KIBERXAVFSIZLIK EVOLUTSIYASI KIBERXAVFSIZLIK MAQSADLARI

Radjabova Madina Shavkatovna, Mirzanazarov M. Sh
Yusupova S.M, Amonov A.H
Abdullayev I.K, Bekbayev J.R
Hafizov Sh.F
Toshkent axborot texnologiyalari unversiteti
abdujabbor.madina.1989@gmail.com[1]

Anatatsiya: *kibermakonning odatiy hayotga kirib kelishi natijasida xavfsizlikning yanada mukammal raqamlashtirilgan darajasi, kiberxavfsizlik tushunchalarining insonlar hayotiga kirib kelishi hamda uning odatiy hayotga ta'sirini o'rgangan holda kiberxavfsizlikni ta'minlash mumkin.*

Kalit so'zlar: *kibermakon, kiberxavfsizlik, avtomatlashtirish, diffuziya – chalkashtirish, tarmoq texnologiyalari, kibermakon arxitekturasi.*

Kiberxavfsizlik siyosatini tushunish uchun kiberxavfsizlik qanday rivojlanganligi haqida tushinchaga ega bo'lishimiz kerak. Kompyuterlar birinchi avtomatlashtirilgan jarayonlarni ishga tushirganda, bunday loyihalarning barchasida asosiy maqsad inson kalkulyatorlarini aniqroq natijalarni beradigan avtomatlashtirilgan dasturlarga almashtirish natijasida unumdorlikni oshirish edi. Ko'proq dasturiy ta'minot mavjud bo'lganda, kompyuterlarning unumdorlik afzalliklari oshadi. Internetning joriy etilishi, ma'lumotlarni tez va to'g'ri uzatish imkonini berib, unumdorlikni yanada oshirdi. Bu to'g'ridan-to'g'ri biznes operatsiyalarini onlayn tarzda qayta ishlash imkoniyatiga olib keldi. Bu qobiliyat elektron tijorat deb nomlandi. 2000-yilga kelib, iqtisodiyot elektron tijoratga shunchalik qaram bo'lib qoldiki, u tez-tez kiber jinoyatchilar nishoniga aylandi va xavfsizlik texnologiyasi firibgarlik operatsiyalarini amalga oshirish uchun ishlatilishi mumkin bo'lgan ma'lumotlarni himoya qilish uchun rivojlandi. Bunday texnologiya odatda *qarshi choralar* deb ataladi, chunki ular ma'lum bir tahdidga qarshi turish uchun mo'ljallangan xavfsizlik choralaridir. Bugungi kunda kiberxavfsizlik texnologiyasining rivojlanishi dunyoda kiber qurollanish poygasini keltirib chiqardi, bunda qarshi choralar ortda qolmoqda.

Kiberxavfsizlik tarixi 1960-yillarda meynfreymdan boshlanadi. Bu elektron ma'lumotlarni qayta ishlash tizimlaridan investitsiya daromadini ko'rish uchun korxonalar uchun yetarlicha arzon bo'lgan birinchi kompyuter edi. Bu vaqtgacha "kompyuter" so'zi hisob-kitoblarni amalga oshiruvchi shaxsni

nazarda tutgan va “kiber” so‘zi ilmiy fantastika sohasi edi. O‘sha kunlarda kompyuterlar qo‘riqchilar va maxsus usullar bilan himoyalangan. Jismoniy xavfsizlik tartib-qoidalari faqat kompyuterlarda ishlashga ruxsat berilgan odamlarning ularga jismoniy kirishini ta’minlash uchun ishlab chiqilgan. Kompyuterlar shunchalik katta ediki, yuzlab kvadrat fut maydonlar maxsus xavfsizlik xodimlari bilan ishlashi uchun moslashtirilardi. Qo‘riqchi funktsiyasi ba’zan kompyuter operatori roli bilan birlashtirilib, ishni boshqarish bo‘yicha texnik deb atalardi. Kompyuterdan foydalanishi kerak bo‘lgan odamlar o‘z ma’lumotlari va dasturlarini perfokartalar to‘plamida ushlab, qo‘riqchi oldida navbatda turishardi. Qo‘riqchi foydalanuvchining kompyuterdan foydalanishga ruxsatini tekshiradi, kartalar to‘plamini oladi va uni kartalardagi teshiklarni bit va baytlarga avtomatik ravishda tarjima qiladigan kartani o‘quvchiga joylashtiradi (Schacht 1975). 1960-yillarning oxiriga kelib, masofadan ulanish orqali asosiy kompyuterga kabel orqali ulangan bir nechta ofis joylaridan perfokartalarni qabul qilish imkoni yaratildi. Keyin kompyuter xavfsizligi xodimlari ushbu kabellarni baland pollar ostida, devor bo‘shliqlari va uzatish kanallari orqali vakolatli shaxs boshqa uchida o‘tirganiga ishonch hosil qilish uchun qo‘shimcha mas’uliyatga ega edilar.

Ushbu dastlabki avtomatlashtirilgan kompyuter tizimlarining menejerlari xavfsizlik xavfini juda yaxshi bilishgan, ammo konfidentsiallik, yaxlitlik (butunlik), foydalanuvchanlik triadasi hali sanoat standarti emas edi. Harbiy va razvedkadagi bir nechta qurilmalardan tashqari, konfidentsiallik asosiy xavfsizlik talabi emas edi. Garchi korxonalar mijozlar ro‘yxatini maxfiy saqlashni xohlashsa-da, turli sinovlardan o‘tmagan dasturiy ta’minot doimo ishlamay qolar edi, shuning uchun ularning asosiy tashvishi konfidentsiallik emas, balki yaxlitlik edi. Ma’lumotlarning yaxlitligidagi halokatli xatolarga olib kelishi mumkin bo‘lgan inson xatosi ehtimoli har doim kompyuter dasturlarini ishlab chiqish va operatsiyalarida aniq bo‘lgan. Dasturiy ta’minot muhandisligi tashkilotlari xavfsizlik signalini birinchi bo‘lib ko‘tardilar, chunki kompyuterlarda noto‘g‘ri ishlash hayotni xavf ostiga qo‘yishi mumkin bo‘lgan tizimlarni boshqarishni boshladi (Ceruzzi 2003). Bundan tashqari, moliyaviy firibgarlik ko‘rinishidagi kompyuter jinoyati 1970-yillarning boshlariga kelib keng tarqalgan bo‘lib, uni badiiy adabiyot va televideniyening asosiy oqimiga aylantirdi (McNeil 1978). Xavfsizlik tahdidlari doirasidan inson omili yo‘q qilingan deb hisoblasak ham, tizimdagi nosozliklar kompyuter tizimidagi vakuum naychalari orasida aniqlangan birinchi haqiqiy xatolikdan boshlab aybsiz sodir bo‘lishi ma’lum edi (Slater 1987, 223-bet). 1970-yillarda perfokartalar klaviatura va terminallar orqali elektron kiritish va chiqarish bilan almashtirildi. Kabellar va terminallar ruxsat etilgan foydalanuvchilar

ma'lumotlarni qayta ishlash vaqtida o'tirishlari mumkin bo'lgan diapazonni yanada kengaytirdi. Tizimlar xavfsizligi kengayib, kabellar vakolatli kompyuter foydalanuvchilari egallagan ofislarda tugatilishini ta'minlash uchun devor bo'laklari va uzatish kanallari orqali kabellarni kuzatishni o'z ichiga oladi. Bu haqiqiy kompyuterdan uzoqda joylashgan ofislardagi odamlarga kiritish-chiqarish portiga ulanishi va undan ish stolidan foydalanish imkonini berdi. Kompyuter xonasi eshigi oldida qo'riqchi qoldi, lekin asosan kompyuter xonasini aylanib chiqadigan tashrif buyuruvchilar yoki texnik xizmat ko'rsatgan sotuvchilarni ro'yxatdan o'tkazish uchun qoldi. Axborot xavfsizligi moslashtirilgan biznes mantig'i sohasiga o'tkazildi.

Foydalanuvchilar uchun ekran menyulari

Foydalanuvchilarga o'zlarining ish funksiyalarini bajarishlari uchun zarur bo'lgan ekranlarni taqdim etadigan menyular bilan bog'liq bo'lgan login nomlari berildi. Buning ta'siri shundaki, ko'pchilik foydalanuvchilar bir xil asosiy ekranni ko'rar edilar, ammo turli xil ma'lumotlar maydonlari va menyu tanlovlari turli foydalanuvchilar uchun mavjud edi. Ekranlar dasturiy ta'minotga kodlangan *biznes mantig'i* bilan cheklangan. Misol uchun, agar xizmatchilar mijozlarga xizmat ko'rsatish ekraniga ega bo'lsa, ular mijozlar yozuvlarini ko'rishlari mumkin, ammo balanslarini o'zgartiraolmaydilar. Biroq, biznes mantiqiy ekranlari ko'pincha bekor qilishlarni o'z ichiga oladi. Misol uchun, mijozlarga xizmat ko'rsatuvchi xodimni kuzatayotgan nazoratchi ekranning cheklangan funksiyasi orqali balansni bir martalik o'zgartirishga ruxsat berish uchun maxsus kod kiritishi mumkin. Klaviatura texnologiyasi yordamida ishlaydigan kompyuterlarning keng qo'llanilishi konfidentsiallikni nazorat qilish masalasiga e'tibor qaratdi. Harbiy va razvedka kompyuterlaridan foydalanish ko'paydi. Hukumat tomonidan moliyalashtiriladigan kriptografiya bo'yicha tadqiqotlar ma'lumotlarni blokirovka qiladigan va ochadigan "kalitlar" deb nomlangan bitlarning uzun ketma-ketligidan foydalangan holda ma'lumotlarni o'qib bo'lmaydigan formatlarga aylantiradigan bir nechta algoritmlarni ishlab chiqdi.

Bunday kriptografik algoritmlar *diffuziyaga*, xabarni statistik jihatdan uzoqroq va noaniqroq formatlarga tarqatishga va *chalkashlikka*, shifrlangan xabar va tegishli kalit o'rtasidagi munosabatlarni juda uzoq va taxmin qilish uchun jalb qilishga asoslangan (Shannon 1949). Biroq, kompyuter quvvatidagi yutuqlar qat'iy raqibning xabarlar va kalitlar o'rtasidagi munosabatni aniqlash qobiliyatini sezilarli darajada oshirdi. Mavjud avtomatlashtirilgan kriptografiya usullari avtomatlashtirilgan statistik tahlilni buzadigan darajada murakkab bo'lmagan kunni tasavvur qilish oson edi(Grampp va McIlroy 1989).Bundan tashqari, AQSh Ijtimoiy xavfsizlik ma'muriyati va ichki daromad

xizmati kabi davlat idoralari tomonidan qaydlarni avtomatlashtirish, kibermakondagi manfaatdor tomonlar jismoniy hayoti ularni ifodalovchi bit va baytlarga chambarchas bog‘langan shaxslarni o‘z ichiga olganligini tan olishga yordam berdi. Konfidentsiallik talablarining ortib borayotganini e’tirof etgan holda, lekin ularni qondirishning yaxshi usuli bo‘lmagan holda, AQSh Milliy Standartlar Byurosi (hozirgi Milliy Standartlar va Texnologiyalar Instituti [NIST]) ushbu maqsadga erishish uchun harakat boshladi.

1974 yilda AQShning Kompyuter xavfsizligi to‘g‘risidagi qonuni (Maxfiylik to‘g‘risidagi qonun) axborot tarqalishi ustidan nazoratni o‘rnatish uchun mo‘ljallangan birinchi qonun edi. Hujjat faqat davlat tomonidan kompyuterlardan foydalanishni va faqat bugungi kunda shaxsiy identifikatsiya qilinadigan ma’lumot (PII) deb ataladigan ma’lumotlarni qamrab oldi. Ammo u kiberxavfsizlikning asosiy maqsadlari sifatida konfidensiallikni va shifrlash texnologiyasini takomillashtirish bo‘yicha tegishli sa’y-harakatlarni qat’iy belgiladi. 1970-yillar davomida texnologiya rivojlanib borar ekan, DEC PDP-11 kabi mini-kompyuterlar tez-tez yirik kompaniyalarning meynfreymlarini to‘ldirib va tez orada kichik kompaniyalarga aylanib borar edi, endi ularga matnni qayta ishlash kabi ofis vazifalarini avtomatlashtirish imkoniyatini bera olardi. Hali har qanday o‘lchamdagi kompyuterni sotib olishga qodir bo‘lmaganlar uchun texnologiyani yaxshi biladigan tadbirkorlar odamlarga kompyuterni ma’lum vaqtga ijaraga olish imkonini beradigan xizmatlarni ishga tushirishgan. Bular "timeshareing xizmatlari" deb nomlandi, chunki bu biznesdagi kompaniyalar o‘z mijozlaridan kompyuter sarflagan vaqtiga qarab haq olishardi.

Terminal va klaviatura texnologiyasi IO qurilmalarini kabellar orqali kengaytirishga imkon yaratgandan so‘ng, ular analog modulyatsiya demodulyatsiyasi texnologiyasidan (modemlar va multipleksorlar) foydalanib, kompyuter terminalining bino devorlaridan tashqariga chiqishini kengaytirish uchun oddiy telefon liniyalaridan foydalanganlar. Bu kompaniyalar ish haqi solig‘i hisob-kitoblari va tijorat ijarasi hisob -kitoblari kabi murakkab dasturiy ta’minotni ishlab chiqib, sanoat bo‘yicha ixtisoslasha boshladilar.[1]

Bunday dasturiy ta’minotni ishlab chiqish dasturiy ta’minot biznesida bo‘lmagan kompaniya uchun foyda-xarajat tahlilida yaxshi natija berishi dargumon, ammo bu ko‘plab korxonalar tomonidan boshqariladigan vaqtni talab qiluvchi qo‘lda ishlov berish jarayoni edi. Vaqtni taqsimlash xizmatlari biznesning asosiy qismi bo‘lmagan bo‘limlarga avtomatlashtirishdan foydalanishga imkon berdi, garchi ular buni amalga oshirish uchun boshqa birovning kompyuteriga kirishlari kerak edi. Bugungi kunda ushbu xizmatlar

Internet orqali mavjud, ammo ularning zaryadlash modellari o‘zgargan va ular endi "vaqtni taqsimlash" emas, balki "bulutli hisoblash" deb nomlanadi.

Ushbu vaqt taqsimlash xizmatlari foydalanuvchi faoliyatiga asoslangan resurslarni hisoblash uchun haq olinadi, shuning uchun ular hisob-kitob qilish uchun foydalanuvchilarni aniqlash usuliga ega bo‘lishlari kerak edi. Ko‘pincha, bu foydalanuvchi identifikatori shunchaki kompaniya nomi edi, lekin parol ba’zan vaqt taqsimlash xizmatlarida raqobatchilar bo‘lgan mijozlarga ega bo‘lgan joylarda chiqariladi. Biroq, mijozning foydalanuvchisi nuqtai nazaridan, foydalanuvchi nomi ularni kompyuterdagi ma’lumotlariga bog‘ladi va modemga ulanishi xavfsizlikka xavf tug‘dirmaydi. O‘sha paytda kompyuterga egalik qilish uchun yetarlicha katta bo‘lgan har qanday kompaniya ma’lum bir mulk va mazmunga ega bo‘lgan firma edi, shuning uchun timesharing xizmati kompaniyalari o‘z kompyuterlari atrofida jismoniy xavfsizlikka muhtoj deb taxmin qilgan va parollar ularning xavfsizligini sinchkovlik bilan tekshirishning yana bir dalili edi. Timesharing xizmati sotuvchisi uchun mijozlarga mantiqiy kirishga ruxsat berish xavfli deb hisoblangan va ularning boyligi va mohiyatini hisobga olgan holda, ular o‘z aktivlarini shunga mos ravishda himoya qilishlarini kutish mumkin edi. 1970-yillardan 1980-yillarga qadar mini-kompyuterlar arzonroq bo‘ldi va oxir-oqibat odamlarga o‘zlari foydalanishi uchun butun kompyuterga ega bo‘lish imkonini berdi. Apple shaxsiy kompyuterlarini 1970-yillarning oxirida taqdim etdi. Tez orada ular ma’lumotlarni qayta ishlash muhitiga kirdi va 1981 yilda IBM shaxsiy kompyuteri paydo bo‘ldi. Bu kichik kompyuterlar uchun jismoniy xavfsizlik hali ham norma bo‘lib qoldi va qulflangan ofis eshiklari asosiy himoya mexanizmi edi.

Tarmoq texnologiyalari arxitekturasi

Tarmoq texnologiyalari keyinchalik bir binodagi ish stoli kompyuterlariga bir-biri bilan ma’lumot almashish imkonini berdi va kompyuterlarning nomlari odamlar tarmoqdagi boshqa kompyuterlar bilan axborot almashishi uchun muhim bo‘la boshladi. Mahalliy tarmoq (LAN) kabellari xuddi kompyuter terminallarining meynfreymga ulanishi kabi himoyalangan edi, bundan tashqari yangi turdagi tarmoq uskunasi “hub” deb nomlangan aloqani amalga oshirishga imkon berdi va hublar xavfsiz hududda saqlanishi kerak edi. Biror kishiga o‘z kompyuterini LANga ulash imkonini beradigan markazlar qulflangan shkaflar orqali himoyalangan. LANlar joriy etilgunga qadar, hisoblash muhitiga kirish boshqaruvlari normadan ko‘ra istisno edi. Agar login identifikatorlari tarqatilgan bo‘lsa, ular kamdan-kam hollarda o‘chirilgan. Ular ma’lumotlarga kirishni cheklashdan ko‘ra, kimga tegishli ekanligini bilish uchun ko‘proq ma’lumotlarni belgilashning qulay usuli sifatida ishlatilardi.

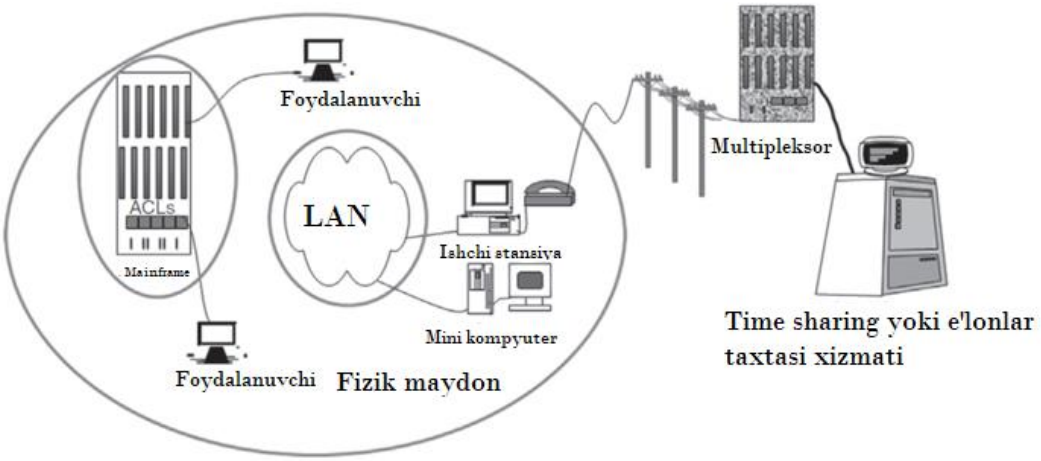
Biroq, LANga ulangan hisoblash muhitlari va tegishli shaxsiy kompyuterlarning ko‘pligi tarmoqdagi kompyuter faolligini alohida shaxslarga kuzatishni juda qiyinlashtirdi, chunki ular odatda faqat ish stolidagi mashinaga kirishgan. LANlar kattalashgan sari, davlat tadqiqot laboratoriyalarining markazlashtirilgan boshqaruv sxemalari korporativ meynfreymlar uchun ishlab chiqildi (Schweitzer 1982, 1983). Majburiy kirishni boshqarish tizim kompyuter ob’ektlarini (dasturlar va fayllar) belgilash va ularga kirish mumkin bo‘lgan sub’ektlarni (foydalanuvchilarni) nazoratlash imkonini berdi. Ular ixtiyoriy sxemalar bilan to‘ldirildi, bu har bir foydalanuvchiga o‘z fayllariga yana kim kirishi mumkinligini belgilash imkonini berdi.

Ko‘pgina LAN kompyuter foydalanuvchilarining stollarida asosiy kompyuter terminali bo‘lganligi sababli, ko‘p o‘tmay, bu kompyuterlar terminal funksiyasini o‘zlashtirdilar va LAN asosiy kompyuterga ulandi. Aynan mana shu rivojlanish kiberxavfsizlikni texnologiya boshqaruvida dolzarb mavzuga aylantirdi. LAN tarmog‘ida ba’zi vaqt almashinuvi tipidagi parol texnologiyasidan foydalanilgan bo‘lsa-da, LAN foydalanuvchi nomlari, birinchi navbatda, aniqlangan hujumlarning oldini olish uchun emas, balki katalog xizmatlarini osonlashtirish uchun qo‘llab-quvvatlandi. Ya’ni, ma’lum bir faylni yozgan yoki mijozning yozuviga eslatma joylashtirgan shaxsning ismini bilish foydali bo‘ldi. Kompyuter foydalanuvchilariga kirish nomlarini belgilash dasturlarga to‘g‘ri menyu va ekranlarni taqdim etish uchun biznes mantig‘ining bir qismi sifatida ushbu nomdan foydalanishga imkon berdi.

Kibermakon evolyutsiyasining shu nuqtasiga qadar, meynfreymdagi tranzaktsiyalar ma’lum bir jismoniy joylashuvdagi individual terminalda kuzatilishi mumkin edi, jismoniy va raqamli sud-tibbiyot ekspertizasi yordamida keyingi tergov gumonlanuvchini aniqlash uchun jangovar imkoniyatga ega edi. Biroq, LAN va modemlar foydalanuvchilar o‘rtasidagi muloqotni yashirin qildi va jinoyatchi uchun LAN ish stoli orqali amalga oshirilgan faoliyatni *rad* etish yoki so‘zning tez tarqaladigan kompyuter xavfsizligi versiyasidan foydalanish oson edi . Parollar talab qilingan joylarda ham ular taxmin qilish uchun yetarlicha zaif edi.

Tarmoqni shifrlash tushunchasi yo‘q edi, shuning uchun markazlarga kirish huquqiga ega bo‘lgan har bir kishi tarmoqda sayohat qilayotgan parollarni ko‘rishi mumkin edi. Bundan tashqari, ko‘plab tarmoq dasturlari anonim kirishga ruxsat berdi, shuning uchun foydalanuvchi nomlari har bir ulanish uchun mavjud emas edi. Rahbariyatga joriy vaziyat barqaror bo‘lishi uchun juda katta xavf mavjudligini tushunish uchun bir necha insayder firibgarlik holatlari kerak bo‘ldi. Shunday qilib, shu paytgacha harbiy

tadqiqotlar mavzusi bo‘lgan xavfsizlik texnologiyasi yirik kompyuter sotuvchilari tomonidan shoshilinch ravishda amalga oshirildi va asosiy kompyuter ma’lumotlar to‘plamlari va LAN fayl resurslariga tatbiq etildi. Bularga foydalanuvchi identifikatori, tobora qiyinlashib borayotgan parollar ko‘rinishidagi autentifikatsiya va kompyuterga kirish uchun boshqaruv ruxsati kiradi. Tez orada AQSH Mudofaa vazirligining qarori asosida “Apelsin kitobi” nomli muhitda ishlashni ta’minlash uchun zarur bo‘lgan tizim funksiyalarining to‘liq to‘plami osongina mavjud bo‘ldi (DoD 1985). To‘liq xususiyatlar to‘plami kiritilgan texnik amalga oshirish uchun standartlar va murakkab terminologiya, foydalanuvchilarning aniqlanishi va autentifikatsiya qilinishini ta’minlash uchun jarayonlar tekshirildi. Shifrlash ham a uchun aniq yechim sifatida e’lon qilindi va turli xil kompyuter xavfsizligi muammolari yechimi topildi (NRC 1996), lekin bu hashamat edi armiyadan tashqarida kam sonlilar yetarlicha zaxira kompyuterga ega edilar, shuning uchun kompyuter qanchalik kichik bo‘lsa, sotuvchining shifrlash algoritmlari shunchalik zaif bo‘lishi mumkin edi va shifrlash aniqlik bilan qo‘llanildi. Garchi tranzaktsiyalarni qayta ishlash uchun javobgarlik tez bo‘lib qolgan bo‘lsa-da firibgarlik konferentsiyalarida dolzarb mavzu, domendagi huquqni muhofaza qilish faoliyati kompyuterning ishlashi cheklangan edi. Shunga qaramay, 1980-yillarning boshlari ham raqamli dalillar davrining boshlanishi edi.



1-rasm. 1980-yillardagi kibermakon arxitekturasi.

Huquqni muhofaza qilish organlari bilan hamkorligida texnologiya sotuvchilari jinoyatchilar fayllarini qayta tiklaydigan dasturiy ta’minot ishlab chiqarish uchun kompyuterlardan o‘chirishga harakat qilgan (Schmidt 2006). 1-rasmda odatda konfiguratsiya qilinganidek kibermakon arxitekturasi tasvirlangan 1980-yillarning boshlarida. Mainframe, mikro va mini-kompyuterlar yonma-yon mavjud bo‘lib, ular tarmoq orqali ulanishi shart emas edi. Biroq, mini-kompyuterlar ko‘pincha ovozli qo‘ng‘iroqlarni amalga oshiradigan bir xil turdagi telefon liniyalari orqali masofaviy kompyuterlarga

ulanish uchun ishlatilgan. Biroq, texnologiya innovatsiyalarining tez sur'atda rivojlanishi sababli, bu holat doimo rivojlanib borardi va o'zgarish muqarrar edi.

Xulosa

Xulosa o'rnida shuni takidlash kerakki, kompyuter texnologiyalari yillar davomida rivojlanishi natijasida kibermakon tushunchasi yuzaga keldi va bu kibermakon tushunchasi hozirgi kunda raqamlashtirilgan virtual olam ma'nosini anglatib, endilikdan insonlar xavfsizligini taminlash uchun avvalo kibermakondagi kiberxavfsizlikni ta'minlash muhim ahamiyatga egadir.

FOYDALANILGAN ADABIYOTLAR:

- S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O'quv qo'llanma. – T.: «Aloqachi», 2020, 221 bet.
- Cyber Security Policy Guidebook
- **Jennifer L.** Bayuk Independent Cyber Security Governance Consultant Industry Professor at Stevens Institute of Technology, Hoboken
- **NJ Jason Healey** Director of the Cyber Statecraft Initiative Atlantic Council of the United States, Washington
- **D.C. Paul Rohmeyer** Information Systems Program Director Howe School of Technology Management Stevens Institute of Technology, Hoboken
- **NJ Marcus H. Sachs** Vice President for National Security Policy Verizon Communications, Washington
- **D.C. Jeffrey** Schmidt Chief Executive Officer JAS Communications LLC, Chicago, IL
- **Joseph Weiss** Professional Engineer Applied Control Solutions, LLC, Cupertino, CA