



KIBER XAVFSIZLIK VA RAQAMLI IQTISODIYOTDAGI XAVFSIZLIGI MASALALARI



Bobomurodova Dilshoda Ibodulla qizi

Qarshi davlat universiteti Iqtisodiyot
fakulteti iqtisodiyot yo'nalish 3-bosqich talabasi.

Yaxshiqulova Moxinur Toxir qizi

Ilmiy rahbar: Qarshi davlat universiteti Iqtisodiyot
fakulteti o'qituvchisi

Annotatsiya: Ushbu maqola raqamli iqtisodiyot rivojlantirishning asosiy omillaridan biri hisoblangan kiberxavfsizlikni ta'minlash masalalariga bag'ishlangan. Kiberxavfsizlik va uning asosiy tushunchalari, axborotning kriptografik himoyasi, foydalanishni nazoratlash, tarmoq xavfsizligi, foydalanuvchanlikni ta'minlash usullari, dasturiy vositalar xavfsizligi, axborot xavfsizligi siyosati va risklarni boshqarish, kiberjinoyatchilik, kiberhuquq, kiberetika hamda inson xavfsizligini nazariy va amaliy asoslarini qo'llanilishi, shuningdek, maqolada kiberxavfsizlik bo'yicha O'zbekistonda amalga oshirilayotgan ishlar ko'rib chiqilgan. Shuningdek mamlakatimizning kiberxavfsizlik bo'yicha xalqaro global reytingdagi o'rni qisqacha yoritilgan.

Kalit so'zlar: Kiberxavfsizlik, kiberxujum, axborot tizimlari, konfidensiallik, risk, SSL, milliy segment, "Kiberxavfsizlik Markazi" DUK.

Kiberxavfsizlik" atamasi va kontsepsiyasini oshkor qilish bo'yicha muhokama takliflari asosli ravishda taqdim etgan. "Kiberxavfsizlik" atamasining ochilishi, shuningdek, "kiberxavfsizlik" va "axborot xavfsizligi" tushunchalarining funksional korrelyatsiyasini (paradigmasini) qiyosiy tahlil qilish natijalariga asoslanib, axborot qarama-qarshiligida paritetga zaruriy rioya qilishni hisobga olgan. Rossiya Federatsiyasida kiberxavfsizlikni joriy etish va rivojlantirish bo'yicha ba'zi takliflar shakllantirilgan [1].

Zamonaviy dunyoda yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat kundan-kun axborot-kommunikatsiya texnologiyalariga tobora ko'proq qaram bo'lib borayotganligini hisobga olib, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega va juda muhim mavzuga aylanmoqda. Bugungi kunda axborot jamiyatini rivojlantirishning zaruriy sharti bu kiberxavfsizlikdir, uni xavfsizlikning texnik va qonunchilikgacha bo'lgan deyarli cheksiz ro'yxati va ularni hal qilish yo'li bilan ta'minlash mumkin. kiberxavfsizlik masalalari alohida kompyuter vositasida axborot xavfsizligi darajasidan har bir davlatning axborot va milliy xavfsizligining ajralmas qismi

sifatida yagona kiberxavfsizlik tizimini yaratish darajasigacha boradi. Shu sababli, har bir tashkilot uchun kiberxavfsizlikni ta'minlash maqsadida mazkur soha bilan shug'ullanuvchi xodimlar jalb qilinmoqda va xodimlarni kiberxavfsizlikka oid bilimlar bilan doimiy tanishtirib boorish uchunqator seminartreyning mashg'ulotlari tashkil etilmoqda. Oliy ta'lim muassasalarida ham kiberxavfsizlikni fan sifatida o'tilishi buning yaqqol misolidir.

"Kiberxavfsizlik va raqamli iqtisodiyotdagi xavfsizlik masalalari" bo'yicha maqola mavzusi raqamli iqtisodiyotning global rivojlanishida dolzarb masala sanaladi. Ushbu mavzuni yoritishda quyidagi asosiy yo'nalishlarga e'tibor qaratish mumkin:

1. Raqamli iqtisodiyotda kiberxavfsizlikning roli

Raqamli iqtisodiyotda kiberxavfsizlikning asosiy vazifalari va uning ahamiyati.

Internet orqali amalga oshiriladigan moliyaviy operatsiyalar va shaxsiy ma'lumotlarning himoya qilish zaruriyati.

Ma'lumotlar xavfsizligini ta'minlash orqali iqtisodiy jarayonlarga ijobiy ta'sir ko'rsatish.

2. Kiber tahdidlar va ularning raqamli iqtisodiyotga salbiy ta'siri

Hakerlik hujumlari, fishing, ziyonli dasturlar kabi kiber tahdidlar va ularning iqtisodiyotga yetkazishi mumkin bo'lgan zarar.

Xakerlar tomonidan olib boriladigan firibgarliklar va ma'lumot o'g'irliklari iqtisodiy yo'qotishlarga olib kelishi.

Korxonalar va tashkilotlarga qaratilgan kiber hujumlar va ularning moliyaviy jihatdan olib keladigan talafotlari.

3. Kiberxavfsizlikning global iqtisodiyotga ta'siri

Dunyo mamlakatlaridagi kiberxavfsizlik siyosatlari va ularning global iqtisodiy o'zgarishlarga ta'siri.

Xalqaro tashkilotlarning kiberxavfsizlikni ta'minlash bo'yicha olib borayotgan tadbirlari va standartlashtirish jarayonlari.

Transmilliy korxonalar uchun raqamli xavfsizlik bo'yicha xalqaro me'yor va ko'rsatmalarning ahamiyati.

4. Raqamli iqtisodiyotda davlatning kiberxavfsizlikni ta'minlashdagi roli

Davlat tomonidan ishlab chiqilgan kiberxavfsizlik siyosati va qonunchilik me'yorlari.

Raqamli xavfsizlik sohasidagi davlat dasturlari va ularning iqtisodiyotni himoya qilishdagi ahamiyati.

Iqtisodiyotning raqamli transformatsiyasi jarayonida davlat va xususiy sektor hamkorligining o'rni.

5. Kiberxavfsizlik sohasidagi zamonaviy texnologiyalar

Sun'iy intellekt va mashina o'rganish texnologiyalari orqali kiber tahdidlarni aniqlash va bartaraf etish.

Kriptografiya va blokcheyn texnologiyalari orqali ma'lumotlarni xavfsiz saqlash usullari.

Bulutli saqlash xizmatlarida xavfsizlik choralari rivojlanishi va ularning foydalari.

6. Raqamli iqtisodiyotdagi kiberxavfsizlik masalalari bilan bog'liq muammolar

Raqamli tafovut va texnologik bilim yetishmasligi sababli kiberxavfsizlikka e'tibor yetarlicha qaratilmasligi.

Xodimlarning axborot xavfsizligi sohasidagi bilim va ko'nikmalarini rivojlantirish masalasi.

Moliyaviy cheklovlar tufayli kichik va o'rta bizneslar uchun yuqori darajadagi kiberxavfsizlik choralarini tatbiq etish qiyinligi.

7. Kiberxavfsizlikda o'zgaruvchan muhit va yangi yo'nalishlar

Kiberxavfsizlikda tahdidlarni muntazam kuzatish va himoya strategiyalarini yangilash zaruriyati.

Bozorda paydo bo'layotgan yangi texnologiyalarning xavfsizlikka ta'siri va ularni boshqarish usullari.

“Zero Trust” (nol ishonch) modeli va unga asoslangan himoya yondashuvlari.

Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan ba'zi mutaxassislar kiberxavfsizlikka oid atamalarga quyidagicha ta'rif berishgan:

Konfidensiallik - axborot yoki uni eltuvchining shunday holati bo'lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo'ladi. Konfidensiallik axborotni ruxsatsiz "o'qish"dan himoyalash bilan shug'ullanadi. Ayniqsa, bank sistemasida bank uchun konfidensiallik juda muhim.

Risk - potensial foyda yoki zarar bo'lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo'shilganida risk paydo bo'ladi. ISO "risk - bu noaniqlikning maqsadlarga ta'siri" sifatida ta'rif bergan.

Axborot xavfsizligi - axborotning holati bo'lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz undan foydalanishga yo'l qo'yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalani sathi holati.

Kiberxavfsizlik 8 ta bilim sohasiga bo'lingan:

- Ma'lumotlar xavfsizligi;
- Dasturiy ta'minot xavfsizligi;
- Tashkil etuvchilar xavfsizligi;
- Aloqa xavfsizligi;
- Tizim xavfsizligi;
- Inson xavfsizligi;
- Tashkilot xavfsizligi;
- Ijtimoiy xavfsizlik.

O'zbekiston Respublikasi prezidentining “2017 –2021 yillarda O'zbekiston respublikasini rivojlantirishning beshta ustuvor yo'nalishi bo'yicha harakatlar strategiyasini «Ilm, ma'rifat va raqamli iqtisodiyotni rivojlantirish yili»da amalga oshirishga oid davlat dasturi to'g'risida”gi Farmoni, 2020 yil 2 mart, PF-5953-son Kiberxavfsizlik keng ma'noda axborot texnologiyalari, ya'ni qurilmalar, dasturlar, axborot tizimlari va ma'lumotlar himoyasiga qaratilgan chora-tadbirlar majmuidir. Ya'ni ma'lumotlar konfidentsialligini saqlash, ularning butunligini himoyalash, dastur va axborot tizimlarini buzilishsiz to'laqonli ishlashi demakdir. Bu esa ishlab chiqarish samaradorligining oshishiga xizmat qiladi.

Dobrodeev Aleksandr Yurievich texnika fanlari doktori, professor tadqiqotlarida xalqaro va milliy kiberxavfsizlikni ta'minlashning dolzarb muammolarini ko'rib

chiqqan va zamonaviy tahdidlarga mos keladigan harbiy va davlat organlarining avtomatlashtirilgan tizimlarining kiberxavfsizligini ta'minlashning adekvat tizimini yaratishga yondashuvlar taklif etgan. Xalqaro va milliy kiberxavfsizlikning dolzarb muammolari ko'rib chiqilib, harbiy va hukumat avtomatlashtirilgan tizimlarining kiberxavfsizligining hozirgi tahdidlarining adekvat tizimini ishlab chiqishga yondashuvlar keltirilgan [2].

Sachin Bhosale texnika fanlari doktori, professoro'z tadqiqotlarida texnologiyalar va tarmoq ulanishlari bilan boshqariladigan hozirgi dunyoda kiberxavfsizlik nima ekanligini bilish va undan samarali foydalana olish juda muhimdir. Tizimlar, muhim fayllar, ma'lumotlar va boshqa muhim virtual narsalar, agar ularni himoya qilish uchun xavfsizlik bo'lmasa, xavf ostida. Bu IT firmasi bo'ladimi, har bir kompaniya bir xil darajada himoyalangan bo'lishi kerak. Kiberxavfsizlikda yangi texnologiyalarning rivojlanishi bilan tajovuzkorlar ham xuddi shunday ortda qolmaydi. Ular yaxshi va takomillashtirilgan xakerlik usullarini iste'mol qilmoqdalar va u erdagi ko'plab korxonalarining zaif tomonlarini maqsad qilib qo'ymoqdalar. Kiberxavfsizlik juda muhim, chunki harbiy, hukumat, moliyaviy, tibbiy va korporativ tashkilotlar shaxsiy kompyuterlar va boshqa qurilmalarda misli ko'rilmagan miqdordagi ma'lumotlarni to'playdi, mashq qiladi va zaxiralaydi. Ushbu ma'lumotlarning muhim kvotasi maxfiy ma'lumotlar bo'lishi mumkin, xoh bu moliyaviy ma'lumotlar, intellektual mulk, shaxsiy ma'lumotlar yoki noqonuniy kirish yoki tanishish salbiy tashvishlarni keltirib chiqarishi mumkin bo'lgan boshqa turdagi ma'lumotlar [3].

Raqamli ma'lumotlarni boshqarishda kiberxavfsizlikni ta'minlash muhim omil sanaladi. Bunda asosiy e'tibor raqamli ma'lumotlarga ruxsatsiz kirish, ularni axborot vositachilaridan himoya qilgan holda xavfsizligini ta'minlash va axborotlar uzatishning soddaligi va foydalanuvchanligini ta'minlashga qaratilishi lozim.

Iqtisodiyotning barcha sohalarida avtomatlashtirish axborot tizimlaridan foydalanilganda, kiberxavfsizlik masalasiga alohida e'tibor qaratish lozim.

Ma'lumotlar raqamli formatga o'tkazilsa, elektron ko'rinishda saqlansa, shundagina axborot va kiberxavfsizlik masalasi dolzarblik kasb etadi. Davlatimiz rahbari tomonidan kiberxavfsizlikni ta'minlash sohasi mutaxassislariga shunday talab qo'yilganki, ular bu borada ro'y bergan. noxush hodisalarni o'rganishlari va bartaraf etishlari emas, balki bunday holatni oldindan ko'ra bilishlari, ya'ni oldini olishga xarakat qilishlari kerak [4].

Raqamlashtirish va kiberxavfsizlik tushunchalari doimo yonma-yon keladi. Chunki barcha tizim va jarayonlarni raqamlashtirish bilan birga, ularning texnik jihatdan mukammal va bexato ishlashini, xavfsizligini ta'minlash muhim hisoblanadi. Yurtimizda raqamli iqtisodiyotni rivojlantirishga qanchalik e'tibor qaratilayotgan bo'lsa, kiberxavfsizlikni ta'minlashga ham shuncha ahamiyat berilmoqda. Bunga yaqqol misol sifatida har yili Halqaro elektroaloqa ittifoqi tomonidan e'lon qilinadigan kiberxavfsizlik bo'yicha halqaro global reytingda yuqori o'rinlardan joy olishini ko'rsatish mumkin.

Kiberxavfsizlik bo'yicha xalqaro global reyting ABI Research va HEI (Halqaro elektroaloqa ittifoqining qo'shma loyihasi bo'lib, indeks davlatlarning kiberxavfsizlik sohasidagi ishtiroki darajasini baholash imkonini beradi. Bunda majburiyatlar darajasi

bash sohada baholanadi: huquqiy choralar, texnik choralar, tashkiliy choralar, salohiyatning rivoji va xalqaro hamkorlik.

Kiberxavfsizlik keng ma'noda axborot texnologiyalari, ya'ni qurilmalar, dasturlar, axborot tizimlari va ma'lumotlar himoyasiga qaratilgan chora- tadbirlar majmuidir. Ya'ni ma'lumotlar konfidentsialligini saqlash, ularning butunligini himoyalash, dastur va axborot tizimlarini buzilishlarsiz to'laqonli ishlashi demakdir. Bu esa ishlab chiqarish samaradorligining oshishiga xizmat qiladi [5].

"Kiberxavfsizlik markazi" DUK tahlillariga ko'ra, 2023 yilda internetning milliy tarmog'i segmenti 677 ta rasmiy veb-saytlarida 1 168 ta zaiflik, 158 ta kiberxavfsizlik intsidenti aniqlangan va zaifliklarning 587 tasi bartaraf etilgan. Shulardan 105 tasi kontentni ruxsatsiz yuklash. 26 tasi defeys. 15 tasi ma'lumotlarga ruxsatsiz kirish, 4 tasi DDOS hujum. 3. tasi Spam xabar yuborish, 2 tasi URLni qayta yo'naltirish, 2 tasi Saytlararo scripting va bittasi Fishing xabar ulushiga to'g'ri keladi [7].

Kibermakonda xavfsizlik bilan bog'liq muammolarning yuzaga kelishiga dasturiy kodda xavfsizlik xatolari mavjud bo'lgan kontentni boshqarish, dasturiy vositalarning eskirgan versiyalari bilan ishlash, kirish parallarining osonligi, xavfsiz bo'lmagan manbalardan yuklab olingan shablonlar, viruslar bilan zararlangan kompyuterlarda veb-saytlarni boshqarish kabilar sabab bo'ladi.

"Kiberxavfsizlik to'g'risida"gi qonunda esa axborot kommunikatsiya va texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo'yicha zamonaviy mexanizmlarni joriy etish. mazkur sohada davlat organlari, korxonalar va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish kabilar aks etishi kutilmoqda. Yurtimizda olib borilayotgan barcha islohotlar zamirida xalqimizga qulayliklar yaratish maqsadi yotibdi. Kiberxavfsizlikni ta'minlashga alohida e'tibor qaratilishi raqamli imkoniyatlardan ishonchli va xavfsiz tarzda foydalanishga zamin bo'lib kelmoqda. Iqtisodiyotning barcha sohalarini raqamlashtirish jahon hamjamiyatiga integratsiyalashuv, dunyo bozorida o'z o'rniga ega bo'lish, iqtisodiy ravnaq topish, aholiga qulayliklar yaratish imkoniyatini beradi. Quvonarlisi, bu mamlakatimizda asosiy kun tartibidagi masala. Raqamlashtirish borasida O'zbekiston dadil odimlar bilan ildamlamoqda. Mamlakatimizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta'lim, sog'liqni saqlash va qishloq xo'jaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish bo'yicha kompleks chora-tadbirlar amalga oshirilmoqda. Xususan, elektron hukumat tizimini takomillashtirish, dasturiy mahsulotlar va axborot texnologiyalarining mahalliy bozorini yanada rivojlantirish, respublikaning barcha hududlarida IT-parklarni tashkil etish, shuningdek, sohani malakali kadrlar bilan ta'minlashni ko'zda tutuvchi 220 dan ortiq ustuvor loyihalarni amalga oshirish boshlangan. Bundan tashqari, 40 dan ortiq axborot tizimlari bilan integratsiyalashgan geoportalni ishga tushirish, jamoat transporti va kommunal infratuzilmani boshqarishning axborot tizimini yaratish, ijtimoiy sohani raqamlashtirish va keyinchalik ushbu tajribani boshqa hududlarda joriy qilishni nazarda tutuvchi Raqamli Toshkent kompleks dasturi amalga oshirilmoqda. Yuqorida sanab o'tilgan vazifalarni amaliyotga joriy etishda ma'lumotlar xavfsizligiga alohida ahamiyat qaratish kerak. Chunki mamlakatning iqtisodiy, ijtimoiy, madaniy rivojlanishining statistik

ko'rsatkichlarining haqqoniyligi, ishonchliligi va konfidentsialligini ta'minlash bugungi kundagi dolzarb muammolardan biri hisoblanadi.

Xulosa va takliflar:

Kiberxavfsizlikka doir me'yorlarning huquqiy jihatdan mustahkamlanishi nihoyatda zarur. Raqamli olam hali-hamon huquqiy jihatdan o'z maqomini aniq belgilay olgani yo'q. Kun sayin tahdidlarning yangi tur va shakllari paydo bo'layotganligi, ularni qonunchilikda aks ettirish zarurligi talab etadi. Kiberxavfsizlikka doir milliy strategiyani ishlab chiqish milliy kibermakonda jinoyatchilikka qarshi qurashish sohasidagi faoliyatni tartibga soladi. Zero, virtual olamdagi jinoyatchilikning zarar va xavfi real olamdagidan kam emas. 2020- 2023 yillarga mo'ljallangan kiberxavfsizlikka doir milliy strategiyaga ko'ra kiberxavfsizlikning yagona tizimi va muhim hisoblangan infratuzilmani kiberhujumlardan himoya qilish sohasidagi huquqiy baza shakllantiriladi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi prezidentining "2017 –2021 yillarda O'zbekiston respublikasini rivojlantirishning beshta ustuvor yo'nalishi bo'yicha harakatlar strategiyasini «Ilm, ma'rifat va raqamli iqtisodiyotni rivojlantirish yili»da amalga oshirishga oid davlat dasturi to'g'risida"gi Farmoni, 2020 yil 2 mart, PF-5953-son

2. O'zbekiston Respublikasi prezidentining "Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to'g'risida"gi Farmoni, 2018 yil 19 fevral, PF-5349-son

3. O'zbekiston Respublikasi prezidentining "«Raqamli O'zbekiston -2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi Farmoniga 1-ilova "Raqamli O'zbekiston –2030" strategiyasi. 2020 yil 5 oktyabr, PF-6079-son.

4. O'zbekiston Respublikasi prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to'g'risida"gi qarori. 2018 yil 21 noyabr, PQ- 4024-son.

5. www.itu.int - Xalqaro elektroaloqa uyushmasining rasmiy sayti

6. <https://tace.uz> - Kiberxavfsizlik markazi davlat unitar korxonasi rasmiy sayti.

7. cyberleninka.ru

Copyright: © 2024 by the authors. This work is licensed under a Creative Commons Attribution- 4.0 International License (CC - BY 4.0)

