

MASOFAVIY TA'LIM PLATFORMALARIDA AXBOROT XAVFSIZLIGINI TA'MINLASH USULLARI

O'R HX va MU HAI

Toshov Fazlidin Kulmuradovich

Aviatsiya mutaxassislarini bilim va malakalarini baholash markazi dotsenti

Annotatsiya: Ushbu maqolada masofaviy ta'lim platformalarida axborot xavfsizligini ta'minlashning zamonaviy usullari, kiberxavfsizlik tahdidlari va ularni bartaraf etish yo'llari tahlil qilingan. Shuningdek, elektron ta'lim tizimlarida foydalanuvchi ma'lumotlarini himoyalash, autentifikatsiya tizimlari, ma'lumotlarni shifrlash hamda sun'iy intellekt texnologiyalaridan foydalanishning ahamiyati yoritilgan. Masofaviy ta'lim platformalarida xavfsizlikni ta'minlash bo'yicha amaliy tavsiyalar ishlab chiqilgan.

Kalit so'zlar: Masofaviy ta'lim, axborot xavfsizligi, kiberxavfsizlik, elektron ta'lim, autentifikatsiya, shifrlash, ma'lumotlar bazasi, sun'iy intellekt, raqamli texnologiyalar, himoya tizimlari.

Kirish. Hozirgi kunda dunyoda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi barcha sohalar qatori ta'lim tizimiga ham katta ta'sir ko'rsatmoqda. Ayniqsa, masofaviy ta'lim texnologiyalari zamonaviy ta'limning muhim tarkibiy qismiga aylanib bormoqda. So'nggi yillarda internet tarmoqlarining kengayishi, elektron platformalarning rivojlanishi hamda raqamli texnologiyalarning ommalashuvi natijasida ta'lim jarayonlarini masofadan turib tashkil etish imkoniyatlari sezilarli darajada oshdi.

Masofaviy ta'lim platformalari o'qituvchi va talaba o'rtasidagi aloqani onlayn tarzda tashkil etadi. Ushbu platformalar orqali videodarslar o'tkazish, topshiriqlar yuborish, test sinovlari tashkil qilish va elektron hujjatlar almashinuvi amalga oshiriladi. Shu sababli mazkur tizimlarda katta hajmdagi muhim axborotlar saqlanadi. Elektron ta'lim tizimlarida foydalanuvchilarning shaxsiy ma'lumotlari, parollari, bank rekvizitlari, test natijalari va boshqa maxfiy ma'lumotlar mavjud bo'ladi. Ushbu ma'lumotlarning himoyasizligi turli kiberjinoyatlar va noqonuniy harakatlarga sabab bo'lishi mumkin. Shu bois masofaviy

ta'lim platformalarida axborot xavfsizligini ta'minlash bugungi kunning eng dolzarb masalalaridan biri hisoblanadi.

Axborot xavfsizligi — bu axborotning maxfiyligi, yaxlitligi va foydalanish imkoniyatini himoya qilish jarayonidir. Zamonaviy ta'lim platformalarida axborot xavfsizligini ta'minlash uchun turli texnologiyalar va dasturiy vositalardan foydalaniladi.

Masofaviy ta'lim tizimlarida uchraydigan xavfsizlik muammolari.

Hozirgi kunda masofaviy ta'lim platformalari ta'lim jarayonining muhim qismiga aylanib bormoqda. Elektron ta'lim tizimlari orqali o'quv materiallari almashinuvi, videodarslar tashkil etish, test sinovlarini o'tkazish va foydalanuvchilar ma'lumotlarini saqlash ishlari amalga oshiriladi. Shu sababli ushbu platformalarda axborot xavfsizligini ta'minlash dolzarb vazifalardan biri hisoblanadi. Masofaviy ta'lim tizimlarida turli xil xavfsizlik tahdidlari uchrab turadi va ular tizimning ishonchli ishlashiga salbiy ta'sir ko'rsatishi mumkin.

Masofaviy ta'lim tizimlarida eng ko'p uchraydigan muammolardan biri foydalanuvchi akkauntlarini buzish holatlaridir. Ko'plab foydalanuvchilar oddiy va himoyasiz parollardan foydalanishadi. Natijada xakerlar maxsus dasturlar yordamida akkauntlarga noqonuniy kirish imkoniyatiga ega bo'ladilar. Akkaunt buzilishi foydalanuvchilarning shaxsiy ma'lumotlari, o'quv natijalari va boshqa maxfiy axborotlarning tarqalib ketishiga olib keladi. Shu sababli murakkab parollardan foydalanish va xavfsizlik choralarini kuchaytirish muhim hisoblanadi.

Bundan tashqari, fishing hujumlari ham keng tarqalgan kiberxavfsizlik tahdidlaridan biri sanaladi. Fishing hujumlarida foydalanuvchilarga soxta havolalar yoki qalbaki elektron xatlar yuboriladi. Foydalanuvchi ushbu havolalar orqali o'z login va parollarini kiritganda, ma'lumotlar xakerlar qo'liga tushib qoladi. Ta'lim platformalari foydalanuvchilari ham bunday tahdidlarga tez-tez duch kelishlari mumkin. Masofaviy ta'lim tizimlari zararli dasturlar tahdidiga ham duch keladi. Viruslar, troyan dasturlari va boshqa zararli fayllar orqali tizimga noqonuniy kirish holatlari kuzatiladi. Ushbu dasturlar foydalanuvchi qurilmalaridagi ma'lumotlarni o'g'irlashi, tizim faoliyatini izdan chiqarishi

yoki ma'lumotlarni yo'q qilishi mumkin. Natijada ta'lim platformalarining ishlash samaradorligi pasayadi.

DDoS hujumlari ham zamonaviy kiberjinoyatlar orasida keng tarqalgan hisoblanadi. Ushbu hujumlar serverlarga juda katta hajmdagi so'rovlarni yuborish orqali tizimni ishdan chiqarishga qaratiladi. Natijada platforma vaqtincha ishlamay qoladi va foydalanuvchilar tizimdan foydalana olmaydi. Bu esa ta'lim jarayonining uzilishiga sabab bo'ladi. Texnik nosozliklar yoki zararli hujumlar natijasida ma'lumotlarning yo'qolishi ham muhim muammolardan biridir. Agar ma'lumotlar bazasi zarar ko'rsa, muhim hujjatlar, test natijalari va o'quv materiallari yo'qolib ketishi mumkin. Shu sababli ma'lumotlarni muntazam zaxiralab borish talab etiladi.

Axborot xavfsizligini ta'minlash usullari.

Masofaviy ta'lim platformalarida xavfsizlikni ta'minlash uchun zamonaviy himoya texnologiyalaridan foydalanish muhim ahamiyatga ega. Axborot xavfsizligi foydalanuvchilar ma'lumotlarini himoya qilish, tizimning uzluksiz ishlashini ta'minlash hamda noqonuniy kirishlarning oldini olishga xizmat qiladi. Xavfsizlikni ta'minlashning asosiy usullaridan biri kuchli autentifikatsiya tizimlarini joriy etish hisoblanadi. Foydalanuvchilarni identifikatsiya qilish axborot xavfsizligining muhim bosqichidir. Oddiy parollar o'rniga murakkab va kuchli parollardan foydalanish tavsiya etiladi. Harflar, raqamlar va maxsus belgilar kombinatsiyasidan tashkil topgan parollar tizim xavfsizligini oshiradi. Ikki bosqichli autentifikatsiya tizimi (2FA) foydalanuvchi xavfsizligini sezilarli darajada oshiradi. Ushbu usulda foydalanuvchi tizimga kirishda nafaqat paroldan, balki telefon raqamiga yuborilgan maxsus koddan ham foydalanadi. Bu esa akkauntlarning buzilish ehtimolini kamaytiradi. Biometrik autentifikatsiya texnologiyalari ham zamonaviy himoya vositalaridan biri hisoblanadi. Bunda barmoq izi, yuzni aniqlash yoki ko'z qorachig'i orqali foydalanuvchi shaxsi tasdiqlanadi. Ushbu texnologiyalar xavfsizlik darajasini yanada oshiradi. Ma'lumotlarni shifrlash texnologiyalari axborot xavfsizligini ta'minlashning eng samarali usullaridan biri hisoblanadi. Shifrlash orqali ma'lumotlar maxsus kodlarga aylantiriladi va ularni noqonuniy o'qishning oldi olinadi. Natijada ma'lumotlar xavfsiz saqlanadi.

SSL va TLS protokollari internet orqali ma'lumot almashinuvi xavfsizligini ta'minlaydi. Ushbu texnologiyalar foydalanuvchi va server o'rtasidagi axborotni himoyalangan holda uzatishga yordam beradi. Zamonaviy platformalarda aynan ushbu protokollardan keng foydalaniladi. AES va RSA kabi zamonaviy kriptografik algoritmlar ma'lumotlarni yuqori darajada himoya qilish imkonini beradi. Ushbu algoritmlar bank tizimlari va elektron platformalarda keng qo'llaniladi. Masofaviy ta'lim platformalarida antivirus dasturlaridan foydalanish ham muhim ahamiyatga ega. Antivirus tizimlari zararli dasturlarni aniqlaydi va ularni bartaraf etadi. Natijada foydalanuvchi qurilmalari va serverlar himoyalanaadi.

Xavfsizlik monitoringi tizimlari server va tarmoqlardagi shubhali harakatlarni kuzatib boradi. IDS va IPS tizimlari yordamida noqonuniy kirish urinishlari aniqlanadi hamda tezkor choralar ko'riladi. Monitoring tizimlari real vaqt rejimida ishlaydi va administratorlarga xavf haqida darhol xabar beradi. Ma'lumotlarni zaxiralash axborot xavfsizligining muhim tarkibiy qismlaridan biri hisoblanadi. Muhim hujjatlar va ma'lumotlar muntazam ravishda backup serverlarda saqlanishi kerak. Bu esa texnik nosozliklar yoki hujumlar natijasida ma'lumotlarni qayta tiklash imkonini beradi. Bulutli texnologiyalar yordamida ma'lumotlarni xavfsiz saqlash imkoniyatlari yanada kengaymoqda. Google Cloud, Microsoft Azure va Amazon Web Services kabi platformalar zamonaviy backup xizmatlarini taklif etadi. Ushbu xizmatlar ma'lumotlarni xavfsiz saqlash va tezkor tiklash imkonini yaratadi. Shunday qilib, masofaviy ta'lim platformalarida axborot xavfsizligini ta'minlash uchun zamonaviy texnologiyalar va himoya tizimlaridan samarali foydalanish muhim hisoblanadi. Bu esa ta'lim tizimlarining ishonchliligini oshirish va foydalanuvchilar ma'lumotlarini himoya qilishga xizmat qiladi.

Talabalar va o'qituvchilarga:

- kuchli parol yaratish;
- fishing havolalarni aniqlash;
- noma'lum fayllarni yuklab olmaslik;
- antivirus dasturlaridan foydalanish;
- shaxsiy ma'lumotlarni himoya qilish

bo'yicha muntazam treninglar tashkil etilishi kerak.

Sun'iy intellekt texnologiyalarining o'rni.

Sun'iy intellekt texnologiyalari axborot xavfsizligini ta'minlashda muhim rol o'ynamoqda. AI texnologiyalari yordamida kiberhujumlarni oldindan aniqlash va xavfli faoliyatlarni avtomatik monitoring qilish imkoniyati mavjud.

Machine Learning algoritmlari foydalanuvchilarning odatiy harakatlarini tahlil qiladi va shubhali faoliyatlarni aniqlaydi. Natijada xavfsizlik tizimlarining samaradorligi ortadi. AI asosidagi tizimlar katta hajmdagi ma'lumotlarni tezkor tahlil qilish imkonini beradi.

O'zbekistonda masofaviy ta'lim va axborot xavfsizligi.

O'zbekistonda ham so'nggi yillarda masofaviy ta'lim tizimlari keng rivojlanmoqda. Oliy ta'lim muassasalarida Moodle, Google Classroom, Zoom va Microsoft Teams platformalaridan keng foydalanilmoqda. Raqamli ta'lim tizimlarining rivojlanishi bilan bir qatorda kiberxavfsizlik masalalariga ham katta e'tibor qaratilmoqda. Davlat tomonidan axborot xavfsizligini ta'minlashga oid qonun va dasturlar ishlab chiqilgan. "Raqamli O'zbekiston – 2030" strategiyasi doirasida elektron ta'lim tizimlarini rivojlantirish va xavfsizligini oshirish bo'yicha keng ko'lamli ishlar amalga oshirilmoqda.

Xulosa.

Xulosa qilib aytganda, masofaviy ta'lim platformalarida axborot xavfsizligini ta'minlash bugungi kunning muhim masalalaridan biri hisoblanadi. Zamonaviy ta'lim tizimlarida katta hajmdagi ma'lumotlar saqlanishi sababli ularni himoyalash dolzarb ahamiyat kasb etadi. Kuchli autentifikatsiya tizimlarini joriy etish, ma'lumotlarni shifrlash, antivirus dasturlaridan foydalanish, xavfsizlik monitoringi va backup tizimlarini tashkil etish orqali ta'lim platformalarining ishonchliligini oshirish mumkin. Kelajakda sun'iy intellekt va avtomatlashtirilgan xavfsizlik tizimlari axborot xavfsizligini yanada rivojlantirishga xizmat qiladi. Shu sababli ta'lim tizimlarida zamonaviy kiberxavfsizlik texnologiyalarini keng joriy etish muhim ahamiyatga ega.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni.

2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.
3. Stallings W. Cryptography and Network Security. — Pearson Education, 2020.
4. Behrouz A. Forouzan. Data Communications and Networking. — McGraw Hill, 2019.
5. Kaspersky Cybersecurity Report, 2024.
6. Cisco Networking Academy materiallari.
7. Microsoft Security Documentation.
8. Google Cloud Security Whitepaper.
9. Zamonaviy kiberxavfsizlik texnologiyalari bo‘yicha ilmiy maqolalar.
10. Internet manbalari va elektron resurslar.