# KIBERXAVFSIZLIK, SUN'IY INTELLEKT, MA'LUMOTLARNI HIMOYA QILISH

**Sodiqov Muhammadqodir Abdumutalib o'g'li**
*Toshkent davlat yuridik universiteti Xalqaro huquq va qiyosiy huquqshunoslik fakultiteti 3-kurs talabasi*

*Kiberxavfsizlik - bu aql-idrokka erishish uchun tenglik mavjud bo’lgan yangi maydon.*

***Stefan Nappo***

**Annotatsiya:** *Mazkur maqolada kiberxavsizlikning elementlari va uning kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma’lumotlarni zararli hujumlardan himoya qilish usullari to’g’risida ma’lumotlar berilgan. Ushbu maqola xavfsizlik prinsiplari, muhim xavfsizlik nazorati va kiberxavfsizlikning eng yaxshi amaliyotlarini o’z ichiga olgan xavfsizlik asoslarini tushuntiradi. Xavfsizlik dasturlari potensial zararli dasturlarni foydalanuvchining xatti-harakatlarini tahlil qilish va yangi infeksiyalarni qanday yaxshiroq aniqlashni o’rganish uchun yo’l yo’riqlar ko’rsatilgan.*

**Kalit so’zlar:** *Elektron, xavfsizlik, protokollar, virus, mobil, axborot, kiberxavfsizlik, pochta, texnologiya, biznes, kiberjinoyat.*

Zamonaviy dunyoda yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat kundan kun axborotkommunikatsiya 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 dolzarb mavzuga aylanmoqda. Har bir tashkilot uchun kiberxavfsizlikni ta’minlash maqsadida mazkur soha bilan shug’ullanuvchi xodimlar jalb qilinmoqda hamda xodimlarni kiberxavfsizlikka oid bilimlar bilan doimiy tanishtirib borish uchun qator seminar treyning mashg’ulotlari tashkil etilmoqda. Oliy ta’lim muassasalarida ham kiberxavfsizlikni fan sifatida o’tilishi buning yaqqol misolidir.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo’lib, unga berilgan turlicha ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta’rif berilgan: ***kiberxavfsizlik –*** hisoblashlarga asoslangan bilim sohasi bo’lib, buzg’unchilar mavjud bo’lgan sharoitda amallarni to’g’ri bajarilishini kafolatlash uchun o’zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o’z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo’lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o’z ichiga oladi. Tarmoqlar sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda

maxfiy axborotni boshqarish, almashtirish yoki yo’q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg'unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda. [117]

Kiberxavfsizlik bilim sohasining zaruriyati ilk bor meynfreym kompyuterlar ishlab chiqarilganidan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalar va ularning vazifalari himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta'minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga sabab bo‘lgan.

Bugunga kelib, hayotning har bir jabhasi raqamlashmoqda, tug‘ilishdan tortib vafot etishgacha raqamli boshqaruv asosida hayot kechirmoqdamiz. Aholi demografiyasining o‘sishi hamda pasayishi, jinoyatchilik miqdorining harakatlanishi, valyuta qimmatliklarining harakatlari, onlayn savdo, shuningdek, masofaviy ta’lim, masofaviy boshqaruv kabilar shular jumlasidandir. Mazkur vositalar asosidagi hayot tarzi bizga beqiyos qulayliklar bermoqda, biroq bugun shaxsning qadrsizlanishi, shaxsiy ma’lumotlarning dunyo bo‘ylab tarqalib ketishi, firibgarlik qurboniga aylanishi har qachongidan osonlashmoqda. Buning tub sababi ham aynan raqamli dunyodir. 1995-yilda nashr etilgan M. Ethan Katshning “Raqamli dunyoda huquq” nomli kitobining kirish qismida William Gates tomonidan bir jumla aytiladi: “Kelajakda barcha narsa raqamli bo‘ladi” (Katsh, 1995). Oradan 27 yil muddat o‘tdi hamki, mazkur fikrning tasdig‘ini ko‘rmoqdamiz. Yuqorida aytilganidek, har bir soha va hayotning har bir jabhasi raqamlashmoqda. www.datareportal.com sayti tomonidan taqdim etilgan ma’lumotlarga qaraganda, bugungi kunda dunyo bo‘ylab jami 5 milliard kishi internetdan foydalanmoqda – bu dunyo aholisining 63 foiziga teng demakdir. Xuddi shunday ma’lumot www.statista.com sayti tomonidan ham taqdim etilgan. Joseph Johnsonning tahlillariga ko‘ra, “2022-yil aprel oyida dunyo aholisining umumiy sonidan 4,65 milliard kishi ijtimoiy tarmoq foydalanuvchilari sanalishadi”. Internet foydalanuvchilari ham o‘sishda davom etmoqda, so‘nggi ma’lumotlar shuni ko‘rsatadiki, dunyodagi internet bilan bog‘langan aholi soni 2022-yil aprel oyigacha bo‘lgan 200 oy ichida deyarli 12 millionga o‘sdi. Bu esa aholining kundan kunga jahon intenet tarmog‘i bilan bog‘lanib borayotganligini anglatadi. Bu kabi statistik ma’lumotlar ijobiyligi sababli ham rivojlanish sari turtki bo‘la oladi. Biroq masalaning dolzarbligi aynan yuqoridagi ijobiy jihatlarda emasligini unutmaslik kerak.

Kiberhujumlar, kiberjinoyat, xakerliklarning zararli ta’siri raqamli dunyoda shaxsiy hayot xavfsizligini, shaxsiy ma’lumotlar daxlsizligi haqidagi qarashlarni tubdan o‘zgartirib yubordi. Hozirda biz tomonimizdan “yangi sanoat inqilobi” deb nomlanayotgan jarayon yangi jamiyatni, yangi muhitni taqdim etganligi bilan bir tomondan ijobiy ahamiyat kasb etsa, ikkinchi tomondan

[117] S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma. – T.: «Aloqachi», 2020, 221 bet.

real xavfni ham keltirib chiqarmoqda. Misli ko‘rilmagan rivojlanishga qaramay, internet bizga qo‘rquvning yangicha ko‘rinishlarini, xavfning yangicha shakllarini olib keldi. *Majir Yar va Kevin F.Steinmetzlarning* fikriga ko‘ra, “Kibermakon, kompyuterlashtirilgan o‘zaro aloqalar va almashinuvlar sohasi jinoyatchilar va deviant faoliyat uchun juda ko‘p yangi imkoniyatlarni taqdim etadi (Yar, Majid, and Kevin F. Steinmetz, 2019). [118]Shuningdek, aksariyat manbalarda “kiberjinoyat” tushunchasi “kiberhujumlar”, “kompyuterda sodir etilgan jinoyatlar” yoki “kompyuter jinoyatlari” kabi nomlar bilan atalishi, Gudmen va Benner tomonidan XXI asrning boshidayoq ilgari surilgan edi (Goodman, Brenner, 2002). [119]Biroq mazkur tushunchalar bir xil ma’no-mazmun anglatmasligini aytib o‘tish joiz. Misol uchun, “kiberjinoyatchilik” atamasi kompyuter bilan bog‘liq jinoyatlarga qaraganda torroq tushunchani ifodalashi bilan ajralib turadi. Sababi, u faqatgina kompyuter tarmog‘ini o‘z ichiga olib, u bilan sodir etiladigan jinoiy qilmishlarni qamrab oladi. Kompyuterlar bilan bog‘liq jinoyatlar esa hatto tarmoq bilan hech qanday aloqasi bo‘lmagan, faqat shaxsiy kompyuter tizimlariga ta’sir qiladigan jinoyatlarni ham qamrab oladi (Gercke, 2012). [120]Kiberjinoyatchilik transmilliy jinoyatchilikning rivojlanayotgan shaklidir. Birlashgan Millatlar Tashkilotining Jinoyatchilikning oldini olish va huquqbuzarlarni profilaktika qilish bo‘yicha 10-Kongressida tegishli seminar doirasida raqamli texnologiyalar orqali sodir etiladigan jinoyatlar uchun ikkita asosiy ta’rif ishlab chiqilgan edi. Tor ma’noda, kiberjinoyatchilik (kompyuter jinoyati) bu kompyuter tizimlari xavfsizligining buzib kirilishi va aynan kompyuterlar tomonidan ma’lumotlarning g‘arazli maqsadlarda qayta ishlanib foydalanilishi tushuniladi. Kiberjinoyatchilik, keng ma’noda esa, (kompyuter bilan bog‘liq jinoyatlar) kompyuter tizimi yoki tarmog‘i orqali yoki aynan kompyuterga va raqamli tizimlarga nisbatan sodir etilgan har qanday noqonuniy xatti-harakatlarni, shu jumladan, kompyuter tizimi yoki tarmog‘i orqali noqonuniy egalik qilish va ma’lumotlarni taqdim etish yoki tarqatish kabi jinoyatlarni qamrab oladi (Patri, 2009).[121] Kibermakonning chegarasiz hududida sodir bo‘ladigan jinoyatning murakkab tabiati uyushgan jinoyatchilik guruhlarining tobora ko‘payib borishi bilan murakkablashadi hamda mazkur omillarning ta’sirida jinoyatchilikning yangicha ko‘rinishi tobora xavflilik kasb etmoqda.

***Kiberxafszlik nima, uni qanday qilib yaratish va ta’minlash mumkin?*** Kiberxavfsizlik tushunchasi bu raqamli muhitning turli xil tashqi xavflardan himoya, muhofaza etilishini anglatadi. Yanada aniqroq qilib aytganda, kiberxavfsizlik – bu kiber(raqamli) muhitni va tashkilot va foydalanuvchi

[118] Yar, Majid, and Kevin F. Steinmetz. (2019). Cybercrime and society. SAGE.
[119] Goodman, Brenner. (2002). The emerging consensus on criminal conduct in cybercrime. International journal of law and information technology, 144.
[120] Gercke D.M. (2012). Understanding cybercrime: phenomena, challenges and legal response. Geneva: International Telecommunication Union (ITU).
[121] Patri A.K. (2009). Cyber Law. Lucknow.

aktivlarini himoya qilish uchun ishlatilishi mumkin bo‘lgan vositalar, siyosat, xavfsizlik tushunchalari, xavfsizlik kafolatlari, ko‘rsatmalar, xatarlarni boshqarish yondashuvlari, harakatlar, treninglar, eng yaxshi amaliyotlar, ishonch va texnologiyalar to‘plami. Unga tashkilot va foydalanuvchi aktivlariga ulangan hisoblash moslamalari, xodimlar, infratuzilma, dasturlar, xizmatlar, telekommunikatsiya tizimlari va kibermuhitda uzatiladigan va/yoki saqlanadigan ma’lumotlarning yig‘indisi kiradi. Kiberxavfsizlik tashkilot va foydalanuvchi aktivlarining xavfsizlik xususiyatlariga erishish va texnik xizmat ko‘rsatishni ta’minlashga intiladi.

Kiberjinoyatchilar va ularning qurbonlari turli mintaqalarda joylashgan bo‘lishi mumkin va uning ta’siri butun dunyo bo‘ylab jamiyatlar orqali o‘tib, shoshilinch, dinamik va kompleks javob berish zarurligini taqozo etmoqda. Hozirda barcha davlatlar tomonidan kiberxavfsizlikni rivojlantirishga qaratilgan chora-tadbirlar olib borilmoqda. Bugungi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar soni va turlarining kattaligi va buzg’unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.

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 himoyalanish 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.[122]

[122] Ganiyev S.K. “Kiberxavfsizlik asoslari”. O’quv qo’llanma.

Darhaqiqat, O’zbekiston rivojlanayotgan mamlakatlar qatoriga kirgan.Shu bois mamlakatimiz iqtisodiyoti va boshqa ko’lab sohalar raqamlashtirilmoqda. Bank sohasidan tortib tibbiyot sohasigacha, harbiy sohadan tortib qishloq xo’jaligigacha raqamlashtirish jarayoni olib borilmoqda. Bu albatta milliy axborot tizimi uchun xavfsizlik masalalarini tug’diradi. Ayniqsa, siyosat va harbiy sohalar bo’yicha ma’lumotlar aslo oshkor bo’lmasligi lozim. Biroq, yurtimizda kiberxavfsizlikka yetarlicha e’tibor berilmaganligi sababli O’zbekistonning rasmiy internet tarmog’iga nisbatan kiberattakalar va noqonuni yfaoliyatlar amalga oshirilmoqda.

“Kiberxavfsizlik markazi” DUK(Davlat unitar korxonasi) tahlillariga ko’ra, 2020yilda internetning milliy segmenti(.uz) veb-saytlarida 27 milliondan ortiq zararli va shubhali tarmoq hujumlari kuzatilgan. Bularning asosiy qismi botnet tizimlariga tegishli bo’lib, ular 19 491 783 tani tashkil qiladi. Keyin esa, himoyasiz http protokolida 4 631 375 ta va boshqa insidentlarda ham nisbatan kichikroq kiberhujumlar ro’yxatga olingan.

Xususan, bugungi kunga qadar kiberxavfsizlik bo‘yicha mutaxassislarni tayyorlovchi davlat oliy ta’lim muassasasi, maktab, litsey va kollejlarning mavjud emasligi kadrlarning sifatiga salbiy ta’sir ko‘rsatmoqda. Kiberxavfsizlikni tartibga soluvchi vakolatli organ tomonidan kadrlarni tayyorlash borasida yagona metodikaning ishlab chiqilmaganligi, yagona malakaviy talablarning bugungi kunga qadar mavjud emasligi, kadrlarning tizimli asosda tayyorlanmasligiga sabab bo‘lmoqda, maktabgacha ta’lim, maktab, litsey, kollej, oliy ta’lim muassasasi, oliy ta’limdan keyingi davrning izchillik asosda olib borilmayotganligi sohada kadrlarning yetishmovchiligiga sabab bo‘lmoqda. Shu sababdan ham bugungi kunga qadar ichki ishlar organlarining kiberxavfsizlik bo‘linmalariga nomzodlar jismoniy tayyorgarliksiz qabul qilinish mexanizmi yaratildi, kadrlarning yetishmovchiligi tufayli bugungi kunga qadar har tomonlama salohiyatli kadrlarga bo‘lgan talab yurtimizda judda katta. Xususan, “Kiberxavfsizlik sohasidagi inson resurslarini tadqiq qilish–2019” hisobotiga asosan, 2019-yilda dunyoda kiberxavfsizlik bo‘yicha 4 mlndan ortiq tashkil etgan bo‘lsa, J. K. Marshall nomidagi Yevropa xavfsizlikni o‘rganish markazi direktori Kit V. Deytonning fikricha, ushbu raqamlar hozirgi kunda 1,8 mlndan oshadi.

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.Shu bois, 2020-yilda milliy “UZ” domen hududining zamonaviy axborot tizimlari va resurslari xavfsizligini oshirish bo’yicha chora-tadbirlarni amalga oshirish davomida 297 ta tadqiqot va ekspertiza o’tkazildi.Amalga oshirilgan ishlar natijasida 695 ta zaifliklar aniqlanib zaifliklar haqida axborot tizim va resurs egalari darhol xabardor qilindi.Aniqlangan

zaifliklarning asosiy qismi o’ta xavfli (466 ta), o’rta xavfli(205ta) va past xavfli(24 ta) hodisalarga tegishli tartibda choralar ko’rildi.

Kiberxavfsizlik bo’yicha global reytinglarda 2019- yil sarhisobiga ko’ra O’zbekiston Milliy kiberxavfsizlik indeksi (National Cyber Security Index) da 90-o’rinda, Global kiberxavfsizlik indeksi (Global Cybersecurity Index) da 52-o’rinda, AKT rivojlanganlik indeksi (ICT Development Index) da 95-o’rinni egallab kelmoqda. Yuqorida sanab o’tilgan amaliyotlar barchasi milliy xavfsizlikni ta’minlashdab iborat. Chunki mamlakatning iqtisodiy, ijtimoiy, madaniy rivojlanishining statistik ko’rsatkichlarining haqqoniyligi, ishonchliligi va konfedentsialligini ta’minlash bugungi kundagi dolzarb muammolardan biri hisoblanadi.

Fikrimizcha, ushbu muammolarning yagona yechimi ushbu yo‘nalishda ilg‘or xorijiy tajribaga asoslangan, milliy, xalqaro xorijiy tajribani yaxshi biladigan, kiberxavfsizlik sohasini takomillashtirish bo‘yicha yuksak darajada fikrlaydigan kadrlarni tayyorlash yuqori bo‘g‘indan emas, balkir quyidan yuqoriga qarab, maktabgacha ta’lim-maktab-litsey-kollej-oliy ta’lim muassasasi-oliy ta’limdan keyingi davrning izchillik olib boriladigan yagona pedagogik-metodik yondashuvni amalga oshirish, har bir ta’lim davri o‘quvchisining aqliy imkoniyatlariga munosib darslik va o‘quv qo‘llanmalarini tayyorlash, ularni bosqichma-bosqich raqamli ko‘nikmalar tayyorlash orqali kiberxavfsizlik bo‘yicha bilim va salohiyatini yuksaltiradigan yagona mexanizmni ishga tushrish bugungi kunda dolzarb vazifalarimizdan biri bo‘lmog‘i darkor. Bugungi kunda Rossiya-Ukraina, Xitoy-Tayvan va boshqa malakatlar o‘rtasidagi qurolli to‘qnashuvlar faqatgina qurol yordamida emas, balki kiberurushlar orqali ham hal etilayotganligini yodda tutgan holda, ushbu yo‘nalishda kadrlarni tayyorlashning yangi tartib-taomillarini o‘ylab ko‘rmog‘iz va amaliyotga tezroq joriy etishimiz juda muhim.

Shuningdek, bugungi kunda onlayn muvaffaqiyatga erishmoqchi bo'lgan tashkilotlar uchun AI kiberxavfsizlikning eng yaxshi variantidir. Samarali ishlash va o'z tashkilotlarini kiberhujumlardan himoya qilish uchun xavfsizlik bo'yicha mutaxassislar aqlli mashinalar va sun'iy intellekt kabi ilg'or texnologiyalardan muhim yordamga muhtoj.

Mashinani o'rganish va AI algoritmlari ushbu tendensiyada hal qiluvchi ahamiyatga ega. Ular qaror qabul qilish jarayonlarini tez avtomatlashtirish va to'liq bo'lmagan yoki o'zgartirilgan ma'lumotlardan namunalarni aniqlash uchun juda foydali, garchi ular barcha kiberxavfsizlik muammolari uchun bir martalik yechim bo'lmasa ham. Ushbu algoritmlar dastlab haqiqiy ma'lumotlardan, masalan, joriy xavfsizlik xatarlari, noto'g'ri pozitivlar va butun dunyo bo'ylab mutaxassislar tomonidan aniqlangan eng so'nggi xavflarni o'rganish orqali ishlaydi.

AI algoritmlari eskirgan ro'yxatga asoslangan xavfsizlik usullaridan sezilarli ustunlikka ega kuchli naqshlarni aniqlash vositalaridir. Xavotirli naqshlarni ko'rsatadigan paydo bo'lgan tahdidlarni aniqlash orqali AI bu tizimlarni yaxshilaydi va undan ustun turadi. AI tajribasining bunday darajasi katta hajmdagi o'rganishni talab

qiladi va faqat har bir xavf vektori uchun ishonchli ma'lumotlar manbalari bilan mumkin.

Sun'iy intellekt (AI) mutaxassislarga turli xil muammolarni hal qilishda yordam beradi, ularning ba'zilari kiberxavfsizlik bilan bog'liq. Sun'iy intellekt (AI) va mashinani o'rganish (ML) korxonalarga xakerlar bilan kurashishda va o'z tarmoqlari, tizimlari va ma'lumotlari xavfsizligini avtomatlashtirilgan tahdidlarni aniqlash, dasturiy ta'minot bilan ishlaydigan oddiy usullardan ko'ra tahdidlarga tezroq javob berish va hokazolar orqali yordam berishi mumkin. Professionallar AIga asoslangan kiberxavfsizlik yechimlaridan foydalangan holda kiberxavfsizlikdan foydalanish orqali hal qilish qiyin bo'lgan turli muammolarni hal qilishlari mumkin bo'ladi. Turli texnologiyalar o'z-o'zini o'rganadigan kompyuterlarni muntazam ravishda tashkilot tizimlaridan ma'lumotlarni to'plashni, ushbu ma'lumotlarni baholashni va tizim himoyasi va potentsial hujumlar haqida ko'proq ma'lumot olish uchun tegishli signallar bo'ylab naqshlarni izlashni o'rgatadi.

Sun‘iy Intellekt hayotimizga jadallik bilan kirib kelar ekan uning inson hayotiga ta‘sir qilishida muayyan qoidalar majmuiga ehtiyoj seziladi. Bu borada bir qator davlatlar hususan Xitoy, AQSh va Yevropa Ittifoqi umumiy mexanizmlar ishlab chiqishga ulgurdi. Ekspertlarning ta‘kidlashicha bular orasida dunyoga eng keng ta‘sir qilishi kutilayotgan Yevropadagi Sun‘iy Intellektni huquqiy tartibga solish mexanizmlari eng istiqbolli bo‘lishi bilan bir qatorda Yevropa Ittifoqiga kata mas‘uliyat yuklaydi.[123]

Shuningdek, bu sohada qilinajak har qanday ilmiy kashfiyotlar umuminsoniy qadriyatlarni asrab uni yanada mustahkamlash uchun xizmat qilishi maqsadida olib borilishiga va bu orqali insonlarning yashash sharoitlarini yanada yaxshilash orqali umumiy manfaatlarga erishish yo‘lini tutishiga xizmat qilishi lozim. Bu borada O‘zbekistonda ham ushbu sohaning naqadar ahamiyati kech bo‘lsa ham anglab yetilgan holda bir qator boshlang‘ich qadamlarni bosib ulgurdi xususan O‘zbekistonda —Sun‘iy Intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish to‘g‘risida qabul qilingan president qarorida ham ushbu sohada ilg‘or yangiliklarni mamlakatimizda keng qo llash, raqamli ma‘lumotlardan samarali foydalanish imkoniyatini va ularning yuqori sifatini ta‘minlash, ushbu sohada malakali kadrlar tayyorlash uchun qulay shart-sharoitlar yaratish maqsadida amalga oshirilishi lozim bo‘lgan qator amaliy chora-tadbirlar dasturi tasdiqlandi. Ammo bu jarayon faqatgina ilk harakatlar bo‘lib bu jarayonning maksimal tezlikda rivojlanishida kata ma‘lumotlar bazasi (big data) yuqori ahamiyat kasb etadi. Bundan tashqari tartibga soluvchi normalarni to‘g‘ri qo‘llay biladigan kadrlar ham o‘z o‘rnida muhim.

Umumiy xulosa qilib aytganda, bugungi juda ham tez harakatlanayotgan raqamli dunyoda, avvalo, shaxsning, shuningdek, ma’lumotlarning xavfsizligi amalga oshirilayotgan chora-tadbirlarning ko‘lami hamda ta’sir darajasiga har jihatdan bog‘liqdir. Yuqorida qayd etilganidek va tahlil qilinganidek,

[123] https://hashdork.com/uz/artificial-intelligence-in-cybersecurity/

kiberjinoyatchilik jamiyat va davlatning eng xavfli dushmanidan biriga aylanmoqda. Unga qarshi kurashda esa eng samarali tizimlarni joriy etish, amaliyotga kiritish hamda integratsiyani kuchaytirish talab etilmoqda. Yana muhim jihat esa kiberxavfsizlik, raqamli huquq hamda raqamli gigiyenani shakllantirish, kundalik turmushning ajralmas qismiga aylantirish zamon talabi sifatida qayd etilmoqda.

## FOYDALANILGAN ADABIYOTLAR RO`YXATI:

1. Ganiyev S.K. “Kiberxavfsizlik asoslari”. O’quv qo’llanma.
2. Thomas A.Johanson. “Cyber-security, Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”.
3. Niall Adams, Nicholas Heard. “Data Analysis for network cyber-security”.
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
6. https://perconcordiam.com/perCon_V10N4_RUS.pdf.
7. https://lib.itsec.ru/articles2/job/defitsit-kadrov-v-sfere-ib-i-podgotovkamolodyh-spetsialistov.
8. O‘zbekiston Respublikasi Prezidentining 2021-yil, 17 fevraldagi PQ-4996-son qarori
9. Patri A.K. (2009). Cyber Law. Lucknow.
10. Akbarov D.Y.Axborot xavfsizligini ta’minlashningkriptografik usullari va ularning qo’llanilishi. – Toshkent, “O’zbekiston markasi” nashriyot, 2009-432 bet.
11. Rakhimjon, H. (2022). 6 NEW PROGRAMMING LANGUAGES TO LEARN. Academicia Globe: Inderscience Research, 3(04), 126-135.
12. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, U.Xolimtayeva. Kriptografiyaning matematik asoslari. O’quv qo’llanma. T: M.Ulug’bek nomidagi OzMU, 2018-144 bet.
13. Yar, Majid, and Kevin F. Steinmetz. (2019). Cybercrime and society. SAGE.
14. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma. – T.: «Aloqachi», 2020, 221 bet.
15. Goodman, Brenner. (2002). The emerging consensus on criminal conduct in cybercrime. International journal of law and information technology, 144.
16. Gercke D.M. (2012). Understanding cybercrime: phenomena, challenges and legal response. Geneva: International Telecommunication Union (ITU).
17. https://hashdork.com/uz/artificial-intelligence-in-cybersecurity/