2-TOM, 5-SON

AXBOROT XAVFSIZLIGINI BUZILISHIGA OLIB KELUVCHI TAXDIDLARNING TURLARI VA ULARNING TASNIFI

Sattarov Baxtiyor Ravshan o'g'li
Termiz davlat universiteti kompyuter tizimlari va
ularning dasturiy ta'minoti 1-kurs magistranti

Annotatsiya: Ushbu tezisda Axborot xavfsizligi, Axborotlarni kodlash shifrlash, almashtirish, saqlash, foydalanish jarayonlarini o'z ichiga oladi. Axborot xavfsizligida kriptotizim xavfsizligi muhim ahamiyat kasb etadi..

Kalit so'zlar: Axborot xavfsizligi tarixi, kriftografik kodlar , kriptografik shifrlar, kodlash va shifrlar.

Ta`sir etish maqsadi bo`yicha xavfsizlik xavfini uchta asosiy turga farqlanadi:

1. Axborot maxfiyligining buzilish xavfi;
2. Axborot butunligining buzilish xavfi;
3. Tizimning ishlash layoqatligining buzilish xavfi (xizmat ko`rsatishdagi inkor (rad) etishlar).

Axborot maxfiyligining buzilish xavfi maxfiy yoki sirli axborotni xavfni amalga oshirishda axborot unga murojaat qilishi mumkin bo`lmagan shaxslarga ma`lum bo`lib qoladi.

Kompyuter tizimida, bir tizimdan boshqasiga uzatilayotgan yoki kompyuter tizimida saqlanayotgan biror yopiq axborotga ruxsat etilmagan murojaat qilish bo`lganda har safar axborot maxfiyligini buzilishi havfi sodir bo`ladi.

Tizimning ishlash layoqatligini buzilish xavfi (xizmat ko`rsatishdagi inkor etishlar) ma`lum bir oldindan mo`ljallangan ta`sirlar yoki tizimning ishlash layoqatligini susaytiradigan yoki uning ba`zi bir resurslariga murojaat qilishni blokirovkalaydigan xolatlarni yaratishga yo`naltirilgandir. Masalan, tizimning bir foydalanuvchisi biror xizmatga murojaat qilishga so`rov bersa, boshqasi esa bu murojaat qilishni blokirovkalash bo`yicha xarakterlarni amalga oshirsa, unda birinchi foydalanuvchi xizmat ko`rsatishga rad javobini oladi.

Resursga murojaat qilishni blokirovkalash doimiy va vaqtincha bo`lishi mumkin.

Axborot xavfsizligini buzish bo`yicha sabablar tasodifiy va yomon niyatli (oldindan mo`ljallangan) bo`lishi mumkin. Birinchi holda buzuvchi, xalaqit beruvchi va boshqa jarayonlarning manbalari bo`lishi mumkin:

- tasodifiy holatlar (er qimirlashi, yongin, dovul va b.);

- tizimning tarkibiy elementlarini izdan chiqishi (texnik buzilishlar);
- chop qilingan bank xujjatlarini o`g`irlash;
- axborotni ataylab yo`qotish;
- bank xodimlari tomonidan moliyaviy hujjatlarni, hisobot va ma`lumot bazasini ruxsatsiz o`zgarish;
- aloqa kanallari bo`yicha uzatilayotgan ma`lumotlarni qalbakilashtirish;
- virusli harakatlar keltirib chiqargan axborotning buzilishi;
- magnit tashuvchilarda saqlanayotgan arxivdagi bank axborotlarini buzilishi;
- tizim tashkil etuvchilari va tugunlarini o`g`irlanishi.

Axborot xavfsizligigining asosiy taxdid turlari:

1. Texnik vositalarda axborotlarni saqlanishi yoki ruxsatsiz kirishdagi qayta ishlashlar;
2. Telekommunikatsiya kanallari orqali uzatilayotgan axborotlarni texnik vositalar yordamida tutib olish;
3. Qayta ishlangan axborotlarni elektromagnit nurlanishi orqali chiqib ketishi (tarqalishi);

Tashkilotning himoyalash tizimiga bo`lgan haqiqiy ehtiyojini aniqlash va xavfsizlikning mavjud barcha xilma-xil choralaridan kerakligini tanlashda turli yondashishlardan foydalaniladi. Bunday yondashishlardan biri axborot himoyasining quyidagi uchta jihatiga asoslangan.

1. Himoyaning buzilishlari. Korxonaga tegishli axborotni saqlash va ishlatish xavfsizligiga zarar keltiruvchi har qanday xarakatlar.
2. Himoya mexanizmi. Himoyaning buzilishlarini aniqlash va bartaraf etish, hamda buzilishlar oqibatini yo`qotish mexanizmlari.
3. Himoya xizmati. Ma`lumotlarni ishlash tizimlari va korxonaga tegishli axborotni tashish xavfsizligi saviyasini ko`tarishga mo`ljallangan servis xizmati.

Himoyaning buzilishlari. Komp`yuter tizimi yoki tarmog`i himoyasini buzishga urinishlarni komp`yuter tizimini axborot bilan ta`minlovchi ob`ekt sifatida ko`rish orqali klassifikatsiyalash mumkin. Umumiy holda qandaydir manbadan (masalan, fayl yoki xotira qismi) axborot oqimining adresatga (masalan, boshqa fayl yoki bevosita foydalanuvchi) uzatilishi kuzatiladi. Shu nuqtai nazardan quyidagi xujumlarni farqlash mumkin:

- Uzish (raz`edinenie);
- Ushlab qolish (perexvat);
- Turlash (modifikatsiya);
- Soxtalashtirish (fal`sifikatsiya).

Uzish (raz`edinenie). Tizim resursi yo`q qilinadi, axborotdan foydalanuvchanlik buziladi. Bunday buzilishlarga misol tariqasida uskunaning ishdan chiqishi, aloqa

liniyasining uzilishi yoki fayllarni boshqaruvchi tizimning buzilishini ko`rsatish mumkin. Ushlab qolish (perexvat). Resursdan ruxsat berilmagan foydalanishga yo`l ochiladi.

Ko`pincha axborot mazmunini maskirovka qilishda shifrlash qo`llaniladi. Ammo, axborot mazmuni shifrlash yordamida ishonchli tarzda berkitilgan bo`lsada, buzg`unchida uzatiluvchi ma`lumotlarning o`ziga hos alomatlarini kuzatish imkoniyati qoladi. Masalan, uzatuvchini va axborotlarni uzatishga ishlatiluvchi tugunlarni, axborotlar uzunligini va ularning almashinuv chastotasini aniqlash mumkin. Bunday axborot ma`lumotlar almashinuvidan ko`zlangan maqsadni aniqlashda juda ham qo`l kelishi mumkin.

Himoyaning passiv buzilishlarini aniqlash juda qiyin, chunki ularda ma`lumotlarga qandaydir o`zgartirishlar kiritish ko`zda tutilmaydi. Ammo, bunday xil buzilishlarni oldini olishni amalga oshirsa bo`ladi. Shu sababli passiv buzilishlar xolida e`tiborni ularni aniqlashga emas, balki ularni oldini olishga qaratish lozim.

Imitatsiya deganda ob`ektning o`zini boshqa ob`ekt qilib ko`rsatishi tushuniladi. Odatda imitatsiya aktiv buzilishlarning boshqa bir xilining urinishi bilan birgalikda bajariladi. Masalan, buzg`unchi tizimlar almashinayotgan autentifikatsiya ma`lumotlarining oqimini ushlab qolib so`ngra autentifikatsiya axborotlarining haqiqiy ketma-ketligini tiklashi mumkin. Bu esa vakolati chegaralangan ob`ektning o`zini vakolati kengroq ob`ekt qilib ko`rsatishi (imitatsiya) orqali vakolatini kengaytirishiga imkon beradi.

Tiklash deganda ma`lumotlar blokini passiv ushlab qolib, keyin uni ruxsat berilmagan natijani hosil qilish maqsadida retranslyatsiya qilish tushuniladi. Ma`lumotlarni modifikatsiyalash deganda ruxsat berilmagan natijani hosil qilish maqsadida qonuniy axborot qismini o`zgartirish, yoki axborot kelishi ketma- ketligini o`zgartirish tushuniladi.

Himoyaning aktiv buzilishlarini butunlay oldini olish juda murakkab, chunki bunga faqat barcha aloqa vositalarini uzluksiz fizik himoyalash orqali erishish mumkin. Shu sababli himoyaning aktiv buzilishlarida asosiy maqsad ularni operativ tarzda aniqlash va tezdan tizimning ishga layoqatliligini tiklash bo`lishi shart. Buzilishlarning o`z vaktida aniqlanishi buzg`unchini to`xtatish vazifasini xam o`taydi, va bu vazifani buzilishlardan ogoxlantirish tizimning qismi deb ko`rish mumkin.

Himoya mexanizmlari. Amaliyotda ishlatiladigan ximoya mexanizmlarining aksariyati kriptografiya usullariga asoslangan. Shifrlash yoki shifrlashga yaqin axborotni o`zgartirishlar ma`lumotlarni ximoyalash usullari xisoblanadi.

Foydalanilgan adabiyotlar ro'yxati

1. Alferov A.P., Zubov A.YU., Kuzmin A.S., CHeremushkin
2. Uchebnoye posobiye/ Izd.:Gelios ARV, 2001. – 480 s.

3. Akbarov D.E., Xasanov P. F., Xasanov X. P., Axmedova O. P. "Kriptografiyaning matematik asoslari" – Toshkent, 2010 – 210 bet.
4. ISO/IEC 11770 -1. "Key management – Introduction".
5. ISO/IEC 11770 -2. "Key management – Symmetric techniques".
6. ISO/IEC 11770 -3. "Key management – Asymmetric techniques".
7. Menezes A., van Oorschot R., Vanstone S. Handbook of Applied Cryptography. - CRC Press, 1996. – 780 rr.