Pedagogical Cluster- Journal of Pedagogical Developments
PCJPD: Volume 1, Issue 2, December 2023, online: ISSN 2956-896X
PEDAGOGICAL CLUSTER
JOURNAL OF PEDAGOGICAL DEVELOPMENTS
Website: https://euroasianjournals.org/index.php/pc/index

Raqamli davrda shaxsiy ma’lumotlarni himoya qilish. Kiber tahdidlar va ularni bartaraf etish choralari

To‘xtasinov Alyorbek Ravshanbek o‘g‘li
Muxammad al - Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
(TATU) Nurafshon filiali 2-bosqich talabasi
alyortuxtasinov2@gmail.com

Annotatsiya

Raqamli texnologiyalar jadal rivojlangan davrda shaxsiy ma’lumotlarni himoya qilish eng asosiy muammoga aylandi. Raqamli dunyoning tez suratlarda kengayishi bilan mustahkam kiberxavfsizlik choralarining ahamiyatini haddan tashqari yuqori baholab bo‘lmaydi. Ushbu maqolada kiber tahdidlarning rivojlanayotgan tabiati, shaxsiy ma’lumotlarni himoya qilishda kiberxavfsizlikning ahamiyati va sohaning kelajakdagi istiqbollari o‘rganiladi. Ushbu maqolada hozirgi tendensiyalarni va potensial qiyinchiliklar o‘rganib chiqilib, shaxsiy ma’lumotlarning yaxlitligi va maxfiyligini saqlab qolishda kiberxavfsizlikning zarur roli to‘g‘risida keng qamrovli tushunchalar berishga harakat qilinadi.

Kalit so‘zlar: Kibernetik xavfli holatlar, ma’lumotlar buzilishi, shifrlash, regulyatorlik kadrlar, sun’iy intellekt, maxfiylik huquqlari, kvant hisoblash, xavfli axborot, IoT xavfsizligi.

Raqamli inqilob tengsiz qulaylik va ulanishni keltirib chiqardi, kishilarning o‘zaro aloqasi, ishlashi va kundalik ishlarini olib borishini tubdan qayta shakllantirdi. Elektron tijoratning tarqalishidan tortib, bulutli hisoblashning uzluksiz integratsiyasigacha raqamli soha zamonaviy hayotning ajralmas qismiga aylandi. Biroq, raqamli platformalarga bo‘lgan bu misli ko‘rilmagan tayanish shaxslar va tashkilotlarni ma’lumotlarning buzilishi va shaxsiy o‘g‘irlikdan tortib,

kuchli xakerlik va to‘lov dasturlari hujumlarigacha bo‘lgan minglab kiber tahdidlarga ham duchor qildi. Natijada, mustahkam kiberxavfsizlik choralariga bo‘lgan ehtiyoj ushbu xavflarni yengillashtirish, muhim ma’lumotlarning maxfiyligini himoya qilish uchun jiddiy zarurat sifatida paydo bo‘ldi.

Zamonaviy raqamli olam shiddat bilan to‘xtovsiz rivojlanadigan ko‘p sonli kiber tahdidlar bilan to‘lib-toshgan. Zararli dasturlar va fishing hujumlaridan tortib, ijtimoiy muhandislik va ichki tahdidlargacha, xakerlar raqamli tizimlar ichidagi zaifliklardan foydalanishga intilishdagi harakatlari tinimsiz davom etmoqda. Internet Narsalari (IoT) orqali o‘zaro bog‘langan qurilmalarning tarqalishi hujum qamrovini yanada kengaytirdi, kiber jinoyatchilar uchun tarmoqlarga kirib borish va nozik ma’lumotlarni buzish uchun qo‘shimcha kirish nuqtalarini yaratdi. Bundan tashqari, o‘zaro bog‘liq global iqtisodiyot xalqaro kiber tahdidlarning ko‘payishiga olib keldi, xalqaro hamkorlik va bir-biriga mos kiberxavfsizlik protokollariga bo‘lgan ehtiyojni kuchaytirdi.

Kiber tahdidlar kuchaygan bugungi sharoitda mustahkam kiberxavfsizlik choralarining ahamiyatini kam baholab bo‘lmaydi. Samarali kiberxavfsizlik amaliyotlari nafaqat shaxsiy ma’lumotlarni himoya qiladi, balki iste’molchilarning raqamli platformalarga bo‘lgan ishonchini kuchaytiradi. Shifrlash protokollari, multifaktor autentifikatsiya va mustahkam xavfsizlik devorlarini yaratish orqali tashkilotlar o‘zlarining raqamli infratuzilmasini mustahkamlashlari va ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashlari mumkin. Bundan tashqari, muntazam xavfsizlik auditlari, xodimlarni o‘qitish va hodisalarga javob berish rejalari kabi faol chora-tadbirlar ehtimoliy zaifliklarni oldindan aniqlash va kamaytirishda, shu bilan birga ma’lumotlarning buzilishi va kiber hujumlar xavfini minimallashtirishda juda muhim rol o‘ynaydi.

Kiber tahdidlarning dinamik tabiati kiberxavfsizlik qoidalari va texnologiyalarining doimiy evolyutsiyasini talab qiladi. Kiber hujumlarning kuchayib borayotganligiga javoban tashkilotlar va xavfsizlik ekspertlari paydo bo‘lgan tahdidlarni real vaqt rejimida aniqlash va neytrallashtirish uchun hujumlar tahlili va tahdid razvedkasi kabi ilg‘or texnologiyalardan yanada

ko‘proq foydalanmoqda. Bundan tashqari, xavfsizlikni avtomatlashtirish va tashkillashtirish integratsiyasi tezkor hodisalarga javob berishini osonlashtiradi va raqamli infratuzilmalarning umumiy o‘zgaruvchanligini oshiradi.

Kiberxavfsizlik amaliyotdagi yutuqlarga qaramay, kiber tahdidlardan keng qamrovli himoyani tashkil etilishida bir qator qiyinchiliklar o‘z yechimini kutmoqda. Kiberxavfsizlik bo‘yicha malakali mutaxassislar yetishmovchiligi sezilarli to‘siq bo‘lib xizmat qiladi, chunki tashkilotlar murakkab xavfsizlik muammolarini bartaraf etishga qodir iste’dodni ishga qabul qilish va saqlab qolishga qiynalmoqda. Bundan tashqari, ish joyida xodimlarning o‘z shaxsiy mobil qurilmalari yoki kompyuterlari bilan ishlashga ruxsat berish (“Bring Your Own Device”) siyosatini qabul qilish xavfsiz va boshqariladigan raqamli muhitni saqlashda qo‘shimcha qiyinchiliklarni keltirib chiqaradi. Birgina 2020-yilda xakerlik hujumlari tufayli jahon iqtisodiyoti trillion dollardan ziyod zarar ko‘rgan va ushbu raqamlar yildan-yilga oshib bormoqda.

O‘zbekiston ham rivojlanayotgan mamlakat sifatida o‘z iqtisodiyoti va ko‘plab boshqa sohalarda raqamlashtirish siyosatini amalga oshirmoqda. Harbiy sohadan tortib tibbiyot sohasigacha, bank sohasidan tortib qishloq xo‘jaligi sohasigacha raqamlashtirish ishlari olib borilmoqda. Bu albatta milliy axborot tizimi uchun xavfsizlik muammolarini tug‘diradi. Ayniqsa, siyosat va harbiy sohalar bo‘yicha oshkor etib bo‘lmas ma’lumotlarning maxfiyligi ta’minlanishi lozim. Biroq, yurtimizda kiberxavfsizlikka o‘z vaqtida yetarlicha e’tibor berilmaganligi sababli O‘zbekistonning rasmiy internet tarmog‘iga nisbatan kiber hujumlar va noqonuniy faoliyatlar amalga oshirilmoqda. “Kiberxavfsizlik markazi” DUK(Davlat unitar korxonasi) tahlillariga ko‘ra, 2020-yilda internetning milliy segmenti(.uz) veb-saytlarida 27 milliondan ortiq zararli tarmoq hujumlari kuzatilgan. Ushbu hujumlarning 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.

Bugungi kunga qadar kiberxavfsizlik bo‘yicha mutaxassislarni tayyorlovchi davlat oliy ta’lim muassasasi, maktab, litsey va kollejlarning mavjud emasligi

kadrlarning salmog‘i va sifatiga salbiy ta’sir ko‘rsatmoqda. Kiberxavfsizlikni tartibga soluvchi vakolatli organ tomonidan kadrlarni tayyorlash borasida yagona maqsadli tizimning 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 juda katta. Xususan, “Kiberxavfsizlik sohasidagi inson resurslarini tadqiq qilish–2019” hisobotiga asosan, 2019-yilda dunyoda kiberxavfsizlik bo‘yicha kadrlarga bo‘lgan ehtiyoj 4 milliondan ortiqni tashkil etgan bo‘lsa, J. K. Marshall nomidagi Yevropa xavfsizlikni o‘rganish markazi direktori Kit V. Deytonning fikricha, ushbu raqamlar hozirgi kunda 1,8 milliondan oshadi.

Kiberxavfsizlikka doir me’yorlarning huquqiy jihatdan mustahkamlanishi nihoyatda zarur hisoblanadi. 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 zarurligini ko‘rsatadi. Kiberxavfsizlikka doir milliy strategiyani ishlab chiqish milliy kibermakonda jinoyatchilikka qarshi kurashish sohasidagi faoliyatni tartibga soladi. Zero, virtual olamdagi jinoyatchilikning zarar va xavfi real olamdagidan kam emas.

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.

Mamlakatning iqtisodiy, ijtimoiy, madaniy rivojlanishining statistik ko’rsatkichlarining haqqoniyligi, ishonchliligi va konfidensialligini ta’minlash bugungi kundagi dolzarb muammolardan biri hisoblanadi. 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 tizimi va resurs egalari darhol xabardor qilindi. Aniqlangan zaifliklarning asosiy qismi o'ta xavfli (466 ta), o'rta xavfli(205 ta) va past xavfli(24 ta) hodisalarga ajratilib, tegishli tartibda choralar ko'rildi.

Kiber tahdidlarning kuchayib borayotgan murakkabligi arafasida butun dunyo bo'ylab hukumatlar va tartibga soluvchi organlar kiberxavfsizlik choralarini yanada kuchaytirish, jismoniy shaxslar va tashkilotlarning shaxsiy hayotini himoya qilishga qaratilgan kompleks normativ-huquqiy bazalarni ishlab chiqish bo'yicha amaliy faoliyatlarini kuchaytirdi. Yevropa Ittifoqidagi "Umumiy ma'lumotlarni himoya qilish to'g'risida"gi nizom (GDPR) va AQShdagi "Kaliforniya maxfiylik huquqi akti" (CCPA) kabi tartibga solish tashabbuslari ma'lumotlarni himoya qilish va maxfiylik huquqlarini birinchi o'ringa qo'yishda paradigma o'zgarishini bildiradi. Bundan tashqari, xalqaro hamkorlik va xalqlar o'rtasida axborot almashish transmilliy kiber tahdidlarga qarshi kurashishning ajralmas qismiga aylandi, bu esa kiberxavfsizlik qiyinchiliklarini global miqyosda bartaraf etishga kollektiv yondashuvni shakllantirdi.

Geosiyosat va kiberxavfsizlik o'rtasidagi o'zaro ta'sir global kiber tahdid manzarasini shakllantirishda juda muhim determinant sifatida paydo bo'ldi. Davlat miqyosidagi kiber janglar va josuslik keng tarqaldi. Millat-davlatlar hukmronlikni da'vo qilish, dushmanlarni kamsitish va strategik maqsadlarga erishish uchun kibernetik imkoniyatlarni qo'llamoqda. Kiber fazoning qurollanishining kuchayib borayotgani natijasida tanqidiy infrastruktura, davlat institutlari va asosiy sohalarga qaratilgan kiber hujumlar xavfi kuchaydi, bu esa milliy xavfsizlik va geosiyosiy barqarorlikka sezilarli tahdid solmoqda. Kiber hujumlarning aniq millat-davlatlar bilan bog'liqligi diplomatik ziddiyatlarga sabab bo'ldi va kiber fazoda davlat xatti-harakatlarini tartibga solish bo'yicha xalqaro normalar va shartnomalarni talab qildi.

Kiberxavfsizlikni yo‘lga qo‘yuvchi texnologik yutuqlar va murakkab algoritmlar orasida inson faktori ham tanqidiy omil, ham sezilarli zaiflik bo‘lib qolmoqda. Inson xatosi, beparvolik va zararli ichki ishlar tashkilot kiberxavfsizligi uchun katta xavf tug‘dirishda davom etmoqda, bu esa xodimlarni keng qamrovli o‘qitish dasturlari zarurligini ko‘rsatib bermoqda. Fishing va boshqa ijtimoiy muhandislik taktikasi inson zaifliklaridan foydalanib, maxfiy ma’lumotlarga ruxsatsiz kirish imkoniyatiga ega bo‘ladi, xodimlar o‘rtasida xushyorlik va mas’uliyatli raqamli amaliyot madaniyatini rivojlantirish muhimligini ta’kidlaydi. Bundan tashqari, kiberxavfsizlikda paydo bo‘lgan texnologiyalardan foydalanish bilan bog‘liq axloqiy masalalar shaxsiy maxfiylik va asosiy huquqlarni himoya qilishni birinchi o‘ringa qo‘yadigan yaxlit yondashuvni talab qiladi.

Ma’lumotlarga asoslangan texnologiyalarning tarqalishi va shaxsiy ma’lumotlarning keng to‘planishi ko‘plab xavotirlarga va maxfiylikka ta’sirni keltirib chiqardi, bu esa xavfsizlik imperativlari va alohida maxfiylik huquqlari o‘rtasidagi tarozida bahs-munozaralarga sabab bo‘ldi. Texnologiya kompaniyalari tomonidan shaxsiy ma’lumotlarning o‘zgartirilishi va kuzatuv texnologiyalarining keng tarqalganligi ma’lumotlar ekspluatatsiyasi va maxfiylik chegaralarining eroziyasi to‘g‘risidagi qo‘rquvlarni yanada kuchaytirdi. Kiberxavfsizlikda ma’lumotlar tahlili va sun’iy intellektdan foydalanish shaffof ma’lumotlar amaliyotiga rioya qilishni, rozilikka asoslangan ma’lumotlarni to‘plashni, alohida maxfiylikni ta’minlash va maxfiy ma’lumotlar asosida firibgarlik amaliyotlarining oldini olish uchun ma’lumotlarni himoya qilish mexanizmlarini amalga oshirishni talab qiladi. 2023-yil 13-oktabr holatiga ko‘ra hakerlar tomonidan yuritilishi taxmin qilingan internet tarmoqlaridan birida dunyo bo‘ylab 180 milliondan ortiq foydalanuvchilarning turli platformalardagi login va parollari ochiqlangan holda tarqaldi. Soha mutaxassislari fikriga ko‘ra, ushbu hakerlar tarqatgan login-parollar qatorida yagona identifikatsiya tizimi — OneID, DTM, tashkilotlar va oliy ta’lim muassasalari o‘quv tizimlari, turli ko‘ngilochar portallar, onlayn do‘kon, qidiruv xizmatlari, veb-xizmatlar ko‘rsatuvchilar va o‘quv markazlari, banklar va to‘lov tizimlari va turli saytlarning boshqaruv panellariga kirish kodlari ham bo‘lgan. Umumiy qilib aytganda, turli

platformalardagi o‘n minglab o‘zbekistonlik foydalanuvchilarning ma’lumotlari tarqatilgan.

Ekspertlarning aytishicha, ushbu vaziyatda holat taxminan shunday bo‘lgan**: dunyo bo‘ylab millionlab foydalanuvchilarning kompyuterlariga tushgan viruslar ularning brauzerida saqlangan login-parollarni yig‘gan. Hakerlar to‘plangan ma’lumotlarni bitta faylga yig‘ib, tarqatib yuborgan.**

“Oq hakerlar”ning fikriga ko‘ra esa, bunday holat quyidagi sabablarga ko‘ra sodir bo‘lishi mumkin:

- **Zaif parol siyosati**. Taxmin qilinadigan darajada zaif parollarni ishlatish va ularni bir nechta resurslar uchun qayta ishlatish kibergigiyena talablariga zid bo‘lib, ularni buzib kirish xavfini oshiradi;
- **Lisenziyasiz yoki eskirgan dasturlardan foydalanish.** Xavfsizlik login va parollarining ochiq internetga chiqib ketishi, tashkilotlar uchun jiddiy kiberxavfsizlik hodisalarini keltirib chiqarishi mumkin. Hakerlar ushbu ma’lumotlardan infratuzilmalarni yorib kirish va keyinchalik infratuzilma ichkarisidan turib boshqa kiberhujumlarni amalga oshirishda foydalanishlari mumkin.
- **Zararlangan qurilma.** Qurilmaga mobil troyan yoki stiler kabi zararli dasturlar o‘rnatilgan hollarda, login-parol yordamida boshqa maxfiy ma’lumotlar to‘planadi va hujumning keyingi bosqichlarida jiddiy tus oladi.
- **Ichki (insayder) ma’lumotlar.** Bu odatiy hollardan biri hisoblanadi, ya’ni tashkilotdan norozi bo‘lgan xodimlar mijozlar bazasiga va boshqa muhim tizimlarga kirib, ulardan yashirincha g‘arazli maqsadlarda foydalanadi.
- **Ijtimoiy muhandislik (fishing yoki vishing).** Manipulyatsiya va aldashni o‘z ichiga olgan ushbu kiberhujum texnikasi tajovuzkorlarga tizim yoki ma’lumotlarga kirishga imkon yaratib beradi. Bu esa katta kiberhujumlarni boshlash oldidan yuqoridagi usullar orqali tashkilot haqida qo‘shimcha ma’lumotlar to‘plash imkonini yaratadi.

Tahdid manzarasi rivojlanishda davom etar ekan, kiber o‘zgaruvchanlik madaniyatini shakllantirish kiber tahdidlarga qarshi samarali kurashish va xavfsizlik buzilishlarining ehtimoliy ta’sirini minimallashtirish uchun eng asosiy vazifa bo‘lib qolmoqda. Tashkilotlar muntazam xavfni baholash, xavfsizlikni ta’minlash bo‘yicha treninglar va kiber o‘zgaruvchanlik pozitsiyasini mustahkamlash uchun hodisalarga javob berish protokollarini joriy etish kabi faol choralarni amalga oshirishlari kerak. Kiber o‘zgaruvchanlik nafaqat kiber tahdidlarning oldini olish va aniqlash qobiliyatini, balki xavfsizlik hodisalaridan tezkor javob olish va samarali tiklanish, biznesning davomiyligini ta’minlash va moliyaviy yo‘qotishlar va obro‘ga yetkazilgan zararni minimallashtirish imkoniyatini ham nazarda tutadi. Kiber o‘zgaruvchanlikni o‘zlarining asosiy biznes strategiyalariga birlashtirish orqali tashkilotlar raqamli chegarani samarali yo‘lga qo‘yishlari va doimo rivojlanayotgan kiber xavflarni proaktiv tarzda yengillashtirishlari mumkin.

Kiberxavfsizlik manzarasining kelajakdagi trayektoriyasi tahdid razvedkasi va proaktiv mudofaa mexanizmlarini amalga oshirishga qaratilgan tezkor texnologik yutuqlar va transformatsiyaviy yangiliklar bilan aniqlanishga tayyor. Kvant hisoblashning tarqalishi va uning kriptografiya va ma’lumotlar xavfsizligiga ta’siri raqamli muloqot va sezgir ma’lumotlarni himoya qilish uchun kvantga chidamli shifrlash usullarini ishlab chiqishda paradigma o‘zgarishini e’lon qiladi. 5G texnologiyasi va “cheti hisoblash”ning birlashtirilishi raqamli infrastrukturani o‘zgartirishi belgilangan bo‘lib, ma’lumotlarni tezroq qayta ishlash va real vaqt rejimida tahdidlarni aniqlash imkonini beradi, shu bilan birga desentralizatsiya qilingan tarmoq arxitekturasini ta’minlashda yangi qiyinchiliklar tug‘diradi. Biometrik autentifikatsiya va “Zero Trust Security” modellarining integratsiyasi kirishni nazorat qilish chora-tadbirlarini qayta tasniflash, shaxsni aniqlashni kuchaytirishni ta’minlash va tanqidiy tizimlar va ma’lumotlarga ruxsatsiz kirishni minimallashtirishi kutilmoqda.

Kiber tahdidlarning kuchayishi va rivojlanayotgan tahdid manzarasi qarshisida kiberxavfsizlikka kollektiv yondashuvni shakllantirishda hamkorlikdagi tashabbuslar va davlat-xususiy sherikchilik muhim ahamiyatga

ega bo‘ldi. Axborot almashish va tahlil qilish markazlari (ISAC) va Kompyuter favqulodda vaziyatlarga javob berish guruhlari (CERT) kabi hamkorlik platformalari sanoat yetakchilari o‘rtasida tahdid razvedkasi va eng yaxshi amaliyotlarni baham ko‘rishni osonlashtiradi, bu esa paydo bo‘lgan kiber tahdidlarga proaktiv javob berish imkonini beradi. Hukumatlar, akademiya va xususiy sektor o‘rtasidagi davlat-xususiy sheriklik bilimlar almashinuvi, mahoratni rivojlantirish va tadqiqotlar hamkorligini shakllantiradi, zamonaviy kiberxavfsizlik yechimlarini ishlab chiqishni va murakkab kiber qiyinchiliklarni bartaraf etishga qodir malakali ishchi kuchini yetishtirishni rag‘batlantiradi.

Sun’iy intellekt (AI) va Mashina o‘rganish (ML) kiberxavfsizlik imkoniyatlarini kuchaytirishda muhim imkoniyatlar sifatida paydo bo‘ldi, tashkilotlarga real vaqt rejimida murakkab kiber tahdidlarni proaktiv ravishda aniqlash, tahlil qilish va ularga javob berish imkoniyatini berdi. AI tomonidan boshqariladigan tahdidlarni aniqlash tizimlari kuchayishidan oldin ehtimoliy xavfsizlik buzilishlarini aniqlash va yengillashtirish uchun bashoratli tahlil va anomaliyani aniqlash algoritmlaridan foydalanadi, bu esa raqamli infrastrukturalarning umumiy o‘zgaruvchanligini oshiradi. Mashina o‘rganish algoritmlari ulkan ma’lumotlar to‘plamini tahlil qilish zararli ishlarni ko‘rsatuvchi namunalar va tendensiyalarni aniqlash imkonini beradi, bu esa xavfsizlik mutaxassislariga mustahkam mudofaa strategiyalari va adaptiv xavfsizlik choralarini ishlab chiqish imkonini beradi. Biroq, kiberxavfsizlik sohasida AIga asoslangan qaror qabul qilishning axloqiy ta’siri javobgarlikni ta’minlash va algoritmik tarafkashlik va firibgarlik amaliyotlari xavfini kamaytirish uchun shaffof va tushunarli AI modellarini amalga oshirishni talab qiladi.

Rivojlanayotgan kiber tahdid manzarasi arafasida raqamli savodxonlikni targ‘ib qilish va raqamli landshaftni xavfsiz yo‘lga qo‘yish uchun zarur bo‘lgan bilim va ko‘nikmalarga ega shaxslarga kuch berishda ta’lim tashabbuslari juda muhim rol o‘ynaydi. Ta’lim muassasalari va o‘quv markazlari talabalar va mutaxassislarni zamonaviy kiber qiyinchiliklarni bartaraf etish uchun zarur texnik va amaliy tajriba bilan qurollantirish uchun yetarli darajada keng qamrovli kiberxavfsizlik o‘quv dasturlarini joriy etishi kerak. Turli demografik

ko‘rsatkichlarga qaratilgan kiberxavfsizlikni ta’minlash kampaniyalarida parollar gigiyenasi, ma’lumotlarni shifrlash va xavfsiz ko‘rib chiqish odatlari bo‘yicha eng yaxshi amaliyotlarni qabul qilish, jamoalar va tashkilotlar bo‘ylab raqamli mas’uliyat va o‘zgaruvchanlik madaniyatini shakllantirish talab qilinadi.

Tashkilotlar tobora kuchayib borayotgan va davomli tahdid manzarasiga duch kelar ekan, qiyinchiliklar qarshisida o‘zgaruvchanlikni shakllantirish kiber hujumlarning ehtimoliy ta’sirini yengillashtirish va biznes operatsiyalarining davomiyligini ta’minlash uchun zarurligicha qolmoqda. Kiber o‘zgaruvchanlik strategiyalari mustahkam hodisalarga javob berish rejalarini amalga oshirish, muntazam xavfsizlik tahlillari, uzluksiz nazorat va tahdidlarni aniqlashni ta’kidlaydigan proaktiv xavfsizlik pozitsiyasini qabul qilishni qamrab oladi. Adaptiv xavfsizlik choralari va tezkor javob protokollarini muhimlashtiradigan bardoshli tashkiliy madaniyatni o‘stirish orqali korxonalar kiber hodisalarning moliyaviy oqibatlarini samarali minimallashtirishi va hamkorlarning raqamli ekotizimga bo‘lgan ishonchini saqlab qolishi mumkin.

Xulosa qilib shuni ta’kidlash mumkinki, raqamli davrda shaxsiy ma’lumotlarni himoya qilish jismoniy shaxslar, tashkilotlar va hukumatlar uchun ham zaruriy topshiriq bo‘lib xizmat qiladi. Kiberxavfsizlik maxfiy ma’lumotlarni himoya qilish hamda raqamli operatsiyalarning maxfiyligi va yaxlitligini saqlab qolishda linchpin (jamoa yoki tashkilotning konturlarini birlashtiradigan yagona shaxs yoki narsa) sifatida paydo bo‘ladi, bu esa mustahkam xavfsizlik choralari va proaktiv mudofaa strategiyalariga bo‘lgan jiddiy ehtiyojni ko‘rsatadi. Texnologik yutuqlar va o‘zaro bog‘liq qurilmalarning tarqalishi raqamli muhitni qayta shakllantirar ekan, kiberxavfsizlik sohasi yangi paydo bo‘lgan kiber tahdidlarga qarshi turishga, xavfsiz va bardoshli raqamli ekotizimni ta’minlashga qaratilgan doimiy innovatsiyalar va transformatsiyaviy o‘zgarishlarga muhtoj. Hamkorlik va ko‘p tomonlama yondashuvni shakllantirish, kompleks normativ-huquqiy bazalarni takomillashtirish, ilg‘or texnologiyalar va malakali ishchi kuchini rivojlantirishga investitsiya kiritish orqali global hamjamiyat raqamli chegarani birgalikda yo‘lga qo‘yishi va barcha uchun xavfsizroq va bardoshliroq raqamli kelajakni ta’minlashi mumkin.

Foydalanilgan adabiyotlar ro‘yxati:

1. Ganiyev, S.K. (2020). Kiberxavfsizlik asoslari. O‘quv qo‘lanma.
2. Ichki ishlar akademiyasi rasmiy sayti.
3. https://akadmvd.uz/oz/news/kiber-olamdagi-hatarlar-dolzarb-muammo
4. California Legislative Information. (2018). California Consumer Privacy Act (CCPA). Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
5. Kun.uz – axborot veb sayti.
6. https://kun.uz/uz/news/2023/10/20/misli-korilmagan-kiberhujum-hakerlar-200-mingdan-ortiq-ozbekistonlik-foydalanuvchilarning-login-parollarini-sizdirdi#
7. Elissa M. Redmiles.(2020). Toward the Science of Security and Privacy in Machine Learning. Google Schoolar.
8. **LexUz** — internetdagi O‘zbekiston qonun hujjatlari ma’lumotlari milliy bazasi.
9. O‘zbekiston Respublikasi Prezidentining 2017-yil 29-noyabrdagi PQ-3413-son qarori bilan tasdiqlangan “Ichki ishlar organlarida xizmatni o‘tash tartibi to‘g‘risida”gi Nizom.