

TA'LIM MUASSASALARIDA UCHRAYDIGAN KIBERXAVFLAR

*Kariyeva Xilola Alisher qizi***Annotatsiya**

Ushbu maqolada ta'lim muassasalarida uchraydigan kiberxavflar va ularning ta'lim jarayoniga ta'siri tahlil qilinadi. Kiberxavflarning asosiy turlari, xususan, ma'lumotlarning o'g'irlanishi, zararli dasturlar, phishing va kiberhujumlar kabi hodisalar ko'rib chiqiladi. Shuningdek, muassasalarda kiberxavfsizlikni ta'minlashning samarali usullari va zamonaviy texnologiyalardan foydalanish yo'llari muhokama qilinadi. Maqola ta'lim jarayonidagi raqamli xavfsizlikni oshirish va xavfsizlik madaniyatini shakllantirishga qaratilgan tavsiyalarni ham o'z ichiga oladi.

Kalit so'zlar: Kiberxavfsizlik, ta'lim muassasalari, kiberhujum, ma'lumotlarni himoya qilish, raqamli texnologiyalar, phishing, zararli dasturlar.

Bugungi kunda ta'lim muassasalari faoliyatida raqamli texnologiyalar va internetdan foydalanish ortib bormoqda. Bu esa ta'lim jarayonini samarali va interaktiv qiladi, ammo shu bilan birga kiberxavf va kiberhujumlar xavfini ham oshiradi. Kiberxavflar nafaqat muassasalarning ma'lumotlar bazasiga, balki o'quvchilarning shaxsiy ma'lumotlariga ham tahdid soladi. Shu sababli, ta'lim muassasalarida kiberxavfsizlikni ta'minlash, xavflarni aniqlash va oldini olish choralari dolzarb masala hisoblanadi. Ushbu maqola kiberxavflarning asosiy turlarini, ularning ta'lim jarayoniga ta'sirini va muassasalarda xavfsizlikni kuchaytirish yo'llarini tahlil qilishga qaratilgan.

Ta'lim muassasalarida uchraydigan kiberxavflar turli shakllarda namoyon bo'ladi. Eng keng tarqalganlari orasida zararli dasturlar (viruslar, trojanlar), phishing xujumlari, ma'lumotlar o'g'irlanishi va tarmoq orqali hujumlar mavjud. Zararli dasturlar kompyuter tizimlariga zarar yetkazib, o'quv jarayonini to'xtatishi yoki ma'lumotlarni yo'q qilishi mumkin. Phishing xujumlari esa o'quvchi va xodimlarning shaxsiy ma'lumotlarini o'g'irlashga qaratilgan.

Kiberxavflar nafaqat muassasalarning ma'lumotlar bazasini, balki o'quvchilarning shaxsiy ma'lumotlarini ham tahdid ostiga qo'yadi. Tizimlar buzilganda, darslar onlayn tarzda o'tkazilmay qolishi yoki o'quv jarayoni sekinlashishi mumkin. Shu bilan birga, kiberxavflar o'quvchilarda ishonchsizlikni yaratadi va pedagoglarning ishlash samaradorligini kamaytiradi.

Ta'lim muassasalarida kiberxavfsizlikni ta'minlash uchun bir qator choralar ko'riladi. Ularga antivirus dasturlarini o'rnatish, xavfsiz parollar tizimini joriy etish, tarmoq trafikini nazorat qilish va xodimlar hamda o'quvchilarni kiberxavfsizlik bo'yicha muntazam o'qitish kiradi. Shuningdek, muassasalarda ma'lumotlarni zahira

qilish va maxfiylik siyosatini ishlab chiqish muhim hisoblanadi. Kiberxavfsizlikni kuchaytirishda zamonaviy texnologiyalar katta rol o'ynaydi. Bulutli saqlash tizimlari, ikki faktorli autentifikatsiya, tarmoq monitoring tizimlari va sun'iy intellekt asosidagi xavfsizlik dasturlari kiberhujumlardan himoya qilishda samarali vositalardir. Shu bilan birga, ta'lim muassasalari uchun xavfsizlik siyosatini doimiy yangilab borish zarur. Ta'lim muassasalarida xavfsizlikni ta'minlash faqat texnologiyaga bog'liq emas. O'quvchi, o'qituvchi va ma'muriyat xodimlarida kiberxavfsizlik madaniyatini shakllantirish muhimdir. Xodimlar va o'quvchilar onlayn xavflardan ehtiyot bo'lishni, shaxsiy ma'lumotlarni himoya qilishni va xatarli saytlardan uzoq turishni bilishi lozim. Ta'lim muassasalarida onlayn darslar va elektron ta'lim platformalaridan foydalanish ortib bormoqda. Shu bilan birga, ushbu platformalarda ham kiberxavf mavjud. Masalan, noto'g'ri konfiguratsiya qilingan tizimlar yoki zaif parollar orqali tizimga ruxsatsiz kirish mumkin. Shuning uchun muassasalar elektron platformalarni muntazam yangilab turishi va foydalanuvchilarni xavfsiz foydalanish bo'yicha o'qitishi zarur.

Ta'lim muassasalarida yig'ilgan shaxsiy va akademik ma'lumotlar maxfiyligi katta ahamiyatga ega. Ma'lumotlar bazasining himoyasizligi yoki noto'g'ri boshqarilishi kiberxujum va ma'lumotlarni yo'qotish xavfini oshiradi. Shu sababli, ma'lumotlarni shifrlash, ruxsatlar tizimini joriy etish va muntazam zaxira qilish kabi chora-tadbirlar muhim hisoblanadi. Muassasalar o'z tizimlarini kiberxavflarga tayyorlash va ehtimoliy hujumlarni aniqlash uchun muntazam testlar o'tkazishi kerak. Bu testlar tizimdagi zaifliklarni aniqlash va ularni vaqtida bartaraf etish imkonini beradi. Shu bilan birga, xodimlar va o'quvchilarda kiberhujumlarga javob berish ko'nikmalarini rivojlantirish ham muhimdir. Ta'lim muassasalari kiberxavfsizlik sohasida boshqa ta'lim muassasalari, texnologik kompaniyalar va hukumat organlari bilan hamkorlik qilishi zarur. Bu nafaqat zamonaviy xavf-xatarlarni tez aniqlashga yordam beradi, balki xodimlarning malakasini oshirish va eng yaxshi amaliyotlarni joriy etishga imkon yaratadi.

Kiberxavfsizlik ta'lim muassasalarida doimiy e'tibor talab qiladigan soha hisoblanadi. Muassasalar xavflarni kamaytirish, tizimlarni himoya qilish va foydalanuvchilarning xavfsizlik madaniyatini shakllantirish orqali onlayn ta'lim sifatini oshirishi mumkin. Shu bilan birga, zamonaviy texnologiyalar va muntazam treninglar kiberxavflardan samarali himoya qilishda asosiy vositalar sifatida xizmat qiladi.

Kiberxavfsizlikni ta'minlashda nafaqat texnologiyalar, balki xodimlarning malakasi va hushyorligi muhim ahamiyatga ega. O'qituvchilar va ma'muriyat xodimlari shaxsiy ma'lumotlarni himoya qilish, onlayn platformalarda xavfsiz ishlash va kiberhujumlarga tez javob berish bo'yicha muntazam treninglardan o'tishi kerak. Xodimlarning bilim va tajribasi kiberxavflarning oldini olish va ularni minimal zarar

bilan bartaraf etishga yordam beradi. O'quvchilarga ham kiberxavfsizlik bo'yicha ko'nikmalarni shakllantirish zarur. Bu ularga shaxsiy ma'lumotlarni himoya qilish, onlayn xatarlardan ehtiyot bo'lish, kuchli parol va ikki faktorli autentifikatsiyadan foydalanish, shuningdek zararli dasturlarni aniqlash va ulardan himoyalaniшни o'rgatadi. Kiberxavfsizlik madaniyati o'quvchilarda mas'uliyat hissini oshiradi va ta'lim jarayonini xavfsiz qiladi. Ta'lim muassasalarida xavfsizlikni mustahkamlash uchun aniq siyosat va me'yoriy hujjatlar ishlab chiqilishi kerak. Bu hujjatlar tizimlar va ma'lumotlar xavfsizligini ta'minlash bo'yicha standartlar, foydalanuvchilarning majburiyatlari, ma'lumotlarni zaxiralash va monitoring qilish tartibini belgilaydi. Siyosat doimiy ravishda yangilanib, zamonaviy xavf-xatarlarni qamrab olishi muhimdir.

Muassasalar kiberxavflarni doimiy ravishda monitoring qilishi va ularning xavf darajasini baholashi lozim. Bu tizimdagi zaifliklarni va xavfli vaziyatlarni erta aniqlash imkonini beradi. Shu bilan birga, xavf tahlili asosida oldini olish strategiyasi ishlab chiqilishi va amalga oshirilishi muhimdir. Raqamli texnologiyalar rivojlanishi bilan birga, yangi kiberxavflar ham yuzaga keladi. Masalan, sun'iy intellekt asosidagi xujumlar, mobil qurilmalardagi zaifliklar va internet-of-things (IoT) qurilmalariga ruxsatsiz kirish xavfi oshmoqda. Shu sababli ta'lim muassasalari texnologik yangiliklarga moslashib, xavfsizlik tizimini doimiy takomillashtirishi zarur. Kiberxavfsizlikni ta'minlash ta'lim jarayonining sifatini oshiradi. Tizimlar barqaror ishlashi, ma'lumotlar xavfsizligi va onlayn resurslarga ishonchli kirish o'quvchilarning o'qish samaradorligini oshiradi. Shu bilan birga, kiberxavfsizlik madaniyati shakllangan muassasalarda pedagoglar va o'quvchilar xavfsizlikka oid xatolarga kam duch keladi.

Ta'lim muassasalarida kiberxavfsizlikni oshirish uchun xodimlar va o'quvchilarni muntazam trening va seminarlar orqali o'qitish muhim hisoblanadi. Bu treninglar ularga yangi xavf-xatarlarni aniqlash, shaxsiy ma'lumotlarni himoya qilish, zararli dasturlardan ehtiyot bo'lish va onlayn muhitda xavfsiz harakat qilish ko'nikmalarini beradi. Shu tarzda, kiberxavfsizlik bo'yicha tizimli tayyorgarlik jarayoni tashkil etiladi. Kiberxavf yuzaga kelganda muassasa xodimlari va IT bo'limi tezkor choralar ko'rishi lozim. Kiberhujumga javob berish rejasi, texnik va tashkiliy choralarni o'z ichiga oladi. Tezkor javob berish tizimdagi zararni kamaytiradi, o'quv jarayonining uzluksizligini ta'minlaydi va ma'lumotlarni himoya qiladi.

Muassasalar o'z tizimlarini muntazam ravishda auditdan o'tkazishi va xavf-xatarlarni baholashi lozim. Bu mavjud tizimdagi zaifliklarni aniqlashga, himoya choralarni kuchaytirishga va yangi xavflarga qarshi tayyor turishga imkon yaratadi. Shu bilan birga, baholash natijalari asosida xavfsizlik siyosati va strategiyasi doimiy ravishda yangilanadi. Kiberxavfsizlikni ta'lim jarayoniga integratsiya qilish muhimdir. Bu nafaqat tizim va ma'lumotlar xavfsizligini ta'minlaydi, balki o'quvchilarda

mas'uliyat, ehtiyotkorlik va onlayn xavfsizlik madaniyatini shakllantiradi. Shu tarzda, ta'lim muassasalarida raqamli texnologiyalardan xavfsiz va samarali foydalanish ta'minlanadi.

Bugungi kunda ta'lim muassasalari bulutli xizmatlardan faol foydalanmoqda. Bulutli saqlash va onlayn xizmatlar o'quv jarayonini soddalashtiradi, lekin ular ham kiberxavflarga ochiq bo'lishi mumkin. Shu sababli bulutli xizmatlarga kirishdagi autentifikatsiya tizimlarini kuchaytirish, shifrlash va foydalanuvchi ruxsatlarini aniq belgilash zarur.

O'quvchilarning va xodimlarning mobil qurilmalari, planshet va IoT qurilmalari orqali ta'lim resurslariga kirishi xavflarni oshiradi. Zaif parol yoki noto'g'ri sozlangan qurilmalar kiberhujumga olib keladi. Shu sababli mobil qurilmalar xavfsizligini ta'minlash, ilovalarni tekshirish va foydalanuvchilarga xavfsiz foydalanish bo'yicha ko'rsatmalar berish muhimdir. O'quvchilar va xodimlar tomonidan ijtimoiy tarmoqlarda amalga oshiriladigan harakatlar ham kiberxavf manbai bo'lishi mumkin. Ma'lumotlarni noto'g'ri ulash, phishing xabarlar yoki zararli havolalarga bosish orqali tizimlar buzilishi ehtimoli mavjud. Shu sababli ijtimoiy tarmoqlarda xavfsiz xulq-atvor qoidalarini o'rgatish zarur. Ta'lim muassasalari o'z tizimlarini doimiy monitoring qilish va kiberxavf yuzaga kelishini oldindan aniqlash tizimlarini joriy etishi kerak. Sun'iy intellekt va analitik dasturlar yordamida xavf-xatarlarni prognozlash va ularga qarshi choralar ko'rish samarali vositalardir. Texnologiyalar rivojlanishi bilan kiberxavf doimiy yangilanadi. Shu sababli ta'lim muassasalari xavfsizlik strategiyasini doimiy yangilab borishi, xodimlar va o'quvchilarni yangi tahdidlar haqida muntazam xabardor qilishi muhimdir. Bu tizimli yondashuv ta'lim jarayonining barqarorligini va ma'lumotlarning xavfsizligini ta'minlaydi.

Kiberxavflar nafaqat tizim va ma'lumotlarga zarar yetkazadi, balki ta'lim muassasalarining iqtisodiy resurslariga ham salbiy ta'sir ko'rsatadi. Tizimlarni tiklash, ma'lumotlarni qayta tiklash va xavfsizlikni ta'minlash uchun qo'shimcha xarajatlar talab qilinadi. Shuningdek, o'quvchilarda ishonchsizlik, pedagoglarda esa stress va ish samaradorligining pasayishi kabi ma'naviy zararlar ham yuzaga keladi.

Kiberxavflardan himoya qilish uchun muassasalar kompleks strategiya ishlab chiqishi zarur. Bu strategiya texnik chora-tadbirlar (antivirus, firewall, shifrlash), tashkiliy choralar (treninglar, xavfsizlik siyosati) va xodim hamda o'quvchilarni xabardor qilishni o'z ichiga oladi. Strategiya muntazam yangilanib, zamonaviy tahdidlar bilan uyg'un bo'lishi muhimdir. Ta'lim muassasalari kiberxavfsizlik sohasida boshqa muassasalar, hukumat organlari va texnologik kompaniyalar bilan hamkorlik qilishi zarur. Hamkorlik orqali eng yangi xavf-xatarlar aniqlanadi, tajriba almashiladi va xavfsizlik bo'yicha eng yaxshi amaliyotlar joriy etiladi.

Kiberxavfsizlik choralarini samarali amalga oshirish ta'lim jarayonining uzluksizligini ta'minlaydi. Onlayn darslar, elektron resurslar va ma'lumotlar

xavfsizligi kafolatlangan holda o'quvchilar faol ishtirok etadi. Shu bilan birga, tizim buzilishining oldi olinadi va pedagoglarning ish samaradorligi oshadi. Kelajakda ta'lim muassasalarida kiberxavfsizlikning roli yanada oshadi. Sun'iy intellekt, IoT va boshqa raqamli texnologiyalar keng qo'llanilishi bilan birga, yangi xavf-xatarlar ham paydo bo'ladi. Shu sababli, ta'lim muassasalari doimiy ravishda innovatsion xavfsizlik yechimlarini joriy etishi va xodim hamda o'quvchilarning kiberxavfsizlik ko'nikmalarini oshirishi zarur.

Ta'lim muassasalarida kiberxavflarning yuzaga kelishida inson omili muhim rol o'ynaydi. Ko'plab kiberhujumlar texnik zaifliklardan ko'ra, foydalanuvchilarning ehtiyotsizligi, xabardorlik darajasining pastligi yoki noto'g'ri qarorlari natijasida sodir bo'ladi. Masalan, noma'lum havolalarga bosish, shubhali fayllarni yuklab olish yoki parollarni begonalarga oshkor qilish kiberxavfni kuchaytiradi. Shu bois inson omiliga alohida e'tibor qaratish zarur.

Zaif va bir xil parollardan foydalanish ta'lim muassasalarida keng tarqalgan muammolardan biridir. Kuchli parol siyosati joriy etilmagan taqdirda, tizimlarga ruxsatsiz kirish ehtimoli ortadi. Ikki bosqichli autentifikatsiya, biometrik himoya va parollarni muntazam yangilab borish kabi choralar kiberxavflarning oldini olishda muhim ahamiyatga ega.

Ta'lim muassasalarida elektron jurnal, reyting tizimi, diplom va sertifikatlar kabi muhim hujjatlar saqlanadi. Ushbu ma'lumotlarning buzilishi yoki o'zgartirilishi ta'lim jarayonining adolatliligiga putur yetkazadi. Shuning uchun akademik ma'lumotlar maxfiyligini ta'minlash, ularni shifrlash va kirish huquqlarini qat'iy nazorat qilish zarur hisoblanadi. Kiberxavflar bilan bog'liq muammolar huquqiy jihatdan ham muhimdir. Ta'lim muassasalarida sodir bo'ladigan kiberjinoyatlar uchun javobgarlik masalalari aniq belgilanishi lozim. Kiberxavfsizlikka oid milliy va xalqaro qonunchilik talablari muassasalarda to'liq tatbiq etilishi, foydalanuvchilar esa o'z huquq va majburiyatlarini bilishi kerak. Kiberxavflarning oldini olishda eng samarali usullardan biri raqamli savodxonlikni oshirishdir. O'quvchilar va o'qituvchilarga internetdan xavfsiz foydalanish, shaxsiy ma'lumotlarni himoyalash va kiberxavf belgilarini aniqlash bo'yicha bilimlar berilishi muhimdir. Profilaktik yondashuv kiberxavflarning yuzaga kelish ehtimolini sezilarli darajada kamaytiradi.

Masofaviy ta'limning keng joriy etilishi bilan kiberxavflar yanada murakkablashdi. Uy sharoitida foydalaniladigan tarmoqlar va shaxsiy qurilmalar ko'pincha yetarli darajada himoyalangan bo'ladi. Bu esa zararli dasturlar, ruxsatsiz kirish va ma'lumotlar sizib chiqishiga olib kelishi mumkin. Shu sababli masofaviy ta'limda xavfsiz aloqa kanallari va himoyalangan platformalardan foydalanish muhimdir.

Elektron pochta ta'lim muassasalarida asosiy aloqa vositalaridan biri hisoblanadi. Phishing va spam xabarlar orqali foydalanuvchilarni aldash, ularning login va

parollarini qo'lga kiritish hollari tez-tez uchraydi. Bunday hujumlarning oldini olish uchun elektron pochta filtrlari, xavfsizlik ogohlantirishlari va foydalanuvchilarning hushyorligini oshirish zarur.

Ba'zi ta'lim muassasalarida foydalanilayotgan axborot tizimlari eskirgan bo'lib, zamonaviy xavfsizlik talablariga to'liq javob bermaydi. Dasturiy ta'minotni o'z vaqtida yangilamaslik va texnik xizmat ko'rsatishning sustligi kiberhujumlar ehtimolini oshiradi. Shu bois tizimlarni muntazam auditdan o'tkazish va yangilab borish talab etiladi. Ayniqsa maktab ta'limida ota-onalar ham elektron kundalik, baholash tizimlari va onlayn platformalardan foydalanadi. Agar ota-onalar kiberxavfsizlik qoidalaridan bexabar bo'lsa, bu ham xavf manbai bo'lishi mumkin. Shu sababli ota-onalar uchun ham axborot xavfsizligi bo'yicha tushuntirish ishlari olib borilishi maqsadga muvofiqdir. Kiberxavfsizlikni samarali ta'minlash uchun muassasalarda yagona boshqaruv tizimi bo'lishi zarur. Bu tizim xavflarni aniqlash, monitoring qilish, javob choralarini belgilash va javobgarlikni taqsimlashni o'z ichiga oladi. Tizimli yondashuv kiberxavflarning oldini olishda muhim ahamiyat kasb etadi.

Xulosa.

Xulosa qilib aytganda, ta'lim muassasalarida raqamli texnologiyalardan keng foydalanilishi kiberxavflarning paydo bo'lishi va murakkablashuviga olib kelmoqda. Ma'lumotlar bazalari, onlayn ta'lim platformalari, elektron hujjatlar va shaxsiy axborotlar kiberhujumlar uchun asosiy nishon hisoblanadi. Ushbu xavflar ta'lim jarayonining uzluksizligi, sifati va ishonchliligiga salbiy ta'sir ko'rsatishi mumkin. Ta'lim muassasalarida kiberxavfsizlikni ta'minlash faqat texnik vositalar bilan cheklanib qolmasdan, balki tashkiliy va pedagogik yondashuvni ham talab etadi. Xodimlar, o'quvchilar va ota-onalarda kiberxavfsizlik madaniyatini shakllantirish, raqamli savodxonlikni oshirish hamda muntazam treninglar tashkil etish kiberxavflarning oldini olishda muhim omil hisoblanadi. Zamonaviy xavfsizlik texnologiyalaridan foydalanish, axborot tizimlarini doimiy monitoring qilish, huquqiy-me'yoriy talablarni amaliyotga joriy etish va muassasalararo hamkorlikni kuchaytirish orqali ta'lim muassasalarida barqaror va xavfsiz raqamli muhitni yaratish mumkin. Natijada, kiberxavfsizlik ta'lim sifatini oshirishga xizmat qiluvchi muhim omil sifatida namoyon bo'ladi.

Foydalanilgan adabiyotlar.

1. O'zbekiston Respublikasi "Axborotlashtirish to'g'risida"gi Qonuni.
2. Kaspersky Lab. Cybersecurity Basics.
3. UNESCO. Digital Literacy and Online Safety.
4. Microsoft Security Intelligence Reports.
5. ITU rasmiy portali — global kiberxavfsizlik hisobotlari.
6. O'zbekiston Respublikasi Prezidentining raqamli texnologiyalar va axborot xavfsizligini rivojlantirishga oid nutqlari va farmonlari.

7. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — Wiley.
8. Auezov, O. P., Baltaniyazov, A. S., Tursimuratov, S. Ye., & Xojabaev, N. M. (2025, November). Saksavul ekadigan seyalkaning yangi egat shakllantiruvchi ishchi organining texnologik va konstruktiv parametrlarini asoslash. In Conferences (Vol. 1, No. 4, pp. 425-428).

