



RAQAMLI DUNYODAGI XAVFLAR

Quldoshev Otabek Zarif o'g'li
kuldoshevotabek87@gmail.com

Annotatsiya: Shu qatorda Raqamli dunyodagi xavflar mavzusidagi annatatsiya, kiberxavfsizlik va ma'lumotlar himoyalash sohasidagi muhim masalalar va ularning yechimlari bo'yicha ma'lumotlar, ko'ngil ochar, o'qituvchi, va ilmiy tadqiqotchilar uchun qiziqarli bo'lishi mumkin. Bu masalalar kiberxavfsizlik sohasidagi yangi rivojlanishlarni o'rganish, mavjud xavf-faktorlarini tushuntirish va ularni kamaytirish uchun tavsiyalarni izlashga yordam berishi mumkin.

Kalit so'zlar: Raqamli dunyodagi xavflar haqida maqolada kiberxavfsizlik va ma'lumotlar himoyalash sohasidagi muhim mavzularni tushunish uchun quyidagi kalit so'zlar foydalanish mumkin: Kiberxavfsizlik, ma'lumotlar himoyalash, internet xavflari, kiberjahon, shaxsiy axborotlar, kiberhamyonlik, veb-xavflar, kiberatakalar, ma'lumotlar to'plashi, kiberhamyonlar, xavf-faktorlar, xavfni baholash.

Raqamli dunyodagi xavflar, internet va boshqa kompyuter tarmoqlarida sodir bo'lgan potentsial xavf yo'nalishlaridir. Bu xavflar odatda kompyuter tarmoqlariga erishish, ma'lumot almashish va uzatish jarayonlarida yuz beradi. Ular turli shakllarda sodir bo'lishi mumkin, masalan, kiber-hujumlar, ma'lumotlar olish, xavfli dasturlar, ma'lumotlar muhofazasi, shaxsiy ma'lumotlar hisobining doimiy ravishda xavfsizligi va boshqalar. Raqamli dunyodagi xavflar bilan bog'liq kengroq ma'lumot quyidagi yo'nalishlarni o'z ichiga oladi:

Kiber-hujumlar: Bu xavflar internet tarmoqlarini va dasturlarni yo'qotish, hizmatni to'xtatish yoki o'zgartirishni maqsad qiladi.

Ma'lumotlar olishi va uzatishi: Kiber-g'alaba tuzumlarida foydalanuvchilarning shaxsiy ma'lumotlarini olish uchun yoritiladi.

Kiber-atakalar: Kompyuter tarmoqlariga zararli kodlar kiritish yoki xavfsizlikni buzishga urinishlar.

Shaxsiy ma'lumotlar himoyalash: Shaxsiy ma'lumotlarni himoyalash sohasidagi xavf-faktorlar, masalan, kimlik uchun identifikatsiya ma'lumotlari, moliyaviy ma'lumotlar va boshqalar.

Kiber-jarayonlar: Xavfsizlik faoliyati, ma'lumot almashish va xavfni qarshilash jarayonlari bo'yicha kiber-atakalar va qabul qiluvchilar orasidagi menejerlik operatsiyalari.



Xavfni baholash va tahlil qilish: Xavfli dasturlar va internet saytlari uchun xavfni baholash va tahlil qilishni o'z ichiga oladi.

Shifrlash va xavfsizlik protokollari: Ma'lumotlarni shifrlash va xavfsizlik protokollari orqali ma'lumotlar almashish va uzatish jarayonlari.

Ma'lumot almashish va tarqatishning xavfsizligi: Ma'lumot almashish va tarqatish jarayonlarida to'g'ri xavfsizlikning ta'minlanishi.

Ma'lumotlarni xavfsiz saqlash: Ma'lumotlarni o'z ichiga oluvchi xavf-faktorlar, shu jumladan, elektron pochta xavflari, shifrlash, foydalanish tanlangan ma'lumotlar va boshqalar.

Internet xavflari: Internet tarmoqlarida tarqatish va internet saytlarining yopilishi yoki hujumlar.

Bu kabi muammolar, shaxsiy ma'lumotlar va korxonalar ma'lumotlarini xavfsizlikni oshirish, kiberxavfsizlik tizimi, xavf-faktorlarini baholash va boshqalar kabi ko'plab turli xavfni tuzatish tizimlari orqali oldin olinishi lozim.

Hozirgi kunda raqamli dunyoda kiberxavfsizlik muammolari va yangiliklari juda muhimdir. Bu muammolar, internet foydalanuvchilarining ma'lumotlarini himoyalash, tarmoq xavfi, dasturlar va tizimlar uchun xavf, shaxsiy ma'lumotlarini himoyalash, kiber-hujumlar va boshqalar kabi xavf-faktorlariga ega. Quyidagi muhim yangiliklar va tushunchalar kiberxavfsizlik sohasida keng ko'miladi:

Zero-Day Vulnerabilities: Zero-day xavfliyatlar, dasturlar yoki tizimlar uchun aniqlik bilan aniqlik bilan topilgan xavfliyatlaridir. Bu xavfliyatlar xavf doimo bilinmaydigan va to'ldirilmaydigan hisoblanadi, shuning uchun ularga tez-tez dastur yoki tizimning loyihasiga oid yangilanishlar orqali javob berish kerak.

Ransomware Attacks: Ransomware hujumlari, ma'lumotlarni shifrlash va ular uchun foydalanuvchidan keyingi harajatlar olish uchun foydalaniladigan zararli dasturlar hisoblanadi. Ular shaxsiy ma'lumotlarni yoki korxonalar ma'lumotlarini egallay oladi va ularni bo'shatish uchun kiber-jalb qilish mumkin.

Phishing Attacks: Fishing hujumlari, odamlarni shaxsiy ma'lumotlarini bermaslikka qo'zg'atish maqsadida elektron pochta, internet saytlari yoki ijtimoiy tarmoqlar orqali yuzaga keladigan qo'lda jarayonlardir. Ular odamlarni shaxsiy ma'lumotlarini, hisob raqamlarini va boshqa ma'lumotlarni olish uchun qo'llaniladi.

Internet of Things (IoT) Security: IoT qurilmalari, ko'plab texnologiyalar, masalan, uy qurilmalari, maishiy qurilmalar va boshqalar bilan bog'liq bo'lgan cihazlar, internetga ulanadigan cihazlar uchun yangi xavf-faktorlar yaratish mumkin. Ular xavfsizlik so'rovnomalari va ma'lumot almashish jarayonlarini kuchaytirish uchun katta imkoniyatlar yaratadi.



Artificial Intelligence (AI) in Cybersecurity: Sun'iy matn o'qish (NLP), ma'lumotlar analizi, model yaratish va boshqalar kabi sun'iy matn texnologiyalari kiber-xavfsizlik sohasida katta rol o'ynaydi. AI va ma'lumotlar analizi yordamida kiberxavfsizlik echimlari aniqlanishi va ta'minlashi mumkin.

Regulatory Compliance: Qonunchilik va tartibga solish sohasida yangiliklar, masalan, GDPR (Umumiy Ma'lumotlar Muhofazasi Tartiboti), kiber-xavfsizlikning yuridik tomonini takomillashtirish, ma'lumotlar muhofazasi bo'yicha yon bera oladigan kuchayishlar.

Cloud Security: Bulut xavfsizligi, bulut xizmatlariga xavfsizlikni ta'minlashni talab qiladi. Bu yo'nalishdagi yangiliklar, bulut xavfsizligi echimlari, shifrlash, identifikatsiya va qo'llanish ma'lumotlarini himoya qilishning yangi yechimlari va protokollari bilan bog'liq.

Blockchain Security: Blokchain xavfsizligi, blokchain tizimlarida ma'lumotlar uchun xavfsizlikni ta'minlashga qaratilgan usullar va texnologiyalarni o'z ichiga oladi. Yangi blokchain xavfsizlik echimlari, blokchain tizimlarini xavfsiz va ishonchli qilishga yordam beradi.

Bu kabi muhim yangiliklar, kiberxavfsizlik sohasidagi muammolarni yechish va ma'lumotlarni himoya qilishda ustunlikli yechimlar va texnologiyalarni izlashda keng foydalaniladi. Raqamli iqtisodiyotning quyidagi afzalliklari ajratiladi [6]:

mehnat unumdorligini 40 % gacha oshirishi taxmin qilinadi;

raqamli iqtisodiyot juda katta miqdordagi mashina o'qishi mumkin bo'lgan ma'lumotlarni (raqamli ma'lumotlar) to'plash, foydalanish va tahlil qilish qobiliyatiga ega;

onlayn platformalar orqali sotiladigan yangi ish shakllarining yuzaga kelishi;

raqamli transformatsiya maxsus xizmatlar uchun savdo infrastrukturasi o'zgarishi;

sanoat mahsulotlari eksporti endilikda AKT mahsulotlari va xizmatlariga bog'liq bo'lib qolmoqda;

raqamli iqtisodiyot juda qisqa vaqt ichida ulkan boyliklarni keltirib chiqardi, ammo bu boylik oz sonli shaxs, kompaniya va mamlakatlar atrofida to'plangan. Amaldagi siyosat va qoidalar asosida ushbu traektoriya davom etishi mumkin, lekin bu tengsizlikning kuchayishiga olib keladi. Shu bilan birga ushbu iqtisodiyotning ayrim ziddiyatli tomonlari ham mavjud. Ular quyidagilar:

- yangi texnologiyalar, ayniqsa sun'iy intellekt, muqarrar ravishda mehnat bozorida katta o'zgarishlarga olib keladi, jumladan, ba'zi tarmoqlarda ish



o‘rinlarining yo‘qolib ketishi va boshqalarida keng miqyosda imkoniyatlar yaratilishiga olib keladi;

raqamli iqtisodiyot bir qator yangi va turli xil ko‘nikmalar, ijtimoiy himoya siyosatining yangi avlodi, ish va bo‘sh vaqt o‘rtasidagi yangi munosabatlarni talab qiladi; “Iqtisodiyot va innovatsion texnologiyalar” ilmiy elektron jurnali. № 1, yanvar-fevral, 2021 yil 1/2021 (№ 00051) <http://iqtisodiyot.tsue.uz> 311

raqamli iqtisodiyot, shuningdek, kiberxavfsizlik buzilishlaridan tortib noqonuniy iqtisodiy faoliyatga ko‘maklashish va shaxsiy hayotning maxfiy tushunchalariga qadar yangi xavflarni keltirib chiqaradi. Raqamli iqtisodiyot deyarli hamma narsaga oid juda katta miqdordagi mashina o‘qishi mumkin bo‘lgan ma’lumotlarni (raqamli ma’lumotlar) to‘plash, foydalanish va tahlil qilish qobiliyatiga asoslangan holda katta tezlikda rivojlanishda davom etmoqda [7]. Masalan, Global Internet Protokol (IP) trafigi, ma’lumotlar oqimi uchun proksi 1992-yilda kuniga 100 gigabaytdan (GB) 2017- yilda sekundiga 45000 Gb dan oshdi va dunyo faqat ma’lumotlarga asoslangan iqtisodiyotning dastlabki kunlaridadir. Shu yo‘sinda 2022-yilga kelib global IPtrafik sekundiga 150,700 Gbaytga yetkazilishi prognoz qilinmoqda.

Xulosa

Raqamli dunyodagi xavflar kiberxavfsizlik sohasida ko‘plab muammolar va yangiliklarni o‘z ichiga oladi. Bu muammolar, internet foydalanuvchilarining ma’lumotlarini himoyalash, tarmoq xavfi, dasturlar va tizimlar uchun xavf, shaxsiy ma’lumotlarini himoyalash, kiber-hujumlar va boshqalar kabi xavf-faktorlariga ega. Quyidagi kalit so‘zlar kiberxavfsizlik va ma’lumotlar himoyalash sohasidagi muhim mavzularni tushunish uchun yordam berishi mumkin:

Foydalanilgan adabiyotlar:

1. https://en.wikipedia.org/wiki/Digital_economy
2. <http://xs.uz/uzkr/post/davlatimiz-rahbari-2030-jilgacha-raqamli-ozbekiston2030-dasturini-amalga-oshirishni-taklif-etdi>
3. Gulyamov, S.S. va b. (2019). Raqamli iqtisodiyotda blokcheyn texnologiyalari. - T.: Iqtisod-Moliya. 396 b. 4. Ayupov, R.X., Baltabaeva, G.R. (2018). Raqamli valyutalar bozori: innovatsiyalar va rivojlanish istiqbollari. –T: Fan va texnologiya. 172 b.
5. <https://www.texnoman.uz/post/raqamli-iqtisodiyot-nima.html>



6. https://www.hse.ru/data/2019/04/12/1178004671/2%20%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D1%8D%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%B0.pdf
7. United Nations Conference on Trade and Development (UNCTAD). Digital economy report 2019.
8. <file:///C:/Users/user/Downloads/global-top-100-companies-2019.pdf>
9. Digital 2019: global digital overview. Value creation and capture: implications for developing countries. UNCTAD, 2020.
10. World Trade Statistical Review 2019 - World Trade Organization.
11. Kurpayanidi, K., Ilyosov, A. (2020) Problems of the use of digital technologies in industry in the context of increasing the export potential of the country// ISJI Theoretical & Applied Science. p. 113-117.
12. Abdullayev, A. M., & Kurpayanidi, K. I. (2020) Analysis of industrial enterprise management systems: essence, methodology and problems. Journal of Critical Reviews, 7 (14), 1254-1260. <https://dx.doi.org/10.17605/OSF.IO/E6JFS>