TEXNIK VA TEXNOLOGIK JARAYONLARDA AXBOROT XAVFSIZLIGI

Abdullayeva Saodat Mengbayevna
Termiz davlat muhandislik va agrotexnologiyalar universiteti assistenti

Anotatsiya. Bugungi kunda yangi texnologiyalar yaratilmoqda. Butun dunyo tadqiqotchilari, ishlab chiqaruvchilari va dizaynerlari hayotimizni yengillashtirishga hamda qiziqarli qilish maqsadida turli xil kashfiyotlar yaratishmoqda. Aynan shunday texnologiyalar orqali axborot va axborot tizimlari bo‘layotgan tahdidlarning turlari bugungi kun texnologiyalari kabi turli tumandir.

Tayanch so‘zlar: komputer, texnologiya, internet, xaker, qidiruv tizimi, buzib kirish, axborot xavfsizligi, tarmoq.

Bugungi kunda Internetning rivojlanishi, chekka hududlarga kirib borishi bilan birga shaxsiy ma'lumotlar, muhim korporativ resurslar, davlat sirlari va boshqalarni oshkor qilishning misli ko‘rilmagan tahdidlari yuzaga keldi. Har kuni xakerlar ushbu axborotlarga maxsus hujumlar orqali kirishga harakat qiladi hamda ularni xavf ostiga qo‘yadi. Quyidagi ikkita asosiy omil ta'siri ostida bu hujumlar tobora xavfli bo‘lib bormoqda.

Birinchidan, Internetning hamma joyda keng tarqalgan hamda millionlab qurilmalar allaqachon ushbu tarmoqqa ulangan. Shuning uchun xakerlarning eng zaif qurilmalarga kirish ehtimoli doimiy ravishda oshib boradi. Bundan tashqari, foydalanuvchilarning Internetdan keng foydalanishi xakerlarga global miqyosda axborot almashish imkonini beradi. "Xaker", “buzib kirish” («vzlom»), "xakerlik", "hack", "crack" yoki "phreak" turidagi kalit so‘zlar bo’yicha oddiy qidiruvda bizga qidiruv tizimi minglab saytlarni taqdim etadi, va ularning ko‘plarida zararli kodlar va ulardan foydalanish yo‘llari to‘g‘risidagi ma’lumotlarga ega bo‘lishimiz mumkin [1].

Ikkinchidan, ishlatish uchun qulay operatsion tizimlar va ularni ishlab chiqish vositalarining ommaviy ravishda tarqalganligi. Bu holat xakerning vazifasini ancha osonlashtiradi. Ilgari xaker foydalanish uchun oson va sodda ilovalarni yaratish va tarqatish uchun dasturlash tillarini bilishi kerak edi. Hozirda xakerlik vositasiga kirish uchun biz shunchaki kerakli saytning IP-manzilini bilib olishimiz va xaker hujumni amalga oshirish uchun sichqoncha tugmasini bosishimiz kifoya qiladi [2].

Axborot tizimlaridan foydalanish ma’lum xavflar majmuasi bilan to‘qnash kelinishi bilan amalga oshirilib, tizimdan foydalanish maxsus axborot xavfsizligi bo‘linmalari yoki tizim administratorlari (kichik tashkilotlar uchun) tomonidan doimiy ravishda tahlil qilinishi kerak.

Tizimni himoya qilish va barcha hodisalarning qayd etilishini ta’minlash uchun ba’zi bir xavfsizlik texnologiyalari kompyuterning o‘ziga o‘rnatilishi, boshqalari esa – dasturlarga, uchinchisi esa ishchi – xizmatchilar uchun mo‘ljallangan bo‘lib, tegishli hujjatlarda ko‘rsatilgan rahbariyat ko‘rsatmalarini bajarishi mumkin [2].

Axborot xavfsizligiga tahdidlarning quyidagi xususiyatlari qayd etishimiz mumkin. Bunday tahdidlarning mohiyati, odatda ishlab chiqarish korxonasiga (tashkilotga) qandaydir zarar yetkazishdan iboratdir. Yetkaziladigan zararning xillari turlicha bo‘lishi mumkin:

■ tashkilotning ishbilarmonlik obro‘siga ma’naviy va moddiy zarar yetkazish;

■ alohida shaxslarning shaxsiy ma’lumotlarini oshkor etish orqali ma’naviy, jismoniy yoki moddiy zarar yetkazish;

■ himoyalangan (maxfiy) ma’lumotlarni oshkor qilishdan yetkazilgan moddiy (moliyaviy) zarar;

■ buzilgan himoyalangan axborot resurslarini tiklash zaruratidan yetkazilgan moddiy (moliyaviy) zarar;

■ uchinchi tomon oldidagi majburiyatlarni bajara olmaslikdan moddiy zarar (yo‘qotishlar) ko‘rish;

■ butun korxona ishini izdan chiqarishdan ko‘rilgan ma’naviy va moddiy zarar [3].

Odatda tarmoq hujumlari xakerlar maqsad qilgan tizimlar kabi turli tuman. Ba'zi hujumlarni uyushtirish juda qiyin bo‘lsa, ba’zilari esa, uning faoliyati qanday oqibatlarga olib kelishini tasavvur qilib bo‘lmaydigan darjada oddiy operator tomonidan amalga oshirilishi mumkin. Xakerlik hujumlarini baholash uchun TPC/IP protokoliga xos bo‘lgan ba'zi cheklovlarni bilishimiz lozim. Internet davlat muassasalari va o‘quv yurtlari o‘rtasida o‘quv jarayoni, ilmiy tadqiqotlarga ko‘maklashish maqsadida muloqot qilish uchun yaratilgan qulay vosita. Bu tarmoqni yaratuvchilar uning qanchalik keng tarqalishini bilishmagan. Natijada, Internet Protocol (IP)ning dastlabki versiyalarining texnik xususiyatlarida xavfsizlik talablari bo’lmagan. Shu sababli ko'pgina IP-lar tabiatan juda zaif [5].

Atrof – muhitdan keladigan tahdidlar juda xilma – xildir. Birinchi navbatda korxonaning infratuzilmasida sodir bo‘ladigan buzilishlarni ta’kidlash lozim – elektr ta’minotidagi bizilishlar, vaqtinchalik aloqaning bo‘lmasligi, suv ta’minotidagi

uzilishlar, fuqarolik tartibsizliklari va boshqalar. Yong'in, suv va shunga o'xshash "dushmanlar" qatorida eng xavflisi – past sifatli elektr ta'minoti hisoblanadi va undan axborot tizimlari ko'radigan zarar miqdori 13% ni tashkil etadi [4].

Qizig'i shundaki, deyarli har bir Internet-server kuniga bir necha marta ruxsatsiz kirishga urinishlarga duchor bo'ladi: ba'zida bunday urinishlar muvaffaqiyatli bo'lib chiqadi; ko'pincha ular josuslik bilan bog'liq. Bu yerdan axborot xavfsizligi qanchalik jiddiy soha ekanligini bilish mumkin.

Odatda, tahdidlarning ta'siri axborotni oshkor qilish, o'zgartirish, yo'q qilish yoki axborot xizmatini rad etishga olib keladi. Tahdidning uzoq muddatli oqibatlari biznesning yo'qolishiga, maxfiylikning buzilishiga, fuqarolik huquqlarining buzilishiga, ma'lumotlarning yetarliligini yo'qotishiga, inson hayotining yo'qolishiga va boshqa noxush oqibatlarga olib keladi.

Sodir bo'lishi mumkin bo'lgan tahdidlar, xavfsizlik tizimining zaif tomonlarini bilish xavfsizlikni ta'minlashning eng tejamkor vositalarini tanlash uchun zarurdir.

Zarar o'lchami nuqtai nazardan eng xatarli xavf bu tahdidlar emas, balki foydalanuvchilar, operatorlar, tizim ma'murlari va axborot tizimlariga xizmat ko'rsatadigan shaxslarning bexosdan sodir etgan xatolari hisoblanadi. Ba'zida bunday xatolar tahdid hisoblanib (noto'g'ri kiritilgan ma'lumotlar, dasturdagi xatolar) va ba'zida bu insonning zaif tomonlarining natijasidir, ammo bu yovuz niyatli shaxs tomonidan ishlatilishi mumkin - bu odatda ma'muriy xatolar hisoblanadi, uning oqibatidagi yo'qotishlarning 65% bexosdan sodir etilgan xatolar natijasidir. Yong'in va toshqinlar oqibatida yetkazilgan zararlarni xodimlarning savodsizligi va intizomsizligi oqibatida sodir etilgan xatolar oqibatidagi yetkazilgan zararlar bilan solishtirganda arzimas narsa deb hisoblash mumkin [4].

Foydalanilgan adabiyotlar:

1. Ganiyev S.K., Karimov M.M., Tashev K.A., Axborot xavfsizligi. – T.: "Fan va texnologiya", 2017, 372 bet.

2. А. Бирюков, Информационная безопасность: защита и нападение. 3 изд. Учебное пособие.– М.: ДМК Пресс, 2023. – 442 с.

3. В.Я. Ищейков, Информационная безапастность и защита информации: словар терминов и понятий. – Москва: РУСАЙН, 2021. – 228 стр.

4. Н. Гришина, Основы информационной безопасности предприятия. Учебное пособие. М.: Инфра-М, 2020. – 216 с.

5. В.И. Лойко, В.Н. Лаптев, Г.А. Аршинов, С.В. Лаптев, Информационная безопасность: учеб, пособие. – Краснодар: КубГАУ, 2020. - 332 с.

6. Ищейнов, В. Я., Информационная безопасность и защита информации: теория и практика: учебное пособие. — Москва; Берлин: Директ-Медиа, 2020. — 270 с.