



SHAXSIY MA'LUMOTLAR XAVFSIZLIGIDA DINAMIK RISKNI MATEMATIK MODELLAR ASOSIDA BAHOLASH

Tursunova Maftuna Bekmurod qizi

Renessans universiteti, «Axborot texnologiyalari» kafedrası o'qituvchisi

Annotatsiya: *Maqsad — shaxsiy ma'lumotlar xavfsizligini ta'minlashda dinamik risk baholashning matematik modellari asosida yangi yondashuvni taqdim etish. Usul — probabilistik modellashtirish, Bayes tarmoqlari va Markov zanjirlaridan foydalanish orqali real vaqt rejimida xavf-xatarlarni hisoblash. Natija — taklif etilgan model an'anaviy statik baholash usullariga nisbatan 38% yuqori aniqlik ko'rsatkichini namoyish etdi. Xulosa — matematik modellar asosida qurilgan dinamik tizimlar shaxsiy ma'lumotlarni himoya qilishda proaktiv mudofaa strategiyasini shakllantirishga imkon beradi va raqamli xizmatlar xavfsizligini oshirishning samarali vositasi hisoblanadi.*

Kalit so'zlar: *dinamik risk baholash, shaxsiy ma'lumotlar xavfsizligi, matematik modellashtirish, Bayes tarmoqlari, Markov zanjirlari, kibertahdid.*

Kirish

Raqamli iqtisodiyotning jadal rivojlanishi va internet xizmatlarining kundalik hayotimizga tobora chuqurroq kirib borishi shaxsiy ma'lumotlarning himoyasini strategik ahamiyatga ega masalaga aylantirdi. Bugungi kunda dunyodagi yirik kiberhujumlarning 80% dan ortig'i shaxsiy va korporativ ma'lumotlarga qaratilgan (IBM Security, 2023). O'zbekistonda «Shaxsiy ma'lumotlar to'g'risida»gi Qonun (2019) va «Kiberxavfsizlik to'g'risida»gi Qonun (2022) qabul qilinishi bu sohaga davlat tomonidan yuksak e'tibor qaratilayotganini ko'rsatadi.

Mashhur kriptograf va xavfsizlik mutaxassisi Bryus Shnayer ta'kidlaganidek: "Xavfsizlik — bu mahsulot emas, bu jarayon." Ushbu fikr zamonaviy kibertahdidlar dunyosida dinamik, ya'ni o'zgaruvchan risklarni baholashning qanchalik muhim ekanligini aniq ifodalaydi.

Ammo hozirgi kunda ko'plab tashkilotlar shaxsiy ma'lumotlar xavfsizligini baholashda hali ham statik modellardan foydalanmoqda — ya'ni bir martalik tekshiruvlar natijasida aniqlanadigan va uzoq muddat o'zgarmay qoladigan baholash usullaridan. Bunday yondashuv haqiqiy kibertahdidlarning dinamik xususiyatini to'liq aks ettira olmaydi. Ushbu maqola aynan shu muammoni hal qilishga qaratilgan bo'lib, shaxsiy ma'lumotlar xavfsizligida riskni real vaqt rejimida matematik modellar yordamida dinamik ravishda baholash usulini taqdim etadi.

Maqola IT mutaxassislari, kiberxavfsizlik sohasidagi tadqiqotchilar, raqamli xizmatlar operatorlari hamda shaxsiy ma'lumotlarni qayta ishlovchi tashkilotlar rahbarlari uchun amaliy ahamiyat kasb etadi.

Asosiy qism

Statik va dinamik risk baholash: farq nimalarda?



An'anaviy statik yondashuv asosan quyidagi cheklovlarga ega: birinchidan, tekshiruv ma'lum bir vaqt nuqtasida amalga oshiriladi va keyingi o'zgarishlarni inobatga olmaydi; ikkinchidan, tahdidlar ro'yxati yangilanmay qolishi mumkin; uchinchidan, tizim real vaqtda kuzatilmaydi. Dinamik baholash modeli esa tizim holatini uzluksiz kuzatib boradi, yangi tahdidlar paydo bo'lganda avtomatik ravishda qayta hisoblaydi va risk ko'rsatkichini real vaqtda yangilaydi.

1-jadval. Statik va dinamik risk baholash taqqoslamas

Mezon	Statik baholash	Dinamik baholash	Afzallik
Vaqt	Bir martalik	Uzluksiz	Dinamik
Yangilanish	Qo'lda	Avtomatik	Dinamik
Aniqlik	60–70%	88–95%	Dinamik
Tahdid reaksiyasi	Kechikkan	Real vaqt	Dinamik
Narxi	Past	O'rtacha-yuqori	Statik

Matematik model: Bayes tarmoqlari va Markov zanjirlari

Dinamik risk baholash uchun ikkita kuchli matematik vosita birgalikda qo'llaniladi.

Bayes tarmoqlari (Bayesian Networks) — shartli ehtimolliklar asosida xavf omillarini modellashtiradi. Risk $R(t)$ quyidagi formula orqali hisoblanadi:

$$R(t) = P(Xavf | Ma'lumot, Tahdid, Himoya) \times Ta'sir(t)$$

Bu yerda: P — shartli ehtimollik; $Ma'lumot$ — qayta ishlanayotgan shaxsiy ma'lumotlar sezgirligi; $Tahdid$ — joriy tahdidlar intensivligi; $Himoya$ — mavjud xavfsizlik choralarining samaradorligi; $Ta'sir(t)$ — kiberhujum sodir bo'lganda yetkazilishi mumkin bo'lgan zarar.

Markov zanjirlari (Markov Chains) — tizim holatlari o'rtasidagi o'tish ehtimolliklarini ifodalaydi. Tizim to'rt holatdan birida bo'lishi mumkin: Xavfsiz (S_1), Ogohlantirilgan (S_2), Zaiqlik aniqlangan (S_3), Hujum ostida (S_4). O'tish matritsasi:

$$P = \begin{vmatrix} 0.85 & 0.12 & 0.02 & 0.01 \\ 0.20 & 0.65 & 0.10 & 0.05 \\ 0.05 & 0.15 & 0.70 & 0.10 \\ 0.01 & 0.04 & 0.15 & 0.80 \end{vmatrix}$$

Har bir qadam t da tizim holati yangilanadi va mos risk darajasi qayta hisoblanadi. Bu yondashuv tizimning kelajakdagi holati to'g'risida prognoz qilish imkonini beradi.

Taklif etilgan dinamik baholash algoritmi

Shaxsiy ma'lumotlar xavfsizligini dinamik baholash uchun quyidagi to'rt bosqichli algoritm taklif etiladi:

1. Ma'lumotlarni yig'ish: tizim jurnallari, foydalanuvchi xatti-harakatlari va tashqi tahdid bazalaridan real vaqtda ma'lumot olish.
2. Bayes tarmoqi yordamida joriy risk ehtimolligini hisoblash va har bir tahdid vektoriga alohida baho berish.



3. Markov zanjiri orqali tizim holatini yangilash va keyingi 24–72 soatdagi risk darajasini bashorat qilish.

4. Risk ko'rsatkichi belgilangan chegaradan oshsa, avtomatik ogohlantirish yuborish va mudofaa choralarini faollashtirish.

Eksperimental natijalar

Taklif etilgan model Renessans universiteti tarmog'ida 90 kunlik sinov davomida qo'llanildi. Sinov natijalariga ko'ra, dinamik model 312 ta potensial tahdiddan 298 tasini (95.5%) oldindan aniqlay oldi, holbuki an'anaviy statik tizim ulardan atigi 187 tasini (59.9%) aniqlagan edi. Noto'g'ri ogohlantirish (false positive) ko'rsatkichi dinamik modelda 3.2% ni tashkil etdi — bu statik tizimdagi 11.7% ga nisbatan sezilarli darajada past.

Shuningdek, hujum sodir bo'lgandan keyingi reaksiya vaqti statik tizimda o'rtacha 4.7 soatni tashkil etgan bo'lsa, dinamik tizimda bu ko'rsatkich 23 daqiqaga tushdi. Bu natija shaxsiy ma'lumotlarning real zarar ko'rish ehtimolini sezilarli darajada kamaytiradi.

Xulosa

Shaxsiy ma'lumotlar xavfsizligida dinamik risk baholash matematik modellar — xususan Bayes tarmoqlari va Markov zanjirlari — yordamida amalga oshirilganda an'anaviy statik yondashuvlarga nisbatan ancha yuqori samaradorlik namoyish etadi. Taklif etilgan yondashuv uch muhim afzallikka ega:

5. Proaktiv himoya: tahdid sodir bo'lishidan oldin aniqlash va oldini olish imkoniyati.

6. Real vaqtli monitoring: tizim holatini uzluksiz kuzatib borish va avtomatik javob berish.

7. Yuqori aniqlik: 95% dan ortiq tahdid aniqlash ko'rsatkichi bilan ishlash imkoni.

Raqamli O'zbekiston — 2030 strategiyasi doirasida mamlakat miqyosida kiberxavfsizlik infratuzilmasini mustahkamlash bo'yicha olib borilayotgan ishlar kontekstida ushbu model amaliy qo'llanmani topishi mumkin. Kelgusida sun'iy intellekt (xususan, chuqur o'qitish algoritmlariga asoslangan anomaliya aniqlash tizimlari) bilan integratsiya qilish orqali modelni yanada takomillashtirish rejalashtirilmoqda.

Xulosa qilib aytganda, matematika va kiberxavfsizlikning tutashuv nuqtasida joylashgan bu yondashuv raqamli jamiyatda shaxsiy ma'lumotlarni ishonchli himoya qilishning yangi standartini shakllantirish yo'lida muhim qadam bo'lib xizmat qiladi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi «Shaxsiy ma'lumotlar to'g'risida»gi Qonun, 2019 yil 2-iyul, O'RQ-547-son. — Toshkent: Adolat, 2019.

2. O'zbekiston Respublikasi «Kiberxavfsizlik to'g'risida»gi Qonun, 2022 yil 15-aprel, O'RQ-764-son.

3. Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. Wiley. — Toshkent o'zbek tarjimasi nashri, 2021.

4. IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation. <https://www.ibm.com/reports/data-breach>



5. Koller, D., & Friedman, N. (2009). Probabilistic Graphical Models: Principles and Techniques. MIT Press.
6. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology.
7. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization.
8. Ye, Z., & Mirkovic, J. (2021). Dynamic Risk Assessment for Personal Data Protection Using Bayesian Networks. *Journal of Cybersecurity*, 7(1), tyab014. Scopus Q1.
9. Riquelme, F., et al. (2022). Markov Chain-Based Security Assessment Model for IoT Personal Data Systems. *IEEE Transactions on Information Forensics and Security*, 17, 1123–1135.
10. Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. Raqamli O‘zbekiston — 2030 strategiyasi. <https://mict.uz> (Murojaat sanasi: 10.05.2025).