

GLOBAL AXBOROTLASHUV SHAROITIDA BULUTLI
TEXNOLOGIYALAR MUHITIGA O'QUVCHILARNI
MOSLASHTIRISH OMILLARI VA YO'LLARI

Haydarova Safiya
Qo'qon DPI dotsenti

Nurmatov Sardor Siddiqovich
Qo'qon DPI magistranti

Annotatsiya

Ushbu maqolada global axborotlashuv sharoitida bulutli texnologiyalar muhitiga o'quvchilarni moslashtirish omillari va yo'llari haqida bayon qilingan.

Tayanch so'z va iboralar: global axborotlashuv, bulutli texnologiyalar, o'qitish metodi, masofaviy o'qitish, IP, Smart Boards, interaktiv display, virtual stendlar. Oliy o'quv yurtlarining ko'pgina o'qituvchilari (pedagogika va didaktika o'qituvchilaridan tashqari) "o'qitish metodi" tushunchasiga unchalik qiziqmaydilar. Chunki ko'pchilik o'qituvchilar o'qitish faoliyatini empirik tarzda o'rganib oladilar. Ular asosan kafedra mudirilari yoki yetakchi professor – o'qituvchilariga taqlidan o'qitish usullarini qo'llaydilar. Lekin shu usullar qaysi ta'lim metodlari tizimiga kirishini bilmaydilar yoki qiziqmaydilar. Ta'lim metodini bilish ta'limni takomillashtirishning muhim shartlaridan biridir. Ta'lim metodi har hil o'quv predmetlarini o'qitishni qanday amalga oshirish yo'larini belgilaydi. Ta'lim metodi o'qituvchi va o'quvchi faoliyati to'g'risida nazariy tushuncha beruvchi didaktik kategoriyadir. Masofadan o'qitish har hil ta'lim metodlari orqali amalga oshiriladi va unda bir qancha usullardan foydalaniladi. Har bir usul muayyan harakatlardan iborat bo'lib, o'qitishning hal hil didaktik vositalari yordamida ma'lum bir maqsadga erishishga qaratiladi. Masofadan o'qitish metodlaridan foydalanganda qo'ydagi usullarni qo'llash mumkin: namoyish qilish, illyustratsiya, tushintirish, hikoya, suhbat, mashq, masala yechish, material ni yodlash, yozma ish va takrorlash kabilar.

Pedagogik jihatdan qayta ishlangan o'quv mazmuni o'z ichiga olgan masofaviy o'qitish o'qituvchi va o'quvchi qo'lidagi o'quv vositalari o'quv mazmunini taqdim etish, o'quvchilarning o'rganish faoliyatini tekshirish va boshqarish vazifasini bajaradi. Ma'lum bir o'quv materiali bir qancha o'rgatish vositalari (bosma materiallar, audio-video va boshqalari) bilan berilishi mumkin. Vositalarning har biri o'z didaktik imkoniyatlarga ega. O'qituvchi bu

imkoniyatlarni bilishi va o'quv materialini har hil vositalarga ko'ra bo'lib chiqishi, didaktik vazifalarni amalga oshirishga qaratilgan o'quv axborotlarni tashuvchi tizim sifatida o'quv materiallaridan o'quv vositalari kompleksini yarata olishi kerak. Masofaviy o'qitish tizimi vositalari qo'ydagilardan iborat bo'lishi mumkin:

- 1.Darsliklar(an'anaviydarsliklar,elektrondarsliklar,qo'llanmalar, spravochniklar va boshqalar).
- 2.(Kompyuter) tarmoqdagi o'quv-metodik qo'llanmalar;
- 3.Odatdagi va multimediya variantlaridagi kompyuterli o'qituv tizimlari;
- 4.Audio va o'quv axborot materiallari;
- 5.Video o'quv-axborot materiallari;
- 6.Masofaviy laboratoriya praktikumlari;
- 7.Masofaviy trenajyorlar;
- 8.Masofaviy axborot va bilimlar bazasi;
- 9.Masofaviy elektron kutubxonalar;
- 10.O'rgatuvchi ekspert tizimlariga asoslangan o'qitish vositalari;
- 11.Geoaxborotli tizimlarga asoslangan o'qitish vositalari;
- 12.Virtual reallikka asoslangan o'qitish vositalari.

Ma'lumotlarga ishlov berish markazi resurslaridan foydalanishda apparat va dasturiy ta'minotlarni ahamiyati. Apparat vositalarda to'xtalishlarning asosiy tasdiqi sifatida korporativ tarmoqlarda maxfiy axborotlarni qayta ishlashi yaxshi rivojlangan xisoblanadi. apparat vositalaridan foydalanishdagi afzalliklar, sifatiga kafolati, ish jaroyonida ishonchli va bardoshiligi uchun ajralib turadi. Apparat komponentalarini ishlab chiqaruvchi kompaniyalar ularni kafolatiga javob beradilar. Shuningdek ma'lumotlarga ishlov berish markazidagi apparat qismini noqonuniy foydalana olishdan tashkiliy va texnik muhofaza qilib uning bartaraf etadi. Chunki shunday xolatlar yuzaga kelib chiqadiki, xakker axborot xavfsizligi rejimini buzadi.

Shuning uchun yondosh signallarni va elektromagnit tasirlarni aniqlashda doyimiy monitoring olib boriladi. Bunday holatlarda aniq metodlar bilan signallar tadqiqoti va tashqi ta'sirdan himoya olib boriladi. Bunday harakatlardan foydalanish asosan analog xolatlarda, bulutli hisoblash tizimlarida ijtimoiy kirish orqali bajariladi.

Ishlash prinsipi ikkita asosiy metodlarga qaratilgan: IP - paketlarni apparat va dasturiy ta'minotlar yordamida shifrlash, yoki odiygina ochiq trafik orqali. Deyarli har doim kompaniyalar korporativ tarmoqlarida ishlov berilgan shaxsiy konfidensial ma'lumotlar IP - tarmoq orqali kirish imkoniyati mavjud bo'lishligi

uchun saqlanadi. Barcha paketlarni kodirovka qilish tizimda resurslarni ko'p qismi sariflanishiga sabab bo'ladi. Shifrlash pog'onasini pasayishi ochiq trafiklarni ko'payishiga sabab bo'ladi va bu konfidential axborotlar himoya pog'onasi susayishiga olib keladi. Inson faoliyati soxalarida bunday holat nomaqbul xisoblanadi. Bunung yechimi IP - shifrlash tezligini oshirish orqali xal etsa bo'ladi.

Iste'molchilarning apparat va dasturiy ta'minot bilan ta'minlash.

Hozirgi kunlarga kelib, is'temolchi ish joyida IP - oqimlarni SSL protokoli orqali shifrlash dasturiy va apparat vositalari yondashishda xech qanday muomolarni keltirib chiqarmaydi. Tezlik qayta ishlashsiz 1 Mbit/t ga chiqishi mumkin. Hozirgi kunlarda bunday xizmatlar ko'rsatadigan sertifikatlashgan firmalar yetarlicha xisoblanadi. Iste'molchilar operatsion tizimlaridagi kalitlar va korporativ bulutdagi shaxsiy axborotlar himoyasi axborot xavfsizligini taminlashda katta muomolardan biri xisoblanadi. Is'temolchining shaxsiy kompyuterlarda elektron quluf o'rnatiladi. Bunday blakirovkani nafaqat is'temolchi balki, kompaniya axborot xavfsizligi xizmati ham nazorat qilish imkoniyatiga ega. Lekin bularning hammasi faqat shaxsiy bulutda mavjud bo'lib ijtimoiy bulutda bu imkoniyatlar yo'q (1-rasm).



1- rasm. Iste'molchilarning apparat va dasturiy ta'minot bilan ta'minlash
Gipervizor, dasturiy vosita sifatida apparat resurslarini boshqarishda va resurslarni mexmon operatsion tizimlar o'rtasida taqsimlaydi, shuning uchun virtual muxitda eng zaif qismi xisoblanadi. uning har qanday buzilgan xolati, mexmon operatsion tizimida nosozlikni yuzaga kelib chiqaradi. Gipervizordan foydalana olish o'z o'rnida yovuz niyatdagi shaxslarga turli xil imkoniyatlar kelib chiqaradi. Fakt jixatdan bunday kirish imkoniyati gipervizor orqali o'tadigan barcha axborot oqimlarini nazorat qilishga imkoniyat beradi. Bunday

imkoniyatlar virtual muxitdan umumfoydalanish xuquqini beradi yani: virtual struktura admistratori cheklovsiz har qanday ma'lumotlardan foydalana olish xuquqiga ega bo'ladi.

Shuning uchun axborot resurslari xavfsizligini virtual muhit ichida xal etish mumkin. Mantiqiy virtual infratuzilma fizik infratuzilmadan farq qilmaydi shunga ko'ra birinchidagi taxdidlar ikkinchiga ham taluqli xisoblanadi. Shunda axborot himoya vositalari virtual infratuzilma himoyasini taminlashda, apparat resurslarini opimizatsiyalash qobilyatiga ega bolishlari lozim. Ko'p hajmga ega bo'lgan virtual infratuzilmalarda ratsioanal maqsadda axborot himoya vositaladidan foydalanish gipervizor darajasida qurishga yordam beradi. Bulutda asosiy xavf extimolligi virtualizatsiya spesifikatsiyasi, yangi obektlar yuzaga kelishi orqali - bulutli

boshqarish tizimi va tizim virtualizatsiyasi orqali yuzaga keladi. Ulardan birini kompromentatsiya qilish bulut xavfsizlikni xavfga qo'yish bilan tengdir. Virtual muxitdagi fizik serverlarda virtual mashinalar juda ko'p bo'lishi mumkin. Virtualizatsiyalashgan server operatsion tizimiga oddiy antivirus o'rnatilsa, bitta fizik gipervizorda r antivirusni 100 ta nusxasi yuzaga keladi. Har bir nusxa o'zida antivirus signaturasi, yuritgich bo'ladi: bularning hammasini o'z vaqtida yangilab turish kerak barcha virtual mashinalarda. Bunda gipervizorga yana yangi qo'shimcha og'irlik kelib chiqadi va fizik server resurslari samarasiz sarflana boshlaydi.

Misol qilib, oladigan bo'lsak, virtualizatsiya xavfsizligini taminashda, virusga, xujum va taxdidlarga qarshi gipervizor darajasidagi vositalar ishlatilindi. Shunday xavfsizlik yondashuvlar tarmoq pog'onasida ham qo'llaniladi. Tarmoqlar aro ekran, xujumni payqash va xatarlani aniqlash, hujumlardan himoyalasinish - bunday ananaviy masalalardan foydalanishda tarmoq chegarasiga o'rnatilgan apparat ta'minoti orqali amalga oshiriladi. Virtualizatsiya tizimiga xizmat ko'rsatishda, agar admistratoirlarga tegishli virtual mashinalar orasidagi trafik xavfsizligini ta'minlash kerak bo'lgan xollarda ikki xil yechim imkoniyati bor.

Birinchi yechim shunga asoslanadiki, standart apparat ta'minotini olganda, virtualizatsiya muhitida n o'ziga tegishli trafikni ajratib olishi va uni shu qurilma orqali otkazish va orqaga qaytish xolatida uni o'rab qo'ymoq. Buning uchun xatto standart yechim trafikni filtrizatsiya qilishdan foydalanish mumkin. Lekin bunday yondashish kamsamarali xisoblanadi.

Boshqa yo'li ya'ni ikkinchi yo'li masalalarni (yechimlarni) gipervizor darajasida joylashtirish mumkin.

Foydalanilgan adabiyotlar

1. Amirov D.M, Atajonov A.Y, Ibragimov D.A., Raximjonov Z.Y., Saidxo‘jayev S.S. «Axborot – Kommunikatsiya texnologiyalari izohli lug‘ati» BMTTD ning O‘zbekistondagi vakolotxonasi, 2010.- b.320.
2. Aripov M., M.Fayziyeva, S.Dottayev. Web texnologiyalar. O‘quv qo‘llanma. T.; “Faylasuflar jamiyati”. 2013
3. Azimjanova M.T., Muradova, M. Pazilova. Informatika va axborot texnologiyalari. O‘quv qo‘llanma. Toshkent, “O‘zbekiston faylasuflari milliy jamiyati”, 2013 y.
4. Shirinov, F., & Mamasoliyev, A. (2021, March). AN INTELLIGENT COMPUTER NETWORK-BASED LEARNING PROCESS MANAGEMENT SYSTEM. In Euro-Asia Conferences (Vol. 3, No. 1, pp. 55-57).
5. Ikromovich, H. X., Meliqo'ziyevich, S. I., Mo'ydinovich, I. R., & Shuxratovich, S. F. (2022). Mathematical model of checking the behavior of an industrial robot in the structure of a technological module for stagnation. International Journal of Early Childhood Special Education, 14(7).
6. Shuxratovich, Shirinov Feruzjon. "Technology for Working with Graphic Programs." Open Access Repository 9.12 (2022): 99-102.
7. Shuxratovich, Shirinov Feruzjon, and Botirov Muzaffarjon Mansurovich. "PROBLEMS WORKING WITH COMPUTER GRAPHICS APPLICATIONS IN THE LEARNING PROCESS." Open Access Repository 8.1 (2022): 92-95.