**Axborot xavfsizligi talablari bo‘yicha sertifikatlashtirish ~~-~~**

**kiberhimoya qilishning ishonchli mexanizmidir**

Axborot jamiyati rivojlanishi bilan kiberhujum tahdidlarining davlat tashkilotlari va iqtisodiy va ijtimoiy-madaniy ob’ektlar faoliyati xavfsizligi uchun xavfi va ahamiyati ortib bormoqda.

Ushbu muammoning ahamiyati O‘zbekiston Respublikasining “Kiberxavfsizlik to’g’risida” gi Qonuniga muvofiq davlat organlari va tashkilotlariga axborot tizimlari va resurslarini kiberhimoya qilish uchun sertifikatlangan apparat, apparat-dasturiy va dasturiy vositalardan foydalanish majburiyati yuklatilganligi bilan ta’kidlanadi.

Davlat organlari va tashkilotlarining axborot tizimlari va resurslari, muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash uchun qo’llaniladigan apparat, apparat-dasturiy va dasturiy vositalari majburiy tarzda sertifikatlashtirilishi lozim, jumladan:

- davlat boshqaruvi va davlat xizmatlari ko‘rsatish sohasida,

- mudofaa,

- davlat xavfsizligi, huquq-tartibotni ta’minlash,

- yoqilg‘i-energetika kompleksi (atom energetikasi),

- kimyo, neft-kimyo sohalari,

- metallurgiya,

- suvdan foydalanish va suv ta’minoti,

- qishloq xo‘jaligi,

- sog‘liqni saqlash,

- uy-joy kommunal xizmatlari,

- bank-moliya tizimi,

- transport,

- axborot-kommunikatsiya texnologiyalari,

- ekologiya va atrof-muhitni muhofaza qilish,

- strategik ahamiyatga ega foydali qazilmalarni qazib olish va qayta ishlash,

- ishlab chiqarish sohasi,

- iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada faoliyat ko‘rsatayotgan infratuzilma obyektlari kiradi.

Sertifikatlashtirishda qo‘llaniladigan asosiy majburiy talablar quyidagi davlat standartlari bilan tartibga solinadi:

* O‘z DSt 2814:2014 “Axborot texnologiyasi. Avtomatlashtirilgan tizimlar. Axborotga ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;
* O‘z DSt 2815:2014 “Axborot texnologiyasi. Tarmoqlararo ekranlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;
* O‘z DSt 2816:2014 “Axborot texnologiyasi. Axborotni muhofaza qilish vositalarining dasturiy ta’minotini deklaratsiya qilinmagan imkoniyatlar yo‘qligini nazorat qilish darajasi bo‘yicha tasniflash”;
* O‘z DSt 2817:2014 “Axborot texnologiyasi. Hisoblash texnikasi vositalari. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajasi bo‘yicha tasniflash”.

O‘z DSt 2814 davlat standarti turli avtomatlashtirilgan tizimlarida (AT) axborotni himoya qilish talablarini belgilaydi, shu bilan birga AT muhofazalanganlik darajasini tanlash buyurtmachi va ishlab chiquvchi tomonidan axborotni himoya qilish bo’yicha mutaxassislarni jalb qilgan holda amalga oshiriladi.

“Kiberxavfsizlik markazi” DUK mutaxassislari ATni loyihalash, ishlab chiqish va joriy qilishning har qanday bosqichida ushbu masala bo‘yicha yordam ko‘rsatishga tayyor.

O‘z DSt 2814 standartiga muvofiq, davlat sirlari va maxfiy ma’lumotlarga (muhofazalanganlik darajasidan qat’iy nazar) tegishli ma’lumotlarni qayta ishlash yoki saqlash uchun mo‘ljallangan barcha AT larda quyidagilar qo‘llanilishi kerak:

- O‘z DSt 2815 sertifikatlashtirilgan tarmoqlararo ekranlar;

- O‘z DSt 2816 bo‘yicha deklaratsiya qilinmagan imkoniyatlar yo‘qligi bo‘yicha sertifikatlashtirilgan axborotni himoya qilish vositalarining dasturiy ta’minoti (DT)
(shu jumladan umumiy tizim va amaliy dasturlarga o’rnatilgan DT);

- O‘z DSt 2817 bo‘yicha sertifikatlashtirilgan hisoblash texnikasi vositalari.

ATni ishlab chiqishda boshqa standartlardan (O‘z DSt 2815 – O‘z DSt 2817) foydalanish zarurligini ko‘rsatishdan tashqari, O‘z DSt 2814 davlat standarti axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik uchun dasturiy-texnik vositalar kompleksining bir qator quyi tizimlariga sertifikatlashtirishda sinovdan o’tkaziladigan talablarini o‘z ichiga oladi:

- kira olishni boshqarish;

- ro‘yxatdan o‘tish va hisobga olish;

- kriptografik himoya;

- dasturiy ta’minot va ma’lumotlarning yaxlitligini ta’minlash.

Shuni inobatga olish lozimki, O‘z DSt 2814 davlat standarti foydalanish sogasi keng hamda nafaqat sertifikatlashtirish paytida sinovdan o‘tgan texnik talablarni, balki davlat tashkilotlari va MAI ob’ektlarining egalari o‘zlarining axborot tizimlarini joriy etish va ishlashini ta’minlash bosqichlarida bajarishi kerak bo’lgan tashkiliy masalalarni ham o‘z ichiga oladi.

O‘z DSt 2815 davlat standarti tarmoqlararo ekranlari (firewall) tasnifini axborotdan ruxsatsiz foydalana olishdan muhofazalanganligi ko'rsatkichlari darajasiga muvofiq belgilaydi, xususan, quyidagi funktsional xususiyatlar asosida:

- foydalana olishni boshqarish (ma'lumotlarni filtrlash va adreslarni translatsiya qilish);

- identifikatsiya va autentifikatsiya;

- qayd qilish;

- ma’muriy boshqarish, tiklash va boshqa bir qator ko’rsatkichlar.

Ushbu holatni hisobga olgan holda, tarmoqlararo ekranlarni sertifikatlashtirish sinovining asosiy usuli, tarmoqlararo ekranlarni funktsional imkoniyatlarini ishlab chiqaruvchilarning belgilangan talablari va texnik hujjatlariga muvofiqligiga tekshirishdir.

O‘z DSt 2816 davlat standartining talablari **axborot xavfsizligini ta’minlash vositalarining barcha turlariga** (mahalliy va import qilinadigan) taalluqli bo‘lib, ularning dasturiy ta’minotida deklaratsiya qilinmagan imkoniyatlar yo‘qligini nazorat qilishni tartibga soladi. **Axborot xavfsizligi vositalarini ishga tushirishdan oldin
O‘z DSt 2816 davlat standarti talablari bo‘yicha muvofiqlik sertifikatini olish majburiydir.**

Bunday nazoratni amalga oshirish uchun O‘z DSt 2816 davlat standarti talablariga muvofiq sertifikatlash sinovlarini o‘tkazish sunov metodikasiga asosan, sinov laboratoriyasiga DT ning manba kodini hamda amalga oshiradigan barcha funksiyalar tavsifi va uning yuklash kodlari bilan taqdim etishni hamda ularni o‘rganish va qiyosiy tahlil qilishni o‘z ichiga oladi.

O’z DSt 2817 davlat standarti axborot tizimlari joriy etiladigan operatsion tizimlarga talablarni belgilaydi. Bir qator funktsional parametrlar bo‘yicha ularning xavfsizlik ko‘rsatkichlarini nazorat qilishni ta‘minlaydi, jumladan:

- foydalana olishni nazorat qilish;

- identifikatsiya va autentifikatsiya;

- xotirani tozalash;

- hujjatlarni markirovkalash;

- axborotni ajratib olinadigan tashuvchiga kiritish va undan chiqarishni muhofaza qilish va boshqa ko‘rsatkichlar.

Umuman olganda, yuqoridagilardan ko‘rinib turibdiki, “Kiberxavfsizlik markazi” DUKda sertifikatlashtirish uchun qo‘llaniladigan davlat standartlari axborot tizimlarining kiberhimoyasi ishonchliligini kompleks tekshirish imkonini beruvchi yagona talablar majmuasini tashkil etadi.

 “Kiberxavfsizlik markazi” DUK zamonaviy sinov uskunalari va sertifikatlashtirish sohasida yuqori malakali mutaxassislarga ega boʻlib,
davlat tashkilotlariga, muhim axborot infratuzilmasi obyektlarining egalariga,
ishlab chiquvchilarga va DT yetkazib beruvchilariga axborotni kibertahdidlardan ishonchli himoya qilishga va O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida” gi Qonuni talablarini amalga oshirishda amaliy yordam beradi.