DOI: https://doi.org/10.5281/zenodo.11245308

XALQARO STANDARTLAR. ISO/IEC 15408 (“UMUMIY MEZONLAR”). AQSH XAVFSIZLIK STANDARTLARI TCSEC VA FIPS.

Ramazonova Madina Shavkatovna
Ilmiy rahbar

Tojimuratov Shuxratbek Dilmurodjon o‘g‘li
Mirzayev Bekzod Toxirboy o‘g‘li
Babajanov Jaloliddin Umidjon o‘g‘li
Toshkent axborot texnologiyalar universiteti talabalari
abdujabbor.madina.1989@gmail.com

Annotatsiya: *ISO/IEC 15408 xalqaro standarti, shuningdek, "Umumiy mezonlar" deb nomlanuvchi, axborot texnologiyalari xavfsizligini baholash uchun mo‘ljallangan universal standartdir. 1999-yil dekabrda nashr etilgan bu standart ko‘plab mamlakatlar mutaxassislarining qariyb o‘n yillik hamkorlik mehnati natijasidir. ISO/IEC 15408 axborot tizimlari va texnologiyalari xavfsizlik talablarini baholashda qo‘llaniladi. Ushbu standart Milliy Standartlar va Texnologiyalar Instituti (AQSh), Aloqa xavfsizligini ta’minlash muassasasi (Kanada), Axborot xavfsizligi agentligi (Germaniya) va boshqa xalqaro tashkilotlar hamkorligida ishlab chiqilgan. "Umumiy mezonlar" axborot xavfsizligi talablarini tizimlashtiradi va baholash metodologiyasini taqdim etadi. U xavfsizlik talablarini belgilash, dizayn va ishlab chiqish, testlash va sertifikatlash, shuningdek, joriy qilish kabi hayotiy sikl bosqichlarini o‘z ichiga oladi. Ushbu standartning asosiy afzalliklari uning moslashuvchanligi, to‘liqligi, va kengaytirish uchun ochiqligidir.*

Kalit so‘zlar: *ISO/IEC 15408, Umumiy mezonlar, Axborot texnologiyalar xavfsizligi, Standartlarshtirsh, Xavfsizlik muhiti, Xavfsizlik zaifliklari*

ISO/IEC 15408 xalqaro standarti “Axborot texnologiyalari xavfsizligini baholash mezonlari” “Umumiy mezonlar”.

Integratsiya yo‘lidan borib, 1993 yil iyun oyida Xalqaro Standartlashtirish Tashkiloti (ISO) yuzdan ortiq turli xil hujjatlarni o‘z ichiga olgan "umumiy mezonlar" deb nomlangan umumiy foydalanish uchun mo‘ljallangan axborot texnologiyalari xavfsizligini baholash xalqaro standartini yaratishga kirishdi. Baholash standartlari

orasida eng keng qamrovlisi "Axborot texnologiyalari xavfsizligini baholash mezonlari" standartidir (1999 yil 1 dekabrda nashr etilgan).

Ushbu xalqaro standart bir necha mamlakatlar mutaxassislarining qariyb o‘n yillik mehnati natijasi bo‘lib, o‘sha paytda milliy va xalqaro miqyosda mavjud bo‘lgan hujjatlar tajribasini o‘zida mujassam etgan. Tarixiy sabablarga ko‘ra, ushbu standart ko‘pincha "Umumiy mezonlar" (yoki UM) deb ataladi.

Umumiy mezonlarni ishlab chiqishda quyidagilar ishtirok etgan:

– Milliy standartlar va texnologiyalar instituti va Milliy xavfsizlik agentligi (AQSh);

– Aloqa xavfsizligini ta’minlash muassasasi (Kanada);

– Axborot xavfsizligi agentligi (Germaniya);

– Milliy aloqa xavfsizligi agentligi (Gollandiya);

– AT xavfsizligi va sertifikatlashtirish dasturini amalga oshiruvchi organlar (Angliya);

– Tizimlar xavfsizligini ta’minlash markazi (Frantsiya).

Yangi kriteriyalar AT xavfsizligini baholashni o‘zaro tan olish talablariga moslashtirilgan va bunday baholashlar uchun asos bo‘lib xizmat qilish uchun mo‘ljallangan. Dunyoning eng yaxshi mutaxassislari tomonidan ishlab chiqilgan UM o‘n yil davomida qayta-qayta tahrirlangan. Umumiy mezonlarning (UM) birinchi versiyasi 1.0 1996 yil yanvar oyida yakunlangan va 1996 yil aprel oyida ISO tomonidan tasdiqlangan. UMning 1.0-versiyasi asosida bir qator eksperimental baholashlar o‘tkazildi va hujjatning keng muhokamasi tashkil etildi. 1998 yil may oyida UMning 2.0 versiyasi nashr etildi va uning asosida 1999 yil iyun oyida ISO/IEC 15408 xalqaro standarti qabul qilindi.

ISO/IEC 15408 hujjat matni 1999 yil 1 dekabrda"Axborot texnologiyalari xavfsizligini baholashning umumiy mezonlari" (UM) sifatida nashr etilgan. Standartni qabul qilishning yakuniy bosqichida kiritilgan o‘zgartirishlar UM 2.1 versiyasida hisobga olingan.

ISO/IEC 15408 xalqaro standarti AT xavfsizligini baholash vositalari va ulardan foydalanish tartibini belgilaydigan eng universal va ilg‘or standartdir. U To‘q sariq kitobining analogi hisoblanadi, ammo hujjatlarning turli yurisdiktsiyasi tufayli u To‘q sariq kitobning o‘rnini bosmaydi. To‘q sariq kitob faqat AQSh Mudofaa vazirligi tomonidan qo‘llaniladi, ISO/IEC 15408 ko‘plab mamlakatlar tomonidan ratifikatsiya qilingan. To‘q sariq kitobdan farqli o‘laroq, UM oldindan belgilangan "xavfsizlik sinflarini" o‘z ichiga olmaydi. Bunday sinflar ma’lum bir axborot tizimi uchun mavjud bo‘lgan xavfsizlik talablari asosida tuzilishi mumkin.

"Umumiy mezonlar" global miqyosda AT xavfsizligini baholash natijalarini o‘zaro tan olish uchun yaratilgan va uning asosini ifodalaydi. Ular AT vositalari va

tizimlarining xavfsizlik funksiyalariga qo‘yiladigan umumiy talablar, shuningdek, testlash jarayonida ularga nisbatan qo‘llaniladigan kafolatlar asosida axborot xavfsizligi va risklarga chidamliligini mustaqil baholash natijalarini solishtirish imkonini beradi.

UM ning asosiy afzalliklari:

– axborot xavfsizligi talablarining **to‘liqligi;**

– ilm-fan va texnikaning so‘nggi yutuqlarini hisobga olgan holda **qo‘llashda moslashuvchanlik va** keyingi kengaytirish uchun ochiqligi.

Kriteriyalar AT vositalari yoki tizimining (baholash ob’yekti) xavfsizlik xususiyatlarini o‘rganishda uchchala foydalanuvchilar guruhining (iste’molchilar, ishlab chiquvchilar va baholovchilar) ehtiyojlarini qondirish uchun ishlab chiqilgan. 1C boshqaruv dasturlarini ishlab chiquvchilar nuqtai nazaridan, UMni "dasturlarni" (xavfsizlik vazifalari, standart xavfsizlik profillari va boshqalar) mazmunli yozishga yordam beradigan kutubxonalar to‘plami deb hisoblash mumkin. Dasturchilar yaxshi kutubxona dastur ishlab chiqishni qanday soddalashtirishi va ularning sifatini yaxshilashini biladilar. Kutubxonalarsiz, "noldan" dasturlar anchadan beri yozilmaydi; xavfsizlikni baholash ham murakkablikning taqqoslanadigan darajasiga yetdi va bunda "Umumiy mezonlar" tegishli vositalarni taqdim etdi.

Shuni ta’kidlash kerakki, xavfsizlik talablari kutubxona funktsiyalari bo‘lishi kerak bo‘lganidek parametrlashtirilishi mumkin.

Ushbu standart AT xavfsizlik xususiyatlarini ishlab chiqishda, shuningdek, shunga o‘xshash xususiyatlarga ega tijorat mahsulotlarini sotib olishda qo‘llanma sifatida foydalidir.

Ushbu standartni ishlab chiqish quyidagi asosiy maqsadlarga ega edi:

– AT xavfsizligini baholash sohasidagi milliy standartlarni unifikatsiya qilish;

– AT xavfsizligini baholashga ishonch darajasini oshirish;

– sertifikatlarni o‘zaro tan olish asosida AT xavfsizligini baholash uchun xarajatlarni kamaytirish.

Yangi mezonlar global AT bozorida standartlashtirilgan xavfsizlikni baholash natijalarining o‘zaro tan olinishini ta’minlash uchun ishlab chiqilgan.

Tarkibiy jihatdan "Umumiy mezonlar" 4 qismdan iborat.

"Umumiy mezonlar" ning birinchi qismida umumiy tushunchalar, konsepsiyalar, AT xavfsizligini baholash modeli va metodologiyasining tavsifi mavjud. Unda kontseptual apparat kiritilgan va mavzu sohasini rasmiylashtirish tamoyillari belgilangan.

"Umumiy mezonlar" ning ikkinchi qismida "umumiy mezonlar" himoya vositalarining funksionalligiga qo‘yiladigan talablar keltirilgan va AT-da amalga oshirilgan xavfsizlik funktsiyalarining to‘liqligini baholash uchun xavfsizlikni tahlil qilishda bevosita foydalanish mumkin.

"Umumiy mezonlar" ning uchinchi qismi, xavfsizlik funktsiyalarini amalga oshirishning yetarliligi uchun boshqa talablar bilan bir qatorda, - AVA deb nomlangan himoya vositalari va mexanizmlarining zaifliklarini tahlil qilish uchun talablar sinfini o‘z ichiga oladi:

Zaiflik baholash. Ushbu talablar sinfi quyidagi turdagi zaifliklarning oldini olish, aniqlash va yo‘q qilish uchun ishlatilishi kerak bo‘lgan usullarni belgilaydi:

– axborotning sizib chiqishi uchun yon kanallarning mavjudligi;

– konfiguratsiyadagi xatolar yoki tizimdan noto‘g‘ri foydalanish tizimning xavfli holatga o‘tishiga olib keladi;

– tegishli xavfsizlik funktsiyalarini amalga oshiradigan xavfsizlik mexanizmlarining yetarli darajada ishonchli emasligi (mustahkamligi);

– foydalanuvchilarga mavjud xavfsizlik mexanizmlarini chetlab o‘tgan holda axborotga kirish imkonini beruvchi axborot xavfsizligi vositalarida zaifliklar (“teshiklar”) mavjudligi. Shu bilan birga, UMda asosiy e’tibor ruxsatsiz kirishdan (ATA) himoya qilishga qaratilgan. Tasodifiy yoki qasddan qilingan harakatlar natijasida o‘zgartirishlar yoki ma’lumotlarga kirishni yo‘qotish va axborot xavfsizligining bir qator boshqa jihatlari ko‘rib chiqilmagan. Masalan, ma’muriy xavfsizlik choralarini baholash, garov elektromagnit nurlanishdan xavfsizlikni baholash, turli vositalar va xavfsizlik choralarini hisoblash usullari, axborotni himoya qilishning kriptografik usullarini baholash mezonlari.

Xavfsizlik tekshiruvlarini o‘tkazishda ushbu talablar AT zaifliklarini tahlil qilish uchun qo‘llanma va mezon sifatida ishlatilishi mumkin.

"Umumiy mezonlar" (UM) ning asosiy o‘ziga xos xususiyatlari:

– talablarni ishlab chiqish va AT xavfsizligini baholash uchun maxsus metodologiya va tizimning mavjudligi. Muvofiqlikni atamalar va talablarni taqdim etishning mavhumlik darajasidan IT-mahsulotlari hayotiy siklining barcha bosqichlarida xavfsizlikni baholashda ulardan foydalanishgacha kuzatish mumkin;

– hozirgi kunga qadar AT xavfsizligi talablarining eng to‘liq to‘plami bilan tavsiflanadi;

– talablar va xavfsizlikni ta’minlash talablariga aniq bo‘linishi, xususan:

a) funktsional talablar - xavfsizlik xizmatlariga tegishli (identifikatsiya, autentifikatsiya, kirishni nazorat qilish, audit va boshqalar);

b) ishonch talablari - ishlab chiqish texnologiyasi, testlash, zaifliklarni tahlil qilish, operatsion hujjatlar, yetkazib berish, qo‘llab-quvvatlash, ya’ni AT-mahsulotlarning hayot siklining barcha bosqichlariga tegishli;

– AT mahsulotlari xavfsizligiga ishonchning turli darajalarini shakllantirish uchun ishlatilishi mumkin bo‘lgan xavfsizlik ishonch shkalasi (xavfsizlik ishonchining

baholangan darajalari);

– foydalanish qulayligini ta’minlaydigan yagona talab identifikatorlari bilan "sinf - oila - komponent - element" iyerarxiyasi bo‘yicha talablarni tizimlashtirish va tasniflash ;

– darajasi bo‘yicha tartiblangan, shuningdek, talablar paketiga guruhlangan oilalar va sinflardagi talablarning tarkibiy qismlari;

– AT mahsulotlarining har xil turlari uchun xavfsizlik talablarini shakllantirishga yondashuvning moslashuvchanligi va ularni qo‘llash shartlari UMda belgilangan standartlashtirilgan tuzilmalar (himoya profillari va xavfsizlik vazifalari) shaklida zarur talablar to‘plamini maqsadli shakllantirish imkoniyati bilan ta’minlanadi;

– talablar jamlanmasini keyinchalik kengaytirish uchun ochiqligi.

Ushbu turdagi oldingi mahalliy va xorijiy hujjatlar davlat sirlarini o‘z ichiga olishi mumkin bo‘lgan maxfiy ma’lumotlarni qayta ishlaydigan hukumat yoki harbiy tizim shartlari bilan bog‘liq edi. Ushbu standartning chet elda chiqarilishi va joriy etilishi hisoblash tizimlarining axborot xavfsizligini ta’minlash uchun mo‘ljallangan yangi, standartlashtirilgan arxitekturani ishlab chiqish bilan birga amalga oshirildi. Boshqacha aytganda, umumiy mezonlarga javob beradigan kompyuter texnikasi va dasturiy ta’minoti yaratiladi.

ISO/IEC 15408 xalqaro standarti (“Umumiy mezonlar”) AT xavfsizligini baholash mezonlarini ishlab chiqish va amaliy qo‘llash bo‘yicha turli davlatlar tajribasini sintez qilish natijasidir.

AT xavfsizligini baholashning me’yoriy-huquqiy bazasini rivojlantirish tahlili "umumiy mezonlar" yaratilishiga olib kelgan motivatsion asoslarni tushunishga imkon beradi.

Yangi mezonlar global IT bozorida standartlashtirilgan xavfsizlikni baholash natijalarini o‘zaro tan olishni ta’minlash uchun ishlab chiqilgan.

"Umumiy mezonlar" "To‘q sariq kitob" dan foydalanish mazmuni va tajribasini umumlashtirdi, Yevropa mezonlarining kafolat darajalarini ishlab chiqdi va AQShning "Federal mezonlari" ning himoya profillari kontseptsiyasini haqiqiy tuzilmalarga joriy qildi.

UMda quyidagilar amalga oshirildi:

– keng ko‘lamli funktsional talablar va xavfsizlikni ta’minlash talablarini tasniflandi;

– guruhlash tuzilmalari aniqlandi.

Axborot xavfsizligi sohasidagi ekspertlarning baholashlari shuni ko‘rsatadiki, tizimlashtirish darajasi, to‘liqligi va talablarni batafsil aniqlash imkoniyatlari, universalligi va qo‘llanilishining moslashuvchanligi nuqtai nazaridan, UM hozirda mavjud standartlarning eng ilg‘orini ifodalaydi. Bundan tashqari, eng muhimi, qurilishning o‘ziga xos xususiyatlari tufayli u rivojlanish uchun deyarli cheksiz

imkoniyatlarga ega, bu funktsional standart emas, balki vazifalar metodologiyasi, baholash va to‘planishi va aniqlanishi mumkin bo‘lgan it xavfsizligi talablari katalogi.

Muayyan ma’noda, funktsional standartlarning roli OK talablarining tavsiyalari va katalogini hisobga olgan holda shakllantirilgan himoya profillari tomonidan amalga oshiriladi, ammo ma’lum bir mahsulot yoki AT mahsulotining xavfsizligini ta’minlash uchun zarur bo‘lgan boshqa talablarni ham o‘z ichiga olishi mumkin.

To‘q sariq kitob singari, UMlar xavfsizlik talablarining ikkita asosiy turini o‘z ichiga oladi:

– xavfsizlikning faol tomoniga mos keladigan, xavfsizlik funktsiyalari va ularni amalga oshiruvchi mexanizmlarga taqdim etiladigan – funktsional talablar;

– xavfsizlik funktsiyalarini amalga oshirishning yetarliligiga, passiv tomonga mos keladigan, ishlab chiqish va ishlatish texnologiyasi va jarayoniga qo‘yiladigan – ishonch talablari.

UMda xavfsizlik statik jihatdan emas, balki baholanayotgan ob’yektning hayot sikliga (yaratish va ekspluatatsiya bosqichlariga) nisbatan ko‘rib chiqilishi juda muhimdir.

Quyidagi bosqichlar ajratiladi:

– foydalanish shartlari, maqsadlari va xavfsizlik talablarini aniqlash;
– dizayn va ishlab chiqish;
– testlash, baholash va sertifikatlash;
– amalga oshirish va joriy qilish.

UMda baholash ob’yekti ma’lum shartlar va tahdidlar bilan tavsiflangan xavfsizlik muhiti kontekstida ko‘rib chiqiladi.

O‘z navbatida, tahdidlar quyidagi parametrlar bilan tavsiflanadi :

– tahdid manbai;
– ta’sir qilish usuli;
– foydalanish mumkin bo‘lgan zaifliklar;
– zarar yetkazilishi mumkin bo‘lgan resurslar (aktivlar).

Zaifliklar quyidagi kamchiliklar tufayli yuzaga kelishi mumkin:

– xavfsizlik talablari;
– loyihalash;
– ekspluatatsiya.

Iloji bo‘lsa, zaif tomonlarni yo‘q qilish, minimallashtirish yoki hech bo‘lmaganda ularni ataylab ishlatish yoki tasodifiy faollashtirish natijasida yuzaga kelishi mumkin bo‘lgan zararni cheklashga harakat qilish kerak.

Dasturlash texnologiyasi nuqtai nazaridan, UM eskirgan kutubxona (ob’yekt emas) yondashuvidan foydalanadi. Biroq, talablar maydonini tuzish uchun "Umumiy mezonlar" ierarxiyani kiritilgan: sinf - oila - komponent - element .

Sinflar talablarning eng umumiy, "predmet" guruhini belgilaydi (masalan, funktsional javobgarlik talablari).

Oilalar o‘z talablarining jiddiyligi va boshqa nuanslari bilan farqlanadi.

Komponent - bu bir butun sifatida paydo bo‘ladigan minimal talablar to‘plami.

Element ajralmas talabdir.

Xuddi kutubxona funktsiyalari o‘rtasida bo‘lgani kabi, UM komponentlari o‘rtasida ham bog‘liqliklar mavjud bo‘lishi mumkin. Ular xavfsizlik maqsadiga erishish uchun komponentning o‘zi yetarli bo‘lmaganda paydo bo‘ladi. Aslida, barcha komponentlarning kombinatsiyasi amaliy ma’noga ega emas va qaramlik tushunchasi kutubxona tashkil etishning ekspressivligi yo‘qligining o‘rnini to‘ldirishga yordam beradi, garchi u funktsiyalarni mazmunli ob’yekt interfeyslariga birlashtirish o‘rnini bosa olmaydi.

Kutubxonalar yordamida ikki turdagi me’yoriy hujjatlarni yaratish mumkin: himoya profili va xavfsizlik vazifasi.

Xavfsizlik profili (XP) - ma’lum bir sinfdagi mahsulotlar va/yoki tizimlar qondirishi kerak bo‘lgan odatiy talablar to‘plami (masalan, davlat tashkilotlaridagi kompyuterlardagi operatsion tizimlar).

Xavfsizlik vazifasi - muayyan rivojlanish uchun talablar to‘plamini o‘z ichiga oladi, ularni amalga oshirish belgilangan xavfsizlik maqsadlariga erishishni ta’minlaydi.

"Umumiy mezonlar" bo‘yicha himoya turlari va usullarining tasnifini shakllantirish standart funktsional talablar va xavfsizlikni ta’minlash talablaridan maksimal darajada foydalangan holda bir nechta iyerarxik tartiblangan (ortib borayotgan talablarni o‘z ichiga olgan) himoya profillarini aniqlashni anglatadi.

Himoya profillarining barcha to‘plamidan ma’lum bir kichik to‘plamni tanlash asosan sub’ektivdir. Bir qator sabablarga ko‘ra (ulardan biri ob’yektga yo‘naltirilgan yondashuvga rioya qilish istagi), birinchi navbatda asosiy (minimal) XPni ta’kidlab, tasniflash uchun boshlang‘ich nuqtani shakllantirish va funktsional paketlarga qo‘shimcha talablarni tuzish tavsiya etiladi.

Funksional paket – bu muayyan xavfsizlik maqsadlariga erishish uchun birlashtirilgan komponentlarning qayta ishlatilishi mumkin bo‘lgan to‘plami .

"Umumiy mezonlar" paketlar tuzilishini, tekshirish tartib-qoidalarini, ro‘yxatdan o‘tishni va hokazolarni tartibga solmaydi, ularga XPni yaratishning texnologik vositasi rolini belgilaydi.

Asosiy xavfsizlik profili - asosiy (har qanday holatda ham majburiy) qobiliyatlarga qo‘yiladigan talablarni o‘z ichiga olishi kerak.

Hosil bo‘lgan profillar asosiy profildan kerakli kengaytma paketlarini qo‘shish orqali olinadi, ya’ni ob’yektga yo‘naltirilgan dasturlash tillarida olingan sinflar qanday yaratilganiga o‘xshash.

"Umumiy mezonlar" beshta alohida, o‘zaro bog‘liq bo‘lgan qismlar to‘plamidir. Bularga quyidagilar kiradi:

1. Kirish va umumiy model
2. Xavfsizlik finksional talablari
3. Himoya mexanizmlarining ishonchliligiga qo‘yiladigan talablar
4. Oldindan belgilangan himoya profillari
5. Ximoya profillarini ro‘yhatga olish protseduralari.

Oldindan belgilangan himoya profillari asl mezonlarda belgilangan funktsional va ishonchlilik talablarini ifodalovchi namunaviy himoya profillarini o‘z ichiga oladi, jumladan, TISEC, CTCPEC, FC va TCSEC, shuningdek, ushbu mezonlarda ko‘rsatilmagan talablar.

UMning to‘rtinchi qismi ro‘yxatdan o‘tish protsedurasidan o‘tgan xavfsizlik profillarining reestridir. Ushbu reestr vaqt o‘tishi bilan yangilanadi, chunki yangi himoya profillari Umumiy mezonlarning beshinchi qismida tavsiflangan ro‘yxatga olish protsedurasiga muvofiq ro‘yxatga olinadi.

Yangi xavfsizlik profillari foydalanuvchilar guruhlari va kompyuter ilovalari provayderlari tomonidan ishlab chiqiladi va mustaqil ekspertlar tomonidan “Umumiy mezonlar” da ifodalangan talablarga muvofiq baholanadi.

"Umumiy mezonlar" "To‘q sariq kitob" dan foydalanish mazmuni va tajribasini umumlashtirdi, Yevropa va Kanada mezonlarini ishlab chiqdi va AQSh federal mezonlarining odatiy himoya profillari kontseptsiyasini haqiqiy tuzilmalarda o‘zida mujassam etdi. “Umumiy mezonlar” AT xavfsizligi talablarining keng doirasini tasniflaydi, ularni guruhlash tuzilmalari va foydalanish tamoyillarini belgilaydi.

"Umumiy mezon" ning asosiy afzalliklari:

– xavfsizlik talablarining to‘liqligi va ularni tizimlashtirilganligi;
– qo‘llashda moslashuvchanligi va keyingi rivojlanish uchun ochiqligi.

AT xavfsizligini tahlil qilish bo‘yicha ishlarni olib borishda, "umumiy mezonlar" AT xavfsizligi darajasini unda amalga oshirilgan xavfsizlik funktsiyalarining to‘liqligi va ushbu funktsiyalarni amalga oshirishning ishonchliligi nuqtai nazaridan baholashga imkon beradigan asosiy mezon sifatida foydalanish tavsiya etiladi. Bundan tashqari, ushbu usullar korporativ axborot tizimlarining himoya xususiyatlarini baholash natijalarini mahsulot va tizimlarni himoya qilish funktsiyalari uchun talablarning umumiy ro‘yxati (to‘plami), shuningdek himoya baholarini olish paytida aniq o‘lchash usullari yordamida to‘liq taqqoslash imkonini beradi. Ushbu talablarga asoslanib, himoya darajasini baholashni ishlab chiqish jarayonida ishonch darajasi belgilanadi. Himoyani baholash natijalari kompaniya uchun korporativ axborot tizimini himoya qilishning yetarliligini aniqlashga imkon beradi.

Umumiy mezonlar dasturiy ta’minot darajasidagi xavfsizlik mexanizmlari bilan cheklangan bo‘lsa-da, ular shuningdek, tavsiflangan xavfsizlik funktsiyalari bilan bevosita bog‘liq bo‘lgan tashkiliy darajadagi xavfsizlik mexanizmlari va jismoniy himoya talablari uchun muayyan talablarni o‘z ichiga oladi.

Standart qabul qilingandan so‘ng, uni qo‘llash tajribasini hisobga olgan holda, UMning bir qator talqinlari paydo bo‘ldi, ular Sharhlar bo‘yicha maxsus qo‘mita (CCIMV) tomonidan ko‘rib chiqilgandan so‘ng qabul qilinadi, UMga tegishli o‘zgartirish va qo‘shimchalar sifatida rasman e’lon qilinadi va kuchga kiradi. Sharhga parallel ravishda 3.0 UM versiyasini ishlab chiqish davom etmoqda.

Sertifikatlarni o‘zaro tan olish to‘g‘risidagi shartnoma. 1998 yilda Kanada, Fransiya, Germaniya, Buyuk Britaniya va AQSh hukumat tashkilotlari tomonidan umumiy mezonlar asosida olingan baholarni (The international Mutual Recognition Arrangement – MRA) o‘zaro tan olish to‘g‘risida bitim imzolandi. Ushbu shartnomaga muvofiq, tomonlar umumiy mezonlarni qo‘llash asosida olingan va shartnoma talablariga javob beradigan tashkilotlar tomonidan berilgan bo‘lsa, shartnomaga qo‘shilgan mamlakatlarda olingan AT mahsulotlari va tizimlari uchun sertifikatlarni tan olishni maqsad qilgan. MRA belgilangan qoidalar shartnomaga faqat UM bo‘yicha berilgan sertifikatlarni tan olgan ishtirokchi sifatida ham, ushbu sertifikatlarni bergan ishtirokchi sifatida ham qo‘shilish imkonini beradi. Bu, bir tomondan, xalqaro hamjamiyat tomonidan UMni xavfsizlikni baholashning yagona metodologik asosi sifatida tan olinganligidan boshqa tomondan, tashkilotning demokratiyasidan dalolat beradi.

Hozirgi vaqtda MRA doirasida 6 mamlakatda AT mahsulotlari va tizimlari uchun UM muvofiqlik sertifikatlarini berish huquqiga ega bo‘lgan 8 ta akkreditatsiyadan o‘tgan sertifikatlashtirish organlari, shuningdek, ushbu mamlakatlarda akkreditatsiyadan o‘tgan 30 ga yaqin baholash organlari mavjud bo‘lib, ular hozirgacha UM doirasida 20 dan ortiq AT mahsulotlari va tizimlarini baholash va sertifikatlashni amalga oshirdilar.

MRA kelishuvining paydo bo‘lishi ishlab chiquvchilarni AT mahsulotlari mos kelishi kerak bo‘lgan yagona mezonlarga yo‘naltiradi, shuningdek iste’molchilar uchun sertifikatlangan AT mahsulotlarini tanlash imkoniyatlarini kengaytiradi.

2000 yil may oyida UM sertifikatlarini tan olish to‘g‘risida ko‘proq universal (xCA bilan taqqoslaganda) shartnoma imzolandi (umumiy Criteria sertifikatlarini tan olish bo‘yicha tartibga solish; CCRA)

Hozirgi vaqtda UMni tan olish bo‘yicha xalqaro kelishuvga qo‘shilgan davlatlar qatoriga AQSh, Yevropa Ittifoqi mamlakatlari, Rossiya, Yaponiya kiradi.

“Ishonchli tizimlarning himoyalanganligini baholash mezonlari” standarti (TCSEC)

1983 yilda AQSh mudofaa vazirligining kompyuter tizimlari xavfsizligini baholash standarti sifatida mudofaa vazirligining ishonchli kompyuter tizimlarini baholash mezonlari (Departament of Defence Trust Computer System Evaluation Criteria; TCSEC) qabul qilindi. TCSEC standarti ("Orange Book" nomi bilan tanilgan) muhim ma'lumotlarni qayta ishlashga mo'ljallangan kompyuter tizimiga kiritilgan ma'lumotlarni himoya qilish vositalariga qo'yiladigan talablarni aniqladi.

Baholash jarayonida kompyuter tizimiga (mahsulotiga) qo'yiladigan TCSEC talablarini to'rt turga bo'lish mumkin:

– izchil xavfsizlik siyosati uchun talablar;
– mahsulotdan foydalanish yozuvlarini yuritish uchun talablar;
– mahsulot kafolati talablari;
– mahsulot hujjatlariga qo'yiladigan talablar.

TCSEC ma'lumotlariga ko'ra, kompyuter tizimlari xavfsizlik talablari darajasiga ko'ra to'rtta asosiy guruhga bo'lingan (D, C, B, A), ular o'z navbatida xavfsizlik sinflariga bo'linadi (D, C1, C2, B1, B2, B3, A1). Har bir sinf uchun qat'iy belgilangan talablar to'plami aniqlandi, ular atrof-muhit va muayyan tizimlarni qo'llash xususiyatlari bilan bevosita bog'liq emas edi.

1987 yilda AQSh milliy kompyuter xavfsizligi markazi tarmoq konfiguratsiyasi uchun TCSEC talqinini chiqardi.

Yevropa mezonlari (ITSEC). Integrasiya yo'lidan borgan Yevropa davlatlari (Frantsiya, Germaniya, Buyuk Britaniya va Niderlandiya) 1991 yilda uyg'unlashtirilgan "AT xavfsizligini baholash mezonlari"ni qabul qildilar (Axborot texnologiyalari xavfsizligini baholash mezonlari; ITSEC).

Yevropa mezonlari va "To'q sariq kitob" o'rtasidagi asosiy farq AT xavfsizligini kafolatlash masalalariga ko'proq e'tibor qaratish edi, bu ikki jihat - xavfsizlik vositalarining samaradorligi va to'g'riligiga ta'sir qiladi.

Samaradorlik xavfsizlik funktsiyalari to'plamining baholash ob'yektiga tahdidlarga muvofiqligi, funktsiyalarning o'zaro muvofiqligi, ulardan foydalanish qulayligi, shuningdek ma'lum himoya zaif tomonlaridan foydalanishning mumkin bo'lgan oqibatlari bilan aniqlandi.

To'g'rilik xavfsizlik funktsiyalari va mexanizmlarining to'g'ri bajarilishini anglatadi.

To'g'rilik tekshirilganda, baholash ob'yektining butun hayot sikli tahlil qilinadi- loyihadan tortib, foydalanish va texnik xizmat ko'rsatishgacha.

ITSECda E0 dan E6 gacha bo'lgan aniqlik kafolatining ettita darajasi aniqlandi.

Tizimning umumiy bahosi xavfsizlik mexanizmlarining minimal chidamliligi va aniqlik kafolati darajasidan iborat.

Kanada kompyuter tizimining xavfsizlik mezonlari (CTSEC). Kanada mezonlari (Canadian Trusted Computer Product Evaluation Criteria; CTCPEC) kompyuter tizimlari xavfsizligining milliy standarti sifatida foydalanish uchun ishlab chiqilgan. Asosan ko‘p foydalanuvchi operatsion tizimlarini ishlab chiqish va sertifikatlashga qaratilgan va boshqa ilovalar uchun (masalan, ma’lumotlar bazalari va tarmoqlar uchun) ma’lum bir talqinni talab qiladigan “To‘q sariq kitob”dan farqli o‘laroq,"Kanada mezonlari" dastlab kompyuter tizimlarining keng doirasiga qaratilgan edi. Ushbu standart xavfsizlik talablarini, ish stantsiyalari va ko‘p protsessorli hisoblash tizimlari, shaxsiy va ko‘p foydalanuvchili operatsion tizimlar, ma’lumotlar bazasini boshqarish tizimlari, taqsimlangan tarmoq, o‘rnatilgan, ob’yektga yo‘naltirilgan va boshqa tizimlarning dasturiy ta’minotini himoya qilish va sertifikatlash xususiyatlarini ishlab chiqish uchun ishlatilgan.

Turli xil maqsadli tizimlarning bunday keng doirasiga "Kanada mezonlari" ni qo‘llash imkoniyati ularda ishlatiladigan xavfsizlik talablarini himoya vositalariga funktsional talablar va ularni amalga oshirishning yetarliligi talablari shaklida ikki tomonlama taqdim etish printsipi bilan belgilanadi.

Kompyuter tizimining xavfsizlik darajasi – xavfsizlik darajasining xususiy ko‘rsatkichlari va bitta umumlashtirilgan parametr-xavfsizlik siyosatini amalga oshirishning yetarliligi darajasi bilan tavsiflangan ishlatilgan himoya vositalarining funktsional imkoniyatlari to‘plami sifatida aniqlanadi.

Axborot texnologiyalari xavfsizligining federal mezonlari. "Axborot texnologiyalari xavfsizligining federal mezonlari" (bundan buyon matnda "Federal mezonlar" yoki FM bo‘lib keladi) "Axborotni qayta ishlashning Amerika federal standarti" tarkibiy qismlaridan biri sifatida “To‘q sariq” kitobni o‘rniga qo‘llash maqsadida ishlab chiqilgan.

"Federal mezonlar" AT xavfsizligi talablarining quyidagi turlari katalogini o‘z ichiga oladi: AT mahsulotini tahlil qilish, nazorat qilish va sinovdan o‘tkazishni tartibga soluvchi uchta talablar guruhi.

"Federal mezonlar" axborot xavfsizligi kontseptsiyasining asosiy tushunchasi himoya profili tushunchasidir.

AQSh FIPS (Federal axborotni qayta ishlash standartlari) standarti

Federal ma’lumotlarni qayta ishlash standartlari (FIPS) federal agentliklar va pudratchilar tomonidan maxfiy ma’lumotlar, shaxsiy identifikatsiya qilinadigan ma’lumotlar va moliyaviy ma’lumotlar kabi nozik ma’lumotlarning xavfsizligini ta’minlash uchun talab qilinadi.

Federal AT tizimlarida saqlanadigan ma’lumotlarning konfidensialligi, butunligi, foydalanuvchanligini (CIA triadasi) himoya qilish uchun Milliy Standartlar va

Texnologiyalar Instituti (NIST) tomonidan yaratiladi, qo‘llab-quvvatlanadi va qayta ko‘rib chiqiladi.

FIPS xavfsizlik standartlari kriptografiya, identifikatsiya va kirishni boshqarish, risklarni boshqarish va axborot xavfsizligini boshqarish kabi turli mavzularni qamrab oladi.

Ular NISTning maxsus nashrlarida mavjud bo‘lgan kengroq qoidalar va talablarni qo‘llab-quvvatlaydigan maqbul texnologiyalar, amaliyotlar va tasniflar haqida batafsilroq tushuncha beradi.

Federal hukumat tizimlarida foydalanish uchun FIPS standartlari talab qilinadi. Ular ko‘pincha davlat va mahalliy hukumatlar va hukumat bilan ishlaydigan xususiy sektor tashkilotlariga rahbarlik qilish uchun ishlatiladi. Ko‘pgina davlat shartnomalari va grantlari, shuningdek, ayrim sanoat sertifikatlari uchun FIPS standartlariga muvofiqlik talab qilinadi.

Ta’sir tasnifi, shifrlash standartlari va boshqa eng yaxshi amaliyotlar kabi mavzularni o‘z ichiga olgan o‘nlab FIPS hujjatlari mavjud.

Kiberxavfsizlikka ta’sir qiluvchi eng keng tarqalgan FIPS hujjatlariga quyidagilar kiradi:

FIPS 140-3. FIPS 140-3 kriptografik modul spetsifikatsiyalarining so‘nggi versiyasi bo‘lib, AQSh hukumati va uning pudratchilaridan maxfiy ma’lumotlarni himoya qiladi.

FIPS 140-3 oldingi standart (FIPS 140-2) o‘rnini bosadi va kriptografik modullar uchun yangilangan talablarni o‘z ichiga oladi. FIPS 140-3 dagi ba’zi o‘zgarishlarga quyidagilar kiradi:

1. *Algoritm talablari:* FIPS 140-3 bir nechta yangi kriptografik algoritmlarni va shifrlash va xeshlash algoritmlari uchun kengaytirilgan kalit uzunligi talablarini taqdim etadi.

2. *Testlash va tekshirish.* FIPS 140-3 gibrid dasturiy ta’minot/apparat shifrlash modullari uchun operatsiyadan oldingi o‘z-o‘zini tekshirish (POST) talablarini o‘z ichiga oladi.

3. *Xavfsizlik siyosati:* FIPS 140-3 barcha kriptografik modullardan modulning xavfsizlik funksiyalari, imkoniyatlari va xizmatlarini belgilaydigan rasmiy xavfsizlik siyosatiga ega bo‘lishini talab qiladi. Bundan tashqari, 4-darajali talablar ko‘p faktorli autentifikatsiya (MFA) uchun yangi taxminlarni o‘z ichiga oladi.

4. *Xavfsizlik talablari:* FIPS 140-3 kriptografik modullar javob berishi kerak bo‘lgan qo‘shimcha xavfsizlik talablarini o‘z ichiga oladi. Masalan, modullarda ruxsatsiz kirish, buzish yoki manipulyatsiyani aniqlash va oldini olish mexanizmlari bo‘lishi kerak.

5. *Amalga oshirish bo‘yicha qo‘llanma:* FIPS 140-3 standart talablarini qanday amalga oshirish bo‘yicha batafsil ko‘rsatmalar beradi. Ushbu qo‘llanma maxsus kriptografik funktsiyalarni amalga oshirish va muayyan turdagi testlarni bajarish misollarini o‘z ichiga oladi.

FIPS 186-4. FIPS 186 federal idoralar tomonidan elektron hujjatlar va tranzaktsiyalarni autentifikatsiya qilish uchun foydalaniladigan raqamli imzo algoritmlarini belgilaydigan ma’lumotlarni qayta ishlashning federal standartidir.

FIPS 186-4 uchta raqamli imzo algoritmini belgilaydi:

1. Raqamli imzo algoritmi (DSA)
2. Elliptik egri raqamli imzo algoritmi (ECDSA)
3. Rivest -Shamir- Adleman shifrlashi (RSA)

FIPS 186 ushbu algoritmlarning har biri uchun texnik talablarni belgilaydi, jumladan kalit o‘lchamlari, kalit va imzo yaratish usullari hamda imzolash va tekshirish jarayonlarida foydalaniladigan xavfsizlik parametrlari. Standart shuningdek, kalitlarning tasodifiyligi va xavfsiz xesh qiymatini yaratish uchun talablarni o‘z ichiga oladi.

FIPS 186 ning so‘nggi versiyasi (FIPS 186-5) 2023-yil fevral oyida chiqarilgan va 186-4 versiyasi o‘rnini bosadi. Ushbu yangi versiya oldingi versiyadagi ba’zi talablarni yangilaydi. Xususan, 2024-yil fevral oyida FIPS 186-5 to‘liq joriy etilishidan oldin undan foydalangan tashkilotlar bundan mustasno, DSA’ni yaroqli yechim sifatida olib tashlagan. Shuningdek, u Edvards raqamli imzo algoritmini (EDDSA) qabul qilinadigan algoritmlar ro‘yxatiga qo‘shgan.

FIPS 199 FIPS 199 Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan ishlab chiqilgan standartdir. U axborot va axborot tizimlarini tashkilot faoliyati, aktivlari yoki jismoniy shaxslariga potentsial ta’siridan kelib chiqqan holda toifalarga ajratish bo‘yicha tavsiyalar beradi.

FIPS 199 ning maqsadi tashkilotlarga axborot xavfsizligi talablarini aniqlash va ustuvorligini aniqlashda yordam berishdir. Bu potentsial ta’sir qilishning uchta toifasini aniqlash orqali amalga oshiriladi, ularning har biri turli darajadagi xavfsizlik nazoratini talab qiladi:

1. *Kam ta’sir:* agar buzilgan bo‘lsa, tashkilot faoliyati, aktivlari yoki manfaatdor tomonlarga cheklangan ta’sir ko‘rsatadigan ma’lumotlar.
2. *O‘rtacha ta’sir:* agar buzilgan bo‘lsa, tashkilot faoliyatiga, aktivlariga yoki manfaatdor tomonlarga sezilarli ta’sir ko‘rsatishi mumkin bo‘lgan ma’lumotlar.
3. *Yuqori ta’sir:* agar buzilgan bo‘lsa, tashkilot faoliyati, aktivlari yoki manfaatdor tomonlar uchun jiddiy yoki halokatli oqibatlarga olib kelishi mumkin bo‘lgan ma’lumotlar.

Tashkilotlar FIPS 199 dan axborot tizimlarining toifalanishiga qarab tegishli xavfsizlik boshqaruvlarini aniqlash uchun foydalanishlari mumkin. Misol uchun, past ta’sirli tizimlar faqat kirishni boshqarish va zaxira protseduralari kabi asosiy xavfsizlik choralarini talab qilishi mumkin. Aksincha, yuqori unumdorlikdagi tizimlar shifrlash va tahdidni aniqlash kabi qattiqroq qoidalarni talab qilishi mumkin.

FIPS 200 FIPS 200 NIST 800-53 va FIPS 199 bazaviy standartlariga asoslanib, tashkilotlar uchun Federal Axborot xavfsizligini boshqarish qonuniga (FISMA) rioya qilish uchun minimal talablarni belgilaydi.

FIPS 201: Ushbu standart federal xodimlar va pudratchilar tomonidan xavfsiz ob’yektlar va axborot tizimlariga kirish uchun foydalaniladigan shaxsni tasdiqlovchi kartalar (PIV) uchun talablarni belgilaydi. U autentifikatsiya qilish uchun ishlatiladigan biometrik va kriptografik texnologiyalarni o‘z ichiga olgan kartalar uchun texnik va operatsion talablarni belgilaydi.

FIPS 202 - bu kriptografik xesh-funktsiyalar oilasini, Secure Hash Algoritms (SHA-3) ni belgilaydigan federal ma’lumotlarni qayta ishlash standarti. SHA-3 raqamli imzolar va sertifikatlar kabi ma’lumotlarning haqiqiyligi va butunligini tekshiradi va SHAning oldingi versiyalariga qaraganda ko‘proq hujumga chidamlilik va ishlashini ta’minlash uchun mo‘ljallangan.

FIPS 202 maxfiy ma’lumotlarni himoya qilish va raqamli ma’lumotlarning haqiqiyligi va yaxlitligini ta’minlash uchun AQSh hukumati va uning pudratchilari tomonidan qo‘llaniladi. Bundan tashqari, moliyaviy va sog‘liqni saqlash sohalari kabi kuchli kriptografik xavfsizlikni talab qiladigan boshqa tashkilotlar va tarmoqlar tomonidan qo‘llaniladi.

XULOSA

ISO/IEC 15408 xalqaro standarti, ya’ni "Umumiy mezonlar", axborot texnologiyalari xavfsizligini baholashda keng qo‘llaniladigan eng universal va ilg‘or standartdir. Ushbu standart axborot tizimlari va texnologiyalari xavfsizligini baholashda qatnashadigan uchchala guruh — iste’molchilar, ishlab chiquvchilar va baholovchilar — ehtiyojlarini qondirish uchun ishlab chiqilgan. "Umumiy mezonlar" xavfsizlik talablarini tizimlashtiradi, moslashtiradi va kengaytirish imkoniyatiga ega bo‘lgan kutubxonalar to‘plamini taqdim etadi. Bu orqali dasturchilar xavfsizlik funktsiyalarini mazmunli yozish imkoniyatiga ega bo‘ladi, bu esa dasturiy ta’minot sifatini yaxshilaydi.

"Umumiy mezonlar" axborot xavfsizligini baholash sohasida milliy standartlarni unifikatsiya qilish, baholashga ishonchni oshirish va sertifikatlarni o‘zaro tan olish asosida xarajatlarni kamaytirishga yordam beradi. Bu standart, shuningdek, global IT bozorida xavfsizlikni baholash natijalarining o‘zaro tan olinishini ta’minlaydi va

axborot tizimlari xavfsizligini mustaqil baholashda yuqori darajada ishonchni kafolatlaydi. Shu sababli, ISO/IEC 15408 xalqaro standarti axborot xavfsizligi sohasidagi eng samarali va keng qo‘llaniladigan me’yoriy-huquqiy bazalardan biri hisoblanadi.

ADABIYOTLAR

1. A.Sokolov, O.Stepanyuk. Защита от компьютерного терроризма. O‘quv qo‘llanma. BXV-Peterburg. Arlit, 2002.

2. A.M.Astaxov. Аудит безопасности информационных систем. Konfident.-2003.-1,2.

3. A.V.Belyayev. Методы и средства защиты информации// http://www.citforum.ru/internet/infsecure/its2000_01.shtml.

4. United States Copyright Act, Title 17. U.S.C. 1976. Elektron resurs: http://www.wipo.int (Murojaat sanasi: 21.01.2015).

5. Digital Millenium Copyright Act (DMCA), 1998. Elektron resurs. - Режим доступа: http://www.copyright.gov/legislation/dmca.pdf (Murojaat sanasi: 19.10.2014).

6. Act on Copyright and Related Rights (Copyright Act), нем. – Gesetzüber Urheberrecht und verwandte Schutzrechte.- Copyright Act of 9 September 1965 (Federal Law Gazette Part I, p. 1273), as last amended by Article 8 of the Act of 1 October 2013 (Federal Law Gazette Part I, p. 3714) Elektron resurs: http://www.gesetze-iminternet.de/englisch_urhg/englisch_urhg.html (Murojaat sanasi: 13.08.2015)

7. Christopher Millard. Cloud computing Law// Oxford University Press, 2013