POTENTSIAL BUZG'UNCHINING MODELI TAHLILI

G'aniev Salim Karimovich
Muhammad al-Xorazmiy nomidagi TATU, professor
s.k.ganiyev@gmail.com

Abdullaev Dilmurod G'ulomovich
Muhammad al-Xorazmiy nomidagi TATU, doktorant
dga.abdullayev@gmail.com

ANNOTATSIYA

Ushbu maqolada axborot tizimlarining himoyasini loyihalashda, xavfsizlik bilan bog'liq ishlarda, tahdidlarni aniqlash va himoya tizimini ishlab chiqishdagi dolzarb masalalardan hisoblangan potentsial buzg'unchining modeli tahlil qilinadi.

Kalit so'zlar: *Axborot, tizim, tahdid, xavfsizlik, potentsial buzg'unchi, matematik model, himoya, informatsiya miqdori, hujum, funktsiya, zaiflik, logarifm, ehtimollik, xarakteristika, o'lchov, faraz.*

ABSTRACT

This article analyzes the model of a potential intruder, which is considered as one of the topical issues of designing the protection of information systems, work on ensuring security, detecting threats and developing protection systems.

Keywords: *information, system, threat, security, potential intruder, model, protection, amount of information, attack, function, vulnerability, logarithm, probability, characteristic, measurement, prediction.*

KIRISH

Hozirda xavfsizlikni potentsial buzg'unchisining modeli uning malakasi, texnik va moddiy imkoniyatlari xususidagi farazlar nabori kabi shakllantiriladi. Bunda xarakatlarning sabablari va motivlari, aprior bilimlar, ko'zlangan maqsadlar va ularning buzg'unchi uchun ustuvorligini, qo'yilgan maqsadga erishishning asosiy yo'llarini akslantiruvchi buzg'unchining noformal modeli quriladi. Pirovardida bunday model himoyalanuvchi muayyan axborot tizimi uchun hujumlarning dolzarb tahdidlari majmuini aniqlashda ishlatiladi. Aynan dolzarb tahdidlarni, chunki bo'lishi mumkin bo'lgan tahdidlar ularning texnik amalga oshirilishi imkoniyati orqali aniqlanadi. Buzg'unchini matematik modellash esa himoyalanuvchi tizimga ta'sirlarni modellashga keltiriladi va buzg'unchi harakatlarining mantiqiy-algoritmik ketma-ketligi ko'rinishidagi stsenariylarning formal tavsifi hisoblanadi.

Axborot tizimining tajovuzkori (tabiiy, potentsial bosqinchi) modelini ishlab chiqish muayyan axborot tizimiga hujumning dolzarbligining to'g'ri shakllantirish uchun zarurdir. Ba'zi mulohazalardan kelib chiqib, axborot tizimlariga bo'ladigan potentsial hujumga tegishli bo'lgan talabni shakllantirish zarurati paydo bo'ladi.

Axborot xavfsizligi tizimini loyihalashda potentsial hujumlarni tahlil etish

Tabiiyki, ma'lum bir axborot tizimiga aniq bir hujumni potentsial bosqinchi amalga oshirishi bilan bog'liq bo'ladi. Ma'lum bir axborot tizimiga haqiqiy hujumlar va potentsial hujumlar to'plamini shakllantirish uchun foydalaniladigan natijani (xarakteristikani) olish axborot xavfsizligi tizimini loyihalashda asosiy masala ekanligini ta'kidlash mumkin. Axborot tizimiga bo'ladigan barcha mumkin bo'lgan hujumlarni potentsial manfaatlar va ushbu tizimga hujumlarni qulay amalga oshirilishini inobatga olinishi kerak.

Buzg'unchi modeli (tabiiy ravishda, ma'lum bir tizimga qo'llaniladigan tajovuzkor modelini yaratish haqida gapirish ma'noga ega – ya'ni turli xil axborot tizimlari uchun buzg'unchi modeli keskin o'zgarishi mumkin) ko'p omillarni hisobga olishi kerak, ularning hammasi ham rasmiylashtirilgan tavsifga mos kelmasligi mumkin – jumladan, maxfiy ma'lumotlarni olishga bo'ladigan qiziqquvchanlik darajasi, tajovuzkorning mahorat darajasi, u yoki bu turdagi hujumni amalga oshirish yuzasidan turli xil zaifliklardan xabardorligi, shularga mos ravishda hujumni amalga oshirish uchun tegishli vositalar mavjudligi, amaldagi faoliyat yuritayotgan aniq axborot texnologiyasi va axborot himoyasi texnologiyalaridan, ishlatilayotgan dasturiy ta'minotlardan va boshqa ma'lumotlardan xabardorligini inobatga olinishi darkor.

Ushbu barcha omillarni hisobga olishning murakkabligi nafaqat ularning soni va xilma-xilligi, balki ular orasidagi qandaydir bog'liqlikni formallashtirishning murakkabligi bilan izohlanadi. Shu bilan birga, ushbu barcha omillarni hisobga olishga imkon beruvchi qandaydir integral miqdoriy baho zarur, aks holda muayyan axborot tizimi uchun himoya tizimini qurishga kirishish mumkin emas. Undan tashqari, hujumlarning tabiatan xilma-xilligi tahdidlarningdolzarbligini baholashda qandaydir yagona shkalani kiritishni taqozo etadi. [1]

Axborot tizimini tahdiddan himoyalashda zaiflikka nisbatan axborot miqdoriga ehtimollik o'lchovini hisoblash

Ushbu xilma-xil omillar o'zining aksini muayyan axborot tizimiga buzg'unchining hujumini amalga oshirishdagi murakkablikda topadi. Muayyan axborot tizimi xususida gap ketganda axborotni ishlovchi ma'lum axborot tizimi faraz qilinadi, chunki aynan ishlanuvchi axborotdan ruxsatsiz foydalanish amalga oshiriladi.

Alohida olingan zaiflikka muvaffaqiyatli hujumni amalga oshirish uchun buzg'unchi ushbu zaiflik tahdidi xususida mos axborotga (bunday zaiflik aniqlangan va bartaraf etilmagan), ya'ni zaiflik tahdidiga nisbatan qandaydir axborot miqdoriga, ega bo'lishi lozim. Aytaylik, axborot tizimida zaiflik mavjud, ya'ni zaiflik tahdidi real va hodisaning ikkita natijasi bo'lishi mumkin – zaiflik mavjud yoki mavjud emas.

Ushbu holda zaiflikka nisbatan axborot miqdoriga ehtimollik o'lchovi sifatida qarash mumkin. [2]

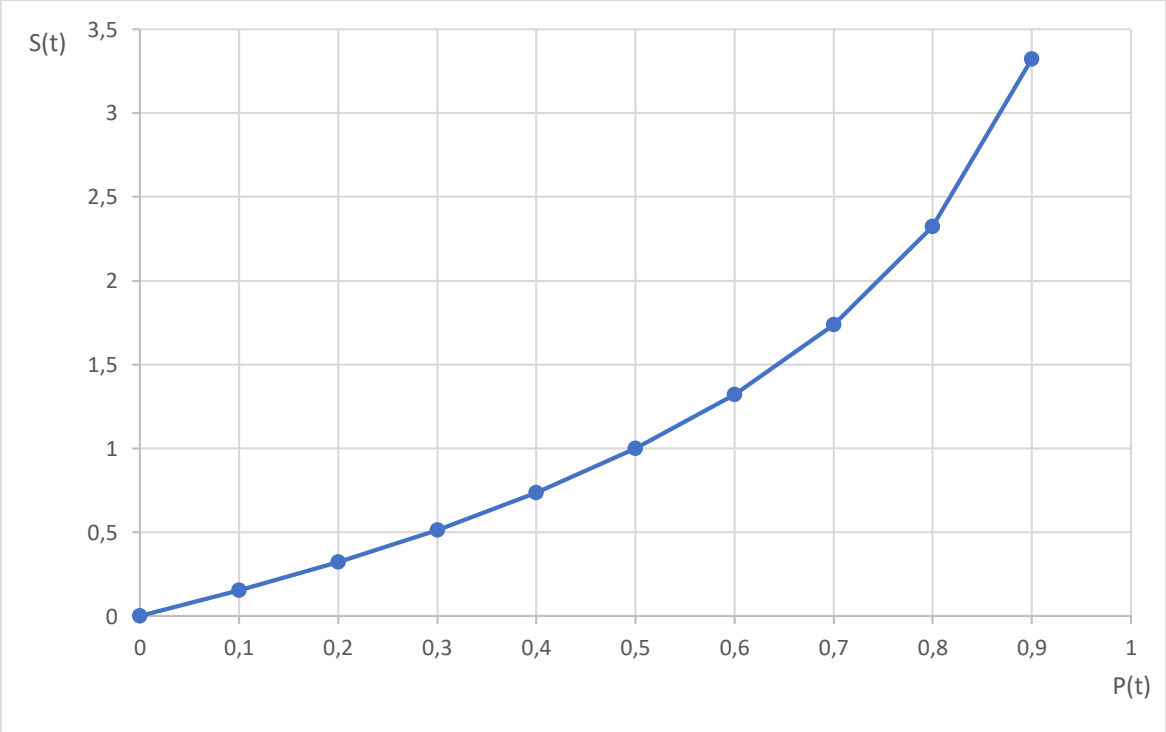
Har bir natijadagi informatsiya miqdorining uning ehtimolligi Ri bilan bog'liqligi quyidagicha aniqlanadi:

$$J = - log_2 P_t$$

Noaniqlik buzg'unchi tarafidan hujum amalga oshirilishida ishlatiluvchi xar qanday zaiflik tahdidiga nisbatan ko'rilishi mumkin. Tizimda zaiflik tahdidining mavjudlik ehtimolligi 1-P_t kabi aniqlanadi. Ravshanki zaiflik tahdidi uchun P_t qiymati qanchalik yuqori bo'lsa, buzg'unchiga mos hujumni amalga oshirish shunchalik qiyin bo'ladi. Yuqorida keltirilganlarni hisobga olgan holda zaiflik tahdidini amalga oshirishning murakkabligi S_t ni, ushbu tahdidni amalga oshirish uchun niyati buzuq egalik qilishi lozim bo'lgan, axborot miqdori J (P_t) ning ehtimollik o'lchovi sifatida sharhlash mumkin, ya'ni

$$S_t = J(P_t) = - log_2(1-P_t)$$

Ushbu o'lchovdan foydalanishning maqbulligi zaiflik tahdidini amalga oshirishni baholashda logarifmik funktsiyaning ishlatilishiga asoslanadi. Logarfmik funtsiya buzg'unchining zaiflik tahdidini amalga oshirishidagi murakkablik funktsiyasi o'zgarishining ehtimollik qiymati $P_t : S_t = f(P_t)$ ga bog'liqligining noaniqligini hisobga olishga imkon beradi. (1-rasm).



1-rasm. Zaiflik tahdidini amalga oshirish murakkabligining uning ehtimollik qiymatiga bog'liqligi.

Misol tariqasida ikkita zaiflik tahdidini amalga oshirish murakkabligini taqqoslaylik. Aytaylik, ulardan birining P_t xarak-teristikasi 0,4 ga teng, ikkinchisiniki 0,8 ga teng bo'lsin. Demak, birinchi holda S_{t1} =0,74, ikkinchi holda S_{t2} =2,32, ya'ni buzg'unchi uchun ikkinchi zaiflik tahdidini amalga oshirish, birinchi zaiflik tahdidini amalga oshirishga qaraganda 3,14 marta murakkabroq. Boshqacha aytganda, tizimda ikkinchi zaiflik tahdidi mavjudligiga nisbatan noaniqlikni bartaraf etish uchun buzg'unchiga 3,14 marta ko'p axborot kerak bo'ladi. [3]

Ta'kidlash lozimki, zaiflik tahdidini amalga oshirish murakkabligi $S_t = J(P_t)=1$ ning birligi P_t =0,5 sharti orqali beriladi, ya'ni tizimda zaiflik teng ehtimollik bilan mavjud yoki mavjud emas.

Hujum tahdidini tizimdagi aniqlangan va bartaraf etilmagan zaifliklar yaratish sababli buzg'unchi uchun hujum murakkabligi hujum tahdidini yaratuvchi har bir zaiflik tahdidiga hujumlarning umumiy murakkabligi orqali aniqlanadi. Agar hujum buzg'unchi tarafidan tizimdagi P_{ti} va S_{ti} , i=1….n xarakteristikalarga ega aniqlangan va barataraf etilmagan zaifliklarning ketma-ket ishlatilishi kabi ko'rilsa, hujum murakkabligining miqdoriy xarakteristikasi $S_{ti} = J(P_{ti})$ ni kiritish mumkin. Ushbu xarakteristika hujumi muvaffaqiyatli amalga oshirish uchun buzg'unchi ega bo'lishi lozim bo'lgan axborot miqdori orqali aniqlanadi.

$$S_t = J(P_{ti}) = -\log_2(1-P_{ti}) = \log_2 \prod_{i=1}^{n}(1 - Pti)$$

Bu yerda $P_{ti} = 1-\prod_{i=1}^{n}(1 - Pti)$- vaqtning xar qanday onida hujum tahdidi real ekanligining ehtimolligi.

Logarifmlarning mos xususiyatlaridan foydalanib, quyidagilarni yozishimiz mumkin.

$$S_t = J(P_t)=\sum_{i=1}^{n} J(Pt2)= \sum_{i=1}^{n} Sti$$

Bunda buzg'unchi ega bo'ladigan axborotga axborot tizimiga muvaffaqiyatli hujumning amalga oshirilishidagi foydalilik (muhimlik) nuqtai nazaridan qaraladi.

Ushbu o'lchov turli printsiplarga asoslangan, tabiati bo'yicha tamomila turli zaiflik tahdidlardan foydalanuvchi xilma-xil hujumlarni amalga oshirish murakkabligini o'zaro taqoslashga imkon beradi.

Axborot tizimiga hujumni amalga oshirishning miqdoriy integral bahosini akslantiruvchi matematik modeli

Yuqorida keltirilganlarni hisobga olgan holda, buzg'unchining muayyan axborot tizimiga hujumni amalga oshirishga manfaatligini va imkoniyatining miqdoriy integral bahosini akslantiruvchi matematik modelni quyidagicha ifodalash mumkin:

$$S_{tb} \approx max\{ S_{tbi} , i=1……n\}$$

bu yerda, S_{tb} – amalga oshirilgan hujumlarning maksimal murakkabligi. Ushbu hujumlar axborot tizimi ekspluatatsiyasi jarayonida amalga oshirilgan hujumlar to'plamida aniqlanadi.

XULOSA

Xulosa sifatida aytish mumkinki, izlangan xarakteristika qiymatini hisoblashda qandaydir ekspert baholashdan foydalanish talab etilmaydi. Ko'rilgan modellash yondashuvida zaiflik tahdidlarining stoxastik parametrlaridan hamda tizim ekspluatatsiyasi xavfsizligiga nisbatan statistikadan foydalanish kifoya. Axborot tizimining himoya qilish tizimini loyihalashdagi ko'rib chiqilgan usullar, ya'ni matematik modellardan foydalanishga asoslangan tegishli optimallashtirish muammosini hal qiladi.

ADABIYOTLAR RO‘YXATI

1. Sheglov A.YU., Sheglov K.A. Matematicheskie modeli i metodi formal`nogo proektirovaniya sistem zashiti informatsionnix sistem. Uchebnoe posobie. Sankt-Peterburg: Universitet ITMO, 2015. S 41-83.

2. Vostretsova YE. V. Osnovi informatsionnoy bezopasnosti. Uchebnoe posobie. Yekaterinburg: Izdatel`stvo Ural`skogo universiteta, 2019. S 68-125.

3. Robert Vrabel,Marcel Abas,Pavol Tanuska,Pavel Vazan,Michal Kebisek,Michal Elias,Zuzana Sutova, Dusan Pavliak. Mathematical Approach to Security Risk Assessment. Mathematical Problems in Engineering. 2015.