MASOFAVIY O‘QITISH TIZIMLARIDA MAVJUD RISKLAR VA ULARNI MINIMALLASHTIRISH ISTIQBOLLARI

Bekmirzayev Obidjon Nuraliyevich, Samarov Husnutdin Kamardinovich, Xabibullayev Jahongirbek Doniyorbek o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti
bekmirzayevobidjon1989@gmail.com

Annotatsiya: *Masofaviy ta’limning ahamiyati va ehtiyojini inobatga olgan holda, so‘nggi yillarda Oliy ta’limda o‘qitish metodologiyasi keskin o‘zgardi. Shubhasiz, Masofaviy o‘qitish tizimiga qaratilgan risklarni minimallashtirish hamda buzg‘unchi hujumlaridan himoyalanish borasida nazariy va ilmiy asoslangan yechimlar taklif qilindi. Masofaviy o‘qitish tizimi har bir darajadagi barcha ob’ektlar o‘rtasida to‘liq yaxlitlikni talab qiladi. Yaxlitlikni ta’minlashdan tashqari, butun tizimda riskni minimallashtirishni ta’minlash uni tashkil etishning yana bir muhim usuli hisoblanadi.*

Kalit so‘zlar: *Masofaviy o‘qitish tizimi, risk, maxfiylik, konfidensiallik, yaxlitlik, foydalanuvchanlik, raqamli imzo, sertifikatsiya, asimmetrik shifrlash.*

RISKS IN DISTANCE EDUCATION SYSTEMS AND THE PROSPECTS OF THEIR MINIMIZATION

Abstract: *Taking into account the importance and need of distance education, the methodology of teaching in higher education has changed dramatically in recent years. Undoubtedly, theoretical and scientifically based solutions have been proposed to minimize risks and protect against hacker attacks aimed at distance education system. A distance learning system requires complete integrity between all facilities at every level. In addition to ensuring integrity, ensuring the minimization of risk throughout the system is another important way of organizing it.*

Keywords: *Distance learning system, risk, privacy, confidentiality, integrity, usability, digital signature, certification, asymmetric encryption.*

Axborot-kommunikatsiya texnologiyalarining eng samarali qo‘llanilishidan biri bu masofaviy o‘qitish tizimlarining paydo bo‘lishidir. Masofaviy ta’limning ahamiyati va ehtiyojini inobatga olgan holda, so‘nggi yillarda Oliy ta’limda o‘qitish metodologiyasi keskin o‘zgardi. Shubhasiz, Masofaviy o‘qitish tizimining uchta asosiy ob’ektini talaba, o‘qituvchi va nazorat qiluvchi organ deb hisoblash mumkin va ular

turli darajalarda bo‘ladi, ammo yaxshi masofaviy o‘qitish tizimi har bir darajadagi barcha ob’ektlar o‘rtasida to‘liq yaxlitlikni talab qiladi. Yaxlitlikni ta’minlashdan tashqari, butun tizimda riskni kamaytirishni ta’minlash uni tashkil etishning yana bir muhim usuli hisoblanadi. Internet butun tizimning asosi bo‘lib, u turli risk hatarlariga boy bo‘lganligi sababli, masofaviy o‘qitish tizimida ma’lumotlarni uzatilish paytida xakkerlar tizimlarning turli bo‘shliqlaridan foydalangan holda hujum qilishadi. Shuning uchun tizimga turli xil riskni kamaytirish choralarini qo‘llash talab etiladi. Ushbu maqolada masofaviy o‘qish tizimining barcha ishtirokchilari uchun mavjud turli xil risklarga va ularni himoya vositalariga e’tibor qaratilgan.

Axborot-kommunikatsiya texnologiyalari asosida ta’limda masofaviy o‘qitish muhitini joriy etilishi oliy ta’lim tizimini yangi ko‘rinishiga olib keldi. Shu nuqtayi nazardan, internet ilg‘or o‘quv materiallari va tegishli manbalarga bo‘lgan talabni bajaradi. Har qanday ta’lim muassasasi masalan, (Universititet, Korporativ Tashkilot va boshqalar) ba’zi moliyaviy ishlar bilan shug‘ullanadi. Ammo globallashuv davrida turli mamlakatlar va jamoalardan kelgan talabalar bir xil daraja yoki diplom uchun paydo bo‘lishi mumkin, chunki masofa va geografik joylashuv umuman muammo emas. Shunday qilib, masofaviy va onlayn ta’lim jarayonida talabalar, o‘qituvchilar va o‘quv jamoalari o‘rtasidagi ta’lim sohasidagi o‘zaro ta’sirlarni rag‘batlantirish uchun masofaviy va onlayn ta’limni o‘rganish kabi turli qoliblarda quriladi [1].

Masofaviy ta’lim tizimi o‘quv faoliyatini internet orqali elektron tarzda amalga oshirishni anglatadi. Turli xil masofaviy o‘qitish tizimlarining rivojlanishi oliy ta’lim tizimini, ayniqsa sifatli elektron ta’lim xizmatlari va qo‘llab-quvvatlash jarayonlariga nisbatan butunlay o‘zgartiradi. Masofaviy ta’lim tizimida beshta muhim ishtirokchi mavjud bo‘llib, Ular: mualliflar, talabalar, o‘qituvchilar va tizim ishlab chiquvchilari (tizim ma’murlari). Masofaviy o‘qitish tizimlarida xakerlar o‘qituvchidan talabalarga yoki mualliflardan talabalarga yuborilgan o‘quv materiallari, sertifikatlar, savollar to‘plami, ma’ruza materiallari, baholarini va boshqa autentifikatsiya talab qilingan hujjatlarini o‘zgartirishi mumkin, qaysiki kerak bo‘lganda yetkaziladi. Masofaviy ta’lim an’anaviy ta’lim tizimiga nisabatan boshqa ssenariydaligi ta’limga qiziqqan o‘quvchilar, kengroq ma’noda “Talabalar”, faqat an’anaviy maktab, kollej va universititet auditoriyalari bilan chegaralanib qolmaydi [2].

Risk - bu ma’lum bir tahdidning yuzaga kelish ehtimoli va kutilayotgan yo‘qotish. Masofaviy o‘qitish tizimlarida risk – masofaviy ulanish paytidagi riskni o‘z ichiga oladi, tahdid esa kutilgan riskni anglatadi. Kompyuterlar uchun keng tarqalgan tahdidlar - viruslar, tarmoqqa suqilib kirish, ma’lumotlarni o‘g‘irlash va ruxsatsiz o‘zgartirish, tinglashlar kiradi.

Masofaviy ulanish davomida asl hujjatlar xakerlarning aktiv va passiv hujumlari natijasida o‘zgartirilishi, noto‘g‘ri ma’lumotlar qo‘shilishi yoki yo‘q qilinishi mumkin.

Shuning uchun masofaviy o‘qitish tizimlaridagi risklarni to‘g‘ri baholab ularga to‘g‘ri usul va choralarni qo‘llashga to‘gri keladi. Ushbu maqolada asosiy e’tibor masofaviy o‘qitish tizimni ishonchli va samarali qilish uchun foydalanuvchilar duch keladigan risklarga va ularni bartaraf etishga qaratilgan [2].

Ma’lumotlarni yo‘qolish tahdidlari yoki risklarni amalga oshirish natijasida yuzaga keladi. Barcha tahdidlar va risklar tizimlardagi turli xil zaiflik orqali amalga oshiriladi:

1. Maxfiylikni buzilishi. Ruxsatsiz shaxs masofaviy o‘qitish tizimidagi ma’lumotlarga kirish huquqiga ega;
2. Butunlikni buzish. Masofaviy o‘qitish tizimidagi ma’lumotlarga ruxsatsiz kirish va unga ishlov berish;
3. Xizmat ko‘rsatishni rad etish. Masofaviy o‘qitish tizimi foydalanuvchilari o‘rtasida ulanishni amalga oshirishda trafikni buzish orqali qonuniy foydalanish huquqlarini cheklash;
4. Noqonuniy foydalanish. Qonuniy foydalanuvchilar imtiyozlardan foydalanish;
5. Zararli dastur. Boshqa dasturlarga zarar yetkazish uchun kod qatorlari;
6. Rad etish. Hujjatlarning har qanday bitimida ishtirok etishni rad etish;
7. Maskarad. Xakerlar tomonidan haqiqatni yashiradigan o‘zini tutish usuli;
8. Trafik tahlili. Aloqa kanalini suiiste’mol qilish orqali ma’lumotlarning sirqib chiqishi;
9. Qo‘pol kuch hujumi. Tizimga kirish uchun barcha mumkin bo‘lgan kombinatsiyalar bilan urinish.

Yuqoridagi tahdidlar natijasida masofaviy tizimning turli ishtirokchilari o‘rtasida matnli va matnli bo‘lmagan xabarlarni o‘tkazishda quyidagi risklar yuzaga kelishi mumkin.

Zamonaviy texnologiyalar mualliflarga kitoblar, jurnallar va boshqa materiallarini talabalar va keng ilmiy kengash doirasiga oson va tez taqdim etish imkonini berdi. Mualliflar o‘zining mualliflik ishini ishlab chiqish va amalga oshirish uchun bir qancha vaqt va bilim sarflashadi. Ko‘pgina mualliflar onlayn ya’ni masofaviy tizimlar orqali taqdim etishdan bosh tortishining sababi, ularning yig‘ilgan materiallari ularga xabarsiz boshqalarga yuborilishi, qayta ishlanishi va xatto o‘g‘irlanishi ham mumkinligidan qo‘rqishadi. Faqatgina ro‘yxatdan o‘tgan talabalar ushbu o‘qituvchi eslatmalari, topshiriqlari va maqolalariga kirishlari mumkinligi sababli, Masofaviy o‘qitish tizimi bilan bog‘liq turli kontekstlarda ma’lumotlardan ruxsatsiz foydalanish, o‘zgartirish va qayta foydalanishdan himoya qilish muallifning vazifasidir [3].

Muallifning ma’ruza matnlari, nazorat savollari, uy topshiriqlari va boshqalar yuqoridagi hujumlar orqali xakerlar tomonidan o‘zgartirilishi yoki yo‘q qilinishi mumkin. Shu sababli, foydalanuvchilar kontentni o‘zgarmagan holda olishlari va foydalanuvchilar matnning yaxlitligini tekshirishlari mumkin bo‘lishi muallifning manfaatlariga mos keladi. Ma’lumotlarning muntazam zaxira nusxalarini yaratish va ayrim komponentlar (masalan, qattiq disk, tarmoq ulanishlari) buzilgan taqdirda harakatlar rejasi risk tahlilining muhim elementlari hisoblanadi. Bunday hollarda moliyaviy manfaatlar ham muhim rol o‘ynaydi [2].

Masofaviy tizimlarda o‘qituvchilar talabalarga o‘quv ishlari bilan bog‘liq har qanday yordamni elektron tarzda ko‘rsatishlari kerak bo‘ladi. O‘qituvchilar kurs talabiga binoan kurs mazmunini, taqdimotlarni uchinchi tomondan kuzatishi yoki sotib olishi mumkin. Masofaviy barcha risklar texnik tizim bilan cheklanib qolmasligi kerak. O‘qitish, tekshirish, baholash va baholashning barcha usullarini qamrab olish lozimdir. O‘qitish metodologiyasi bir o‘qituvchidan boshqasiga o‘zgaradi, lekin ma’ruza o‘qish, eslatma va topshiriqlarni yuborish, javob varaqalarini qabul qilish va belgilash, baholash varaqalarini tayyorlash va tarqatish kabi hodisalarda umumiy risklar mavjud bo‘ladi. Munozaralar har qanday kursni o‘qitishning muhim tarkibiy qismidir. Munozara shakllaridan biri onlayn forum orqali bo‘lishi mumkin. Onlayn forum muhokamalarining og‘zaki muhokamalardan afzalligi shundaki, barcha yozma hujjatlar serverda elektron shaklda saqlanadi, ammo munozaraga qo‘shilgan hissalarning raqamli saqlanishi talabalar va o‘qituvchilarning shaxsiy hayoti uchun katta risk tug‘diradi. Garchi har qanday o‘qitish tizimda maksimal darajada o‘zaro ta’sir o‘tkazish talabalarga ham, o‘qituvchilarga ham o‘z tushunchalarini tushunishga yordam berishi mumkin. Faqat yuqori darajada riskni kamaytirish mexanizmi uzoq muddatda bunday o‘zaro ta’sirga olib kelishi mumkin. Imtihon tizimida imtihon savollarini standartlashtirish va savollar ro‘yxatini o‘z ichiga olgan risk mavjud, ehtimol individual o‘qituvchilarning akademik erkinligini cheklaydi. Ish shartnomasiga qarab, o‘qituvchi akademik markazda rol o‘ynaydi. Bu risklarning barchasiga javob beradigan (oldini oladigan) jamoa bo‘lishi kerak. Tekshiruv bilan bog‘liq risk to‘g‘ridan-to‘g‘ri aldash bilan bog‘liqdir [2]. Aldashdan tashqari, o‘qituvchilar baholarning mavjudligi va rad etilmasligi haqida tashvishlanishlari kerak. Shuningdek, imtihon vaqtida talabalar o‘rganish mazmuniga nisbatan materiallar to‘plashga ko‘proq intiladilar. Barcha o‘qituvchilar imtihonlar boshlanishidan oldin talabalar o‘zgartirilmagan savollar qog‘ozini olishlari va barcha javoblar o‘zgarmagan holda saqlanishi riskidan xabardor bo‘lishlari kerak. Garchi ma’ruza muloqotning eng oddiy va tabiiy shakli bo‘lsa-da, dars ma’ruzasi talabalarga yetib kelganiga qadar uni o‘zgartirish riski doimo saqlanib qoladi.

Mavjud tizimlarda turli hil cheklovchi omillar mavjud. Vaqti-vaqti bilan butun tizimni improvizatsiya qilish uchun bu omillarni o‘zgartirish kerak bo‘ladi. Lekin buning uchun ham uzoq vaqt va ko‘p mablag‘ sarflanadi. Masofaviy tizimda kurslar turli modullarga tasniflanadi. Agar barcha modullar oldin ishlab chiqilmagan bo‘lsa, yangi ishlab chiqish guruhi yangilarini ishlab chiqish va amalga oshirish uchun turli muammolarga duch kelishlari mumkin. Masofaviy tizim mahsulotlarini loyihalash, ishlab chiqish va yetkazib berish yuqori darajadagi veb-server va ma’lumotlar bazasi serveri, yuqori o‘tkazish qobiliyatiga ega bo‘lgan internet liniyasi va sifatli tarmoqlararo ekran apparat komponentalari sifatini, shuningdek, bir nechta foydalanuvchilarni va tarmoq ilovalarini qo‘llab-quvvatlashga qodir mustahkam infratuzilmani talab qiladi. Tizim ichlab chiraruvchi jamoa ushbu risklarni bartaraf etish yo‘llarini to‘g‘ri taklif qilishi kerak, aks holda loyihaning umumiy qiymati deyarli ikki baravar ko‘payadi. Ishlab chiquvchi dastur kodida aniq matnda parollarni saqlash bilan shug‘ullanishi kerak bo‘lgan yana bir risk, qo‘shtirnoq ichidagi aqlli o‘quvchilar zararli kodlarni manba kodiga kiritishi va ma’lumotlar bazasi paroliga buzib kirishi mumkin. Bundan tashqari, parol tizimi buzg‘inchilar tomonidan o‘g‘irlanishi yoki o‘zgartirilishi mumkin bo‘lsa, parol tizimi risk ostida bo‘lishi yoki buzilishi mumkin. Bugungi kunda buzg‘unchi foydalanuvchi parolini aniqlash uchun ko‘plab vositalardan foydalanmoqda. Tizim ishlab chiquvchisi yoki ma’lumotlar bazasi ma’murlari multimediya ma’lumotlar bazasini saqlash uchun SQL injection hamda saytlararo script (XSS) hujumlaridan xabardor bo‘lishi kerak [2].

Tizim foydalanuvchilarining asosiy qismi bu o‘quvchilardir. Kirish ma’lumotlarini (foydalanuvchi login va parollar)ni saqlash riski bu eng ko‘p uchrab turadigan risklardan bir xisoblanadi. Barcha talabalar login ma’lumotlaridan to‘g‘ri foydalanishdan xabardor bo‘lishlari kerak, aks holda buzg‘unchi yuqoridagi hujumlar orqali tizimga kirish huquqi mavjud o‘quvchining tizimga kirishiga to‘sqinlik qilishi mumkin. O‘qituvchilar har doim ham talabalarga yordam bera olmaydi, shuning uchun ular O‘qituvchining yordamisiz mustaqil ishlashlari uchun qoidalarga to‘liq rioya qilishliklari kerak. O‘qituvchilar va boshqa talabalar yuzma-yuz uchrashmasa, nimani nazarda tutganini noto‘g‘ri talqin qilish mumkin. Talabalarning fikr-mulohazalarini bildirishlari har doim o‘qituvchini izlanishga va yana ma’sulyatda undaydi. Nihoyat, barcha o‘quvchilar fishing hujumlaridan xabardor bo‘lishlari kerak, bu yerda buzg‘unchi haqiqiy tizim veb-saytiga o‘xshab ko‘rinadigan soxta veb-saytni shunchalik haqiqiy tizim saytiga o‘xshash qilib yaratadiki, inson ko‘zlari haqiqiy va sohta saytni ajrata olmaydi. Bu yerda o‘quvchilardan ba’zi maxfiy ma’lumotlarni kiritish taklif qilinadi, shu tariqa o‘quvchining ma’lumotlari osongina buzg‘unchini qo‘liga o‘tib qoladi.

Yuqoridagi risklardan tashqari tizimda shu kabi turli xil boshqa risklar mavjud.

Tabiiy tahdidlar yong‘in, bo‘ron, vulqon otilishi, zilzila, suv toshqini va boshqalar kabi tabiiy ofatlar tufayli yuzaga kelishi mumkin. Masofaviy o‘qitish tizimiga bu risklar katta ta’sir ko‘rsatishi mumkin [2].

Shunday qilib, masofaviy o‘qitish tizimining barcha ishtirokchilari riskni tahlil qilish uchun tizim haqida va unga bo‘ladigan hujumlar va tahdidlar haqida yetarlicha bilim va ko‘nikmalarga ega bo‘lishlari kerak, bu yerda tashqi axborot texnologiyalari va riskni minimalashtirish mutahassislari jalb qilinishi kerak. Hatarlar bilan bog‘liq fikrlarni turli xil usullar bilan ifodalanishi mumkin.

Masofaviy o‘qitish tizimi foydalanuvchilari yuqorida aytib o‘tilganidek, turli risk yoki tahdidlarga duch kelishadi. Ushbu risklarni minimallashtirish uchun quyidagi vositalar yoki usullar qo‘llanilishi mumkin.

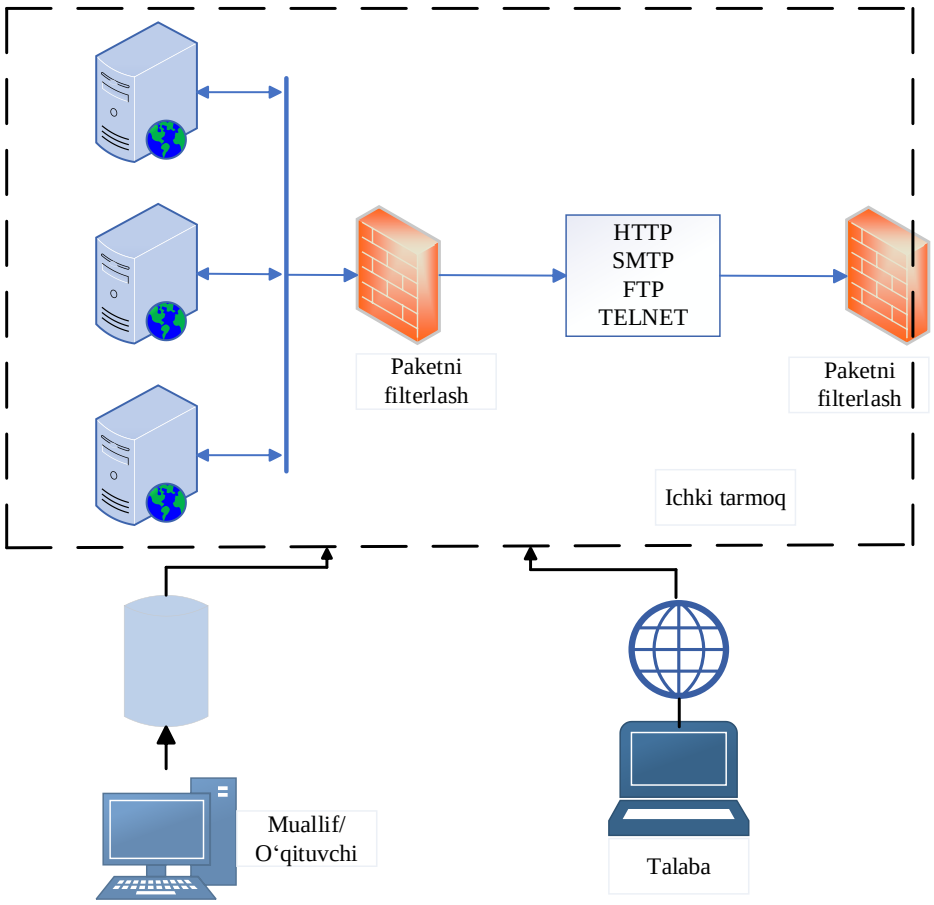
Tarmoqlararo ekran yordaminida foydalanishni boshqarish bu eng keng tarqalgan usul hisoblanadi.

Tarmoqlararo ekran - bu korporativ tarmoqqa tashkilotdan tashqaridan ruxsatsiz kirishni oldini olish uchun o‘rnatilgan apparat yoki dasturiy ta’minot riskni minimallashtirish tizimining kombinatsiyasi hisoblanadi. Texnik jihatdan tarmoqlararo ekran routerning maxsus versiyasidir. Asosiy marshrutlash funksiyalari va qoidalaridan tashqari, marshrutizatorni qo‘shimcha dasturiy ta’minot resurslari yordamida tarmoqlararo ekran funksiyasini bajarish uchun sozlashi mumkin.

Qoidaga asoslangan asosiy printsip shundan iboratki, ichkaridan tashqariga va aksincha barcha trafik tarmoqlararo ekran orqali o‘tishi kerak. Bunga erishish uchun avvalo mahalliy tarmoqqa barcha kirishlar jismonan bloklanishi va faqat tarmoqlararo ekran orqali kirishga ruxsat berilishi kerak. Faqat mahalliy riskni minimallashtirish siyosatiga ko‘ra ruxsat berilgan transport o‘tishi kerak. Tarmoqlararo ekranning o‘zi yetarlicha himoyani ta’minlashi kerak, shunda tizimga va unga qilinadigan hujumlar samarasiz bo‘ladi. Amaliy dasturlarda tarmoqlararo ekran odatda paketli filtrlar va dastur (yoki sxema) shlyuzlarining kombinatsiyasi hisoblanadi. Shunday himoya vositalaridan biri 1-rasmda ko‘rsatilgan. Shunday qilib, murakkab riskni minimallashtirish xavfsizlik devorlari kiruvchi trafikni bloklashi mumkin, ammo masofaviy tizim foydalanuvchilariga (talabalar, o‘qituvchilar va boshqalar bo‘lishi mumkin) tashqaridan erkin muloqot qilishlariga imkon beradi [2].

Masofaviy ta’lim tizimining aktivlari bilan bog‘liq risklarni kamaytirish uchun amalga oshirilishi kerak bo‘lgan asosiy strategiyalardan biri bu raqamli huquqlarni boshqarishdir (DRM - Digital Right Management). Ulashish mumkin bo‘lgan aktiv - bu statik HTML sahifasi yoki PDF hujjati yoki rasmlar va uslublar jadvali kabi fayllar to‘plami kabi oddiy manba. Boshqa tomondan, masofaviy ta’lim tizimining aktivi masofaviy ta’lim tizimining mazmuni (imtihon, eslatmalar va baho), kriptografik kalit tarkibi, foydalanuvchining shaxsiy ma’lumotlari, foydalanuvchilar o‘rtasidagi

xabarlar, turli guruhga a’zolik ma’lumotlari, tarmoq o‘tkazish qobiliyati, xabarning yaxlitligi va xabar sifatida belgilanishi mumkin. Ushbu munozarada mualliflar masofaviy ta’lim tizimining aktivini o‘quv resurslari, imtihon yoki baholash savollari, talabalar natijalari, foydalanuvchi profili, forum mazmuni, talabalarning topshiriqlari va masofaviy ta’lim tiziming tizimidagi e’lon kabi masofaviy ta’lim tiziming tizim tomonidan taqdim etiladigan xizmatlar sifatida belgilaydilar. Raqamli huquqlarni boshqarish tizimni mazmuni uchun risksizroq qiladi. Masofaviy ta’lim tiziming tizimi tarqatilgan tarmoqda yoki internetda ishlaydi, bu yerda kontent va xizmatlar yaratilgan, tarqatilgan, jamlangan, ajratilgan, saqlangan, topilgan va foydalanilganda o‘quvchi, o‘qituvchilar, kontent provayderlari, ma’murlar va boshqalar bilan bog‘liq bir nechta huquqlar o‘ynaydi. Shuning uchun raqamlashtirish zarur. Umumiy ma’noda, raqamli huquqlarni boshqarish litsenziya shartnomasi va mualliflik huquqini himoya qilish uchun ishlatilishi kerak yoki nusxa ko‘chirishni oldini oladi [3].



1-rasm. Masofaviy o‘qitish tizimida tarmoqlararo ekranni tashkil qilish

Shunday qilib, tarmoqlararo ekranni joriy qilish, sozlash, kuzatish va muammolarni bartaraf etish bo‘yicha bilim va ko‘nikmalarga ega bo‘lish barcha tizim ma’murlarining vazifasidir [3].

Maxfiylikning maqsadi ma’lumotlar va ma’lumotlarning ruxsatsiz shaxs yoki tashkilotga oshkor qilinmasligini ta’minlashdir. Shuningdek, o‘quvchilar kursning to‘g‘riligiga ishonishlari kerak. Bu boradagi usullardan biri kriptografiyadir. Internet orqali amalga oshiriladigan bog‘lanishlarda riskni kamaytirishni ta’minlash uchun turli kriptografik vositalar va usullar kerak. Kriptografiyada ikki xil algoritm mavjud.

Yopiq kalitli algoritmlarda shifrlash va shifrni ochish kaliti bir xil bo‘lib, u jo‘natuvchi va qabul qiluvchini ma’lumot almashishidan oldin kalitni kelishib olishlarini talab qiladi, bu algoritmning asosiy vazifasi ma’lumotlarni shifrlashdir. Bunday algoritmlarga misollar: Ma’lumotlarni shifrlash standarti (DES), Xalqaro ma’lumotlarni shifrlash algoritmlari (IDEA) va kengaytirilgan shifrlash standarti (AES). Shuning uchun faqat masofaviy o‘qitish tizimi kontentini shifrlash usullari uchun bu usullardan foydalanish mumkin.

Boshqa tomondan, ochiq kalitli kriptotizimlar xabarlar yoki ma’lumotlarni shifrlash uchun bitta kalitdan (ochiq kalit) va ushbu xabarlar yoki ma’lumotlarni shifrlash uchun ikkinchi kalitdan (maxfiy kalit) foydalanadi. Bu yerda asosan uchta matematik modeldan foydalaniladi - butun son faktorizatsiyasi, diskret logaritmlar va elliptik egri chiziq. Turli ochiq kalit algoritmlari RSA, El-Gamal, DiffieHellman yordamida amalga oshirishiriladi. Savollar to‘plamini yuborish va javob varaqalarini olish vaqtida ushbu usullardan foydalanish mumkin. Ishtirokchini autentifikatsiya qilish uchun ochiq kalit algoritmidan foydalangan holda quyidagi texnologiyalardan foydalanish mumkin [4]:

– Raqamli imzo;
– Raqamli sertifikat.

Bu elektron aloqada ma’lumotlar riskni minimallashtirishini ta’minlash uchun sun’iy neyron tarmoqlarga (Artificial Neural Networks - ANN) asoslangan yangi yondashuvlardan biridir. Bu yana bir bor kriptotizim bo‘lib, u tarmoq arxitekturasi, biologik operatsiyalar va o‘quv jarayonini o‘z ichiga olgan biologik g‘oyalarga asoslangan. Shunday qilib, himoyalangan kanalni yaratishning murakkabligi tarmoq hajmi bilan chiziqli. Ushbu biologik mexanizm doimiy ravishda o‘zgarib turadigan kalitlardan foydalangan holda samarali shifrlash tizimini yaratish uchun ishlatilishi mumkin. Masofaviy o‘qitish tizimlarida hujjatlarni uzatish paytida yuzaga kelishi mumkin bo‘lgan hujum kontekstida amalga oshirish juda oddiy va tezdir.

Elliptik egri chiziqli kriptografiya (Elliptic Curve Cryptography - ECC) ochiq kalitli kriptotizimlarning zamonaviy oilasi bo‘lib, u cheklangan maydonlar ustidagi elliptik egri chiziqlarning algebraik tuzilmalariga va Elliptik egri chiziqli diskret logarifm muammosi (ECDLP - Elliptic-Curve Discrete Logarithm Problem) qiyinligiga asoslangan [5].

ECC assimetrik kriptotizimlarning barcha asosiy imkoniyatlarini amalga oshiradi: shifrlash, raqamli imzolar va kalit almashinuvi.

ECC kriptografiyasi RSA kriptotizimining tabiiy zamonaviy vorisi hisoblanadi, chunki ECC bir xil darajadagi riskni kamaytirish uchun RSA ga qaraganda kichikroq kalitlar va raqamli imzolardan foydalanadi va juda tez kalit yaratish, tezkor kalit almashinuvi va tezkor imzolarni ta’minlaydi.

Parollar, smart-karta, raqamli imzo va raqamli sertifikat kabi autentifikatsiyaning barcha usullari mavjud, lekin talabalar o‘z parollarini sir saqlashiga kafolat yo‘q. Parol topshiriq topshirish, savol varaqalarini qabul qilish, kurs materiallarini yuklab olish va h.k.larda noto‘g‘ri ishlatilishi mumkin, bunda biometrik autentifikatsiyada riskni kamaytirishni yaxshi ta’minlaydi. Ammo bu biroz ko‘proq resurisni talab qiladi.

Ushbu uslub shaxsga yashirin mualliflik huquqiga oid eslatmalar, audio, video, tasvir signallarini qo‘shish imkonini beradi. Shunday qilib, Masofaviy o‘qitish tizimining multimediya ma’lumotlar bazasi serveri raqamli watermarking yordamida ruxsatsiz foydalanishdan himoyalangan bo‘lishi mumkin. Savol varaqlari, muhim o‘quv materiallari va boshqalar kabi tizim ma’lumotlari foydalanuvchiga ko‘rinmas bo‘lsa, buzib kirish ehtimoli nol yoki kamroq bo‘ladi.

Hech qanday tizim mutlaqo himoyalanmagan bo‘lsa-da, riskni minimallashtirish uchun boshqa turli usullarni qo‘llash orqali masofaviy o‘qitish tizimlarida riskni minimallashtirish darajasini yanada oshirishimiz mumkin. Foydalanuvchilar o‘rtasida matnli va matnli bo‘lmagan xabarlarning katta miqdori o‘tkazilishi kerakligi sababli, ECC boshqa kriptografiya usullariga qaraganda kuchliroq variant xisoblanadi [5]. RSA uchun talab qilinadigan mashhur kalit o‘lchami - 2048 bit, ECC esa bir xil riskni minimallashtirish uchun 224 bitni talab qiladi. Shuningdek, Masofaviy tizimlarda hujjatni elliptik egri chiziqli raqamli imzo algoritmi (Elliptic Curve Digital Signature Algorithm - ECDSA) yordamida uzatishda ham maxfiylik, ham autentifikatsiya saqlanishi mumkin. Axborot riskni minimallashtirish mutaxassis hodimlari va tizim ishlab chiquvchilar har doim server, marshrutizator va boshqalar kabi qo‘shimcha dasturiy va apparat vositalaridan foydalangan holda foydalanuvchilarga tizim ishonchli va kafolatlashgan xizmatlar ko‘rsatadi [6]. Kelajakda masofaviy o‘qitish tizimlarining yangi avlodi mobil-o‘qtish tizimi kontseptsiyasi ham jadal rivojlanishi kutilmoqda, va shu bilan parallel ravishda yangi risklar ham paydo bo‘ladi.

XULOSA

Masofaviy ta’lim tizimining turli ishtirokchilari tomonidan yuzaga kelishi mumkin bo‘lgan risklarni minimallashtirish uchun unga qarshi qo‘llash mumkin bo‘lgan apparat-dasturiy va kriptografik algotirmlar kabi vositalar yoki usullarini taklif qilindi. Masofaviy ta’limda faqat talaba o‘zining shaxsiy ma’lumotlarini ochishi mumkin bo‘lsada, o‘quv jarayonini sozlashda yuqori darajadagi maxfiylikni qanday amalga oshirish va saqlash bo‘yicha barcha qiyinchiliklar saqlanib qoladi.

ADABIYOTLAR RO‘YXATI

1. Axmedova N., Bekmirzaev O. Analysis of methods of fighting against network attacks of the “denial of service” category on information systems // central asian journal of education and computer sciences (CAJECS). – 2022. – T. 1. – №. 5. – C. 17-23.

2. Muminov B., Bekmirzaev O. Structure and algorithms of online discussion information system //Scientific Collection «InterConf». – 2022. – №. 114. – C. 373-384.

3. Nuralievich B. O., Boltaevich M. B. Method of Detection and Elimination of Tracks of Attacks in the Information System //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – C. 1-2.

4. Muminov B., Bekmirzaev O. Classification and analysis of network attacks in the category of “denial of service” information system //central asian journal of education and computer sciences (CAJECS). – 2022. – T. 1. – №. 1. – C. 7-15.

5. Karforma Sunil and Ghosh Basudeb,: On Security issues in e-learning System, “Proceedings” of COCOSY-09, University Institute of Technology, Burdwan University, Jan 02-04.2009.

6. Мўминов Б., Бекмирзаев О. Построение узлов о событиях под влиянием атаки в информационной системе //Scientific Collection «InterConf». – 2022. – №. 114. – C. 388-396.