AXBOROT XAVFSIZLIGI

1.Axborot xavfsizligi tushunchasi
2.Axborot himoyasi
3.Axborot xavfsizligi siyosati
4.Axborotni himoyalash usullari

Yarmatov Sherzod

Axborot xavfsizligi (inglizcha: *Information Security*, shuningdek, inglizcha: *InfoSec*) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma’lumotlar qanday shaklda bo‘lishidan qat’iy nazar (masalan, elektron yoki, jismoniy) amal qiladi.

Xavfsizlik sohalari

Axborot xavfsizligini ta‘minlash barcha sohalarda amalga oshirilib, ular asosan quyidagilarga bo‘linadi

- **Tarmoq xavfsizligi**
- **Web da xavfsizlikni ta‘minlash**
- **Ilova va operatsion tizim xavfsizligi**

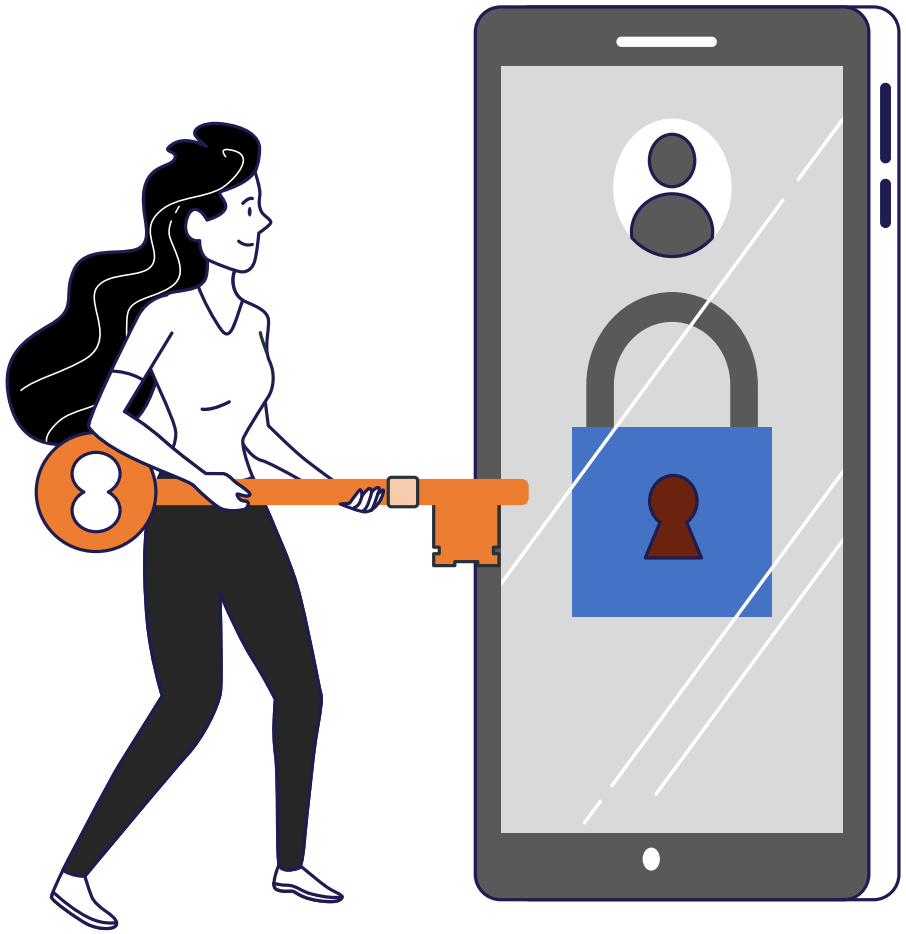
Axborot xavfsizligi muammolari. Axborot xavfsizligida muammolar turi ko‘p bo‘lib, ular asosan quyidagi sabablarga ko‘ra kelib chiqadi:

Ko‘p zararli, xatoli dasturlarni mavjudligi

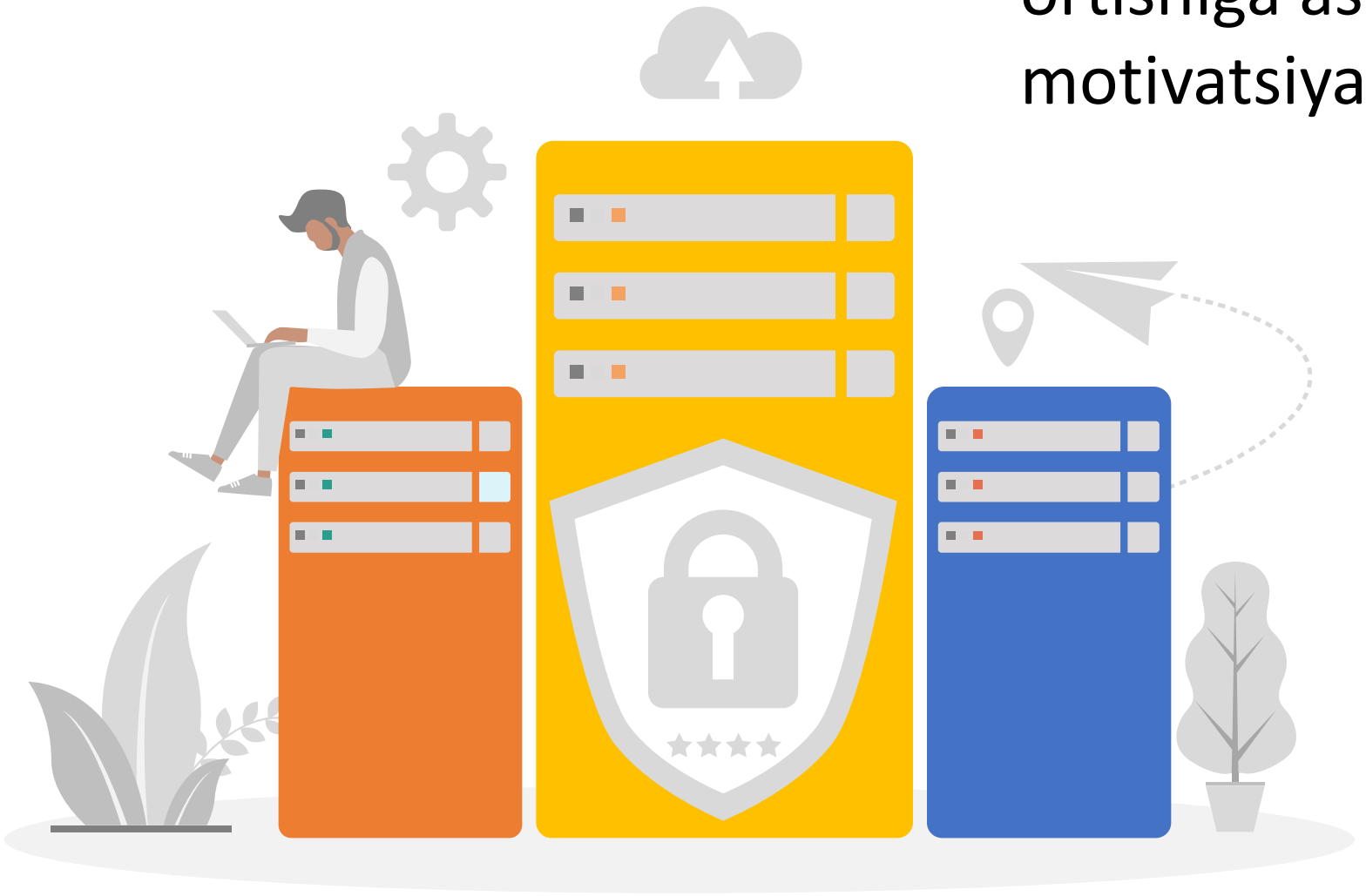
Niyati buzuq foydalanuvchilarni mavjudligi

Sotsial injiniring

Fizik himoya zaifliklari



Axborot xavfsizligida muammolarni ortishiga asosan quyidagilar motivatsiya bo‘lishi mumkin



Foyda

Terrorizm

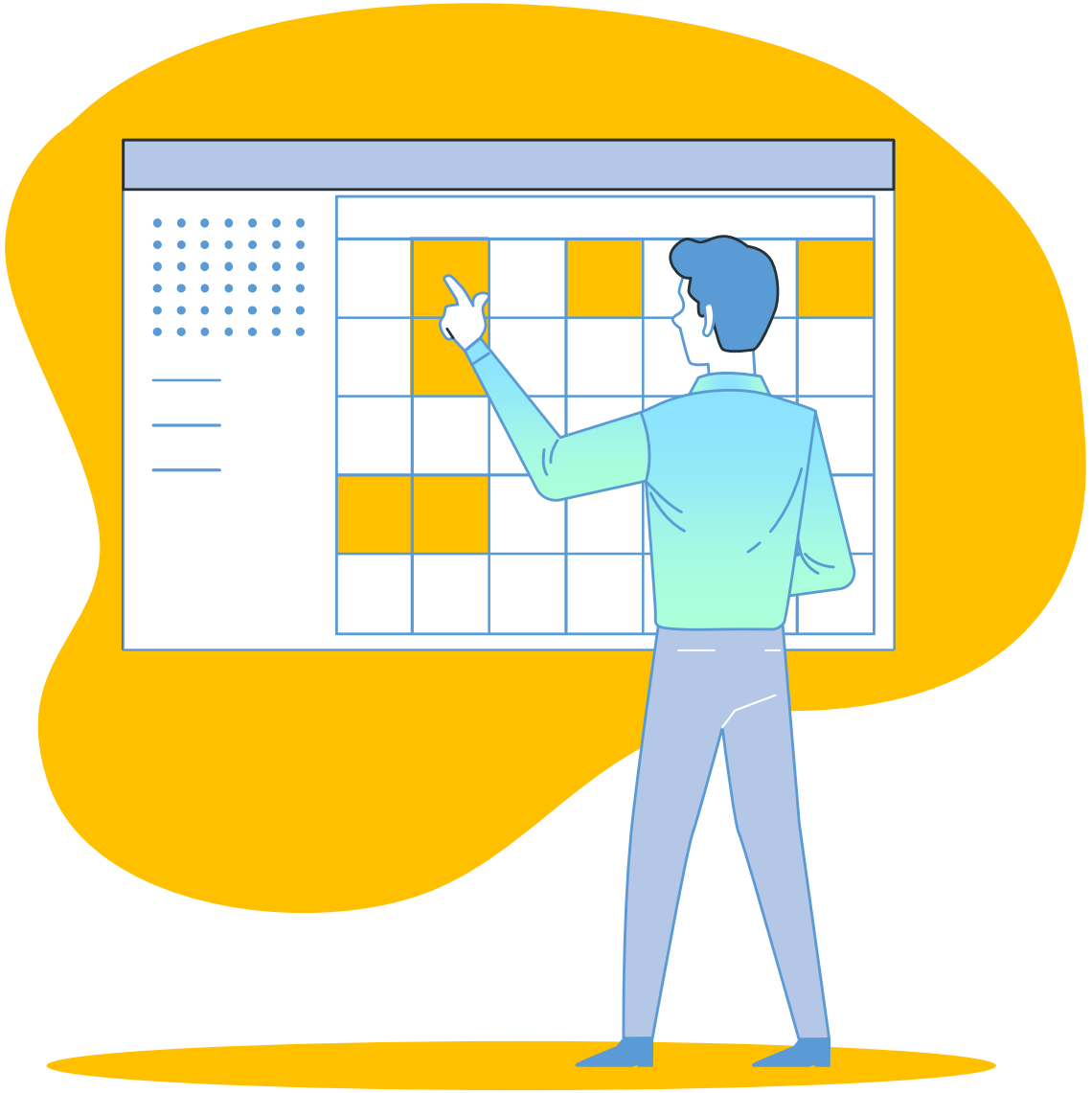
Harbiy soha

Axborot xavfsizligida mavjud muammolar xavflilik darajasiga ko‘ra: zaiflik, tahdid va hujumga olib keluvchilarga bo‘lishi mumkin:

Zaiflik –bu tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi. Zaifliklar tizimlarda katta yoki kichik tarzda mavjud bo‘ladi.

Tahdid –bu mavjud bo‘lgan zaiflik natijasida bo‘lishi mumkin bo‘lgan hujum turi bo‘lib, ular asosan tizimni kamchiliklarini o‘rganish natijasida kelib chiqadi.

Hujum –bu mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi.



Axborot himoyasi

Axborot xavfsizligi konsepsiyasi uchta tashkil etuvchidan iboratligini e‘tiborga olinsa, axborot xavfsizligini ta‘minlash deganda ma‘lumotning quyidagi uchta xususiyatini ta‘minlash tushunish mumkin.

Quyida keltirilgan quyidagi rasmda ushbu uchta xususiyatni ta‘minlashda kriptografik usullarning tutgan o‘rni keltirilgan. Umumiy holda axborot xavfsiziligini ta‘minlash deganda ushbu uchta xususiyatni ta‘minlash tushunilib, har bir xususiyat muhimligi axborotning turiga va foydalanilishga ko‘ra har xil bo‘lishi mumkin.

Konfidensiallik (ruxsatsiz o‘qishning mumkin emasligi) xususiyati axborotning ruxsat etilmagan foydalanuvchilardan yashirish, ma‘lumot ma‘nosini tushunib olmaslik uchun, uni tushunarsiz holatga o‘tkazish kabi vazifalarni bajarish orqali bajariladi. Axborotning ushbu xususiyati kriptografik himoya usullaridan biri sanalgan, shifrlash usullari asosida amalga oshiriladi. Shifrlash usullari yordamida ochiq ma‘lumot yashiringan ko‘rinishdagi shifr matn holatiga aylanadi. Bu esa uni buzg’unchining foydalanishidan oldini oladi.

Butunlik (ruxsatsiz yozishning mumkin emasligi) xususiyati asosida ma‘lumotni uzatish davomida unga o‘zgartirish kiritilganligi yoki kiritilmaganligi aniqlanadi. Ushbu xususiyat boshqacha qilib aytilganda, ma‘lumotni buzg’unchi tomonidan o‘zgartirilgan (almashtirilgan, o‘chirib tashlangan)ligini aniqlashni bildiradi. Axborotning ushbu xususiyati kriptografik himoya usullari asosida amalga oshiriladi. Hozirda kriptografik xesh funksiyalar asosida ma‘lumotning butunligini ta‘minlash usullari amaliyotda keng qo‘llaniladi.

Foydalanuvchanlik xususiyati axborotdan istalgan vaqt doirasida foydalanish imkoniyati mavjudligi bilan belgilanadi. Ushbu xususiyat ochiq turdagi ma‘lumot uchun dastlabki talab etiladigan talabdir. Ushbu xususiyatni buzilishiga olib keluvchi hujum usullaridan biri DOS (Denial Of Service) yoki uning shaklantirilgan ko‘rinishi DDOS (Distributed Denial Of Service) sanalib, ushbu hujum usuli tizimni foydalanuvchanlik xususiyatini buzilishiga olib keladi.

Ushbu uchta xususiyat axborot himoyasining asosiy tashkil etuvchilari sanalib, axborotni himoyalash deganda asosan shu uchta xususiyatni ta‘minlash tushiniladi. Ammo ushbu uchta xususiyat to‘liq bajarilishi uchun bir nechta bajarilishi mumkin bo‘lgan ishlar talab etiladi. Boshqacha qilib aytganda ushbu uchta xususiyatni bajarishdan oldin, quyida keltirilgan amaliyotlarni bajarishga to‘g’ri keladi

Rasm: Foydalanishni boshqarish

Identifikatsiya – bu foydalanuvchini tizimga o‘zini tanitish jarayoni bo‘lib, unda foydalanuvchi nomidan (login), maxsus shaxsiy kartalardan yoki biometrik xususiyatlaridan foydalanish mumkin

Autentifikatsiya – bu foydalanuvchilarni haqiqiyligini tekshirish jarayoni bo‘lib, jarayon natijasida foydalanuvchi tizimdan foydalanish uchun ruxsat oladi yoki olmaydi

Avtorizatsiya – bu foydaluvchiga tizim tomonidan berilgan huquqlar to‘plami bo‘lib, foydalanuvchini tizim doirasida qilishi mumkin bo‘lgan vazifalarini belgilaydi.

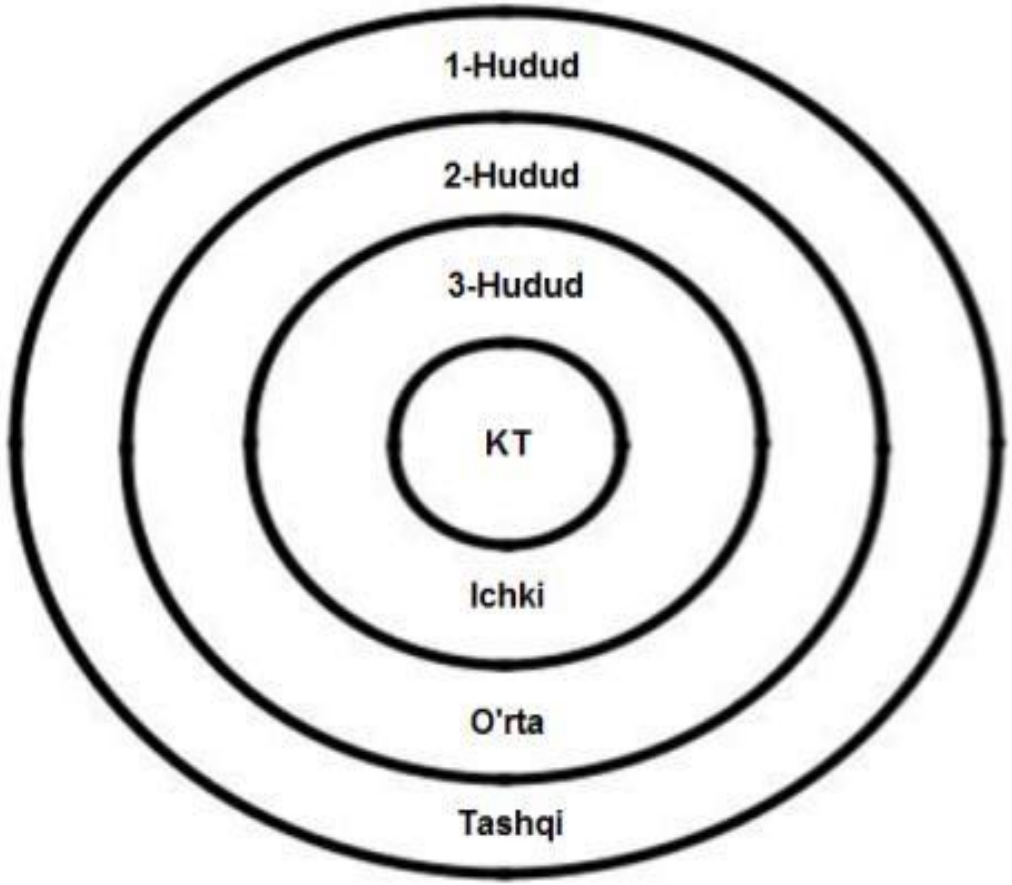
Axborot xavfsizligi siyosati

Axborot xavfsizligi siyosati –tashkilot o‘z faoliyatida rioya qiladigan axborot xavfsizligi sohasidagi hujjatlangan qoidalar, muolajalar, amaliy usullar yoki amal qilinadigan prinsiplar majmui sanalib, u asosida tashkilotda axborot xavfsizligi ta‘minlanadi.

Axborot xavfsizligining siyosatini ishlab chiqishda, avvalo himoya qilinuvchi ob‘ekt va uning vazifalari aniqlanadi. So‘ngra dushmanning bu ob‘ektga qiziqishi darajasi, hujumning ehtimolli turlari va ko‘riladigan zarar baholanadi. Nihoyat, mavjud qarshi ta‘sir vositalari yetarli himoyani ta‘minlamaydigan ob‘ektning zaif joylari aniqlanadi.

Samarali himoya uchun har bir ob‘ekt mumkin bo‘lgan tahdidlar va hujum turlari, maxsus instrumentlar, qurollar va portlovchi moddalarning ishlatilishi ehtimolligi nuqtai nazaridan baholanishi zarur. Ta‘kidlash lozimki, niyati buzuq odam uchun eng qimmatli ob‘ekt uning e‘tiborini tortadi va ehtimolli nishon bo‘lib xizmat qiladi va unga qarshi asosiy kuchlar ishlatiladi. Bunda, xavfsizlik siyosatining ishlab chiqilishida yechimi berilgan ob‘ektning real himoyasini ta‘minlovchi masalalar hisobga olinishi lozim.

Binolar, imoratlar va axborot vositalarining xavfsizlik tizimini nazorat punktlarini bir zonadan ikkinchi zonaga o‘tish yo‘lida joylashtirgan xolda konsentrik halqa ko‘rinishida tashkil etish maqsadiga muvofiq hisoblanadi.



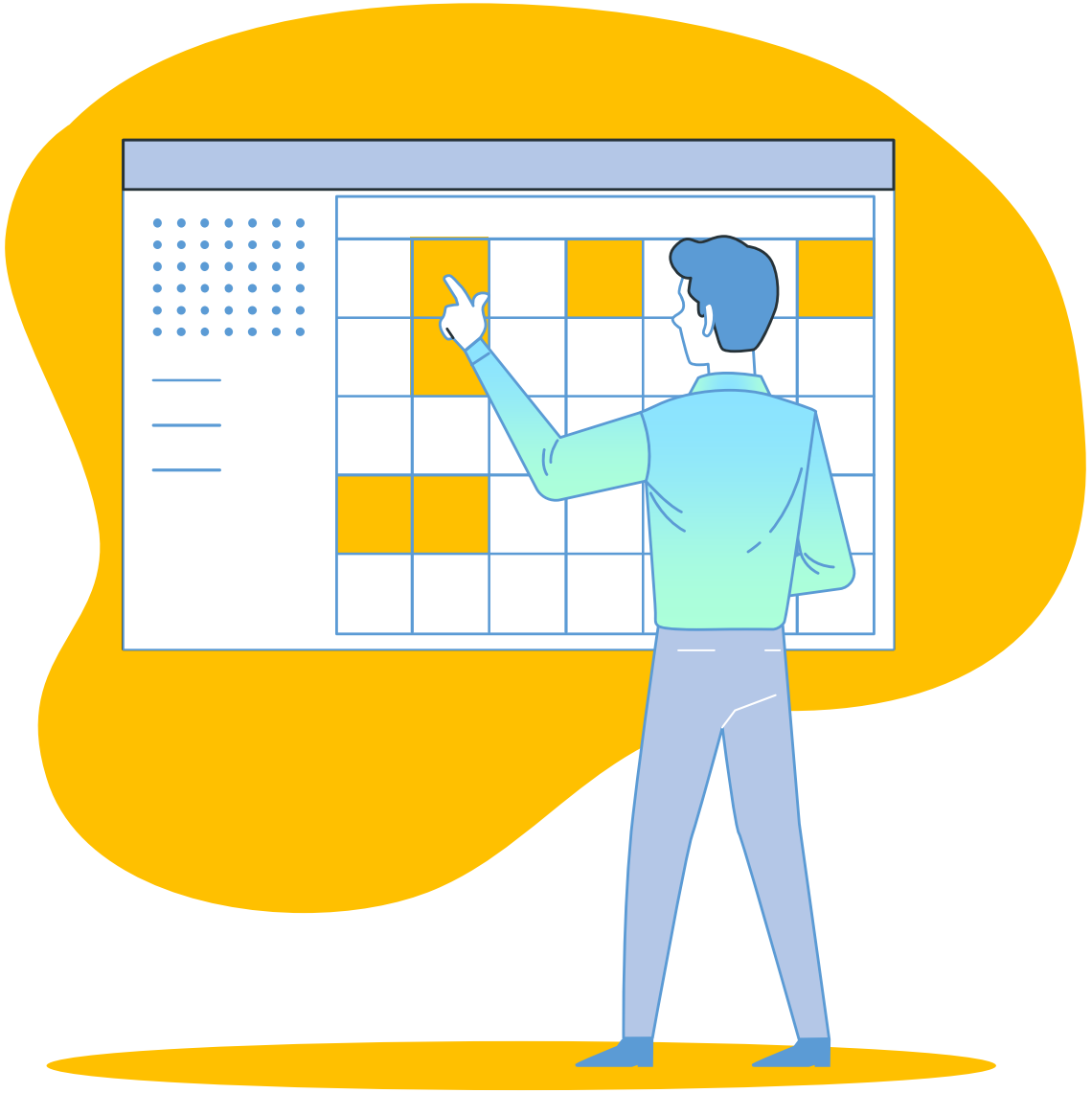
Binodagi kompyuter tizimining xavfsizlik tizimi

1-hudud. Kompyuter tarmog’i (KT) xavfsizligining tashqi zonasi

Ta‘minlanishi: fizik to‘siqlar perimetr bo‘ylab o‘tish joylari xududga kirish nazoratining noavtomatik tizimi;

2-hudud. KT xavfsizligining o‘rtadagi zonasi Ta‘minlanishi: eshiklari elektron himoyalangan nazorat punktlari videokuzatish bo‘sh zonalarini chiqarib tashlash;

3-hudud. KT xavfsizligining ichki zonasi. Ta‘minlash: shaxsiy kompyuterga foydalanish faqat nazorat tizimi orqali identifikatsiyalashning biometrik tizimi;



1.1-расм. Хавфсизликнинг бузилиш манбалари.

Axborotni himoyalash usullari

Kompyuter tarmog’ida axborotni samarali himoyasini ta‘minlash uchun himoya tizimini loyihalash va amalga oshirish uch bosqichda amalga oshirilishi kerak:

-xavf-xatarni tahlillash;

-xavfsizlik siyosatini amalga oshirish;

-xavfsizlik siyosatini madadlash.

Birinchi bosqichda-kompyuter tarmog’ining zaif elementlari tahlillanadi, tahdidlar aniqlanadi va baholanadi, himoyaning optimal vositalari tanlanadi. Xavfxatarni tahlillash xavfsizlik siyosatini qabul qilish bilan tugallanadi.

Ikkinchi bosqich - xavfsizlik siyosatini amalga oshirish moliyaviy xarajatlarni hisoblash va masalalarni yechish uchun mos vositalarni tanlash bilan boshlanadi.

Bunda tanlangan vositalar ishlashining ixtilofli emasligi, vositalarni yetkazib beruvchilarning obro‘si, himoya mexanizmlari va beriladigan kafolatlar xususidagi to‘la axborot olish imkoniyati kabi omillar hisobga olinishi zarur. Undan tashqari, axborot xavfsizligi bo‘yicha asosiy qoidalar aks ettirilgan prinsiplar hisobga olinishi kerak.

Uchinchi bosqich - xavfsizlik siyosatini madadlash bosqichi eng muxim hisoblanadi. Bu bosqichda o‘tkaziladigan tadbirlar niyati buzuq odamlarning tarmoqqa bostirib kirishini doimo nazorat qilib turishni, axborot ob‘ektini himoyalash tizimidagi —tahdidlarni aniqlashni, konfidensial ma‘lumotlardan ruxsatsiz foydalanish hollarini hisobga olishni talab etadi. Tarmoq xavfsizligi siyosatini himoyalashda asosiy javobgarlik tizim adminstratori bo‘ynida bo‘ladi.

Axborotni himoyalashda hozirda qator himoya usullaridan foydalanilib, umummiy holda ular quyidagilarga bo‘linadi:

–**axborotning huquqiy himoyasi;**

–axborotning injiner – texnik himoyasi;

–axborotning tashkiliy himoyasi;

–axborotning dasturiy himoyasi;

–axborotning apparat va apparat-dasturiy himoyasi.

Himoya usullarining turlanishi ularda foydalanilgan vositalar va yondoshishlarga asoslanadi. Himoya usullarining tanlash esa o‘z navbatida tashkilotda ishlab chiqilgan axborot xavfsizligi siyosatiga ko‘ra amalga oshiriladi. Odatda axborot xavfsizligini ta‘minlashda barcha himoya usullaridan kompleks tarzda foydalanish orqali erishiladi.

Nazariy savollar:

1.Axborot xavfsizligi nima?

3.Axborot xavfsizligi sohalari?

4. Foydalanishni boshqarish qanday tashkil qilinadi?

5. Axborot xavsizligi xususiyatlari

6.Axborot xavfsizligi siyosati?

7.Axborotni himoyalash usullari?

8. Axborot xavfsizligida mavjud muammolar: zaiflik, tahdid va hujumga olib keluvchilar haqida ma'lumot bering

9. Axborot xavfsizligi konsepsiyasi tashkil etuvchilari haqida ma'lumot bering

10. Binodagi kompyuter tizimining xavfsizlik tizimi bosqichlari.