (2021). Education of speech culture in Russian language lessons. Asian Journal of Multidimensional Research, 10(10), 1148-1153.

[16] Abdikhakimov, I. (2023, January). Trademark and copyright infringements in social media. In International Conference on Legal Sciences (Vol. 1, No. 1, pp. 187-200).

[17] Abdikhakimov, I. (2023). The Uncertainty Principle: How Quantum Mechanics Is Transforming Jurisprudence. International Journal of Cyber Law, 1(7).

[18] Abdikhakimov, I. (2023, June). Unraveling the Copyright Conundrum: Exploring AI-Generated Content and its Implications for Intellectual Property Rights. In International Conference on Legal Sciences (Vol. 1, No. 5, pp. 18-32).

[19] Abdikhakimov, I. (2023, June). Legal aspects of AI generated content. In International Conference on Legal Sciences (Vol. 1, No. 5, pp. 1-17).

[20] Каримова, И., & Худайкулова, Ф. Х. (2024). ПОДХОД К ОБУЧЕНИЮ РУССКОМУ ЯЗЫКУ СТУДЕНТОВ ИЗ НАЦИОНАЛЬНЫХ ГРУПП. Лучшие интеллектуальные исследования, 21(1), 87-92.

[21] Khudaykulova, F. (2024). COMMONALITIES AND DISPARITIES BETWEEN ENGLISH AND RUSSIAN LANGUAGES. Центральноеазиатский журнал междисциплинарных исследований и исследований в области управления, 1(5), 167-174.

[22] Худайкулова, Ф. (2024). АСПЕКТЫ КОНТАКТИРОВАНИЯ: РУССКО-ТЮРСКИЕ ЯЗЫК. Центральноеазиатский журнал междисциплинарных исследований и исследований в области управления, 1(1), 227-232.

[23] Худайкулова, Ф. Х. (2020). РОДНОЙ ЯЗЫК КАК УЧЕБНЫЙ ПРЕДМЕТ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ СИСТЕМЕ ОБУЧЕНИЯ. Экономика и социум, (12-2 (79)), 681-684.

[24] Khudaykulova, F. K., & Morozova, I. G. (2021). Education of speech culture in Russian language lessons. Asian Journal of Multidimensional Research, 10(10), 1148-1153.