Axborot yo’qotilishiga bo’lgan tahdidlar kelib chiqish sabablari

N.Q.Xudayberdiyev
xudoyberdiyevnortura@gmail.com
Sh.Ch.Jo’rayev
jorayevsherzod2001@gmail.com
Termiz davlat pedagogika instituti
M.T.Jo’rayev
juraevmaruff@gmail.com
O’zbekiston milliy universiteti

Annotatsiya: Axborotga bo’lgan tahdidlar bugungi kunda dolzarb masalalardan biri hisoblanadi. Tahdidlarni kelib chiqish sabablarini o’rganish ularni bartaraf etish imkoniyatini oshiradi. Chunki himoya usullari ham shunga qarab quriladi.

Kalit so’zlar: axborot, axborot xavfsizligi, axborot tahdidi, tasodifiy, qasddan

Reasons for threats to information loss

N.Q.Khudayberdiyev
khudoyberdiyevnortura@gmail.com
Sh.Ch.Jurayev
jorayevsherzod2001@gmail.com
Termiz State Pedagogical Institute
M.T.Jurayev
juraevmaruff@gmail.com
National University of Uzbekistan

Abstract: Threats to information are one of the most pressing issues today. Studying the causes of threats increases the possibility of their elimination. Because protection methods are built accordingly.

Keywords: information, information security, information threat, accidental, intentional

Axborot yo’qotilishiga olib keladigan tahdidlarni kelib chiqish sabablarini quyidagilarga ajratish mumkin:

1. Tabiiy omillar:

1.1 yong’in;

1.2 toshqin;

1.3 bo'ron;

1.4 chaqmoq;

1.5 zilzila va boshqa sabablar.

2. Inson omillari.

Inson omili o'z navbatida quyidagilarga bo'linadi:

•Tasodifiy, bexosdan tahdidlar. Bu axborotni tayyorlash, qayta ishlash va uzatishdagi xatolar bilan bog'liq tahdidlar (ilmiy-texnik, tijorat, pul va moliyaviy hujjatlar);dasturchilar va foydalanuvchilarning malakasi yetarli emasligi va sifatsiz xizmat ko'rsatganligi sababli xatolar, operatorlar ma'lumotlarni tayyorlash, kiritish va chiqarish, ma'lumotlarni tuzatish va qayta ishlashdagi xatolari;

•Qasddan qilingan harakatlaridan kelib chiqadigan tahdidlar. Bular ilmiy kashfiyotlarni, ishlab chiqarish sirlari ixtirolarini, yollanma va boshqa ijtimoiy sabablarga ko'ra yangi texnologiyalarni (hujjatlar, chizmalar, kashfiyotlar va ixtirolarning tavsiflari va boshqa materiallar) buzish va yo'q qilish bilan bog'liq tahdidlar; rasmiy va boshqa ilmiy, texnik va tijorat suhbatlarini tinglash va uzatish; Bular avtomatlashtirilgan axborot tizimining resurslariga ruxsatsiz kirish bilan bog'liq tahdidlar (kompyuter texnologiyalari va aloqa vositalariga texnik o'zgartirishlar kiritish, kompyuter vositalari va aloqa kanallariga ulanish, axborot tashuvchilarni o'g'irlash: disketlar, tavsiflar, bosma nashrlar va boshqalar).

Qasddan qilingan tahdidlar axborot foydalanuvchilariga zarar yetkazishga qaratilgan va o'z navbatida faol va passivga bo'linadi.

Passiv tahdidlar, qoida tariqasida, axborot resurslaridan ularning ishlashiga ta'sir qilmasdan ruxsatsiz foydalanishga qaratilgan. Passiv tahdid, masalan, aloqa kanallarida tinglash orqali aylanayotgan ma'lumotlarni olishga urinishdir.

Faol tahdidlar apparat, dasturiy ta'minot va axborot resurslariga maqsadli ravishda ta'sir o'tkazish orqali tizimning normal ishlash jarayonini buzishga qaratilgan. Faol tahdidlarga, masalan, aloqa liniyalarini yo'q qilish, shaxsiy kompyuterni yoki uni o'chirib qo'yish kiradi. Operatsion tizim buzilishi, ma'lumotlar bazasining ish faoliyatining to'xtashi va hokazo.

Faol tahdidlarning manbalari buzg'unchilarning to'g'ridan-to'g'ri harakatlari, dasturiy ta'minot viruslari va boshqalar bo'lishi mumkin.

Qasddan qilingan tahdidlar manbasiga ikkiga bo'linadi:

Ichki tahdidlar ko'pincha ijtimoiy ziddiyatlar va kelishmovchiliklar bilan belgilanadi.

Tashqi tahdidlar raqobatchilar tomonidan zararli harakatlar, iqtisodiy sharoitlar va boshqa sabablar (masalan, tabiiy ofatlar) ta'sirida bo'lishi mumkin.

Xavfsizlikning asosiy tahdidlariga quyidagilar kiradi.

1. maxfiy ma'lumotlarni oshkor qilish;

2. murosaga keltiruvchi ma’lumotlar;
3. axborot resurslaridan ruxsatsiz foydalanish;
4. resurslardan noto’g’ri foydalanish;
5. ruxsatsiz ma’lumot almashish;
6. ma’lumotni rad etish;
7. xizmat ko’rsatishni rad etish.

Tahdidni amalga oshirish orqali *maxfiy ma’lumotlarni oshkor qilish* ma’lumotlar bazalariga ruxsatsiz kirish, kanallarni tinglash va boshqalar bo’lishi mumkin. Qanday bo’lmasin, ma’lum bir shaxsning (shaxslar guruhining) mulki bo’lgan ma’lumotni olish, bu ma’lumot qiymatining pasayishiga va hatto yo’qolishiga olib keladi. Maxfiy ma’lumotlarning tarqalishi - bu maxfiy ma’lumotlarning xizmatga ishonib topshirilgan shaxs yoki ish jarayonida ma’lum bo’lgan shaxslar doirasidan tashqarida nazoratsiz chiqishidir. Ma’lumotni oshkor qilish uning egasi yoki egasida xizmatda yoki ishda tegishli ma’lumotlar belgilangan tartibda ishonib topshirilgan mansabdor shaxslar va foydalanuvchilarning qasddan yoki ehtiyotsiz harakatlari bo’lsa, bu ushbu ma’lumotlarga ruxsat berilmagan shaxslar bilan tanishishga olib keldi.

Tashkilotda ma’lumotlarning oshkor bo’lish sabablari:

1. korxona xodimlari tomonidan axborotni muhofaza qilish qoidalarini yetarli darajada bilmaslik va ularga ehtiyotkorlik bilan rioya qilish zarurligini tushunmaslik;
2. maxfiy ma’lumotlarni qayta ishlashning sertifikatlanmagan texnik vositalaridan foydalanish;
3. huquqiy, tashkiliy va muhandislik-texnik choralar bilan axborotni muhofaza qilish qoidalariga rioya etilishi ustidan zaif nazorat.

Axborotga ruxsatsiz kirishning asosiy tipik usullari quyidagilardir:

1. elektron chiqindilarni ushlab turish;
3. tinglash qurilmalaridan foydalanish;
4. masofadan suratga olish;
5. akustik chiqindilarni ushlab turish va printer matnini tiklash;
6. ommaviy axborot vositalari va hujjatli chiqindilarni o’g’irlash;
7. vakolatli so’rovlar bajarilgandan so’ng tizim xotirasidagi qoldiq ma’lumotlarni o’qish;
8. himoya vositalarini yengib, axborot tashuvchilarni nusxalash;
9. ro’yxatdan o’tgan foydalanuvchi sifatida yashirinish;
10. hiyla-nayrang (tizim so’rovlarini yashirish);
11. dasturiy tuzoqlardan foydalanish;
12. dasturlash tillari va operatsion tizimlarining kamchiliklaridan foydalanish;
13. dastur kutubxonalariga "troyan oti" turidagi maxsus bloklarni kiritish;
14. uskunalar va aloqa liniyalariga noqonuniy ulanish;
15. himoya mexanizmlarini zararli ravishda o’chirib qo’yish;

16. kompyuter viruslarini kiritish va ulardan foydalanish.

Shuni ta’kidlash kerakki, hozirgi paytda kompyuter viruslari muammosi alohida xavf tug’diradi, chunki ulardan samarali himoya ishlab chiqilmagan. Qolgan ruxsatsiz kirish usullari to’g’ri ishlab chiqilgan va amalga oshirilgan xavfsizlik tizimi bilan ishonchli blokirovka qilishga imkon beradi. Quyida eng keng tarqalgan texnik tahdidlar va ularning sabablari keltirilgan:

1. ruxsatsiz kirish axborot tizimi - noqonuniy foydalanuvchi tomonidan axborot tizimiga kirish huquqi natijasida yuzaga keladi;

2. ma’lumotlarni oshkor qilish - shaxs tomonidan ma’lumotlarga kirish yoki uni o’qish va u tomonidan tasodifan yoki qasddan ma’lumotni oshkor qilish natijasida yuzaga keladi;

3. ma’lumotlar va dasturlarni ruxsatsiz o’zgartirish - shaxs tomonidan ma’lumotlarni o’zgartirish, yo’q qilish yoki yo’q qilish natijasida mumkin bo’lgan va dasturiy ta’minot mahalliy kompyuter tarmoqlari tasodifan yoki qasddan o’zgartirish;

4. mahalliy tarmoqlar trafigini oshkor qilish - ma’lumotlar mahalliy tarmoqlar orqali uzatilganda, foydalanuvchilar ma’lumotlariga kirishi yoki uni o’qishi va uni tasodifiy yoki qasddan oshkor qilishi natijasida yuzaga keladi;

5. mahalliy tarmoq trafigini almashtirish - bu qonuniy talab qilingan jo’natuvchi tomonidan yuborilganga o’xshab ko’rinadigan xabarlar paydo bo’lganida, lekin aslida bunday bo’lmagan taqdirda, uni qonuniy ravishda ishlatish;

6. mahalliy kompyuter tarmoqlarining yaroqsizligi bu mahalliy kompyuter tarmoqlari resurslaridan o’z vaqtida foydalanishga imkon bermaydigan tahdidlarni amalga oshirish natijasidir.

Foydalanilgan adabiyotlar

1. Anvar Kabulov, Firdavs Muhammadiyev, and Inomjon Yarashov. "ANALYSIS OF INFORMATION SYSTEM THREATS" Science and Education, vol. 1, no. 8, 2020, pp. 86-91.

2. Anvar Kabulov, Ma’ruf Jo’rayev, va Inomjon Yarashov. "Computer viruses and virus protection problems" Science and Education, vol. 1, issue. 9, 2020, december pp. 179-184.

3. Juraev, Maruf, and Mirkomil Mamayusufov. "Analysis of network topology using Venn diagram." Science and Education 3.5 (2022): 306-311.

4. Kabulov, A.V., Normatov, I.H. “About problems of decoding and searching for the maximum upper zero of discrete monotone functions” Journal of Physics: Conference Series, 2019, 1260(10), 102006.

5. Kabulov, A.V., Normatov, I.H., Ashurov, A.O. “Computational methods of minimization of multiple functions” Journal of Physics: Conference Series, 2019, 1260(10), 102007.

6. A. Kabulov and I. Yarashov, "Mathematical model of Information Processing in the Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670192.

7. A. Kabulov, I. Yarashov and A. Otakhonov, "Algorithmic Analysis of the System Based on the Functioning Table and Information Security," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746.

8. A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

9. Yarashov I., Normatov I., Mamatov A. THE STRUCTURE OF THE ECOLOGICAL INFORMATION PROCESSING DATABASE AND ITS ORGANIZATION //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 114-117.