



**O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
OLTIARIQ SANOAT VA TEXNOLOGIYALAR TEXNIKUMI**



RAQAMLI ASRDAGI YANGI JUMBOQ

Mavzusidagi ilmiy-maqola.

Farg‘ona - 2025

**RAQAMLI ASRDAGI YANGI JUMBOQ**

Sattorov Abdujabbor Abdunabi o'g'li

Oltiariq sanoat va texnologiyalar texnikumi (Farg'ona viloyati, Oltiariq tumani)

Annotatsiya: Ushbu maqolada raqamli transformatsiya jarayonida yuzaga kelayotgan murakkabliklar — yangi davrning "jumboqlari" ilmiy-nazariy tahlil qilinadi. Jumladan, sun'iy intellektning rivojlanishi, katta hajmdagi ma'lumotlar (Big Data) oqimi, raqamli shaxsiylik, kiberxavfsizlik va inson omilining texnologiyalar bilan o'zaro ta'siri masalalari o'rganiladi. Maqolada insoniyat oldida turgan asosiy savollar — raqamli texnologiyalar nazoratini saqlab qolish, axloqiy chegaralarni belgilash va barqaror raqamli muhitni shakllantirish yo'nalishlarida ilmiy xulosalar keltiriladi.

Kalit so'zlar: Raqamli transformatsiya, sun'iy intellekt, ma'lumotlar xavfsizligi, kiberxavf, algoritmik boshqaruv, raqamli axloq, inson-texnika o'zaro ta'siri.

Raqamli asr dunyoning aloqa va biznes yuritish usulini inqilob qildi. Bu odamlarning o'zaro munosabatini tubdan o'zgartirdi. Biroq, bu yutuqlar bilan birga kiberjinoyat xavfi ortib bormoqda va hukumatlar va jamiyat uchun yangi muammo: kiberxavfsizlik. Dasturiy ta'minot va xavfsizlik choralaridagi kuchli yutuqlarga qaramay, kiberxavfsizlik raqamli tarmoqlar, tizimlar va ma'lumotlarning himoyasini oshirish uchun jamoaviy javob talab qiladigan rivojlanayotgan va dinamik soha bo'lib qolmoqda.

Raqamli tarmoqlar uchun kiberhujumlar xavfi jamiyatning o'zaro bog'liqligi va raqamli texnologiyalarga tayanishi tufayli ortib borayotgan muammodir. So'nggi o'n yillikda kiberjinoyatlar sezilarli darajada oshdi, chunki zararli aktyorlar nozik tarmoqlar va ma'lumotlarga kirishga harakat qilmoqda. Ma'lumotlar tobora ko'proq kuzatilayotgan va saqlanadigan muhitda kiberjinoyatchilar juda murakkablashdi va xavfsizlik choralarini buzish uchun turli usullardan foydalanishdi.



Kiberjinoyatchilar ma'lumotlarni o'g'irlash, kompyuterlarni o'g'irlash, tarmoqlarni o'g'irlash va hatto moliyaviy va maxfiy ma'lumotlarga kirish uchun fishing elektron pochta xabarlarini va zararli dasturlar kabi turli xil vositalardan foydalanadilar.

Kiberjinoyatlarning eksponentsial o'sishi butun dunyo bo'ylab hukumatlar va jamiyat uchun yangi muammo tug'dirdi. Ushbu muammoga qarshi turish uchun hukumatlar fuqarolar va korxonalarni kiberhujumlardan himoya qilish uchun kiberxavfsizlik qonunlari va qoidalarini qabul qilishlari kerak. Ushbu qonunlar tez rivojlanayotgan kiberxavfsizlik landshaftini hisobga olishi kerak, bu yerda jinoyatchilar an'anaviy xavfsizlik choralarini chetlab o'tish uchun murakkab vositalar va usullardan foydalanadilar. Bundan tashqari, kiberxavfsizlik bo'yicha global yechimlarni ishlab chiqish zarur. Ko'pgina hukumatlar allaqachon kiberjinoyatchilik bo'yicha Budapesht konventsiyasi kabi xalqaro tashabbuslarni taklif qilib, buni amalga oshirish uchun choralar ko'rmoqda.

Hukumat tashabbuslaridan tashqari, xususi kompaniyalarning raqamli tarmoqlar xavfsizligini ta'minlash harakatlariga qo'shilishlariga katta ehtiyoj bor. Bunga ko'p faktorli shifrlash, xavfsiz serverlar va xavfsizlik devorlari kabi qat'iy xavfsizlik choralarini qo'llash, shuningdek, kiber tahdidlarni aniqlash va oldini olish mumkin bo'lgan yangi va innovatsion texnologiyalarga sarmoya kiritish kiradi. Bundan tashqari, kompaniyalar o'z xodimlarining so'nggi xavfsizlik tendentsiyalari va eng yaxshi amaliyotlardan xabardor bo'lishini ta'minlashi kerak.

Nihoyat, butun jamiyat kiberxavfsizlik uchun mas'uliyatni o'z zimmlariga olishlari kerak. Bunga to'g'ri parollardan foydalanish, fishing elektron pochta

xabarlaridan ehtiyot bo'lish, shubhali havolalarni bosmaslik va tegishli xavfsizlik dasturlari va xavfsizlik devorlarini o'rnatish kiradi. Hukumatlar fuqarolarni kiberxavfsizlik bo'yicha o'qitish, xususan, bolalar kabi aholining zaif qatlamlarini himoya qilish uchun choralar ko'rishlari kerak.

FDU huzuridagi Oltiariq Sanoat texnikumi "Mutaxassislik" fanlar kafedra mudiri, A.K.T fani o'qituvchisi Shohsanam Musadjonova Vahobjonovna

Kiberxavfsizlik zamonaviy raqamli dunyoda biznes va shaxslar uchun asosiy muammo hisoblanadi. Kibertahdidlar identifikatorni o'g'irlash va zararli



dasturlardan tortib fishing firibgarliklari va hatto kompyuterlar va tarmoqlarni masofadan boshqarishi mumkin bo'lgan zararli dasturlarga qadar turli shakllarda bo'ladi. Bunday tahdidlardan himoyalaniş uchun korxonalar va shaxslarning kiberxavfsizlik amaliyotlarida faol bo'lishlari muhim ahamiyatga ega.

Korxonalar kompaniya ma'lumotlarini, obro'sini va moliyaviy aktivlarini himoya qilish uchun keng qamrovli xavfsizlik strategiyasini yaratishi kerak. Bu xavfsizlik devorlari, antivirus va josuslarga qarshi dasturlardan himoya qilish va xavfsiz tarmoq dizayni kabi kuchli xavfsizlik choralariga ega bo'lishni anglatadi. Bundan tashqari, korxonalar xodimlarning kuchli parollar va ikki faktorli autentifikatsiyadan foydalanishini ta'minlashi, shuningdek, o'z tizimlari va ma'lumotlarini himoya qilish uchun dasturiy ta'minotni muntazam yangilash va zaifliklarni tuzatish kabi boshqa choralarni ko'rishi kerak.

Hech bo'lmaganda, korxonalar o'zlari foydalanayotgan har qanday tizimda muntazam xavfsizlik tekshiruvlarini o'tkazishlari va ularning tuzatilishi va himoyalanganligiga ishonch hosil qilishlari kerak. Bundan tashqari, ular jamoa a'zolariga xavfsizlikning eng yaxshi amaliyotlarini o'rgatish uchun kerak bo'lganda xodimlarni o'qitishga sarmoya kiritishlari kerak. Masalan, xodimlar zararli dasturlar, fishing firibgarliklari va ma'lumotlar buzilishidan kelib chiqadigan xavf-xatarlar va ulardan himoyalaniş choralari haqida bilishlari kerak.

Shaxslar uchun kiberxavfsizlikning asoslari biznes bilan bir xil. Bu kuchli parollar va ikki faktorli autentifikatsiyaga ega bo'lish, xavfsiz tarmoqlardan foydalanish va zararli dasturlar, fishing firibgarliklari va ma'lumotlar buzilishi bilan tanishishni anglatadi.

Bundan tashqari, shaxslar ijtimoiy tarmoq profillari kabi ochiq veb-saytlardan shaxsiy ma'lumotlarni o'chirish yoki elektron pochta hisoblari va bank hisoblari kabi xizmatlar uchun ikki faktorli autentifikatsiyani o'rnatish kabi qadamlarni qo'yish orqali o'zlarining onlayn maxfiyligini himoya qilishga yordam berishi mumkin. Bundan tashqari, shaxslar o'zlarining shaxsiy kiberxavfsizlik amaliyotlaridan xabardor bo'lishlari kerak, masalan, kompyuterlari va mobil



qurilmalarini yangilab turish va endi ishlatilmasligi mumkin bo'lgan eski hisoblarni o'chirish.

Umuman olganda, zamonaviy raqamli dunyoda biznes va shaxslar uchun kiberxavfsizlik muhim ahamiyatga ega. Shaxslar va kompaniyalar raqamli muhitda yuzaga keladigan tahdidlarni, ulardan himoyalaniish choralarini va xavfsizlik amaliyotlarida faol bo'lish muhimligini tushunishlari juda muhimdir. Bunga keng qamrovli xavfsizlik rejasiga ega bo'lish, xodimlarni o'qitishga sarmoya kiritish va tizimlarni zaifliklarni muntazam ravishda tekshirish, shuningdek, shaxsiy onlayn ma'lumotlarni o'chirish, ikki faktorli autentifikatsiyadan foydalanish va kompyuterlar va mobil qurilmalarni muntazam yangilash kabi shaxsiy kiberxavfsizlik bosqichlarini bajarish kiradi.

Raqamli asr kiberxavfsizlik haqida gap ketganda yangi jumboqni yaratdi. Jamiyat o'zlarini kibertahdidlardan himoya qilishlari uchun hukumatlar va biznes kuchli kiberxavfsizlik qonunlari va texnologiyalarini amalga oshirishda hamkorlik qilishi kerak. Shu bilan birga,

fuqarolar kiberxavfsizlikning ahamiyati haqida ma'lumotga ega bo'lishi va o'z xavfsizligini saqlash uchun mas'uliyatni o'z zimmasiga olishi kerak. Faqatgina ushbu harakatlarni amalga oshirish orqali jamiyat o'z tarmoqlari, ma'lumotlari va fuqarolarini raqamli asrning zararli aktyorlaridan himoya qilishi mumkin

XXI asr — bu raqamli texnologiyalar, sun'iy intellekt va global tarmoqlar davridir. Insoniyat oldida turli sohalarda ulkan imkoniyatlar paydo bo'lgan bo'lsa-da, shu bilan birga yangi tahdidlar va jumboqlar ham paydo bo'ldi. Ushbu maqola aynan raqamli asrning mazkur murakkab jihatlarini ilmiy yondashuv asosida tahlil qiladi.

Bugungi kunda sun'iy intellekt (SI) nafaqat ishlab chiqarish va xizmat ko'rsatish sohalariga, balki tibbiyot, huquq, ta'lim kabi ijtimoiy tizimlarga ham chuqur kirib bormoqda. Biroq, SI'ning mustaqil qaror qabul qilish darajasiga chiqishi jamiyat uchun axloqiy, huquqiy va falsafiy savollarni keltirib chiqarmoqda.

“Big Data” va algoritmlarning kundalik hayotga chuqur kirib borishi insoniyatni raqamli boshqaruv ostiga qo'yimoqda. Reklama, siyosiy tanlovlar,



sogʻliqni saqlash va hatto ijtimoiy qarorlar algoritmlar tomonidan boshqarilmoqda. Bu esa shaxsiy hayot daxlsizligiga va ongli tanlov huquqiga tahdid soladi.

Raqamli dunyoda qadriyatlar oʻzgarib bormoqda: axborotni yashirish oʻrniga uni doimiy almashish, shaxsiy hayotni ochiqlik bilan almashtirish kabilar yangi “normal” boʻlib bormoqda. Shuning uchun, raqamli axloq va etik meʼyorlarni belgilash zamonaviy ilmiy muammolardan biridir.

Kiberhujumlar nafaqat moliyaviy yoʻqotishlarga, balki siyosiy va milliy xavfsizlikka ham tahdid solmoqda. Davlatlar, korporatsiyalar va jismoniy shaxslar axborot urushi sharoitida yashamoqdalar. Shunday sharoitda raqamli xavfsizlik strategiyalarini ishlab chiqish muhim ahamiyatga ega.

Texnologiyalar nafaqat inson ishini osonlashtirmoqda, balki uni almashtirib bormoqda. Shu sababli, kelajakda inson mehnati va mashina faoliyati oʻrtasidagi chegarani belgilash muhim boʻlib qolmoqda. Bu esa jamiyatda yangi ijtimoiy va iqtisodiy munosabatlar shakllanishini talab qiladi.

Xulosa

Raqamli asr insoniyat uchun ulkan imkoniyatlar eshigini ochgan boʻlsa-da, yangi jumboqlarni ham keltirib chiqardi. Ularni yechish esa nafaqat texnik, balki falsafiy, ijtimoiy va axloqiy yondashuvni ham talab qiladi. Bu maqola orqali zamonaviy ilm-fan va jamiyat ushbu murakkab muammolarga qanday javob topishi mumkinligi koʻrsatib berildi.

FOYDALANILGAN ADABIYOTLAR:

1. Harari, Y. N. (2018). 21 Lessons for the 21st Century. Spiegel & Grau.
2. Floridi, L. (2014). The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press.
3. Tegmark, M. (2017). Life 3.0: Being Human in the Age of Artificial Intelligence. Penguin.
4. Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age. W. W. Norton & Company.
5. Lanier, J. (2010). You Are Not a Gadget: A Manifesto. Knopf.



6. Solove, D. J. (2007). The Digital Person: Technology and Privacy in the Information Age. NYU Press.
7. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi hisobotlari, 2024–2025 yillar.