TA'LIM MUASSASALARIDA KIBERXAVFSIZLIK MUAMMOLARI

Mirzajonov Axrorbek Ubaydullayevich

Annotatsiya: *Ushbu maqola raqamli asrda ta'lim muassasalari duch kelayotgan kiberxavfsizlik tahdidlarining kuchayishini tahlil qiladi. Maktablar onlayn platformalar va raqamli vositalarni tobora ko'proq qabul qilgani sayin, ular ma'lumotlar buzilishi, fishing hujumlari, to'lov dasturlari va maxfiy ma'lumotlarga ruxsatsiz kirishga nisbatan zaifroq bo'ladi. Maqolada umumiy xavfsizlik muammolari, ularning talabalar va xodimlarga ta'siri va xavfsiz raqamli infratuzilmani yaratish bo'yicha eng yaxshi amaliyotlar o'rganiladi. Kiberxavfsizlik bo'yicha xabardorlikni oshirish, himoya texnologiyalarini joriy etish va institutsional siyosatni ishlab chiqish bo'yicha tavsiyalar berilgan.*

Kalit so'zlar: *kiberxavfsizlik, ta'lim muassasalari, ma'lumotlarni himoya qilish, raqamli tahdidlar, axborot xavfsizligi, onlayn xavfsizlik, kiberxavfsizlikdan xabardorlik.*

Ta'lim muassasalarida kiberxavfsizlik muammolari tobora dolzarb ahamiyat kasb etmoqda. Chunki zamonaviy ta'lim jarayonida axborot texnologiyalaridan keng foydalanish, ta'lim muassasalarini kiberhujumlarga nisbatan zaif holga keltirmoqda. Quyida ta'lim muassasalarida uchraydigan asosiy kiberxavfsizlik muammolari va ularning oqibatlari keltirilgan.

Ma'lumotlar buzilishi :

• Muammo: Ta'lim muassasalarida talabalar, o'qituvchilar va xodimlar haqida shaxsiy ma'lumotlar (ismi, familiyasi, manzili, telefon raqami, elektron pochta manzili, baholari, tibbiy ma'lumotlari va moliyaviy ma'lumotlari) saqlanadi. Kiberhujumlar natijasida ushbu ma'lumotlar o'g'irlanishi yoki oshkor qilinishi mumkin.

So'nggi yillarda texnologiyaning ta'lim muassasalariga jadal integratsiyalashuvi, ayniqsa, COVID-19 pandemiyasi kabi global voqealar nuqtai nazaridan, ta'lim manzarasini keskin o'zgartirdi. Onlayn ta'limga o'tish bilan birga, ta'lim muassasalari elektron ta'limni boshqarish tizimlarini tobora ko'proq qamrab oldi, ular operatsion samaradorlikka va talabalar xavfsizligiga ta'sir qiluvchi ko'plab kiberxavfsizlik tahdidlarini kiritdi. Kiberxavfsizlik bo'yicha mutaxassislarga bo'lgan talab o'sishda davom etar ekan, ikkinchi darajali muassasalar uchun kiberxavfsizlikka e'tiborni o'z ichiga olgan keng qamrovli STEM o'quv dasturlarini ishlab chiqish zaruratga aylandi. Ushbu evolyutsiya texnologik innovatsiyalarning kesishishini va ta'lim muhitida mustahkam xavfsizlik choralari zarurligini ta'kidlaydi, ayniqsa maktablar ortib borayotgan tahdidlar sharoitida nozik ma'lumotlarni himoya qilishga intiladi. Ushbu muammolarning kombinatsiyasi kiberxavfsizlikka proaktiv yondashuvni ta'kidlab, ta'lim sektorining o'ziga xos kontekstiga moslashtirilgan samarali xavflarni kamaytirish strategiyalari zarurligini ta'kidlaydi. Texnologiyalar rolining vizual tasviri ta'limda rivojlangan raqamli infratuzilma va xavfsizlik choralariga bo'lgan ehtiyojni qamrab oladi.

Ta'lim muassasalari raqamli vositalar va onlayn platformalarga tobora ko'proq tayanib borayotganligi sababli, mustahkam kiberxavfsizlik choralarining ahamiyatini ortiqcha baholab bo'lmaydi. Bu muhitlar ular tomonidan boshqariladigan ma’lumotlarning, jumladan, talaba yozuvlari, moliyaviy operatsiyalar va mulkiy ma’lumotlarning nozik tabiati tufayli zaifliklar bilan to‘la. So'nggi tadqiqotlarda ta'kidlanganidek, xodimlar o'rtasida kiberxavfsizlik bo'yicha tegishli treningning yo'qligi bu zaifliklarni kuchaytirishi mumkin, bu esa institutlarni fishing va ma'lumotlarning buzilishi kabi tahdidlarga ochiq qoldirishi mumkin. Bundan tashqari, oliy ta'limda raqamli transformatsiyaga bo'lgan intilish paydo bo'layotgan kiber tahdidlardan himoya qilish uchun kuchli IT infratuzilmasini talab qiladi.

Ushbu muammolarni hal qilish uchun ta'lim muassasalari quyidagi choralarni ko'rishlari kerak:

- Kiberxavfsizlik siyosatini ishlab chiqish va amalga oshirish: Bu siyosat xavfsizlik talablari, xodimlar va talabalar uchun qoidalar va protseduralarni belgilashi kerak.
- Xodimlarni va talabalarni kiberxavfsizlik bo'yicha o'qitish: Kiberxavfsizlik xavflari, fishing, zaif parollar va xavfsiz internetdan foydalanish qoidalari haqida ma'lumot berish.
- Kuchli parollardan foydalanishni talab qilish va ikki faktorli autentifikatsiyani joriy etish.
- Dasturiy ta'minot va operatsion tizimlarni muntazam ravishda yangilab turish.
- Tarmoqni himoya qilish uchun xavfsizlik devorlari va intrusion detection tizimlaridan foydalanish.
- Ma'lumotlarni shifrlash va zaxiralash.
- Kiberxavfsizlik hodisalariga javob berish rejasini ishlab chiqish.
- Kiberxavfsizlik bo'yicha mutaxassislarni jalb qilish yoki tashqi xizmatlardan foydalanish.

Ta'lim muassasalari kiberxavfsizlikni jiddiy qabul qilishlari va o'z tizimlarini va ma'lumotlarini himoya qilish uchun zarur choralarni ko'rishlari kerak. Bu talabalarning, xodimlarning va ta'lim muassasasining obro'sini himoya qilishga yordam beradi