AXBOROT TIZIMLARIDA TAHDID TURLARI

Muxammatqulov Shohruhbek Erkin o‘g‘li

Annotasiya. *Ushbu maqolada bugungi kunda global axborot makonida tahdid turlari hamda ularning ko‘rinishlari haqida so‘z boradi. Shuningdek, mazkur maqola doirasida ilmiy va rasmiy adabiyotlar o‘rganilib mavjud muammo yuzasidan taklif va tavsiyalar keltiriladi.*

Kalit so‘zlar: *Axborot xavfsizligi, kiberterror tahdidlari, zamonaviy tendensiyalar, mafkuraviy polegon, texnologik omillar.*

INFORMATION THREATS IN OPEN INFORMATION SYSTEMS

Abstract. *This article talks about the types of threats and their manifestations in the global information space today. Also, within the framework of this article, scientific and official literature is studied and suggestions and recommendations are made regarding the existing problem.*

Key words: *Information security, cyberterrorist threats, modern trends, ideological battlefield, technological factors.*

Internet tarmog‘i ommalashgandan so‘ng axborot manbalariga ruxsatsiz kirish yoki saqlanadigan ma’lumotlarga ta’sir o‘tkazish, mavjud tizimni ishdan chiqarish, hozirgi global zamonda odatiy holga aylanmoqda. Har qanday resurslarga ta’sir qiladigan bunday tahdidlar ma’lumotlarning buzilishiga, nusxalashga, ruxsatsiz tarqatishga, ularga kirishni cheklashga yoki bloklashga olib kelishi mumkin. Hozirgi kunda turli mezonlarga ko‘ra tasniflanadigan tahdidlarning soni juda ko‘p. Tahdidlarni paydo bo‘lishi tabiatiga ko‘ra **tabiiy va sun’iy** tahdidlarga ajratish mumkin. **Tabiiy tahdidlar** deganda, ob’yektiv fizik jarayonlar yoki tabiiy ofatlarning kompyuter

tizimiga ta’siri tufayli kelib chiqadigan hodisalarni kiritish mumkin. **Sun’iy tahdidlar** deganda, inson faoliyati natijasida kelib chiqadigan tahdidlar tushuniladi. Tashqi tomondan tahdidlarni amalga oshirish darajasiga ko‘ra, **tasodifiy va qasddan** sodir etiladigan tahdidlarga ajratish mumkin. Shuningdek, tahdidlarni to‘g‘ridan-to‘g‘ri manbaiga qarab ajratish mumkin, bu tabiiy muhit (masalan, tabiiy ofatlar), inson (maxfiy ma’lumotlarni oshkor qilish), dasturiy va texnik vositalar: avtorizatsiya qilingan (operatsion tizimdagi xato) va ruxsatsiz (tizimning virusli infeksiyasi) singari holatlarni amalga oshirishi mumkin.

Tahdidlar asosiy kelib chiqish manbai boshqa pozitsiyaga ega bo‘lishi mumkin. Ushbu omilga qarab ularni uch guruhga ajratiladi, bular:

- manbai kompyuter tizimining boshqariladigan guruhidan tashqarida bo‘lgan tahdidlar (masalan, aloqa kanallari orqali uzatiladigan ma’lumotlarni ushlash);

- manbai tizimning boshqariladigan zonasida bo‘lgan tahdidlar (bu axborot tashuvchilarning o‘g‘irlanishi bo‘lishi mumkin);

- to‘g‘ridan-to‘g‘ri tizimning o‘zida bo‘lgan tahdidlar (masalan, resurslardan noto‘g‘ri foydalanish)[9].

Tahdidlar kompyuter tizimiga turli xil ta’sir ko‘rsatishi mumkin. Shuningdek, **passiv effektli** bo‘lishi mumkin, ularni amalga oshirish ma’lumotlar strukturasini o‘zgartirishga olib kelmaydi (masalan, nusxalash). **Faol tahdidlar**, aksincha, kompyuter tizimining tarkibi va tarkibini o‘zgartiradigan tahdidlardir (maxsus dasturlarni kiritish). Tizim resurslaridan foydalanuvchiga yoki dasturiga kirish bosqichlarida tahdidlarni ajratilishiga muvofiq, shunday xavflar mavjudki, ular kompyuterga kirish vaqtida paydo bo‘ladi va ruxsatsiz foydalanuvchi kirganidan so‘ng aniqlanadi (manbalardan ruxsatsiz foydalanish). Tahdidlarni tizimdagi joylashuvi bo‘yicha uchta guruhga bo‘lib tasniflash mumkin: tashqi saqlash qurilmalarida, aloqa liniyalarida aylanib yuradigan ma’lumotlarga kirish tahdidlari. Noqonuniy olingan parollar yordamida yoki qonuniy foydalanuvchilarning terminallaridan noqonuniy foydalanish orqali tahdidlar manbalarga to‘g‘ridan-to‘g‘ri standart yo‘ldan

[9] www.inf74.ru/safetly/ofitsionnay-bezapasnos...

foydalanishlari yoki mavjud himoya vositalarini boshqa yo‘l bilan “chetlab o‘tishlari” mumkin. Axborotni o‘g‘irlash kabi xatti-harakatlar tizim faoliyatidan qat’iy nazar yuzaga keladigan tahdidlar sifatida tasniflanadi.

Shu jumladan, viruslarning tarqalishini faqat ma’lumotlarni qayta ishlash paytida aniqlash mumkin. Tasodifiy yoki beixtiyor amalga oshiriladigan tahdidlar bu tajovuzkorlarning xatti-harakatlari bilan bog‘liq bo‘lmagan xavflardir. Ularni amalga oshirish mexanizmi juda yaxshi o‘rganilgan, shuning uchun qarshi kurash usullari ishlab chiqilgan. Baxtsiz hodisalar va tabiiy ofatlar kompyuter tizimlari uchun alohida xavf tug‘diradi, chunki ular eng salbiy oqibatlarga olib keladi. Tizimlarning jismoniy yo‘q qilinishi sababli, ma’lumotlarga kirish mumkin bo‘lmaydi.

Bundan tashqari, murakkab tizimlardagi nosozliklar hamda ularni oldini olish yoki aksincha oldini olib bo‘lmaydi, buning natijasida ularda saqlanadigan ma’lumotlar buziladi yoki yo‘q bo‘ladi, yohud texnik qurilmalarning ishlash algoritmi buzilishi mumkin. Bundan tashqari, bunday xatolar kiber jinoyatchilar tomonidan tizim resurslariga ta’sir ko‘rsatishda ishlatilishi mumkin. Foydalanuvchilarning 65% yo‘l qo‘yadigan xatoliklari tufayli, axborot tizimi xavfsizligining zaiflashishiga olib keladi. Korxonalarda ishchilar tomonidan funksional majburiyatlarni malakasiz, beparvolik bilan bajarish ma’lumotlarning yo‘q qilinishi, yaxlitligi va maxfiyligini buzilishiga olib keladi. Shuningdek, qoidabuzarning maqsadli harakatlari bilan bog‘liq bo‘lgan qasddan uyishtirilgan tahdidlar aniqlangan. Ushbu sinfni o‘rganish juda qiyin, chunki u juda dinamik xarakterga ega va doimiy ravishda yangi tahdid turlari bilan yangilanib turadi. Axborotni o‘g‘irlash yoki yo‘q qilish maqsadida kompyuter tizimiga kirish uchun josuslik qilishning bunday usullari va vositalari tinglash, o‘g‘irlash dasturlari, xavfsizlik atributlari, hujjatlar va axborot tashuvchisi, vizual kuzatish va boshqalar kabi maqsadlarda ishlatiladi.

Ma’lumotlarga ruxsatsiz kirishda odatda kompyuter tizimlarining standart apparatlari va dasturiy ta’minotidan foydalaniladi, buning natijasida foydalanuvchini yoki axborot resurslaridan foydalanishni qayta ishlashni cheklashning belgilangan qoidalari buziladi. Eng ko‘p uchraydigan qoidabuzarliklar parollarni o‘g‘irlash

(maxsus ishlab chiqilgan dasturlar yordamida amalga oshiriladi), boshqa shaxs nomidan har qanday xatti-harakatlar, shuningdek, tajovuzkor tomonidan qonuniy foydalanuvchilarning imtiyozlaridan foydalanish hisoblanadi.

Maxsus zararli dastur. Ko‘pgina rivojlangan mamlakatlar jahonda iqtisodiy integratsiyani amalga oshirish, fan, texnika, tehnologiya sohasida erishgan yutuqlari bilan rivojlanayotgan mamlakatlarga “yordam” berish bahonasida o‘zlarining milliy-ma’naviy ta’sirlarini o‘tkazish maqsadlarini ham amalga oshirmoqdalar. Albatta, agar dunyodagi xalqlar unga sergaklik va ogohlik bilan qaramas ekanlar, bu ularga bugun yuksak taraqqiy qilgan xalqlarga istiqbolda dunyoda o‘zlarining ma’naviy hukmronligini to‘la o‘rnatish imkonini beradi [10].

Dunyo bo‘ylab foyda keltirish ilinjida bir qator dasturlar ishlab chiqiladi, ularning aksariyati ma’lum maqsadlar uchun yo‘naltirilgan dasturlardir.

- **“kompyuter viruslari”** bu kichik dasturlar bo‘lib, ular kompyuterga kiritilgandan so‘ng o‘zlarining nusxalarini yaratish orqali tarqalishlari mumkin. Muayyan sharoitlarda viruslar tizimga salbiy ta’sir qiladi;

- **“qurtlar”** - har safar kompyuterni ishga tushirishda faol bo‘lgan yordamchi dasturlar. Ular tizim yoki tarmoq ichida harakat qilish va viruslar kabi ko‘payish qobiliyatiga ega. Dasturlarni ko‘chkiga o‘xshash takrorlash aloqa kanallari, xotira tizimining haddan tashqari yuklanishiga va keyinchalik ishning bloklanishiga olib keladi;

- **“Troyan otlari”** - bunday dasturlar foydali dastur niqobi ostida “yashiradi”, lekin aslida kompyuterga zarar yetkazadi: ular dasturiy ta’minotni yo‘q qiladi, maxfiy ma’lumotlarga ega fayllarni nusxalashadi va buzg‘unchilarga yuborishadi va hokazo[11]. Kompyuterda Internet tizimlari orqali kirib keladigan bunday dasturlar, axborot xavfsizligiga daxl qilish darajasi yuqori bo‘ladi. Bu jarayonda jamiyatning axborot tehnologiyalaridan foydalanish salohiyatini oshirish hamda uni ta’lim tizmida chuqurlashtirish lozim.

[10] S. Otamuratov. Globallashuv va millat. -T.: Yangi asr avlodi, 2008. 163-bet.
[11] www.inf74.ru/safetly/ofitsionnay-bezapasnos...

Foydalanilgan adabiyotlar ro‘yxati

1. www.inf74.ru/safetly/ofitsionnay-bezapasnos...
2. S. Otamuratov. Globallashuv va millat. -T.: Yangi asr avlodi, 2008. 163-bet.
3. www.inf74.ru/safetly/ofitsionnay-bezapasnos...