AXBOROT TIZIMLARIDA FOYDALANUVCHILARNI IDENTIFIKATSIYALASH USULLARI VA VOSITALARINING TAHLILI.

Sayftdinov Islombek Zoir ugli
islombek.sayfiddinov.97@bk.ru
Termiz davlat universiteti AKT "Kompyuter tizimlari va boshqaruv dasturlari ta'minoti (tarmoqlar va soxalar bo'yicha)
https://doi.org/10.5281/zenodo.7091358

Annotatsiya: Axborotlarni muhofaza qilishning dasturiy vositalari axborotlar xavfsizligini ta'minlashga mo'ljallangan va kompyuter vositalarining dasturiy ta'minoti tarkibiga kiritilgan maxsus dasturlardir. Ushbu maqolada axborot tizimlarida foydalanuvchilarni identifikatsiyalash usullari va vositalarning tahlili haqida kerakli ma'lumotlar berilgan.

Tayanch so`zlar: foydalanuvchi, parol, shifrlash, havfsizsizlik, globallashuv, axborot, avtomatlashtirilgan tizimlar

Axborotni muhofaza qilishning apparat-dasturiy vositalari – axborotni muhofaza qilish funksiyalarini (foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish, resurslardan foydalana olishni cheklash, voqealarni qayd qilish, axborotni kriptografik himoyalash va shu kabilar) bajaradigan (mustaqil yoki boshqa vositalar bilan birgalikda) turli elektron qurilmalar va maxsus dasturlardir. Axborotlarni muhofaza qilishning dasturiy vositalari axborotlar xavfsizligini ta'minlashga mo'ljallangan va kompyuter vositalarining dasturiy ta'minoti tarkibiga kiritilgan maxsus dasturlardir.

Foydalanuvchi tizimga qayta kirishida, foydalanuvchi paroli dastlab parollar omboridagi IM bilan shifrlash algoritimida kodlanadi va ombordagi KM bilan taqqoslanadi. Shundan so'ng foydalanuvchiga tizimga kirishga ruxsat beriladi.

Tizim xavfsizligi mutaxassis dasturchilar, tizim adminstratorlari tomonidan mustahkamlangandan so'ng muammo foydalanuvchi parolida qoladi. Agar foydalanuvchi o'z parolini birovga oshkor qilsa yoki topilishi oson bo'lgan parol qoysa, tizimga ruxsatsiz kiruvchilar hosil bo'ladi. Buning natijasida ma'lumotlar omborining yaxlitligi buziladi va tizimning xafsizligi buziladi.

Kompyuter viruslaridan va boshqa dasturlar ta'siridan va o'zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo'nalishlaridan hisoblanadi. Ushbu xavfga etarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin.Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlanadi. Buzg'unchi tarmoqning biror-bir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro'sizlantirishi mumkin.Hamma foydalanayotgan tarmoqdan kelib

chiqayotgan tahdidlarni blokirovkalash uchun «tarmoqlararo ekran» (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

Himoyalangan ma'lumotlar - mulk huquqi obyekti bo‘lgan va huquqiy hujjatlar talablariga yoki axborot egasi tomonidan belgilangan talablarga muvofiq himoya qilinadigan ma'lumotlar. Axborot egasi bo‘lishi mumkin: davlat, yuridik shaxs, jismoniy shaxslar guruhi, jismoniy shaxs. Axborotni muhofaza qilish - bu quyidagilarga qaratilgan huquqiy, tashkiliy va texnik choralarni ko‘rishdir.

1) axborotni ruxsatsiz kirish, yo‘q qilish, o‘zgartirish, blokirovka qilish, nusxalash, taqdim etish, tarqatish va shu kabi boshqa noqonuniy harakatlardan himoya qilishni ta'minlash;

2) cheklangan kirish imkoniyatiga ega bo‘lgan ma'lumotlarning maxfiyligiga rioya qilish;

3) ma'lumot olish huquqidan foydalanish.

Axborotlarni muhofaza qilishning dasturiy vositalari deganda, faqatgina axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlar tushuniladi. Axborotlarni muhofaza qilishning asosiy dasturiy vositalariga quyidagilarni kiritish mumkin:

– kompyuter tizimlarida foydalanuvchilarni identifikatsiyalovchi va autentifikatsiyalovchi dasturlar;

– kompyuter tizimlari resurslaridan foydalanuvchilarning huquqlarini cheklovchi dasturlar;

– axborotlarni shifrlovchi dasturlar;

– axborot resurslarini (tizimli va amaliy dasturiy ta’minotni, ma’lumotlar bazalarini, ta’limning kompyuter tizimlarini va hokazo) noqonuniy o‘zgartirishlardan, foydalanishlardan va ko‘paytirishlardan himoyalovchi dasturlar.

Kompyuter tizimlarida axborot xavfsizligini ta’minlashga taalluqli ma’noda identifikatsiyalash atamasi kompyuter tizimlari sub’ektining unikal nomini bir qiymatli tanib olishni bildiradi. Autentifikatsiyalash esa taqdim etilgan nomni ushbu sub’ektga mosligini tasdiqlashni anglatadi (sub’ektning aslligini tasdiqlash).

Axborotlarni muhofaza qilishning yordamchi dasturiy vositalariga misol qilib quyidagilarni keltirish mumkin:

– qoldiq axborotlarni (tezkor xotira blokidagi, vaqtinchalik fayllardagi va hokazo) yo‘q qiluvchi dasturlar;

– kompyuter tizimlarining xavfsizligi tizimiga bog‘liq bo‘lgan turli voqea va hodisalarni tiklash hamda shunday voqea va hodisalar ro‘y berganini isbotlash

uchun foydalaniladigan audit dasturlari (qayd qilish jurnallarini yuritish);
– qoidabuzar bilan ishlashni imitatsiyalovchi dasturlar (qoidabuzarni go‘yoki yopiq axborotlarni olgan deb chalg‘itish);
– kompyuter tizimlarining himoyalanganligini sinovdan o‘tkazuvchi nazorat dasturlar va boshqalar.

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga etarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Viruslarning ta’sir mexanizmlarini, ularga qarshi kurash usullari va vositalarini bilish viruslanishga qarshi harakatlarni samarali tashkil etish, ularning ta’siridan zararlanish ehtimolligini va talafatlarni minimumga keltirish imkonini beradi.

Kompyuter viruslari – bu kompyuter tizimlarida tarqalish va o‘zini o‘zi ishlab chiqish xususiyatiga ega bo‘lgan kichik hajmdagi bajariluvchi dasturlar. Viruslar kompyuter tizimlarida saqlanayotgan dasturiy vositalar yoki ma’lumotlarni yo‘q qilishi yoki o‘chirib yuborishi mumkin.

Axborot texnologiyalari - jarayonlar, ma'lumotlarni izlash, yig‘ish, saqlash, qayta ishlash, taqdim etish, tarqatish usullari va shu kabi jarayonlar va usullarni amalga oshirish usullari. Axborot tizimi - ma'lumotlar bazalari va axborot texnologiyalari va uni qayta ishlashni ta'minlaydigan texnik vositalar tarkibidagi ma'lumotlar to‘plami bo‘yicha Axborot texnologiyalari. Lug‘at, axborot tizimi bu ma'lumotlarni saqlash va tarqatish uchun ma'lumotni saqlash, izlash va qayta ishlash tizimi va tegishli tashkiliy resurslar (inson, texnik, moliyaviy va boshqalar). Axborot-telekommunikatsiya tarmog‘i - aloqa liniyalari orqali ma'lumotlarni uzatish uchun mo‘ljallangan texnologik tizim, unga kirish kompyuter texnologiyalari yordamida amalga oshiriladi. Axborot egasi - mustaqil ravishda ma'lumot yaratgan yoki qonun yoki shartnoma asosida har qanday mezon bilan belgilanadigan ma'lumotlarga kirish huquqini berish yoki cheklash huquqini olgan shaxs.

Axborotni tarqalib ketishdan himoya qilish - himoyalangan ma'lumotni oshkor qilish natijasida uning nazoratsiz tarqatilishini oldini olishga qaratilgan faoliyat, ma'lumotlarga ruxsatsiz kirish va razvedka tomonidan himoyalangan ma'lumotlarni olish. Axborotni ruxsatsiz ta'sirdan himoya qilish - belgilangan huquqlarni va (yoki) ma'lumotlarni o‘zgartirish qoidalarini buzgan holda, uning buzilishiga, yo‘q qilinishiga, ma'lumotlarga kirishni to‘sib qo‘yishga, shuningdek

yo‘qotish, yo‘q qilishga olib keladigan himoyalangan ma'lumotlarga ta'sirini oldini olishga qaratilgan faoliyat. Yoki ommaviy axborot vositalarining ishlamay qolishi. Tarqalish jarayonida viruslar o‘zini modifikatsiyalashi mumkin. Viruslarning ommaviy tarqalib ketishi va ularning kompyuter tizimlari resurslariga ta’siri oqibatlarining jiddiyligi, maxsus antivirus vositalarini va ularni qo‘llash usullarini yaratish va foydalanish zaruriyatini keltirib chiqardi. Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:
– kompyuter tizimlarida viruslarni topish;
– virus – dasturlar ishini blokirovka qilish;
– viruslar ta’sirining oqibatlarini bartaraf qilish.
Viruslarni topishni, ularni joylashib olish bosqichida yoki hech bo‘lmaganda virusning buzg‘unchilik funksiyalarini boshlagunga qadar amalga oshirgan maqsadga muvofiq. SHuni ta’kidlash joizki, barcha turdagi viruslarni topishni kafolatlovchi antivirus vositalar mavjud emas.

Axborotni texnik razvedkadan himoya qilish - razvedkaning texnik vositalar yordamida himoyalangan ma'lumotlarni olishiga yo‘l qo‘ymaslik bo‘yicha faoliyat. Axborotni maxfiy razvedkadan himoya qilish - maxfiy razvedkaning himoyalangan ma'lumotlarni olishiga yo‘l qo‘ymaslik bo‘yicha faoliyat. Axborotni muhofaza qilishning maqsadi - axborotni muhofaza qilishning oldindan belgilangan natijasidir. Axborotni muhofaza qilishning maqsadi ma'lumotlar egasiga, egasiga, foydalanuvchiga mumkin bo‘lgan ma'lumotlarning tarqalishi va (yoki) ma'lumotlarga ruxsatsiz va bila turib ta'sir qilishi natijasida zarar etkazilishining oldini olish bo‘lishi mumkin. Axborot xavfsizligi g‘oyasi - bu axborot xavfsizligi maqsadiga erishish uchun zarur bo‘lgan texnik va tashkiliy chora-tadbirlarning tarkibi, mazmuni, aloqasi va ketma-ketligini ochib beradigan asosiy g‘oya. Axborotni muhofaza qilish samaradorligi - axborotni muhofaza qilish natijalarining belgilangan maqsadga muvofiqligi darajasi. Axborotni muhofaza qilish samaradorligi ko‘rsatkichi - bu axborotni muhofaza qilish samaradorligini baholash uchun o‘lchov yoki xarakteristikadir. Axborotni muhofaza qilish samaradorligi standartlari - axborotni muhofaza qilish samaradorligi ko‘rsatkichlarining me'yoriy hujjatlar bilan belgilangan qiymatlari, axborot xavfsizligini tashkil etish bilan bog‘liq tushunchalar.

Axborotni muhofaza qilishni tashkil etish - axborotni muhofaza qilishni ta'minlashga qaratilgan harakatlarning mazmuni va tartibi. Axborot xavfsizligi tizimi - axborot sohasidagi tegishli huquqiy, tashkiliy, ma'muriy va me'yoriy hujjatlar bilan belgilangan qoidalar asosida tashkil etilgan va faoliyat ko‘rsatadigan organlar va (yoki) ijrochilar, ularning axborot xavfsizligi texnikasi,

shuningdek himoya obyektlari to‘plami, xavfsizlik. Axborotni muhofaza qilish chorasi - axborotni muhofaza qilish usullari va vositalarini ishlab chiqish va (yoki) amalda qo‘llashga qaratilgan harakatlar majmui. Axborotni muhofaza qilish samaradorligini nazorat qilish choratadbirlari - axborotni muhofaza qilish samaradorligini nazorat qilish usullari va vositalarini ishlab chiqish va (yoki) amaliy qo‘llashga qaratilgan tadbirlar majmuasi. Axborot xavfsizligi texnologiyasi - axborot xavfsizligi vositalari, axborot xavfsizligi samaradorligini nazorat qilish vositalari, axborot xavfsizligini ta'minlashga mo‘ljallangan vositalar va boshqaruv tizimlari. Axborotni muhofaza qilish obyekti - axborotni himoya qilishning belgilangan maqsadiga muvofiq himoya qilinishi kerak bo‘lgan axborot yoki axborot tashuvchisi yoki axborot jarayoni.

Kompyuter tarmog‘ida axborotlarning butunligi va foydalanishga qulayligini ta’minlashning asosiy shartlaridan biri ularning zaxiralarini hosil qilishdan iborat. Axborotlar zaxirasini yaratish strategiyasi axborotning muhimligini, kompyuter tizimlarining uzluksiz ishlashiga bo‘lgan talablarni, ma’lumotlarni tiklashdagi qiyinchiliklarni hisobga olgan holda tanlanadi. Himoyalangan kompyuter tizimlarida faqatgina ruxsat etilgan dasturiy ta’minotdan foydalanilishi lozim. Foydalanishiga rasman ruxsat etilgan dasturlarning ro‘yxati, ularning butunligini nazorat qilishning usullari va davriyligi kompyuter tizimlarini ekspluatatsiya qilinishidan oldin aniqlanishi kerak.Dasturlar butunligini nazorat qilishning sodda usullaridan biri nazorat yig‘indilari usuli hisoblanadi.

Adabiyotlar:

1. Henk C.A. van Tilborg, Sushil Jajodia. Encyclopedia of Cryptography and Security.-NY.: Springer, 2011.- P. 957-958.
2. S.K. G`aniyev, M.M. Karimov, K.A. Toshev. Axborot xafsizligi. Axborot-kommunikatsiya tizimlari xafsizligi. T.: Aloqachi, 2008, - B. 379.
3. Shirley Gaw, Edward W. Felten. Password Management Strategies for Online Accounts. Princeton University, 2002.- P. 25-27.
4. William Stallings. Cryptography and Network Security Principles and Practices., Fifth Edition.-NY.: Pearson, 2011. - P. 769-775.