O’ZBEKSITON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

H i m o y a g a
kafedra mudiri
Irgasheva D.Ya._____
«___»_____2015 y.

BAKALAVR BITIRUV MALAKAVIY ISHI

Mavzu: «Bulutli texnologiyalarida axborot taxdidlari va ularga qarshi kurashish metodlarining qiyosiy tahlili»

Bitiruvchi	_____ (imzo)	Boxodirov A.B.
Rahbar	_____ (imzo)	G’ofurov SH..
Taqrizchi	_____ (imzo)	Muqimov J.D. (f.i.sh)
HFX maslahatchisi	_____ (imzo)	Qodirov F.M. (f.i.sh)

Toshkent – 2015

Krish

Axborot texnologiyalar jadal rivojlanayotgan davrda dasturiy taminotni o’rni juda xam katta axamiyatga ega. Dastur to’la qonligicha ishlashi uchun shaxsiy kompyuter minimal tizim talabiga jovob berishi kerak. Internet modernizatsiyalashtirldi va server uskunalar ishlab chiqildi. Shu bilan birga shunday g’oya yuzaga keldki, dasturdan foydalanishda xisoblash tizimlarini birlashtirish va undan yagona manba sifatida foydalanish. 2008 yildan boshlab (Cloud technology) Bulutli texnologiyar so’zi dunyo miqiyosida keng tarqaldi.

Birinchi qarashda «Bulutli texnologiyalar» tushunarsiz ko’rinsada: bu model o’zida biror bir tizmdagi (serverlar, ilovalar, saqlash tizmlari va xizmatlar) dan tez, qulay, samarali foydalanish imkonini beradi. Ortiqcha urinishlarsiz, tez va aniq taqdim etiladi faqatgina provaydir orqali tarmoqga ulanganda.

Bulutli texnologiyalardan foydalanishdagi avzaliklar. Bulut ichida saqlanayotgan malumotlardan xar kim foydalanish mumkin bunga faqatgina, kompyuter, planshet, mobil telefon internet tarmog’iga ulangan bo’lishi kerak.

Bulutli texnologiyalardan foydalanish ATda bir qancha ustunliklarni yaratib beradi.

- Tashkilot boshqaruvida xisoblash resurslarini yanada samarali ishlatish mumkin.
- AT infratuzulmani boshqarishni takomillashtirish.(shu jumladan geografik jihatdan)
- Ish boshqaruvida doimiy soddalashtirish va qulaylashtirish, tizim konsepsiyasni zaxira tarizda saqlash va virtual mashinani migratsiyalash.
- AT infratuzilmani chiqimni kamaytirish, xisoblash resurslari, elektr quvatlarini tejash.

O’zbekiston Respublikasida axborot xavfsizligini taminlash va uni muxofaza etish maqsadida, axborot erkinligi printsiplari va kafolatlari to’g’risida qonun ishlab chiqildi: (Toshkent sh, 2002 yil 12 dekabr,439-II-son)…”[1]

1 modda. Ushbu Qonunning asosiy vazifalari axborot erkinligi printsiplari va kafolatlariga rioya etilishini, har kimning axborotni erkin va moneyliksiz

izlash, olish, tekshirish, tarqatish, foydalanish va saqlash huquqlari ro’yobga chiqarilishini, shuningdek axborotning muhofaza qilinishini hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta'minlashdan iborat.

12-modda. Axborot xavfsizligini ta'minlash sohasidagi davlat siyosati axborot sohasidagi ijtimoiy munosabatlarni tartibga solishga qaratilgan bo'ladi hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta'minlash sohasida davlat hokimiyati va boshqaruv organlarining asosiy vazifalari hamda faoliyat yo'nalishlarini, shuningdek fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining, fuqarolarning o'rni va ahamiyatini belgilaydi.

15-modda. Davlatning axborot borasidagi xavfsizligi quyidagi yo’llar bilan ta'minlanadi: axborot sohasidagi xavfsizlikka tahdidlarga qarshi harakatlar yuzasidan iqtisodiy, siyosiy, tashkiliy va boshqa tusdagi chora-tadbirlarni amalga oshirish; davlat sirlarini saqlash va davlat axborot resurslarini ulardan ruxsatsiz tarzda foydalanilishidan muhofaza qilish; O'zbekiston Respublikasining jahon axborot makoniga va zamonaviy telekommunikatsiyalar tizimlariga integratsiyalashuvi; O'zbekiston Respublikasining konstitutsiyaviy tuzumini zo'rlik bilan o'zgartirishga, hududiy yaxlitligini, suverenitetini buzishga, hokimiyatni bosib olishga yoki qonuniy ravishda saylab qo'yilgan yoxud tayinlangan hokimiyat vakillarini hokimiyatdan chetlatishga va davlat tuzumiga qarshi boshqacha tajovuz qilishga ochiqdan-ochiq da’vat etishni o'z ichiga olgan axborot tarqatilishidan himoya qilish; urushni va zo’ravonlikni, shafqatsizlikni targ’ib qilishni, ijtimoiy, milliy, irqiy va diniy adovat uyg’otishga qaratilgan terrorizm va diniy ekstremizm g’oyalarini yoyishni o'z ichiga olgan axborot tarqatilishiga qarshi harakatlar qilish.

Ishning maqsadi: Bulutli texnologiyalarda axborot tahdidlari va kurashish metodlarini qiyosiy taxlilidan iborat.

Bitiruv malakaviy ishning umumiy strukturasi quydagi bo’limlardan tashkil topgan.

Birinchi bo’lim quydagilarni o’z ichiga oladi.

- Bulut haqida umumiy tushuncha: bulutli texnologiyalar, bulutli xisoblash, virtualizatsiya, servis va taqdimlash modellari, bulutli texnologiyalarni avzalliklari va kamchiliklari.

Ikkinchi bo’lim.

- Bulutli texnologiyalarda amalga oshiriladigan xujumlar ularni bartaraf etish, axborot ximoyasi, apparat va dasturiy taminotlarning qo’llash imkoniyatlari va tahdidlarga qarshi kurashish metodlarining qiyosiy tahlili.

Uchinchi bo’limda.

- Mehnat muhofazasining huquqiy masalalari davlatimizning asosiy Qonuni O’zbekiston Respublikasi Konstitusiyasi bilan tartibga solish, elektromagnit nurlanishlarning inson organizmiga ta’siri va ekologik inqirozni bartaraf qilish

1.Nazariy qism. Bulutli texnologiyalarida evalutsiya jarayoni va modellari

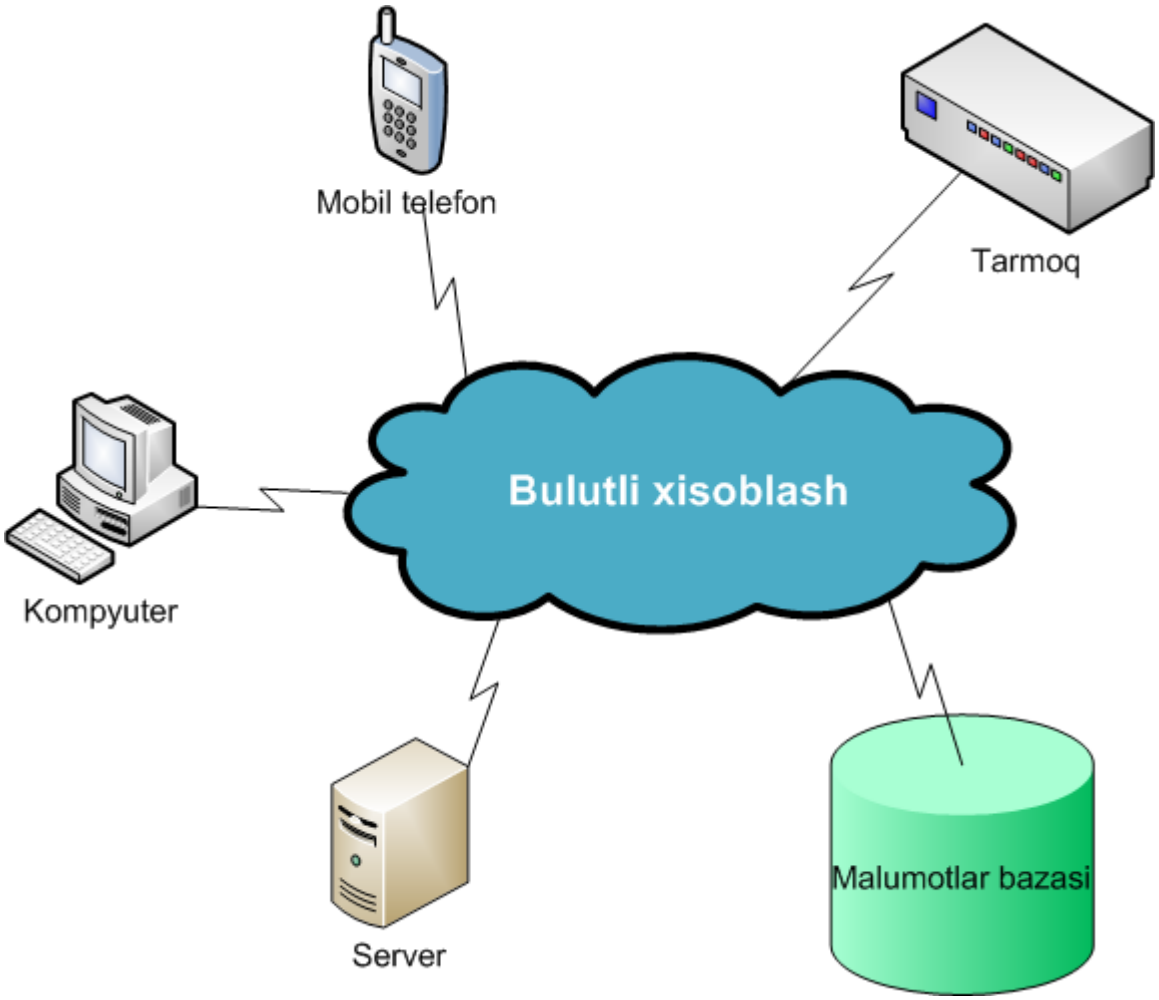
1.1. Bulutli texnologiyalarni yuzaga kelish jarayoni

Bulutli texnologiyalar – bu model istemolchiga ATni servis sifatida internet orqali namoyon qiladi. Bulutli xisoblashlarning yuzaga kelishida «virtualizatsiya» texnologiyalarining axamiyati juda katta hisoblanadi. Birinchi bo'lib 1960 yilda virtualizatsiya texnologiyalari IBM taklif qilingan ammo qimmat meynfreym kompyuter texnologiyalarini arzon x86 protsesorli kompyuter serverlariga o'tgandan so'ng virtualizatsiya termini ancha vaqtgacha esdan chiqarildi. 2000 yildan boshlanib holat o'zgara boshladi, shu yillarga qadar WMware x86 razryadli virtualizatsiyada monopoliyani qo'lga kiritdi. 2005 yilda WMware kompaniyasi virtual mashinalarni DTdan foydalangan xolda bepul tadbiq qildi. 2006 yilda Microsoft kompaniyasi «Microsoft virtual PC» Windows versiyasini ishga tushirild…"[2] 2006 yilda Amazon kompaniyasi o'z qurilmalarida virtual serverlarni kengaytirish orqali «Amazon Elastic Compute Cloud» yuzaga keldi buning yana asosiy sabablaridan biri virtual serverlarni boshqa qurilmalarga (istemolchilarga) ijaraga berish orqali bulutli texnologiyalarni kelib chiqishiga turtki bo'ldi.

Bulut – AT- infratuzilma tashkilotlarining innavatsion modeli (konsepsiya) xisoblanib, u aloxida ajratilgan va taqsimlangan konfiguratsiyalangan apparat va tarmoq resurslaridan, dasturiy taminotdan tashkil topgan va ular masofadagi provayderlarni malumotlar markazida yotadi.

1.2. Bulutli xisoblash

Model yagona puldagi tarmoqdan qulay va bir vaqtning o'zida konfiguratsiyalangan xisoblash resurslaridan birgalikda foydalanish imkoniyatini yaratadi (misol uchun, tarmoqlar, serverlar, malumotlar bazasi, ilovalar va servislar) shu bilan birga minimal boshqarishda xam oparativ va erkin ishlash imkoniyatini taqdim etadi. Bulutning bu modeli 5 ta asosiy xarakteristika, 3 ta servis model va 4 ta taqdimlash modellaridan iborat.



1.1-rasm. *Bulutli xisoblash*

1.2.1. Asosiy model tavsiflari

Ularni, boshqa turdagi hisoblashlardan farqlash (Internet resurslaridan).

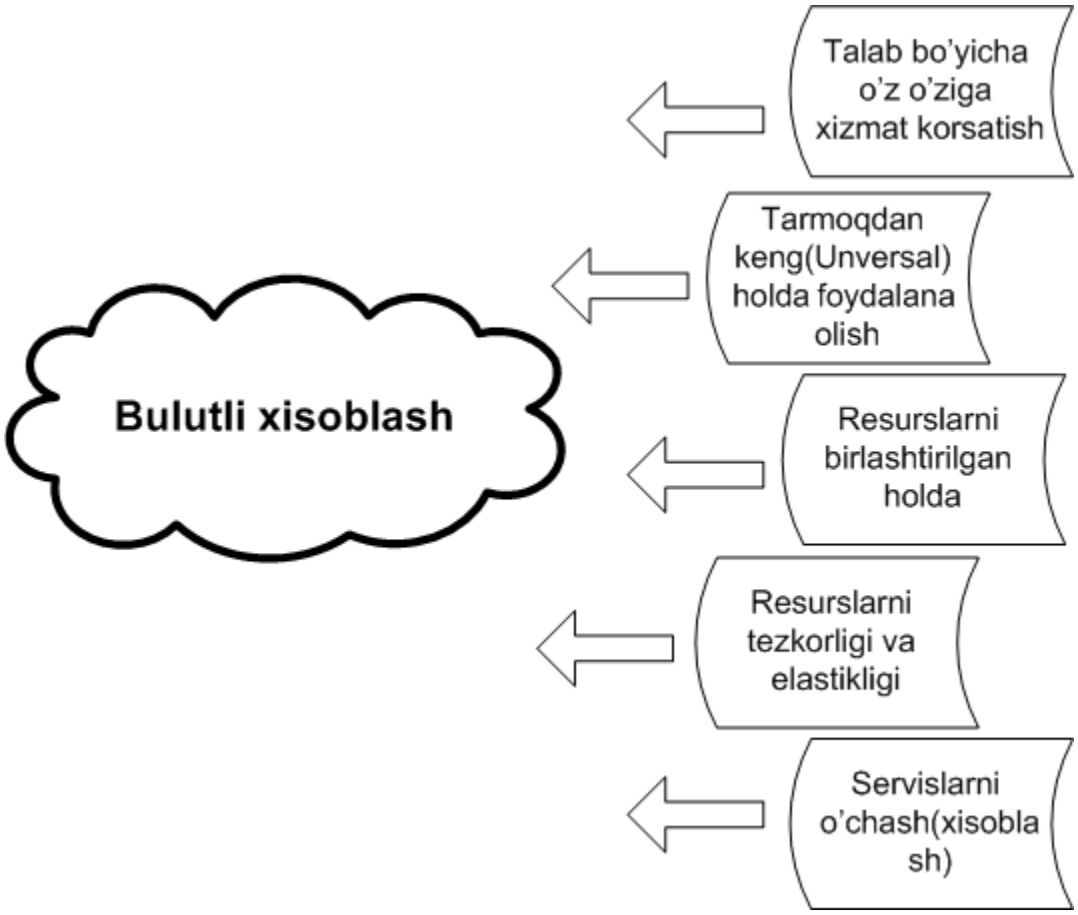
1.Talab bo'yicha o'z o'ziga xizmat ko'rsatish. Foydalanuvchi server vaqtini, malumotlar saqlash ombori xajmini, zarur bo'lganda avtomatik tarizda, xizmat ko'rsatayotgan provayder bilan o'zaro bog'liq bo'lmagan xolda, xisoblash kuchini mustaqil tarizda aniqlash va o'zgartirish mumkin.

2.Tarmoqdan keng holda foydalana olish. Hisoblash kuchi imkoniyatlari tarmoqda standart mexanizimlar orqali katta masofada foydalana olish mumkin. Xar - hil turdagi (yupqa - qalin) mijoz platformasidan (terminal qurilmalar) keng qamrovda foydalanish imkonini beradi.

Resurslarni birlashtirish. Konfiguratsiyalangan provayder xisoblash resurslarini yagona xovuzga birlashtirish orqali ko'p sonli foydalanuvchilar resurslardan birgalikda foydalanish imkoniyatiga ega bo'ladilar.

Resurslarni tezkor elastikligi. Foydalanuvchilarning talabiga qarab bulut xizmatlari kengayishi, tez taqdim etilishi, qisqartirilishi mumkin.

O'lchangan servis. (aslida foydalanilgan bugalteriya istemol servisi va to'lov xizmatlarini imkoniyatlari.) …"[2] Bulutli tizimlar servis turiga qarab abstraksiyaning bazi bir darajalarida o'lchashni amalga oshirish orqali resurslardan foydalanishni optimallashtiradi va ular ustidan avtomatik nazorat qiladi.



1.2- rasm. *Asosiy xarakteristik modellar*

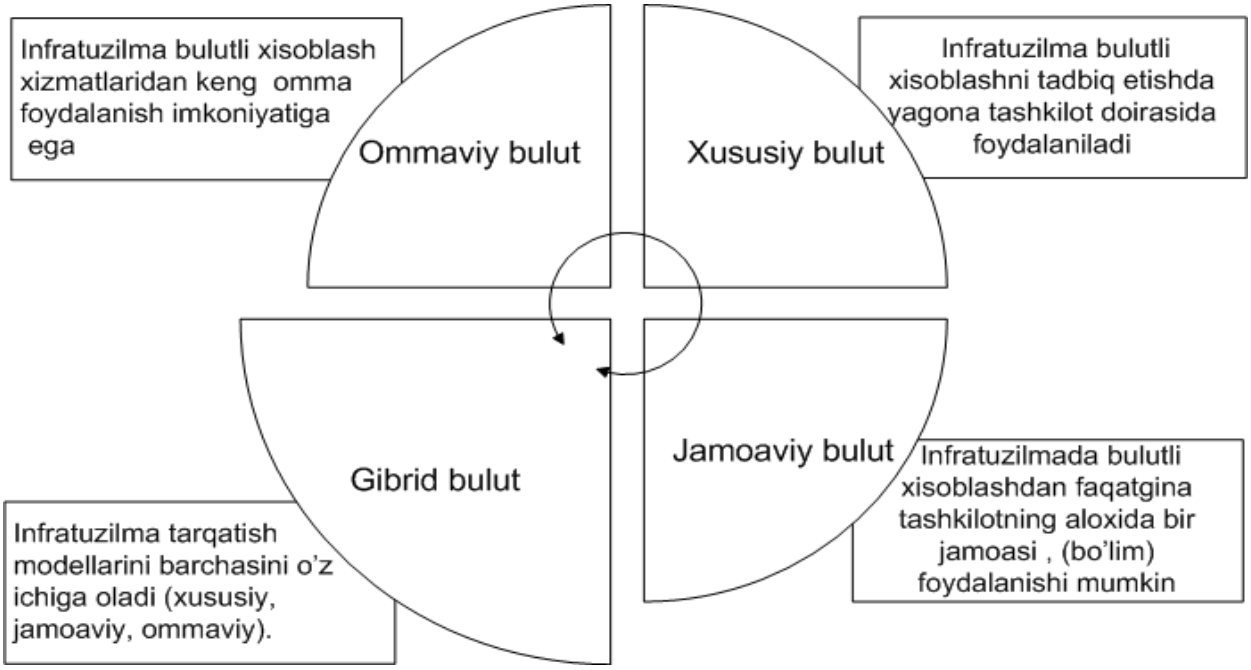
1.2.2. Tarqatish modellari

Private cloud *(xususiy bulut)* – bu infratuzilma bulutli xisoblashni tadbiq etishda yagona tashkilot doirasida foydalaniladi.

Community cloud(jamoaviy bulut) – bu infratuzilmada bulutli xisoblashdan faqatgina tashkilotning aloxida bir jamoasi , (bo'lim) foydalanishi mumkin.

Public cloud (ommaviy bulut) - bu infratuzilma bulutli xisoblash xizmatlaridan keng omma foydalanish imkoniyatiga ega.

Hybrid cloud (gibrid bulut) – bu infratuzilma tarqatish modellarini barchasini o’z ichiga oladi (xususiy, jamoaviy, ommaviy).



1.3-rasm. *Taqdimlash modellari*.

1.2.3.Servis modellari va asosiy yetkazib beruvchi provayderlar

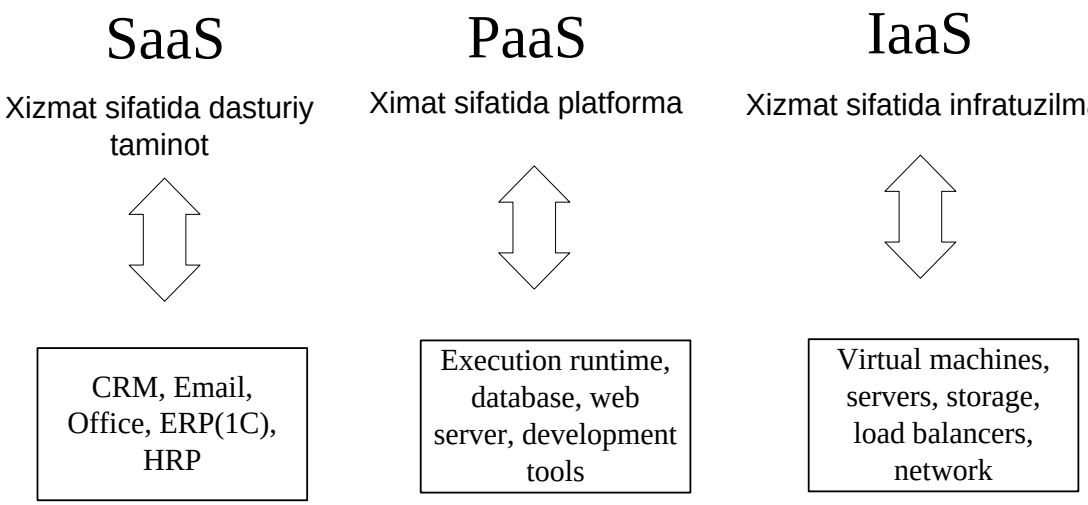
Software as a Service (**SaaS**) – xizmat sifatida dasturiy taminot. Istemolchi ushbu modeldan provayder tomonidan bulutli infratuzilmasida ishga tushurilgan ilovadan foydalanadi. Interfeys (veb-brovzer) yoki dastur interfeysi orqali mijoz foydalana olishi mumkin…”[2] Istemolchi bulutli infratuzilma asosini boshqarish va nazorat qilish xuquqiga ega, shu jumladan: tarmoqni, serverni, operatsion tizimni, malumotlar bazasini xatto ilovalar parameterlarini o’zgartirish imkoniyati berilmagan.

Platform as a Service (**PaaS**) – xizmat sifatida platforma. Bulutli xisoblash istemolchiga dasturiy platformadan foydalanish uchun ruhsat berilgan model xisoblanadi, bunda quydagi imkoniyatlardan foydala oladi: operatsion tizim, malumotlar bazasi, prikladnoy DT, ishlab chiqish vositalari va DT sinovi. Istemolchi uchun, kompyuter platformasiga o’rnatilgan operatsion tizim, web – ilovalarni ishlab chiqish, tarqatish va boshqarish uchun maxsus vositalar ijaraga beriladi. Istemolchi bulut infratuzilma asosini boshqarish xuquqiga ega emas, shu jumladan: tarmoq, serverlar, operatsion tizimlar yoki malumotlar bazasini xam

lekin tarqatilgan ilovalar va ish olib borayotgan muhit konfiguratsiya parametlarni sozlash imkoniyati mavjud.

Infrastructure as a Service (**IaaS**) – xizmat sifatida infrastruktura. Istemolchi ushbu bulutli xisoblash modelida ishlov berish vositalarini boshqarish va saqlash, fundamental hisoblash resurslari (virtual serverlar va tarmoq infrastrukturalar) nazorat qilish xuquqiga ega. Bunda istemolchi o'zining xoxishiga ko'ra operatsion tizimlar va dasturlarni mustaqil tarizda o'rnatish mumkin. Shunda istemolchi abstrak xisoblash kuchi(server vaqti, disk maydoni va tarmoq kanallarni o'tkazish qobilyati) yoki autsorsing IT- infrastrukturalardan foydalanish mumkin. Istemolchi bulut infrasutrukturasini asosini boshqarmaydi, lekin operatsion tizim , saqlanayotgan va tarqalgan ilovalarni boshqarish imkoniyatiga ega.

Bulutli malumotlar markazi yoki malumotlarga ishlov berish markazida (ЦОД) quydagilar joylashtirilgan bo'ladi : fizik uzkunalar yoki hardware (serverlar, malumotlar saqlash bazasi, ish stansiyalar), tizimli dasturiy taminot (ОС, virtualizatsiya vositasi, avtomatizatsiya) instrumental va prikladnoy DT, uskunalarni boshqarish tizimi (Equipment management systems), tarmoq infratuzilmasi (Network infrastructure): marshutizator va kommutatorlar (routers and switches) fizik uskunalarni ulash va birlashtirish uchun. Shu jumladan tizim muxandisi taminoti malumotlar markazi ishini normal taminlaydi (Systems of engineering support).



1.4-rasm *Servis modellari*

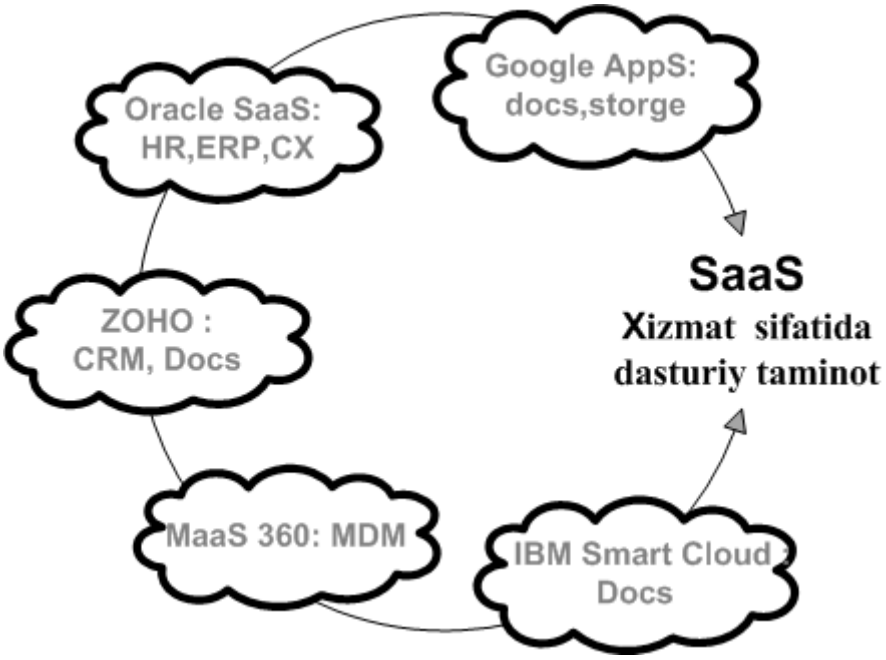
SaaS sxemasi bo'yicha xar xil turdagi bulut ilovalari xizmat ko'rsatadi. Business Apps, Office Web Apps, Management Apps, Communications, Security va boshqalar. SaaS AQSh da keng tarqalgan xisoblanadi. eng ko'p tarqalgan bulutli ilovalarga quydagilar kiradi: CRM (mijozlar o'rtasidagi o'zaro munosabatlarni boshqarish tizimi) , HRM (kadrlar va hodimlar bilan ishlash tizimi), ERP (resurslar va tashkillashtirish tizimi, misol uchun 1C), offis ilovalari, kommunikatsiya manbai va boshqalar. Dunyo miqiyosida Salesforce.com kompaniyasi CRM bulutli ilovalarni tarqatishda yetakchi hisoblanadi. Kommunikatsiya vositalaridan biri elektron ro'yhat (misol uchun , Gmail), avdio va video chatlar (misol uchun, Microsoft Lync Online), bulut servisi (Mobile Device Manegement – mobil qurilmani boshqarish). Bulutli servisda MDM mobil qurilmasi orqali korparativ tizimlar bilan ishlash uchun mo'ljallangan.

MDM bulutli tizimi boshqaruvida ishlaydigan xar – hil turdagi mobil qurilmalarga ilovalar yani agentlar o'rnatiladi. Bu ilovalar o'z o'rnida markazlashgan mobil qurilmalarni sozlashda bulut xizmatidagi SaaS korparativ tarmog'iga kirish imkoniyatini beradi. Bulut kommunikatsion vositalari boshqa SaaS bulutli xizmati orqali integratsiya qilinadi, misol uchun, CRM+MDM, Office Web Apps+Lync Online, Google Docs, Gmail, Hangouts va boshqalar. Saas ning asosiy istemolchilari kichik va o'rta biznes tashkilotlari xisoblanadi. Ko'pgina SaaS – ilovalar xodimlarni xamkorlikda faoliyat yurutishi va qo'llab quvatlashi uchun tadbiq etilib, ularni umum masalalarni birgalikda yechimini topishga undaydi. SaaS – ilova arxetekturasi yagona nusxali ilovalarni serverda ishga tushiriladi, koplab istemolchlarga multijara (Multi - tenant) sifatida xizmat qiladi…"[3] Xar bir bajarilayotgan ish jarayonida istemolchiga o'z virtual nusxa ilovasi taqdim etiladi.

Asosiy SaaS Solution/Vendor:

Salesforcel Sales Cloud/Salesforce (CRM), Oracle Cloud Applications/Oracle (HR, ERP, CX, EMP, SCP, Business Intelligence), Google Apps/Google – bulutli xizmat offis paketi (Google Docs, Google Drive, Google Sites, communication: Hangouts, gmail, Google Calendar va boshqalari), IBM

SmartCloud Docs/IBM, Microsoft Dynamics CRM, Microsoft OneDrive (Office Online), Office365/Microsoft (Office Web Apps, Lync Online, Exchange Online, SharePoint Online), ZohoDocs/Zoho (onlayn offis paketi), Zoho Reports/Zoho (Business Intelligence), Zoho CMR/Zoho CRM/Zoho, Informatica Cloud MDM/Informatica, MaaS360/Fiberlink, Cloud PBX from Vonage Business Solutions.



1.5- rasm. *Bulutli xisoblashda asosiy SaaS provayderlar*.

Bulutli xisoblashda SaaS – xizmatini boshqa hildagilari xam mavjud, Cisco WebEx – web – konferensiyalar o'tkazishdagi bulutli servis; CMS – SaaS modeliga an (SaaS – platform UMI.Cloud); E-Commerce B2B/B2C – SaaS modeliga an; Marketing SaaS ga asoslangan; «Antivirus Dr.Web» SaaS modeliga a-n; SugarCRM – CRM tijorat tizimi ochiq kodlar bilan; BPMonline CRM instrumentlari bilan biznes jarayoni modelashtirish va avtomatlashtirish uchun.

Shuni aytib o'tish joizki, bulutli xisoblash konsepsiyasi istemolchilarga bir qancha qo'shimcha turdagi bulutli xizmatlarni taqdim etadi: Stroge-as-asService, Database-as-a-Service, Information-as-a-Service,Process-as-a-Service, Process-as-a-Service, Integration-as-a-Service, Testing-as-a-Service va boshqalar, bundan tashqari Storage-as-a-Service ning ko'p sonli bulutli saqlash fayllari mavjud: Amazon Simple Stroge Service (Amazon S3), DropBox, GoogleDrive, MicrosoftOneDrive va boshqalar.

Bulutli texnologiyalarni va bulutli xisoblashlarni talim yurtlarida qanday tadbiq qilish mumkin? Google kompaniyasi talim yurtlariga Google Apps for education bulutli ilovani elektron talim sifatida taqdim etadi. Microsoft kompaniyasi esa oliy o'quv yurti talabalariga Office 365 for education (Windows Azure in education) bulut xizmatini tavsiya etadi. Bulutli xisoblashni (Cloud Computing) maktablarga, oliy o'quv yurtlariga tadbiq etish, o'quvchi va talabalarni bilim bilan yetarlicha taminlaydi.

Bulutli xisoblash modelari talablari va internet - resurslari aynan shu modelga tegishli ekanligini aniqlash uchun, ularni xarakteristikalarini bulutli xisoblashni asosiy xarakteristikalari bilan tekshirish mumkin: National Institute of Standards and Technology (talab bo'yicha o'z – o'ziga xizmat ko'rsatish, resurslarda yagona pul bo'yicha xamjihatlikda foydalanish, bir vaqtning o'zida elastic va mashtablashgan, faqatgina real xizmatdan foydalanganda to'lash, universal tarmoq kirishi).

Ikkinchi qatlam – PaaS (dastur platforma)

PaaS xizmati o'zida dastur platformasini va unga servis sifatida taqdim etiladi, bu o'z ichiga :

- OS – operatsion tizim tarmog'i (Unix-sistemalar, shu bilan birga Ubuntu Server, BSD/OS Family, Solaris/SunOS yoki Windows Server)
- Database – malumotlar bazasini boshqarish tizimi MBBT (MySql, Microsoft SQL, SQL Database, PostgreSQL, Oracle va boshqalar.)
- Middleware – o'rtacha qatlam dasturiy taminoti yoki aloqador dasturiy taminot, turli xil dasturlar, ilovalar, tizim va komponentalarni birga ishlashini taminlab beradi.
- Software development tools and testing – instrumental dasturiy taminot veb-ilovalarni ishlab chiqishda vaularni testlashda qo'llaniladi.
- App server – ilovalar server, ishlab chiqishda, testlashda, veb – ilovalar bilan ishlashda qo'llaniladi.

Asosiy PaaS Solution/Vendor:

- AWS Elastic Beanstalk/Amazon (Java, NET, PHP, Node.js, Python, Ruby and Apache HTTP Server, Apache Tomcat, Nginx, Passenger, and IIS)

- IBM Bluemix/IBM (IBM Bluemix bulutli platform keng qamrovdagi tillar ro'yhati va ilovalar qurishda freymorklarni tadbiq etadi, misol uchun, Liberty for Java, SDK for Node.js, ruby on rails)

- Microsoft Asure/Microsoft (ASP.NET, Java, PHP, Python, Django, Node.js and Azure SQL Database)

- Google App Engine/Google (Python, Java, PHP, Go and our MySQL)

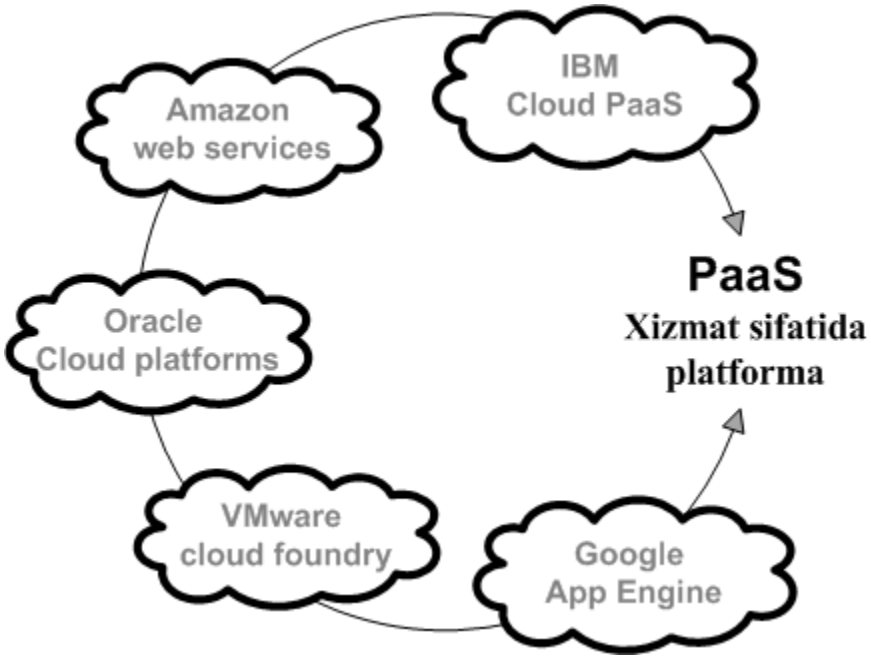
- Salesforcel Platdorm Cloud application development/Salesforce birlashtiradi Force.com, Heroku va ExactTarget yagona bulutli servisga va instrumentlarni ilovalar ishlab chiqishda qo'llaniladi. Misol uchun mobil ilovalarni ishlab chiqishda Salesforcel Mobile App/ Salesforce keng qo'llaniladi.

- Heroku/Salesforce (Ruby, Java, Node.js, Scala, Clojure, Python va PHP and postgreSQL)

- Oracle Cloud Platform Services/Oracle (Oracle Database Cloud Service, Oracle Java Cloud Service, Oracle Database Backup Service)

- OpenShift/Red Hat (Java, JavaEE, Python, Perl, PHP, Ruby, Node.JS, and MySQL, PostgreSQL, MongoDB)

- Cloud Foundry/VMware (Java Spring, Ruby on Rails va Sinatra, NodeJS.Net va MySQL Redis, MongoDB)



1.6-rasm. *Bulutli xisoblashdagi asosiy PaaS provayderlar*.

Bulut xizmatlaridagi birinchi qatlam – IaaS (Infratuzilma)

IaaS – bu kompyuter va tarmoq infratuzilmasini istemolchilarga taqdim etish va virtualizatsiya sifatida xizmat ko'rsatish. Boshqa so'zlar bilan aytganda malumotlar markazi yoki malumotlarga ishlov berish markaz provayderi istemolchilarga servis sifatida virtual infratuzilma yaratadi. Virtualizatsiya vositalari malumotlar markazi fizik infratuzilmasini virtuallashtirish imkoni beradi va shu yo'l bilan birinchi bulutli xizmat qatlami IaaS yuzaga keladi.

Virtualizatsiyani o'zi nima? Resurslarni virtualizatsiyalash texnologiyasi fizik uskunalar (serverlar, malumotlar saqlash bazasi, malumotlarni uzatish tarmog'i) ustidan ish olib borish uchun mo'ljallangan. Ular istemolchilar o'rtasida bir – necha qismlarga bo'linadi. Misol tarizda: bitta fizik serverdan, yuzlab virtual serverlar ishlashi mumkin…"[3] Virtualizatsiyani taqbiq etishda dasturiy va apparat darajada bo'ladi.

Iaas yaratishda virtualizatsiyadan tashqari avtomatizatsiya xam ishlatilinadi, unda provayder ishtrokisiz resurslarni dinamik taqsimlash imkoniyatini beradi. Avtomatik tizim virtual serverlar soni ko'paytirish yoki kamaytirish, malumotlarni saqlash uchun disk maydoni yoki tarmoq kanallar aloqasini o'zgartirish mumkin. Virtualizatsiya va avtomatizatsiya bulut xizmati IaaS da xisoblash resurslari samarali foydalanish, ijara narxini pasaytirish imkonini beradi.

IaaS da korparativ istemolchilar uchun arenda mavjud. Istemolchilar o'z xisoblash infratuzilmasini yaratishda, ularga integratsiyalangan resurslar taqdim etiladi. Bunday holatlarda istemolchining o'zi OS va ishlab chiqish vazifalari uchun zarur bo'lgan dasturlarni, ilovalarni o'rnatishi va sozlashi zarur xisoblanadi. Iaas konsepsiyasi istemolchi faqatgina aniq vazifalarni bajarishu uchun shu xisoblash kuchini sotib olish imkoniyatini beradi. IaaS ni qo'shimcha xizmatlari tarkibiga har bir istemolchining fizik uskunalariga bulut platformasi orqali ulanishni va uni malumotlar markazi tarmog'iga joylashtiradi.

Xizmat sifatida infratuzilma – bu keng qamrovdagi korxonalar uchun korparativ yechim. Infratuzilma malumotlarga ishlov berish markazida, xam va tashqi malumotlar markazida joylashtirilgan bo'lishi mumkin. IaaS xizmati xususiy, ijtimoiy, gibrid bulutlarni yaratish, va ximoya etish uchun tashkillashtirilgan. Provayder gibrid bulut konfiguratsiyasni qurishni taminlashda buyurmachining offisi bilan bulutli tarmoq platformasiga lokal tarmoqni birlashtiradi. Bundan tashqari, IaaS bulutli xisoblash xizmatlariga bulutli xosting xam kiradi. Bulutli xosting – bu xosting resurslarni dinamik ajratadi, resurslarni avtomatik mashtablashtiradi va yuqori barqarorlikni rad etadi. Bulutli xosting vitual xostinga, virtual serverdagi VPS/VDS xostinga va ajratilgan serverdagi fizik xostinga alternativ xisoblanadi.

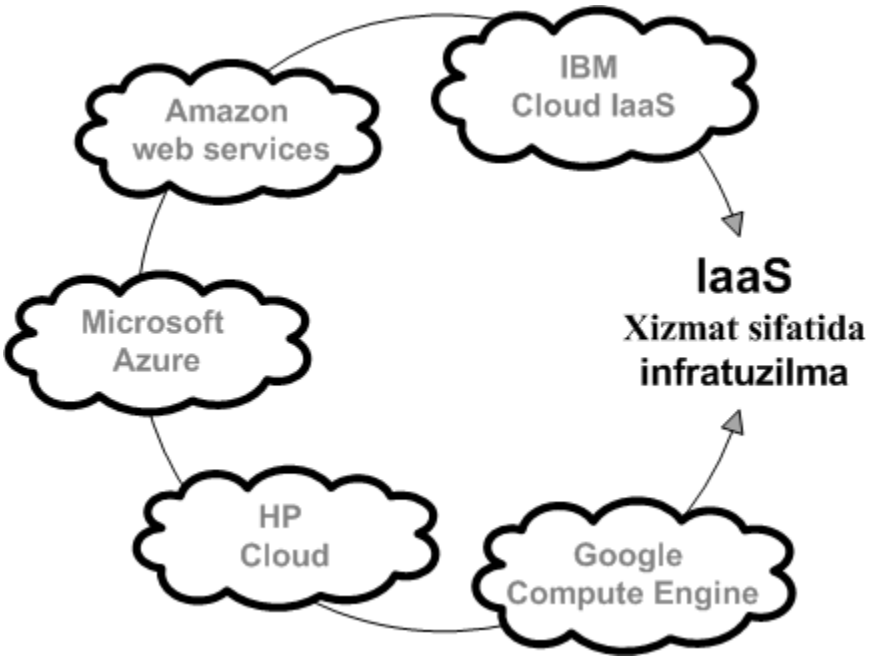
Bulutli xosting provayderi, sayt egalariga faqatgina zarur sayt resurslari: virtual serverlar, operativ xotira soni va qattiq disk xajmi, xosting infratuzilmani boshqarishdagi imkoniyatlar (misol uchun, tanlash imkoniyatlari, operatsion tizim, RAM lar soni, HDD xajmi va turi, CPU yader soni, taktlash chastotasi va kirish tezligi). Bulutli xosting ijarasni to'lash resurslarni sarflanganligi va faktlar asosida amalga oshiriladi: protsessor vaqtlari soni, disklar soni, sarf qilingan operativ xotira soni va saytlarni ochish tezligi. Shu bilan birga bulutli xosting ijarachisi (sayt egasi) xosting resurslarini o'zgartirishi va bosim kuchi oshganda resurslarni xam avtomatik tarizda ko'tarilishini sozlash qo'yishi mumkin. Shunga qaramasdan istemolchilar faqatgina o'zlari sarflagan resurslarga to'laydilar. Bulutli xosting barqarorlikni rad etganda udagi joylashtirilgan sayt bir vaqtning o'zida boshqa

virtual serverlarda ish faoliyati davom etadi ulardan birini rad etilishi sayda olib borilayotgan ishga xalaqit bermaydi. Hozirgi vaqtga kelib xosterlar bulutli xosting bilan tayyorlangan CMSni ijaraga berishni maqul ko'ryabdilar. Xosting – provayderlar, bulutli xostingni tashkilashtirishda , o'z serverlarini infrasutruktura sifatidagi platformaga CMS o'rnatilgan Jelastiga almashtiradilar. Funksional platform Jelastik bir urinishda undagi joylashgan CMS va optimalashtirilgan saxifani xam o'rnatadi.

Jelastik o'z ichiga PaaS funksionaligini va IaaS infrasutrukturasni tez konfiguratsiya qilinganligini o'zida aks etuvchi maxsulot xisoblanadi. Jelastic – bu Java va PHP – ilovalarini ishga tushuruvchi platform xisoblanib, u nafaqat xosterlar tomonidan bulutli xostinglar tashkil etishda, balki korparatsiyalar muhit (xususiy yoki gibrid bulutlarda) va veb-ilovalarni ishlab chiqishida ishlatilinadi. Bulutli xostinglarda, bulutli saytlar – bu zamonaviy ilovalar xisoblanadi. bulutli saytlarda malumotlar, server ilovalari, bulutli MB da saqlanadi va hammasi virtual bulutli serverlarda bajariladi, saytning klient qismi istemolchining bravzerida bajariladi. Bulut xisoblash muxitida bulut masalalarni yaratishimiz mumkin: Amazon EC2, IBM x86, Microsoft Azure, EMC, VMware larni open – source bazalarida echimi topiladi. Qaysiki dinamik IT- muxitida malumotlarga ishlov berish markazi namoyon bo'ladi. Bundan tashqari bulutli xisoblashda bulutli malumotlar bazasi qo'llaniladi.

Bulutli malumotlar bazasining asosi SQL va NoSQL malumotlar modeli xisoblanadi. IaaS xizmati AQSH da keng tadbiq etiladi. Ukrayinaning De Nova kompaniyasida bulutli infratuzilmani VMware, EMC, Microsoft Azure bazasida korparativ mijozlar uchun taqbiq etilgan. Ukrayinaning eng katta malumotlar markazlaridan biri VOLIA, IT – infratuzilma VoliaCloud VMware kompaniyasi tomonidan qurilgan (VMware bulutli masalalarga asoslangan xolda). Xozirga kelib ushbu VoliaCLOUD kompaniyasi 500 dan ortiq virtual malumot – markazlariga ega. Asosiy IaaS Solution/Vendor: Amazon Web Services/Amazon, IBM SmartCloud/IBM, Softlayer IaaS/IBM, Azure Virtual Machines/Mixrosoft, Google Compute Engine/Google, HP Cloud/HP, EMC/EMC Corporation, Oracle

Cloud Infrastructure Services/Oracle. Shuni aytish joizki, IBM ishonchli va ochiq IBM SmartCloud infratuzilmasi IaaS ni boshqarishda yoki o'z o'ziga xizmat ko'rsatishda amalga oshiradi.



1.7-rasm *Bulutli xisoblashda asosiy IaaS provayderlar*.

Hozirgi kunlarga kelib provayderlar bulutli tayanch tarmoqlarini yaratishda keng qamrovli mobil aloqalar(mobil aloqa operatori) IaaS xizmatlari tadbiq etishyabti. Bunday xizmatlarga, misol tariqasida bulutli telekomunikatsion platforma, Huawei kompaniyasidan va NSN Telco Cloud yechimi bo'lib Nokia Siemens Networks xizmat qiladi.

Huawei kompaniyasidan FusionSphere platformasi xisoblash resurslari, saqlash resurslari, tarmoq reserslarini virtualizatsiya qilish bilan taminlaydi va yagona mexanizmni boshqarish va rejalashtirish bilan konfiguratsiyalangan xisoblash resurslarini yagona pulga birlashtiradi. Nokia Siemens Networks kompaniyasi tovush uzatilayotganda uni ushlab qolayotgan LTE (VoLTE) asosiy mobil xizmatlarni kompleks testlashni tashkil etdi.

1.3.Bulutli texnologiyalardan foydalanishda avzalliklari va kamchiliklari

Avzalliklari:

- Istemolchilar kompuyuterlardan ishlash kuchi xarakteristikalariga qaramaydi…”[3] Kompyuterlar yuqori kuchda ishlashi uchun, katta xotira va ko’p xajimli disklarga ega bo’lgan bo’lishlari shart emas. Chunki barcha malumotlar va xamma dasturlar bulut serverlarida saqlanadi. Katta xajimga ega bo’lgan shaxsiy statsionar kompyuterlar, noutbuklar, netbuklar, orqali istemolchilar bulutga kirishlari mumkin.

- Istemolchilar uchun kompuyuterlarni ishlash sifati oshdi. Istemolchilar kompyuter dasturlar, fayllarni masofadan turib ishga tushirishda kam yukli qilishlari uchun kam ilovalardan foydalanishlari kerak. Misol uchun, **Panda Cloud Antivirus –** antivirus dasturi, vebservis sifatida foydalana olish mumkin. Panda Cloud Antivirus kuchli server malumotlaridagi viruslarni masofadan turib skanerlash imkoni beradi. Bu dasturni istemolchi kompyuterida ishga tushirish ishlash yuki ikki barobar ko’payardi.

- IT infratuzilmadan foydalanish samaraforligi oshadi va chiqimlar soni kamayadi. Agar kompaniya uchun server o’rtacha yuklanish boholashini oladigan bo’lsak u 13% ni tashkil etadi. Bazi hollarda kompaniya o’zining qo’shimcha resurslari kuchini ishlatishga to’g’ri keladi, lekin bazi hollarda xisoblash resurslari bo’sh turadi va ishlatilinmaydi. Bunda esa albatta pulning sarifi bekor bo’ladi. Agar kompaniya xisoblash resurslaridan masofadigi bulut serverlaridan foydalansa, bu xolda kompaniya sarflari soni ikki marta kamayadi. Bundan kelib chiqqan xolda nobarqaror iqtisodiy ishlab chiqarish moslashuvchanligi oshib boradi. O’zining malumotlari bosha bir tashkilotlarda saqlashiga ishonchlilik qobilyati yo’qolganda kompaniyaning o’zi shaxsiy bulut yaratib, virtualizatsiya infratuzilmalarini barcha imkoniyatlaridan to’la qonchiligicha foydalansa bo’ladi.

- Xizmat ko’rsatishdagi va DT ni sotib olishdagi xarajatlarni kamaytirish. Bulut xisoblash texnlogiyalarini shaxsiy serverlarda qo’llanilishi kompaniya ko’lamida kichik xisoblanib, shuning uchun ularga xizmat ko’rsatish onson bo’ladi. Katta sonli fizik serverlardan voz kechish orqali DT ni sotib olishdagi muomolar kamayadi. Servis va ilovalar bulut ichida bo’lganligi uchun istemolchilar DT sotib olishlari shart bo’lmaydi.

- Xisoblash kuchi o’sishi. Shaxsiy kompyuterlar bilan bulutli xisoblash resurslarini solishtirganda, bulutli xisoblash resurslari katta imkoniyatlarga ega. Bulutli xisoblash kechi uning serverlari soni bilan o’lchanadi. Istemolchiga superkompyuterdan masofadan turib foydalanish imkoniyatini yaratib beradi, bu albatta oddiy shaxsiy kompyuterda masalalarni yechish imkoniyati bo’lmaganda.
- Malumotlar saqlashdagi cheklanilmagan xajimlar. Malumotlarni saqlash xajmiga qarab bulutli texnologiyalar qulay va avtomatik tarizda (istemolchi hohish istagiga qarab) joylashtiradi. Oddiy shaxsiy kompyuter istemolchisi malumotlarini saqlashga joy yetmaganda, bunday xolat bulutli xisoblash istemochilarida yuzaga kelib chiqmaydi.
- Operatsion tizim bilan mos kelishi. Bulutli texnologiyalar istemolchilarda qanday operatsion tizim turganligiga qaramaydi. Microsoft Windows operatsion tizimidan foydalnilayotgan mijoz, Unix mijozlari bilan muomosiz malumotlarni almashishi mumkin. Servislardan foydalanishda esa har bir operatsion tizim brauzerga qarab standartlashtiradi.
- Xujjat formatlari bilan mos kelishi. Shaxsiy kompyuterdagi fayl Microsoft Word 2007 dasturi asosida bajarilgan bo’lsa, eski versiyalarida yani Microsoft Word 2003 da ochish imkoniyati mavjud emas. Bulutli xisoblashlarda esa to’gri kelmagan xujjatlarni ochish muomosi kelib chiqmaydi.
- Istemolchilarning bir gurux bo’lib ishlashidagi qulayliklari. Bulutli xisoblash tizimlarida bir vaqtning o’zida bir necha istemolchilar ish olib borishlari mumkin. Xujjatlarni bir kompyuterdan boshqasiga ko’chirib o’tkazish kerak bo’lmaydi. Xujjatlarni taxrirlash tez aks etadi, bundan tashqari istemolchilar xujjatning yangilash imkoniyati mavjud.
- Bulutli xisoblashlarda fayllardan erkin foydalanish imkoniyati mavjudligi. Agar malumotlar bulutda saqlanilayotgan bo’lsa, bu malumotlardan istalgan vaqtda istemolchilar foydalanishlari mumkin faqatgina Internet tarmog’i mavjud bo’lgandagina. Istemolchilar uchun keng qamrovdagi qurulmalardan internetga kirish orqali foydalanishlari mumkin. Bulut mijozi shaxsiy kompyuter, planshet, netbook, smartfon, notebooklardan foydalanishlari mumkin.

- Tabiy resurslardan foydalanishni kamaytirish. Bulutli xisoblash texnologiyalarida xisoblash kuchlarini tejash nafaqat elektroenergiya bo'yicha balki fizik maydon va tabiy resurslarni kamaytirish imkoniyati mavjud. Malumotlarga ishlov berish markazi (ЦОД) malum bo'lgan salqin xududlarda xam saqlash imkoniyati bor. Malumotlardan foydalana oladigan qurilmalar xozirda juda ixcham xisoblanib, ishlab chiqarishda kamroq materiallar ketadi.

- Malumotlarni yoqolishiga bardoshligi. Bulutda saqlanilayotgan malumotlar, o'zlarining nusxalarini bir necha serverlarga joylashtiradi. Shuning uchun bulutda saqlanilayotgan malumotlarni yoqolishi extimoli juda xam kam albatta buni istemolchining shaxsiy kopyuteri bilan solishtirganda.

Kamchiliklari:

- Doyimiy Internet tarmog'i bilan aloqada bo'lishi lozim. Bulutli xisoblash texnologiyalaridan foydalanishda har vaqt tarmoq Internetga ulangan bo'lishi lozim. Bundan tashqari bir necha ilovalar mavjud bo'lib, ular kompyuterlarga yuklanadi va ulardan uzoq muddatgacha ishlash imkoniyati bo'ladi. Boshqa holatlarda esa har doimgidek oddiy xisoblanib, ulanish bo'lmasa ish xam bo'lmaydi. K'opchilikning fikricha bu bulutli xisoblashlarning eng katta kamchiligi deb yurutishadi. Axborot texnologiyalari rivojlanishini xisobga olgan xolda shuni aytishimiz mumkunki Interner tarmog'i xozirgi kunda xar bir joyda mavjud. Shuning uchun bu muomoli qarashlar tez vaqatlar ichida umuman etiborda chiqadi.

- Ishlash tezligi sekinligi. Ko'pgina bulutli servislar to'la qonligicha ishlashlari uchun normal Internet – ulanishni talab qiladi. Bu muomoni kelib chiqishini oldini olishda choralar ko'rilyapti va bu muomo tez kunlarda judlik bilan to'g'irlanishiga ishonch yuqori darajada.

- Dasturlarni sekin ishlashi va to'iq funksional imkoniyatlarga ega bo'lmagan xolda. Bir necha dasturlar bulutli tizimlarda sekin ishlashlari mumkin lokal kompyuter tizimiga qaraganda. Bu uzoq masofadagi serverlarni yuklash qiyinchiliklari tufayli yuzaga kelishi mumkin.

- Malumotlar xavfsizligiga xavf borligi. Istemolchilar tomonidan bulut texnologiyalariga qo'yilgan xar bir malumot xavfsizligi xavf ostida bo'lishi mumkin. Lekin bunda birinchi masala provayderga istemolchining ishonish muxim o'rinda turadi. Agar bulutli texnologiyalar provayderi malumotlar almashishini ishonchli shifrlasa, zaxira nusxalasa va bulutli texnologiyalar soxasi bozorida o'ziga yarasha tajribaga ega bo'lsa bu holda xavfsizlik borasida muomolar tug'ilmaydi. Fakt sifatida shuni aytish mumkinki bulutda yo'qolgan malumotlarni qaytarish mumkin emas.

2. Asosiy qism. Bulutli texnologiyalardagi mavjud tahdidlar va ularga qarshi kurashish mexanizmlarini tahlili

2.1. Bulutli texnologiyarga xavf soluvchi tahdidlar

Bulutni boshqarish va nazorat qilish – xavfsizlikning asosiy muomolaridan biri xisoblanadi. Bulut texnologiyalarida barcha resurslar xisoblangan va ular virtual mashinalar tomonidan doimiy nazoratda bo'lgan, qo'shimcha jarayonlar ishga tushurilmagan va bulut elementlari buzilmagan holat hali ko'rilmagan…"[4] Bu yuqori pog'onali tahdid xisoblanib, u bulut boshqaruvi bilan bog'liq, yagona information tizim sifatida xizmat qiladi va uni umumiy ximoyasini yuqori darajada qurish kerak bo'ladi.

Buning uchun albata xavf extimoligni boshqarish modellarini bulutli infratuzilmada qo'llash kerak bo'ladi. Fizik xavfsizlikni taminlash asosida server va tarmoq infratuzilmasiga fizik kira olishni qattiq nazorat qilish kerak bo'ladi. Fizik xavsizlikka qaraganda tarmoq xavfsizligi birinchi o'rinda model tahdidlariga qarshi xavfsizlikni o'zida namoyon qiladi va tarmoqlararo ekran orqali ularni bartaraf etadi. Tarmoqlararo ekran filtr vazifasini bajarib, malumotlarga ishlov berish markaz tarmog'idan (ЦОД) foydalanishda cheklashlarni olib boradi. Bunda aloxida serverlar, yani internet tarmog'idagi foydalanishga ruxsat etilganlaridan yoki tarmoq ichidagi serverlar. Bulutlii xisoblashlardda asosiy rolni platforma sifatida virtualizatsiya o'ynaydi.

Bulutli xisoblashlarda malumotlarni butunligini va xavfsizligini taminlashda, eng ko'p tarqalgan va asosiy tahdidlar .

Bulutli serverlarni, bulutli xisoblashlashlarga joylashtirishdagi qiyinchiliklar.

Bulutli xisoblashlar xavfsizligiga talab, malumotlarga ishlov berish markazi (ЦОД) xavfsizligi talabidan farq qilmaydi. Lekin malumotlarga ishlov berish markazini (ЦОД) virtualizatsiya qilish va bulutli muxitga o'tish yangi taxdidlarni yuzaga kelishiga sabab bo'ladi. Internet orqali xisoblash kuchlarini boshqarish, bulutli xisiblashning kalit xarakteristikalaridan biri xisoblanadi. Ko'plab ananaviy malumotlarga ishlov berish markazida (ЦОД) injinerlarni serverdan foydalanishi,

fizik pog’onada nazoratga olinadi va bulutli muxitda ular internet orqali ishlaydi. Kirishni nazorat qilayotgandagi cheklashlar va shaffof o’zgartirishlarni tizim darajasida taminlash asosiy kriterik ximoya xisoblanadi.

Virtual mashinalarni dinamikligi. Virtual mashinalarni dinamikligi. Yangi mashina yaratishni, ish to’xtatish va boshqatdan ishga tushirishni qisqa vaqt ichida amalga oshirsa bo’ladi. Ular fizik serverlar bilan chalkashib ketishlari mumkin. Buday o’zgarishlar tizim xavfsizlik butunligini qayta ishlab chiqarishda qiyinchiliklar tug’diradi. Biroq operatsion tizim yoki ilovalarni zayifligi virtual muxitda nazoratsiz tarqaladi va qanchadir vaqt oralig’ida tez tarqala boshlaydi (misol uchun, zaxira nusxadan qaytarilishda). Bulutli xisoblash muxitida eng avalo tizim xavfsizligi xolatini tuzatish, shuni xisobga olish kerakki, uning xolati va turar joyi bog’liq bo’lishi kerak emas.

Ichki virtual muxitdagi zayifliklar.Bulutli xisoblash serverlari va local serverlar bir xil operatsion tizim va ilovalardan foydalanishadilar. Bulutli tizimlar uchun uzoqdan buzish yoki zararli dasturiy taminot tahdidlari ko’p xisoblanadi. Paralel virtual mashinalar xujum xafini ko’paytiradi. Protokolarga asoslangan taxdidlar (Система обнаружения вторжений) va ularni bartaraf etish protokollari zararli xarakatlarni virtual pog’onasida aniqlashi lozim.

Ishga tushmagan virtual mashinalar ximoyasi. Qachonki virtual mashina o’chig’ligida, zararlanish xavfi ko’proq bo’ladi. Virtual mashinalardagi saqlanadigan obrazlarga kirish yetarli bo’ladi. Ishga tushmagan virtual mashinada dasturiy xavfsizlik taminotini umuman ishga tushirib bo’lmaydi. Bunday holatda virtual mashinada nafaqat ichki xavfsizlik tadbiq etilgan bo’lishi balki gipervizor darajasida xam bo’lishi kerak.

Hudud xavfsizligi va tarmoqni cheklash. Bulutli xisoblashni qo’llashda xudud tarmog’i susayadi yoki umuman ko’zdan yo’qoladi. Bu shunga olib keladiki, xavfsizlik yuqori darajada emasligi va tarmoq qismi umumiy xavfsizlik pog’onasini aniqlaydi. Bulutda xar– hil ishonchli darajada segmentlarni cheklashda virtual mashinalar o’z xavfsizliklarini o’zlari taminlashi kerak bo’ladi.

2.1.1. Blutli texnologiyalarda amalga oshiriladigan xujumlar va ularni bartaraf etish

DTda ananviy xujumlar.Operatsion tizim, modul komponentlari, tarmoq protokollari va boshqalarini zaifligi – ananaviy taxdidlarga kiradi, ximoyasini taminlash maqsadida tarmoqlararo ekran, antivirus, IPS va boshqa komponentlar o'rnatish orqali muomolarni xal etish mumkin…"[5] Shuni xisobga olish keraki, bunday ximoya yo'li virtualizatsiyada xam samarali ishlashi lozim.

Bulut elementlarida funksional xujumlar.Xujumning buday turi ko'pqatlamli bulut bilan umumiy xavfsizlik prinspga bog'liq. Bulut xavfsizligini to'g'risida quydagilarni yechim sifatida olish mumkin: funksional xujumlardan ximoyalanishda, xar bir bulut qismiga quydagi ximoya manbaini qo'yish lozim: proksi uchun – DoS – xujumdan samarali ximoya taminlanishi, web – server uchun – saxifalarni yaxlitligini nazorat qilish, server ilovalari uchun – ekran pog'onasidagi ilovalar, MBBT uchun – SQL – inyeksiyasi ximoyasi, malumotlarni saqlash tizimi uchun – to'g'ri bekaplar (zaxira nusxalash) berish, foydalanishdan cheklash. Yuqoridagi sanab o'tilgan ximoya mexanizmlari ishlab chiqarilgan, lekin ular birgalikda bulut kompleks ximoyasi taminlash uchun xali birga yig'ilmagan. Shuning uchun bulut yaratilayotgan vaqtda, ularni yagona tizimga integratsiyalash muomoni xal bo'lishiga turtki bo'ladi.

Mijozjlarga xujumlar. Ko'plab mijozlar bulutga ulanayotganda, bravzurdan foydalanishadi. Xujumlardan biri Cross Site Scripting, parollarni «o'g'irlash», veb – sesiyalarni ushlab qolish va boshqalar. Bunday xujumdan yagona to'g'ri va ximoya aniq autetifikatsiya va bog'lanishdagi shifrlash (SSL) bilan o'zaro autetifikatsiya. Ammo bunday usul ximoyasi bulut yaratuvchilariga juda xam noqulay va ko'p vaqt talab qiladi.

Gipervizorga xujumlar. Gipervizor virtual tizimlar uchun kalit elementlaridan biri xisoblanadi. Uning asosiy funksiyalaridan biri virtual mashinalarga resurslarni taqsimlashdan iborat. Gipervizorga xujum shu narsani yuzaga kelib chiqarishi mumkinki, virtual mashinalardan biri boshqa virtual mashina xotirasi, resurslaridan foydalana olishi mumkin. Bundan tashqari u

tarmoq trafigni qo'lga kiritishi, fizik resurslarni o'zlashtirishi va server orqali virtual mashinani ishlashdan to'xtatishi mumkin. Standart ximoyalash metodlarini joriy etishda virtual muxitda kerakli maxsuslashtirilgan maxsulotlar qo'llanilishini tavsiya etadilar. Xost – serverlarni katalog xizmatlari Active Directory bilan integratsiyalash, shuningdek xost – server boshqarish vositalaridan foydalana olish tartibotini standartlashtirish. Shu bilan birga ko'p xollarda ishlatilmaydigan xizmatlardan voz kechish, misol uchun, virtualizatsiya serverga veb – foydalanish.

Boshqarish tizimidagi xujumlar. Bulutda ishlatiladigan ko'pgina virtual mashinalar aloxida tizim boshqaruvini talab etadi. Boshqarish tizimiga xalaqit berish virtual mashinalarda – nosozlikni kelib chiqaradi va bir virtual mashinani bloklash orqali boshqa virtual mashinani ayibdor qilib qo'yadi.

Bulut soxasida eng samarali xavfsizlikni taminlash yo'llaridan birini *Cloud Security Alliance* (CSA) tashkiloti ommaga xavola etgan xisoblanib unda quyidagi malumotlar taxlil qilingan:

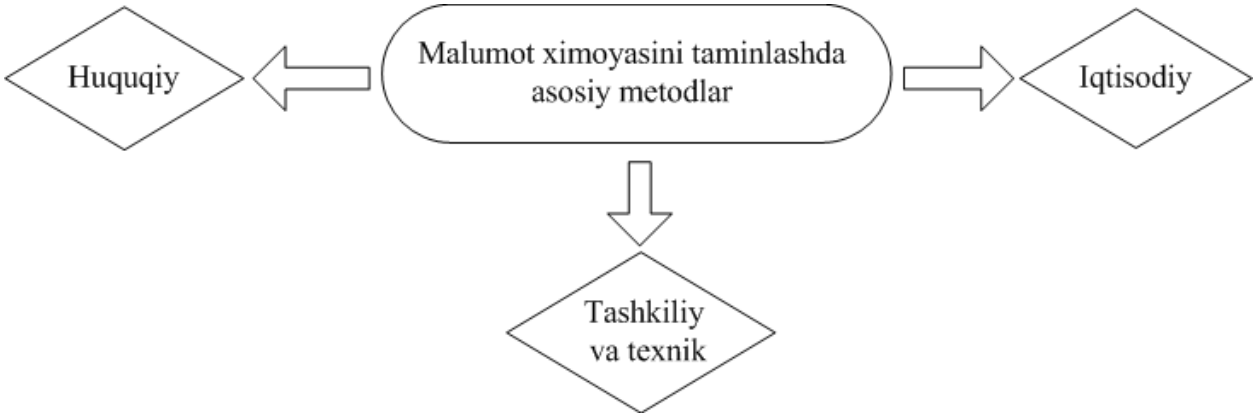
Malumotlarni saqlash. Shifrlash – malumotlarni ximoyalashda eng samarali yo'llardan biri. Malumotlardan foydalana olishga ruxsat beruvchi provayder, malumotlarga ishlov berish markazi (ЦОД) da saqlanayogan mijoz malumotmi shifrlashi, foydalanishdan chiqqan xolda esa ularni qaytarishsiz o'chirib tashlashi kerak.

Uzatishdagi malumotlar xavfsizligi. Shifrlangan malumotlarni uzatish faqatgina aytenifikatsiyalangandan so'nggina amalga oshirilishi mumkin. Malumotlarni o'qish yoki o'zgartirish kirgazish, Ulardan foydalana olish ishonchli bog'lamalar orqali amalga oshiriladi. Bunday texnologiyalar juda xam mashxur algaritmlar va ishonchli protokollar AES, TLS, Ipsec amalga oshiriladi.

Autetifikatsiya. Parol ximoyasi. Katta ishonchlilikni taminlashda tokenlar va sertifikatlar etibor qaratiladi. Provayder identifikatsiya tizimi bilan avtorizatsiyadan o'tishda shaffof tarizda xarakatlanishi lozim. Bunda LDAP (Light Directory Access Protocol) va SAML (Security Assertion Markup Language) protokolari ishlatilinadi.

Istemolchilarni izolatsiyalash. Virtual mashinalar va virtual tarmoqlardan individual foydalanish. Virtual tarmoqlarda quydagi texnologiyalar joriy etilgan bo'lishi kerak. VPN (Virtual Private Network), VLAN (Virtual Local Area Network) va VPLS (Virtual Private LAN Service). Provayderlar ko'pincha yagona dastur muxitida kod o'zgarganligi sababli istemolchilar malumotlarini bir – biridan izolatsiyalaydi. Bunday yondashish xatarli xisoblanib, u standart bo'lmagan koddan yo'l topib , istemolchi malumotlaridan foydalana oladi.

2.2. Bulutli texnologiyalarda malumot ximoyasini taminlashda asosiy metodlar



2.1 – rasm. *Bulutli texnologiyalarda malumot ximoyasini taminlashda asosiy metodlar*.

Huquqliy metodlar. Huquqiy metodlarni xavfsizligini taminlash o'z ichiga normativ – huquqiy aktlarni ishlab chiqarish…"[6] ishtirokchilar o'rtasida axborot munosabatlarini tartibga solish va normative – metodik xujjatlar, axborot xavfsizligi taminlashdagi savollarni qamrab oladi.

Bularning eng muxim faoliyatlariga quydagi harakatlar kiradi:

- davlat qonunchiligi bo'yicha o'z vaqtida kiritilgan o'zgartirishlar va to'ldirishlar, axborot xavfsizligi soxasiga tegishli tartibga solishlar;
- xalqaro shartnomalarga bog'liq ziddiyatlarni bartaraf etish;
- xuquqbuzarlik bo'yicha javobgarlikni o'rnatish;
- axborot xavfsizligini taminlash soxasida vakolatlarni cheklash;
- normative huquqiy aktlarni ishlab chiqish va qabul qilish;

Tashkiliy va texnik. Bunday metodlarga quydagilar kiradi:

- axborot xavfsizligini taminlash bo’yicha tizim yaratish va modernizatsiyalash;
- ishlab chiqarishda, axborot ximoyasi va nazorot qilish metodlarini vositalaridan samarali foydalanish va komolotga yetkazish;
- texnik qurilmalar va dasturlardan kelib chiqadigan xavflarni axborot xavfsizligini taminlashda aniqlash;
- axborot xavfsizligi vositalarini sertifikatsiyalash;
- ximoyalangan axborot tizimlarida, xodimlar qatti - xarakatlarini nazoratda tutish;
- tizim monitoring ko’rsatkichlari va axborot xavfsizligi xarakteristikalarini shakillantirish;

Iqtisodiy. Iqtisodiy metodlar o’ziga quydagi xavfsizliklarni oladi:

- Axborot xavfsizligi bo’yicha rejalarni ishlab chiqish.
- tizimni takomillashtirishda ishlarni moliyalashtirish, tashkilot huquqlari va tashkiliy – texnik metodlar bilan birgalikda.

Xizmat ko’rsatish darajasidagi moslashtirish.Xozirgi vaqtlarda xuquqiy normativ aktlar, bulutli resurslarni tartibga solish qoidalari mavjud emasligi xizmat ko’rsatish darajasiga moslashtirish, bulutli xisoblash provayderlarining eng muxim kriteriyalaridan biri xisoblanadi…”[7] Afsuski xozirgi vaqtlarda ko’p provayderlar xizmat ko’rsatish darajasidagi moslashtirishni shunday tuzadilarki, natijada o’zlariga kam jovobgarlikni oladilar. Bundan kelib chiqqan holda, konfidensial malumotlarni bulutli xisoblashlarda ishlatishdan oldin yaxshi xizmat ko’rsatish darajasiga moslashtirilgan provayderlarni tanlash lozim.

Tizimgacha bo’lgan bulut xavfsizlik kanalini o’rnatish.Bulut ichidagi tizim bilan bog’lanishda kanal shifrlanadi. Xavfsizlik kanallarini o’rnatishda VPN (virtual shaxsiy tarmoq) texnologiyalari qo’llaniladi. Shunga qaramasdan yani telekomunikatsiyaning tarmoqda quyi pog’ona ishonchliligini mavjudligi va kanal dagi ishonch yuqori pog’onada qoladi. Kriptografik vositalarni ishlatilinishiga qarab (shifrlash, autentifikatsiya, ochiq kalitli infratuzilma va jo’natilayotgan malumotlarni o’zgartirilishini oldini olish). Bu usul eng oddiy va eng ishonchli

xisoblanadi, u MITM (insonlar o’rtasida) xujumlaridan ximoya qiladi. Lekin bu usul faqatgina bulutdagi tizim va kanal aloqasini ximoyalaydi. Butun tizimdan o’tayotgan malumotlar ochiq xisoblanadi.

Malumotdan foydalanishda rollarni taqsimlash. Bir necha fayllardan iborat mexmon tizimi faqatgina obraz xisoblansa, virtual infratuzilma admistratori istalgan vaqtda malumotlarni ko’chirib olishi va ularni boshqa kompyuterlarda ishga solish orqali konfidensial malumotlar ustidan tadqiqod olib boradi. Malumotlarni nusxalash – ko’p vaqt talab etmaydigan ish xisoblanib, shunday yo’l orqali konfidensial malumotlarni virtual infratuzilma admistratorlar tomoniga sizib chiqishi sababli admistratorlar o’z manfatlari yo’lida foydalanishlari mumkin. Bunday muomodan qochish maqsadida admistratorlar rollarini taqsimlash yani ularni ikkiga virtual infratuzilma admistratori va xavfsizlik admistratori. Bu ish, malumotlarga ishlov berish markazi (ЦОД) vazifasini xam bo’ladi va bir taraflama xavfsizlik sozlamasini o’zgartirishga imkon bermaydi. Afsuski bunday taqsimlash bulutli texnologiyalar resurslaridan foydalana olishga ruxsat beruvchi provayderning qanday ish yuritishiga bog’liq. Xozirgi vaqtlarga kelib bunday texnologiyalarga xizmat ko’rsatuvchi vositalarni turli xil bulutli texnologiyalarni ishlab chiqaruvchi kompaniyalar ishlab chiqarishyabdi. Misol tariqasida, vGate taminoti ishlab chiqarilgan, u VMware baza tizimida ishlaydi.

Virtual mashinalarni segmentlash. Segmentlashda virtual mashinalar mijozlar va xavfsizlik talablarini taminlashda segmentlarga bo’linadi. Bu o’zida tarmoq trafigni umumiy taqsimlashni va siyosiy boshqaruvdan foydalana olishni taqsimlash, xatto ular umumiy tarmoq infratuzilmasi bilan umumiy fizik uskunalarda ishlayotganda xam. Shaxsiy bulut yaratishda bu taqsimlash misol uchun, bugalteriyaga tegishli virtual mashinalar va qayta ishlash bo’limlariga tegishli virtual mashinalarni segmentlarga bo’ladi. Shuday imkoniyat mavjudki xar – xil tarmoq interfeyslarini ishlashda bu segmentlarni ajratish mumkin.

Bulutda saqlanilayotgan malumotlarni shifrlangan xolda olib borish.Bu metod xar bir faylni kriptografik vositalar bilan shifrlashni o’z ichiga oladi, qaysiki

bulutga saqlash uchun yuboralayotganlarini. Shunday usulga binoan, xech qaysi bir shaxs malumotni olish imkoniyati yoq xisoblanadi faqatgina daslabki deshifrlash kalitiga ega shaxslargina faylni ochish imkoniyati mavjud. Bunday usullar ko'proq yakka tartibdagi shaxslarga yoki kichik tashkilotlarga to'g'ri keladi. Biroq kalitga ega istemolchilar soni ko'pligi bu metod ko'plab kamchiliklarni yuzaga kelib chiqaradi. Bundan kelib chiqqan xolda kalitni nazorat qilish qiyinchiliklarni yuzaga kelishiga sabab bo'ladi.

Malumotlarni shifrlashda proksi serverdan foydalanish.Bunday usulda ishonchli muxitdagi uskunalardan foydalaniladi. Barcha yuborilayotgan malumotlar u orqali o'tadi. Bu usul barcha malumotlarni bulutga jo'natishdan oldin shifrlaydi va so'rovga ko'ra daslabki malumotlarni deshifrlaydi. Shunga asosan ushbu shifrlash va deshifrlash kaliti bergan serverga malumdir. Shu bilan birga server jurnal xisobotini fayldan foydalana olishda ishlatish mumkin. Shunga asosan proksi serverdan foydalanish fayllar bilan ishlashni istemolchi uchun shaffoflaydi.

Bulutdagi tuzatish imkoniyati yoq malumotlarga ishlov berish. Bu metodni qo'llashda bulutga malumotlarni uzatishda undan uchinchi taraf foydalana olmaydi. Buning uchun malumotlar butunligicha emas balki, bo'laklarga bo'linib jo'natiladi, bunga ko'ra tizimdagi malumotlar bir biriga bog'liq bo'la olmaydi. Konfidensial malumot xam o'z o'rnida, ishonchli joyda joylashgan bo'ladi.

2.2.1. Bulutli texnologiyalardan foydalanishda axborot ximoyasi

Agar texnologik nuqtai nazardan bulutli texnologiyalarga qaraydigan bo'lsak, ilovalar ishlashi sharti ananaviy ishlash sharti bilan katta farq qilmaydi. Biznes tizimlari shuningdek, alohida kompyuter kuchi bilan ishlaydi faqatgina bulutli texnologiyalarda ular virtual bo'la oladi. Ma'lumotlar serverlarida saqlanadi, va ular bir necha xisoblash tugunlariga ajratiladi yoki yagona katta serverga joylashtiriladi…"[8] ko'pgina ekspertlar bulutli texnologiyalarda axborot xavfsizligini taminlash, ananaviy tizim ximoyasi prinspi asosida qurilishi kerak deb xisoblashadi.

Fakt asosida bulutli texnologiyalar ximoyasini ikkiga bo'lishimiz mumkin

- uskunalar xavfsizligni oldini olish
- malumotlar xavfsizligi

Provayder mijozlar ximoyasini taminlashda o'zining apparat va dasturiy tizimini ruxsatsiz kirishdan, AT- tizimlarini buzishdan, kod modifikasiyasidan himoyasini tashkil etish zarur xisoblanadi. O'z navbatida mijoz har qanday zarur bo'lgan yoki shaxsiy malumotni tizimga joylashtirayotganda uni tashqi xujumdan ximoyalashda shifrlash texnologiyasidan foydalanish imkoniyatiga ega. Bu «Bulutli texnologiya» larda xavfsizlikni bir – qancha avzalliklarni o'z ichiga oladi.

«Bulutli texnologiya» lar ximoyasi faqatgina operator yoki klent tasarrufida emas balki uning qayerda ishlatilnishi va metodlar turiga qarab belgilanadi.

Xususiy Bulut. Xususiy Bulut muxitda axborot xavfsizligini taminlash juda onson xisoblanadi. Shaxsiy bulut bilan ishlashda , biz faqat hisoblash resurslari va ma'lumotlar saqlash xizmati modeli va grafik foydalanishmiz mumkin. Shunda butun qimmatli malumot kompaniyani o'zida qoladi. Qatiy belgilangan choralarda tarmoq o'chib qolganda virtual ish stolidagi malumotlar saqlanib qolmasligi mumkin. Xususiy Bulut nafaqat platforma va ilovalar to'liq funksiyalarini amalga oshirishda shunindek ximoyani maksimal turlarini taqdim etish mumkin bo'ladi.

Xususiy bulutda admistrator tomonidan kodirovka qilingan, ximoyalangan diferensiyalangan, klaster xal etilgan, autentifikatsiyalangan arsenaliga ega, auditorik operatsiyalar va ximoyalashgan malumotlardan maksimal foydalanish mumkin.

Zamonaviy dasturiy yechim ko'p ishlar qila oladi, malumotlar bazasi tizimidan shaxsiy foydalanish operatsiyasi qulayligni akslantirib beradi. Xsusan shunday funksiyalar «**Run-Time Privilege Analysis**» va «**Data Redaction»** tashkilotlarga «Bulutli texnologiya» larda saqlanayotgan malumotlarga kirayotgan, foydalanayotgan xarakatlarni aniqlash imtiyozni beradi. Lekin Xusisiy Bulut malakali kadrlar bilan ishlashni talab qiladi, qayski serverlarga xizmat qilish darajasi, to'xtovsiz va ishning samarali virtual dasturiy taminotini taminlab beradi.

Shunindek, Bulutda biznes ilovalar, ish uchun mas’ul va xizmat talab darajasini saqlab qoladi. Bulut xavfsizlik sohasida kata va tajribali mutaxassislar bo’lishi kerak. Hamma kompaniyalarda bunday holatni ko’zga tashlanmaydi, shuning uchun hozirda keng tarqalgan turlaridan biri bu ijtimoiy bulut texnologiyalar.

Ijtimoiy Bulut. Jamoat bulutni afzalliklaridan biri bu sizning malumotingizni boshqa tashkilot mas’ul bo’ladi va shu bilan birga uzatishni, saqlanishni taminlaydi. Qimmatli malumot muntazam tarizda tarmog’ni tark etganligi sababli u qo’shimch ximoyani talab etadi. Tasufki ijtimoiy va gibrid yoki ananaviy, xususiy bulut korhona tizimlarida o’rnatilgan xavfsizlik darajasini mohiyatan bir – xil bear olmaydi. Shuning uchun ko’pgina provayderlar ijtimoiy bulutda xavsizlikni samarali darajada amalga oshirish uchun xizmatlar cheklangan faoliyatga etibor qilishlariga to’g’ri keladi. Shunday bo’lsada, ko’p tashkilotlar bulut xavfsizligini taminlash maqsadida provayderlarni tanlashni afzal hisoblaydilar. Songi yillarda sezilarli darajada bulut ichida saqlanilayotgan malumotlar boshqa davlat foydalanuvchilari tomonidan zaif va kuzatish imkoni borligi qo’rquvni oshiradi. «**Verint Systems»** kompaniyasi konsalting bo'limi direktori **Stiv Rose** shunday deb takidlaydi.

Ximoya texnologiyasi. AT soxasida bulut ximoya strategiyasi juda yuqori darajada taminashining imkonini beradi shu vilan birga shaxsiy malumotlarni muxofaza qilish eng yuqori standartlariga ega. Cloud computing da har doim ishtrokchilarni maydoning belgilash, xar bir tarkibiy darajasi uchun talablarini aniqlash imkoni beradi. Bunday talablarni amalga oshirish imkoni bugungi kunda chora topilmoqda. E’tibor ishonchli tarqatilish va amaliyot dasturi foydalanish bo’yicha bo’lishi kerak. Ilya Trifalenkov, axborot xavfsizligi «**R- Style**» markazi direktori – aynan prikladnoy dasturiy taminoti darajasi malumotlarga kirish imkoniyatini beradi. Faqatgina shu prikladnoy dasturiy taminot darajasi maksimal xavf old liniyasida turadi.

Bulut muxitlarida eng ko’p tarqalgan xatarlar virtual mashinalarini ishlab turgan holatidan o’g’irlash o’girlash, faqat dastur parametrlaridan foydalanib AT-

infratuzilmasi tarmoq topologiyasida o’zgartirishlar, AT bo’yicha xujumlar tarmoq ximoya mexanizmlaridan to’g’ridan to’g’ri o’tish. Ushbu xavf virtual muxitni qurilishining barcha bosqichlarida ximoya qilinishi tufayli kamayadi, yani ular: cirtual infratuzilma, tizim boshqaruvi va saqlash tizimi doirasida, apparat, tizim dasturiy ta’minot grafigi (hypervisor).

Zamonaviy yechimlarga ko’z tashlaydigan bo’lsak, virtual mashinalarida tarmoqlararo ekran yaratishni imkoni berib, bu esa virtual mashinalarni doimiy monitoring opirativ nazoratni amalga oshiradi. Servis ximoya darajasi tarmoqlar aro ekran orqali muxofaza qilinadi, cloud computing muxitida faoliyat olib boradi.

Tarmoqlar aro ekran aloxida tarmoq protocolli talablariga muvofiq servis darajasida qayta ishlash mumkin yani ixtisoslashtirilgan protokollarni filtirlash mumkin. Cloud computing xavfsizlik darajasi kaster firewall apparati tomonidan taminlanib, erkin foydalanuvchilarni manzil malumotlarini virtual muxitga kirishni nazorat qilishni o’z ichiga oladi. Jurnalni yangilashda avtomat tarizda yoko qo’lda kiritish mumkin. Himoya qilish darajasi segment AIS apparat yoki shaxsiy firewall taminlab beradi. Tarmoq ishonchliligi talablariga qarab, yuqori ishonchliligi, alohida o’rnatilgan xavfsizlik devori, foydalanuvchi ish stansiyalari o’rnatilgan xavfsizlik devori, bir gruxini foydalanish mumkin.

2.3. Bulutli texnologiyalarda apparat va dasturiy vositalar ularni qo'llash imkoniyatlari va taqbiq etish

Apparat vositalarda to’xtalishlarning asosiy tasdiqi sifatida korparativ tarmoqlarda maxfiy axborotlarni qayta ishlashi yaxshi rivojlangan xisoblanadi. apparat vositalaridan foydalanishdagi afzalliklar, sifatiga kafolati, ish jaroyonida ishonchli va bardoshiligi uchun ajralib turadi…”[9] Apparat komponentalarini ishlab chiqaruvchi kompaniyalar ularni kafolatiga jovob beradilar. Shuningdek malumotlarga ishlov berish markazidagi apparat qismini noqonuniy foydalana olishdan tashkiliy va texnik muxofaza qilib uning bartaraf etadi. Chunki shunday xolatlar yuzaga kelib chiqadiki, xaker 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 tasirdan ximoya olib boriladi. Bunday xarakatlardan foydalanish asosan analog xolatlarda, bulutli xisoblash tizimlarida ijtimoiy kirish orqali bajariladi.

Malumotlarga ishov berish markazi (ЦОД) resurslaridan foydalanishda apparat va dasturiy taminotlarni axamiyati. Ishlash prispi ikkita asosiy metodlarga qaratilgan: IP – paketlarni apparat va dasturiy taminotlar yordamida shifrlash, yoki odiygina ochiq trafik orqali. Deyarli xar doim kompaniyalar korparativ tarmoqlarida ishlov berilgan shaxsiy konfidensial malumotlar 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 konfedensial axborotlar ximoya pog'onasi susayishiga olib keladi. Inson faoliyati soxalarida bunday holat nomaqbul xisoblanadi. Bunung yechimi IP – shifrlash tezligini oshirish orqali xal etsa bo'ladi.

Istemolchilarning apparat va dasturiy taminot bilan taminlash. Hozirgi kunlarga kelib, istemolchi 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 sertifikatsiyalashgan firmalar yetarlicha xisoblanadi. Istemolchilar operatsion tizimlaridagi kalitlar va korparativ bulutdagi shaxsiy axborotlar ximoyasi axborot xavfsizligini taminlashda katta muomolardan biri xisoblanadi. Istemolchining shaxsiy kompyuterlarda elektron quluf o'rnatiladi. Bunday blakirovkani nafaqat istemolchi balki, kompaniya axborot xavfsizligi xizmati xam nazorat qilish imkoniyatiga ega. Lekin bularning xammasi faqat shaxsiy bulutda mavjud bo'lib ijtimoiy bulutda bu imkoniyatlar yo'q.

Gipervizor , dasturiy vosita sifatida apparat resurslarini boshqarishda va resurslarni mexmon operatsion tizimlar o'rtasida taqsimlaydi, shuning uchun

virtual muxitda eng zaif qismi xisoblanadi. uning xar 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 xar qanday malumotlardan foydalana olish xuquqiga ega bo'ladi.

Shuning uchun axborot resurslari xavfsizligini virtual muxit ichida xal etish mumkin. Mantiqiy virtual infratuzilma fizik infratuzilmadan farq qilmaydi shunga ko'ra birinchidagi taxdidlar ikkinchiga xam taluqli xisoblanadi. Shunda axborot ximoya vositalari virtual infratuzilma ximoyasini taminlashda, apparat resurslarini opimizatsiyalash qobilyatiga ega bolishlari lozim. Ko'p xajimga ega bo'lgan virtual infratuzilmalarda ratsioanal maqsadda axborot ximoya 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. Xar bir nusxa o'zida antivirus signaturasi, yuritgich bo'ladi: bularning xammasini 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.

2009 -yilda VMware kompaniyasi gipervizor ishlab chiqaruvchilar qatoridan birinchi bo'lib gipervizorni chuqur joylashtirish yani uni bir virtual mashinadagina ishlatish bunda shu virtual mashinada yagona signatur nusxasi va yagona yuritgich nusxasi bo'lib shu orqali boshqa virtual mashinalarni ximoyasini taminlashda qo'llaniladi. VMware kompaniyasi tomonidan ishlab chiqarilgan gipervizor va

unga yondashish standart xisoblandi. Ximoya virtualizatsiya vositalari va bulutli muxitdagi asosiy talablash shunga qaratilganki: xavfsizlikdagi chiqimlarni kamaytirish, resurslarga bo'lgan talablarni qisqartirish, ishlab chiqarishni ko'tarish va virtualizatsiya beradigan imkoniyatlaridan foydalanish - deb takidlaydi Denis Bezkorovayniy CSA (Cloud Security Alliance) kompaniyasi asoschisi va RISSPA (Russian Information Security Professional Association) kompaniyasi vitsa – prezidenti.

Misol qilib oladigan bo'lsak, virtualizatsiya xavfsizligini taminashda, virusga , xujum va taxdidlarga qarshi gipervizor darajasidagi vositalar ishlatilinadi. Shunday xavfsizlik yondashuvlar tarmoq pog'onasida xam qo'llaniladi. Tarmoqlar aro ekran, xujumni payqash va xatarlani aniqlash, xujumlardan ximoyalasnish – bunday ananaviy masalalardan foydalanishda tarmoq chegarasiga o'rnatilgan apparat taminoti orqali amalga oshiriladi. Virtualizatsiya tizimiga xizmat ko'rsatishda, agar admistratorlarga tegishli virtual mashinalar orasidagi trafik xavfsizligini taminlash kerak bo'lgan xollarda ikki xil yechim imkoniyati bor.

Birinchi echim shunga asoslanadiki, standart apparat taminotini olganda, virtualizatsiya muxitidan 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 yani ikkinchi yo'li masalalarni (yechimlarni) gipervizor darajasida joylashtirish mumkin. Bunday yechim virtual mashinalar o'rtasida kommunikatsiyalarni tekshirish va trafiklarni gipervizor darajasida yuzaga keladigan xujumlardan taxlil qilish orqali vazifasini bajaradi. Shuning uchun savdo bozorida virtualizatsiya muxiti uchun ishlab chiqarilgan yangi maxsulotlar paydo bo'lishni boshlaydi. Shubxasiz ular juda samarali ishlaydi va boshqarishdagi eng zo'r qulayliklarga ega bo'ladilar.

2.4. Bulutli texnologiyalarda axborot tahdidlari va kurashish metodlarining qiyosiy tahlili

Bulutli texnologiyalarda amalga oshiriladigan tahdidlar:	Bulutli texnologiyalardan noqonuniy va tartibsiz foydalanish.
Tahdid tafsiloti:	IaaS provayderlar cheksiz resurslarni iluziyalashni taminlaydi va ulardan foydalanish onson, tez amalga oshadi. Bu jarayon yangi istemolchilarni ro'yhatdan o'tishiga va kredit kartasi bor xar bir kishi ro'yhatga qo'yilishiga olib keladi. Ro'yhatdan o'tishning bunday oddiyligi spamerlar yani zararli kod mualiflari o'zlarini egri maqsadlari yo'lida bulutli servislardan foydalanish mumkin. Bunga o'xshash tahdidlardan faqatgina PaaS provayderlarigina zarar ko'rishgan lekin oxirgi tadqiqot natijalariga ko'ra xakerlar parollarni buzishda IaaS servislar , DDOS xujumlar, zararli kodni joylashtirish va bodnet tarmoqlarini yaratishdan foydalanishyabdi.
Amaldagi misollar:	IaaS servisdan bodnet tarmog'i yaratishda foydalanadi «troyan otlari, InfoStealer, Zevs» va boshqa zayifliklarni topib uni Microsoft Office va AdobePDF larga joylashtiradi.
Tahdidlarga qarshi kurashish metodlar:	- ro'yhatdan o'tish jarayonlarini takomillashtirish. - kredit kartalarini tekshirish va to'lov vositalarini ishlatishdagi monitoring jarayonlarini takomillashtirish. - tarmoq faoliyatidagi servis foydalanuvchilar ustidan umumtadqiqot ishlari olib borish.
Ishtrok etuvchi servis modellar:	IaaS; PaaS.

Bulutli texnologiyalarda amalga oshiriladigan tahdidlar:	Xavfsiz bo’lmagan dasturiy interfeyslar(API)
Tahdid tafsiloti:	Bulutli infratuzilma provayderlari dasturiy interfeyslar to’plamini istemolchilarga, resurslarni, virtual mashinalarni, servislarni boshqarish uchun beriladi. Butun tizim xavfsizligi ushbu interfeys xavfsizligiga bog’liq bo’ladi. Autentifikatsiya va avtorizatsiya tartibotidan boshlab, shifrlashgacha tugatish orqali dasturiy interfeys maksimal ximoya darajasini buzg’unchilar xujumlaridan ximoyalashni taminlash kerak bo’ladi.
Amaldagi misollar:	Interfeysdan anonim foydalanish yoki faktor autentifikatsiyasini qo’llash (parol yoki token) shuningdek xisob malumotlarini ochiq tarizda uzatish xavfsiz bo’lmagan dasturiy interfeyslarni yuzaga kelib chiqishiga sabab bo’ladi. API monitoringni qo’llanilish imkoniyatlari cheklash, tizim jurnali tuzilmaganligi, shuningdek turli servislar o’rtasida nomalum munosabatlar qaltisliklarni kelib chiqishiga sabab bo’ladi.
Tahdidlarga qarshi kurashish metodlar:	- bulut provayderi xavfsizlik modelini taxlilash - barqaror shifrlash algaritimi ishlatilinayotganligiga ishonch xosil qilish - ishonchli autentufikatsiya va avtorizatsiya metodi ishlatilayot ishonch xosil qilish - turli servislar orasidagi bog’liqliklarni tekshirish
Ishtrok etuvchi servis modellar:	IaaS; PaaS; SaaS

Bulutli texnologiyalarda amalga oshiriladigan tahdidlar:	Ichki buzg'unchilar.
Tahdid tafsiloti:	Ichki malumotdan noto'g'ri foydalanish juda xam xavfli xisoblanadi. Ko'pincha provayderlar tomonidan xodimlarning monitoring qilish tizimi amlaga oshirilmaydi, bu esa o'z navbatida buzg'unchilar mijozning xizmat faoliyatidan foydalanib, uning malumotlariga kirish imkoni beradi. Agar provayder xodimlar to'plami siyosatini ochiq tarizda olib borsa, bunda tahdid xavskor – xakker yoki uyushgan jinoiy tuzilmalar tomonidan amalga oshib, ular provayder xodimlari safiga kirib olishlari mumkin.
Amaldagi misollar:	Ayni paytda bunday foydalanishlar misollarda ko'rilmagan.
Tahdidlarga qarshi kurashish metodlar:	- ruxsatsiz kirishni aniqlash uchun kerakli qurilmalarni sotib olish va tegishli tizimdan foydalanish qoidalarini amalga oshirish kerak. - xodimlarni ishga qabul qilish qoidalarini tartibga solishda zaruriy shartnomalar tuzish. - provayder ichki tizimidagi audit xavfsizligi xisobotlarini, shaffof tizim xavfsizligi orqali yaratish.
Ishtrok etuvchi servis modellar:	IaaS; PaaS;SaaS;

Bulutli texnologiyalarda amalga oshiriladigan tahdidlar:	Bulutli texnologiyalardagi zayifliklar.
Tahdid tafsiloti:	IaaS servis provayderlari apparat resurslarni tizim virtualizatsiyasi orqali abstraksiyalab foydalanadi. Ammo apparat vositalari resurslarni ish xisoboti bilan ishlashga moslashtirilmagan bo'lishlari mumkin. Bu faktor tasirini minimallashtirish uchun, gipervizor virtual mashinani apparat resurslaridan foydalana olishini boshqaradi, lekin gipervizor xam jiddiy zayifliklarga duch kelishi mumkin. Yani foydalanishda imtiyozlarni oshib ketishi yoki fizik qurilmadan ruxsatsiz fodalana olishlardir. Bunday muomolardan qochish maqsadida virtual mashinalarni va tizimdagi muffaqiyatlarni payqash izolatsiya mexanizmlarini amalga oshirish kerak bo'ladi.
Amaldagi misollar:	Potensal zayifliklar to'g'risidagi misollar bor, bundan tashqari virtual muxitdan o'tadigan nazariy metodlar xam mavjud.
Tahdidlarga qarshi kurashish metodlar:	- eng ilg'or metodlarni o'rnatish va virtual muxitdagi xavfsizliklarni sozlashni amalga oshirish. - ruxsatsiz foydalanishlarni aniqlash tizimini ishga tushirish. - mamuriy ishlarni olib borishda autentifikatsiya va avtorizatsiya qoidalarini tuzish. - so'rovga ko'ra o'z vaqtida dasturlani yangilab turish. - zamonaviy skanerlash va zayifliklarni topish protseduralarini qo'llash.
Ishtrok etuvchi servis modellar:	IaaS;

Bulutli texnologiyalarda amalga oshiriladigan tahdidlar:	Malumotni yo’qolishi yoki sizib chiqishi.
Tahdid tafsiloti:	Malumotni yo’qolishi ko’p sabablarga ko’ra kelib chiqishi mumkin. Misol uchun, shifrlash kalitini qasddan yo’qotish bu shifrlangan axborotni qaytarilish imkoni bo’lmaydi. Malumot qismini yoki butun xolda yo’qotish, muxim axborotlarga ruxsatsiz kirish, yozuvni o’zgartirish xam misol bo’la oladi.
Amaldagi misollar:	Aytentifikatsiya, avtorizatsiya va audit qoidalarini noto’g’ri qo’llanilishi; shifrlash metodlarini noto’g’ri qo’llanilishi, qurilmalarni yetishmasligi malumotni yo’qolishiga va sizib chiqishiga sabab bo’ladi.
Tahdidlarga qarshi kurashish metodlar:	- ishonchli va xavfsiz API qo’llash - uzalilayotgan malumotlarni ximoyalash va shifrlash. - tizimni barcha bosqichlaridagi malumumotlarni ximoyalash metodlarini analiz qilish. - shifrlash kalitini boshqarishning ishonchli tizimini tashkil etish. - faqat eng ishonchli tashuvchilarni tanlash va sotib olish. - o’z vaqtida malumotlarni zaxira nusxalash.
Ishtrok etuvchi servis modellar:	IaaS; PaaS; SaaS;

Bulutli texnologiyalarda amalga oshiriladigan tahdidlar:	Shaxsiy malumotlarni o'g'irlash va servisdan ruxsatsiz foydalanish.
Tahdid tafsiloti:	Taxdidning bu turi yangi xisoblanmaydi. Bu taxdid bilan istemolchilar xar kuni duch kelishlari mumkin. Bunda buzg'unchining asosiy maqsadi istemolchining logini va paroli xisoblanadi. Bulut tizimi nuqtai nazaridan istemolchilarning logini va parolini o'girlash provayderning bulut infratuzilmasidagi saqlanilayotgan malumotlarga xavf extimolligini oshiradi. Shu orqali buzg'unchilarning vakolat imkoniyatlari oshadi.
Amaldagi misollar:	Xozirgacha misollar ko'rib chiqilmagan.
Tahdidlarga qarshi kurashish metodlar:	- qayd yozuvlarini uzatishdan cheklash. - ikki faktorli autentifikatsiya metodini qo'llash. - ruxsatsiz foydalanishda faol monitoringni amalga oshirish. - bulut provayderi xavfsizlik modulini bayoni.
Ishtrok etuvchi servis modellar:	- IaaS - PaaS - SaaS

Bulutli texnologiyalarda amalga oshiriladigan	Bulutli texnologiyalardagi etiborga olinmaydigan tahdidlar.

tahdidlar:	
Tahdid tafsiloti:	Bulutli texnologiyalarni biznes sifatida taqdim etilayotganda, kompaniya asosiy etiborni IT infratuzilma va bulutli servis provayderlariga qaratadi. Ammo bunday yondashishda xavsizlik taminlash xaqida sovol kelib chiqadi. Bulutli provayder o'zining servisni reklama qilayotganda aniq amalga oshirish detallaridan tashqari, barcha imkoniyatlarini yoritib o'tadi. Bu esa o'z navbatida jiddiy tahdidni yuzaga kelib chiqaradi, ichki infratuzilmasini bilgan buzg'unchi ximoyalanmagan zayiflikka xujum amalga oshiradi.
Amaldagi misollar:	- Amazon kompaniyasi EC2 cloud audit xavfsizligidan voz kechishi. - DT ishlov berishdagi zayiflik, malumotlar markazi Hearthland tizim xavfsizligi buzulishga olib kelgan.
Tahdidlarga qarshi kurashish metodlar:	- Jurnal malumotlarini oshkor qilish - Butun yoki qisman tizim arxitektura malumotlarini va DT ornatishdagi detallarni oshkor qilish. - Zayifliklarga qarshi monitoring qo'llash.
Ishtrok etuvchi servis modellar:	IaaS;PaaS;SaaS

3. Hayot faoliyati xavfsizligi va ekologiya

Fan va texnika taraqqiyoti, ijtimoiy – iqtisodiy xavfsizlikni oshirib, shu bilan birga aholi salomatligi uchun bo'lganidek, atrof-muhit uchun ham xavfsizlikning yangi turlari vujudga kelishiga olib keldi.

Hozirgi zamon ishlab chiqarishdagi jarayonlarni bajarishda ko'plab mashina va uskunalar ishlatiladi. Ularga aloxida–aloxida xavfsizlik talablari ishlab chiqarilgan. Shu boisdan bo'lg'usi kadrlarni tayyorlashda hayot faoliyati xavfsizligi masalalarini qismlarini ma'ruza matnida bayon etish lozim. Hayot faoliyat xavfsizligi fanini o'rganishda texnik, fizik-kimyoviy, tibbiy, biologik, qishloq xo'jaligi, xuquqiy va boshqa fanlarning yutuqlariga asoslanish zarur. Xalq xo'jaligining texnik jixatdan takomillashtirish, mexanizasiyalashtirish, avtomatlashtirish, kompyuterlar bilan ta'minlash, yangi turdagi energiyalardan foydalanish, qishloq xo'jaligini kimyoviy mineral o'g'itlar bilan ta'minlash va boshqa mehnat tizimida ham sifat ko'rsatkichlarini yuqori bo'lishini ta'minlash kerak.

3.1. Mehnat muhofazasining huquqiy masalalari

Mehnat muhofazasining huquqiy masalalari davlatimizning asosiy Qonuni – O'zbekiston Respublikasi Konstitusiyasi bilan tartibga solinadi. Konstitusiya fuqarolar huquq va majburiyatlarini, mehnat va dam olish huquqlarini, keksalikda moddiy ta'minotga va mehnatga layoqatsizlik holatida nafaqa to'lovlari hamda davlat ijtimoiy sug'urta mablag'lari…"[10] evaziga to'lovlar huquqlarini belgilaydi.

Ijtimoiy sugurta mablaglari respublikamiz kasaba uyushmalari va ijtimoiy ta'minot vazirliklari ixtiyoridadir.

Qonunchilik asoslarida mehnat muhofazasi to'g'risidagi asosiy nizom ham bor. Unga muvofiq ishlab chiqarishda jarohatlanishlar va kasbiy kasalliklarni oldini olish, ogohlantirish korxona ma'muriyatining majburiyati sanaladi. Ishlab chiqarish jarohatlarini va kasbiy xastaliklari haqida ogohlantirish, ishlab chiqarish va maishiy xonalar, ish o'rinlarini jihozlash, texnologik jarayonlarni tashkil qilish, MX qoidalari va sanitariya qonunlariga muvofiq ishlayotganlarni himoya qilish

kabi tadbirlarni o’z ichiga oluvchi mehnatning xavfsiz va bezarar sharoitlarni ta’minlashga asoslangan.

Korxona, sex, hudud agar mehnat muhofazasi talablariga javob bermasa, ishga tushirilishi mumkin emas.

Agar ishlatilayotganda mehnatning bezarar sharoitlari ta’minlangan bo’lmasa, mexanizmlar, asboblar va mashinalar turkum ishlab chiqarishga kiritilmaydi.

Korxona ma’muriyati ishchi va xizmatchilarni ishlashning xavfsiz uslublariga o’rgatilishi, mehnat sharoitida zarar uchun korxonalarda ishlayotganlarni zarur narsalar, maxsus kiyim-boshlar, maxsus poyafzallar va boshqalar bilan ta’minlashi shart.

Misol uchun, akkumulyatorchilar; kostyumlar, rezina yarim bo’tiklar, fartuklar, ko’zoynaklar, qo’lqoplar bilan taminlanadilar.

Zararli ishlab chiqarishda band insonlar salomatligi va mehnatga qobiliyatlarini saqlash uchun qisqartirilgan ish haftasi, qo’shimcha ta’til belgilanib, belgilangan me’yorlar bo’yicha doimiy davolash-profilaktika, sut, oziq-ovqat beriladi.

Agar ishlar yilning sovuq paytida ochiq havoda bajarilsa, u holda ishchilar va xizmatchilarga ish vaqtida isinish uchun, dam olish uchun tanaffuslar beriladi. Ayrim toifadagi xodimlar (ro’yxat bo’yicha) har yili tibbiy ko’rikdan o’tadilar.

Ayniqsa, ayollar va o’smirlar mehnati alohida muhofazaga muhtoj. Aloqa tarmog’ida barcha ishlayotganlarning 80 foizga yaqini ayollardan iborat.

Ishlab chiqarishda qo’yidagi ish turlari bajarilayotganda ayollar mehnati ta’qiqlanadi:

1. Qo’rg’oshin akkumulyatorlar tayyorlash va payvandlash;
2. Polietilen va polivinilxlorid qobiqlardagi kabellarni svarkasida (kovsharlashda);
3. Pnevmoasboblar yordamida teshiklar qilish;
4. G’o’la, daraxtlarni sug’urish;
5. Quduqlar kovlash;

6. Liniya va antenna tayanchlarida ishlash.

Hmilador ayollar va go’dak farzandlarini tarbiyalayotgan ayollar davlatimizning yuksak g’amxo’rligi ostida. Ularni tungi vaqtlarda, ishdan tashqari ishlarga jalb qilish, bayram va dam olish kunlarida band etish, shuningdek, ularni roziligisiz xizmat safarlariga jo’natish ma’n etiladi.

Voyaga yetmaganlarga ham davlatimiz g’amxo’rlik ko’rsatib keladi, ya’ni 18 yoshga yetmaganlarga. Yigit va qizlar 16 yoshdan, istisno tarzda korxona kasaba fo’mitasi roziligi bilan 15 yoshdan ishga qabul qilinadi.

Voyaga yetmaganlarning barchasi albatta ishga qabul qilinishdan avval dastlabki tibbiy ko’rikdan o’tadilar, so’ngra 18 yoshdan boshlab har yili tibbiy ko’rikdan o’tashlari shart.

O’smirlarni og’ir, yer osti ishlarida hamda zararli va xavfili ishlarda, balandlikka ko’tarilish (liniya va antenna tayanchlarida) kabi ishlarda ishlatish ta’qiqlanadi.

Og’ir yuklarni ko’tarishdagi me’yor chegaralar:

16 yoshdan 18 yoshgacha bo’lgan o’smirlar uchun – 16 kilogramm

16 yoshdan 18 yoshgacha bo’lgan qizlar uchun – 10 kilogramm

15 yoshlilarning og’ir yuklar ko’tarishiga yo’l qo’yilmaydi.

18 yoshgacha bo’lganlarni tungi vaqtda, ish vaqtidan tashqari, bayram va dam olish kunlari ishlarga jalb qilish ma’n etiladi. O’smirlar uchun ish haftasi qisqartiriladi.

15 – 16 yosh – 24 soat (haftasiga)

16 – 18 yosh – 36 soat.

Ish haki, to’liq ish kuni uchun to’lanadi. Ta’til olish uchun imtiyozlar yozda yoki ularning ixtiyoriga ko’ra yilning boshqa davrida 1 kalendar oy davomiyligida beriladi.

Yoshlarning ishga joylashishi bilan, hokimiyatlardagi mehnat – ishga joylash bo’yicha komissiyasi bilan voyaga yetmaganlar ishlari bo’yicha komissiyaci shug’ullanadi.

O’smir jo’natilgan korxona ma’muriyati uni ishga joylashtirishi shart, chunki, korxonada voyaga yetmaganlarni ishlab chiqarish ta’limi va ishlashi uchun ma’lum o’rin soni ajratiladi.

O’smirlarni ishdan bo’shatish hokimiyat huzuridagi voyaga yetmaganlar ishlari bo’yicha komissiya roziligisiz amalga oshirilmaydi.

Oliy o’quv yurtlari, hamda o’rta maxsus o’quv yurtlarining sirtqi bo’limlarida ta’limlarini ish bilan birgalikda olib borayotgan ishchilar va xizmatchilar ham imtiyozlarga egadirlar.

Har yili ularga laboratoriya imtihon sessiyalari uchun to’lanadigan ta’tillar beriladi. Oliy o’quv yurti yoki texnikum manziliga borish – kelish yo’l kira haqining 50 foizini ma’muriyat to’laydi. Haftada 1 ozod kun (ish kuni) 50 foiz to’lanadi.

3.2. Elektromagnit nurlanishlarning inson organizmiga ta’siri

Elektromagnit nurlanishlar turli chastotalarda, aloqa tarmog’ida keng qo’llaniladi. Radiotexnik qurilmalarda antennaga generatorlar, antenna qurilmalari, yuqori chastotali transformatorlar, fider yo’nalishlar, materiallarni termik ishlov terish uchun qurilmalarda – elektromagnitlar, kondensatorlar elektromagnit nurlanish manbai sanaladi…”[11] ko’rsatilgan qurilmalar ishida ularni o’rab turgan makonida elektromagnit maydonlar bunyod bo’ladi. Elektromagnit maydonlarning foydali harakati bilan bir qatorda inson tanasiga kirib, unga noqulay, salbiy ta’sir qo’rsatishi va kasbiy kasalliklarga sabab bo’lishi mumkin. Ular asab, endokrinologik va yurak-qon tomirlari tizimi kasallanishini chaqirishi mumkin, insonda qon bosimi pasayadi, pulsi sekinlashadi, reflekslar tormozlanadi, qon tarkibi o’zgaradi. Elektromagnit maydonlar ta’siri organizmga issiqlik ta’sirida o’z aksini berishi mumkin. Inson tanasi tomonidan ichga yutilgan elektromagnit maydonlar quvvati tanani va ayrim organlarni qizishini yuzaga keltirib, issiqlikka aylanib, kasalliklarga olib kelishi mumkin. Tananing 10 S dan ziyod isib ketishiga yo’l qo’yib bo’lmaydi.

Ayniqsa, miya, ko’z, ichak, buyrak va urug’donlar elektromagnit maydonlar ta’siriga yo’naladi. Elektromagnit maydonlarining ta’siri subyektiv bunyod bo’lishi

juda toliqish, bosh og’riq, jizzakilikda, seruyqulik, nafas siqishi, ko’rish qobiliyatining yomonlashuvi, tana haroratining ko’tarilishida o’z ifodasini topadi.

Elektromagnit maydonlar ta’sirida zararlanish darajasi nurlanish sur’ati, harakat chastotasi davriga bog’liq. Elektromagnit maydonlar sur’ati, harakat chastota va davri qanchalik ko’p bo’lsa, inson organizmiga ta’siri shunchalik kuchli bo’ladi.

Elektromagnit maydonlarning insonga zararli ta’sirlarini ogoxlantirish maqsadida ish joylarida elektromagnit maydonlar energiya oqimi mustahkamliligi

(EOM) va keskinlashuvning imkon qadar ahamiyati belgilaniladi. Yuqori chastotalar va ultra yuqori chastotalar to’lqinlari, diapazonlari, diapazonlari uchun elektrik (Ye) va elektromagnit maydonlari barpo qiluvchi magnit keskiplik me’yorlashtiriladi. O’ta yuqori chastotalar to’lqinlari, diapazonlari uchun W organizmga energetik yukning kerakli ahamiyati va T nurlanish zonasida bo’lish vaqtidan kelib chiqib, belgilanadigan elektromagnit maydonlarning quvvat oqimi imkon qadar kerakli mustahkamlilikni me’yorlaydi.

Energiya oqimi mustahkamligi

EOM =W/T

Xodimning ish joylarida va bo’lishi ehtimoli bor joylarda elektromagnit maydonlar quvvat oqimining imkon qadar kerakli bo’lgan mustahkamliligi 300 MGs chastota diapazonida – 300 GGs bo’ladi.

Imkon qadar kerakli bo’lgan mustahkamlilik < = 10 Vt/m^2 yoki 103 mkVt/cm^2, ish joylarida, binolarida rentgen nurlanishi yoki havo haroratining balandligida > 280C – 1 Vt/m^2 yoki 100 mkVt/cm^2 .

Nurlanish jadalligi ustidan nazorati yiliga kamida 1 marta o’tkazilishi kerak, shuningdek, yangi yoki eski generator qurilmalar ishga tushirilishi yoki ta’mirlanishi va mehnat sharoitlari o’zgarishida o’tkaziladi. O’lchov poldan 0,5 – 1 – 1,7 m masofada 3 nuqtadagi maksimal – quvvatda o’tkaziladi.

Elektromagnit maydonlarni tashkil qiluvchi elektromagnit o’lchovlar uchun 1 – IEMP asbobidan, quvvat oqimi mustahkamliligini o’lchash uchun esa, 1-PO, 3-PO, 9 – PO, 13 – PO asboblaridan foydalaniladi. Shu asboblar yordamida

elektromagnit maydonlar jadalligi imkon qadar kerak bo’lgan me’yorlardan oshadigan hududni aniqlash va tegishli himoya choralarini ko’rish mumkin.

Elektromagnit maydonlarni ta’siridan himoyalashning asosiy usullari va vositalariga quyidagilar taalluqli:

1. Himoyalashning tashkiliy choralari.

2. Manbadan nurlanishning jadalligini kamaytirish.

3. Nurlanish manbaining ekranlashuvi.

4. Nurlanish manbaidan ishchi o’rinlarini ekranlashtirish va yoki holi qilish.

5. Signalizasiya vositalarini qo’llash.

6. Individual himoya vositalarini qo’llash.

Ishning muayyan sharoitlariga bog’liq tarzda shu vositalardan 1 yoki ularning ixtiyoriy kombinasiyasi qullanilishi mumkin.

1. Tashkiliy choralar – uskunalarning rasional joylashuvi, qurilmalar va xizmat ko’rsatilayotgan personal ishi muayyan rejimini belgilashdir.

Yuqori chastotalar va o’ta yuqori chastotalar qurilmalari ishiga tibbiy ko’rikdan o’tgan 18 yoshdan kichik bo’lmagan, texnika xavfsizligi bo’yicha o’qib, imtihon topshirgan shaxslarga ruxsat etiladi. Har yili xizmat ko’rsatayotgan personal tibbiy ko’rikdan o’tkaziladi.

Agar ish yuqori xavfli sharoitlarda, nurlanishda, ketayotgan bo’lsa, xodimlar uchun qisqartirilgan ish kuni va qo’shimcha ta’til belgilanadi.

2. Kelishgan yuklar, quvvat yutuvchilar qo’llovida, manbay nurlanishi jadalligini kamaytirilishga erishiladi.

O’ta yuqori chastotalar generatorlarini regulirovka qilish va sinashda, peredatchiklarning chastota va amplituda tavsifnomalarini olishda oxirgi atalgan antennaga emas, balki elektromagnit to’lqinlar o’chadigan nagruzkaga ulanadi.

Shu tariqa ularning antenna orqali atrof-muhitga nurlanishi mustasnodir. Hozirgi paytda qo’llaniladigan kuch (antenna ekvivalenti) yuqori chastotalar - quvvatni 40-60 Db ga kuchsizlantirish imkonini beradi.

Qabul qilish, indikator, antenna-fider traktlari, avtomatika va radiostansiya boshqaruv tizimlari ishini tekshirishda signallarning kam quvvatli imitatorlaridan

foydalanish mumkin. Bu holatda uzatuvchi qurilmadan tashqari stansiyalarning butun tizimi ishlaydi. Bu esa ishlayotganlarning nurlanish extimolini istisno etadi.

3. Nurlanish manbai maxsus ekranlar yordamida ekranlashtiriladi. Ekranlarning himoya xossalari turli materiallar bilan elektr magnit nurlanishlarning aks etishi va yutilishiga asoslanadi.

3.3. Ekologik inqirozni bartaraf qilish

Hozirda mavjud ekologik muammolarni hal qilishda ikki xil yo'l bilan yondashilinadi. Texnologik yondoshish va ekosentrik yondashishdir. Texnologik yondoshish ekologik muammolarni hal qilishning texnologik choralari asosiy, deb hisoblaniladi va tabiatning imkoniyatlari, qonuniyatlari yetarlicha e'tiborga olinmaydi…"[12]Tabiiy boyliklardan foydalanishda texnologik qudrat hal qiluvchi rol o'ynaydi. Texnik imkoniyatlar yordamida biosfera barqarorligini tiklash. ekologik muammolarini hal qilish mumkinligi ta'kidlaniladi.

Ekologik yondoshishda tabiatdagi qonuniyatlarni hisobga olish, mavjud tabiiy ekotizimlarni asl holida saqlab qolish ustivor vazifa hisoblaniladi.

Ekologik inqiroz deganda atrof-muhitga inson ta'sirining me'yoridan ortishi natijasida munosabatlarini keskinlashuvi holati tushuniladi. Ekologik inqirozni bartaraf qilish uchun insonlarning ahloqiy poklanish, yangilanish hayotiy zaruriyatdir. Buning uchun har bir inson tafakkurini, ongini ekologiyalashtirish, mavjud ta'lim tizimini qayta tiklash, yangi madaniyatni shakllantirish talab qilinadi.

XX1 asrga kelib, ekologik ta'limdan barqaror rivojlanish uchun ta'limga o'tish hayotiy zarur masala bo'lib qoldi. Insonlarning ayrim ehtiyojlaridan voz kecha bilish, tabiatga jonkuyar bo'lish biosfera barqarorligini saqlab qolishning asosiy shartlaridan biri bo'lib hisoblaniladi.

Ta'lim, madaniyatni rivojlantirish, milliy, umuminsoniy qadriyatlarni tiklash mavjud muammolarini hal etishda yetakchi rol o'ynaydi.

Insonlarni biosferaga salbiy ta'sirlarini kamaytirish, tabiiy resurslardan oqilona foydalanish, barqaror rivojlanishni ta'minlash hayotiy zaruriyatdir. Bu dolzarb masalani hal qilishda aholining ekologik savodxonligini oshirish muhim

ahamiyatga egadir. Ekologik ta’lim va tarbiyani tegishli darajada yo’lga qo’yilgan va atrof-muhitni muhofaza qilish uchun yetarlicha mablag’ sarflanadigan mamlakatlarda inqiroz vaziyatlari tugatila boshlangan va barqaror rivojlanish yo’liga o’tilgan.

Ekologik muammolar O’zbekistonda ham dolzarb bo’lib, Respublikamizdagi ekologik vazifalar o’ziga hos milliy hususiyatlarga ega, ularga quyidagilarni – aholinig 20 % ortig’ining kasallanishi ekologik vaziyatning yomonligiga bog’liq bo’lib qolmoqda. Shu bilan urbanizasiya, Orol dengizining qurib qolishdan asrash muammolari bilan bog’liq loyhalashdan iborat.

Yerning cheklanganligi va uning sifat tarkibi pastligi bilan bog’liq xavf to’xtovsiz ortib bormoqda. Yerning nihoyat darajada sho’rlanishi biz uchun ulkan ekologik muammodir. Yerni ommaviy suratda o’zlashtirilishi, hatto sho’rlangan va melorasiyaga yaroqsiz yirik-yirik, yaxlit maydonlarni ishga solish ham ana shunday noxush oqibatlarga olib keldi.

Paxta maydonlarining ko’paytirilishi paxta monopoliyasi yerlarning kuchsizlantirishga, tuproqning unumdorligini pasayishiga, hamda tuproqning buzilishiga va nurashiga olib keldi.

Noorganik moddalarni, gerbisidlarni va pestitsidlarning qo’llanishi me’yoridan o’nlab barobar ortib ketishi, tuproqni daryo, ko’l, yer osti suvlarni ifloslanatiradi. Yangi yerlarni o’zlashtirishda yangi texnologiyalardan foydalanmaslik, paxtalarni nazoratsiz sug’orish ishlari, tuproq namligini oshirishga sabab bo’la boshladi va oqibatda tuproqni qayta sho’rlanishiga sabab bo’ldi.

O’zbekiston Respublikasining Prezidenti I.A.Karimovning ta’kidlashicha…”[13] “ekologiya hozirgi zamonnning keng miqyosdagi keskin ijtimoiy muammolaridan biridir. Uni hal etish barcha xalqlarning manfatlariga mos bo’lib, sivilizasiyaning hozirgi kuni va kelajagini ko’p jihatidan ana shu muammolarni hal etishga bog’liqdir”.

Demak, tabiatni muhofaza qilish ekologik talablarga doimo muammolarni oldini olish, ekologik talablarga doimo rioya qilish, mustaqil davlatimizning ijtimoiy – iqtisodiy, huquqiy masalasi bo’libgina qolmay, balki ekologik

siyosatining asosiga aylanishi lozim. Chunki ushbu muammolar mustaqil davlatimiz ravnaqi bilan bevosita bog'liqdir.

I.A Karimovning BMT Bosh Assambleyasining "Ming yillik sammiti"sida so'zlagan nutqida Markaziy Osiyo, jumladan O'zbekistondagi ekologik muammolarga alohida e'tibor qaratdi.

1997 yil 29 avgustdagi O'zbekiston Respublikasi Oliy Majlisining "Jamiyatda xuquqiy madaniyatni yuksaltirish milliy dasturi to'g'risida"gi qarori va O'zbekiston Respublikasining "Ta'lim to'g'risida"gi qonuni O'zbekiston Respublikasi Vazirlar Mahkamasining "Jamiyatda xuquqiy madaniyatni rivojlantirish milliy dasturini amalga oshirish chora –tadbirlari to'g'risida"gi 1998 yil 29 may qarorlari ham bozor iqtisodiyati sharoitida ekologik xuquqiy ta'lim va tarbiyaga alohida e'tibor berishni, aholini, ayniqsa yoshlarimizning ekologik madaniyatini, ma'naviyatini zamon talabi, dunyo andazalari darajasiga yetkazishni taqazo qiladi.

Ekologiya yunoncha so'z bo'lib, uning ma'nosi tirik mavjudodlarning yashash sharoiti yoki tashqi muhit bilan o'zaro munosabatni bildiradi.

Ona tabiat muhofazasini bir me'yorda boshqarishni tashkil etish, rivojlantirishda insonning ekologik ongi o'sib borishi katta ahamiyatga ega.

Atrof-muhit muhofazasini tashkil etish va amalga oshirishda turli chora tadbirlarni qo'llash bilan birga ona tabiatni, jamiyatning barcha a'zolariini eng yosh fuqarolaridan keksa kishilarigacha asrab – avaylashga, ularga nisbatan ongli munosabatda bo'lishga, tabiat manbalarini tejab tergashga, me'yorida foydalanish, salbiy, fojiaviy hollarining oldini olish, saqlab qolish uchun chora-tadbirlar izlash, xullas atrof-muhitni doimo pok saqlashga muntazam da'vat etish benihoya ulug'vor vazifadir.

Haqiqatdan ham, ekologiya - bu poklik, ozodalik toza zamin, ob- havo, suv, qolaversa, ona tabiatning eng ongli a'zosi – insonning ijobiy tabiati, fe'l- atvori demaqdir.

Har qanday jamiyatda ham insonni ekologik jihatidan tarbiyalash umumiy ta'lim-tarbiyaning mas'uliyatini oshirish va yanada mustaxkamlashga yordam

beradi. Aholi ongiga ”tabiat-bu men va sen. Biz yashaydigan makon, tabiat butun Yer kurrasi mavjudotlari yashaydigan yagona zamin” degan asosiy nazariy va amaliy bilimlarni singdirish lozimdir. Zero, hayot kishilardan atrof-muhitni nafaqat bugungi kun uchun, balki kelajak avlod uchun ham asrash talab qilmoqda. Jahonning barcha mamalakatlarida ekologik muammolarni o’rganish borasidagi ilmiy izlanishlar xalq sog’lig’ini saqlash uchun qilingan hayrli ishlardan hisoblanadi.

Insonlarning ta’siri biosferaning sig’imidan oshib ketmasligi, tabiiy resurslardan oqilona foydalanishga erishish, barqaror rivojlanishni ta’minlash hayotiy zarurdir. Bu dolzarb maslalarni hal qilishda aholining ekologik savodxonligini oshirish muhim ahamiyatga egadir. Ekologik ta’lim va tarbiya tegishli darajada yo’lga qo’yilgan va atrof-muhitga muhofaza qilish uchun yetarli mablag’ sarflanadigan mamlakatlarda inqiroz vaziyatlari tugatiladi va barqaror rivojlanish yo’liga o’tiladi.

Xulosa

Ushbu bituruv malakaviy ishining asosiy maqsadi bulutli texnologiyalarda amalga oshiriladigan taxdidlar va ularga qarshi kurashish metodlarining qiyosiy taxlili xisoblanib, bunda biz taxdidlarni yetti xil turi, xar bir taxdid tavfsifi va ularga qarshi kerashish metodlari, shu tahdidlarda ishtrok etuvchi servis modellari va ularni amaldagi misollar orqali tahlil qilindi. Bulutli texnologiyalardagi modellar va ularning axborot xavfsizligini ta'minlash darajalari keltirildi.

Bundan tashqari tizim axborot xavfsizligini taminlashning huquqiy, tashkily, texnik va iqtisodiy metodlari ko'rib chiqildi.

Bulutli texnologiyalarda axborot ximoyasining ikki xil turi ko'rib chiqildi.

- uskunalar xavfsizligni oldini olish
- malumotlar xavfsizligi

Blutli texnologiyalarda amalga oshiriladigan hujumlar:

- DT da ananviy xujumlar
- Bulut elementlarida funksional xujumlar
- Mijozjlarga xujumlar
- Gipervizorda xujumlar
- Boshqarish tizimidagi xujumlar

Ularni bartaraf etish usullari:

- Malumotlarni saqlash. Shifrlash
- Uzatishdagi malumotlar xavfsizligi.
- Autetifikatsiya.
- Istemolchilarni izolatsiyalash.

Vaqt o'tishi bilan birga bulutli texnologiyalardan foydalanishdagi tajribalar oshib bormoqda, xar bir tahdidlarga, xujumlarga , zayiflik va tushunmovchiliklarga chora tadbirlar ishlab chiqilyapti, ko'pgina kamchiliklar bartaraf etilib, foydalanishdagi bir qancha yangiliklar va qulayliklar yuzaga kelmoqda, bulutli xisoblash texnologiyalari jamiyat va davlatning barcha soxalarda o'z o'rni topib kelmoqda, buning natijasida bulutli texnologiyalar mukammal tizim sifatida rivojlanishiga katta turtki bo'lmoqda.

Foydalanilgan adabiyotlar ro'yhati.

1. O'zbekiston Respublikasining Prezidenti I. KARIMOV Toshkent sh., 2002 yil 12 dekabr 439-II-son «AXBOROT ERKINLIGI PRINTSIPLARI VA KAFOLATLARI TO'G'RISIDA» dagi qarori.
2. Axmedova O. «Axborot xavfsizligiga oid terminlarning ruscha-o'zbekcha izoxli lug'ati» Toshkent, fan nashriyoti, 2009.- b.54.
3. Amirov D.M. , Atajonov A.Y. , Ibragimov D.A. , Raximjonov Z.Y. , Saidxo'jayev S.S. «Axborot – Kommunikatsiya texnologiyalari izoxli lug'ati» BMTTD ning O'zbekistondagi vakolotxonasi, 2010.- b.320.
4. Internet/Universitet Axborot texnologiyalari http://www.intuit.ru/department/security/secbasics/1/secbasics_1.html
5. Хореев П.В. Методы и средства защиты информации в компьютерных системах. – М.: издательский центр "Академия", 2005. – с. 205.
6. http://www.cnews.ru/reviews/new/oblachnye_servisy_2013/articles/zashchishchaem_oblachnuyu_sredu_novye_tehnologii_bezopasnosti/
7. http://bureausolomatina.net/ru/themes_in_progress/clouds/6
8. www.ec.europa.eu/justice
9. www.enisa.europa.eu
10. Муравей Л.А. Экология и безопасность жизнедеятельности. М.: ЮНИТИ-ДАНА, 2000. - 447 с
11. Белов С.В. Безопасность жизнедеятельности. , Высшая школа, 2007. 616 с.
12. Yormatov G'.Yo., Isamuxamedov Yo.U. Mehnatni muxofaza qilish. Darslik. O'zbekistan nashriyoti. Toshkent 2002. – b.47.
13. Karimov I.A. O'zbekiston XXI asr bo'sag'asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqqiyot kafolatlari. – Toshkent: «O'zbekiston». 1997 y.