4-Ma’ruza

Mavzu: Kiberxavfsizlik arxitekturasi, strategiyasi va siyosati:

Reja:

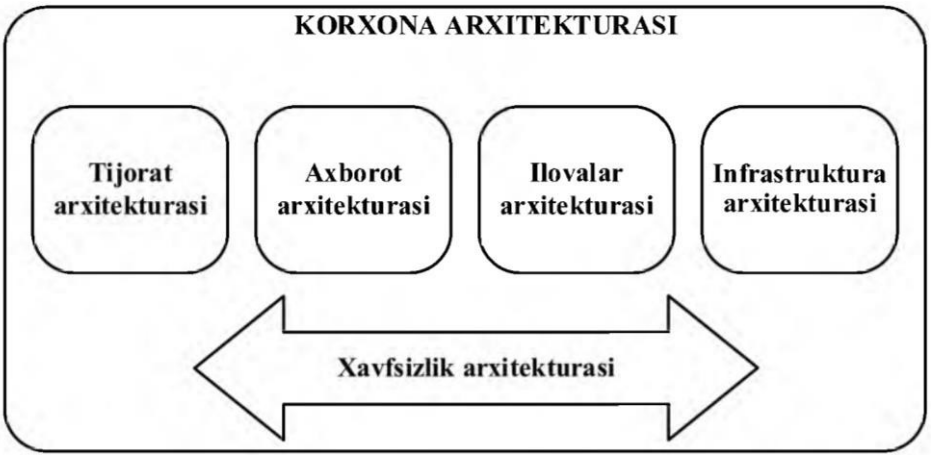
1. Kiberxavfsizlik arxitekturasi, strategiya
2. Kiberxavfsizlik siyosati va uni amalga oshirish
3. Axborot xavfsizligi siyosati
4. Xavfsizlik siyosatining zaruriyati
5. Xavfsizlik siyosatining afzalliklari
6. Xavfsizlik siyosatining iyerarxiyasi
7. Xavfsizlik siyosati xususiyatlari
8. Axborot xavfsizligi siyosatining turlari

Tayanch iboralar: *arxitekturasi, strategiya, axborot siyosati, kibersiyosat, togaf, zachman framework, feaf, dodaf, risk, strategiya*

Zamonaviy tijorat oldida murakkab masalalar to‘plami ko‘ndalangki, beqaror iqtisodiy vaziyatda ularning dolzarbligi yanada oshadi. Bunday masalalarga quyidagilarni kiritish mumkin:

- daromadning oshishi;
- o‘zgaruvchi vaziyatlarga reaksiya tezligining oshishi;
- harajat va chiqimlarning pasayishi;
- innovatsiyaning tezlashishi;
- bozorga mahsulot va xizmatlarni taqdim etish vaqtining qisqarishi;
- buyurtmachilar va sheriklar xolisligining oshishi;
- raqobatlik qobiliyatining oshishi;
- me’yoriy talablarga moslikni ta’minlash.

Yuqorida keltirilgan barcha masalalarni yechishda korxona arxitekturasidan foydalaniladi (4.1-rasm). Korxona arxitekturasi prinsiplar, yondashishlar va texnologiyalar majmuini shakllantirishga imkon beradiki, ular tashkilotning joriy holatini hisobga oigan holda uning kelgusi transformasiyasi, o‘sishi va rivojlanishi asosini belgilaydi.



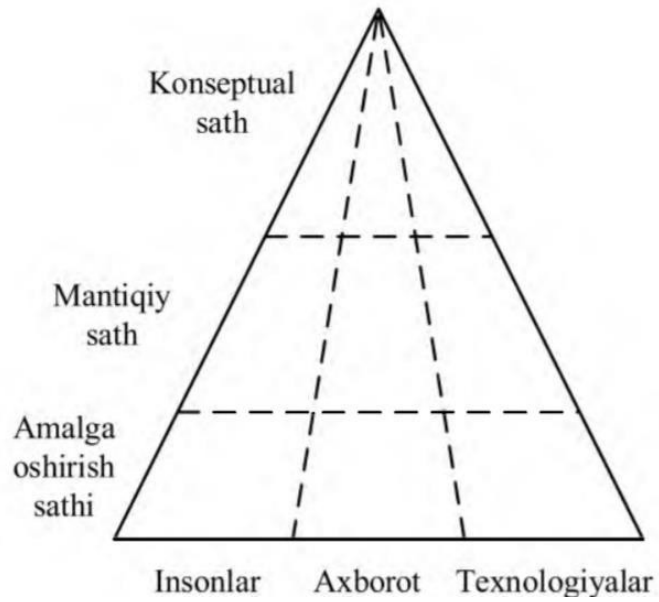
4.1-rasm. Korxona arxitekturasi va uning boshqa arxitekturalar bilan bog‘liqligi

Hozirda bunday arxitekturalarni yaratishda bir necha yondashishlar mavjud, masalan TOGAF, Zachman Framework, FEAF, DoDAF va h.k

Ammo, qaysi bir yondashish tanlanmasin, hozirgi sharoitda axborotdan va axborot tizimidan foydalanmay rivojlanish mumkin emas. Axborot va axborot tizimlari nafaqat tijoratdagi har qanday o‘zgarishlarni madadlaydi, balki ularni oldindan sezadi, ularga oldindan tayyorlanadi, ba’zi xollarda esa yangi tijorat-imkoniyatlarining paydo bo‘lishiga yordam beradi. Biroq tijorat doimo istalgancha rivojlanmaydi. Bunda ma’lumotlarning sirqib chiqishi, axborot texnologiyalari infrastrukturasi elementlarining ishdan chiqishi va h. bilan bog‘liq axborot operatsion risklar anchagina rol o‘ynaydi. Hozirgi va kelajak risklarga tayyor bo‘lish uchun korxonaning boshqa arxitekturalari bilan uzviy bog‘langan axborot xavfsizligi arxitekturasi zarur.

Kiberxavfsizlik arxitekturasi jarayonlarni, inson rolini, texnologiyalarni va turli xil axborotni tavsiflaydi, hamda zamonaviy korxonaning murakkabligini va o‘zgaruvchanligini hisobga oladi. Boshqacha aytganda, kiberxavfsizlikning arxitekturasi tashkilotning va u bilan bog‘liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi. Bunda axborot xavfsiziligi arxitekturasi tijoratning joriy va eng muhimi, kelgusidagi ehtiyojini akslantiradi.

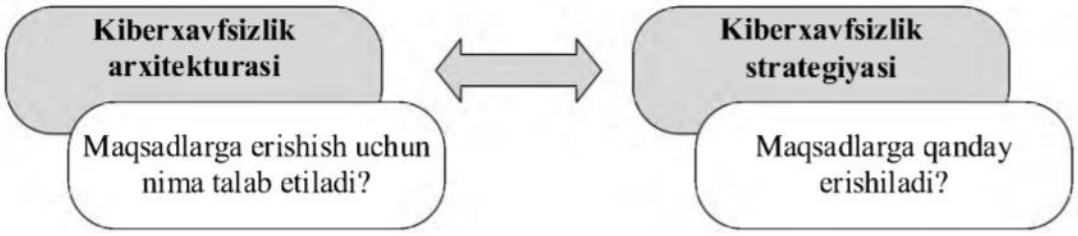
Odatda arxitekturaning 3 ta sathi ajratiladi - konseptual, mantiqiy va amalga oshirish (texnologik). 4.2-rasmda bunday arxitektura keltirilgan bo‘lib, odatda texnologiyalar jihatidagi qismi xavfsizlik xizmati nazoratidan chetda qoladi.



4.2-rasm. Kiberxavfsizlik arxitekturasi

Joriy holatdan qanday qilib yangi, mukammalroq va qo‘yilgan maqsadlarga mos holatga o‘tish mumkin? Buning uchun strategiya, ya’ni qo‘yilgan maqsadlarga erishish uchun harakat yo‘nalishi mavjud.

Strategiya - korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo‘ljallangan strukturalangan va o‘zaro bog‘langan harakatlar to‘plami. 4.3-rasmda arxitektura bilan strategiyaning o‘zaro bog‘liqligi keltirilgan. Strategiya kiberxavfsizlik arxitekturasi ko‘rinishidagi maqsadga ega bo‘lgan holda unga erishishning optimal yo‘lini belgilaydi.



4.3-rasm. Arxitektura bilan strategiyaning o ‘zaro bog‘liqligi

Ko‘pincha strategiya va arxitektura tushunchalarini farqlamay arxitektura tavsifini o‘z ichiga oigan kiberxavfsizlik strategiyasi ishlab chiqiladi. Bu unchalik to‘g‘ri emas, chunki arxitektura, ya’ni maqsadlar vaqt o‘tishi bilan o‘zgarmasligi, bu maqsadlarga erishishdagi strategiya esa tashqi va ichki omillarga bog‘liq holda jiddiy o‘zgarishi mumkin. Strategiya va arxitektura bitta hujjatda tavsiflansa, strategiya o‘zgarganida arxitekturani ham o‘zgartirishga to‘g‘ri keladi.

Kiberxavfsizlik siyosati va uni amalga oshirish

Axborot xavfsizligi siyosati (yoki xavfsizlik siyosati) - tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar

tavsiflanadigan yuqori darajadagi reja. Siyosat xavfsizlikni umumlashgan atamalarda tavsiflaydi. U xavfsizlikni ta’minlashning barcha dasturlarini rejalashtiradi. Axborot xavfsizligi siyosati tashkilot masalalarini yechish jarayoni himoyasini yoki ish jarayoni himoyasini ta’minlashi shart.

Apparat vositalar va dasturiy ta’minot ish jarayonini ta’minlovchi vositalar hisoblanadi va ular xavfsizlik siyosati tomonidan qamrab olinishi shart. Shu sababli, asosiy vazifa sifatida tizimni (jumladan tarmoq xaritasini) to‘liq inventarizatsiyalashni ko‘zda tutish lozim. Tarmoq xaritasini tuzishda har bir tizimdagi axborot oqimini aniqlash lozim. Axborot oqimlari sxemasi axborot oqimlarining biznes-jarayonlarni qanchalik ta’minlayotganini, hamda axborotni himoyalash va yashovchanligini ta’minlash uchun qo‘shimcha choralarni ko‘rish muhim bo‘lgan soxani ko‘rsatishi mumkin. Undan tashqari, bu sxema yordamida axborot ishlanadigan joyni, ushbu axborot qanday saqlanishi, qaydlanishi, joyini o‘zgartirishi va nazoratlanishi lozimligini aniqlash mumkin.

Inventarizatsiya apparat va dasturiy vositalardan tashqari dasturiy va apparatura hujjatlari, texnologik hujjat va hakazo kabi kompyuterga taalluqli bo‘lmagan resurslarni ham qamrab olishi shart. Ushbu hujjatlar tarkibida tijoratni tashkil etish xususiyatlari to‘g‘risidagi axborot bo‘lishi mumkin va bu hujjatlar buzg‘unchilar foydalanishi mumkin bo‘lgan joylarni ko‘rsatadi.

Xavfsizlik siyosatining zaruriyati:

- Tashkilot bo‘ylab foydalanilayotgan qurilmalar soni ortib borishi tarmoqda uzatilayotgan va saqlanadigan axborot hajmini ortishiga olib kelmoqda. Bu holat esa o‘z navbatida turli zaifliklar natijasida hosil bo‘lgan xavfsizlik tahdidlarini ortishiga ham sababchi bo‘ladi. Xavfsizlik siyosati tashkilotga ushbu tahdidlarga qarshi kurashish va unga axborotning yo‘qolishidan himoyalash imkonini beradi.
- Xavfsizlik siyosati tashkilotning barcha funksiyalarini xavfsiz tarzda amalga oshirish orqali xavfsizlik prinsiplarining kelishilgan vazifalarini ta’minlaydi.
- Xavfsizlik siyosati mijozlar bilan ishonchga asoslangan aloqani qurishda axborot xavfsizligi standartlarining mosligini ta’minlaydi.
- Xavfsizlik siyosati tashqi axborot tahdidlariga kompaniyaning duchor bo‘lishi xavfíni pasaytirishga yordam beradi.
- Xavfsizlik siyosati tarmoqda qanday qoidalar foydalanishi kerakligini, konfidensial axborot qanday saqlanishi va tashkilot ma’lumotlarini oshkor bo‘lishi va majburiyatlarni kamaytirish uchun qanday shifrlash algoritmlari kerakligini aniqlash orqali qonuniy himoyani ta’minlaydi.
- Xavfsizlik siyosati tahdidlarning sodir bo‘lishidan oldin ularni bashoratlash va zaifliklarni aniqlash orqali xavfsizlik buzilishlari holatining ehtimolini kamaytiradi.

- U shuningdek, zaxira nusxalash va qayta tiklash amallarini joriy qilish orqali tashkilot ma’lumotlarining yo‘qolishi va sirqib chiqishi xavfíni minimallashtiradi.

Xavfsizlik siyosatining afzalliklari:

- *Kuchaytirilgan ma’lumot va tarmoq xavfsizligi*: tashkilotlar o‘z ma’lumotlari xavfsizligini ta’minlovchi tarmoqqa asoslangan siyosatini amalga oshiradilar. Xavfsizlik siyosati tarmoqda boshqa tizimlardan ma’lumotlar uzatilishida himoyani ta’minlaydi.
- *Risklarni kamaytirish*: xavfsizlik siyosatini amalga oshirish orqali tashqi manbalardan bo‘lishi mumkin bo‘lgan risklar kamaytiriladi. Agar xodimlar xavfsizlik siyosati asosida harakat qilsalar, ma’lumot va resurslarning yo‘qolishi holatlari deyarli kuzatilmaydi.
- *Qurilmalardan foydalanish va ma ’lumotlar transferining monitoringlanishi va nazoratlanishi*: xavfsizlik siyosati xodimlar tomonidan amalga oshirilgani bois, ma’murlar tashkilotdagi trafikni va foydalanilgan tashqi qurilmalarni doimiy tarzda monitoringlashi zarur. Kiruvchi va chiquvchi trafikning monitoringi va auditi doimiy ravishda amalga oshirilishi shart.
- *Tarmoqning yuqori unumdorligi:* xavfsizlik siyosati to‘g‘ri amalga oshirilganida va tarmoq doimiy monitoring qilinganida ortiqcha yuklamalar mavjud bo‘lmaydi. Tarmoqda ma’lumotni uzatish tezligi ortadi va bu umumiy samaradorlikni ortishiga olib keladi.
- *Muammolarga darhol javob berish va harakatsiz vaqtning kamligi:* xavfsizlik siyosatini amalga oshirilishi tarmoq muammolari kuzatilganida darhol javob berish imkoniyatini taqdim etadi.
- *Boshqaruvdagi hayajon darajasining kamayishi:* xavfsizlik siyosati amalga oshirilganida boshqaruvchi kam hayajonga ega bo‘ladi. Xavfsizlik siyosatidagi bir vazifa tashkilotning biror xodimiga biriktirilishi shart. Agar ushbu holat amalga oshirilsa, tarmoqda biror nojo‘ya holat kuzatilsa ham, boshqaruvda hech qanday xavotir bo‘lmaydi.
- *Xarajatlarning kamayishi:* agar xodimlar siyosatga to‘g‘ri amal qilsalar, tashkilotga ta’sir qiluvchi turli xalaqitlar uchun ortiqcha harajat kamayadi.

Xavfsizlik siyosatining iyerarxiyasi:

Tashkilotlarda xavfsizlik siyosatini ishlab chiqishda turli hujjatlardan foydalaniladi. Ushbu hujjatlarni ishlab chiqish xavfsizlik siyosatining iyerarxiyasining sathi va uning soniga bog‘liq.

- *Qonunlar*. Qonunlar iyerarxiyaning eng yuqori sathida joylashgan bo‘lib, ular tashkilotdagi har bir xodim amalga oshirishi kerak bo‘lgan vazifalarni o‘z ichiga oladi. Ushbu qonunlarga amal qilmagan har bir xodim uchun javobgarlik choralari ko‘rilishi shart bo‘ladi.

- *Normativ hujjatlar.* Normativ hujjatlar iyerarxiyadagi ikkinchi tashkil etuvchi bo‘lib, ular xodimlarning qonunlarga rioya qilishini kafolatlaydi. Normativ hujjatlar xavfsizlik siyosati qonuniga mos bo‘lgan yo‘l yo‘riq ko‘rsatuvchi hujjatlar to‘plarni bo‘lib, ular hukumat yoki ijtimoiy normativ hujjatlardan tashkil topadi.
- *Siyosatlar***.** Siyosatlar yordamida tashkilot shaxsiy tarmoq xavfsizligi uchun qonuniy ichki tarmoq talablarini yaratadi. Siyosat turli muolajalardan iborat bo‘lib, ular tashkilot uchun xavfsizlik arxitekturasini ko‘rsatadi. Ushbu siyosatlarning amalga oshirilishi tashkilotga standartlarni o‘rnatish va risklarni boshqarish kabi vazifalarni bajarishiga imkon yaratadi.
- *Standartlar.* Standartlar siyosatni amalga oshirish usullarini tavsiflaydi va tashkilotlar tomonidan amalga oshiriladi. Standartlar korxona siyosatiga ixtiyoriy va mandatli aloqador bo‘lib, ishlab chiqilgan standartni ma’lum vaqtdan so‘ng o‘zgartirish talab etilmasligi zarur. Shuningdek, standartlar texnologiya, qurilma va dasturiy vositaga bog‘liq holda xavfsizlik nazoratini o‘z ichiga oladi.
- *Yo‘riqnomalar.* Yo‘riqnomalar tashkilot siyosati va standartlarini amalga oshirish strategiyasini aniqlab, tashkilotning tahdidlarga qarshi tura olishida yordam beradi. Shuning uchun, tashkilot xodimlari yo‘riqnomalarni bajarish uchun, maxsus o‘qitiladi.
- *Muolajalar.* Muoalajalar tashkilot siyosatini amalga oshiruvchi ketma-ket bosqichlar to‘plarni bo‘lib, ularni amalga oshirishda imtiyozga ega subyektdan tasdiq talab etiladi. Muolajalar quyidagi savollar asosida ishlaydi:
  - kim nimani bajaradi?;
  - ular qanday bosqichlarga ega?;
  - ular qaysi shakl va hujjatlardan foydalanadilar?
- *Umumiy qoidalar.* Umumiy qoidalar tanlovga ko‘ra maslahatlar bilan ta’minlovchi hujjat bo‘lib, ulardan biror maxsus standartlar bo‘lmagan holda foydalaniladi. Umumiy qoidalar tavsiyalar sifatida bo‘ladi va tashkilotlar ularni rad eta olmaydi. Umumiy qoidalarni amalga oshirish risklarni kamaytirsada, biznes talablari o‘zgarganida umumiy qoidalarni ham o‘zgartirish tavsiya etiladi.

Xavfsizlik siyosati quyidagi xususiyatlarga ega bo ‘lishi shart:

- *Qisqa va aniq:* xavfsizlik siyosati infrastmkturada joriy qilishda qisqa va aniq bo‘lishi shart. Murakkab xavfsizlik siyosati tushunish uchun qiyin bo‘lib, xodimlar tomonidan kutilgani kabi amalga oshirilmaydi.
- *Foydalanuvchan bo ‘lishi:* siyosat tashkilotning turli sektorlari bo‘ylab oson foydalanishli yozilishi va loyihalanishi shart. Yaxshi yozilgan siyosatlar boshqarishga va amalga oshirishga oson bo‘ladi.

- *Iqtisodiy asoslangan bo‘lishi:* tashkilotlar tejamkor va o‘z xavfsizligini kuchaytimvchi siyosatni amalga oshirishlari shart.
- *Amaliy bo‘lishi:* siyosatlar reallikka asoslangan amaliy bo‘lishi kerak. Real bo‘lmagan siyosatning amalga oshirilishi tashkilotga muammo tug‘diradi.
- *Barqaror bo‘lishi:* tashkilot o‘zining siyosatini amalga oshirishda barqarorlikga ega bo‘lishi kerak.
- *Mulojaviy bardoshli bo‘lishi:* siyosat muolajalari amalga oshirilganida, ular ish beruvchi va ishlovchiga mos bo‘lishi kerak.
- *Kiber va yuridik qonunlarga, standartlarga, qoidalarga va yo ‘riqnomalarga mos bo ‘lishi:* amalga oshiriluvchi ixtiyoriy siyosat kiber qonunlar asosida ishlab chiqilgan qoidalar va yo‘riqnomalarga mos bo‘lishi zarur.

Axborot xavfsizligi siyosatining turlari.

Tashkilotda axborot xavfsizligini rejalashtirish, loyihalash va amalga oshirishda siyosat muhim hisoblanib, ular foydalanuvchilarga xavfsizlik maqsadlariga erishishda mavjud muammolarni bartaraf etish choralarini taqdim etadi. Bundan tashqari, xavfsizlik siyosati tashkilotdagi dasturiy ta’minot va jihozlar vazifasini tavsiflaydi.

Axborot texnologiyalari sohasidagi korxonalarda quyidagi xavfsizlik siyosatlari qo‘llaniladi:

- ***Tashkilot axborot xavfsizligi siyosati*** (Enterprise Information Security Policies, EISP): mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi.
- ***Muammoga qaratilgan xavfsizlik siyosatlari*** (Issue-Specific Security Policies, ISSP): bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profílaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi.
- ***Tizimga qaratilgan xavfsizlik siyosatlari*** (System-Specific Security Policies, SSSP): mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga oigan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi. Bu siyosat texnologiyani amalga oshirish, sozlash va foydalanuvchilar harakatlarini hisobga olishi mumkin.

Tashkilotlarda turli maqsadlarga qaratilgan ko‘plab xavfsizlik siyosatlari mavjud bo‘lishi mumkin. Quyida ularning ayrimlari keltirilgan.

Internetdan foydalanish siyosati. Mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi. Internetdan foydalanish siyosati o‘z ichiga Internetdan foydalanish ruxsati, tizim xavfsizligi, tarmoqni o‘rnatish, AT xizmati va boshqa yo‘riqnomalarni qamrab oladi.

Internetdan foydalanish siyosatini quyidagi to‘rtta kategoriyaga ajratish mumkin:

1.***Tartibsiz siyosat*** (Promiscuous Policy): ushbu siyosat tizim resurslaridan foydalanishda hech qanday cheklovlarni amalga oshirmaydi. Masalan, bu siyosatga ko‘ra foydalanuvchi istalgan saytga kirishi, istalgan dasturni yuklab olishi, masofadagi kompyuterdan yoki tarmoqdan foydalanishi mumkin. Bu siyosat korporativ tashkilotlarning ofislarida ishlovchi yoki tashkilotga kelgan mehmonlar uchun foydali hisoblansada, kompyutemi zararli dasturlar asosidagi tahdidlarga zaif qilib qo‘yishi mumkin. Ya’ni, Internetdan foydalanishda cheklanishlar mavjud bo‘lmagani bois, foydalanuvchilar bilimsizligi natijasida zararli dasturlar kirib kelishi mumkin.

2.***Ruxsat berishga asoslangan siyosat*** (Permissive Policy): Bu siyosatga ko‘ra faqat xavfli xizmatlar, hujumlar yoki harakatlar bloklanadi. Masalan, ruxsat berishga asoslangan Internet siyosatida qator keng tarqalgan zararli xizmatlar, hujumlardan tashqari Internet trafigining asosiy qismi ochiq bo‘ladi. Faqat keng tarqalgan hujumlar va zararli dasturlar bloklanganligi tufayli, ma’mur joriy holatdagi zararli harakatlarga qarshi himoyani ta’minlay oladi. Bu siyosatda har doim yangi hujumlarni va zararli dasturiy ta’minotlarni tutish va bazaga kiritib borish talab etiladi.

3.***Paranoid siyosati*** (Paranoid Policy): Paranoid siyosatga ko‘ra barcha narsa bloklanadi va tizim yoki tarmoqdan foydalanuvchi tashkilot kompyuterlarida qat’iy cheklovlar mavjud bo‘ladi. Bu siyosatga ko‘ra foydalanuvchi Internetga umuman ulanmagan yoki qat’iy cheklovlar bilan ulangan bo‘lishi mumkin. Bunday hollarda, foydalanuvchilar odatda siyosatdagi qoidalarni aylanib o‘tishga harakat qiladilar.

4.***Ehtiyotkorlik siyosati*** (Prudent Policy): Ehtiyotkorlik siyosati barcha xizmatlar bloklangandan so‘ng amalga oshirilib, unda xavfsiz va zarur xizmatlarga ma’mur tomonidan individual ravishda ruxsat beriladi. Bu maksimal xavfsizlikni ta’minlab, tizim, tarmoq faoliyatiga oid barcha hodisalarni qaydlaydi.

Maqbul foydalanish siyosati. Maqbul foydalanish siyosati tarmoq va web sayt egalari tomonidan qaror qilingan qoidalardan iborat va u hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi. Ushbu siyosatda foydalanuvchilarning o‘z akkauntlarida mavjud bo‘lgan ma’lumotlarni himoya qilish majburiyati ko‘rsatilgan

bo‘lib, foydalanuvchidan tarmoqdan yoki Internetdagi kompyuterdan foydalanishida siyosat cheklovlarini qabul qilishi talab etiladi. Ehtiyotkorlik siyosati prinsiplar, taqiqlar, qayta ko‘rib chiqish va jazo choralarini o‘z ichiga olib, foydalanuvchini, shaxsiy sabablarga ko‘ra, korporativ resurslardan foydalanishini taqiqlaydi.

Maqbul foydalanish siyosati axborot xavfsizligi siyosatining ajralmas qismi hisoblanadi. Bunda, tashkilotlar, o‘zlarining yangi xodimlariga axborot resurlaridan foydalanishga ruxsat berishdan oldin, maqbul foydalanish siyosati bo‘yicha tanishganligi xususida kafolat imzosi olinadi. Maqbul foydalanish siyosati foydalanuvchilarni axborot texnologiyalari infrastrukturasida nimalarni bajarish kerak va nimalarni bajarmaslik kerakligi haqidagi asosiy jihatlarni o‘z ichiga oladi.

Maqbul foydalanish siyosati to‘g‘ri amalga oshirilganiga ishonch hosil qilish uchun ma’mur doimiy ravishda xavfsizlik auditini olib borishi kerak. Masalan, aksariyat tashkilotlar o‘z saytlarida va pochtalarida siyosatga aloqador va diniy mavzularda muzokaralar olib borilishini taqiqlaydi. Maqbul foydalanish siyosatlarining aksariyatida siyosatni buzganlik uchun jazolar tayinlanadi. Bunday jazolar foydalanuvchi akkauntini vaqtincha yopib qo‘yishdan tortib qonuniy jazo choralarigacha bo‘lishi mumkin.

Nazorat savollari:

1. Axborot xavfsizligi arxitekturasi va uning sathlari mohiyatini tushintiring.
2. Axborot xavfsizligi strategiyasi tushunchasi haqida ma’lumot bering.
3. Korxona arxitekturasini tuzishda xavfsizlik strategiyasi va arxitekturasining o‘rni qanday?
4. Axborot xavfsizligi siyosati va uning asosiy vazifasi nimadan iborat?
5. Xavfsizlik siyosati nima uchun zarar?
6. Xavfsizlik siyosatining tarkibi va tuzilishini tushintiring.
7. Xavfsizlik siyosatining asosiy turlari nimalardan iborat?