O'QUVCHI MA'LUMOTLARI XAVFSIZLIGI: SOFENA TEXNIK-HUQUQIY TAHLILI

Zubaytova Mehriniso Husniddinovna
Buxoro davlat innovatsiyalar universiteti magistranti
E-mail: zubaytovazubaytova@gmail.com
ORCID: https://doi.org/10.5281/zenodo.21195984

Annotatsiya. Mazkur maqolada raqamli ta'lim tizimlarida o‘quvchilarga oid shaxsiy ma'lumotlarni himoya qilish muammosi SOFENA axborot platformasi misolida texnik-huquqiy nuqtai nazardan tahlil qilinadi. Zamonaviy ta'lim platformalari foydalanuvchining identifikatsiya ma'lumotlari, o‘quv faoliyati, baholash natijalari, tizimga kirish tarixi va xulq-atvorga oid raqamli izlarni qayta ishlashi mumkin. Ushbu ma'lumotlarning markazlashgan shaklda saqlanishi ta'lim jarayonini individuallashtirish imkoniyatini oshirishi bilan birga, maxfiylik, ruxsatsiz foydalanish va ma'lumotlardan ikkilamchi maqsadlarda foydalanish bilan bog‘liq xavflarni yuzaga keltiradi. Tadqiqotda SOFENA tizimi uchun tahdidlarni modellashtirish, ma'lumotlar hayotiy siklini tahlil qilish va normativ-huquqiy talablarni texnik boshqaruv mexanizmlari bilan muvofiqlashtirish metodologiyasi taklif etildi. STRIDE tahdid modeli, CIA triadasi va privacy by design tamoyillari asosida o‘quvchi ma'lumotlari xavfsizligining konseptual arxitekturasi ishlab chiqildi. Tahlil natijasida shifrlash, rollarga asoslangan kirish nazorati, psevdonimlashtirish, audit jurnallari va ma'lumotlarni minimallashtirish alohida xavfsizlik vositalari emas, balki yagona boshqaruv tizimining o‘zaro bog‘liq komponentlari sifatida qo‘llanilishi lozimligi asoslandi. Maqolada texnik xavfsizlik va huquqiy muvofiqlik o‘rtasidagi farq ko‘rsatilib, ta'lim platformalari uchun riskka asoslangan integratsiyalashgan himoya modeli taklif qilinadi.

Kalit so‘zlar: o‘quvchi ma'lumotlari, shaxsga doir ma'lumotlar, SOFENA, axborot xavfsizligi, ta'lim platformasi, privacy by design, STRIDE, RBAC, psevdonimlashtirish, ma'lumotlarni minimallashtirish, texnik-huquqiy muvofiqlik.

Kirish. Ta'lim tizimining raqamlashtirilishi natijasida o‘quvchi haqida shakllantiriladigan ma'lumotlar hajmi va ularning analitik qiymati sezilarli darajada oshmoqda. An'anaviy ta'lim muhitida o‘quvchi haqidagi asosiy ma'lumotlar shaxsiy hujjatlar, davomat jurnali va baholash natijalari bilan chegaralangan bo‘lsa, zamonaviy raqamli ta'lim platformasi foydalanuvchining tizim bilan deyarli har bir o‘zaro ta'sirini qayd etish imkoniyatiga ega.

Tizimga kirish vaqti, topshiriqni bajarishga sarflangan vaqt, noto‘g‘ri javoblar ketma-ketligi, o‘quv materialini takror ko‘rish holatlari va boshqa telemetrik ko‘rsatkichlar pedagogik tahlil uchun muhim ma'lumot manbai hisoblanadi. Biroq ayni

ma'lumotlar birlashtirilganda o‘quvchining bilim darajasi va o‘quv xulq-atvoriga oid batafsil raqamli profil shakllanishi mumkin.

Ushbu holat ta'lim texnologiyalarida fundamental qarama-qarshilikni yuzaga keltiradi. Bir tomondan, individual ta'lim trayektoriyasini shakllantirish uchun tizim o‘quvchi faoliyati haqida yetarli ma'lumotga ega bo‘lishi kerak. Ikkinchi tomondan, ortiqcha ma'lumot yig‘ilishi maxfiylik va axborot xavfsizligi xavfini oshiradi.

Mazkur muammoni quyidagi konseptual munosabat orqali ifodalash mumkin:

P ↑ → D ↑ → R ↑

bu yerda:

P — ta'limni personallashtirish darajasi;

D — qayta ishlanadigan ma'lumotlar hajmi va detallashtirish darajasi;

R — ma'lumotlar bilan bog‘liq potensial xavf.

Mazkur formula universal matematik qonun emas. U tadqiqot doirasida qo‘llanilayotgan konseptual model bo‘lib, personallashtirish uchun ko‘proq ma'lumot qayta ishlanishi xavf yuzasini kengaytirishi mumkinligini ifodalaydi.

SOFENA kabi raqamli ta'lim tizimlarida ushbu muammo ayniqsa dolzarbdir. Platformada o‘quvchi, o‘qituvchi va ma'mur kabi turli subyektlar ishtirok etishi mumkin. Har bir subyektning ma'lumotlardan foydalanish maqsadi va vakolati turlicha bo‘ladi. Shu sababli faqat foydalanuvchini autentifikatsiya qilish o‘quvchi ma'lumotlarini to‘liq himoya qilish uchun yetarli emas.

Tadqiqotning maqsadi SOFENA ta'lim platformasi kontekstida o‘quvchi ma'lumotlari xavfsizligini texnik va huquqiy mezonlar asosida tahlil qilish hamda privacy by design tamoyiliga asoslangan himoya modelini ishlab chiqishdan iborat.

Tadqiqotning asosiy savoli quyidagicha shakllantirildi: ta'lim platformasida o‘quvchi ma'lumotlarini pedagogik maqsadlarda qayta ishlash imkoniyatini saqlagan holda ruxsatsiz foydalanish, ortiqcha ma'lumot yig‘ish va ikkilamchi maqsadlarda foydalanish xavfini qanday kamaytirish mumkin?

Tadqiqot gipotezasi quyidagicha: o‘quvchi ma'lumotlari xavfsizligi faqat kriptografik himoya orqali emas, balki ma'lumotlarni minimallashtirish, maqsadga bog‘langan qayta ishlash, granular kirish nazorati va tekshiriladigan audit mexanizmlarini yagona arxitekturada integratsiya qilish orqali samaraliroq ta'minlanadi.

Adabiyotlar tahlili. Axborot xavfsizligi bo‘yicha klassik nazariyalarda ma'lumotlarni himoya qilish maxfiylik, yaxlitlik va mavjudlikdan iborat CIA triadasi orqali tushuntiriladi. Maxfiylik — ma'lumotdan faqat vakolatli subyektlar foydalanishini; yaxlitlik — ma'lumotning ruxsatsiz o‘zgartirilmasligini; mavjudlik esa vakolatli foydalanuvchi zarur vaqtda tizim va ma'lumotlardan foydalana olishini anglatadi.

Ta'lim platformalarida ushbu uch komponent o‘ziga xos xususiyatga ega. Masalan, o‘quvchining bahosi maxfiy saqlanishi kerak. Shu bilan birga, bahoning o‘qituvchi yoki

boshqa subyekt tomonidan ruxsatsiz o‘zgartirilishiga yo‘l qo‘yilmasligi lozim. Tizimning mavjudligi ham ta'lim jarayonining uzluksizligi uchun muhim hisoblanadi.

NIST tomonidan ishlab chiqilgan Cybersecurity Framework 2.0 axborot xavfsizligi risklarini boshqarishni Govern, Identify, Protect, Detect, Respond va Recover funksiyalari orqali tizimlashtiradi [1]. Mazkur yondashuv xavfsizlikni faqat hujumni bloklash bilan cheklamaydi. Tashkilot avvalo boshqaruv va risk kontekstini belgilashi, aktivlarni aniqlashi, himoya vositalarini qo‘llashi, hodisalarni aniqlashi va ularga javob berishi kerak.

Maxfiylik masalasida Cavoukian tomonidan shakllantirilgan Privacy by Design konsepsiyasi alohida ahamiyatga ega [2]. Ushbu yondashuvga ko‘ra, maxfiylik tizim ishlab chiqilgandan keyin qo‘shiladigan qo‘shimcha funksiya emas. U tizim arxitekturasining boshlang‘ich talablaridan biri sifatida loyihalashtirilishi lozim.

Privacy by Design tamoyili Yevropa Ittifoqining General Data Protection Regulation hujjatida data protection by design and by default konsepsiyasi bilan normativ ahamiyat kasb etgan. GDPRning 25-moddasi ma'lumotlarni himoya qilish tamoyillarini qayta ishlash vositalariga integratsiya qilish va standart holatda faqat muayyan maqsad uchun zarur bo‘lgan shaxsiy ma'lumotlarni qayta ishlash zaruratini belgilaydi [3].

GDPR O‘zbekiston hududidagi barcha ta'lim platformalariga avtomatik ravishda tatbiq etiladi, degan xulosa chiqarish noto‘g‘ri. Uning hududiy qo‘llanish doirasi alohida huquqiy mezonlar asosida aniqlanadi. Biroq privacy by design, data minimisation va purpose limitation kabi tamoyillar axborot tizimining texnik arxitekturasini tahlil qilish uchun muhim xalqaro metodologik asos bo‘lib xizmat qiladi.

O‘zbekiston Respublikasida shaxsga doir ma'lumotlarni qayta ishlash bilan bog‘liq asosiy munosabatlar “Shaxsga doir ma'lumotlar to‘g‘risida”gi Qonun bilan tartibga solinadi [4]. Mazkur normativ kontekst ta'lim platformasida ma'lumotlarni yig‘ish, qayta ishlash, saqlash va himoya qilish jarayonlarini faqat texnik masala sifatida ko‘rib chiqish mumkin emasligini ko‘rsatadi.

Voyaga yetmagan foydalanuvchilar bilan bog‘liq tizimlarda maxfiylik masalasi yanada murakkablashadi. UNICEF bolalar uchun sun'iy intellekt va raqamli tizimlarni loyihalashda ularning maxfiyligi, xavfsizligi va manfaatlarini alohida hisobga olish zarurligini ta'kidlaydi [5].

Mavjud adabiyotlarning tahlili shuni ko‘rsatadiki, ta'lim texnologiyalarida xavfsizlik ko‘pincha autentifikatsiya, parol siyosati yoki ma'lumotlar bazasini shifrlash bilan bog‘lanadi. Biroq texnik jihatdan yaxshi himoyalangan tizim ham ma'lumotlarni ortiqcha yig‘ishi yoki ularni dastlabki maqsaddan tashqari qayta ishlashi mumkin.

Demak:

Security ≠ Privacy.

Axborot xavfsizligi ma'lumotni ruxsatsiz subyektdan himoya qiladi. Maxfiylik esa vakolatli subyektning ham ma'lumotdan qanday maqsadda va qanday chegarada foydalanishi mumkinligi masalasini qamrab oladi.

Mazkur farq SOFENA tizimining texnik-huquqiy tahlilida asosiy nazariy nuqta sifatida qabul qilindi.

Tadqiqot metodologiyasi

Tadqiqotda texnik-huquqiy, tizimli va riskka asoslangan tahlil metodlaridan foydalanildi. Tadqiqot real penetratsion test natijalarini taqdim etishni emas, balki SOFENA turidagi ta'lim axborot tizimi uchun takrorlanadigan xavfsizlik baholash modelini shakllantirishni maqsad qiladi.

Metodologiya to‘rt bosqichdan tashkil topadi:

1. ma'lumotlar hayotiy siklini xaritalash;
2. aktivlar va tahdidlarni identifikatsiya qilish;
3. texnik himoya vositalarini baholash;
4. texnik mexanizmlarni huquqiy talablar bilan muvofiqlashtirish.

Ma'lumotlar hayotiy siklini tahlil qilish

O‘quvchi ma'lumotining tizimdagi harakati quyidagi model asosida tahlil qilinadi:

Collection → Transmission → Processing → Storage → Sharing → Deletion.

Birinchi bosqichda ma'lumot foydalanuvchi, o‘qituvchi yoki avtomatik telemetriya mexanizmi orqali yig‘iladi.

Ikkinchi bosqichda ma'lumot mijoz qurilmasidan serverga uzatiladi.

Uchinchi bosqichda ma'lumot pedagogik yoki analitik algoritmlar tomonidan qayta ishlanadi.

To‘rtinchi bosqich ma'lumotlarning doimiy yoki vaqtinchalik saqlanishini qamrab oladi.

Beshinchi bosqichda ma'lumot ichki xizmatlar, vakolatli xodimlar yoki tashqi integratsiya tizimlari bilan almashilishi mumkin.

Oltinchi bosqich ma'lumotni o‘chirish yoki identifikatsiya imkoniyatini qaytarib bo‘lmaydigan darajada yo‘qotish jarayonidir.

Har bir bosqich uchun alohida tahdid va huquqiy savol mavjud.

Masalan:

Bosqich	**Texnik xavf**	**Huquqiy-maxfiylik savoli**
Yig‘ish	Zararli ma'lumot kiritish	Ma'lumot zarurmi?
Uzatish	Traffic interception	Uzatish himoyalanganmi?
Qayta ishlash	Vakolatdan tashqari foydalanish	Maqsad aniqmi?
Saqlash	Ma'lumotlar bazasi buzilishi	Saqlash muddati asoslanganmi?
Almashish	Data leakage	Qabul qiluvchi vakolatlimi?

O‘chirish	Backup nusxada qolish	Haqiqiy o‘chirish ta'minlanganmi?

Tahdidlarni STRIDE modeli asosida baholash

SOFENA tizimining konseptual xavfsizlik tahlili uchun STRIDE modeli qo‘llanildi.

STRIDE quyidagi tahdid toifalarini qamrab oladi:

S — Spoofing;

T — Tampering;

R — Repudiation;

I — Information Disclosure;

D — Denial of Service;

E — Elevation of Privilege.

O‘quvchi ma'lumotlari kontekstida spoofing hujumi boshqa o‘quvchi yoki o‘qituvchi hisobiga noqonuniy kirishni anglatishi mumkin.

Tampering holatida baholar, topshiriq natijalari yoki o‘quv faoliyati haqidagi yozuvlar ruxsatsiz o‘zgartiriladi.

Repudiation tizimda amalga oshirilgan operatsiyani keyinchalik inkor qilish bilan bog‘liq.

Information Disclosure o‘quvchi ma'lumotlarining vakolatsiz shaxsga oshkor bo‘lishini anglatadi.

Denial of Service ta'lim platformasining mavjudligini buzadi.

Elevation of Privilege oddiy foydalanuvchining o‘qituvchi yoki administrator vakolatlarini noqonuniy egallashini ifodalaydi.

Riskni miqdoriy baholash

Tadqiqot doirasida soddalashtirilgan risk modeli qo‘llanildi:

$R = L \times I \times E$.

Bu yerda:

R — umumiy risk balli;

L — tahdidning amalga oshish ehtimoli;

I — potensial ta'sir darajasi;

E — ma'lumotning ekspozitsiya koeffitsienti.

Har bir ko‘rsatkich 1 dan 5 gacha bo‘lgan shkalada baholanadi.

Natijada:

$1 \leq R \leq 125$.

Risk darajalari tadqiqot modeli doirasida quyidagicha tasniflandi:

Risk balli	Daraja
1–20	Past
21–50	O‘rta
51–80	Yuqori

81–125 Kritik

Mazkur shkala qonunchilikda belgilangan rasmiy risk tasnifi emas. U turli texnik tahdidlarni qiyosiy baholash uchun tadqiqot instrumenti sifatida taklif etiladi.

SOFENA tizimida o‘quvchi ma'lumotlarining konseptual tasnifi. Axborot tizimida barcha ma'lumotlarni bir xil darajada himoya qilish resurslardan samarasiz foydalanishga olib kelishi mumkin. Shu sababli ma'lumotlarni xavf darajasiga qarab tasniflash taklif qilinadi.

D1 — ochiq yoki past xavfli ma'lumotlar

Mazkur toifaga ommaviy o‘quv materiali, fan nomi va umumiy kurs tavsifi kiritilishi mumkin.

D2 — ichki ma'lumotlar

Tizimning ichki konfiguratsiyasiga bog‘liq ayrim texnik ma'lumotlar va autentifikatsiya qilinmagan foydalanuvchiga ko‘rsatilmasligi kerak bo‘lgan resurslar ushbu toifaga kiritiladi.

D3 — shaxsga doir o‘quv ma'lumotlari

O‘quvchining identifikatsiya ma'lumotlari, individual baholari, topshiriq natijalari va davomat ko‘rsatkichlari mazkur toifaga mansub bo‘lishi mumkin.

D4 — yuqori xavfli profil va autentifikatsiya ma'lumotlari

Parol xeshlari, autentifikatsiya tokenlari, sessiya identifikatorlari hamda birlashtirilganda o‘quvchining batafsil xulq-atvor profilini shakllantiruvchi ma'lumotlar yuqori himoya talab qiluvchi toifa sifatida baholanadi.

Ma'lumotlar tasnifi quyidagi funksiyaga ta'sir qilishi kerak:

Security Control = F(Data Class, User Role, Processing Purpose).

Demak, himoya vositasi faqat foydalanuvchining roliga emas, ma'lumot turi va qayta ishlash maqsadiga ham bog‘liq bo‘lishi lozim.

Natijalar va texnik-huquqiy tahlil. Ko‘plab axborot tizimlarida foydalanuvchi login va parol orqali tizimga kirgandan keyin “ishonchli” subyekt sifatida qabul qilinadi. Mazkur yondashuv ta'lim platformasi uchun yetarli emas.

Faraz qilaylik, o‘qituvchi tizimga qonuniy autentifikatsiya qilindi. Bu fakt unga platformadagi barcha o‘quvchilarning barcha ma'lumotlarini ko‘rish huquqini avtomatik ravishda bermasligi kerak.

Shu sababli:

Authentication ≠ Authorization.

Autentifikatsiya “foydalanuvchi kim?” savoliga javob beradi.

Avtorizatsiya esa “ushbu foydalanuvchi ayni resurs bilan qanday operatsiya bajarishi mumkin?” savolini hal qiladi.

SOFENA tizimi uchun rollarga asoslangan kirish nazorati — Role-Based Access Control modelidan foydalanish mumkin.

Konseptual rollar quyidagilardan iborat:

- Student;

- Teacher;
- School Administrator;
- System Administrator;
- Security Auditor.

Kirish qarori quyidagi funksiya bilan ifodalanadi:

A = F(U, R, O, P, C),

bu yerda:

U — foydalanuvchi;

R — foydalanuvchi roli;

O — obyekt yoki ma'lumot;

P — bajarilayotgan operatsiya;

C — kontekst.

Masalan, Teacher roli “student_result” obyektini o‘qish huquqiga ega bo‘lishi mumkin. Biroq kontekstual shart o‘qituvchi faqat o‘zi dars beradigan sinf yoki guruh o‘quvchilarining natijalarini ko‘rishini talab qilishi mumkin.

Bu holatda sof RBAC modeli yetarli bo‘lmasligi mumkin. RBAC va Attribute-Based Access Control elementlarini birlashtirish maqsadga muvofiq:

Permit if Role = Teacher AND Teacher.school_id = Student.school_id AND Teacher.class_id ∈ Student.class_ids.

Mazkur nazorat server tomonida bajarilishi kerak. Faqat foydalanuvchi interfeysida tugmani yashirish xavfsizlik mexanizmi hisoblanmaydi.

Ta'lim tizimlari uchun potensial xavflardan biri Insecure Direct Object Reference turidagi zaiflikdir.

Masalan, API so‘rovi quyidagi mantiqiy ko‘rinishga ega bo‘lishi mumkin:

GET /api/students/1024/results

Agar autentifikatsiya qilingan o‘quvchi URL yoki API parametridagi 1024 identifikatorini 1025 qiymatiga almashtirish orqali boshqa o‘quvchining natijasini olsa, tizimda obyekt darajasidagi avtorizatsiya buzilgan bo‘ladi.

Texnik jihatdan server har bir so‘rovda quyidagini tekshirishi kerak:

CanAccess(current_user, requested_object) = true.

Mazkur tekshiruv frontend darajasida emas, ma'lumot taqdim etuvchi server komponentida amalga oshirilishi lozim.

Huquqiy nuqtai nazardan ham ushbu zaiflik muhimdir. Tizim operatorining ma'lumotni qayta ishlash uchun huquqiy asosi mavjud bo‘lishi ma'lumotni istalgan autentifikatsiya qilingan foydalanuvchiga oshkor qilish huquqini anglatmaydi.

Ma'lumotlarni shifrlash

SOFENA tizimida shifrlash ikki asosiy holat bo‘yicha tahlil qilinishi kerak:

data in transit;

data at rest.

Mijoz va server o‘rtasidagi aloqa TLS protokoli orqali himoyalanishi lozim. Bu tarmoq orqali uzatilayotgan autentifikatsiya va o‘quv ma'lumotlarini passiv kuzatish xavfini kamaytiradi.

Saqlanayotgan ma'lumotlar uchun disk yoki ma'lumotlar bazasi darajasidagi shifrlash qo‘llanilishi mumkin.

Biroq shifrlashning muhim cheklovi mavjud.

Agar dastur serveri ma'lumotni qonuniy ravishda deshifrlash kalitiga ega bo‘lsa va hujumchi aynan dastur darajasidagi yuqori vakolatni egallasa, at-rest encryption ma'lumotni bunday hujumchidan avtomatik ravishda himoya qilmaydi.

Demak:

Encryption ≠ Complete Access Control.

Shifrlash va kirish nazorati bir-birini almashtiruvchi emas, balki to‘ldiruvchi xavfsizlik mexanizmlaridir.

Parollarni saqlash

Foydalanuvchi paroli qayta tiklanadigan shaklda saqlanmasligi kerak.

Noto‘g‘ri model:

Database → AES(password).

Bunday arxitekturada shifrlash kaliti buzilgan taqdirda barcha foydalanuvchi parollarini qayta tiklash mumkin.

Parollar uchun maxsus password hashing algoritmidan foydalanish talab qilinadi:

H = KDF(P, S, C),

bu yerda:

P — foydalanuvchi paroli;

S — tasodifiy salt;

C — hisoblash xarajati parametrlari;

H — saqlanadigan xesh.

Argon2id kabi zamonaviy password hashing algoritmlari mazkur vazifa uchun qo‘llanilishi mumkin. Amaliy parametrlar server resurslari va xavfsizlik siyosati asosida alohida benchmark orqali tanlanishi kerak.

Psevdonimlashtirish

Ta'lim analitikasi har doim o‘quvchining ism va familiyasini bilishni talab qilmaydi.

Masalan, tizim quyidagi savolni tahlil qilishi mumkin:

“7-sinf o‘quvchilarining qaysi matematik mavzuda xatolar soni ko‘p?”

Ushbu analitik vazifa uchun quyidagi ma'lumot yetarli bo‘lishi mumkin:

student_pseudo_id

grade_level

topic_id

error_count

O‘quvchining ism-familiyasi analitik ma'lumotlar to‘plamidan ajratilishi mumkin.

Konseptual model:

Identity DB: P123 → Student Identity

Analytics DB: P123 → Learning Events

Identifikatsiya va analitika ma'lumotlarini mantiqiy yoki fizik jihatdan ajratish ma'lumotlar buzilishi holatidagi potensial ta'sirni kamaytirishi mumkin.

Biroq psevdonimlashtirish anonimlashtirish bilan teng emas.

Agar P123 identifikatorini real shaxs bilan qayta bog‘lash imkoniyati mavjud bo‘lsa, ma'lumot psevdonimlashtirilgan hisoblanadi. Shu sababli bunday ma'lumot uchun xavfsizlik nazorati saqlanib qolishi kerak.

Audit jurnallari va javobgarlik

O‘quvchi ma'lumotlaridan kim va qachon foydalanganini aniqlash imkoniyati xavfsizlikning muhim komponentidir.

Audit yozuvi quyidagi konseptual struktura asosida tashkil etilishi mumkin:

L = {actor, action, object, timestamp, result, context}.

Masalan:

actor = teacher_45

action = READ

object = student_result_1024

timestamp = T

result = ALLOWED

context = class_7A

Audit jurnali faqat texnik diagnostika vositasi sifatida ko‘rilmasligi kerak. U hisobdorlikni ta'minlash mexanizmi hisoblanadi.

Shu bilan birga, audit jurnalining o‘zi ham maxfiy ma'lumotga aylanishi mumkin. Masalan, “qaysi o‘qituvchi qaysi o‘quvchi profilini ko‘rgan” haqidagi ma'lumot foydalanuvchi faoliyati tarixini ifodalaydi.

Shuning uchun:

Security log is also data.

Audit jurnallariga kirish cheklanishi, ularning yaxlitligi himoyalanishi va saqlash muddati belgilanishi kerak.

Huquqiy talablarni texnik nazoratga transformatsiya qilish muammosi

Texnik-huquqiy tahlilning asosiy muammolaridan biri normativ talablarning ko‘pincha yuqori darajadagi tushunchalar bilan ifodalanishidir.

Masalan:

“ma'lumot faqat zarur maqsadda qayta ishlanishi kerak”.

Dasturiy ta'minot esa “zarur maqsad” tushunchasini bevosita bajara olmaydi. Mazkur huquqiy tamoyil texnik talabga transformatsiya qilinishi kerak.

Tadqiqot doirasida quyidagi model taklif qilinadi:

Legal Principle → System Requirement → Technical Control → Audit Evidence.

Masalan:

Huquqiy tamoyil: ma'lumotlarni minimallashtirish.

Tizim talabi: ro‘yxatdan o‘tishda pedagogik xizmat uchun zarur bo‘lmagan ma'lumot yig‘ilmasligi kerak.

Texnik nazorat: API schema faqat belgilangan maydonlarni qabul qiladi.

Audit dalili: ma'lumotlar bazasi sxemasi va API konfiguratsiyasi.

Yana bir misol:

Huquqiy tamoyil: maqsadni cheklash.

Tizim talabi: o‘quv analitikasi ma'lumotlaridan reklama profili yaratish uchun foydalanilmasligi kerak.

Texnik nazorat: analitika ma'lumotlar bazasiga marketing xizmatining service account hisobiga kirish berilmaydi.

Audit dalili: IAM siyosati va access log.

Shunday qilib, huquqiy muvofiqlikni faqat privacy policy hujjati orqali ta'minlash yetarli emas.

Huquqiy talab tizim arxitekturasida kuzatiladigan texnik nazoratga ega bo‘lishi lozim.

Risklarning texnik-empirik modeli

SOFENA tizimi uchun shartli tahdid ssenariylarini risk modeli asosida baholash mumkin.

Tahdid	L	I	E	Risk
Boshqa o‘quvchi profiliga IDOR orqali kirish	4	5	5	100
Administrator hisobining egallanishi	3	5	5	75
Audit jurnalining o‘zgartirilishi	2	4	4	32
TLSsiz ma'lumot uzatish	3	5	5	75
Ortiqcha telemetriya yig‘ish	5	3	5	75
Xizmatga DoS hujumi	3	4	3	36

Jadvaldagi ballar real SOFENA infratuzilmasida o‘tkazilgan penetratsion test natijalari emas. Ular taklif etilgan metodologiyaning ishlash mexanizmini ko‘rsatuvchi ssenariy qiymatlaridir.

Tahlilda IDOR ssenariysi 100 ball bilan kritik risk sifatida baholandi. Buning sababi hujumning nisbatan amalga oshirilishi mumkinligi, ta'sirning yuqoriligi va potensial ravishda ko‘p sonli o‘quvchi ma'lumotlari ekspozitsiyasi bilan bog‘liq.

Tadqiqot natijalari o‘quvchi ma'lumotlari xavfsizligini faqat kiberxavfsizlik muammosi sifatida ko‘rib chiqish yetarli emasligini ko‘rsatadi.

Serverni tashqi hujumdan himoya qilish, TLS sertifikatini o‘rnatish va parollarni xeshlash zarur texnik choralar hisoblanadi. Biroq ular tizimning ma'lumotlarni qonuniy, maqsadga muvofiq va minimal hajmda qayta ishlashini avtomatik ravishda ta'minlamaydi.

Masalan, o‘qituvchining o‘quvchi natijalariga kirishi texnik jihatdan ruxsat etilgan bo‘lishi mumkin. Lekin o‘qituvchi o‘zi ta'lim bermaydigan hudud yoki maktab o‘quvchilarining individual ma'lumotlarini ko‘ra olsa, muammo autentifikatsiyada emas, avtorizatsiya modelining haddan tashqari kengligidadir.

Shuningdek, platforma o‘quvchining har bir sichqoncha harakati, qurilma xususiyati va tizimdagi faoliyatini cheklanmagan muddat davomida saqlashi mumkin. Bunday tizim tashqi hujumga qarshi yuqori darajada himoyalangan bo‘lsa ham, ma'lumotlarni minimallashtirish nuqtai nazaridan xavfli arxitekturaga ega bo‘lishi mumkin.

Shu sababli xavfsizlikning an'anaviy savoli:

“Hujumchi ma'lumotni o‘g‘irlay oladimi?”

quyidagi savollar bilan kengaytirilishi kerak:

“Nima uchun ushbu ma'lumot yig‘ilmoqda?”

“Kim undan foydalanishi mumkin?”

“Qancha vaqt saqlanadi?”

“Boshqa maqsadda foydalanishni qaysi texnik mexanizm cheklaydi?”

“Amaldagi foydalanishni keyinchalik tekshirish mumkinmi?”

Mazkur savollarning texnik javobi mavjud bo‘lmasa, huquqiy talablar deklarativ darajada qolib ketishi mumkin.

SOFENA tizimi uchun eng istiqbolli yondashuv huquqshunos, axborot xavfsizligi mutaxassisi va dasturiy ta'minot arxitektori o‘rtasidagi integratsiyalashgan boshqaruv modelidir.

Huquqshunos ma'lumotlarni qayta ishlash chegaralarini aniqlaydi.

Tizim arxitektori ushbu chegaralarni dasturiy talabga transformatsiya qiladi.

Xavfsizlik mutaxassisi nazorat mexanizmlarini tekshiradi.

Audit tizimi esa talabning amalda bajarilganini ko‘rsatuvchi texnik dalillarni shakllantiradi.

Xulosa. Mazkur maqolada SOFENA ta'lim platformasi kontekstida o‘quvchi ma'lumotlari xavfsizligi texnik-huquqiy nuqtai nazardan tahlil qilindi. Tadqiqot natijalari ta'lim tizimida ma'lumotlarni himoya qilishni faqat autentifikatsiya, shifrlash yoki tarmoq xavfsizligi bilan cheklash metodologik jihatdan yetarli emasligini ko‘rsatdi.

O‘quvchi ma'lumotlarining xavfsizligi ma'lumot yig‘ilgan vaqtdan boshlab uning uzatilishi, qayta ishlanishi, saqlanishi, almashilishi va o‘chirilishigacha bo‘lgan to‘liq hayotiy siklni qamrab olishi lozim.

STRIDE modeli asosidagi tahlil identifikatsiyani soxtalashtirish, ma'lumotlarni o‘zgartirish, axborotni oshkor qilish va vakolatlarni oshirish kabi klassik tahdidlarning ta'lim platformasi uchun dolzarbligini ko‘rsatadi. Shu bilan birga, ortiqcha telemetriya yig‘ish singari tashqi hujum bilan bog‘liq bo‘lmagan maxfiylik xavflari ham alohida baholanishi zarur. Umuman olganda, o‘quvchi ma'lumotlarini himoya qilish ta'lim

platformasining qo‘shimcha xavfsizlik funksiyasi emas. U tizim arxitekturasining fundamental sifati sifatida qaralishi lozim.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. Gaithersburg, MD, 2024.

2. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada, 2009.

3. European Parliament and Council of the European Union. *Regulation (EU) 2016/679: General Data Protection Regulation*. Official Journal of the European Union, 2016.

4. O‘zbekiston Respublikasi. *Shaxsga doir ma'lumotlar to‘g‘risida*. O‘RQ-547-son Qonun, 2019-yil 2-iyul.

5. UNICEF. *Policy Guidance on AI for Children*. Version 2.0. United Nations Children's Fund, 2021.

6. National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*. NIST, 2020.

7. OWASP Foundation. *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. OWASP, 2021.

8. OWASP Foundation. *OWASP API Security Top 10*. OWASP, 2023.

9. National Institute of Standards and Technology. *Digital Identity Guidelines: Authentication and Lifecycle Management*. NIST Special Publication 800-63B.

10. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., Youman, C. E. “Role-Based Access Control Models.” *IEEE Computer*, Vol. 29, No. 2, 1996, pp. 38–47.

11. Hu, V. C., Ferraiolo, D., Kuhn, R. et al. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. NIST Special Publication 800-162, 2014.

12. Biryukov, A., Dinu, D., Khovratovich, D. “Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications.” *IEEE European Symposium on Security and Privacy*, 2016.