Yevropa Ittifoqi tomonidan moliyalashtiriladi

ZAMONAVIY JURNALISTIKANI RIVOJLANTIRISH MARKAZI

LPRC LEGAL POLICY RESEARCH CENTRE

UDRMI O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI

FUQAROLIK FAOLLARI VA NNTLAR UCHUN RAQAMLI HUQUQLAR

Qanday tushunish, qo‘llash va amalda himoya qilish kerak?

FUQAROLIK FAOLLARI VA NNTLAR UCHUN RAQAMLI HUQUQLAR

Qanday tushunish, qo‘llash va amalda himoya qilish kerak?

Toshkent
2026

Fuqarolik faollari va NNTlar uchun raqamli huquqlar. Qanday tushunish, qo‘llash va amalda himoya qilish kerak? Toshkent, 2026 — 86 sahifa.

Ushbu qo‘llanma Yevropa Ittifoqining moliyaviy ko‘magida tayyorlandi. Uning mazmuni uchun to‘liq mas’uliyat Zamonaviy jurnalistikani rivojlantirish markazi zimmasiga yuklatilgan bo‘lib, unda bildirilgan fikrlar Yevropa Ittifoqining rasmiy nuqtai nazarini aks ettirmasligi mumkin.

Mualliflar jamoasi:
Lola Mahmudova (O‘zbekiston)
Madina Tursunova (O‘zbekiston)
Olga Didenko (Qozog‘iston)
Roman Reymer (Qozog‘iston)
Artyom Goryaynov (Qirg‘iziston)

Muharrir:
Lola Islamova

Mundarija

Ushbu qo‘llanmadan qanday foydalaniladi?

Ushbu qo‘llanma raqamli muhitda faoliyat yurituvchi notijorat tashkilotlar vakillari va fuqarolik faollari uchun amaliy vosita sifatida ishlab chiqilgan. U raqamli huquqlarning nazariy asoslarini, qonunchilik sharhini va kundalik faoliyatda foydalanish mumkin bo‘lgan amaliy tavsiyalarni birlashtiradi. Matn shunday tuzilganki, o‘quvchi nafaqat asosiy tamoyillarni tushunishi, balki ularni aniq ish vaziyatlarida qo‘llay olishi ham mumkin.

Qo‘llanmadan ketma-ket, ya’ni asosiy tushunchalardan amaliy masalalarga o‘tish orqali yoki tanlangan holda, ya’ni joriy vazifaga qarab alohida bo‘limlarga murojaat qilish orqali foydalanish mumkin. Birinchi bo‘lim raqamli huquqlar va ularning huquqiy tabiati haqida umumiy tushuncha beradi, ikkinchisi amaliy qo‘llanilishiga — kommunikatsiyalar, axborot va kontent bilan ishlashga qaratilgan, uchinchisi esa xavf-xatarlar va xavfsizlik choralariga bag‘ishlangan. Bunday bo‘linish matnda tezda mo‘ljal olish va kerakli ma’lumotni hujjatni to‘liq o‘qimasdan topish imkonini beradi.

Kundalik ishda qo‘llanmadan ma’lumotnoma sifatida foydalanish qulay. Masalan, axborot kampaniyasini tayyorlash, davlat organlariga so‘rovlar bilan ishlash, kontent nashr etish yoki xavflarni baholashda. Bunday hollarda darhol tegishli bo‘linmalarga murojaat qilish va taklif etilgan yondashuvlardan qaror qabul qilish uchun asos sifatida foydalanish mumkin. Shu bilan birga, qo‘llanmadagi tavsiyalar umumiy xususiyatga ega ekanligini va muayyan tashkilotning vazifalari hamda uning faoliyati kontekstini hisobga olgan holda moslashtirishni talab etishini hisobga olish muhimdir.

Material xodimlar va hamkorlarni o‘qitish uchun ham asos bo‘lib xizmat qilishi mumkin. Undan treninglar o‘tkazishda, ichki muhokamalarda va ish tartiblarini ishlab chiqishda foydalanish mumkin. Alohida bo‘limlar malaka oshirish dasturlariga kiritilishi yoki yangi xodimlar uchun uslubiy material sifatida foydalanilishi mumkin. Qo‘llanmaning amaliy ahamiyati NNTlar raqamli muhitda duch keladigan misollar, tizimli tushuntirishlar va namunaviy vaziyatlar orqali yanada kuchaytiriladi.

Qo‘llanma bilan ishlashda xavflarni baholashga alohida e’tibor qaratish lozim. Raqamli muhit nafaqat aloqalarni kengaytirish va ma’lumotlardan foydalanish imkoniyatlarini, balki harakatlar va kontent uchun yuqori mas’uliyatni ham nazarda tutadi. Matnda bir necha bor ta’kidlanishicha, ko‘plab qarorlar oqilona yondashuvni va ehtimoliy huquqiy hamda obro‘-e’tibor oqibatlarini tushunishni talab qiladi. Shuning uchun materialdan tayyor javoblar to‘plami sifatida emas, balki tahlil qilish va asosli qarorlar qabul qilish uchun asos sifatida foydalanish muhimdir.

Shunday qilib, qo‘llanmani raqamli muhitda yanada barqaror, xavfsiz va samarali amaliyotlarni shakllantirishga yordam beradigan ishchi vosita sifatida ko‘rish mumkin. Uning qimmati nafaqat me’yorlar va tamoyillarni bayon etishida, balki ularni amalda — kundalik ishda, loyihalarda va muloqotda qo‘llash imkoniyatidadir.

1-bo‘lim
Raqamli huquqlar nima?

1.1. Raqamli huquqlar nazariyasiga kirish

Zamonaviy dunyo hayotning deyarli barcha sohalarini qamrab olgan shiddatli raqamli transformatsiyani boshdan kechirmoqda. Axborot olish, ta’lim olish, ishga joylashish, biznes yuritish va xizmatlardan foydalanish tobora ko‘proq raqamli muhitda yuz bermoqda. Bugungi kunda xizmatlarning katta qismi ham davlat, ham xususiy sektor tomonidan ishlab chiqilgan onlayn platformalar orqali taqdim etilmoqda. Natijada raqamli infratuzilma kundalik hayotning ajralmas qismiga aylanmoqda.

Shu bilan birga, internetdan foydalanuvchilar soni ham tez sur’atlar bilan o‘sib bormoqda. Oktyabr oyi holatiga ko‘ra, dunyodagi foydalanuvchilarning umumiy soni 6,4 milliard kishidan[1] oshdi. DataReportal ma’lumotlariga ko‘ra, O‘zbekistonda 32,7 millionga yaqin kishi internetdan foydalanadi, bu aholining 92,2% tashkil etadi[2]. Ushbu ko‘rsatkichlar raqamli kirib borish ko‘lamini va uning jamiyat uchun ahamiyatini yaqqol ko‘rsatib beradi.

Bunday sharoitda raqamli makonni tartibga solish alohida ahamiyat kasb etadi. Bu an’anaviy huquqiy mexanizmlar har doim ham yetarli bo‘lmagan yangi muhitda inson huquqlarini ta’minlash va himoya qilish zarurati bilan bog‘liq. Aynan shu kontekstda raqamli huquqlar konsepsiyasi shakllanadi va rivojlanadi.

Raqamli inson huquqlari jamiyatning texnologik va axborot transformatsiyasi natijasidir. Aslida, ular xalqaro hujjatlarda mustahkamlangan klassik inson huquqlarining raqamli muhit sharoitlariga moslashuvi bo‘lib, zamonaviy huquqiy tizimning muhim qismiga aylanmoqda.

Inson huquqlarining zamonaviy tushunchasi Inson huquqlari umumjahon deklaratsiyasi (1948-yil), Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt (1966-yil) va Iqtisodiy, ijtimoiy va madaniy huquqlar to‘g‘risidagi xalqaro pakt (1966-yil) kabi asosiy hujjatlar, shuningdek, boshqa bir qator xalqaro va mintaqaviy hujjatlar asosida shakllangan. Bu tushunchaga ko‘ra, inson huquqlari — millati, yashash joyi, jinsi, etnik kelib chiqishi, tili, dini va boshqa belgilaridan qat’i nazar, har bir shaxsga tegishli bo‘lgan ajralmas huquqlar majmui sifatida qaraladi.

Ushbu huquqlar bir nechta fundamental tamoyillarga asoslanadi.

Birinchidan,

universallik tamoyili ularning istisnosiz barcha odamlarga tatbiq etilishini anglatadi.

Ikkinchidan,

ajralmaslik tamoyiliga ko‘ra, huquqlar qonunda qat’iy belgilangan cheklangan holatlardan tashqari, o‘zboshimchalik bilan tortib olinishi mumkin emas.

Uchinchidan,

bo‘linmaslik tamoyili fuqarolik, siyosiy, iqtisodiy va ijtimoiy huquqlarning o‘zaro bog‘liqligini va ularning alohida holda to‘liq amalga oshirilishi mumkin emasligini ta’kidlaydi.

---

1 https://www.statista.com/statistics/617136/digital-population-worldwide/?srsltid=AfmBOopuoIjbxLwhRpgdDEsIhkuTmSJ-jYKK6UPJ25PPsIw826z9BPwD

2 https://datareportal.com/reports/digital-2025-uzbekistan

Inson huquqlarining rivojlanishini tushunish uchun 1979-yilda huquqshunos Karel Vashak tomonidan taklif etilgan «huquq avlodlari» konsepsiyasidan foydalaniladi. U Buyuk fransuz inqilobi (1789-yil) shiori bilan ifodalangan «Ozodlik, Tenglik, Birodarlik» g‘oyasiga tayanadi va huquqiy fikrning tarixiy evolyutsiyasini aks ettiradi.

Huquqlarning birinchi avlodi erkinlik g‘oyasi bilan bog‘liq bo‘lib, fuqarolik va siyosiy huquqlarni o‘z ichiga oladi. Ularning asosiy vazifasi insonni davlat aralashuvidan himoya qilishdir. Gap davlatning muayyan harakatlardan o‘zini tiyish majburiyatini nazarda tutuvchi «salbiy huquqlar» haqida bormoqda. Bu shuni anglatadiki, ularni amalga oshirish uchun davlat xususiy sohaga aralashmasligi, qonuniy asoslarsiz erkinlikni cheklamasligi va shaxsning asosiy kafolatlarini buzmasligi kerak. Boshqa huquq toifalaridan farqli o‘laroq, bunday huquqlar murakkab infratuzilmani yaratishni yoki davlatning faol harakatlarini talab qilmaydi, balki birinchi navbatda aralashmaslik tamoyiliga asoslanadi. Hokimiyatdan ma’lum sohalarda «hech narsa qilmaslik» (o‘ldirmaslik, sudsiz qamamaslik, qiynoqqa solmaslik, qullikda saqlamaslik, senzura qilmaslik) talab qilinadi.

Asosiy huquqlar:

- Yashash va jismoniy daxlsizlik huquqi.
- Qiynoqlardan ozod bo‘lish huquqi.
- Qullikdan ozod bo‘lish huquqi.
- So‘z, vijdon va din erkinligi huquqi.
- Adolatli sudlovga bo‘lgan huquq (habeas corpus).
- Saylov huquqlari (faol va sust).
- Mulk huquqi

Huquqlarning ikkinchi avlodi tenglik g‘oyasi bilan bog‘liq bo‘lib, insonning munosib turmush darajasi va ijtimoiy himoyasini ta’minlashga qaratilgan ijtimoiy-iqtisodiy huquqlarni o‘z ichiga oladi. Bu yerda insonning jamiyatda to‘laqonli ishtirok etishi uchun zarur bo‘lgan shart-sharoitlar — mehnat, ta’lim, tibbiy yordam va ijtimoiy qo‘llab-quvvatlashdan foydalanish e’tibor markazida turadi.

Birinchi avlod huquqlaridan farqli o‘laroq, bu huquqlar «ijobiy» huquqlar toifasiga kiradi. Ularni amalga oshirish davlatdan nafaqat aralashuvdan tiyilishni, balki faol harakatlarni ham talab etadi. Gap tegishli infratuzilmani yaratish, ijtimoiy dasturlarni ishlab chiqish va insonga o‘z huquqlarini amalda ro‘yobga chiqarish imkonini beruvchi mexanizmlarni ta’minlash haqida bormoqda. Shunday qilib, davlat shunchaki aralashmaslik kafolati emas, balki munosib hayot sharoitlarini ta’minlovchi faol ishtirokchi sifatida namoyon bo‘ladi.

Asosiy huquqlar:

- Mehnat qilish va adolatli haq olish huquqi.
- Dam olish huquqi (me’yorlangan ish kuni).
- Ijtimoiy ta’minot (pensiyalar, nafaqalar) huquqi.
- Sog‘liqni saqlash va tibbiy yordam olish huquqi.
- Ta’lim olish huquqi.

Huquqlarning uchinchi avlodi birodarlik g‘oyasi bilan bog‘liq bo‘lib, jamoaviy huquqlar yoki birdamlik huquqlarini o‘z ichiga oladi. Avvalgi avlodlardan farqli o‘laroq, ular alohida odamga emas, balki odamlar guruhiga — xalqlarga, millatlarga yoki hatto butun insoniyatga tegishlidir.

Asosiy huquqlar:

- Rivojlanish huquqi.
- Tinchlik va xavfsizlik huquqi.
- Ekologik huquqlar, sog‘lom va toza atrof-muhitga bo‘lgan huquq.
- Insoniyatning umumiy merosiga bo‘lgan huquq.

Ushbu huquqlar bir qator global jarayonlar va muammolarni faqat individual erkinliklar darajasida ko'rib chiqish mumkin emasligini tushunishni aks ettiradi. Gap barqaror rivojlanish, tinchlik va xavfsizlik, qulay atrof-muhit va insoniyatning umumiy merosi kabi sohalar haqida bormoqda. Ularni amalga oshirish nafaqat alohida davlatlarning harakatlarini, balki xalqaro hamkorlikni ham talab etadi, chunki bu huquqlarning ko'pchiligi milliy chegaralardan tashqariga chiqadi va butun jahon hamjamiyati manfaatlariga daxldordir.

Karel Vashakning konsepsiyasi xalqaro tashkilotlar, jamoat harakatlari, ilmiy hamjamiyat vakillari, huquq himoyachilari va faollar tomonidan ancha xayrixohlik bilan kutib olindi.

Xayrixoh munosabatdan tashqari, raqamli makonda, genom tadqiqotlarida va boshqa innovatsion sohalarda **inson huquqlarining to'rtinchi avlodini**[3] asoslash hamda shakllantirishga doir urinishlar ham bo'ldi.

Bizni avvalo raqamli huquqlar fenomenining rivojlanishi qiziqtiradi va biz diqqatimizni faqat unga qaratamiz.

Axborot inqilobi nafaqat mavjud ishlab chiqarish usullari va turmush tarzining kengayishi va tarqalishiga, balki an'anaviy sanoat-tijorat jamiyatining yangi, «aqlli» jamiyat bilan global almashinuviga olib keldi, natijada inson huquqlarining to'rtinchi avlodi — «raqamli inson huquqlari» paydo bo'ldi.

Insonning raqamli huquqlarining o'ziga xos xususiyatlaridan biri aniq obyekt bo'lib, bu maxsus raqamli ko'rinishda taqdim etilgan axborot (ma'lumotlar) dir.

Insonning raqamli huquqlari raqamli texnologiyalar yordamida amalga oshiriladi (huquqni raqamli amalga oshirish) va faqat «raqamli odamlarga» (raqamli atributlarga ega bo'lgan odamlarga) tegishli bo'ladi.

Raqamli inson huquqlari sohasidagi majburiyatlar davlatlar va xususiy subyektlarning ijobiy va salbiy majburiyatlarini o'z ichiga oladi. Shunday qilib, insonning raqamli huquqlari huquqlarning yangi avlodi (yoki tizimi) bilan yaxshiroq bog'langan[4].

Raqamli huquqlar insonning internet makonidagi huquqlaridir, deb taxmin qilish mantiqan to'g'ri.

Shunday bo'lsa-da, bunday fikr yuritish uchun tegishli huquqiy asos ham yaratilishi kerak.

[3] https://bigenc.ru/c/prava-cheloveka-i-grazhdanina-chetviortogo-pokoleniia-9a58d6

[4] Gun Nan. 2024. «Aqlli jamiyatda inson huquqlarining to'rtinchi avlodi va asosiy konstitutsiyaviy huquqlarning o'zgarishi»

Inson huquqlari bo‘yicha kengash tomonidan qabul qilingan «Internetda inson huquqlarini himoya qilish va amalga oshirishni rag‘batlantirish»[5] rezolyutsiyasi quyidagilarni ta’kidlaydi:

Internetdagi ma’lumotlardan foydalanish butun dunyoda qulay va inklyuziv ta’lim olish uchun keng imkoniyatlarni yaratadi, shu bilan ta’lim olish huquqini rag‘batlantirishning muhim vositasi bo‘lib, raqamli savodxonlikni ta’minlash va raqamli tafovutni bartaraf etish zarurligini ta’kidlaydi, chunki bu ta’lim olish huquqini amalga oshirishga ta’sir qiladi;

Internetda inson huquqlarini, xususan, so‘z erkinligi huquqini amalga oshirish tobora katta qiziqish va ahamiyat kasb etayotgan masaladir;

Internetning global, ochiq va o‘zaro ishlash (interoperable) xususiyatini[6] saqlab qolish uchun davlatlar xavfsizlik muammolarini inson huquqlari sohasidagi xalqaro majburiyatlariga muvofiq hal qilishlari juda muhimdir;

Internetdan foydalanishni ta’minlash va kengaytirishda keng qamrovli inson huquqlari yondashuvini qo‘llash muhimligi

Onlayn muhitda shaxsiy hayot daxlsizligi o‘z fikrini erkin ifodalash va u yoki bu qarashlarga to‘siqsiz amal qilish huquqini hamda tinch yig‘ilishlar va uyushmalar erkinligi huquqini amalga oshirish uchun muhim ahamiyatga ega;

Barcha ayollar va qizlarning axborot-kommunikatsiya texnologiyalaridan foydalanish imkoniyatlarini kengaytirish orqali ularning huquq va imkoniyatlarini kengaytirish muhimligi.

Rezolyutsiya insonning oflayn muhitda ega bo‘lgan huquqlari onlayn muhitda ham himoya qilinishi kerakligini tasdiqlaydi.

Shu tariqa, Inson huquqlari bo‘yicha Kengash onlayn muhitda amalga oshirilishi mumkin bo‘lgan inson huquqlari (ya’ni raqamli huquqlarga aylanuvchi huquqlar) himoya qilinishi shartligini ta’kidlaydi.

E’tibor berish lozimki, gap siyosiy huquqlar (so‘z erkinligi va fikr bildirish erkinligi), iqtisodiy huquqlar (ta’lim olish huquqi), shuningdek kollektiv huquqlar (Internetning global tabiati) haqida bormoqda.

---

[5] https://www.refworld.org/ru/legal/resolution/unhrc/2016/ru/112398

[6] «Interoperabel» atamasi (inglizcha «interoperable») turli tizimlar, xizmatlar yoki texnologiyalarning birgalikda ishlash va bir-biri bilan muammosiz ma’lumot almashish qobiliyatini anglatadi.

Birlashgan Millatlar Tashkiloti Bosh Assambleyasi tomonidan qabul qilingan “Raqamli texnologiyalar kontekstida inson huquqlarini ragʻbatlantirish va himoya qilish”[7] rezolyutsiyasi avvalgi hujjatni quyidagilar bilan toʻldiradi:

Barcha inson huquqlari universal, boʻlinmas, oʻzaro bogʻliq, oʻzaro ta’sirchan va bir birini toʻldiruvchi ekanligi tasdiqlanadi hamda odamlar Internetdan tashqarida ega boʻlgan huquqlar Internetda ham xuddi shunday darajada himoya qilinishi lozimligi qayd etiladi.

Raqamli texnologiyalardan tobora keng foydalanish inson huquqlarining keng doirasiga ta’sir koʻrsatayotgani ta’kidlanadi. Raqamli texnologiyalar inson huquqlarini amalga oshirishga koʻmaklashishi mumkinligi tan olinadi, biroq tegishli kafolatlar boʻlmasa, ular inson huquqlarini himoya qilish va toʻliq amalga oshirish uchun jiddiy xavf tugʻdirishi mumkinligi qayd etiladi.

Shunday qilib, Birlashgan Millatlar Tashkiloti darajasida raqamli huquqlar, birinchidan, mavjud ekani, ikkinchidan, inson huquqlarining bevosita davomi ekani, uchinchidan esa, universal, boʻlinmas, oʻzaro bogʻliq, bir-biriga tobe va bir-birini toʻldiruvchi ekani tan olinadi.

Universalligi, boʻlinmasligi va huquqiy yondashuvga qaramay, raqamli huquqlarni Internetsiz hamda turli raqamli texnologiyalar, platformalar va xizmatlardan foydalanish imkoniyatisiz tasavvur qilib boʻlmaydi.

Shu munosabat bilan asosiy raqamli huquq Internetga kirish huquqi hisoblanadi.

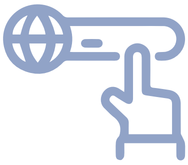
Insonning Internetga kirishi davlatlar, texnologik kompaniyalar va boshqa uchinchi shaxslar tomonidan yuzaga keltiriladigan turli xil chaqiriqlar, xavf xatarlar va tahdidlar bilan bogʻliq.

Misol uchun, raqamli uzilish, internetda fikr bildirishni cheklash, internetga kirishni bloklash, shaxsiy hayotning maxfiyligini buzish va boshqalar.

Bundan kelib chiqadiki, Internetdan foydalanish bilan bogʻliq «muammolar» raqamli platformalar va kengroq Internetdan foydalanish holatlarida koʻproq qoʻllaniladigan raqamli huquqlar roʻyxati koʻrinishidagi «javob»ni shakllantirdi.

[7] https://docs.un.org/ru/a/res/78/213

Raqamli huquqlar ro‘yxati

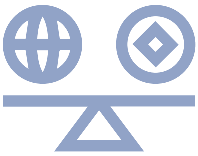


Internetdan foydalanish huquqi

Insonning so‘z erkinligini amalga oshirish, ta’lim olish, shuningdek zamonaviy ijtimoiy va iqtisodiy hayotda ishtirok etishi uchun zarur bo‘lgan global tarmoqqa ulanishning texnik va iqtisodiy imkoniyatiga ega bo‘lish huquqi.

Internetda fikr bildirish erkinligi

Insonning davlat chegaralaridan qat’i nazar, hokimiyat yoki korporatsiyalarning asossiz aralashuvisiz (senzurasiz) raqamli texnologiyalar va onlayn platformalar orqali har qanday turdagi axborot va g‘oyalarni izlash, olish va tarqatish huquqi.



Tarmoq neytralligi

Internetning ishlash tamoyili bo‘yicha, internet-provayderlar tijoriy yoki siyosiy maqsadlarda muayyan kontent, ilova yoki saytlarni bloklamasdan, sekinlatmasdan va ularga ustunlik bermasdan, barcha uzatilayotgan ma’lumotlarga bir xil yondashishi kerak.

Unutilish huquqi

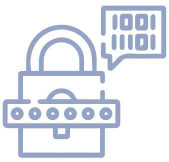
Shaxsga doir ma’lumotlar subyektiga muayyan asoslar mavjud bo‘lgan taqdirda, unga taalluqli ma’lumotlarni ommaviy manbalardan olib tashlashni yoki ularning tarqatilishini to‘xtatishni talab qilish imkonini beruvchi huquqiy mexanizm.

Kuzatuvdan himoya

Texnik vositalar orqali shaxsiy hayotga o‘zboshimchalik bilan aralashishning oldini olishga qaratilgan shaxsiy daxlsizlik huquqining o‘ziga xos kafolati.

Ma’lumotlar maxfiyligi va himoyasi

Insonning raqamli muhitda o‘zi haqidagi har qanday axborotni nazorat qilish (to‘plash, saqlash, qayta ishlash) huquqi, shuningdek, ushbu axborotni uchinchi shaxslar (korporatsiyalar yoki davlat) tomonidan ruxsatsiz foydalanish, sizib chiqish va suiiste’mol qilishdan himoya qilishni kafolatlovchi huquqiy va texnik choralar majmui.



Shifrlash huquqi

Inson o‘zining raqamli kommunikatsiyalari va saqlanayotgan ma’lumotlarining maxfiyligi, yaxlitligi va haqiqiyligini ta’minlash uchun kriptografik texnologiyalar va axborotni himoya qilish vositalaridan uchinchi shaxslarga (shu jumladan davlatga) deshifrlash kalitlarini taqdim etish majburiyatisiz moneliksiz foydalanish huquqi.

1.2. Raqamli huquqlar sohasidagi xalqaro va mintaqaviy standartlar

Jamiyatning raqamli transformatsiyasi inson huquqlarining klassik doktrinasini qayta koʻrib chiqish va ularni virtual makonga koʻchirish zaruratini keltirib chiqardi. Bu jarayonning asosida BMT darajasida mustahkamlangan tamoyil yotadi: inson huquqlari ham oflayn, ham onlayn muhitda bir xil darajada himoya qilinishi kerak.

2026-yil holatiga koʻra, raqamli sohani tartibga solish endi faqat milliy ixtiyoriylik masalasi emas. U BMTning universal paktlaridan tortib, kiberxavfsizlik va ma’lumotlarni himoya qilish sohasidagi maxsus konvensiyalargacha boʻlgan murakkab xalqaro majburiyatlar tizimi doirasida shakllanadi. Ushbu me’yoriy asos koʻp bosqichli tizim boʻlib, unda global standartlar Yevropa Kengashi, Yevropa Ittifoqi, YEXHT, SHHT va MDHning mintaqaviy vositalari bilan toʻldiriladi va aniqlashtiriladi, bu esa shaxsning raqamli maqomining yagona huquqiy konturini shakllantiradi.

Bu tizimda asosiy raqamli huquqlar kafolatlari markaziy oʻrinni egallaydi. Bularga Internetga kirish huquqi, algoritmik cheklovlarsiz fikr bildirish erkinligi va ma’lumotlar iqtisodiyoti sharoitida shaxsiy hayotni himoya qilish kiradi. Huquqlarning yoʻl qoʻyiladigan cheklovlarini belgilashda xalqaro normalar alohida ahamiyat kasb etadi. Aynan shu yerda «uch tarkibli test» qoʻllaniladi, u qonuniylik, qonuniy maqsad va mutanosiblik talablarini belgilaydi, davlat tomonidan tartibga solishning raqamli avtoritarizm vositasiga aylanishining oldini oladi.

Shu bilan birga, standartlarni ishlab chiqish davom etmoqda. Ular toʻrtinchi sanoat inqilobi bilan bogʻliq yangi muammolarga, jumladan, sun’iy intellekt etikasi, algoritmik kamsitish va transmilliy raqamli platformalarning mas’uliyati masalalariga moslashmoqda.

Shunday qilib, xalqaro-huquqiy asosni tahlil qilish global raqamlashtirish sharoitida davlat suvereniteti chegaralari va inson huquqlarini himoya qilish mexanizmlarini tushunish uchun zarurdir.

Shuni e’tiborga olish kerakki, quyida keltirilgan standartlar va yondashuvlar umumlashtirilgan holda bayon etilgan. Ularning vazifasi — oʻquvchiga huquqiy fikr mantiqi haqida tushuncha berish va shu bilan birga materialning tushunarli hamda oʻqishli boʻlishini saqlab qolishdir.

Xalqaro standartlar

Global tartibga solishning asosi BMT Inson huquqlari bo‘yicha kengashining (A/HRC/20/L.13, 2012-yil[8]) rezolyutsiyasida mustahkamlangan huquqlarning tengligi tamoyilidir: «Insonning oflayn muhitda ega bo‘lgan huquqlari onlayn muhitda ham himoya qilinishi kerak.»

Normativ baza asosini **Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt (FSHXP)**[9] tashkil etadi va u quyidagi moddalarni o‘z ichiga oladi:

19 modda (Fikr bildirish erkinligi hamda axborot olish huquqi)	Axborotni “davlat chegaralaridan qat’i nazar” va “har qanday usulda” (shu jumladan, Internet orqali) tarqatish huquqini kafolatlaydi. Bu haqda Inson huquqlari bo‘yicha qo‘mita o‘zining 34-sonli Umumiy tartibdagi mulohazalarida[10] to‘g‘ridan-to‘g‘ri ko‘rsatib o‘tgan.
17-modda (Shaxsiy hayot daxlsizligi)	Shaxsiy hayotga o‘zboshimchalik bilan aralashishdan himoya qiladi. BMTning Inson huquqlari bo‘yicha qo‘mitasi 16-sonli umumiy tartibdagi izohida[11] buni davlatlarning shaxsiy ma’lumotlarni kompyuterlar va ma’lumotlar banklarida to‘plash va saqlashni qonuniy tartibga solish majburiyati sifatida talqin qiladi.

BMTning Fuqarolik va siyosiy huquqlari to‘g‘risidagi konvensiyasi va Umumiy tartibdagi mulohazalardan tashqari Maxsus ma’ruzachilarning rolini alohida ta’kidlash lozim.

BMT maxsus ma’ruzachilari o‘zlarining mavzuga oid ma’ruzalari orqali fikr erkinligi va uni erkin ifodalash huquqini himoya qilish va rag‘batlantirish sohasidagi standartlarni ishlab chiqishda muhim rol o‘ynaydilar.

Maxsus ma’ruzachilarning pozitsiyasi amalda ‘yumshoq huquq’ (soft law) maqomiga ega bo‘lib, alohida davlatlar uchun majburiy qo‘llash yoki implementatsiya talab etilmasa-da, ular milliy huquqiy tizimlar uchun huquqiy tafakkur yo‘nalishi va uslubini belgilab beradi.

Shunday qilib, Maxsus ma’ruzachilar ishi tufayli xalqaro standartlar ayrim raqamli huquqlarni amalga oshirish va himoya qilish yondashuvini tartibga soluvchi o‘ta muhim elementlar bilan to‘ldirildi.

Masalan, Frank La Rue (A/HRC/17/27) ma’ruzasiga tayanib, xalqaro huquq internet-shatdaunlar (Internetga kirish huquqi) bo‘yicha qat’iy pozitsiyani ishlab chiqdi.

Ya’ni, Internet yoki mobil aloqadan foydalanishni to‘liq to‘xtatish har qanday sharoitda (hatto favqulodda holat rejimida ham) nomutanosib chora hisoblanadi, chunki u favqulodda xizmatlar ishini falajlaydi va favqulodda holat predmetiga bevosita jalb qilinmagan aholiga nomutanosib zarar yetkazadi.

---

[8] Internetda inson huquqlarini rag‘batlantirish, himoya qilish va amalga oshirish

[9] https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[10] https://hrlibrary.umn.edu/russian/gencomm/Rhrcom34.html

[11] https://hrlibrary.umn.edu/russian/gencomm/Rhrcom16.html

Asosiy ma’ruzalar

Fikr erkinligi va uni erkin ifodalash huquqini rag‘batlantirish va himoya qilish bo‘yicha maxsus ma’ruzachi Frank La Rue ma’ruzasi, 2011-yil, A/HRC/17/27[12]	Mazkur ma’ruzada barcha shaxslarning Internet orqali har qanday axborot va g‘oyalarni izlash, olish hamda tarqatish huquqi bilan bog‘liq asosiy yo‘nalishlar va muammolar ko‘rib chiqilgan. Maxsus ma’ruzachi Internetning o‘ziga xos va o‘zgaruvchan tabiati shaxslarga nafaqat o‘z fikri va uni erkin ifoda etish huquqini, balki boshqa bir qator inson huquqlarini ham amalga oshirish, shuningdek, umuman jamiyat taraqqiyotiga hissa qo‘shish imkonini berishini alohida ta’kidlaydi. Hisobotda davlatlar tomonidan internetdagi axborotga nisbatan senzuraning kuchaytirilishiga oid ayrim usullar bayon etilgan, xususan: • kontentni o‘zboshimchalik bilan bloklash yoki filtrlash; • qonuniy fikr bildirishni jinoyat deb hisoblash; • javobgarlikni vositachilar zimmasiga yuklash; • foydalanuvchilarni internetdan, jumladan, intellektual mulk huquqi to‘g‘risidagi qonunchilikni buzganlik asosida mahrum qilish; • kiberhujumlar hamda shaxsiy hayot daxlsizligi va ma’lumotlar himoyasi huquqini yetarli darajada ta’minlamaslik.
Fikr erkinligi va uni erkin ifoda etish huquqini rag‘batlantirish va himoya qilish masalalari bo‘yicha maxsus ma’ruzachi Devid Keyning 2015 yildagi ma’ruzasi, A/HRC/29/32[13]	Ushbu ma’ruzada Maxsus ma’ruzachi raqamli xabarlarni uzatishda shifrlash va anonimlik vositalaridan foydalanish masalasini ko‘rib chiqadi. Hisobotda shifrlash va anonimlik odamlarga raqamli asrda o‘z fikr erkinligi va uni erkin ifoda etish huquqlarini amalga oshirish imkonini berishi va shu sababli ular haqli ravishda ishonchli himoyaga ega bo‘lishi kerakligi ta’kidlangan. *Asosiy tezis:* Ma’ruzachi shifrlash va anonimlikni erkin fikr bildirish uchun zarur bo‘lgan **«maxfiylik hududi»** deb ta’rifladi. Uning ta’kidlashicha, «anonimlikni taqiqlash zo‘ravonlik va qatag‘on qurbonlariga sezilarli «sovutuvchi ta’sir» (chilling effect) ko‘rsatadi,» ularni tanib qolishdan qo‘rqib jim turishga majbur qiladi.
Dezinformatsiya va fikrlar erkinligi hamda ularni erkin ifoda etish huquqi Fikrlar erkinligi va ularni erkin ifoda etish huquqini rag‘batlantirish va himoya qilish masalalari bo‘yicha maxsus ma’ruzachi Iren Xonning 2021 yilgi ma’ruzasi, A/HRC/47/25[14]	Ushbu hisobotda Fikrlar erkinligi va ularni erkin ifoda etish huquqini rag‘batlantirish va himoya qilish masalalari bo‘yicha maxsus ma’ruzachi dezinformatsiya natijasida inson huquqlari, demokratik institutlar va rivojlanish jarayonlariga tahdid solayotgan xavf-xatarlarni ko‘rib chiqadi. Raqamli davrda dezinformatsiya keltirib chiqaradigan murakkabliklar va muammolarni e’tirof etgan holda, Maxsus ma’ruzachi davlatlar va kompaniyalar tomonidan ko‘rilayotgan choralar muammoli, yetarli emas va inson huquqlariga salbiy ta’sir ko‘rsatayotgan deb hisoblaydi. *Asosiy tezis:* Xan «soxta yangiliklar»ga qarshi kurash to‘g‘risidagi qonunlarni tanqid qilib, noaniq iboralar davlatlarga senzura uchun «siyosiy erkinlik» berishini ta’kidladi. U standartni tasdiqladi: yolg‘onga qarshi blokirovkalar bilan emas, balki ishonchli ma’lumotlar va raqamli savodxonlikni targ‘ib qilish orqali kurashish kerak.

[12] https://docs.un.org/ru/A/HRC/17/27
[13] https://docs.un.org/ru/a/hrc/29/32
[14] https://docs.un.org/ru/a/hrc/47/25

Keyinchalik, A/HRC/29/32 hisobotida Devid Key kriptografiya masalalarida (maxfiylik huquqi va shifrlash) davlatlarga qo‘yiladigan aniq talablarni bayon etdi:

1. Davlatlar platformalardan «bekdorlar» (maxsus xizmatlar uchun zaifliklar) joriy etishni talab qilmasligi kerak.

2. Davlatlar shifrlash kalitlarini saqlashni (ularni uchinchi tomonga topshirishni) talab qilmasligi kerak.

3. Shifrlashni cheklashga butun xizmat uchun ommaviy ravishda emas, balki faqat individual asosda (sud qarori bilan muayyan qurilma uchun) yo‘l qo‘yiladi.

Nihoyat, Devid Key (A/HRC/38/35) o‘z ma’ruzasida foydalanuvchi kontentini tartibga solish (Sun’iy intellekt va moderatsiya) bo‘yicha quyidagi ma’ruzani taqdim etdi:

Kompaniyalar moderatsiya paytida «protsessual adolat»ni ta’minlashlari kerak. Bu shuni anglatadiki, agar algoritm (SI) foydalanuvchi postini o‘chirib tashlasa, odam quyidagilarni olishi kerak:

- Aniq sabab ko‘rsatilgan xabarnoma;

- Qarorga bot emas, balki haqiqiy xodim oldida e’tiroz bildirish imkoniyati mavjud.

Raqamli huquqlarni cheklash: “uch bosqichli test”

Raqamli huquqlar mutlaq emas va ma’lum shartlar asosida cheklanishi mumkin.

Masalan, FSHXP (Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt) 19-moddasining 3-bandiga ko‘ra, cheklovlar faqat uchta shartga rioya qilinganda qonuniy hisoblanadi:

Qonuniylik:

Cheklov fuqaro o‘z harakatlarining oqibatlarini oldindan ko‘ra olishi uchun ochiq, tushunarli va yetarlicha aniq bayon etilgan qonunda nazarda tutilishi kerak. (Qonunda ta’rif berilmagan «ijtimoiy adovatni qo‘zg‘atish» kabi noaniq iboralar ushbu tamoyilni buzadi).

Qonuniy maqsad:

Milliy xavfsizlik, tartib, sog‘liq, axloq va boshqa shaxslarning huquqlarini himoya qilish.

Zarurat va mutanosiblik:

Eng kam aralashuv tamoyili: Davlat tanlangan chora (masalan, bloklash) maqsadga erishishning eng yengil usuli ekanligini isbotlashi shart. Agar bitta sharhni o‘chirish mumkin bo‘lsa, butun saytni bloklash mumkin emas.”

Isbotlash majburiyati: Foydalanuvchiga emas, davlatga yuklatiladi.

Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt (1984) qoidalariga oid cheklovlar va chekinishlarni sharhlash bo‘yicha Sirakuza tamoyillari (Sirakuza tamoyillari) muhim hujjat hisoblanadi.

Boshqa teng sharoitlarda FSHXP muayyan maqsadlar (masalan, jamoat tartibi) uchun ba’zi inson huquqlarini (masalan, so‘z yoki yig‘ilishlar erkinligi) cheklash imkonini beradi. Biroq, davlatlar ko‘pincha ushbu shartlarni suiiste’mol qiladilar.

Sirakuza tamoyillarining maqsadi «milliy xavfsizlik,» «jamoat tartibi» va «zarurlik» atamalarining ma’nosini aniq huquqiy ta’riflashdan iborat bo‘lib, ulardan qatag‘on qilish uchun bahona sifatida foydalanish imkoniyatini istisno qiladi.

Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt qoidalaridan cheklovlar va chekinishlarni talqin qilishning Sirakuza tamoyillari (bundan keyin matnda «Sirakuza tamoyillari» deb yuritiladi) quyidagilarni belgilaydi:

- «Inson huquqlarini amalga oshirishdagi hech qanday cheklov Paktga zid bo‘lmagan va cheklov joriy etilgan paytda amalda bo‘lgan umumiy qo‘llaniladigan milliy qonunga muvofiq joriy etilmaydi»[15]. (B.i.15 Sirakuza tamoyillari).
- Bundan tashqari, «Pakt bilan kafolatlangan huquqning cheklanishini asoslash majburiyati davlat zimmasida bo‘ladi» (A.12. Sirakuza tamoyillari).

> «Sirakuza tamoyillari (1984) inson huquqlarining yo‘l qo‘yilishi mumkin bo‘lgan cheklovlarini sharhlashning nufuzli manbai hisoblanadi. Ular milliy xavfsizlikka havola qilish hukumatni tanqiddan himoya qilish yoki huquqbuzarliklarni yashirish uchun qo‘llanilmasligi va har qanday cheklovlar qat’iy zarur va tahdidga mutanosib bo‘lishi kerakligini belgilaydi. Raqamli asrda bu tamoyillar ixtiyoriy blokirovka va yalpi kuzatuvga qarshi asosiy huquqiy dalil bo‘lib xizmat qiladi.»

Mintaqaviy standartlar

Ko‘pgina me’yorlar deklarativ xususiyatga ega bo‘lgan universal darajadan farqli o‘laroq, inson huquqlarining mintaqaviy tizimlari majburiy huquqiy rejimlarni yaratadi. Jahonda raqamli tartibga solishning bir nechta «raqobatlashuvchi» tizimlari shakllangan. Ushbu qo‘llanmada biz Yevropa raqamli tartibga solish tizimiga e’tibor qaratamiz.

Yevropa tizimi (Yevropa Kengashi va Yevropa Ittifoqini o‘z ichiga oladi)

Yevropa hozirda raqamli huquqlarni kodifikatsiya qilishda global yetakchi bo‘lib, Yevropa me’yorlari de-fakto global bo‘lib borayotgan «Bryussel effekti»[16] ni shakllantirmoqda.

Normativ-huquqiy baza markazida Inson huquqlari bo‘yicha Yevropa konvensiyasi (IHYK) turadi. Ushbu konvensiya Inson huquqlari bo‘yicha Yevropa sudi tomonidan mohiyatan raqamli voqelikka moslashtirilgan 10-modda (fikrni ifoda etish erkinligi) va 8-moddani (shaxsiy hayot daxlsizligi) o‘z ichiga oladi.

[15] Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt qoidalaridan cheklovlar va chekinishlarni talqin qilishning Sirakuza tamoyillari http://adilet.zan.kz/rus/docs/O850000001

[16] https://sg-sofia.com.ua/kogda-rech-zahodit-o-rinkah-evropa-vovse-ne-ugosayushaya-sila#:~:text=%C2%AB%D0%91%D1%80%D1%8E%D1%81%D1%81%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D0%B9%20%D1%8D%D1%84%D1%84%D0%B5%D0%BA%D1%82%C2%BB%20%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D0%BE%D0%BB%D0%B0%D0%B3%D0%B0%D0%B5%D1%82%2C%20%D1%87%D1%82%D0%BE,%D0%BD%D0%B5%D0%BC%D0%BD%D0%BE%D0%B3%D0%B8%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8%20%D0%B7%D0%B0%D1%85%D0%BE%D1%82%D0%B5%D0%BB%D0%B8%20%D0%B1%D1%8B%20%D0%BE%D1%82%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D1%8C%D1%81%D1%8F%D1%8F

Misollar	
Cengiz and Others v. Turkey (2015-y.)[17]	Da’vogarlar, xususan, ularni YouTube’ga kirishdan butunlay mahrum qilgan chora ustidan shikoyat qilishdi. Inson huquqlari bo‘yicha Yevropa sudi bitta video tufayli butun platformaga (bu holatda YouTube) kirishni bloklash Konvensiyani buzish deb hisoblaydigan standartni o‘rnatdi, chunki bu fuqarolarni ulkan hajmdagi qonuniy ma’lumotlardan (“video kontent ensiklopediyasi”) foydalanish imkoniyatidan mahrum qiladi.
Delfi AS v. Estoniya (2015-y.)[18]	Yevropa sudi o‘z amaliyotida birinchi marta ommaviy axborot vositasining foydalanuvchilar tomonidan uning veb-saytiga joylashtirilgan kontent uchun javobgarligi masalasini ko‘rib chiqdi. Yangiliklar portallari foydalanuvchilarning nafratni qo‘zg‘atuvchi sharhlari uchun, agar portal bundan tijoriy foyda ko‘rsa, javobgarlikni belgiladi.

Mazkur kontekstda 2022 yilda qabul qilingan **Digital Services Act (DSA)**[19] alohida e’tiborga loyiq.

Agar 108+ Konvensiyasi va GDPR (quyida keltirilgan) ma’lumotlaringizni himoya qilsa, Digital Services Act qonuni platformalarning mazmuni va javobgarligini tartibga soladi.

Ushbu qonunni qabul qilishdan maqsad — kontent (onlayn-kontent) va foydalanuvchilar xavfsizligini nazorat qilish orqali xavfsiz raqamli muhit yaratish hamda texnologiya gigantlarining ta’sirini cheklashdir.

Shuni ta’kidlash joizki, Digital Services Act ko‘pincha **Digital Markets Act (2022-y.)**[20] bilan birgalikda tilga olinadi. Uni qabul qilishdan maqsad qonun **«gatekeeperlar»**[21] deb ataydigan eng yirik texnologiya kompaniyalarining kuchini cheklashdir.

Ilgari Google yoki Apple ga qarshi antimonopoliya tekshiruvlari o‘n yillab davom etardi; Digital Markets Act esa yondashuvni o‘zgartirmoqda: endi qoidalar oldindan belgilangan va kompaniyalar ularga amal qilishga majbur, aks holda ulkan jarimalar xavfi mavjud.

№	Digital Services Act	Digital Markets Act
1	Qoidabuzarliklarga munosabat bildirish qoidalarini belgilaydi.	Muayyan amaliyotlar zarar yetkazmasidan oldin taqiqlanadi.
2	“Aldamchi interfeyslar” (interfeys manipulyatsiyasi) va bolalarga mo‘ljallangan reklamalarni taqiqlash.	“O‘zini afzal ko‘rish ” (o‘z xizmatlarini raqobatchilarnikidan ustun qo‘yib targ‘ib qilish) ni taqiqlash.
3	Shikoyatlarning shaffof mexanizmlarini joriy etish va bloklash sabablarini tushuntirish.	Messenjerlar va tizimlarning "interoperabelligi" (mosligi) ni ta’minlash.
4	Maxfiylikni himoya qilish. Din, salomatlik va jinsiy moyillik asosida targetingni taqiqlash	Iqtisodiy adolat. ‘Gatekeeper’larga hamkorlarining ma’lumotlaridan ularga qarshi raqobat qilish maqsadida foydalanish taqiqlanadi
5	Soxta ma’lumotlarga qarshi kurashish va alohida foydalanuvchi akkauntining bloklanishiga e’tiroz bildirishning huquqiy tartibi.	Oldindan o‘rnatilgan ilovalarni o‘chirib tashlashingiz va turli manbalardan dasturiy ta’minotni yuklab olishingiz mumkin.

[17] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159188%22]}
[18] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-155105%22]}
[19] https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html
[20] https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng
[21] gatekeepers — «darvozabonlar» yoki «kirish nazoratchilari»

6	Yevropa Ittifoqining har bir mamlakatidagi raqamli xizmatlar koordinatorlari + Yevrokomissiya (raqamli/texnologik gigantlar uchun).	Faqat Yevropa Komissiyasi (Bryusseldan bevosita nazorat).
7	Qoidabuzarliklar uchun jarima kompaniya yillik aylanmasining **6%** gacha miqdorda belgilanadi	Qoidabuzarliklar uchun jarima kompaniya yillik aylanmasining **10%** gacha miqdorda belgilanadi

Agar Digital Services Act va Digital Markets Act platformalarning mazmuni va mas'uliyatini tartibga solsa, 108+ Konvensiyasi, 95/46/EC Direktivasi va GDPR shaxsiy ma'lumotlarni himoya qiladi.

Shaxsiy ma'lumotlarni himoya qilish mavzusi bilan bog'liq xalqaro standartlar murakkab «evolyutsion» yo'lni bosib o'tmoqda va hozirgi vaqtda ma'lumotlar maxfiyligi tamoyillarining uchta «avlodi»ni ifodalaydi.

Ma'lumotlar maxfiyligi tamoyillarining birinchi «avlodi»ga Yevropa Kengashining Shaxsiy ma'lumotlarga avtomatlashtirilgan ishlov berishda jismoniy shaxslarni himoya qilish to'g'risidagi konvensiyasi yoki 1981-yilda qabul qilingan 108[22]-konvensiya kiradi.

Ma'lumotlar maxfiyligi tamoyillarining ikkinchi "avlod"iga ko'proq Yevropa Ittifoqining 95/46/EC[23] sonli "Shaxsiy ma'lumotlarga ishlov berishda jismoniy shaxslarni himoya qilish va bunday ma'lumotlarning erkin aylanishi to'g'risida"gi Direktivasini kiritish mumkin.

Nihoyat, ma'lumotlar maxfiyligi standartlarining uchinchi "avlodi"ga 2016-yilda qabul qilingan GDPR[24] hamda 108-sonli Konvensiya asosida 2018-yilda qabul qilingan 108+ Konvensiyasi kiradi.

Shuni ta'kidlash joizki, ma'lumotlar maxfiyligi tamoyillarining har bir "avlodi"da shartli ravishda (!) 10 tadan standartni ajratib ko'rsatish mumkin.

	Standartlarning birinchi «avlodi»
1	Ma'lumotlarni to'plash — cheklangan (me'yordan ortiq bo'lmagan), qonuniy (qonuniy maqsadlarda) va halol vositalar orqali amalga oshirilishi lozim.
2	Ma'lumotlar sifati — dolzarblik, aniqlik va yangilanganlik.
3	Yig'ish vaqti bo'yicha maqsadlarni belgilash.
4	Maqsad/huquqlar haqida xabarnoma.
5	Foydalanish — ko'rsatilgan yoki ular bilan mos keladigan maqsadlar doirasida cheklangan (jumladan, oshkor etish ham).
6	Oqilona ehtiyot choralari yordamida xavfsizlik.
7	Shaxsiy ma'lumotlardan foydalanish amaliyotiga nisbatan ochiqlik (nafaqat ma'lumotlar subyektlari uchun).
8	Kirish huquqi — shaxsning o'z ma'lumotlariga kirish bo'yicha individual huquqi.
9	Tuzatish — tuzatishga bo'lgan yakka tartibdagi huquq.
10	Hisobdorlik — identifikatsiya qilingan ma'lumotlar nazoratchisi.

[22] https://rm.coe.int/1680078c46

[23] https://www.tgl.net.ru/files/infosafety/%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B0%2095-46.pdf

[24] https://gdpr-info.eu/

Standartlarning ikkinchi «avlodi»	
1	Maqsadga erishish uchun zarur bo‘lgan minimal ma’lumotlarni yig‘ish (ma’lumotlarni minimallashtirish.
2	Maqsadga erishilgandan so‘ng ma’lumotlarni yo‘q qilish yoki egasizlantirish.
3	Muayyan toifadagi maxfiy ma’lumotlarni qo‘shimcha himoyalash.
4	Ma’lumotlarni qayta ishlashning qonuniy asoslari belgilandi.
5	Ayrim sezgir ishlov berish tizimlariga qo‘shimcha cheklovlar; “oldindan tekshirish” tartibi.
6	Avtomatlashtirilgan qaror qabul qilish cheklovlari (jumladan, qayta ishlash mantiqini bilish huquqi).
7	Qayta ishlashga jiddiy qonuniy sabablarga ko‘ra e’tiroz bildirish.
8	Qabul qiluvchi davlatdan "muvofiq" yoki muqobil kafolatlar talab qiladigan ma’lumotlarning cheklangan eksporti.
9	Ma’lumotlarni himoya qiluvchi mustaqil organning mavjudligi.
10	Ma’lumotlarning maxfiyligini ta’minlash uchun sudga murojaat qilish.
Standartlarning uchinchi "avlodi"	
1	Reja va sukut bo‘yicha ma’lumotlarni himoya qilish.
2	Namoyish etilgan hisobdorlik.
3	Ma’lumotlarni himoya qilish bo‘yicha mustaqil organga ma’lumotlar buzilishi/sizib chiqishi haqida xabar berish.
4	Ishlov beruvchilarning (shaxsiy ma’lumotlarning) bevosita javobgarligi.
5	Rozilik olishning yanada qat’iy talablari.
6	Ishlov berishning barcha jabhalarida mutanosiblik talablari.
7	Qarorlar qabul qilish va ma’muriy jazo choralarini, shu jumladan jarimalarni qo‘llash uchun ma’lumotlarni himoya qilish bo‘yicha mustaqil organning mavjudligi.
8	Biometrik va genetik ma’lumotlarni himoya qilishga qo‘yiladigan yuqori (qo‘shimcha) talablar.
9	Ma’lumotlarni o‘chirish bo‘yicha kuchaytirilgan huquq, jumladan “unutish huquqi”.
10	Ma’lumotlarni himoya qilish bo‘yicha mustaqil organ xalqaro shikoyatlarni ko‘rib chiqishda hamkorlik qilishi shart.

1.3. O‘zbekistonning raqamli huquqlar sohasidagi milliy qonunchiligi

O‘zbekiston Respublikasi Konstitutsiyasi xalqaro huquqning umume’tirof etilgan normalari ustunligini tan oladi. Konstitutsiyaning 15-moddasida xalqaro huquq prinsiplari va normalari O‘zbekiston huquq tizimining ajralmas qismi sifatida e’tirof etilib, inson huquq va erkinliklarini ta’minlash hamda ularni himoya qilish faqat davlatning ichki ishi doirasidan tashqariga chiqishi ko‘rsatib o‘tilgan. Xalqaro normalar va milliy qonunchilik bir-biriga zid bo‘lgan taqdirda xalqaro shartnoma qoidalari qo‘llaniladi. Konstitutsiyaviy tamoyillar so‘z erkinligi, axborot olish, Internet va raqamli xizmatlardan foydalanish sohasidagi xalqaro standartlarning ustunligini tan olish uchun asos yaratadi.

Fikr bildirish erkinligi va axborot olish huquqi O‘zbekiston Konstitutsiyasining 33-moddasida kafolatlangan bo‘lib, unda shunday deyiladi: «Har kim fikrlash, so‘z va e’tiqod erkinligi huquqiga ega. Har kim istalgan axborotni izlash, olish va tarqatish huquqiga ega,» shuningdek, davlatning axborotdan raqamli shaklda foydalanishni ta’minlash majburiyati: «Davlat Internet jahon axborot tarmog‘idan foydalanishni ta’minlash uchun shart-sharoitlar yaratadi.»

Konstitutsiyaning 34-moddasida belgilangan axborot olish huquqlarining hajmi davlat organlari va tashkilotlari, fuqarolarning o‘zini o‘zi boshqarish organlari hamda ularning mansabdor shaxslari har kimga uning huquqlari va qonuniy manfaatlariga daxldor hujjatlar, qarorlar va boshqa materiallar bilan tanishish imkoniyatini ta’minlash majburiyatini nazarda tutadi.

Boshqa konstitutsiyaviy norma jamoatchilik nazorati shaklida axborotdan foydalanish huquqi uchun asosni belgilaydi:

> Har kim qulay atrof-muhit, uning holati to‘g‘risida ishonchli axborot olish huquqiga ega. Davlat fuqarolarning ekologik huquqlarini ta’minlash va atrof-muhitga zararli ta’sir ko‘rsatishning oldini olish maqsadida shaharsozlik faoliyati sohasida jamoatchilik nazoratini amalga oshirish uchun shart-sharoitlar yaratadi. Shaharsozlik hujjatlari loyihalari qonunda belgilangan tartibda jamoatchilik muhokamasidan o‘tkaziladi.
>
> Konstitutsiyaning 31-moddasida shaxsiy hayot va shaxsga doir ma’lumotlarni himoya qilish huquqi belgilangan: «Har bir inson shaxsiy hayotining daxlsizligi, shaxsiy va oilaviy siri, o‘z sha’ni va qadr-qimmati himoya qilinishi huquqiga ega.
>
> Har kim yozishmalari, telefon orqali so‘zlashuvlari, pochta, elektron va boshqa xabarlari sir saqlanishi huquqiga ega. Bu huquqni cheklashga faqat qonunga muvofiq va sud qarori asosida yo‘l qo‘yiladi».

Har kim o‘z shaxsiy ma’lumotlarini himoya qilish, shuningdek noto‘g‘ri ma’lumotlarni tuzatishni, o‘zi to‘g‘risida qonunga xilof ravishda to‘plangan yoki bundan buyon huquqiy asosga ega bo‘lmagan ma’lumotlarni yo‘q qilishni talab qilish huquqiga ega.

Ushbu qoidalar ma’lumotlarni himoya qilish va shaxsiy hayot bilan bog‘liq mamlakat huquqiy bazasining eng muhim qismini tashkil etadi. Ushbu maqola axborotdan foydalanish huquqi va shaxsiy hayot hamda shaxsiy ma’lumotlarni himoya qilish zarurati o‘rtasidagi muvozanatning muhimligini ta’kidlaydi.

Axborot erkinligi to‘g‘risidagi qonunchilik.

Axborot erkinligi to‘g‘risidagi qonun hujjatlarining vazifalari axborot erkinligi prinsiplari va kafolatlariga rioya etilishini ta’minlashni; har kimning axborotni erkin va moneliksiz izlash, olish, o‘rganish, tarqatish, undan foydalanish va uni saqlash huquqini amalga oshirishni; axborot muhofazasini hamda shaxs, jamiyat va davlatning axborot xavfsizligini ta’minlashni o‘z ichiga oladi. Axborot olish huquqi davlat hokimiyati va boshqaruvi organlari hamda ular mansabdor shaxslarining qabul qilinayotgan qarorlar uchun mas’uliyatini oshirishni ta’minlashga qaratilgan. Har bir shaxs davlat organlarining tashkil etilishi va faoliyat ko‘rsatishi hamda mazkur shaxsga yoki shaxslar guruhiga taalluqli hujjatlarni qabul qilish jarayonlari to‘g‘risidagi axborotdan foydalanish huquqiga ega. Biroq amaldagi qonunchilik bazasida axborotga bo‘lgan to‘g‘ridan-to‘g‘ri huquq nazarda tutilmagan, aksincha, axborotni izlash huquqi nazarda tutilgan.

Axborot olish huquqi asosan «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni, «Axborot olish kafolatlari va erkinligi to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni, «Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni, «Ommaviy axborot vositalari to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni, «Rasmiy statistika to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni, «Korrupsiyaga qarshi kurashish to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni, «Huquqiy axborotni tarqatish va undan foydalanish to‘g‘risida»gi O‘zbekiston Respublikasi Qonuni kabi birlamchi qonunchilik hujjatlari bilan ta’minlanadi.

Qonunchilik ham axborotga, ham hujjatlar yoki yozuvlarga kirishning umumiy huquqini nazarda tutadi. Huquqiy talablarning davlat hokimiyatining barcha tarmoqlariga qo‘llanilishiga nisbatan qonun axborot egasiga qat’iy tartibda axborotga egalik qiluvchi, undan foydalanuvchi va uni tasarruf etuvchi hamda bunga bo‘lgan huquqlari qonun hujjatlarida yoki axborot egasi tomonidan belgilangan huquqlar bilan cheklanmagan yuridik yoki jismoniy shaxs sifatida keng ta’rif beradi.

Shu bilan birga, qonunchilikda davlat nazorati ostidagi korxonalar, jamg‘armalar, davlat funksiyalari berilgan tashkilotlarning o‘z faoliyati to‘g‘risidagi axborotdan foydalanishini ta’minlash bo‘yicha to‘g‘ridan-to‘g‘ri majburiyati mavjud emas. Vaholanki, xalqaro standartlar barcha davlat hokimiyati organlariga, shuningdek, davlat tomonidan moliyalashtiriladigan, davlat nazorati ostida bo‘lgan yoki davlat funksiyalarini bajaruvchi xususiy tashkilotlarga taalluqli bo‘lishi kerak bo‘lgan axborotdan foydalanish foydasiga prezumpsiya o‘rnatishni talab qiladi.

Konstitutsiyaning 33-moddasiga muvofiq «Axborotni izlash, olish va tarqatish huquqini cheklashga faqat qonunga muvofiq va faqat konstitutsiyaviy tuzumni, aholi sog‘lig‘ini, jamoat axloqini, boshqa shaxslarning huquq va erkinliklarini, jamoat xavfsizligini va jamoat tartibini himoya qilish, shuningdek davlat siri yoki qonun bilan qo‘riqlanadigan boshqa sir oshkor etilishining oldini olish uchun zarur bo‘lgan darajada yo‘l qo‘yiladi.»

O‘zbekiston Respublikasi “Davlat organlari faoliyatining ochiqligi to‘g‘risida”gi Qonunining 6 moddasiga muvofiq, davlat hokimiyati va boshqaruvi organlari faoliyati to‘g‘risidagi axborotga kirish cheklanadi, agar ushbu axborot qonunda belgilangan tartibda davlat siri yoki qonun bilan muhofaza qilinadigan boshqa sirlar toifasiga kiritilgan bo‘lsa. Umumiy qoida sifatida davlat organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari, korxonalar, muassasalar, tashkilotlar va mansabdor shaxslar davlat siri yoki qonun bilan muhofaza qilinadigan boshqa sirlarni o‘z ichiga olgan axborotni taqdim etishga haqli emas.

Quyidagi ma’lumotlar cheklanishi mumkin emas:

Fuqarolarning huquq va erkinliklari, ularni amalga oshirish tartibi to‘g‘risidagi, shuningdek davlat hokimiyati va boshqaruvi organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining huquqiy maqomini belgilovchi qonun hujjatlari;

Ekologik, meteorologik, demografik, sanitariya-epidemiologik, favqulodda vaziyatlar to‘g‘risidagi ma’lumotlar hamda aholi, aholi punktlari, ishlab chiqarish obyektlari va kommunikatsiyalarning xavfsizligini ta’minlash uchun zarur bo‘lgan boshqa ma’lumotlar;

Axborot-kutubxona muassasalarining ochiq fondlarida, arxivlarda, idoraviy arxivlarda, O‘zbekiston Respublikasi hududida faoliyat ko‘rsatayotgan yuridik shaxslarning axborot tizimlarida mavjud bo‘lgan axborot.

Qonunchilik davlat hokimiyati va boshqaruvi organlariga maxfiy ma’lumotlar ro‘yxatini buyruqlar yoki ichki hujjatlar shaklida belgilashga ruxsat beradi, xalqaro standartlarga ko‘ra esa har qanday cheklovlar qonunda nazarda tutilgan bo‘lishi va uch komponentli testga mos kelishi kerak. Biroq, xalqaro standartlarga mos kelish uchun istisnolar konstitutsiyaviy majburiyatlarga mos kelishi va axborotdan foydalanish huquqi hajmini cheklamaslik uchun uch komponentli testni o‘z ichiga olishi kerak.

Axborot olish erkinligining xalqaro standartlariga ko‘ra, istisnolar davlatning konstitutsiyaviy majburiyatlariga muvofiq bo‘lishi va axborot olish huquqining asossiz cheklanishiga yo‘l qo‘ymaslik uchun uch komponentli testni o‘z ichiga olishi kerak. Davlat sirlari to‘g‘risidagi qonunchilikka muvofiq quyidagi ma’lumotlar maxfiylashtirilmaydi:

- favqulodda vaziyatlar hamda fuqarolarning hayotiga, sog‘lig‘iga va xavfsizligiga tahdid soluvchi boshqa hollar va ularning oqibatlari, shuningdek, tabiiy ofatlar, ularning rasmiy prognozlari va oqibatlari to‘g‘risidagi ma’lumotlar;

- ekologiya, sog‘liqni saqlash, sanitariya, demografiya, ta’lim, madaniyat, tibbiy xizmat, ijtimoiy ta’minot va qishloq xo‘jaligi holati to‘g‘risidagi ma’lumotlar;

- jinoyatchilik holati to‘g‘risidagi ma’lumotlar;

- makroiqtisodiy ko‘rsatkichlar, O‘zbekiston Respublikasi Davlat byudjeti parametrlari, shuningdek, O‘zbekiston Respublikasining ijtimoiy-iqtisodiy rivojlanishi to‘g‘risidagi yig‘ma statistik ma’lumotlar;

- inson huquqlari va erkinliklarining buzilishiga oid ma’lumotlar;

- davlat organlari, boshqa tashkilotlar va ularning mansabdor shaxslari tomonidan qonunchilikning buzilishlari haqidagi ma’lumotlar;

- foydalanilishi, tarqatilishi va taqdim etilishi qonun bilan cheklanmagan boshqa ma’lumotlar.

Axborotdan foydalanish to‘g‘risidagi qonunlarda axborotni oshkor qilish foydasiga istisnolardan foydalanish imkonini beruvchi jamoat manfaatlarining ustuvorligi to‘g‘risidagi qoidalar mavjud emas. Xalqaro maksimal oshkor qilish standartlariga javob berish uchun asosiy ijtimoiy ahamiyatga ega bo‘lgan ma’lumotlar proaktiv yoki avtomatik ravishda e’lon qilinishi kerak.

Axborot so‘rovi

O‘zbekiston Respublikasi qonunchiligi davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligini kafolatlaydi. Fuqarolar va yuridik shaxslar davlat hokimiyati va boshqaruvi organlarining faoliyati to‘g‘risida axborot olish uchun bevosita yoxud o‘z vakillari orqali so‘rov bilan murojaat qilishga haqli.

Davlat hokimiyati va boshqaruvi organlarining faoliyati to‘g‘risida axborot olishga doir so‘rov (bundan buyon matnda so‘rov deb yuritiladi) — axborotdan foydalanuvchining davlat hokimiyati va boshqaruvi organlariga va (yoki) ularning mansabdor shaxslariga ushbu organlarning faoliyati to‘g‘risida axborot taqdim etish haqida yuboriladigan og‘zaki yoki yozma shakldagi (shu jumladan elektron hujjat shaklidagi) talabi. («Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida»gi O‘zbekiston Respublikasi Qonunining 18-moddasi.)

Axborot olish so‘rovi fuqarolar va yuridik shaxslarning murojaatlaridan tubdan farq qiladi.

Mezon	Fuqarolar/yuridik shaxslarning murojaati	Ma'lumot olish uchun so‘rov
Maqsad	Huquqlarni amalga oshirishga ko‘maklashish, buzilgan huquqlarni tiklash, qonuniy manfaatlarni himoya qilish, ishni yaxshilash bo‘yicha takliflar.	Davlat organi faoliyati to‘g‘risida aniq ma’lumotlar (hokimiyat va boshqaruv organlari faoliyati to‘g‘risida axborot) olish.
Mazmun	**Ariza** — yordam so‘rash. **Shikoyat** — huquqlarni tiklash talabi. **Taklif** — faoliyatni takomillashtirish bo‘yicha tavsiyalar.	Ma’lumot taqdim etish talabi. So‘rov og‘zaki/yozma/elektron shaklda bo‘lishi mumkin.
Konstitutsiyaviy asos	Ariza, taklif va shikoyatlar bilan murojaat qilish huquqi.	Axborotni izlash, olish va tarqatish huquqi. Shuningdek, huquq va manfaatlarga daxldor hujjatlar bilan tanishish huquqi.
Huquqiy asos	O‘zbekiston Respublikasining "Jismoniy va yuridik shaxslarning murojaatlari to‘g‘risida"gi Qonuni (murojaat turlari, talablari, muddatlari).	O‘zbekiston Respublikasining “Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida”gi Qonuni (so‘rov tushunchasi, muddatlar). O‘zbekiston Respublikasining “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonuni (so‘rov huquqi, shakllari va muddatlari). Davlat hokimiyati va boshqaruvi organlari faoliyati to‘g‘risidagi axborotni taqdim etish bo‘yicha so‘rovlarni qabul qilish, ro‘yxatdan o‘tkazish va ko‘rib chiqish tartibi to‘g‘risidagi Yo‘riqnoma (ro‘yxat raqami: 2769).
Kim murojaat qiladi	Jismoniy va yuridik shaxslar.	Har qanday axborot foydalanuvchisi (jismoniy yoki yuridik shaxs).
Til	Murojaatlar davlat tilida, shuningdek boshqa tillarda ham berilishi mumkin.	So‘rovlar davlat tilida, shuningdek boshqa tillarda ham berilishi mumkin.

Qayerga yuboriladi	Davlat organlari/davlat muassasalariga (va ba'zi hollarda qonun vakolatiga ko'ra boshqa tashkilotlarga).	So'rov masalalari bo'yicha ma'lumot berish vakolatiga ega bo'lgan hokimiyat organiga/ mansabdor shaxsga.
Ko'rib chiqish muddati	Ariza/shikoyat — **15 kungacha**. Qo'shimcha o'rganish talab etilganda — **1 oygacha**; taklif — **1 oygacha**.	Foydalanuvchi so'rovi — ro'yxatdan o'tgan kundan boshlab **15 kungacha** OAV so'rovi — **7 kungacha**.
Agar qabul qiluvchi vakolatli bo'lmasa	Vakolatiga ko'ra boshqa organga yuborish va murojaatchini xabardor qilish (qonunda belgilangan muddatlar doirasida).	Ro'yxatdan o'tkazilgan kundan e'tiboran **3 ish kuni** ichida vakolatli organga yuborish va foydalanuvchini xabardor qilish.
Ko'rib chiqish natijalari	Решение по существу обращения и ответ о результатах и принятых мерах.	Ma'lumot taqdim etish; yoki asosli rad etish; yoki allaqachon e'lon qilingan manbalarga havola berish (rasmiy nashrlar/sayt). Rad etilgan taqdirda asoslantirilgan javob yuboriladi.
Identifikatsiya talablari	Murojaatning F.I.O./manzili (jismoniy shaxs uchun) yoki nomi/ manzili (yuridik shaxs uchun) va mohiyati ko'rsatilishi shart.	So'rovning F.I.O/manzili (jismoniy shaxs uchun) yoki nomi/manzili (yuridik shaxs uchun) va mohiyati ko'rsatilishi shart.
Ma'nosi	Huquq va manfaatlarni harakat va qarorlar orqali himoya qilish.	Huquq va manfaatlarni harakat va qarorlar orqali himoya qilish.

Davlat hokimiyati va boshqaruvi organlarining faoliyati to'g'risidagi axborotdan foydalanish mazkur axborot qonunda belgilangan tartibda davlat sirlarini yoki qonun bilan qo'riqlanadigan boshqa sirni tashkil etuvchi ma'lumotlar toifasiga kiritilgan taqdirda cheklanadi.

Ma'lumot olish uchun so'rov yuborish algoritmi

1-bosqich. Vakolatli davlat organini aniqlang

So'ralgan ma'lumotlarga vakolati bo'yicha ega bo'lgan organni aniqlang. So'rov so'rovga doir masalalar bo'yicha axborot berish vakolatiga ega bo'lgan organ yoki mansabdor shaxsga yuborilishi kerak.

2-bosqich. Organ vakolatlarini aniqlashtiring

Organning rasmiy veb-sayti va uning vazifa va funksiyalari to'g'risidagi nizomni tekshiring. Bu so'rovni qayta yo'naltirish va vaqtni yo'qotish xavfini kamaytiradi.

3-bosqich.
So‘rovni to‘g‘ri tuzing

So‘rov — axborotdan foydalanuvchining organ faoliyati to‘g‘risidagi ma’lumotlarni taqdim etish haqidagi talabidir. So‘rov og‘zaki, yozma yoki elektron hujjat shaklida bo‘lishi mumkin. Bir yoki bir nechta aniq savollarni shakllantiring.Agar hujjatni so‘rayotgan bo‘lsangiz, agar ular ma’lum bo‘lsa, nomi va rekvizitlarini ko‘rsating.

4-bosqich.
So‘rovning majburiy ma’lumotlarini tekshiring

Jismoniy shaxs uchun F.I.O., yashash joyi haqidagi ma’lumotlarni va so‘rovning mohiyatini ko‘rsating. Yuridik shaxs uchun to‘liq firma nomi, pochta manzili va so‘rovning mohiyatini ko‘rsating. Yozma so‘rov axborotdan foydalanuvchi tomonidan imzolanishi kerak. Identifikatsiya uchun ma’lumotlarsiz so‘rov anonim hisoblanadi va ko‘rib chiqilmaydi.

5-bosqich.
Yo‘nalish kanalini tanlang

Qonun so‘rovning og‘zaki, yozma shakliga va elektron hujjatga to‘g‘ridan to‘g‘ri yo‘l qo‘yadi. Elektron murojaatlar amalda organning rasmiy veb-sayti, YIDXP (my.gov.uz) orqali rasmiy elektron pochtasi yoki.

6-bosqich.
So‘rov yuborilganini tasdiqlang

So‘rovdan nusxa oling. Ro‘yxatdan o‘tish belgisini, kiruvchi raqamni yoki pochta kvitansiyasini saqlang.

7-qadam.
Muddatlar va yozishmalarni nazorat qiling

Axborot so‘rovini ko‘rib chiqish muddati **so‘rov ro‘yxatdan o‘tkazilgan kundan boshlab** hisoblanadi. Agar belgilangan muddat tugagunga qadar axborotga javob taqdim etilmasa, bu **amaldagi qonunchilikning buzilishi** hisoblanadi. Axborot berishni qonunga xilof ravishda rad etish ustidan fuqarolar va yuridik shaxslar prokuratura organlariga yoki ma’muriy sudga shikoyat qilishlari mumkin.

Huquqiy axborotdan foydalanish

Huquqiy axborotning asosiy manbasi O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi (Lex.uz) bo‘lib, unda amaldagi qonunchilik, shu jumladan qonunlar, prezident farmonlari va qarorlari, hukumat hujjatlari, mahalliy davlat hokimiyati organlarining qarorlari va boshqa normativ-huquqiy hujjatlar taqdim etilgan.

Qonun loyihalarining umumxalq muhokamasi **regulation.gov** portalida qonunlar, farmonlar, qarorlar, buyruqlar va davlat hokimiyati markaziy hamda mahalliy organlarining qarorlari loyihalari e’lon qilinadi.

O‘zbekiston Respublikasining «Huquqiy axborotni tarqatish to‘g‘risida»gi Qonuni (O‘RQ-461-son) har bir fuqaroning ishonchli, o‘z vaqtida va to‘liq huquqiy axborot olish huquqini mustahkamlaydi. Bunga qonunlar, qonunosti hujjatlari, xalqaro shartnomalar, shuningdek, mahalliy o‘zini o‘zi boshqarish organlarining hujjatlari to‘g‘risidagi ma’lumotlar kiradi.

Hujjat huquqiy axborotni taqdim etishda amal qilinishi lozim bo‘lgan asosiy tamoyillarni belgilaydi:

- Ochiqlik va hammaboplik.
- To‘liqlik va ishonchlilikni ta’minlash.
- Axborot to‘plash va tarqatishda shaxsiy hayotga aralashishga yo‘l qo‘yilmasligi.
- Fuqarolarning axborot olishdagi teng huquqliligi.

Davlat organlari rasmiy veb-saytlar va boshqa rasmiy manbalar orqali huquqiy axborotdan bepul foydalanish imkoniyatini ta’minlashi shart. Normativ-huquqiy hujjatlar matnlarining elektron nusxalari ularni qabul qilgan organlarning rasmiy veb-saytlarida belgilangan tartibda majburiy joylashtirilishi lozim. Shuningdek, qonun ularning aholini qonunchilikdagi o‘zgarishlar haqida xabardor qilish hamda fuqarolarga huquqiy masalalar yuzasidan maslahat berish majburiyatini ham belgilaydi. Huquqiy axborotni tarqatish shakllari ommaviy axborot vositalarida rasmiy nashr etish, davlat axborot resurslariga joylashtirish va davlat muassasalarida bosma shaklda taqdim etishni o‘z ichiga oladi.

Har bir davlat organida axborot xizmati tashkil etilgan bo‘lib, uning vazifalariga davlat organi faoliyatini tartibga soluvchi huquqiy axborotni taqdim etish kiradi. Davlat organlari va tashkilotlari jismoniy hamda yuridik shaxslarning so‘roviga binoan o‘z faoliyatiga oid masalalar bo‘yicha normativ-huquqiy hujjatlarni qo‘llash tartibini tushuntirib beradi. Davlat organlari va tashkilotlari tomonidan tayyorlangan normativ-huquqiy hujjatlarni qo‘llash tartibi to‘g‘risidagi tushuntirishlar ushbu organlar va tashkilotlarning tarkibiy hamda hududiy bo‘linmalari uchun majburiy kuchga ega hisoblanadi.

Qonun hujjatlarini huquqiy targ‘ib qilish quyidagi usullar bilan amalga oshiriladi:

- Konferensiyalar, uchrashuvlar, seminarlar, davra suhbatlari va suhbatlar o‘tkazish;
- Ommaviy axborot vositalari, shu jumladan teleradioeshittirishlarni tashkil etish, bosma va elektron ommaviy axborot vositalarida maqolalar va axborot-huquqiy materiallarni joylashtirish orqali;
- Izohlar, broshyuralar, plakatlar, bukletlar va flayerlarni tarqatish;

- Ijtimoiy reklama (videoroliklar, infografikalar va boshqalar) va qonunchilikda taqiqlanmagan boshqa targ‘ibot turlari orqali amalga oshiriladi.

Jismoniy va yuridik shaxslar o‘z faoliyatiga taalluqli huquqiy axborotni taqdim etish to‘g‘risida davlat organlari va tashkilotlariga so‘rov bilan murojaat qilish huquqiga ega. Huquqiy axborot taqdim etish to‘g‘risidagi so‘rov u kelib tushgan kundan e’tiboran **o‘n besh kundan** ortiq bo‘lmagan muddatda ko‘rib chiqilishi lozim.

Huquqiy axborotni elektron shaklda taqdim etish bepul amalga oshiriladi. Huquqiy axborotni qog‘ozda taqdim etganlik uchun taraflarning kelishuviga binoan haq olinishi mumkin. Huquqiy axborot taqdim etish to‘g‘risidagi so‘rovni qanoatlantirishni rad etish asoslantirilgan bo‘lishi kerak. Fuqarolar, agar mansabdor shaxslarning noqonuniy harakatlari yoki harakatsizligi ularning huquqiy axborotdan foydalanish huquqini buzayotgan bo‘lsa, shikoyat qilish huquqiga egadirlar. Qonunda huquqiy axborot olishga to‘sqinlik qilganlik uchun javobgarlik ham belgilangan.

2-bo‘lim
Fuqarolik faollari va NNTlar uchun raqamli huquqlar

2.1. NNTlar uchun raqamli muhitdagi kommunikatsiyalar

O‘zbekistondagi nodavlat notijorat tashkilotlari uchun raqamli muhitda muloqot qilish, bir tomondan, o‘z maqsadli auditoriyasini kengaytirish, jamiyat uchun zarur bo‘lgan ijtimoiy ahamiyatga ega loyihalar va tashabbuslarni amalga oshirish uchun potentsial homiylar va xayriyachilarni jalb qilish imkoniyati bo‘lsa, boshqa tomondan, kontent, sharhlar, shaxsiy ma’lumotlarni tarqatish va raqamli muhitga xos bo‘lgan boshqa qonunbuzarliklar uchun javobgarlikning huquqiy xavf-xatarlarini keltirib chiqaradi.

Muloqot tashqi kanallar — matbuot xizmatlari, ommaviy axborot vositalari orqali ham, ichki kanallar — shaxsiy veb-saytlar, ijtimoiy tarmoqlardagi hamjamiyatlar, telegram-kanallar, media loyihalar, masalan, podkastlar kanali yoki YouTube’dagi videolar orqali ham amalga oshirilishi mumkin.

Saytlar, ijtimoiy tarmoqlar va onlayn platformalar, messenjerlarda NNT kontenti bir necha darajada nazorat qilinadi: onlayn platformalarning o‘zlari tomonidan moderatsiya qilish, auditoriya shikoyatlari va vakolatli tuzilmalar reaksiyasi. Shu sababli, aloqalarning barqarorligi nafaqat matn sifatiga, balki jarayonga ham bog‘liq: aloqa uchun kim mas’ul, tashkilot inqirozlarga qanday munosabat bildiradi, izohlar qanday nazorat qilinadi, kontentni e’lon qilishdan oldin tekshirish amalga oshiriladimi? Ushbu bob loyiha va tashabbuslarning kommunikatsiya va axborot ta’minoti uchun mas’ul bo‘lgan NNT vakillari uchun foydali bo‘ladi.

2.1.1. NNTlarning samarali kommunikatsiya strategiyasi

Mediakontentni yaratish va tarqatishning ulkan imkoniyatlari hamda soddaligiga qaramay, OAV asosiy kommunikatsiya kanallaridan biri bo‘lib qolmoqda. Nega? Buning uchta sababi bor.

Birinchidan, OAV NNT kontentini auditoriya va qamrov bilan ta’minlaydi. OAV tahririyatlari o‘z auditoriyasining ishonchi va kengayishi haqida allaqachon g‘amxo‘rlik qilgan. Qamrovni kengaytirish strategiyalari doimiy ravishda ishlaydi — kontentni yaxshilash, ijtimoiy tarmoqlar va auditoriyani jalb qilish.

Ikkinchidan, kampaniyalarni bepul targ‘ib qilish. Aksariyat OAV NNT loyihalari va kampaniyalarini bepul targ‘ib qilishga, ekspert sifatida fuqarolik jamiyati vakillarini jalb qilishga tayyor.

Uchinchidan, ommaviy axborot vositalari NNTlarga xayriya tadbirlarida beqiyos yordam ko‘rsatmoqda. Turli xil mablag‘ yig‘ish va xayriya aksiyalari OAV yordamida o‘z ta’sirini sezilarli darajada kuchaytirmoqda. Auditoriyaning ommaviy axborot vositalariga ishonchi ijtimoiy tarmoqlarga qaraganda kuchliroq.

Shuning uchun raqamli muhitda NNTning samarali kommunikatsiya strategiyasi bir necha bosqichlardan iborat bo‘lishi kerak, har bir bosqichni amalga oshirish butun strategiyaning ajoyib natijasini ta’minlaydi.

1-bosqich
Tartibsiz va nomuntazam kommunikatsiyalar o‘rniga media-rejani ishlab chiqish va amalga oshirish.

Axborot maydonidagi rolingiz? Asosiy sanalar, ma’ruzachilar, asosiy xabarlar. Asosiy formatlar (press-reliz, ijtimoiy tarmoqlardagi post, podkast, video intervyu va boshqalar) va tarqatish kanallari.

2-bosqich
Maqsadli auditoriyani aniqlash

Auditoriyangiz qanday axborot kanallarini iste’mol qiladi? Faqat xabarlaringizni auditoriyangizga maqsadli yetkazadigan ommaviy axborot vositalari bilan ishlang.

3-bosqich
Tajribangizni axborot yordamiga aylantiring

OAV ko‘pincha NNT vakillaridan axborot kun tartibidagi barcha masalalar bo‘yicha izoh so‘raydi. Loyiha va kampaniyalaringizni qo‘llab-quvvatlash sharti bilan rozilik bildiring.

4-bosqich
Aloqa uchun mas’ul xodimni (tashkilotingiz vakilini) belgilang.

Media-rejaning amalga oshirilishi uchun mas’ul bo‘lgan mas’ul xodim nazorat va monitoringni amalga oshiradi. Alohida xodim emas, lekin mas’uliyatli va media muhitida yaxshi aloqalarga ega.

5-bosqich
Inqirozli vaziyatlarda nima qilish kerak? Inqirozga qarshi harakatlar rejasi.

Ommaviy axborot vositalari va ijtimoiy tarmoqlardagi asosiy xabarlar va harakatlar. Bu davrdagi sharhlar va auditoriya ishtirokiga ehtiyot bo‘ling. Maqsadli guruhingiz uchun aniq va ravshan xabarlar tayyorlanishi kerak.

6-bosqich
Nashrlar monitoringi.

Media tahririyatlari sizga post va hikoyalar havolalarini taqdim etmaydi, lekin tomoshalar va qamrov statistikasini taqdim etishi mumkin. Nashrlar monitoringi siz tomoningizdan ta’minlanishi kerak.

2.1.2. NNTning o‘z media loyihalari va OAV bilan aloqalar

Ko‘pgina NNTlar o‘z loyihalari va maqsadli guruhlari haqidagi ma’lumotlarni OAVda e’lon qilish imkoniyatlari yetishmasligini yoki umuman yo‘qligini his qilib, o‘z media-loyihalarini yaratish haqida o‘ylaydilar (va ko‘pincha amalga ham oshiradilar).

O‘z media-loyangizni yaratish va OAV bilan aloqa o‘rnatish o‘rtasidagi tanlov — bu resurslar va mas’uliyat masalasidir. Shaxsiy media-loyiha mavzular, sur’at va materialni uzatish sifati ustidan nazoratni ta’minlaydi, “o‘z maromida” ishlashga, tashkilotga nisbatan ishonchni shakllantirishga hamda uzoq muddatli kampaniyalarni qo‘llab-quvvatlashga yordam beradi. Lekin uning kamchiliklari ham bor: doimiy moliyalashtirish izlash, vaqt va inson resurslari sarfi, xodimlarni o‘qitish zarurati, sifatli audiovizual kontent yaratish uchun texnikaga ehtiyoj, qo‘shimcha huquqiy javobgarlik.

Quyidagi jadvalda NNTlar uchun ikki yondashuvning — OAV bilan aloqa o‘rnatish yoki o‘z media-loyasini ishga tushirishning afzalliklari va kamchiliklari bilan tanishishingiz mumkin.

	Afzalliklari	Kamchiliklari
OAV bilan kommunikatsiya	Keng auditoriyaga tez chiqish va tahririyatga bo‘lgan ishonch. Tahririyat tomonidan mavzuni tekshirish va to‘g‘ri formatni tanlash. Kontent ishlab chiqarish va targ‘ibot uchun kamroq xarajat.	Tahririyat kun tartibi va formatiga qaramlik. Sarlavha, vizuallar va taqdimot ustidan cheklangan nazorat. Kechikishlar, qisqartirishlar yoki materialni chiqarishni rad etish ehtimoli.
O‘z media loyihasini ishga tushirish	Mavzular, tezlik va sifat ustidan to‘liq nazorat. Auditoriya bilan bevosita aloqa va sodiqlikni shakllantirish. Uzoq muddatli kampaniyalarni yuritish va materiallar arxivini saqlash qulay.	Jamoa, o‘qitish, texnika, saytlar va kontent ishlab chiqarish uchun doimiy xarajatlar. Kontent va izohlar uchun qo‘shimcha huquqiy mas’uliyat. Platformalar siyosati va algoritmlariga qaramlik (shikoyatlar, qamrov cheklovlari, blokirovkalar) hamda muntazam moderatsiya zarurati.

Amalda notijorat tashkilotlar ko‘pincha aralash modeldan foydalanadilar — muntazam kun tartibi va materiallar arxivini yaratish uchun o‘z tibbiy kanallarini ishlab chiqish va targ‘ib qilishni birlashtiradilar hamda asosiy mavzularni kuchaytirish va axborot kampaniyalarini o‘tkazish uchun ommaviy axborot vositalari bilan hamkorlik qiladilar. Bu sezilarli resurslarni talab qiladi, ammo maksimal barqarorlikni ta’minlaydi: tashkilot asosiy kontent va «o‘z ovozi» ustidan nazoratni saqlab qoladi, ommaviy axborot vositalari orqali esa qo‘shimcha qamrov va auditoriya ishonchini qozonadi.

2.1.3. NNT faoliyatida axborot kampaniyalari

NNTlarning axborot kampaniyalari ko‘pincha turli onlayn platformalarda xabardorlikni oshirish, xulq-atvorni o‘zgartirish, qo‘llab-quvvatlash, hamkorlarni jalb qilish yoki qarorga ta’sir o‘tkazish maqsadini ko‘zlamagan holda vaziyatli va tartibsiz postlar seriyasiga o‘xshaydi. Ammo aynan raqamli muhitda axborot kampaniyasini rejalashtirayotganimizda, biz ayniqsa kontent va onlayn platformaga juda bog‘liq bo‘lamiz. Bir xil xabar turli onlayn platformalarda turlicha «ishlaydi,» xatolar esa repostlar va izohlar orqali tezda kengayadi. Shu sababli, kampaniyani maqsad, auditoriya, asosiy xabarlar, nashr sanalari, ma’ruzachilar va oldindan tanlangan muvaffaqiyat ko‘rsatkichlarini aniqlab, loyiha sifatida qurish oqilona bo‘ladi.

Rejalashtirishda shuni yodda tutish kerakki, kontent bir nechta darajada parallel ravishda nazorat qilinadi: platformalar (moderatsiya, qamrov cheklovlari, bloklash), auditoriya (shikoyatlar, muammoli fikrlar) va vakolatli davlat organlari tomonidan. Bu shuni anglatadiki, kommunikatsiya jamoasiga nafaqat kontent uchun g'oyalar, balki tushunarli sharhlash qoidalari va murakkab vaziyatlarda harakat qilish algoritmlari ham zarur.

Quyidagi jadvalda raqamli muhitda media kontent va kampaniyalarni baholash uchun yetarli bo'lgan KPI (key performance indicators, asosiy ko'rsatkichlar) ning qisqartirilgan to'plami keltirilgan.

KPI ko'rsatkichi	Nimani ko'rsatadi?	Qayerdan ko'riladi?
Qamrovlar va namoyishlar	Kontentni qancha odam ko'rdi?	Onlayn platformalar tahlili
Auditoriya jalb qilinishi (reaksiyalar, izohlar, repostlar)	Kontent auditoriya uchun qanchalik qiziqarli?	Onlayn platformalar tahlili
Havolalar orqali o'tishlar	Postdan tashqaridagi material yoki harakatga qiziqishni	Harakatlar, o'tishlar statistikasi
Auditoriya harakati (ro'yxatdan o'tish, ariza berish va hokazo)	Kampaniyaning haqiqiy natijasini	Ariza shakllari, so'rovnomalar va boshqalar.
Fikr-mulohaza sifati	Auditoriyaning mavzuni qanchalik tushunganini va ishonchini ko'rsatadi (mazmunli savollar, murojaatlar).	Murojaatlar statistikasi

Bu ko'rsatkichlar axborot kampaniyasi samarali yoki samarasiz ekanligini ortiqcha tafsilotlarsiz ko'rish uchun yetarli. Qamrov va ishtirok kampaniyangizning axborot makonida qanchalik ko'zga tashlanishini, o'tishlar va konversiyalarni — belgilangan maqsadlarga qanchalik samarali erishayotganingizni, fikr-mulohaza sifati esa sizni qanchalik tushunishlarini va sizga qanchalik ishonishlarini ko'rsatadi.

2.1.4. Kommunikatsiyalarda ekspert roli

O'zbekistondagi NNT vakillari OAV uchun nafaqat "o'z" mavzusi bo'yicha, balki ijtimoiy siyosat, zaif guruhlar huquqlari, ta'lim, sog'liqni saqlash, mehnat nizolari, raqamli xavflar va xayriya kabi keng ko'lamli masalalarda ham ekspert sifatida qatnashadilar. Ushbu/ Bunday rolni saqlab qolish uchun quyidagi uchta muhim jihatni yodda tuting:

- OAV har doim izohni imkon qadar tez olishni istaydi. Tezkor javob berish sizning ekspert sifatidagi obro'yingizni oshiradi.
- OAV mavzuga oid, ortiqcha "suvsiz" izohlarni qadrlaydi. Mazmunli va aniq fikr yuqori malaka belgisi hisoblanadi.
- OAV sezgir kontent qanchalik ko'pligini yaxshi biladi, shu sababli mavzu, iboralar va spikerlarni tanlashda ehtiyotkorlik zarur. Agar siz tezkor, mazmunli va sezgir mavzularga ortiqcha tegmagan holda izoh bersangiz, siz OAV uchun ideal ekspertsiz./ mukammal mutaxassissiz.

Boshqacha aytganda, OAV tasdiqlanadigan manbalar va shaxsiy amaliyotga tayangan holda, hissiy baholar va keskin bayonotlarsiz tez va tushunarli sharh bera oladigan ekspertni tanlaydi.

Quyida ekspert uchun **“to do / to do not”** formatidagi qisqa qoidalar ro‘yxati keltirilgan (uni NNT spikerlari uchun ichki standart sifatida ishlatish mumkin).

TO DO (Qiling)	TO DO NOT (Qilmang)
So‘rovni aniqlashtiring — mavzu, format, muddat (deadline), izoh qaysi shaklda kerakligi: matn, audio yoki video.	Faktlarsiz javob bermang — kontekst yoki dalillarsiz “yo‘l-yo‘lakay” izoh bermang.
OAV uchun izohni imkon qadar qisqa, lekin tushunarli qiling. Ideal variant: bitta asosiy tezis, unga ikkita dalil va bir necha tavsiya.	Uzoq ma’ruzalarga o’tib ketmang va o‘zingiz yoki yutuqlaringiz haqida gap boshlamang.
Tekshiriladigan manbalarga tayaning — hujjatlar, statistika, tadqiqotlar (deadline imkon berganida).	Noma’lum yoki yopiq manbalarga tayanmang, e’lon qilib bo‘lmaydigan yoki ishonchingiz komil bo‘lmagan manbalarni keltirmang.
Neytral iboralardan foydalaning, ayniqsa nozik mavzularda; bahsli faktlar haqida ehtiyotkorlik bilan gapiring.	Ommaviy ayblovlar, balandparvoz bayonotlar va bahsli fikrlar bildirmang. Bularning barchasi internetda tarqalib, memlarga aylanadi va sizning mutaxassisligingizga foyda keltirmaydi.

OAV uchun ekspert bo‘lish qiziqarli, ammo har doim ham oson emas: doim izoh berishga tayyor turish, kun tartibida tezda mo‘ljal olish, qisqa va aniq javob berish kerak. Ammo afzalliklari kamchiliklardan ko‘proq: ekspertlarning sharhlari NNTga bo‘lgan ishonchni oshiradi, hamkorlar va tarafdorlar doirasini kengaytiradi, muhim mavzularni jamoatchilik muhokamasiga olib chiqishga yordam beradi. OAV NNTlarni ishonchli axborot manbai sifatida qabul qiladi va jurnalistlar ularga qayta-qayta murojaat qiladi.

2.2. NNT loyihalari va faoliyati uchun axborot olish

Axborotdan foydalanish imkoniyatini davlatdan ma’lumot berishini so‘rash deb tushunmaslik kerak. Bu — fikrni erkin ifodalashning bir qismi va jurnalistning kasbiy qurolidir. U davlat chegaralaridan qat’i nazar, har qanday ma’lumot va g‘oyalarni izlash, olish hamda tarqatish huquqini o‘z ichiga oladi. Amalda bu tahririyat va muallifning davlat idoralari hamda tashkilotlari tasarrufidagi ma’lumotlar, hujjatlar va yozuvlarni so‘rab olish, shuningdek, bunday axborotning ijtimoiy ahamiyatini asoslash huquqiga ega ekanini anglatadi.

Shu bilan birga, mintaqaviy amaliyot shuni ko‘rsatadiki, huquq rasmiy ravishda tan olinsa-da, uni amalga oshirish qiyin: Global Right to Information Rating reytingida O‘zbekiston 140 davlat orasida 129-o‘rinni egallaydi. Bu juda past ko‘rsatkich bo‘lib, axborot ochiqligi bilan bog‘liq barqaror muammolarni, so‘rovlarga javob berish muddatlariga rioya qilinmasligini, javoblar sifati pastligini va shikoyat qilish mexanizmlarining deyarli ishlamasligini aks ettiradi.

2.2.1. Axborot va hujjatlarni izlash uchun ochiq ma’lumotlar bazalari, reyestrlar va axborot tizimlariga kirish

Xalqaro huquqda axborotdan foydalanish fikr bildirish erkinligining bir qismi sifatida qaraladi: bu huquq nashr qilish bilan cheklanmaydi — u axborotni olishdan boshlanadi.

1. Davlat organlari axborotiga kirish

Birinchi navbatda jamoatchilikka oid masalalarga taalluqli materiallar, ma’lumotlar va hujjatlar ochiq bo‘lishi kerak: qarorlar, hisobotlar, reyestrlar, bayonnomalar, statistika, davlat xaridlari, byudjetlar, tekshiruv natijalari. Bu nafaqat OAVning jamoatchilik uchun muhim mavzular bo‘yicha axborot olish huquqi, balki jamiyatning tekshirilgan hujjatlarga asoslangan sifatli mediakontent olish huquqini ham o‘z ichiga oladi.

2. O‘zi haqidagi shaxsiy ma’lumotlarga kirish

Har bir inson avtomatlashtirilgan bazalarda o‘zi haqidagi ma’lumotlar mavjud yoki yo‘qligini, aynan qanday ma’lumotlar yig‘ilayotgani va saqlanayotganini, kim tomonidan va qanday maqsadda foydalanilayotganini bilish huquqiga ega.

Bu, ayniqsa, notijorat tashkilotlarining ma’lumotlar bilan amaliy ishlashida muhim ahamiyatga ega. NNTlar muntazam ravishda shaxsiy ma’lumotlarni to‘playdi va ularga ishlov beradi — masalan, tadbir ishtirokchilarini ro‘yxatdan o‘tkazishda, benefitsiarlar, donorlar, ko‘ngillilar bilan ishlaganda yoki tadqiqotlar o‘tkazganda. Bunday sharoitda tashkilot qanday ma’lumotlarni, nima asosida yig‘ayotganini va ularning himoyasini qanday ta’minlayotganini tushunishi lozim.

Bu huquq xavf-xatarlarni baholashda ham muhimdir. Ma’lumotlar oshkor bo‘lib qolgan yoki ulardan noqonuniy foydalanilgan hollarda, NNT axborotga ishlov berishning qonuniyligini tekshirishga, oqibatlarini baholashga va to‘g‘ri chora ko‘rishga tayyor bo‘lishi kerak. Bundan tashqari, muloqot chog‘ida va materiallarni e’lon qilishda odamlarning huquqlarini buzmaslik hamda tashkilot uchun huquqiy xavf-xatarlar tug‘dirmaslik uchun jamoat manfaati bilan shaxsiy hayotga aralashuv o‘rtasidagi chegarani aniq belgilash lozim.

3. Jamoatchilik manfaati — ma’lumotlarni oshkor qilishning asosiy omili sifatida

So‘rovlar o‘z vaqtida, tushunarli tartibda ko‘rib chiqilishi, ishlov berish uchun to‘lov esa asossiz to‘siqlar yaratmasligi kerak. Har qanday rad etish asoslantirilgan bo‘lishi shart: davlat organi aynan nima uchun kirish cheklanganligini, qanday huquqiy asosga ko‘ra va nima uchun cheklash zarurligini tushuntirishi lozim.

Albatta, ideal holatda axborot OAV, fuqarolik jamiyati va fuqarolarga birinchi talabda taqdim etilishini istaymiz. Ammo cheklovlar bor, bo‘lgan va bo‘ladi — bu real holat. Cheklovlar faqat qat’iy asoslangan hollarda maqbul bo‘lishi mumkin. Bunga quyidagilar kiradi: xavfsizlik va mudofaa, xalqaro munosabatlar, jamoat xavfsizligi, jinoyatlarni tergov qilish, shaxsiy hayotni himoya qilish, tijorat manfaatlari, iqtisodiy va valyuta siyosati, adolat manfaatlari, atrof-muhitni muhofaza qilish, ichki muhokamalarning maxfiyligi.

Ammo **mavzuning o‘zi** cheklovning qonuniyligini isbotlamaydi. Kasbiy faoliyatingizda axborotdan foydalanishni cheklashga bo‘lgan har qanday urinishga nisbatan uchta savolni bering:

1. Buning uchun qonunda to‘g‘ridan-to‘g‘ri asos bormi?
2. Axborotning aynan shu qismini yopiq saqlash zarurmi?
3. Hujjatni butunlay yopmasdan, uning sezgir qismlarini olib tashlagan holda qisman ochish mumkinmi?

Axborotning bir necha yirik toifalarini (hujjatlar, ma’lumotlar) farqlash foydali bo‘lib, ularga kirish butunlay yopilishi yoki vaqtincha cheklanishi mumkin.

Axborot toifasi

Davlat siri
Bu — hujjatlarning eng murakkab va yopiq toifasi sanaladi, biroq bu yerda ham cheklovlarning vaqtinchalik ekani va qat’iy qonuniylikka asoslanishi tamoyili amal qiladi. Davlat sirlaridan faqat cheklangan doiradagi shaxslargina xabardor bo‘lishi mumkin. Jurnalistlar bu doiraga kirmaydi.

Vaqtincha cheklanishi mumkin bo‘lgan axborot
Bu eng keng va amaliyotda eng ko‘p bahsli toifa. Cheklovlar aniq, proportsional va asoslangan bo‘lishi kerak. Ammo amaliyotda vaqtinchalik cheklovlar ko‘pincha doimiy cheklovga aylanadi. Ko‘pincha hujjatning faqat zarur qismi emas, butun hujjat yopiladi.

Maxfiylashtirilishi yoki cheklanishi mumkin bo‘lmagan axborot
Bu ma’lumotlar qonunga ko‘ra ochiq bo‘lishi kerak, chunki ular davlat organlari faoliyatining shaffofligi va davlat mablag‘larining sarflanishi (byudjetlar, xaridlar, qarorlar, hisobotlar, tekshiruvlar natijalari va ijtimoiy ahamiyatga molik masalalar bo‘yicha statistika) bilan bevosita bog‘liq.

Huquqiy sirlar (shaxsiy hayot, tijorat siri va boshqalar)
Ushbu rejimlar ijtimoiy ahamiyatga ega ma’lumotlarga bo‘lgan huquqni bekor qilmaydi, lekin yanada sinchkov tahririyat tekshiruvini va shaxsiy hayotga aralashuvni kamaytirishni talab qiladi.

O‘zbekiston, Markaziy Osiyoning barcha mamlakatlari singari, davlat boshqaruviga raqamlashtirishni muvaffaqiyatli joriy etmoqda. Bu shuni anglatadiki, jamoatchilik nazorati endilikda davlat idoralariga so‘rov yuborish bilan emas, balki ko‘pincha ochiq raqamli manbalarni o‘rganishdan boshlanadi. Bu faktcheking sifatini tubdan o‘zgartiradi: avvaliga asosiy faktlarni (me’yoriy-huquqiy baza, mahalliy hokimiyat qarorlari, xaridlar to‘g‘risidagi ma’lumotlar, statistika) tezda aniqlab olish, shundan so‘ng zarur hujjatni taqdim etishni talab qilib, aniq so‘rovlar yuborish mumkin bo‘ladi. Bunday yondashuv “mavhum va umumiy javob” olish xavfini kamaytiradi va so‘rov yuboruvchining mavqeyini mustahkamlaydi. Chunki davlat idorasi tahririyatning hujjatlardan xabardorligini va “umuman olib” emas, balki aniq masala yuzasidan murojaat qilayotganini ko‘radi.

Onlayn ma’lumot olish uchun manbalar ro‘yxati

Resurs nomi	Havola	Tavsif
Qonunchilikning me’yoriy bazasi Lex.UZ	https://lex.uz/en/	Amaldagi qonunlar, qonunosti hujjatlari va rasmiy matnlarni tez topish mumkin bo‘lgan milliy qonunchilik bazasi LexUZ (LEX.UZ)
E-Qaror	https://cabinet-eqaror.gov.uz/ru/auth/login	Mahalliy davlat hokimiyati organlari tomonidan qabul qilinadigan qarorlarni ishlab chiqish, kelishish va ro‘yxatdan o‘tkazishning yagona elektron tizimi
Open Data Portal of the Republic of Uzbekistan	https://data.egov.uz/eng?utm_source=chatgpt.com	O‘zbekiston davlat organlarining ochiq ma’lumotlar portali. Ma’lumotlarning ko‘pligi, shu jumladan mashina o‘qiy oladigan format.
Davlat xaridlari portali	https://xarid.uzex.uz/home	UzEx platformasidagi davlat xaridlari elektron tizimi (xarid.uzex.uz va tegishli xizmatlar) e’lonlar, xarid jarayonlari va asosiy ma’lumotlarni topish imkonini beradi.
Sud hujjatlari bazasi	https://publication.sud.uz/ — !/sign/view	O‘zbekiston Respublikasi sudlari tomonidan chiqarilgan va qonuniy kuchga kirgan sud hujjatlari.
Milliy statistika portali	https://stat.uz/ru/47-ofitsialnaya-statistika	O‘zbekiston iqtisodiyoti, aholisi va boshqa sohalar bo‘yicha statistik ma’lumotlar.
O‘zbekiston Respublikasi Prezidentining Virtual qabulxonasi	https://pm.gov.uz/ru#/	Davlat rahbariga keng ko’lamli ichki va tashqi siyosat masalalari bo’yicha murojaatlar yuborish xizmati
O‘zbekistondagi kompaniyalar reyestri	https://orginfo.uz/	Yuridik shaxslarning holati va faoliyati to’g’risidagi ma’lumotlar portali

Bu to‘liq ro‘yxat emas, lekin bu yerda muhim ma’lumotlarni olish uchun asosiy onlayn platformalar keltirilgan.

2.2.2. Verifikatsiya va faktcheking

Agar ularning so‘roviga davlat organidan javob olingan bo‘lsa, uni tasdiqlash yoki verifikatsiya qilish shart emasmi? Darhaqiqat, biror voqea yoki tadbir haqida xabar berayotganimizda, ko‘pincha davlat organining so‘rovga bergan javobini keltirishimiz kifoya. Shunday qilib, muvozanatga erishiladi — nashrda manfaatdor tomonlarning barcha nuqtai nazarlari aks ettiriladi.

Ammo agar gap byudjet mablag‘lari hisobidan amalga oshiriladigan tekshiruvlar, davlat xaridlari, loyihalar va hokazolar haqida ketsa, davlat organlarining javoblari va boshqa har qanday faktik ma’lumotlar **tekshirilishi, verifikatsiya qilinishi yoki faktcheking qilinishi lozim**.

O‘zbekistonda yolg‘on ma’lumot tarqatganlik uchun ham ma’muriy, ham jinoiy javobgarlik nazarda tutilganligini hisobga olsak, verifikatsiya va faktcheking haqiqatan ham muhim ahamiyat kasb etadi. Quyidagi jadvalda ma’lumotlar va hujjatlarni, shu jumladan davlat idoralaridan olingan hujjatlarni tekshirishning asosiy bosqichlarini ko’rib chiqing.

Hujjatlar, javoblar va ma'lumotlarni verifikatsiya qilish (tekshirish) bo'yicha amallar (qadamlar)

1-bosqich.
Tasdiqlash va kerakli hujjatni qayd etish

Bitta tekshiriladigan faktni shakllantiring (summa, sana, yetkazib beruvchi, «bir manbadan,» tekshirish natijasi) va u qaysi hujjat yoki reyestr bilan tasdiqlanishini aniqlang.

Natija: Nimani tekshirish va nimani izlash kerakligi aniq.

2-bosqich.
Birlamchi manba va hujjatni topish

Mansabdor shaxsning izohi yoki savoliga bergan javobi yetarli emas. Bu birlamchi manba emas. Birlamchi manbani — hujjatlashtirilgan ma'lumotni izlang.

Natija: Fikr yoki mulohazaga emas, hujjatga tayaniladi.

3-bosqich.
Tasdiqlash uchun muqobil manbani topish va o'rganish

Har bir faktni o'zaro bog'liq bo'lmagan uchta axborot manbasida tasdiqlash maqsadga muvofiqdir.

Natija: Yolg'on ma'lumot tarqatishda ayblanish xavfi kamayadi

4-bosqich.
Hujjatdagi faktik ma'lumotlarni tekshirish

Hujjat rekvizitlarini solishtiring: raqami, sanasi, organ/tashkilot nomi, predmeti, summasi, muddatlari, hujjatni imzolagan shaxsning F.I.Sh. va lavozimi.

Natija: Xatolar va «to'liq bo'lmagan» hujjatlar istisno qilinadi. Shikoyat va ayblovlar xavfi kamayadi.

2.2.3. Akkreditatsiya

Axborotdan tezroq foydalanish tartibi sifatida akkreditatsiya an'anaviy ravishda jurnalistlar uchun vosita sifatida qaralgan, biroq O'zbekistonda amaliyotda undan cheklangan holda foydalaniladi. Aksariyat hollarda gap davlat rahbari, vazirlar va boshqa mansabdor shaxslar ishtirokidagi alohida tadbirlarga vaqtinchalik akkreditatsiyadan o'tish haqida bormoqda. Kundalik faoliyatda axborotdan foydalanish tobora ko'proq boshqa mexanizmlar orqali ta'minlanmoqda.

Raqamlashtirishning rivojlanishi bilan davlat organlari axborotdan ochiq foydalanishning muqobil usullarini bosqichma-bosqich joriy etmoqdalar. Ochiq majlislarni onlayn translyatsiya qilish, bayonnomalar, qarorlar va boshqa hujjatlarni rasmiy saytlarda e'lon qilish, shuningdek, ma'lumotlarni real vaqt rejimida joylashtirish shular jumlasidandir. Ushbu vositalar tobora muhim ahamiyat kasb etib, an'anaviy akkreditatsiya tartib-qoidalarining o'rnini qisman egallamoqda.

Rasmiy ravishda akkreditatsiya davlat organlari bilan muntazam hamkorlik qilish usuli sifatida qonunchilikda mustahkamlangan. Qonunlar hokimiyat organlari faoliyati to'g'risida axborot olish, ochiq tadbirlarda qatnashish va hujjatlar bilan ishlash imkoniyatini nazarda tutadi. Biroq, ushbu huquqlarni amalga oshirish tartibi ko'p jihatdan organlarning o'z ichki qoidalari — jumladan, kirish qoidalari, ro'yxatdan o'tish, kvotalar va xavfsizlik talablari bilan belgilanadi.

Notijorat tashkilotlar uchun bu shuni anglatadiki, rasmiy huquqlarning mavjudligi har doim ham ma'lumotlarga haqiqiy kirishni kafolatlamaydi. Amaliyotda NNTlar akkreditatsiya tartibidan foydalanishdan ko'ra ko'proq ochiq manbalar va raqamli kanallar bilan hamkorlik qiladilar.

Bu borada onlayn translyatsiyalar va davlat organlari materiallarini e'lon qilish alohida ahamiyat kasb etadi. Ular muhokamalarni, mansabdor shaxslarning pozitsiyalarini va qabul qilinayotgan qarorlarni jismoniy ishtirok etish zaruratisiz tezkor kuzatish imkonini beradi. NNT uchun bu resurslarni tejashga va kun tartibida tezroq mo'ljal olishga yordam beradigan qulay monitoring vositasidir.

Bundan tashqari, bunday materiallar keyingi ishlar uchun boshlang'ich nuqta bo'lib xizmat qilishi mumkin. Tashkilot ko'rilgan majlislar va e'lon qilingan ma'lumotlar asosida so'rovlarni aniqroq shakllantirishi, qo'shimcha ma'lumot olish uchun murojaat qilishi va o'z faoliyatida dalillar keltirishi mumkin. Shunday qilib, akkreditatsiyadan cheklangan tarzda foydalanilgan taqdirda ham, raqamli vositalar va ochiq manbalar orqali ma'lumotlardan foydalanish imkoniyati saqlanib qolmoqda.

2.2.4. Axborot manbalarining himoyalanishi va maxfiy saqlanishi

Axborot manbalarining maxfiyligini saqlash nafaqat jurnalistika, balki notijorat tashkilotlar faoliyati uchun ham muhim tamoyildir. NNTlar ko'pincha nozik ma'lumotlar bilan ishlaydi, anonimlik sharti bilan ma'lumot berishi mumkin bo'lgan benefitsiarlar, arizachilar, ekspertlar, hamkorlar va ma'lumot beruvchilar bilan hamkorlik qiladi. Maxfiylik kafolatlari bo'lmasa, bunday shaxslar ma'lumotlarni, ayniqsa qoidabuzarliklar, suiiste'molliklar yoki jamoat manfaatlariga taalluqli boshqa masalalar haqida ma'lumot berishni rad etishlari mumkin.

O'zbekiston qonunchiligida manbalarni himoya qilish bevosita OAVga nisbatan mustahkamlangan, biroq maxfiylik tamoyillarining o'zi NNT faoliyatiga ham taalluqlidir. Bu, xususan, shaxsiy ma'lumotlar bilan ishlashga, shuningdek, oshkor qilmaslik sharti bilan berilgan ma'lumotlarga taalluqlidir. Tashkilot ba'zi hollarda bunday ma'lumotlarning saqlanishi va manbaning roziligisiz uning shaxsini oshkor etilishiga yo'l qo'ymaslik uchun javobgar ekanligini tushunishi lozim.

Amaliyotda NNTlar ulardan axborot manbasini oshkor qilish, aloqa ma'lumotlarini taqdim etish yoki ma'lumotlarning kelib chiqishini tasdiqlash talab qilinadigan vaziyatlarga duch kelishlari mumkin. Bunday talablar davlat organlari tomonidan ham, boshqa manfaatdor tomonlar tomonidan ham bo'lishi mumkin. Bunday sharoitda maxfiy ma'lumotlar bilan ishlashning ichki tartib-qoidalarini ishlab chiqish va yuzaga kelishi mumkin bo'lgan xavf-xatarlarni oldindan hisobga olish muhimdir.

Manba bilan muloqotda, masalan, yozishmalarda yoki kelishuvlar doirasida maxfiylik shartlarini boshidanoq qayd etish tavsiya etiladi. Shu bilan birga, agar ish uchun zarurat bo'lmasa, shaxsni aniqlash imkonini beruvchi ma'lumotlarni to'plash va saqlashni minimallashtirish muhimdir. Bu sizib chiqish xavfini kamaytiradi va himoya darajasini oshiradi.

Manbani oshkor qilish to'g'risidagi talablar kelib tushgan taqdirda, axborotni avtomatik ravishda uzatmaslik kerak. Bunday so'rovning huquqiy asoslarini baholash, huquqshunosni jalb qilish va tashkilot hamda manbaning o'zi uchun ehtimoliy oqibatlarni hisobga olgan holda qaror qabul qilish zarur. Shuni yodda tutish kerakki, maxfiylikni himoya qilish nafaqat axloqiy masala, balki xavf-xatarlarni, jumladan obro' va huquqiy xavflarni boshqarishning bir qismi hamdir.

Shunday qilib, NNTlar uchun axborot manbalarini himoya qilish ma’lumotlar va odamlar bilan ishlashga mas’uliyatli yondashuvni shakllantirishni anglatadi. Bu ishonchni saqlab qolish, axborot beruvchilarning xavfsizligini ta’minlash va jarayonning barcha ishtirokchilari uchun bosim yoki salbiy oqibatlar ehtimolini kamaytirish imkonini beradi.

2.2.5. Messenjerlar va telegram-kanallar orqali rasmiy ma’lumotlarni olish

Davlat organlarining aloqalari tobora tezkor va to‘liq raqamli formatga o‘tmoqda. Matbuot xizmatlari ijtimoiy tarmoqlarda o‘z akkauntlariga ega bo‘lib, messenjerlardagi kanallar va chatlardan nafaqat jurnalistlar bilan tezkor aloqa qilish, balki favqulodda va inqirozli aloqalar uchun ham foydalanadilar. Matbuot xizmatlari darhol bayonotlar, raqamlar va tushuntirishlarni e’lon qilishi, shov-shuv va xatolarga tezda javob berishi, pozitsiyani to‘g‘ridan-to‘g‘ri auditoriyaga yetkazishi, fotosuratlar, videolar va hujjatlarni ilova qilishi mumkin. Bunday kommunikatsiyalar teskari aloqani ta’minlaydi.

Biroq, davlat organlari bilan telegram-kanallar orqali muloqot qilishda ikki darajani ajratish kerak — (1) tezkor muloqot — savollarga javob berish, qayta aloqa, avvalgi ma’lumotlarni aniqlashtirish yoki to‘ldirish, fotosurat yoki video so‘rash, lavozimlar va boshqa ma’lumotlarni tuzatish va (2) davlat organini, veb-saytga havolani albatta ko‘rsatgan holda, nashrda ishonch bilan tayanish mumkin bo‘lgan rasmiy ma’lumotni olish.

Ba’zi hollarda davlat organlari matbuot xizmatlari telegram-kanal rasmiy ma’lumot manbai emasligini darhol aniqlashtiradi. Bunday hollarda rasmiy manbalar orqali qo‘shimcha ma’lumot so‘rash va telegram-kanal orqali olingan faktlar yoki hujjatlarning ishonchliligiga tayanmaslik xavfsizroqdir.

2.2.6. Muammolar yuzaga kelganda qanday harakat qilish kerak? Axborot toifalari — «Xizmatda foydalanish uchun,» davlat sirlari va foydalanish cheklangan bo‘lishi mumkin bo‘lgan boshqa toifalar

O‘zbekiston va Markaziy Osiyo mamlakatlaridagi notijorat tashkilotlarining ish amaliyoti o‘xshash tendensiyalarni ko‘rsatmoqda: rasmiy qonuniy kafolatlarga qaramay, axborotdan foydalanish ko‘pincha cheklangan bo‘ladi. Ijtimoiy ahamiyatga ega mavzular bilan ishlovchi NNTlar loyihalarni amalga oshirish, monitoring qilish va tahlillarni tayyorlash uchun zarur bo‘lgan ma’lumotlarni olishda muntazam ravishda qiyinchiliklarga duch kelishadi.

Ko‘p hollarda yopiqlik madaniyati shaffoflik tamoyillaridan ustunlik qilishda davom etmoqda. Davlat organlari ma’lumotlarni oshkor qilish o‘rniga ularni cheklashni afzal ko‘rib, inersiya bo‘yicha harakat qilishlari mumkin. Rasmiy veb-saytlar va axborot resurslari har doim ham dolzarb va to‘liq ma’lumotlarni o‘z ichiga olmaydi, muntazam ravishda yangilanmaydi, hujjatlar esa tanlab nashr etiladi.

Ma’lumot olish uchun murojaat qilishda NNT vakillari ham qo‘shimcha to‘siqlarga duch kelishlari mumkin. So‘rovlar ma’lumot olish maqsadlari, ma’lumotlardan foydalanish mo‘ljali va tashkilotning keyingi harakatlari to‘g‘risidagi aniqlashtiruvchi savollar bilan birga keladi. Bunday savollar har doim ham qonuniy asosga ega bo‘lmasa-da, amalda ular jarayonni kechiktirish yoki kirishni cheklash usuli sifatida qo‘llanilishi mumkin.

Natijada NNT faoliyatida axborotdan foydalanish bilan bog‘liq tipik muammolar yuzaga kelmoqda.

Axborot olish sohasidagi qonunbuzarlik	Qoidabuzarlik tavsifi va qanday harakat qilish kerak?
Javob muddati buzilishi	Javob qonunda belgilangan muddatda berilmaydi yoki tushuntirishsiz kechikib yuboriladi. Ba’zan ariza beruvchiga so‘rovning ro‘yxatdan o‘tkazilganligi haqida xabar berilmaydi va oraliq ma’lumot berilmaydi (kim ko‘rib chiqadi, javob qachon tayyor bo‘ladi). Tahririy yondashuv quyidagicha bo‘lishi mumkin. Yuborish va ro‘yxatdan o‘tish sanasini qayd eting, dastlabki so‘rovga havola va ko‘rib chiqish holatini tasdiqlash so‘rovi bilan qisqa eslatma yuboring. Agar muddat o‘tib ketgan bo‘lsa, kechikish sababi va javob berish sanasini ko‘rsatish talabi bilan qayta so‘rov yuboring. Zarurat tug‘ilganda, darhol prokuratura organlariga shikoyat yuboring.
OAV tahririyati so‘roviga to‘liq bo‘lmagan javob	Javobda umumiy ta’riflar keltiriladi, ammo aniq savollarga javob berilmaydi, so‘ralgan hujjatlar yoki ma’lumotlar berilmaydi, javoblar uchun faqat qulay bandlar tanlanadi yoki ma’lumot taqdim etmasdan saytga yo‘naltiriladi. Ko‘pincha hujjat rekvizitlari (raqami, sanasi), ma’lumotlar manbalari va mas’ul mansabdor shaxs ko‘rsatilmaydi. Tahririyat qanday ish tutishi kerak? Javobni so‘rov bandlari bilan solishtiring va aynan nima berilmaganini ro‘yxat orqali aniqlashtiring. Hujjatlarning nusxalari yoki ulardan ko‘chirmalar, rekvizitlar va ma’lumotlar manbasini taqdim etishni so‘rang. Agar ma’lumotlarning bir qismini oshkor qilish mumkin bo‘lmasa, rad etishning huquqiy asosini so‘rash va ma’lumotlarning qolgan qismini taqdim etish to‘g‘risida talabnoma yuborish mumkin.
So‘ralayotgan axborot faqat xizmatda foydalanish uchun mo‘ljallanganligini vaj qilib, ma’lumot berishni rad etish.	Xizmat doirasida foydalanish uchun mo‘ljallangan axborotlar toifasiga kiritish tartibiga rioya qilinmayapti: juda ko‘p hujjatlarga “XDFU” belgisi qo‘yilmoqda, cheklov muddati hisobga olinmayapti, hujjat qisman cheklanishi o‘rniga to‘liqligicha yopib qo‘yilmoqda. Bunday vaziyatda tahririyat yondashuvi quyidagicha bo‘lishi lozim: agar hujjat to‘liq yopilgan bo‘lsa, uning aynan qaysi qismlari himoyaga olinganini va nima uchun qolgan qismini taqdim etish imkoni yo‘qligini tushuntirishni talab qiling.
So‘ralayotgan axborot sir, masalan, tijorat siri ekanligini sabab qilib ko‘rsatib, uni taqdim etishdan bosh tortish.	Tijorat siri ko‘pincha xususiy tashkilotlar va davlat organlari tomonidan ma’lumotlarni oshkor qilishga qarshi dalil sifatida ishlatiladi. Har doim so‘rovingiz ijtimoiy ahamiyatga ega ekanligini ta’kidlang (masalan, gap davlat mablag‘larini sarflash yoki ijtimoiy sohalar uchun dasturlar, loyihalar haqida ketganda). Ijtimoiy ahamiyatga ega bo‘lgan ma’lumotlarni oshkor qilish har doim ustuvor bo‘lishi kerak.

Xususiy kompaniyalar va tashkilotlarning davlat organlariga so‘rovlar bo‘yicha ma’lumot taqdim etishdagi turli cheklovlarga qaramay, OAV tahririyatlariga huquqiy yordam ko‘rsatishning amaliy tajribasiga asoslangan bir nechta umumiy tavsiyalar mavjud:

- So‘rovlarni aniq va ravshan ifodalash maqsadga muvofiqdir. So‘rov qanchalik aniq ifodalangan yoki talab qilinadigan hujjatlar belgilangan bo‘lsa, siz talab qilingan ma’lumotni olishingiz ehtimoli shunchalik yuqori bo‘ladi.
- Faqat so‘rovlarga tayanmang. Muqobil axborot manbalari — ochiq ma’lumotlar, reyestrlar, ma’lumotlar bazalaridan faol foydalaning, axborot manbai sifatida esa bloglar va ijtimoiy tarmoqlardan foydalaning.

Davlat idoralaridan izoh emas, hujjatlar so‘rang. Izohlarni sizga ekspertlar taqdim etishi mumkin. Bunday holda, siz talqin va subyektiv fikrlarga kamroq bog‘liq bo‘lasiz.

2.3. Raqamli muhitda kontent uchun javobgarlik

Raqamli muhitda notijorat tashkilotlar nafaqat axborot qabul qiluvchilar, balki uning faol tarqatuvchilari sifatida ham namoyon bo‘ladilar. Saytlar, ijtimoiy tarmoqlar, messenjerlar va boshqa onlayn platformalardagi nashrlar tashkilotning ommaviy pozitsiyasini shakllantiradi va uning obro‘siga bevosita ta’sir ko‘rsatadi.

Shu bilan birga, joylashtirilgan har qanday ma’lumot — matnlar, tasvirlar, foydalanuvchilarning izohlari — qonuniy javobgarlikka sabab bo‘lishi mumkin. Bu NNTning o‘z materiallariga ham, tashkilot nomidan tarqatiladigan yoki uning saytlariga joylashtiriladigan kontentga ham tegishli.

Shu sababli, qaysi turdagi kontent qonunchilikni buzish deb hisoblanishi mumkinligini, ruxsat etilgan fikrning chegarasi qayerda ekanligini va raqamli muhitda ishlashda qanday xavflar yuzaga kelishini tushunish muhimdir.

2.3.1. Noqonuniy (taqiqlangan) va nozik mazmundagi kontentga nimalar kiradi?

Markaziy Osiyo mamlakatlarida kontent yaratuvchilar, shu jumladan NNTlar uchun mavzular ro‘yxati mavjud bo‘lib, ular ba’zi mamlakatlarda qonunchilik darajasida noqonuniy hisoblanadi (masalan, Qozog‘iston), boshqa mamlakatlarda esa bu mavzulardagi nashrlar nomaqbul hisoblanadi, chunki ular nashr mualliflari, NNTlar, OAV tahririyatlari va ularning mulkdorlari uchun jiddiy muammolarni keltirib chiqarishi mumkin.

O‘zbekistonning xalqaro majburiyatlari shuni taqozo etadiki, eng aniq taqiqlovchi choralar quyidagi holatlar bilan bog‘liq bo‘lgan hollarda ko‘rilishi kerak:

- ekstremizm va terrorizmni targ‘ib qiluvchi hamda taqiqlangan tashkilotlarning materiallariga (shu jumladan, materiallar yoki ramzlar, turli chaqiriqlar tarqatishni taqiqlash);
- giyohvand moddalarni targ‘ib qilish bilan bog‘liq jinoyatlar;
- Davlat sirlarini oshkor qilish va milliy xavfsizlik masalalari bilan bog‘liq;
- milliy, etnik yoki diniy adovatni qo‘zg‘atish, nafrat nutqi;
- bolalarni pornografiya va behayo kontentdan himoya qilish;
- agar ochiq-oydin jamoatchilik manfaati bo‘lmasa, shaxsiy hayot va shaxsiy ma’lumotlar bilan bog‘liq.

Biroq, jurnalistlar, OAV va NNTlar uchun nozik hisoblangan mavzularning katta bir ro‘yxati mavjud. Sababi, agar OAV tahririyati yoki NNT o‘z media loyihasi yoxud axborot resursi faoliyati doirasida ushbu ro‘yxatdagi masalalarni yoritsa, ehtimoliy va real huquqiy muammolarga duch kelishi mumkin. Ayni paytda, bu mavzularni yoritishga to‘g‘ridan-to‘g‘ri taqiq yo‘q, biroq barcha kontent yaratuvchilar ularning naqadar nozik ekanini yaxshi anglaydi.

Bu mavzularning nozikligi, shuningdek, huquqni qo‘llash amaliyoti hamda raqamli muhitda media-kontent ishlab chiqaruvchi va tarqatuvchilarga nisbatan ochilayotgan ishlar sonining ortgani bilan ham belgilanadi.

Ro'yxatda ko'rsatilgan mavzular OAV uchun tabu yoki yopiq emas, lekin ular o'ta ehtiyotkor bo'lishni, faktlarni bir necha bor tekshirishni hamda ehtimoliy bosim yoki ta'qib xavflarini baholashni talab etadi.

Nashr mavzusi	Mavzu nimani qamrab oladi?
Taqiqlangan partiyalar faoliyati	Taqiqlangan tashkilotlar faoliyati, ularning bayonotlari, materiallari, ramzlari, shiorlari, atributikasi; ularning resurslariga havolalar; qo'llab quvvatlash, ishtirok etish yoki moliyalashtirishga chaqiriqlar.
O'z joniga qasd qilishlar	O'z joniga qasd qilish yoki o'z joniga qasd qilishga urinish holatlari haqida sabablari va holatlari batafsil bayon etilgan xabarlar. Voyaga yetmaganlar orasida sodir bo'lgan holatlarning batafsil tavsifi; "ko'rsatma" beruvchi tafsilotlarni (usullar, joylar, harakatlar ketma-ketligi) o'z ichiga olishi mumkin bo'lgan nashrlar, bu esa Verter[25] effektini keltirib chiqarishi mumkin.
Yuqori mansabdor shaxslarning shaxsiy hayoti	Oila va shaxsiy munosabatlar; sog'liq; yashash joyi va maishiy tafsilotlar; shaxsiy yozishmalar va fotosuratlar (oila a'zolarining o'zlari fotosuratlar va ma'lumotlarni ijtimoiy tarmoqlarga joylashtirgan hollar bundan mustasno); bolalar va yaqinlari haqidagi ma'lumotlar; ommaviy vazifa va vakolatlarni bajarish bilan bevosita bog'liq bo'lmagan ma'lumotlar.
Tarixiy voqealar	Tarixiy davrlar va voqealarga berilgan baholar hamda talqinlar; repressiyalar, mojarolar, chegaralar, identiklik mavzulari; bahsli xotira sanalari; jamoatchilik bahslarini keltirib chiqarishi mumkin bo'lgan tarixiy taqqoslashlar.
Millatlararo mojarolar	"Guruhlararo" hodisa va nizolar; millatlararo tus olgan maishiy mojarolar; etnik kelib chiqishi bo'yicha kamsitish; nafrat tili; etnik guruhlarga nisbatan ayblovlar.
Tashqi siyosat	Xalqaro munosabatlar va mansabdor shaxslar bayonotlari; diplomatik mojarolar; urushlar va inqirozlar bo'yicha pozitsiyalar; xalqaro kelishuvlar; tashriflar, muzokaralar, notalar; boshqa davlatlar va ularning yetakchilariga berilgan baholar.
Sanksiyalar	Sanksiya ro'yxatlari va cheklovlar (shaxslar, kompaniyalar, tarmoqlarga nisbatan); aktivlarni muzlatish, bitimlar, yetkazib berish va kirish taqiqlari; biznes uchun ikkilamchi oqibatlar.
Korrupsiya	Korrupsiyaga qarshi surishtiruvlar; mansabdor shaxslarga nisbatan ayblovlar; manfaatlar to'qnashuvi; davlat xaridlari va byudjet mablag'larini taqsimlash.
Ijtimoiy mojarolar	Tariflar, narxlar, kommunal xizmatlar, yer va uy-joy bilan bog'liq nizolar; aholi va hokimiyat hamda biznes o'rtasidagi nizolar; ommaviy shikoyatlar; rezonansli hodisalar.
Diskriminatsiya	Jins, yosh, nogironlik, kelib chiqish, til, din va boshqa belgilar bo'yicha teng bo'lmagan muomala va cheklovlar, shuningdek nafrat tili; inson qadr-qimmatini kamsitish; guruhlarni stereotiplashtirish.
Mitinglar va norozilik namoyishlari	Ommaviy yig'inlar, aksiyalar, piketlar; ularda ishtirok etishga chaqiriqlar; qatnashchilarning talablarini yoritish; qo'lga olishlar va ma'muriy choralar; ishtirokchilar va tashkilotchilarning foto va videolarini e'lon qilish.
Ish tashlashlar	Jamoaviy mehnat nizolari; ishni to'xtatish; xodimlarning talablari; ish beruvchi bilan muzokaralar; ishdan bo'shatish yoki bosim; xodimlar va kasaba uyushmasi faollarining shaxsiy ma'lumotlarini e'lon qilish.
LGBT hamjamiyati masalalari	Huquqlar, kamsitish va xavfsizlik haqidagi postlar; zo'ravonlik va tajovuz holatlari; tibbiy va inson huquqlari mavzulari; jinsiy aloqaga oid kontent./ jinsiylik bilan bog'liq kontent.
Til masalalari	Tillarning maqomi, til siyosati; ta'lim va xizmat ko'rsatish tili atrofidagi mojarolar; "falon tilda gapiring" degan talablar; til belgisi bo'yicha kamsitish; rezonansli bayonotlar va nizolar.

[25] Verter effekti; Verter sindromi — televideniye yoki boshqa ommaviy axborot vositalarida keng yoritilgan yoki mashhur adabiyot yoki kino asarida tasvirlangan o'z joniga qasd qilishdan so'ng sodir etiladigan o'z joniga qasd qilishga taqlid qilishning ommaviy to'lqini.

Din	Diniy tashkilotlar faoliyati; diniy marosimlar va ramzlar; diniy mojarolar; ekstremizmda ayblovlar; haqoratomuz deb hisoblanishi mumkin boʻlgan nozik nashrlar.
Gender masalalari	Teng huquq va imkoniyatlar; oiladagi/gender asosidagi zoʻravonlik; ayollarning siyosat va iqtisodiyotdagi ishtiroki; reproduktiv huquqlar; jins boʻyicha kamsitish; oʻzaro kamsitishga duchor boʻlgan ayollar, qizlar va qizlarning zaif guruhlari.

Yana bir bor taʼkidlaymizki, yuqorida koʻrsatilgan mavzular taqiqlangan yoki yopiq emas, balki maksimal ehtiyotkorlikni, faktlarni qayta-qayta tekshirishni va xavflarni baholashni talab qiladi.

2.3.2. Diffamatsiya, tuhmat va haqorat uchun javobgarlik

Jismoniy va yuridik shaxslarning shaʼni, qadr-qimmati va obroʻsini himoya qilish sud tartibida fuqarolik daʼvosi orqali ham, tuhmat va haqorat qilingan taqdirda maʼmuriy va jinoiy tartib-taomillar orqali ham amalga oshirilishi mumkin.

Qoidabuzarlik turi	Qoʻllaniladigan tartib-qoidalar	Huquqiy oqibatlar
Shaʼn, qadr qimmat va ishchanlik obroʻsini himoya qilish	Oʻzbekiston Respublikasi Fuqarolik kodeksining 100-moddasiga[26] muvofiq sud tartibida daʼvo taqdim etish orqali fuqarolik-huquqiy tartib	Shaʼn va qadr-qimmatga putur yetkazuvchi maʼlumotlarga raddiya eʼlon qilish, maʼnaviy zararni qoplash, ularni tarqatishni toʻxtatish.
Tuhmat	Oʻzbekiston Maʼmuriy javobgarlik toʻgʻrisidagi kodeksining (MJTK) 40-moddasi[27] boʻyicha maʼmuriy ish. Oʻzbekiston Respublikasi Jinoyat kodeksining 139-moddasiga muvofiq[28] tartib-taomil (shu jumladan, agar qilmish maʼmuriy jazo qoʻllanilganidan keyin sodir etilgan boʻlsa; ommaviy axborot vositalari, Internet orqali tarqatish alohida koʻrsatilgan)	Maʼmuriy jarima 20–60 BHM. Jinoiy tartibda javobgarlik choralari. Jarima (shu jumladan BHMning 200 baravarigacha; OAV yoki Internet orqali eʼlon qilinganda jarima 200–400 BHMni tashkil etadi), majburiy ishlar yoki axloq tuzatish ishlari, ozodlikni cheklash mumkin; kvalifikatsiya belgilari mavjud boʻlsa, yanada qattiqroq sanksiyalar qoʻllanilishi mumkin (shu jumladan BHMning 300–500 baravarigacha jarima yoki 3 yilgacha ozodlikni cheklash).
Haqorat	MJTKning 41-moddasiga[29] muvofiq maʼmuriy tartib. Asoslar mavjud boʻlganda, Oʻzbekiston Respublikasi Jinoyat kodeksining 140-moddasiga muvofiq jinoiy-huquqiy taomillar qoʻllanilishi mumkin (shu jumladan, maʼmuriy jazo qoʻllanilganidan keyin sodir etilgan boʻlsa; alohida hollarda ommaviy axborot vositalari yoki Internet orqali tarqatilganda)[30].	Maʼmuriy jarima BHMning 20 baravaridan 40 baravarigacha boʻladi. Jinoiy javobgarlik choralari: 200 BHMgacha jarima; OAV/Internet orqali eʼlon qilinganda — 200–400 BHM), majburiy ishlar yoki axloq tuzatish ishlari; kvalifikatsiya belgilari mavjud boʻlsa, 400 dan 600 BHMgacha jarima yoki 1 yildan 2 yilgacha ozodlikni cheklash.

[26] 100-modda. Oʻzbekiston Respublikasining Fuqarolik kodeksi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://lex.uz/docs/111181#159215

[27] Oʻzbekiston Respublikasi Maʼmuriy javobgarlik toʻgʻrisidagi kodeksining 40-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/97661

[28] Oʻzbekiston Respublikasi Jinoyat kodeksining 139-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/111457

[29] Oʻzbekiston Respublikasi Maʼmuriy javobgarlik toʻgʻrisidagi kodeksining 41-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/97661

[30] Oʻzbekiston Respublikasi Jinoyat kodeksining 140-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/111457

2.3.3. Yolg‘on axborot tarqatganlik uchun javobgarlik

Yolg‘on ma’lumot tarqatganlik uchun javobgarlik pandemiya davridagi feyklar to‘lqiniga javob chorasi sifatida joriy etilgan bo‘lib, ular asosan emlash, davolanish, pandemiya oqibatlari va boshqalarning xavf-xatarlari va oqibatlari bilan bog‘liq edi. Pandemiya allaqachon tugagan, biroq yolg‘on axborot tarqatganlik uchun javobgarlik hozirda asosan jurnalist va blogerlarga nisbatan keng qo‘llanilmoqda. Shu bilan birga, ma’lumki, kontent yaratuvchilarga nisbatan jinoiy javobgarlikning haddan tashqari keng asoslari va choralari sovituvchi ta’sirga ega — ya’ni jurnalistlar, OAV tahririyatlari, blogerlar o‘tkir mavzulardan qochishni boshlaydilar, iboralarni yumshatadilar, surishtiruvlar va tanqidiy materiallardan voz kechadilar, javobgarlikka tortilish xavfi tufayli maqolalarni tezroq o‘chiradilar va muhokamalarni yopadilar; o‘z-o‘zini senzura qilish darajasi ortadi. NNT vakillariga nisbatan ham shunday ta’sir bo‘lishi mumkin.

O‘zbekistonda yolg‘on ma’lumot tarqatganlik uchun javobgarlik ikki turda — ma’muriy va jinoiy javobgarlikda nazarda tutilgan. Quyidagi jadvalda biz qoidabuzarliklarning yuzaga kelishining huquqiy asoslari va yolg‘on ma’lumotlar tarqatilgan taqdirda qo‘llanilishi mumkin bo‘lgan javobgarlik choralarini ko‘rsatib o‘tdik.

Javobgarlik turlari	Qachon qo‘llanadi?	Javobgarlik choralari
Ma’muriy javobgarlik 	1. Shaxsning qadr-qimmatini kamsitishga yoki uni obro‘sizlantirishga olib keladigan yolg‘on axborotni, shu jumladan OAVda, internetda tarqatish[31]. 2. Jamoat tartibiga yoki xavfsizligiga tahdid soladigan yolg‘on axborotni, shu jumladan OAVda, internetda tarqatish[32]. BHMning 50 baravari yoki BHMning 50 baravaridan 100 baravarigacha miqdorda ma’muriy jarima (moddaning qismiga qarab)	Ma’muriy jarima BHMning 50 baravari yoki BHMning 50–100 baravari (moddaning qismiga qarab)
Jinoiy javobgarlik 	Shaxsning qadr-qimmatini kamsitishga yoki uni obro‘sizlantirishga olib keladigan yolg‘on axborotni tarqatish, shu jumladan ommaviy axborot vositalarida, internetda tarqatish, shunday harakatlar uchun ma’muriy jazo qo‘llanilganidan keyin sodir etilgan bo‘lsa[33]	150–200 BHMgacha jarima; 240–300 soatgacha majburiy ishlar yoki 2 yilgacha axloq tuzatish ishlari yoki 2–3 yilgacha ozodlikni cheklash;

2.3.4. «Nafrat tili» (Hate speech)

Markaziy Osiyo mamlakatlarida, shu jumladan O‘zbekistonda ham hate speech (nafrat nutqi) mavzusi, eng avvalo, milliy, irqiy, etnik yoki diniy adovat qo‘zg‘atishning jinoiy-huquqiy taqiqlanishi bilan bog‘liq. O‘zbekistonda bunday taqiq Jinoyat kodeksining 156-moddasi[34] «Milliy, irqiy, etnik yoki diniy adovatni qo‘zg‘atish»da amalga oshirilgan.

Modda ko‘rsatilgan belgilar bo‘yicha adovatni qo‘zg‘atish va qadr-qimmatni kamsitishga qaratilgan qasddan qilingan harakatlarni, shuningdek, bunday adovatni targ‘ib qiluvchi materiallarni tarqatish maqsadida tayyorlash, saqlash va tarqatishni qamrab oladi. Bu shuni

[31] O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi kodeksining 202-moddasi. Kodeks matni havola orqali mavjud: https://www.lex.uz/acts/97661

[32] O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi kodeksining 202-moddasi. Kodeks matni havola orqali mavjud: https://www.lex.uz/acts/97661

[33] O‘zbekiston Respublikasi Jinoyat kodeksining 244-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/111457

[34] O‘zbekiston Respublikasi Jinoyat kodeksining 156-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

anglatadiki, xavf zonasi nafaqat mualliflik matnida, balki boshqalarning materiallarini e'lon qilishda, sarlavhalar va illyustratsiyalarda, shuningdek, OAV tahririyati maydonchalarida yoki NNTning kontent tarqatuvchisi sifatidagi axborot resurslarida auditoriyaning izohlarida ham yuzaga keladi.

Alohida turdosh xavf — «urushni targ'ib qilish» (O'zbekiston Jinoyat kodeksining 150-moddasi[35]). Moddaning ta'sir doirasiga bir davlatning boshqasiga qarshi tajovuzini qo'zg'atish maqsadida g'oyalar yoki chaqiriqlar tarqatish kiradi; sanksiya 5 yildan 10 yilgacha ozodlikdan mahrum qilishni nazarda tutadi. Amaliy xulosa oddiy: nafrat tili yoki zo'ravonlikka da'vat qilish mumkin bo'lgan mavzularda imkon qadar betaraf taqdimot, umumlashtirish va stereotiplardan voz kechish, aniq iqtiboslar keltirish (haqoratli so'zlarni ko'paytirmasdan) va izohlarni tezda nazorat qilish kerak, shunda sizning resursingiz taqiqlangan materiallarni tarqatish kanaliga aylanmaydi.

2.3.5. Sharhlar uchun javobgarlik

Endi NNTlarning foydalanuvchilar tomonidan postlar ostida qoldiriladigan kontent uchun javobgarligi masalasiga batafsilroq to'xtalamiz. Sharhlar muhokama qilinayotgan maqolaga taalluqli bo'lmasligi mumkin, ammo sharhlar matnida noqonuniy kontent, haqorat, nafrat nutqi, boshqalarning shaxsiy ma'lumotlari, ma'lumotlarga putur yetkazuvchi, yolg'on ma'lumotlar bo'lishi xavfi mavjud. Sharhlar sharh muallifi va OAV tahririyati yoki bloger o'rtasida mas'uliyatni taqsimlash nuqtayi nazaridan muammoli bo'lishi mumkin.

Biroq OAV tahririyatlari, blogerlar, NNT vakillari «Axborotlashtirish to'g'risida»[36] gi qonunda to'g'ridan-to'g'ri belgilanganidek, taqiqlangan ma'lumotlarni joylashtirish uchun saytlar, bloglardan foydalanishga yo'l qo'ymasliklari shart. Shuning uchun moderatsiyaning[37] yo'qligi va murojaatlarni e'tiborsiz qoldirish xavflarni oshiradi.

Izoh muallifi va onlayn resurs egalari o'rtasidagi mas'uliyat chegarasi qayerdan o'tadi? Ommaviy axborot vositalari tahririyatlari va nodavlat notijorat tashkilotlari uchun muammoli sharh uchun javobgarlikka tortilish xavfi, agar uchta omildan kamida bittasi mavjud bo'lsa, keskin ortadi:

Muammoli izohni ma'qullash (mahkamlash, ajratib ko'rsatish, «auditoriya pozitsiyasi» sifatida ko'rsatish)

Moderatsiyaning yo'qligi (mas'ul shaxs yo'q, qoidalar yo'q, o'chirish yo'q)

Izohlardagi murojaatlarni e'tiborsiz qoldirish (aniq qoidabuzarlikni o'chirib tashlamaysiz, munosabatni qayd etmaysiz)

Muammoli sharhlar uchun javobgarlikdan qochish maqsadida quyidagilarni ishlab chiqish va joriy etish mumkin:

- Foydalanuvchilar uchun fikr bildirish qoidalari
- Premoderatsiya va moderatsiya ichki tartib-qoidalari

[35] O'zbekiston Respublikasi Jinoyat kodeksining 156-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

[36] «Axborotlashtirish to'g'risida»gi O'zbekiston Respublikasi Qonunining 12-moddasi. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/acts/82956

[37] Moderatsiya — bu foydalanuvchilar tomonidan e'lon qilinadigan kontentning sayt, ijtimoiy tarmoq yoki forum qoidalariga muvofiqligini nazorat qilish jarayonidir. Asosiy maqsad — xavfsizlikni ta'minlash, spam, haqorat va taqiqlangan materiallarni olib tashlash, shu orqali sayt obro'sini himoya qilishdir. U qo'lda (moderator) yoki avtomatik (algoritmlar) bo'lishi mumkin.

Foydalanuvchilar uchun fikr bildirish qoidalari — bu kontent yaratuvchining ehtimoliy muammoli fikrlar uchun mas'uliyatni taqsimlash bo'yicha ommaviy siyosati (pozitsiyasi). Bu qoidalarga kiritilishi kerak bo'lgan majburiy minimumlar quyidagilardir:

- Foydalanuvchilar uchun fikr bildirish qoidalari NNTning veb-sayti va ijtimoiy tarmoqlar hamda messenjerlardagi akkauntlaridagi barcha fikrlarga nisbatan qo'llaniladi.
- Izoh qoldirish orqali foydalanuvchi qoidalarga roziligini tasdiqlaydi va kontent uchun shaxsan javobgardir.
- Izohlarda haqoratlash va qadr-qimmatni kamsitish, kamsitish, adovat qo'zg'atish va zo'ravonlikka chaqirish, ekstremizm, urushni targ'ib qilish, pornografiya va giyohvand moddalar, yolg'on ma'lumotlar, shuningdek, fishing, spam, bezovta qiluvchi reklama, shaxsiy ma'lumotlar va shaxsiy yozishmalarni e'lon qilish, skrinshotlar, haqoratli so'zlar (so'kinish) taqiqlanadi.
- NNT qoidalarni buzuvchi fikrlarni o'chirib tashlash va foydalanuvchilarni bloklash huquqiga ega.
- NNT buzilishlar to'g'risidagi murojaatlarni ko'rib chiqadi va choralar ko'radi, shu jumladan olib tashlash va kirishni cheklash.

Sharhlash qoidalaridan tashqari, OAV yoki NNT tahririyati sharhlarni **moderatsiya qilishning ichki tartibini** ishlab chiqishi va qabul qilishi mumkin. Ushbu hujjatga quyidagi qoidalar kiritilishi lozim (minimal ro'yxat):

- Model belgilanadi — bu premoderatsiya yoki postmoderatsiya bo'ladimi? Xavf darajasi yuqori mavzular (nizo, zo'ravonlik, urush, feyklar, shaxsiy ma'lumotlar) uchun kuchaytirilgan rejim (masalan, premoderatsiya yoki sharhlarni cheklash) o'rnatiladi.
- Muddatlar belgilanadi: yangi sharhlar qanchalik tez tekshiriladi va shikoyatlarga qanchalik tez javob qaytarasiz (masalan, ish kuni davomida yoki yuqori xavf darajasidagi mavzular uchun bir necha soat ichida).
- Taqiqlangan kontentga ega bo'lgan va Sharh qoldirish qoidalarini buzadigan izohlar o'chirilishi (yoki yashirilishi), takroriy qoidabuzarliklarga yo'l qo'ygan foydalanuvchilar esa bloklanishi belgilanadi. Qarorlar yagona mezonlar asosida qabul qilinadi.
- Bahsli yoki potensial xavfli holatlar uchun muammoli sharhlarni qayd etib borish ko'zda tutiladi. Bu sharh havolasini, sanasi va vaqtini saqlab qo'yish kerakligini anglatadi. Muammoli sharhlarning skrinshotlari faqat ichki arxiv uchun olinadi va tarqatilmaydi.
- Qaysi holatlar rahbariyatga yoki yuristga majburiy tartibda taqdim etilishi aniqlanadi. Bular — adovat qo'zg'atish belgilari, zo'ravonlikka da'vatlar, ekstremizm, shaxsiy ma'lumotlarni e'lon qilish, yolg'on axborot, giyohvand moddalar targ'iboti va boshqa taqiqlangan kontent mavjud bo'lgan sharhlardir.
- Muammoli sharhlarni "auditoriya pozitsiyasi" sifatida qadash, ulardan iqtibos keltirish yoki qayta e'lon qilish taqiqlanadi. Har qanday sharhni alohida ajratib ko'rsatish qo'shimcha mas'uliyat omili sifatida qaraladi.

2.3.6. Kontent bo‘yicha onlayn platformalar (ijtimoiy tarmoqlar) qoidalari

Onlayn platformalarning kontent qoidalari masalasiga alohida to‘xtalib o‘tamiz. Yuqorida biz O‘zbekiston milliy qonunchiligiga muvofiq raqamli muhitda kontent uchun javobgarlik yuzaga kelishi mumkin bo‘lgan muammoli vaziyatlarni tahlil qildik. Ammo onlayn platformalar ham o‘z qoidalariga ko‘ra ishlaydi. Bu alohida xavf, chunki kontent bloklanishi, tanbeh berilishi, monetizatsiya faolsizlantirilishi yoki hisob tugatilishi mumkin. Har bir onlayn platforma o‘zining ommaviy va bajarilishi majburiy bo‘lgan siyosatiga ega.

Onlayn platformalar siyosati nuqtayi nazaridan qaysi kontent muammoli hisoblanadi?

- Yuqorida aytib o‘tilganidek, nafrat tili (gumanizatsiyadan mahrum etish, kamsitish, diskriminatsiya yoki zo‘ravonlikka da’vat qilish);
- Xavfli kontent va zo‘ravonlikka da’vatlar, ekstremistik va terroristik kontent;
- Nozik mavzularda (salomatlik, xavfsizlik, inqirozlar) dezinformatsiya;
- Bulling (tazyiq o‘tkazish), ta’qib qilish yoki tahdidlar;
- Shaxsiy daxlsizlikni buzadigan shaxsiy ma’lumotlar va postlar.

Onlayn platformalar siyosati:

Meta (Facebook, Instagram) Hateful Conduct

https://transparency.meta.com/policies/community-standards/hateful-conduct/?utm_source=chatgpt.com

YouTube Hate Speech Policy

https://support.google.com/youtube/answer/2801939?hl=en&utm_source=chatgpt.com

TikTok

https://ads.tiktok.com/help/category?id=535nt8Z20sG4lW62MZPJvL

Telegram

https://telegram.org/moderation

Amaliy xulosa: nashr siyosatida nafaqat O‘zbekistonning amaldagi qonunchiligiga, balki onlayn platformalarning aniq belgilangan taqiqlangan hududlariga, ayniqsa kamsitish, zo‘ravonlik, soxta xabarlar va shaxsiy ma’lumotlar masalalariga oid mavzularga ham e’tibor qarating. Bahsli vaziyatlarda xavflarni kamaytirish, muammolarni keltirib chiqarmaydigan, ammo ijtimoiy ahamiyatga ega mavzularni chetlab o‘tmaydigan kontentni nashr etish xavfsizroqdir.

2.4. Mualliflik huquqlari va NNT

O‘zbekiston Respublikasining «Mualliflik huquqi va turdosh huquqlar to‘g‘risida»gi Qonuni (O‘RQ-42, 20.07.2006-y.) mualliflik huquqi «yaratish fakti tufayli» yuzaga kelishini va ro‘yxatdan o‘tkazish yoki boshqa rasmiyatchiliklarni talab qilmasligini belgilaydi.

Raqamli muhitda Internet tarmog‘ida e’lon qilish «barchaning e’tiboriga yetkazish» bo‘lib, unda foydalanuvchilar «o‘zlari xohlagan joydan va istalgan vaqtda» kirishlari mumkin. Bu amal muallif yoki mualliflik huquqi egasining eksklyuziv huquqlariga tegishli (ya’ni ruxsat/litsenziya talab qiladi), shuningdek, ko‘paytirish va tarqatishga ham taalluqlidir.

O‘zbekiston mualliflik huquqini himoya qilishning xalqaro tizimiga kiritilgan. Mamlakat 2005-yil 19-apreldan boshlab Adabiyot va san’at asarlarini muhofaza qilish bo‘yicha Bern konvensiyasida (Bern konvensiyasi), shuningdek, 2019-yil 17-iyuldan boshlab Butunjahon intellektual mulk tashkilotining «internet shartnomalari» — BIMTning mualliflik huquqi to‘g‘risidagi shartnomasi (WCT) va BIMTning ijrolar va fonogrammalar to‘g‘risidagi shartnomasi (WPPT) da ishtirok etmoqda.

Bern konvensiyasi a’zo mamlakatlarning mualliflari va asarlari uchun milliy muhofaza rejimi tamoyilini, mualliflik huquqini yaratish fakti bo‘yicha avtomatik himoya qilishni va mualliflik huquqini himoya qilishning minimal muddatini 50 yil davomida mustahkamlaydi. BIMT shartnomalari mualliflik huquqlarini himoya qilishni raqamli muhitga moslashtiradi: jumladan, texnik choralarni (masalan, himoya/shifrlashni chetlab o‘tish) va huquqlarni boshqarish ma’lumotlarini (rights management information) himoya qilish.

Qonunning 5-moddasiga muvofiq, «Mualliflik huquqi ijodiy faoliyat natijasi bo‘lgan fan, adabiyot va san’at asarlariga, asarning maqsadi va qadr-qimmati, shuningdek uning ifodalanish usulidan qat’i nazar, tatbiq etiladi.» Mualliflik huquqi ham e’lon qilingan (nashr etilgan, biron-bir usulda, shu jumladan internet tarmog‘ida tarqatilgan), ham biron-bir obyektiv shaklda bo‘lgan e’lon qilinmagan asarlarga nisbatan tatbiq etiladi.

Mualliflik huquqi muallifning shaxsiy nomulkiy va mulkiy huquqlaridan iborat. Shaxsiy nomulkiy huquqlar begonalashtirilmaydi, muddatsiz amal qiladi va quyidagilarni o‘z ichiga oladi:

Mulkiy huquqlar huquqlarning keng ro‘yxatini va mualliflik asaridan har qanday formatda foydalanish usulini, shu jumladan asarni boshqa formatlarga tarjima qilish va qayta ishlashni o‘z ichiga oladi. Mulkiy huquqlar muallif (hammualliflar) ning butun umri davomida va muallif (hammualliflar) vafotidan keyin 70 yil davomida amal qiladi.

Huquqlar turi	Toifa	Himoya hajmi	Buzilish usullari
Shaxsiy nomulkiy huquqlar	Mualliflik huquqi	Asar muallifi sifatida e'tirof etilmoq	Asardan muallif nomini ko'rsatmasdan nusxa ko'chirish va tarqatish yoki mualliflikni o'zlashtirish (plagiat)
	Muallif nomiga bo'lgan huquq	Asardan foydalanilganda muallifning ismi yoki uning taxallusi ko'rsatilishi shart	Asarni muallifning roziligisiz yoki boshqa shaxs nomi ostida yoxud muallif nomini buzib ko'rsatgan holda nashr etish va tarqatish, muallifning taxallusini oshkor qilish
	Mualliflik huquqida e'lon qilish huquqi	Asarni har qanday shaklda ommaga e'lon qilish yoki e'lon qilishga ruxsat berish huquqi, shu jumladan asarni ommaga e'lon qilishdan voz kechish (asarni qaytarib olish) huquqi.	Muallifning e'lon qilinmagan asari nusxalarini uning roziligisiz chop etish
	Muallif obro'sini himoya qilish huquqi	Asarni, shu jumladan uning nomini muallifning sha'ni va qadr-qimmatiga putur yetkazishi mumkin bo'lgan har qanday buzib ko'rsatishdan yoki boshqa har qanday tajovuzdan himoya qilish huquqi	Asarni muallifning roziligisiz buzib ko'rsatish va tahrir qilish
Mulkiy huquqlar	Ko'paytirish huquqi	Asarning raqamli yoki jismoniy nusxalarini (nusxalarini) yaratish	Muallif ruxsatisiz asarni yaratish va nusxa ko'chirish (qaroqchilik)
	Tarqatish huquqi	Asarning raqamli yoki jismoniy nusxalarini tarqatish va sotish, shu jumladan ijaraga berish huquqi	Muallif ruxsatisiz sotish, ijaraga berish (kitoblar, musiqa yoki filmlarning noqonuniy savdosi)
	Ommaviy namoyish va ijro etish huquqi	Ommaviy ijro va omma oldida namoyish qilish	Muallif ruxsatisiz jamoat joylarida asarni namoyish qilish yoki ommaviy ijro etish
	Qayta ishlash huquqi	Asl nusxa asosida yangi (hosilaviy) asarlar yaratish	Muallif ruxsatisiz asarni boshqa formatlarga qayta ishlash, chet tillariga tarjima qilish, ssenariy, pyesa, sahna ko'rinishiga moslashtirish, musiqiy kaver va remikslar yaratish
	Omma e'tiboriga etkazish	Raqamli nusxalarni Internetda tarqatish	Asarning raqamli nusxalarini muallifning ruxsatisiz raqamli muhitga yuklash va tarqatish

Muallifga (huquq egasiga) mualliflik haqini olish huquqi kafolatlanadi. Qonunchilik asarlarning aniq turlari va ulardan foydalanish usullari uchun mualliflik haqining eng kam stavkalarini belgilaydi.

MUHIM MA’LUMOT

Mualliflik huquqining vujudga kelishi va o‘tkazilishining asosiy usuli mualliflik huquqi obyekti, undan foydalanish usullari va mualliflik haqining miqdorlari ko‘rsatilgan mualliflik shartnomasini tuzishdir.

O‘zgalar asarlaridan foydalanish qoidalari

Internet tarmog‘i, ijtimoiy tarmoqlar, messenjerlar va veb-saytlarda kontentning keng tarqalishi mualliflik huquqi egalarining ruxsatisiz foydalanilishi mumkin bo‘lgan o‘zgalar kontentiga kirish imkonini beradi. Internetdagi materiallardan foydalanish erkin emas, ularni mualliflar va (yoki) huquq egalarining roziligisiz hamda haq to‘lamasdan takrorlash mumkin emas. Har bir matn yoki fotosurat, audio yoki video kontentning muallifi yoki mualliflik huquqi egasi bo‘ladi. Saytlar va ijtimoiy tarmoqlardagi materiallardan foydalanish siyosatini diqqat bilan o‘qib chiqish zarur. **Ochiq akkauntda matn yoki fotosuratlarni e’lon qilish ulardan uchinchi shaxslar foydalanishi va e’lon qilishi mumkinligini anglatmaydi.**

Umumiy qoidaga ko‘ra, mutlaq mualliflik huquqlari boshqa jismoniy shaxslar yoki kompaniyalarga tegishli bo‘lgan asarlardan foydalanmoqchi bo‘lgan shaxs mutlaq huquqlar egasining ruxsatini olishi shart («Mualliflik huquqi va turdosh huquqlar to‘g‘risida»gi qonunning 19-moddasi). Ruxsatnoma mualliflik shartnomasini tuzish orqali yozma shaklda rasmiylashtirilishi (Qonunning 38-moddasi) va mualliflik haqi to‘lanishi lozim.

Internetda boshqalarning kontentidan erkin foydalanishga misollar

Mualliflik huquqi obyektlaridan quyidagi majburiy shartlarga rioya etgan holda, huquq egasining alohida ruxsatisiz cheklangan hajmda foydalanishga yo‘l qo‘yiladi:

- **muallif va manba (va/yoki agar mavjud bo‘lsa, huquq egasi) ko‘rsatilishi shart;**
- **foydalanish maqsaddan kelib chiqqan holda oqlanadigan hajmda bo‘lishi kerak;**
- **foydalanish asardan normal foydalanishga zarar yetkazmasligi va muallifning qonuniy manfaatlariga putur yetkazmasligi lozim.**

Quyidagi hollarda:

- ilmiy, tadqiqot, munozara, tanqidiy va reklama bilan bog‘liq bo‘lmagan axborot maqsadlarida e’lon qilingan asarlardan parchalar keltirish;
- joriy siyosiy, iqtisodiy, ijtimoiy va diniy masalalar bo‘yicha chop etilgan materiallarni muallif/huquq egasining maxsus taqiqi bo‘lmagan taqdirda takrorlash;
- omma oldida so‘zlangan siyosiy nutqlar, murojaatlar, ma’ruzalar va shunga o‘xshash chiqishlarni axborot maqsadiga mos hajmda takrorlash;
- joriy voqealar davomida ko‘rilgan yoki eshitilgan asarlardan axborot maqsadi bilan oqlangan hajmda foydalanish.

Boshqalarning kontentidan foydalanishda "qizil bayroqlar"

Agar quyidagi belgilardan birortasi mavjud bo'lsa, kontentdan erkin foydalanish uchun qo'shimcha tekshiruv o'tkazish va/yoki muallif yoki huquq egasidan ruxsat olish talab etiladi:

Reklama maqsadi yoki targ'ibot

Agar material reklama, mahalliy reklama, homiylik kontenti, PR nashrlari yoki sotuv/obunalarni rag'batlantirish uchun ishlatilsa.

O'ta katta hajmdagi o'zlashtirish

Matnning katta qismlarini nusxalash, to'liq fotoreportaj/to'liq video/to'liq audioyozuvni e'lon qilish «maqsadga muvofiq hajm»dan tashqariga chiqadi va mualliflik huquqining buzilishi xavfini tug'diradi.

To'g'ri atributsiyaning yo'qligi (manbani ko'rsatmaslik)

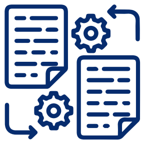
Muallif, manba ko'rsatilmagan, havola berilmagan yoki to'liq bo'lmagan ma'lumotlar ko'rsatilgan bo'lsa, hatto foydalanishning o'zi maqbul bo'lishi mumkin bo'lgan hollarda ham da'vo uchun asos bo'ladi.

Muallif + manba + sana + havola (mavjud bo'lsa)

Atributning oltin qoidasi

Muallif/huquq egasining maxsus taqiqi mavjudligi

Agar birlamchi manba qayta chop etish/nashr etishni to'g'ridan to'g'ri taqiqlasa (saytda, material oxirida, foydalanish shartlarida), joriy maqolalarni qayta chop etish bandi bo'yicha erkin foydalanishga tayanish mumkin emas.



Cheklangan hajmda iqtibos keltirish o'rniga qayta ishlash

Tarjima qilish, moslashtirish, montaj qilish, musiqa qo'shish, «hosila» kontent yaratish, hatto asl material axborot maqsadlarida cheklangan miqdorda ishlatilgan bo'lsa ham, alohida ruxsat talab qilishi mumkin.

MUHIM!

© mualliflik belgisi qo'yilishi, o'zlashtirilgan manba (masalan, boshqa OAV yoki sayt) ko'rsatilishi yoki unga havola qilinishi, mualliflik asaridan notijorat maqsadlarda foydalanish mualliflar yoki huquq egalarining noqonuniy foydalanish bo'yicha da'volaridan ozod etmaydi.

Mualliflik huquqini himoya qilish usullari

Agar muallif yoki huquq egasi o'zining mualliflik huquqlari buzilgan deb hisoblasa, ularni himoya qilish uchun huquqbuzarga (yaxshisi, yozma ravishda) noqonuniy foydalanishni to'xtatish talabi bilan murojaat qilishga haqli. Agar huquqbuzar talablarni bajarishdan bosh tortsa, muallif (huquq egasi) fuqarolik (agar taraflardan biri jismoniy shaxs bo'lsa) yoki iqtisodiy ishlar bo'yicha (agar ikkala taraf ham yuridik shaxs bo'lsa) sudiga quyidagi da'vo bilan murojaat qilishga haqli:

- huquqlarni tan olish;

- huquq buzilgunga qadar mavjud boʻlgan holatni tiklash va huquqni buzuvchi yoki uni buzish xavfini tugʻdiruvchi harakatlarni toʻxtatish;
- agar huquq egasining huquqi buzilmaganida, huquq egasi fuqarolik muomalasining odatdagi sharoitlarida olishi mumkin boʻlgan olinmagan daromadlar miqdorida zararni qoplash. Agar huquqbuzar mualliflik huquqi yoki turdosh huquqlarni buzish oqibatida daromad olgan boʻlsa, huquq egalari boshqa zararlar bilan bir qatorda boy berilgan foydaning oʻrnini ushbu daromadlardan kam boʻlmagan miqdorda qoplashni talab qilishga haqli;
- zarar yetkazilganligidan qat’i nazar, ish muomalasi odatlarini hisobga olgan holda, huquqbuzarlikning xususiyati va huquqbuzarning aybdorlik darajasidan kelib chiqib, zararni qoplash oʻrniga bazaviy hisoblash miqdorining yigirma baravaridan ming baravarigacha miqdorda kompensatsiya toʻlash;

Muallif (yoki huquq egasi) oʻz huquqlari buzilgan taqdirda, huquqbuzardan ma’naviy zararni qoplashni talab qilishga haqli. Qonunchilikda mualliflik huquqlarini buzganlik uchun ma’muriy va jinoiy javobgarlik belgilangan.

Javobgarlik turlari	Qachon qoʻllanadi	Javobgarlik choralari
MJtK 177^{1}-moddasi. Mualliflik huquqi va turdosh huquqlarni buzish	Asarlardan yoki turdosh huquqlar obyektlaridan qonunga xilof ravishda foydalanish, xuddi shuningdek asarlarning yoki turdosh huquqlar obyektlarining kontrafakt nusxalarini koʻpaytirish, tarqatish, barchaning e’tiboriga yetkazish **Mulkiy huquqlar** yoxud asarlar yoki turdosh huquqlar obyektlari nusxalarida ularni tayyorlaganlar, ishlab chiqarilgan joylari, shuningdek mualliflik huquqi va turdosh huquqlar egalari toʻgʻrisida yolgʻon ma’lumotlar koʻrsatish **Nomulkiy huquqlar**	Birlamchi qoidabuzarlik Fuqarolar uchun — BHMning 1 baravaridan 5 baravarigacha miqdorda jarima Mansabdor shaxslar uchun — BHMning 5 baravaridan 10 baravarigacha miqdorda jarima. Yil davomida takroriy qoidabuzarlik Fuqarolar uchun — BHMning 5 baravaridan 10 baravarigacha miqdorda jarima Mansabdor shaxslar uchun — BHMning 10 baravaridan 20 baravarigacha miqdorda jarima. Kontrafakt mahsulotlar, materiallar va uskunalar musodara qilinadi.
149-modda. Mualliflik yoki ixtirochilik huquqlarini buzish	Intellektual mulk obyektlariga nisbatan mualliflik huquqini oʻzlashtirish, hammualliflikka majburlash, xuddi shuningdek ushbu obyektlar toʻgʻrisidagi ma’lumotlarni ular rasman roʻyxatdan oʻtkazilgunga yoki e’lon qilingunga qadar muallifning roziligisiz oshkor qilish **Nomulkiy huquqlar**	BHMning 50 baravaridan 70 baravarigacha jarima Muayyan huquqdan 5 yilgacha mahrum qilish 360 soatgacha boʻlgan majburiy ishlar 2 yilgacha ozodlikni cheklash
149^{1}-modda. Mualliflik huquqi va turdosh huquqlarni buzish	Asarlardan yoki turdosh huquqlar obyektlaridan qonunga xilof ravishda foydalanish, shuningdek asarlarning yoki turdosh huquqlar obyektlarining kontrafakt nusxalarini takrorlash, tarqatish, barchaning e’tiboriga yetkazish, ularning tayyorlovchilari, tayyorlangan joyi, shuningdek mualliflik huquqi va turdosh huquqlar egalari toʻgʻrisidagi yolgʻon ma’lumotlar bilan nusxalar tayyorlash, agar bu ancha miqdorda zarar yetkazgan boʻlsa **Mulkiy huquqlar**	50 dan 100 BHMgacha jarima 2 yilgacha axloq tuzatish ishlari 2 yilgacha ozodlikni cheklash 2 yilgacha ozodlikdan mahrum qilish

Raqamli muhitda mualliflik huquqi obyektlaridan foydalanishni cheklash mexanizmlari

Oʻzbekiston Respublikasining «Axborotlashtirish toʻgʻrisida»gi qonuni boshqa shaxslarga tegishli boʻlgan intellektual mulk obyektlaridan foydalanishni taqiqlaydi. Veb-saytning va (yoki) veb-sayt sahifasining yoxud boshqa axborot resursining egalari, shu jumladan blogerlar oʻz veb-saytlaridan va (yoki) veb-saytlarining sahifalaridan yoxud Internet jahon axborot tarmogʻidagi boshqalarning mualliflik asarlaridan huquq egasining roziligisiz foydalanilishiga yoʻl qoʻymasliklari shart.

Oʻzbekiston Respublikasi Vazirlar Mahkamasining 2018-yil 5-sentyabrdagi «Internet jahon axborot tarmogʻida axborot xavfsizligini taʼminlashni takomillashtirish chora-tadbirlari toʻgʻrisida»gi 707-sonli qarori (707-sonli qaror) mualliflik huquqini buzadigan, tarqatilishi cheklangan onlayn kontentni olib tashlash mexanizmini nazarda tutadi. 707-sonli qaror bilan Raqamli texnologiyalar vazirligi huzuridagi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat boʻyicha «Oʻzkomnazorat» inspeksiyasiga veb-saytlar va ijtimoiy tarmoqlardagi maʼlumotlarni oʻchirish toʻgʻrisida koʻrsatmalar berish vakolati berildi.

Huquq egasi (muallif) «Oʻzkomnazorat»ga mualliflik huquqi obyektlaridan noqonuniy foydalanish holatlari toʻgʻrisida ariza bilan murojaat qilishga haqli. «Oʻzkomnazorat» veb-sayt, veb-sayt sahifasi yoki axborot resursi egasiga noqonuniy materiallarni 24 soat ichida olib tashlash zarurligi toʻgʻrisida xabarnoma yuboradi.

Agar axborot koʻrsatilgan muddatda oʻchirib tashlanmasa, «Oʻzkomnazorat» quyidagi choralarni koʻrish huquqiga ega:

Tegishli ijtimoiy tarmoq yoki messenjer maʼmuriyatiga toʻgʻridan-toʻgʻri murojaat qilib, maʼlumotni oʻchirishni talab qilish.

Noqonuniy materiallar joylashtirilgan veb-sayt yoki veb-sayt sahifasiga kirishni cheklash.

Platforma maʼmuriyatiga nisbatan taqiqlangan kontentni olib tashlash talabi bilan sudga daʼvo arizasi bilan murojaat qilishi mumkin.

Raqamli muhitda mualliflik huquqlari buzilganligi toʻgʻrisidagi ariza intellektual mulk sohasidagi nizolarni sudgacha koʻrib chiqish boʻyicha vakolatli organ — Oʻzbekiston Respublikasi Adliya vazirligining Intellektual mulk departamentiga yuborilishi mumkin.

Ijtimoiy tarmoqlar va raqamli platformalarda mualliflik huquqlarini himoya qilish mexanizmlari

Internetda huquqbuzarliklar ommaviy ravishda sodir boʻladi va oflayn muhitdan farqli oʻlaroq, katta xarajatlarni talab qilmaydi. Eng koʻp uchraydigan qoidabuzarliklar — birovning mualliflik kontentini noqonuniy nusxalash va tarqatish, plagiat, asarlarni qayta ishlash va ulardan tijorat maqsadlarida foydalanishdir.

Aksariyat raqamli platformalar va ijtimoiy tarmoqlar mualliflik huquqi buzilishi haqida shikoyat qilish mexanizmini taqdim etadi. Mualliflik huquqi egalari kontent joylashtirilgan sayt yoki platforma egasiga da'vo yuborishi va mualliflik huquqi buzilishi haqida bildirishnoma yuborishi mumkin.

Shikoyat platforma tomonidan taqdim etilgan shaklda yuboriladi va quyidagi ma'lumotlarni ko'rsatishni talab etadi:

- boshqa mualliflik asarlari joylashtirilgan havolalar;
- muallif yoki huquq egasining mualliflik huquqi obyekti bo'yicha huquqlarini tasdiqlovchi hujjat (mualliflik shartnomasi, mualliflik huquqini ro'yxatdan o'tkazish to'g'risidagi guvohnoma;
- muallif va mualliflik huquqi egasining aloqa ma'lumotlari;
- agar shikoyat huquq egasining vakili tomonidan taqdim etilayotgan bo'lsa, ishonchnoma.

Qidiruv tizimlarida matn yoki tasvir bo'yicha qidiruv, ijtimoiy tarmoqlar monitoringi, havolalar va eslatmalarni tekshirish yoki o'xshash mavzudagi saytlarni ko'rib chiqish mualliflik huquqi buzilishlarini aniqlash imkonini beradi;

Qoidabuzarlikni aniqlashda yordam beradigan ayrim maxsus avtomatik vositalar:

Google Image Search
internetdagi tasvir nusxalarini qidirish imkonini beruvchi bepul vosita

Copyscape
matn materiallarida plagiatni aniqlash uchun xalqaro xizmat. Kengaytirilgan imkoniyatlarga ega bepul va pullik versiyalar mavjud

Pixsy
tasvir bo'yicha qidirish funksiyasiga ega fotosuratlar platformasi

2.5. Onlayn xayriya aksiyalari va yig'imlari

2.5.1. Onlayn xayriya faoliyatining umumiy tavsifi va davlatning huquqiy yondashuvi

Onlayn muhitda, shu jumladan ijtimoiy tarmoqlar, messenjerlar, saytlar va raqamli platformalarda amalga oshiriladigan xayriya aksiyalari va mablag' yig'ish O'zbekiston Respublikasida huquqiy tartibga solishning mustaqil turini tashkil etmaydi. Qonunchilik texnologik betaraflik tamoyilidan kelib chiqadi, unga ko'ra axborotni tarqatish va xayriyalarni jalb qilish usuli yuzaga keladigan huquqiy munosabatlarning huquqiy tabiatini o'zgartirmaydi. Onlayn-format faqat xayriya faoliyatini amalga oshirishning texnik kanali sifatida qaraladi, unga nisbatan amaldagi qonunchilikning umumiy normalari to'liq qo'llaniladi.

Onlayn mablag' yig'ishni to'g'ridan-to'g'ri tartibga soluvchi maxsus qonunning yo'qligi huquqiy bo'shliq mavjudligini anglatmaydi. Aksincha, onlayn xayriya aksiyalari xayriya, nodavlat notijorat tashkilotlari to'g'risidagi qonunchilik, fuqarolik huquqi, moliyaviy nazorat me'yorlari va ma'muriy javobgarlik to'g'risidagi nizomlarni o'z ichiga olgan keng qamrovli tartibga solinadi. Aynan ushbu hujjatlarning birgalikda qo'llanilishi onlayn xayriya faoliyatining huquqiy rejimini shakllantiradi va NNTlar uchun yo'l qo'yiladigan xatti-harakatlar chegarasini belgilaydi.

2.5.2. Xayriya onlayn-aksiyalarini oʻtkazishning normativ-huquqiy bazasi

Onlayn xayriya yigʻimlarini huquqiy tartibga solish quyidagi normativ-huquqiy hujjatlar majmuiga asoslanadi.

Oʻzbekiston Respublikasining «Homiylik toʻgʻrisida»gi Qonuni ushbu sohadagi tizimni tashkil etuvchi hujjat hisoblanadi. U xayriya faoliyatining asosiy tamoyillarini mustahkamlaydi, ular ham oflayn, ham onlayn formatlarga bir xil darajada tatbiq etiladi. Xayriya ixtiyoriy faoliyat sifatida taʼriflanadi, bu esa mablagʻ yigʻishda har qanday majburlash, yashirin bosim yoki manipulyatsiya shakllarini istisno etadi. Onlayn yigʻimlar uchun bu auditoriyada ishtirok etish majburiyati hissini uygʻotish yoki xayriyalarni boshqa toʻlovlar bilan niqoblash mumkin emasligini anglatadi.

Qonunning 3 va 4-moddalariga muvofiq xayriya ixtiyoriylik asosida amalga oshiriladi, uning subyektlari esa, shu jumladan, nodavlat notijorat tashkilotlari hisoblanadi. 6-7-moddalar xayriya faoliyatini amalga oshirish, jumladan, xayriya mablagʻlarini yigʻish shakllari va tartibini belgilaydi, 21-modda esa belgilangan tartibni buzganlik, jumladan, mablagʻlardan maqsadsiz foydalanganlik va shaffoflik tamoyillarini buzganlik uchun javobgarlikni mustahkamlaydi.

Oʻzbekiston Respublikasining «Nodavlat notijorat tashkilotlari toʻgʻrisida»gi Qonuni NNT faoliyatining institutsional doiralarini belgilab, onlayn xayriya faoliyatining huquqiy rejimini toʻldiradi. Asosiy tamoyil ustav shartlanganligidir. NNT xayriya aksiyalari va mablagʻlar yigʻishni faqat oʻz ustavida belgilangan maqsad va vazifalar doirasida oʻtkazishga haqli. Ustav faoliyati bilan bogʻliq boʻlmagan onlayn yigʻim, uning ijtimoiy foydali xususiyatidan qatʼi nazar, qonunchilikni buzish sifatida malakalanishi mumkin.

NNT toʻgʻrisidagi qonunda, shuningdek, moliyaviy hisobni yuritish, moliyalashtirish manbalarining shaffofligini taʼminlash va vakolatli davlat organlariga hisobot taqdim etish majburiyati mustahkamlangan. Ushbu talablar barcha xayriyalarga, jumladan, ijtimoiy tarmoqlar va raqamli platformalar orqali olingan xayriyalarga, ularning hajmi va yigʻilish muddatidan qatʼi nazar, tatbiq etiladi. Shunday qilib, hatto qisqa muddatli yoki bir martalik onlayn aksiyalar ham moliyaviy hisobdorlik rejimiga tushadi.

Oʻzbekiston Respublikasining «Jinoiy yoʻl bilan olingan daromadlarni legallashtirishga qarshi kurashish toʻgʻrisida»gi Qonuni NNTlarga moliyaviy operatsiyalarni amalga oshiruvchi subyektlar sifatida tatbiq etiladi. Onlayn yigʻimlar kontekstida bu rasmiy bank hisobvaraqlaridan foydalanishning majburiyligini, moliyaviy monitoring tartib-qoidalariga rioya qilishni va anonim yoki shubhali mablagʻ manbalarini jalb qilishga yoʻl qoʻymaslikni anglatadi.

Oʻzbekiston Respublikasining Maʼmuriy javobgarlik toʻgʻrisidagi kodeksi pul mablagʻlarini qonunga xilof ravishda toʻplash, xayriya mablagʻlaridan maqsadli foydalanmaslik, majburiy hisobotlarning mavjud emasligi va xayriya qiluvchilarni chalgʻitish uchun javobgarlik choralarini belgilaydi.

Qoʻshimcha ravishda, **Oʻzbekiston Respublikasining 2025-yil 21-avgustdagi OʻRQ-1083-sonli Qonuni** bilan kiritilgan oʻzgartirishlarni inobatga olish lozim, ular bilan:

- jismoniy shaxslarga faqat oʻzi yoki yaqin qarindoshlari uchun xayriya mablagʻlarini yigʻishga ruxsat beriladi;

- uchinchi shaxslar foydasiga mablag‘ yig‘ishga faqat rasmiy huquqiy maqomga ega bo‘lgan tashkilotlar orqali yo‘l qo‘yiladi;
- xayr-ehsonlarni naqd pulda to‘plashda faqat shaffof, plombalangan qutilardan foydalanishga yoki mablag‘larni bank hisob raqamlariga o‘tkazishga yo‘l qo‘yiladi.

Amaldagi qonunchilikni tahlil qilish shuni ko‘rsatadiki, onlayn muhitda xayriya aksiyalari va mablag‘ yig‘ish huquqiy maydondan tashqarida emas. Aksincha, ular NNTdan yuqori darajadagi huquqiy ong, moliyaviy intizom va ommaviy mas’uliyatni talab qiladigan kompleks tartibga solinadi. Aynan qonunchilik bazasini tizimli tushunish nodavlat notijorat tashkilotlariga nafaqat huquqiy xavf-xatarlarni minimallashtirish, balki donorlar, davlat va umuman jamiyat bilan barqaror, ishonchli munosabatlarni o‘rnatish imkonini beradi.

2.5.3. Onlayn xayriya aksiyalari va mablag‘ yig‘ishning soliq oqibatlari

Nodavlat notijorat tashkilotlari xayriya aksiyalari va onlayn mablag‘ yig‘ishni tashkil etishda xayriya faoliyatining barcha ishtirokchilari: xayriya qiluvchi, xayriya tashkiloti va yordam oluvchi uchun soliq oqibatlarini hisobga olishlari zarur.

Xayriya jamg‘armasi (NNT) uchun. Homiylik jamg‘armasiga xayriya tariqasida kelib tushadigan pul mablag‘lari maqsadli tushumlar jumlasiga kiradi va ulardan qat’iy belgilangan maqsadda foydalanish va alohida hisob yuritish sharti bilan soliq solinmaydi (O‘zbekiston Respublikasi Soliq kodeksining 48, 58-moddalari va 318-moddasi 1-bandi 1-qismi). Xayriyalarni, shu jumladan onlayn platformalar orqali olish faktining o‘zi NNT uchun soliq majburiyatini tashkil etmaydi.

Yuridik shaxslar — xayriya qiluvchilar uchun. Korxonalar tomonidan xayriya jamg‘armalariga o‘tkaziladigan xayriya yordami summalari, yordam shaklidan qat’i nazar, foyda solig‘ini hisoblab chiqarishda chegirilmaydigan xarajatlar deb e’tirof etiladi (Soliq kodeksining 317-moddasi 7-bandi). Metsenatlik yordami, shuningdek, qonun hujjatlarida belgilangan ayrim ijtimoiy ahamiyatga molik yo‘nalishlar uchun istisnolar nazarda tutilgan.

Jamg‘arma orqali yordam oluvchi jismoniy shaxslar uchun. Jismoniy shaxs tomonidan xayriya jamg‘armasidan olingan mablag‘lar boshqa daromad sifatida kvalifikatsiya qilinadi, biroq agar ularning summasi soliq davri mobaynida 15 mln so‘mdan oshmasa, jismoniy shaxslardan olinadigan daromad solig‘i solinmaydi (Soliq kodeksining 377-moddasi 1-bandi va 378-moddasi 20-bandi). Ko‘rsatilgan limitdan oshib ketganda, soliq faqat oshgan summadan ushlab qolinadi.

Mablag‘lar jismoniy shaxsga to‘g‘ridan-to‘g‘ri o‘tkazilganda. Agar xayriya yordami xayriya jamg‘armasini chetlab o‘tib, to‘g‘ridan-to‘g‘ri jismoniy shaxsga (masalan, uning shaxsiy bank kartasiga) o‘tkazilsa, olingan mablag‘lar boshqa daromad sifatida to‘lov manbayida soliqqa tortiladi (Soliq kodeksining 377-moddasi 15-bandi va 387-moddasi 1-qismining 4-bandi).

Soliq qonunchiligi nuqtai nazaridan xayriya qilishning eng xavfsiz va shaffof shakli — bu rasmiy bank hisob raqamlaridan foydalangan holda va keyinchalik hisobot berish orqali ro‘yxatdan o‘tgan xayriya jamg‘armalari va NNTlar orqali mablag‘larni yig‘ish va taqsimlashdir. Bu donorlar uchun ham, yordam oluvchilar uchun ham soliq xatarlarini kamaytiradi.

2.5.4. Onlayn mablagʻ yigʻish jarayonida xavfsizlik boʻyicha asosiy talablar

Amaldagi qonunchilik va huquqni qoʻllash amaliyoti nuqtai nazaridan xayriya onlayn-aksiyalarini xavfsiz oʻtkazish oʻzaro bogʻliq talablar majmuasiga rioya qilishni nazarda tutadi.

Avvalo, yigʻin tashkilotchisining identifikatsiya qilinishi. NNT mablagʻ yigʻish toʻgʻrisidagi har bir ommaviy e'londa tashkilotning toʻliq nomi, uning roʻyxatdan oʻtish ma'lumotlari va rasmiy aloqa ma'lumotlari koʻrsatilishini ta'minlashi shart. Jismoniy shaxslar nomidan yigʻimlar oʻtkazish, shaxsiy bank kartalari yoki norasmiy rekvizitlardan foydalanish bunday faoliyatni noqonuniy deb topish xavfini tugʻdiradi.

Ikkinchi majburiy element yigʻish maqsadining aniq belgilanganligidir. Maqsad aniq, tekshiriladigan va oldindan e'lon qilingan boʻlishi kerak. Yordam oluvchilarni, mablagʻlarni sarflash yoʻnalishlarini va kutilayotgan natijalarni koʻrsatmasdan umumiy xarakterdagi ta'riflarga yoʻl qoʻyilmaydi. Xayriyalardan maqsadli foydalanish tamoyili ham xayriya, ham fuqarolik qonunchiligi uchun asosiy hisoblanadi.

Uchinchi talab vaqt boʻyicha cheklanganlikdir. Xayriya aksiyasi oldindan belgilangan muddatga ega boʻlishi kerak. Vaqt chegarasining yoʻqligi ishonch darajasini pasaytiradi va shaffoflik hamda halollik tamoyillarining buzilishi sifatida baholanishi mumkin.

Toʻrtinchi element — shaffof moliyaviy mexanizmlar. Onlayn yigʻimlar faqat NNTning rasmiy bank hisobvaraqlari yoki qonuniy toʻlov vositalari orqali amalga oshirilishi kerak. Bu moliyaviy nazoratni, moliyaviy monitoring talablariga rioya etilishini va mablagʻlardan foydalanishni keyinchalik tekshirish imkoniyatini ta'minlaydi.

Nihoyat, ommaviy hisobot berish xayriya aksiyasining majburiy yakuniy bosqichi hisoblanadi. Onlayn yigʻim yakunlari boʻyicha NNT kelib tushgan xayriyalar summasi, ulardan foydalanish yoʻnalishlari va erishilgan natijalar toʻgʻrisidagi ma'lumotlarni oshkor qilishi shart. Hisobot nafaqat huquqiy majburiyat, balki ishonchni shakllantirishning asosiy vositasi boʻlib xizmat qiladi.

2.5.5. Xayriya qiluvchilarning huquqlarini va shaxsiy ma'lumotlarni himoya qilish

Nodavlat notijorat tashkilotlari xayriya aksiyalari va onlayn yigʻimlarni oʻtkazishda homiylarning huquqlari himoya qilinishini ta'minlashi hamda Oʻzbekiston Respublikasining shaxsga doir ma'lumotlar toʻgʻrisidagi qonun hujjatlari talablariga rioya etishi shart. Oʻzbekiston Respublikasining «Shaxsga doir ma'lumotlar toʻgʻrisida»gi Qonuniga muvofiq, xayriya qiluvchini identifikatsiya qilish imkonini beruvchi har qanday ma'lumotlarni (jumladan, ismi, aloqa ma'lumotlari, toʻlov rekvizitlari, taxalluslari va ijtimoiy tarmoqlardagi izohlari) qayta ishlashga faqat tegishli shaxsning roziligi bilan va mablagʻ yigʻishning belgilangan maqsadi doirasida yoʻl qoʻyiladi.

Homiylar toʻgʻrisidagi ma'lumotlarni e'lon qilish, donorlar roʻyxatlarini, tashakkurnomalarni, tarjimalarning skrinshotlarini va boshqa materiallarni joylashtirish faqat homiyning roziligi bilan va ma'lumotlarni minimallashtirish tamoyiliga rioya qilgan holda amalga oshirilishi mumkin. NNT shaxsga doir ma'lumotlardan foydalanishni cheklash va ularning ruxsatsiz tarqatilishining oldini olish boʻyicha tashkiliy va texnik choralarni koʻrishi shart.

Shu bilan birga, NNT xayriya qiluvchilarning xayriya to‘g‘risidagi qonun hujjatlari va halollikning umumiy prinsiplaridan kelib chiqadigan yig‘im tashkilotchisi, uning maqsadlari, muddatlari va natijalari to‘g‘risida ishonchli axborot olish huquqlarini amalga oshirishni ta’minlashi shart. Xayriya faoliyatining shaffofligi va xayriyachilarning shaxsiy hayotini himoya qilish o‘rtasidagi muvozanat NNTlarning raqamli muhitda qonuniy va barqaror faoliyat yuritishi uchun majburiy element hisoblanadi.

2.5.6. Xayriya faoliyatining obro‘-e’tibor jihatlari va barqarorligi

Onlayn xayriya xavfsizligi NNT sektori uchun nafaqat huquqiy, balki strategik ahamiyatga ham ega. Alohida yig‘imlarni o‘tkazishdagi qoidabuzarliklar muayyan tashkilotga bo‘lgan ishonchga putur yetkazishi va umuman xayriya haqidagi jamoatchilik tasavvuriga salbiy ta’sir ko‘rsatishi mumkin. Axborot bir zumda tarqaladigan raqamli muhitda, aynan huquqiy va axloqiy standartlarga rioya qilish xayriya faoliyatining barqarorligi va qonuniyligining asosiga aylanadi.

Onlayn xayriya O‘zbekiston Respublikasi qonunchiligiga, mablag‘lardan maqsadli foydalanish, shaffoflik va hisobdorlik tamoyillariga qat’iy rioya qilgan holda nodavlat notijorat tashkilotlari faoliyatining qonuniy va samarali shakli hisoblanadi. NNT uchun ushbu talablarga rioya qilish rasmiy majburiyat emas, balki huquqiy himoyalanish, donorlar ishonchi va barqaror rivojlanishning zaruriy sharti hisoblanadi.

2.6. NNTlar uchun muhim hujjatlar va siyosatlar

Yuqorida ta’kidlanganidek, NNTlar uchun huquqiy xavf-xatarlar raqamli mediakontentni yaratish bilan ham, ushbu mediakontent tarqatiladigan kanallar bilan ham bog‘liq. Ko‘pincha ommaviy axborot vositalaridagi faoliyatingiz muvaffaqiyatli rivojlanishi uchun ko‘rilishi zarur bo‘lgan barcha xavf-xatarlar va chora-tadbirlar yozma hujjatlarda — maxsus siyosatlarda aks ettiriladi. Bunday siyosatlarni yozma shaklda ishlab chiqish va qabul qilish, ularni faqat tashkilot ichida e’lon qilish yoki foydalanish tavsiya etiladi.

Quyidagi jadvalda media biznesning o‘ziga xos xususiyatlaridan kelib chiqqan holda, onlayn faoliyatlar uchun minimal siyosat ro‘yxati (jami 5 ta siyosat) keltirilgan — media kontent yaratish va uni raqamli muhitda tarqatish. Ilovada tavsiya etilgan hujjatlar (siyosat) namunalarini ham topish mumkin:

- Materiallardan foydalanish qoidalari
- Shaxsiy ma’lumotlar siyosati
- Foydalanuvchilar (obunachilar) uchun izoh qoldirish qoidalari
- Xayriya tadbirlarini onlayn yoki ijtimoiy tarmoqlarda o‘tkazish qoidalari

Quyida O‘zbekiston media muhitida ishlash kontekstida har bir siyosatning qisqacha tavsifi va nima uchun bunday siyosatni ishlab chiqish hamda qabul qilish zarurligi keltirilgan.

2.6.1. Onlayn nashr materiallaridan (kontentdan) foydalanish qoidalari

Ushbu siyosatning maqsadi onlayn nashr tahririyati yoki NNT turli platformalar va kanallar orqali yaratilayotgan hamda tarqatilayotgan kontentning mualliflik huquqi egasi ekanligini ochiq e’lon qilishdir. Bu siyosat, shuningdek, huquq egasining o‘z kontentidan uning roziligisiz, lekin ma’lum shartlarga rioya qilgan holda foydalanish borasidagi pozitsiyasini (ruxsatini) belgilab beradi:

- Iqtibos keltirish holatlarida — onlayn nashr tomonidan belgilangan iqtibos hajmiga rioya qilish (matnning 30% dan oshmasligi, birinchi xatboshi va hokazo), shuningdek, birlamchi manbaga giperhavola qo‘llash va hokazo.

- Illyustratsiyalar, mualliflik fotosuratlaridan foydalanish holatlarida — fotosurat muallifi ko‘rsatilishi shart bo‘lgan holda e’lon qilinishi mumkin bo‘lgan fotosuratlar yoki boshqa vizual materiallar soni va hokazo.

- Dayjestlar va sharhlarda foydalanilgan hollarda — onlayn nashr tahririyati tomonidan belgilangan iqtiboslar hajmiga rioya qilish (matnning 30% dan oshmasligi, birinchi xatboshi va hokazo), shuningdek, birlamchi manbaga giperhavola qo‘llash va hokazo.

Mazkur siyosat, shuningdek, UGC (foydalanuvchi kontenti; users-generated content)[38] dan foydalanish tartib-qoidalarini, jumladan, foydalanuvchidan nashr etish uchun rozilik olish, foydalanuvchining yuborilgan materiallarga bo‘lgan huquqlari uchun javobgarligi, uchinchi shaxslarning murojaati bo‘yicha UGCni olib tashlash tartibini belgilaydi.

Siyosat internet, ijtimoiy tarmoqlar, messenjerlardan olingan materiallardan foydalanish bo‘yicha asosiy tamoyillarni o‘z ichiga oladi va huquqlarni tekshirmasdan «internetdan olingan» matnli va audiovizual materiallardan foydalanishni taqiqlaydi.

2.6.2. Shaxsiy ma’lumotlar bo‘yicha siyosat

Siyosatning maqsadi — sayt foydalanuvchilari, obunachilari va boshqalarning shaxsiy ma’lumotlarini qonuniy ravishda to‘plash va ulardan foydalanish. Siyosat quyidagi ma’lumotlarni o‘z ichiga olishi kerak:

- Qanday ma’lumotlar to‘planishi (ro‘yxatdan o‘tish, tarqatma xabarlar, sharhlar, arizalar, cookies/tahlil, mahsulot sotish, xayriya aksiyalarini o‘tkazish davrida shaxsiy ma’lumotlarni to‘plash va boshqalar);

- Qayta ishlash maqsadlari, saqlash muddatlari, qabul qiluvchilar toifalari;

- Murojaatlar uchun mas’ul shaxs/kanalning aloqa ma’lumotlari;

- Ma’lumotlar subyektini himoya qilish choralari va huquqlari.

[38] UGC (User-Generated Content, foydalanuvchi tomonidan yaratilgan kontent) — bu brendlar yoki mutaxassislar emas, balki oddiy odamlar (mijozlar, obunachilar) tomonidan yaratilgan har qanday material: sharhlar, suratlar, video sharhlar, izohlar, ijtimoiy tarmoqlardagi postlar.

2.6.3. Izohlar va moderatsiya qoidalari

Ushbu siyosatning maqsadi — auditoriya uchun talablarni (red flags) oldindan belgilash va sahifalaringizdagi izohlarda taqiqlangan, tuhmat qiluvchi, yolg'on ma'lumotlarni tarqatganlik uchun javobgarlik xavfini kamaytirishdir.

Bunday siyosat quyidagi ma'lumotlarni o'z ichiga olishi lozim:

- Taqiqlangan (noqonuniy) va nozik kontent (nafrat tili/kamsitish, zo'ravonlikka chaqirish, ekstremistik materiallar, pornografiya, shaxsiy ma'lumotlarni oshkor qilish, tahdidlar, ta'qib qilish, ochiqdan-ochiq yolg'on ma'lumotlar, boshqa qonunbuzarliklar).
- Tahririyat izohlarni qanday nazorat qilishi (oldindan moderatsiya yoki moderatsiyadan keyin), bloklash, o'chirish, muhokamalarni cheklash qoidalari.
- Qoidabuzarliklar haqida xabar berish tartibi (qoidabuzarliklar haqida qanday xabar berish va bu yetarli asos deb hisoblanishi)
- Nashrning ijtimoiy tarmoqlar va messenjerlardagi sayti va akkauntlari uchun yagona qoidalar.

Nima uchun bunday siyosat ham onlayn nashrlar tahririyatlari, ham NNTlar uchun muhim? O'zbekiston Respublikasining «Axborotlashtirish to'g'risida»gi Qonunida veb-saytlar va (yoki) veb-saytlar sahifalari (shu jumladan, ijtimoiy tarmoqlar va messenjerlarda joylashtirilgan) egalarining manbadan taqiqlangan maqsadlarda foydalanishga yo'l qo'ymaslik va taqiqlangan ma'lumotlarni olib tashlash bo'yicha majburiyatlari to'g'ridan-to'g'ri belgilangan. Qoidabuzarlik holatlarida resursga kirishni cheklash imkoniyati mavjud[39].

[39] O'zbekiston Respublikasining «Axborotlashtirish to'g'risida»gi Qonuni. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/acts/82956

3-bo‘lim
Raqamli muhitda fuqarolik faollari va NNTlar uchun tahdidlar

3.1. Asosiy tahdidlar

So‘nggi o‘n yillikda raqamli makonning rivojlanishi tufayli fuqarolik jamiyatiga qanday tahdidlar ustunlik qilishi borasida tub o‘zgarishlar yuz bermoqda. Ilgari asosiy e’tibor jismoniy tahdidlarga qaratilgan bo‘lsa, bugungi kunda front chizig‘i virtual bo‘lib, smartfonlarimiz, noutbuklarimiz va bulutli xotiralarimiz orqali o‘tmoqda. Biz «shisha uy» davrida yashayapmiz, bu davrda g‘oyalarni tarqatish va tarafdorlarni jalb qilishga yordam beradigan raqamli shaffoflik va «hamma joyda» bo‘lish bizni bu faoliyatga to‘sqinlik qilmoqchi bo‘lganlar oldida zaif qilib qo‘yadi.

Markaziy Osiyodagi NNT faollari va xodimlari uchun raqamli tahdidlar manzarasini tushunish shunchaki «axborot uchun» savol bo‘lmay qoldi. Endi bu omon qolish, erkinlik va obro‘ni saqlab qolish masalasi. «Mening yashiradigan hech narsam yo‘q» yoki «menga qiziqish uchun juda kichikman» degan illyuziya juda xavfli yanglishishdir. Zamonaviy ommaviy kuzatuv tizimlarida (DPI, yuzni aniqlash, katta ma’lumotlar tahlili) «muhim bo‘lmagan» maqsadlar yo‘q; hamma nishonga olinishi mumkin.

Onlayn tahdidlar bilan oflayn oqibatlar o‘rtasidagi chegaralar yo‘qolganini tushunish juda muhim. Elektron pochtani buzish shunchaki texnik nosozlik emas, balki keng doiradagi shaxslarga ta’sir ko‘rsatadigan uzoq muddatli oqibatlarga ega bo‘lgan muhim xavfsizlik hodisasidir, geolokatsiya metama’lumotlari bilan fotosurat yopiq uchrashuv ishtirokchilariga jismoniy hujumga olib kelishi mumkin, kiberbulling va dezinformatsiya kampaniyalari esa tashkilotlarning charchashi va faoliyatini to‘xtatishiga olib keladigan haqiqiy psixologik jarohatlarni keltirib chiqaradi.

Ko‘plab tashkilotlar raqamli xavfsizlikni antivirus sotib olishdek qabul qilishadi: o‘rnatib qo‘yib, unutib yuborishadi, bunda soxta xavfsizlik hissi paydo bo‘ladi. Biroq haqiqiy himoya mexanizmi boshqacha tuzilgan. U tahdidlar manzarasini (kontekst, tashqi muhit) tushunishni, **hujum vektorlarini** (tahdidlar amalga oshirilishi mumkin bo‘lgan yo‘llarni) bilishni va o‘zining raqamli resurslari hamda ularning zaif tomonlarini aniq tasavvur qilishni talab etadi. Aynan shu bilimlar asosida tashkilotning barqaror **xavfsizlik profili** (security posture) shakllanadi — bu shunday holatki, bunda xavfsizlikni ta’minlash bir martalik harakat emas, balki uzluksiz jarayonga aylanadi.

Biroq, zamonaviy raqamli dunyoda raqamli aktivlarni himoya qilishning texnik komponentlarini sozlashning o‘zi yetarli emas. Hozirgi kunda xavfsizlikka xolistik (yaxlit) yondashuv tobora ommalashib bormoqda, bu esa raqamli, jismoniy va ruhiy-ijtimoiy xavfsizlikning ajralmasligidan kelib chiqadi. Ular yagona ekotizimni tashkil etadi, bu yerda bir sohadagi zaiflik muqarrar ravishda boshqalardagi himoyani buzadi.

Masalan:

Psixologik bosim

(do‘q-po‘pisa, shantaj) xodimning hissiy charchashiga olib keladi.

Charchagan xodim

hushyorligini yo‘qotadi va fishing yoki ijtimoiy muhandislikning (raqamli zaiflik) osongina qurboniga aylanadi.

Raqamli resurslarni buzish

orqali nozik shaxsiy ma’lumotlar (jinsiy oriyentatsiya, OIV holati, ...) oshkor etiladi, bu esa benefitsiarlarning jismoniy xavfsizligiga to‘g‘ridan-to‘g‘ri tahdid soladi.

Ma’lumotlarning sizib

chiqishi davlatning huquqiy sanksiyalariga, obro‘siga putur yetishiga, donorlarning ishonchsizligiga va natijada moliyaviy yetishmovchilikka hamda tashkilot faoliyatining yopilishiga olib keladi.

Shu sababli, ushbu to‘plamda tahdidlar alohida emas, balki birgalikda ko‘rib chiqiladi, bunda inson har qanday xavfsizlik tizimidagi **asosiy aktiv va bir vaqtning o‘zida hujumning asosiy vektori** ekanligiga e’tibor qaratiladi.

Qulaylik uchun biz tahdidlarni ta’sir doirasiga ko‘ra bir necha toifalarga ajratishimiz mumkin: texnik, jismoniy, huquqiy, ruhiy-ijtimoiy, iqtisodiy hamda insoniy va tashkiliy xarakterdagi tahdidlar. Bo‘linish yetarlicha shartli, chunki aksariyat tahdidlar gibrid bo‘lib, ularni turli toifalarga mansub tarkibiy qismlarga ajratish mumkin, masalan, «xorijiy agentlar» to‘g‘risidagi qonunlar bir vaqtning o‘zida bir nechta toifaga bo‘linadi: huquqiy — bu javobgarlik yuzaga keladigan shartlarni belgilaydigan qonun; iqtisodiy — tashkilotlarning moliyaviy barqarorligini xavf ostiga qo‘yadi; ruhiy-ijtimoiy — xorijiy agent ta’rifi ostida qolganlarni kamsitadi; tashkiliy — tashkilotga qo‘shimcha hisobotlar va belgilar shaklida qo‘shimcha ma’muriy yuk yuklaydi; texnik — talablarga rioya qilmaslik akkauntlar, saytlar va domenlarning bloklanishiga olib kelishi mumkin. Bunda tahdidni kim ko‘rib chiqayotganiga qarab, ko‘rib chiquvchiga yaqin bo‘lgan toifa birinchi o‘ringa chiqadi: huquqshunos uchun — huquqiy, moliyachi uchun — iqtisodiy, direktor uchun — operatsion, raqamli xavfsizlik bo‘yicha mutaxassis uchun — texnik. Ushbu qo‘llanmada biz tahdidlarning raqamli tarkibiy qismiga e’tibor qaratamiz va ularni aynan shu nuqtai nazardan baholaymiz.

1. Texnik tahdidlar — raqamli infratuzilma, qurilmalar va ma’lumotlarning ishlashini buzish, ularni xavf ostiga qo‘yish yoki ularga ruxsatsiz kirishga qaratilgan tahdidlar)

- **Ma’lumotlarni yig‘ish va razvedka qilish (OSINT)** — to‘g‘ridan-to‘g‘ri tahdid emas, lekin ko‘pincha maqsadli hujumning dastlabki bosqichi bo‘lib, texnikadan tortib psixologik-ijtimoiygacha bo‘lgan turli xil zaifliklarni aniqlash uchun ochiq ma’lumotlarni tahlil qilishni o‘z ichiga oladi.

- **Zararli dasturlar (josuslik dasturlari, shifrlovchi viruslar) bilan zararlanish eng keng tarqalgan kibertahdid** bo‘lib, u, masalan, ma’lumotlarni shifrlaydigan va to‘lov talab qiladigan ommaviy viruslarni ham, qurilmani masofadan turib to‘liq boshqarishni ta'minlaydigan murakkab josuslik dasturlari (masalan, Pegasus, Predator va boshqalar) yordamida maqsadli hujumlarni ham o'z ichiga oladi.

- **Raqamli akkauntlarni buzish** — ruxsatsiz kirishning barcha turlarini (pochta, ijtimoiy tarmoqlar, messenjerlar, moliyaviy akkauntlarga) birlashtiradi. Bu asosan fishing, ijtimoiy muhandislik usullari va parollarning sizib chiqishi tufayli sodir bo'ladi. Natija — aloqa kanallari va obro' ustidan nazoratni yo'qotish.

- **Veb-saytlarga hujumlar (DDoS, saytlarni buzish)** — tashkilotning ommaviy resurslariga to'g'ridan-to'g'ri hujumlar DDoS-hujumlarning maqsadi — zararlangan qurilmalardan so'rovlar bilan qayta yuklash orqali resursni auditoriya uchun mavjud bo'lmaydigan qilish. Buzib kirishning maqsadi odatda defes (kontentni almashtirish), ma'lumotlarni o'g'irlash yoki zararli kodni joylashtirishdir.

- **Himoyalanmagan tarmoqlarda ma'lumotlarning ushlab qolinishi** — jamoat joylarida (kafe, aeroportlar) o'zingiz nazorat qilmaydigan Wi-Fi nuqtasidan foydalanganda yuzaga keladigan dolzarb tahdiddir. Bunday holda tajovuzkor shifrlanmagan trafikni, jumladan, login va parollarni qo'lga kiritishi mumkin. Xuddi shu xavf shifrlashdan foydalanmaydigan (http protokoli) saytlarga kirganda ham mavjud bo'lib, bu haqda odatda brauzer va ba'zi antiviruslar ogohlantiradi.

- **Kompromat ma'lumotlarni "tashlab qo'yish"** — bu juda kam uchraydigan, biroq xavfli tahdid. Hujumchi qurilmaga kirish huquqini qo'lga kiritib, ma'lumotlarni o'g'irlash o'rniga, unga noqonuniy kontentni (ekstremistik materiallar, pornografiya va boshqalar) joylashtiradi. Maqsad — keyinchalik obro'sizlantirish yoki jinoiy ta'qib uchun asos yaratish.

- **Ta'minot zanjiri hujumlari (Supply Chain Attacks) — bu tobora ommalashib borayotgan tahdid** bo'lib, unda sizga to'g'ridan-to'g'ri emas, balki ishonchli hamkoringizga (masalan, veb-saytingiz ishlab chiqaruvchisiga, dasturiy ta'minot ta'minotchisiga yoki kompyuter xizmatiga) hujum qilib, ularning tizimlari orqali infratuzilmangizga kirish mumkin.

2. Psixosotsial tahdidlar —
bu faolning shaxsiyatiga, uning obro'siga, ruhiy holatiga va ijtimoiy aloqalariga nisbatan axloqni buzish va faoliyatini to'xtatish maqsadida qaratilgan tahdidlardir

- **Koordinatsiyalangan onlayn ta'qib va dezinformatsiya kampaniyalari (Kiberbulling, trollar fabrikalari)** — bu sharhlar, ijtimoiy tarmoqlar va boshqa manbalarda ommaviy hujumlar, haqoratlar, tahdidlar va yolg'onlarni tarqatish, shu jumladan dipfeyklar yordamida, odatda obro'ni tushirish maqsadida tashkil etiladi.

- **Doksing** — raqamli tahdidni haqiqiy jismoniy xavfga aylantirish va faolni qo'rqitish maqsadida shaxsiy ma'lumotlarni (manzillar, telefon raqamlari, qarindoshlar ma'lumotlari) to'plash va ommaviy ravishda e'lon qilish.

- **Sekstorshn (sextortion), porno qasos va seks josuslik** — bu intim xarakterdagi materiallar (haqiqiy yoki sun'iy intellekt yordamida soxtalashtirilgan) orqali shantaj qilishga asoslangan tahdidlar bo'lib, ular ayniqsa konservativ jamiyatlarda faol ayollarga qarshi keng qo'llanadi.

3. Huquqiy va tartibga solish tahdidlari — qonunchilik, davlat institutlari va huquqiy tizimdan bosim, senzura va ta’qib vositasi sifatida foydalanadigan tahdidlar

- Repressiv qonunchilikni qo‘llash («feyklar,» «tuhmat,» «ekstremizm» to‘g‘risida) — internetda e’lonlar uchun ma’muriy va jinoiy ish qo‘zg‘atish uchun qonunlardagi noaniq ta’riflardan foydalanish tahdidi.
- «Xorijiy agentlar/vakillar» to‘g‘risidagi qonunlarning qo‘llanilishi gibrid tahdid bo‘lib, u o‘z mohiyatiga ko‘ra huquqiy hisoblanadi, ammo bevosita iqtisodiy, ruhiy-ijtimoiy va operatsion oqibatlarga ega.
- Davlat organlari talabiga ko‘ra onlayn resurslarni bloklash yoki o‘chirish — kontentni senzura qilish bo‘yicha suddan tashqari yoki sud qarori tufayli saytni, ijtimoiy tarmoqdagi sahifani bloklash yoki kontentni o‘chirish tahdidi.
- Platformalarning huquqiy mexanizmlarini suiiste’mol qilish (DMCA hujumlari) — mualliflik huquqi shikoyatlari, ijtimoiy tarmoqlardagi rasmiy kanallar orqali kontent, messenjerlar kabi platformalarning qonuniy vositalaridan noqonuniy maqsadlarda foydalanish (tovlamachilik, senzura).
- Davlat raqamli nazorati — TQTT, DPI, yuzni tanib olish tizimlari va biometriya kabi rasmiy-qonuniy vositalarni suiiste’mol qilishning bilvosita tahdidi, e’lon qilingan maqsadlardan (masalan, terrorizm yoki og‘ir jinoyatlarga qarshi kurash) ancha tashqarida bo‘lgan ommaviy va maqsadsiz ma’lumotlarni to‘plash uchun raqamli profillarni yaratish.

4. Iqtisodiy tahdidlar — asosan gibrid tahdidlar bo‘lib, ularning asosiy maqsadi yoki mexanizmi tashkilotning moliyaviy barqarorligiga bevosita ta’sir qilishdan iborat

- **To‘g‘ridan-to‘g‘ri raqamli firibgarlik va mablag‘larni o‘g‘irlash — buzish yoki ijtimoiy muhandislik orqali moliyaviy akkauntlarga ruxsatsiz kirish**
- **Bank hisobvaraqlari va moliyaviy operatsiyalarni blokirovka qilish** — rasmiy huquqiy bahona bilan (masalan, da’voni ta’minlash bo‘yicha iltimosnomani ta’minlash doirasida) boshlanishi mumkin bo‘lgan harakat.
- **Fandrayzing yoki kraudfandingga hujumlar** — klon saytlarni yaratish, xayriya mablag‘larini o‘zlashtirish kabi to‘g‘ridan-to‘g‘ri firibgarlik, shuningdek, mablag‘larni qo‘lga kiritadigan raqobatchi loyihalarni (GONGO) sun’iy ravishda yaratish kabi bilvosita bo‘lishi mumkin.
- **Ikkilamchi sanksiyalar yoki qo‘shimcha zarar tahdidi** — bu xalqaro banklar, IT-kompaniyalar, donorlar va platformalar sanksiyalar rejimini buzishdan qo‘rqib, sanksiyaga yaqin bo‘lgan butun mintaqa bilan ishlashni butunlay to‘xtatishi yoki cheklashi, bu esa bank operatsiyalari, hisob raqamlari bloklanishiga, xizmatlar tomonidan cheklanishiga olib kelishi mumkin bo‘lgan «muvofiqlikdan tashqari» tahdid.

5. Inson omili va tashkiliy tahdidlar — ichki jarayonlardagi kamchiliklar, inson omili, shuningdek, qurilmalarning jismoniy xavfsizligi tufayli yuzaga keladigan tahdidlar

- **Xodimlarning beixtiyor xatolari va zaifliklari — beparvolik, raqamli savodsizlik va toliqish** kabi tahdidlarni birlashtiradi. Charchagan, oʻqitilmagan yoki gʻayratsiz xodim — bu koʻplab texnik va ruhiy-ijtimoiy tahdidlar (masalan, fishing) amalga oshiriladigan zaiflikdir.

- **Ichkaridan qasddan qilingan dushmanlik harakatlari (insayderlar)** — xodim yoki koʻngillilardan kelib chiqadigan tahdid boʻlib, ular ataylab ishni buzadi, maʼlumotlarni oshkor qiladi yoki uchinchi shaxslarga kirish huquqini beradi.

- **Qurilmalar va maʼlumot tashuvchilarning jismoniy yoʻqolishi, oʻgʻirlanishi yoki olib qoʻyilishi** — siz texnika ustidan jismoniy nazoratni yoʻqotadigan (taksida unutib qoldirilgan, oʻgʻirlangan, tintuv paytida musodara qilingan) barcha ssenariylarni birlashtiradi. Shifrlashsiz bu maʼlumotlarning toʻliq chiqib ketishiga, zaxira nusxalarsiz esa maʼlumotlarning butunlay yoʻqolishiga tengdir.

Tashqi tahdidlarni shunchaki sanab oʻtishdan himoya strategiyasini ishlab chiqishga oʻtish oʻzimizga berishimiz kerak boʻlgan savollarni yanada kengaytirishni talab qiladi. Bu nafaqat «Kim yoki nima tahdid solishi mumkin?» degan savol, balki «Biz aynan nimani himoya qilyapmiz?» va «Bizning zaif tomonlarimiz qayerda?» degan savollar hamdir. Koʻpincha bizning nazoratimizdan tashqarida boʻlgan faqat tashqi omillarga eʼtibor qaratish oʻrniga, tashkilotning ichki muhitiga eʼtibor qaratish lozim. Har qanday strategiyaning asosida tashkilot uchun qaysi aktivlar muhim ekanligini aniq tushunish yotadi. Fuqarolik sektori uchun bu, birinchi navbatda, oshkor etilishi odamlarga bevosita zarar yetkazishi mumkin boʻlgan axborot va maʼlumotlar; qonuniylik poydevori boʻlib xizmat qiladigan obroʻ va jamoatchilik ishonchi; farovonligi ish qobiliyatining sharti boʻlgan jamoa; va tashkilotga tashqi dunyo bilan oʻzaro aloqa qilish imkoniyatini taʼminlaydigan aloqa kanallari. Tashqi tahdidlar oʻzlariga mos zaifliklarni topib, ulardan foydalangandagina haqiqiy xavfga aylanadi. Har bir muvaffaqiyatli hujum tashqi omilning ichki himoyadagi boʻshliqlardan qanday foydalanganligi haqidagi hikoyadir.

Ushbu tahlil bizni xavfning rasmiy taʼrifiga olib keladi. Xavf — bu tahdidning oʻzi ham, zaiflikning oʻzi ham emas, balki muayyan tahdidning muayyan zaiflikdan muvaffaqiyatli foydalanishi va bu tashkilot aktivlariga maʼlum darajada zarar yetkazishi ehtimolidir.

Masalan, josuslik dasturiy taʼminotini joriy etish kabi texnik tahdidlar bevosita axborot aktivlariga qaratilgan. Biroq, ularning muvaffaqiyati deyarli har doim zaifliklar mavjudligi bilan bogʻliq: zaif parol siyosati, ikki bosqichli autentifikatsiyaning yoʻqligi yoki koʻpincha inson omilining zaifliklari, masalan, xabardorlikning yetishmasligi yoki charchash tufayli hushyorlikning pasayishi. Maʼlumotlar bazasi boʻlgan shifrlanmagan qattiq disk qurilma jismonan yoʻqolganda yoki olib qoʻyilganda oson oʻljaga aylanadi.

Oʻz navbatida, psixo-ijtimoiy hujumlar, jumladan, dezinformatsiya, doksing va chuqur feyklardan foydalanish obroʻ va ishonchga putur yetkazishga qaratilgan. Ular xodimlarning ijtimoiy tarmoqlarda shaxsiy maʼlumotlarini haddan tashqari oshkor qilishi yoki tashkilotning soxta maʼlumotlarga qarshi kurashish uchun aniq kommunikatsiya strategiyasiga ega emasligi kabi zaifliklarda qulay zamin topmoqda. Hujum shaxsiy va ommaviy raqamli izlar oʻrtasidagi chegaralar xiralashgan joyda muvaffaqiyatli boʻladi.

Xuddi shunday, huquqiy va iqtisodiy bosim tashkiliy zaifliklarga qaratilganda ayniqsa samarali bo'ladi. «Xorijiy agentlar» to'g'risidagi qonunlar bir manbaga moliyaviy qaramlikni ekspluatatsiya qiladi, hisobvaraqlarning to'satdan blokirovka qilinishi esa tashkilotda diversifikatsiyalangan moliyaviy oqimlar va zaxira fondlarining yo'qligini ko'rsatadi. Tuhmat uchun qonuniy javobgarlikka tortish ko'pincha puxta ishlab chiqilgan tahririyat siyosati va faktlarni tekshirish tartib-qoidalari mavjud bo'lmaganda mumkin bo'ladi.

Har qanday tashkilotning resurslari cheklanganligi sababli, barcha zaifliklarni bir vaqtning o'zida bartaraf etib bo'lmaydi. Xavf-xatarlarga ustuvorlik berish asosiy vazifaga aylanadi. Bu jarayon har bir tahdidni ikkita asosiy mezon bo'yicha baholash orqali amalga oshiriladi: uning amalga oshish ehtimoli va muvaffaqiyat qozongan taqdirda ehtimoliy zarar. Ehtimollik tashkilotning maqsad sifatida jozibadorligi va uning zaif tomonlaridan foydalanish osonligiga bog'liq. Zarar zarbaga uchragan aktivning qiymati va uni tiklash qiymati bilan belgilanadi. Ikki bosqichli autentifikatsiya yo'qligi sababli maxfiy ma'lumotlarga ega ma'lumotlar bazasining buzilishi kabi yuqori ehtimollik va yuqori potensial zarar keltiruvchi xavflar zudlik bilan e'tibor qaratishni talab etadi. Shu bilan birga, ehtimoli past va kam zarar keltiradigan xatarlar vaqtincha kechiktirilishi mumkin.

Xavflar baholanib, ularga ustuvorlik berilgandan so'ng, tashkilot ularning har biri uchun to'rtta asosiy **boshqaruv strategiyasidan** birini tanlashi mumkin. Birinchidan, bu **qochish (Avoidance)** — yuqori xavf bilan bog'liq faoliyatni to'xtatishning strategik qaroridir. Masalan, tashkilot o'z missiyasi uchun mutlaqo zarur bo'lmasa, ma'lum turdagi nozik ma'lumotlarni to'plamaslikka qaror qilishi mumkin, bu esa ularning sizib chiqish xavfini butunlay bartaraf etadi. Ikkinchidan, **qabul qilish (Acceptance)** strategiyasi mavjud bo'lib, u past ustuvorlikka ega bo'lgan tavakkalchiliklarga nisbatan qo'llaniladi, bunda ularni kamaytirish qiymati potensial zarardan oshib ketadi. Uchinchidan, bu risklarni o'tkazish **(Transfer)** — riskning bir qismini uchinchi tomonga o'tkazishdir. Ma'lumotlarni saqlash uchun ishonchli bulutli provayderdan foydalanish klassik misol bo'lib, bu unga serverlarning jismoniy xavfsizligi va uskunalarning ishdan chiqishi bilan bog'liq xavflarni o'tkazadi. Nihoyat, bu xavfni kamaytirish **(Mitigation)** eng keng tarqalgan strategiya bo'lib, u ehtimollik yoki zararni kamaytirish uchun choralar ko'rishdan iborat. Masalan, shifrlashni joriy etish, xodimlar uchun treninglar o'tkazish yoki zaxira nusxalarini yaratish. Bu keyingi bo'limda ko'rib chiqiladigan asosiy strategiyadir.

3.2. Fuqarolik faollari va NNTlar xavfsizligini ta'minlash choralari

O'z raqamli resurslaringiz xavfsizligini ta'minlash juda murakkab jarayon, ayniqsa alohida IT bo'limi yoki mutaxassis va resurslar bo'lmasa. Oldingi bo'limda sanab o'tilgan tahdidlarning to'liq bo'lmagan ro'yxati tushkunlikka tushirib, qo'lni tushirishga majbur qilishi mumkin, chunki hamma narsadan himoyalanish imkonsizdek tuyuladi. Shunga qaramay, bu yondashuv konstruktiv emas va ushbu bo'limda biz ko'pchilik tashkilotlar va alohida faollar uchun variantlarni tanlashga harakat qilamiz.

Avvalo, mutlaqo zarur bo'lgan minimal talablar mavjud — bu muammolarning 80 foizini hal qiladigan 20 foizlik sa'y-harakatdir:

- Raqamli resurslar inventarizatsiyasi — bu eng muhim raqamli resurslarning ro'yxatini tuzish jarayonidir. Odatda bunday ro'yxatga **barcha email manzillar** (shaxsiy va ishchi), **ijtimoiy tarmoqlardagi akkauntlar (FB, IG, ...), messenjerlardagi akkauntlar**

(WhatsApp, Telegram, Signal,...), bulutli saqlash xizmatlari (Google Drive, Dropbox, OneDrive,...), shuningdek eng muhim hujjatlar va ularning saqlanish joylari kiradi. Bu bosqich alohida shaxslar yoki kichik tashkilotlar uchun kamdan-kam hollarda bir soatdan koʻproq vaqt oladi, biroq uning ahamiyatini ortiqcha baholash qiyin. Biz eslay olmaydigan raqamli resurslarni himoya qila olmaymiz, shuning uchun bu bosqich eng qimmatli raqamli aktivlarni koʻrish zonasiga kiritadi.

- **Parollar menejeri** — bu har bir sayt uchun oʻta murakkab parollarni yaratadigan va eslab qoladigan dastur. Siz faqat bitta asosiy parolni eslab qolishingiz kerak. Bu hisoblaringiz xavfsizligidagi eng katta boʻshliqni darhol yopadi. Jiddiy zaifliklardan biri bu juda zaif parollardan foydalanish yoki bir xil parolni bir nechta resurslar uchun qayta ishlatishdir. Parollar menejeri bilan bu muammolar hal qilinadi. Chunki barcha parollar parollar menejerida saqlanadi va ularni eslab qolishning hojati boʻlmaydi. Parollardan tashqari, parol menejerlarida turli xil maxfiy qaydlar, bank kartalari maʼlumotlari, shaxsiy maʼlumotlar va boshqa maʼlumotlarni saqlash mumkin. Muhim jihati shundaki, parollar menejeridagi parollaringiz shifrlangan holda saqlanadi va hatto ularning xizmati buzilsa ham, buzgʻunchilar parollaringizga kira olmaydi. Faqat sinovdan oʻtgan, ishonchli parol menejerlaridan foydalanish kerak, masalan, bepul versiyaga ega Bitwarden yoki 1Password. Hozirgi kunda koʻplab xizmatlar parolsiz kirishni joriy etmoqda, parol kalitlari yordamida, bu parollarga ideal muqobil boʻlib tuyulishi mumkin — murakkab kalit qurilmangizda saqlanadi, eslab qolishni talab qilmaydi va hech qayerga uzatilmaydi. Shu bilan birga, bu usul ham tahdidlardan himoyalanmagan. Shunday qilib, kalitga kirish PIN-kodni kiritish yoki biometrik aniqlash orqali amalga oshiriladi va agar kimdir sizning PIN-kodingizni bilib olsa yoki barmoq izi yoki FaceID'dan foydalanishga majbur qilsa, u sizning hisoblaringizga kirish huquqiga ega boʻladi. Parolsiz sxemalardan farqli oʻlaroq, parollar menejeridan foydalanish turli tahdidlarda turli xil foydalanish variantlariga moslashtirilishi mumkin.

- **Ikki bosqichli autentifikatsiya (Two-factor authentication, 2FA)** hisoblaringiz uchun ikkinchi himoya chizigʻidir. Agar parolingiz oʻgʻirlansa ham, telefoningizdagi kod, token, barmoq izi yoki FaceIDsiz firibgar hisobingizga kira olmaydi. **Bu buzib kirishga qarshi eng samarali chora.** Koʻpgina xizmatlarda u avtomatik ravishda yoqiladi (masalan, Google bildirishnomalari), baʼzilarida esa qoʻlda yoqish kerak boʻladi. Shunga qaramay, u nafaqat barcha xizmatlarda yoqilganligiga, balki toʻgʻri sozlanganligiga ishonch hosil qilish kerak. Xususan, SMS orqali autentifikatsiya qilish xavfsiz emas va SMS xabarni ushlash orqali osongina buzib kirilishi mumkin, shuning uchun bu usul muqobil usullar mavjud boʻlgan joylarda oʻchirilishi kerak. Shunday qilib, qulaylik va xavfsizlik nuqtai nazaridan «oltin oʻrtalik» kirish uchun kodlarni mustaqil ravishda yaratuvchi autentifikator ilovasidan (Google Authenticator, Authy, Microsoft Authenticator, ...) foydalanishdir. Bundan tashqari, zaxira tiklash kodlari (backup codes) ishonchli va xavfsiz joyda saqlanishiga ishonch hosil qilish kerak, bu bir martalik kodlar telefon ishlamagan taqdirda ishlatiladi. Bu juda muhim qadam, aks holda hisobingizga kira olmay qolishingiz mumkin. Siz foydalanadigan messenjerlarda ham ikki bosqichli autentifikatsiya mavjudligini alohida tekshiring. Turli messenjerlarda u turlicha nomlanishi mumkin: WhatsApp — ikki bosqichli tekshiruv, Telegram — bulutli parol, Signal — roʻyxatdan oʻtishni bloklash. Ushbu sozlamalar roʻyxatdan oʻtish SMS xabarini ushlab qolish yoki SIM kartani almashtirish orqali messenjerni buzish imkoniyatining oldini oladi.

- **Zaxira nusxalarini yaratish (backup)** — mahalliy qurilmalarda saqlanadigan maʼlumotlarni apparat nosozliklari, zararli dasturiy taʼminot (xususan, shifrlovchi dasturlar) hujumlari va uskunaning jismonan yoʻqolishi yoki olib qoʻyilishi kabi tahdidlardan himoya qilishning oʻta muhim tarkibiy qismidir. Samarali zaxira nusxalashning asosiy tamoyili — bu jarayonni avtomatlashtirishdir. Foydalanuvchi tomonidan fayllarni qoʻlda nusxalashga asoslangan tizimlar inson omili tufayli ishonchliligi past boʻladi. Avtomatlashtirilgan zaxira nusxalashni amalga oshirishning ikkita asosiy yondashuvi mavjud: tashqi tashuvchilardan foydalangan holda mahalliy zaxiralash hamda bulutli zaxiralash va sinxronlash. Mahalliy zaxira nusxalash uchun tashqi axborot tashuvchilar (qattiq disklar, SSD-toʻplagichlar va hokazo) ishlatiladi. Bu jarayonni avtomatlashtirish uchun operatsion tizimning oʻrnatilgan vositalaridan foydalanish mumkin. Microsoft Windows'da bu vazifani "Fayllar tarixi" (File History) vositasi bajaradi; u foydalanuvchi papkalaridagi fayllarni koʻrsatilgan tashqi diskka davriy nusxalashni sozlash imkonini beradi. Apple macOS'da esa shunga oʻxshash funksionallikni Time Machine tizimi taqdim etadi. U butun tizimning inkremental sur'atlarini yaratib, ham alohida fayllarni, ham butun operatsion tizimni ma'lum bir vaqtga qayta tiklashga imkon beradi. Bulutli zaxira nusxalash uchun Google Drive, Microsoft OneDrive, Dropbox kabi bulutli xizmatlardan foydalaniladi. Aksariyat zamonaviy bulutli xizmatlar avtomatik sinxronizatsiya tamoyili asosida ishlaydi: bunda mahalliy ilova oʻrnatiladi, u mahalliy diskda maxsus papka yaratadi va shu papkaga joylashtirilgan har qanday fayl avtomatik ravishda bulutli xotiraga nusxalanadi hamda barcha ulangan qurilmalar oʻrtasida sinxronlanadi. Oʻta maxfiy ma'lumotlar bilan ishlaydigan tashkilotlarga boshdan-oyoq (end-to-end) shifrlashni taklif qiluvchi ixtisoslashtirilgan bulutli xizmatlarni koʻrib chiqish tavsiya etiladi. Bunday tizimlarda (masalan, Proton Drive, Sync.com, Tresorit, Mega.io) ma'lumotlar serverga yuborilishidan oldin foydalanuvchining qurilmasida shifrlanadi. Bu esa ma'lumotlardan hatto xizmat xodimlarining oʻzi ham foydalana olmasligini ta'minlab, maksimal darajadagi maxfiylikni kafolatlaydi. Mobil qurilmalarda sinxronlash odatda ulangan akkauntlar (Google, iCloud) orqali amalga oshiriladi, biroq bulutli xizmatlar ilovalarining mobil versiyalaridan ham foydalanish mumkin. Eng yaxshisi, ikkala usulni "3-2-1" formulasi boʻyicha birga qoʻllashdir: ma'lumotlarning 3 ta nusxasi boʻlib, ulardan ikkitasi turli jismoniy tashuvchilarda va bittasi bulutda saqlanadi. Bunday yondashuv nosozliklarga nisbatan eng yuqori darajadagi barqarorlikni ta'minlaydi va aksariyat inqirozli holatlarda ma'lumotlar saqlanishini kafolatlaydi. Bunda faqat ma'lumotlarning mavjudligi ta'minlanadi; zaxira nusxalarning himoyasi esa bulutli zaxiralashda akkauntni himoyalash, mahalliy saqlashda esa diskni toʻliq shifrlash orqali amalga oshiriladi.

Oldinga siljish va xavfsizlik boʻyicha ijobiy oʻzgarishlarni doimiy qilish uchun treninglar yoki xavfsizlik uchun zarur boʻlgan sozlamalarni oʻrnatish kabi bir martalik aksiyalar kam. Kelajakda xavfsizlik tashkilotning butun faoliyatining ajralmas qismiga aylanganda, tizimli yondashuv muhim ahamiyat kasb etadi. Buning uchun korporativ xavfsizlikning Due Diligence va Due Care kabi ikki tushunchasini kiritish zarur. Toʻgʻridan-toʻgʻri tarjima yoʻq, lekin quyidagicha aniqlash mumkin:

- **Due Diligence** — bu "amal qilishdan oldin oʻylab koʻrish", ya'ni xavflarni baholash va harakatlarni rejalashtirishdir. Bu quyidagi savolga javob beradi: "Tahdidlarga tayyorlanish uchun qoʻlimizdan kelgan barcha choralarni koʻrdikmi?"

- **Due Care** — bu "har kuni harakat qilish majburiyati", ya'ni yaratilgan tizimni ishchi holatda saqlab turish boʻyicha kundalik sa'y-harakatlardir. Bu quyidagi savolga javob beradi: "Tahdidlarga tayyor turish uchun doimiy ravishda barcha zarur choralarni koʻryapmizmi?"

Buning uchun har bir darajada rejalashtirish va ijro etish uchun qabul qilinishi kerak boʻlgan chora-tadbirlar joriy etiladi. Shunga koʻra, har bir darajada minimal talablar va oldingi darajadagi talablar bajarilishi muhimdir.

1-daraja:
Intizom va asosiy gigiyenani shakllantirish — alohida faollar va kichik jamoalar uchun mo‘ljallangan bo‘lib, uning maqsadi yakka tartibdagi amaliyotlarni umumiy intizom va xavfsizlik madaniyatiga aylantirishdir.

Rejalashtirish va asosiy poydevorni tayyorlash (Due Diligence): Bu bosqichda operatsion xavfsizlik poydevori qo‘yiladi. U yuqorida keltirilgan zaruriy minimumni, shuningdek, bir nechta asosiy qo‘shimcha qadamlarni o‘z ichiga oladi.

Iloji boricha faqat litsenziyalangan dasturiy ta’minotdan foydalanishga harakat qilish. Ro‘yxatdan o‘tgan NNTlar uchun ko‘plab sotuvchilar o‘zlarining dasturiy mahsulotlarini bepul yoki katta chegirma bilan taqdim etadilar. Yirik ishlab chiqaruvchilar NNTlar uchun maxsus dasturlarga ega, masalan, notijorat tashkilotlar uchun Google va notijorat tashkilotlar uchun Microsoft, ular doirasida tijorat xizmatlaridan bepul foydalanish mumkin yoki Techsoup NNTlar uchun ko‘plab mahsulotlarga, shu jumladan Windows litsenziyalariga maxsus narxlarda kirish nuqtasi hisoblanadi.

Windows uchun — Bitlocker, MacOS uchun — Filevault to‘liq diskli shifrlashni ta’minlash, tiklash kalitlarini ishonchli va xavfsiz joyda (masalan, parol menejerida) saqlash zarur.

Jamoa uchun dastlabki trening o‘tkazish, unda nafaqat texnik jihatlar, balki fishingni aniqlash asoslari, ijtimoiy muhandislik va jismoniy xavfsizlik asoslari ham tushuntiriladi.

Nazoratni kuchaytirish va raqamli izni kamaytirish uchun ijtimoiy tarmoqlardagi shaxsiy va umumiy sahifalarda maxfiylikni baholash va sozlashni amalga oshirish.

Jamoa ichida norasmiy qoidalarni ishlab chiqish — masalan, «barcha ish yozishmalarini faqat Signalda olib boramiz» yoki «parollarni Google Docs’da saqlamaymiz.» Bu hali xavfsizlik siyosati emas, lekin unga birinchi qadamlardir.

Mamlakat qonunchiligidagi asosiy “qizil chiziqlar” (ekstremizm, tuhmat to‘g‘risidagi qonunlar va h.k.) hamda ularning tashkilot faoliyatiga ehtimoliy ta’siri yuzasidan yurist yoki ekspert ishtirokida dastlabki huquqiy yo‘riqnoma o‘tkazish.

Kundalik amaliyot (Due Care): Bu, birinchi navbatda, barcha qurilmalarga dasturiy ta’minot yangilanishlarini o‘z vaqtida o‘rnatishdan iborat, chunki bu ma’lum zaifliklardan himoyalanishning asosiy usuli hisoblanadi. Bunga qurilmalarning jismoniy xavfsizligi amaliyoti ham kiradi — ish joyidan ketayotganda kompyuter ekranini bloklash odati. Ommaviy Wi-Fi nuqtalaridan foydalanilganda VPNdan foydalanish. Nihoyat, bu tanqidiy fikrlashni rivojlantirishning doimiy motivatsiyasi: shubhali so‘rovlarni tekshirish va jamoada har qanday shubhali xabarlar, tahdidlarni ochiq muhokama qilish, qulay muloqot muhitini yaratish. Shuningdek, NNT faoliyati va so‘z erkinligiga oid qonunchilikdagi o‘zgarishlar haqidagi yangiliklarni doimiy ravishda kuzatib borish muhim ahamiyatga ega.

2-daraja:
Rasmiylashtirilgan tashkiliy jarayonlarni joriy etish — xavfsizlik bo‘yicha tizimli ishlashga o‘tishga tayyor bo‘lgan jamoalar va ro‘yxatdan o‘tgan NNTlar uchun mo‘ljallangan.

Rejalashtirish va asosiy poydevorni tayyorlash (Due Diligence): Bu bosqichdagi asosiy qadam yagona Axborot xavfsizligi siyosatini ishlab chiqish va tasdiqlashdir. Ushbu hujjat parollarga, dasturiy ta’minotdan foydalanishga, ma’lumotlarni saqlashga, jismoniy xavfsizlikka qo‘yiladigan talablarni rasmiylashtiradi va barcha keyingi harakatlar uchun asos bo‘ladi. Eng kam imtiyozlar tamoyiliga asoslangan (xodimlarga faqat ish uchun mutlaqo zarur bo‘lgan ma’lumotlardan foydalanish imkoniyatini berish) kirish huquqini boshqarish tartibi joriy etiladi. Bundan tashqari, foydalanilayotgan tashqi xizmatlarning asosiy xavfsizlik bahosi o‘tkaziladi. Misol uchun, har bir xizmat uchun tekshiruv varaqasi tuzish mumkin: xavfsiz ikki bosqichli autentifikatsiya qo‘llab-quvvatlanadimi, rollar bo‘yicha kirish taqsimoti mavjudmi, zaxira nusxalari qanday yaratiladi va hokazo. Xuddi shu bosqichda barcha yangi xodimlar uchun xavfsizlik bo‘yicha kirish yo‘riqnomasi dasturi yaratiladi hamda stressni boshqarish, raqamli charchoq va asosiy psixologik o‘z-o‘ziga yordam berish bo‘yicha treninglar o‘tkaziladi. Bundan tashqari, tashkilot faoliyatining qonunchilikning barcha talablariga muvofiqligiga ishonch hosil qilish uchun yuridik va moliyaviy audit o‘tkazish zarur.

Kundalik amaliyot (Due Care): Ushbu darajadagi operatsion faoliyat yanada tizimli bo‘lishi kerak. Aslida, bu ishlab chiqilgan xavfsizlik siyosatini har kuni amalga oshirishdir. Zaxira nusxalarning ishlash qobiliyati muntazam ravishda tekshirilishi kerak, «3-2-1» zaxira nusxalash formulasiga tiklashda nol xato qo‘shiladi va formula «3-2-1-0» bo‘ladi. Shuningdek, asosiy xizmatlarga kirish huquqlari muntazam ravishda tekshirilishi kerak. Bu, ayniqsa, kadrlar qo‘nimsizligi yoki xodimlarning lavozimlari o‘zgarganda muhim ahamiyat kasb etadi. Tekshiruvning yo‘qligi tashkilotdan ketgan xodimning tashkilot xizmatlaridan foydalanishiga yoki amaldagi xodimning xizmatlar yoki hujjatlardan ortiqcha foydalanishiga olib kelishi mumkin. Xuddi shu darajada ma’lumotlarni majburiy kriptografik o‘chirishni o‘z ichiga olgan eski texnikani foydalanishdan xavfsiz chiqarish tartibi ishlab chiqilishi kerak. Jamoa uchun vaqti-vaqti bilan qisqa treninglar o‘tkazilishi va umumiy yig‘ilishlarda dolzarb tahdidlar, jumladan huquqiy, psixosotsial va iqtisodiy tahdidlar muhokama qilinishi kerak.

3-daraja:
Strategik va faol himoyani yaratish — xavf darajasi yuqori bo‘lgan muhitda ishlaydigan tashkilotlar uchun mo‘ljallangan bo‘lib, bunda tahdidlarni oldindan ko‘ra bilish va inqiroz sharoitida harakatlarni rejalashtirish zarur bo‘ladi.

Rejalashtirish va asosiy poydevorni tayyorlash (Due Diligence): Bu bosqichda tashkilot uchun strategik rejalashtirish asosiy bo‘ladi. Xavflarni baholash asosiy poydevorga aylanmoqda, uning asosida hodisalarga javob berishning batafsil rejasi (Incident Response Plan) — turli xil hujumlar (buzib kirish, doksing, DDoS) uchun bosqichma-bosqich harakatlar ssenariysi ishlab chiqilishi lozim. Bu reja faoliyatning uzluksizligini ta’minlash rejasi (Business Continuity Plan) bilan to‘ldiriladi, u halokatli ssenariylar amalga oshirilgan taqdirda tashkilot o‘z missiyasini qanday davom ettirishini tavsiflaydi. Nafaqat ofis, balki asosiy xodimlarning yashash joylari uchun ham jismoniy tahdidlarga qarshi protokollar ishlab chiqilishi kerak.

Shuningdek, xavfsizlik uchun mas'ul shaxsning rasmiy roli belgilanishi, tashqi ekspertlar (huquqshunoslar, IT-mutaxassislar) bilan aloqalar o'rnatilishi va inqiroz holati uchun aloqa rejasi ishlab chiqilishi kerak. Iqtisodiy tahdidlarga qarshi kurashish uchun tashkilotning bir necha oy davomida ishlashini ta'minlash uchun zaxira jamg'armasini shakllantirish zarur.

Kundalik amaliyot (Due Care): Ushbu bosqichda tashkilot hodisalarga shunchaki munosabat bildirmasdan, balki oldindan ko'ra bilishi va tayyorgarlik ko'rishi lozim. Buning uchun tahdidlarni erta aniqlash uchun o'zining raqamli izi va axborot maydonini muntazam ravishda kuzatib borishi kerak. Turli xarakterdagi hodisalarga javob berish rejasini va faoliyatning uzluksizligini ta'minlash rejasini tekshirish hamda ishlab chiqish uchun ichki hujum simulyatsiyalari va o'quv trevogalari o'tkazilishi lozim. Barcha ishlab chiqilgan siyosat va rejalar har yili qayta ko'rib chiqilishi va yangi sharoitga moslashtirilishi kerak.

3.3. NNT saytlari va media resurslarini himoya qilish choralari

Raqamli transformatsiya davrida NNT saytlari va onlayn platformalari ularning vazifalari uchun muhim infratuzilmaga aylandi. Biroq, bu ularni o'sib borayotgan kiberhujumlar oldida zaif qilib qo'ydi. Ayniqsa, inson huquqlari tashkilotlari, mustaqil ommaviy axborot vositalari va faollar guruhlari ayniqsa zaif bo'lib, ular jinoyatchilar va haktivistlar, shuningdek, davlat subyektlari, shu jumladan xorijiy subyektlar uchun ham nishon bo'lishi mumkin.

Onlayn resurslarni, xususan, veb-saytlarni samarali himoya qilish tizimini yaratish uchun tashkilot qanday turdagi tahdidlarga duch kelishi mumkinligini tushunish zarur. Barcha hujumlarni shartli ravishda to'rtta asosiy toifaga bo'lish mumkin, ularning har biri oldini olish va javob berishga o'ziga xos yondashuvni talab qiladi.

Resursning komprometatsiyasi (buzib kirish)

Bu toifaga begona shaxslar saytingizning «ichki qismi»ga — uning boshqaruv tizimi, serveri yoki administrator hisoblariga ruxsatsiz kiradigan barcha hodisalar kiradi. Bunday kirishning oqibatlari tajovuzkorning maqsadlariga qarab turlicha bo'lishi mumkin. Ba'zan bu ommaviy vandalism - defeys (deface) bo'lib, bosh sahifada begona xabar joylashtiriladi. Murakkabroq hollarda, bu ma'lumotni yashirincha o'zgartirishdir, ya'ni saytda sizning ishonchingizga putur yetkazish uchun raqamlar yoki faktlar sezdirmasdan o'zgartiriladi. Ko'pincha asosiy maqsad shaxsiy, moliyaviy va boshqa ma'lumotlarni o'g'irlashdir. Bundan tashqari, veb-saytingiz spam yuborish yoki tashrif buyuruvchilarning qurilmalarini zararlash uchun qurolga aylanishi mumkin. Shuningdek, buzib kirish natijasida saytdagi ma'lumotlar butunlay yo'q qilinishi mumkin.

Xizmat ko'rsatishni rad etish hujumi (DDoS hujumlari)

Bu toifa asosiy maqsadi saytingizni tashrif buyuruvchilar uchun mavjud bo'lmaydigan qilish, auditoriyangizning saytdan foydalanishiga deyarli imkon bermaydigan hujumlarni birlashtiradi. Qoida tariqasida, bu texnik hujum bo'lib, unda sizning resursingiz zararlangan qurilmalar tarmog'idan (botnet) foydasiz so'rovlarning katta oqimi bilan sun'iy ravishda qayta yuklanadi va u yuklamani boshqarish va foydalanuvchilar so'rovlariga javob berishni to'xtatadi. Ko'pincha bunday hujum qandaydir muhim voqealar, masalan, saylovlar, norozilik namoyishlari, auditoriyaga ma'lumot olish imkoniyatini bermaslik uchun qandaydir shov-shuvli materiallarni nashr etish paytida qo'llaniladi.

Huquqiy va ma’muriy bosim

Bu toifaga tashkilotingizning onlayn manbasi orqali unga bosim o‘tkazish uchun qonunlar va rasmiy tartib-qoidalardan foydalanish kiradi. Bu hokimiyat yoki boshqa tuzilmalar sanksiyalar, mamlakatda resursni bloklash yoki domen nomini qaytarib olish tahdidi ostida muayyan materiallarni olib tashlashni talab qilganda, kontentni majburiy o‘chirish (senzura) shaklida namoyon bo‘lishi mumkin. Shuningdek, bu saytdagi nashrlar yoki sharhlar tashkilotga qarshi ish qo‘zg‘atish uchun asos bo‘lgan hollarda qonuniy ta’qib orqali amalga oshirilishi mumkin.

Shaxsiyat va ishonchga qarshi hujumlar

Bu toifa sizning resursingizga emas, balki sizning nomingizga, brendingizga va auditoriyangiz ishonchiga qaratilgan tahdidlarni birlashtiradi. Bunday hujumlar tashrif buyuruvchilaringizni aldash uchun turli usullardan foydalanadi. Asosiy usullarga domen nomini o‘g‘irlash kiradi, bunda veb-manzilingiz nazorat qilinadi va tashrif buyuruvchilar soxta saytga yo‘naltiriladi. Yana bir mashhur usul — sizni obro‘sizlantirish yoki sizning nomingizdan xayriya yig‘ish uchun siznikiga juda o‘xshash manzillarda yoki sayt dizayni bilan bir xil bo‘lgan klon saytlarni yaratishdir. Bunday hujumlardan maqsad — yillar davomida qurgan obro‘yingizga putur yetkazishdir.

Avval ta’kidlanganidek, tahdidlarni tushunish xavfsizlik sari qo‘yilgan birinchi qadamdir. Keyingi qadam — ularning oldini olish va oqibatlarini yumshatish uchun aniq chora-tadbirlarni joriy etish. Quyida to‘rtta asosiy tahdid toifasiga muvofiq guruhlangan asosiy himoya strategiyalari keltirilgan.

Veb-resursni buzishga qarshi kurashish choralari

Ishonchli hosting provayderi — Hosting provayderini tanlash onlayn resursingizning xavfsizligi va barqarorligini belgilovchi asosiy qarordir. Baholashda texnik, huquqiy va operatsion omillar majmuasini ko‘rib chiqib, uzluksiz ishlash narxi va vaqtidan tashqariga chiqish lozim. Texnik ishonchlilik zamonaviy infratuzilmaning mavjudligini, DDoS hujumlaridan majburiy himoyani, shuningdek, tezkor tiklash imkoniyatiga ega avtomatlashtirilgan kundalik zaxiralash tizimini o‘z ichiga oladi. Huquqiy himoya ham muhim ahamiyatga ega: provayderning yurisdiksiyasi, uning maxfiylik siyosati va davlat organlarining so‘rovlariga javoban mijozlar manfaatlarini himoya qilishga tayyorligini baholash zarur. Ideal provayder o‘z faoliyatida shaffoflikni namoyish etishi va boshqa fuqarolik jamiyati tashkilotlarining fikr-mulohazalari bilan tasdiqlangan benuqson obro‘ga ega bo‘lishi kerak.

Operatsion ishonchlilik 24/7 texnik qo‘llab-quvvatlash sifati va mavjudligi, shuningdek, saytni boshqarish uchun boshqaruv panelining qulayligi bilan belgilanadi. Biroq, NNT uchun axloqiy jihat ham juda muhim: provayder nafaqat xizmatlarni taqdim etishi, balki inson huquqlari himoyachilari va mustaqil ommaviy axborot vositalari duch keladigan o‘ziga xos xavflarni ham tushunishi kerak. So‘z erkinligi qadriyatlarini baham ko‘radigan, fuqarolik jamiyatini faol qo‘llab-quvvatlaydigan va inqirozli vaziyatlarda, jumladan, buzib kirishga urinishlarni tekshirishda qo‘shimcha yordam ko‘rsatishga tayyor bo‘lgan kompaniyalarga ustunlik berilishi kerak.

VirtualRoad.org (https://www.qurium.org/) yoki eQPress loyihasi doirasidagi eQualitie kabi WordPress veb-saytlari uchun xavfsiz xosting (https://deflect.ca/solutions/hosting/) taqdim etuvchi maxsus xizmatlar, shuningdek, Cloudflare kompaniyasining Project Galileo (https://www.cloudflare.com/galileo/) kabi qo‘llab-quvvatlash dasturlari eng maqbul tanlovdir, chunki ular dastlab sektor duch keladigan tahdidlarga qarshi kurashish uchun mo'ljallangan va o'z xizmatlarini yuqori xavf darajasiga ega fuqarolik jamiyati tashkilotlariga bepul taqdim etadi.

Microsoft for nonprofits dasturi doirasida (https://nonprofit.microsoft.com/) Microsoft, shuningdek, o'zining Azure platformasidan foydalanish uchun yillik 2000 AQSh dollari miqdorida kredit taqdim etadi, undan xosting uchun ham foydalanish mumkin, ammo undan foydalanish o'rtacha NNT uchun murakkab bo'lishi mumkin va sozlash uchun texnik mutaxassis talab qilinishi mumkin.

Saytni boshqarishga xavfsiz kirishni ta'minlash — saytingizning administrativ paneliga, ya'ni kontent va sozlamalarni boshqarish tizimiga, shuningdek hosting paneliga kirish huquqlarini maksimal darajada himoya qilish zarur. Mustaqil ravishda amalga oshirilishi mumkin bo'lgan minimal choralar — murakkab va noyob parollardan foydalanish hamda ikki faktorli autentifikatsiyani (2FA) majburiy yoqishdir. Yaxshi hosting xizmatlarida bu odatda ro'yxatdan o'tish vaqtida standart tarzda sozlangan bo'ladi. WordPress, Drupal kabi kontentni boshqarish tizimlari (CMS) uchun uchinchi tomon modullaridan foydalanishga to'g'ri keladi. Texnik yordamni talab qilishi mumkin bo'lgan qo'shimcha himoya usullari faqat VPN orqali boshqaruv paneliga kirishni ta'minlash yoki standart kirish manzilini boshqasiga o'zgartirishdir. Bundan tashqari, parol bir necha marta noto'g'ri kiritilganda hisobni vaqtincha bloklashni sozlash mumkin.

Dasturiy ta'minotni o'z vaqtida yangilash — veb-resurslarning ko'plab buzilishlari yangilanmagan dasturiy ta'minot tufayli sodir bo'ladi, odatda bu kontentni boshqarish tizimi (CMS), qo'shimcha modullar (plaginlar) va sayt yozilgan platforma hisoblanadi. Ko'pincha veb-sayt ishlab chiquvchilar o'z vazifasiga « qo'l uchida» yondashadilar va xavfsizlikka e'tibor bermaydilar, natijada mijoz yangilanmaydigan yoki zaif mavzular, plaginlar yoki «qo'lda yozilgan» tizimlar holatida butunlay zaif va qo'llab-quvvatlanmaydigan tizimga ega bo'ladi. WordPress, Drupal, Joomla kabi eng mashhur tizimlarda o'rnatilgan avtomatik yangilash tizimlari mavjud bo'lib, ular tizim komponentlarini avtomatik ravishda yangilaydi. Bu xavfsizlik nuqtai nazaridan yaxshi va to'g'ri, ammo shuni yodda tutish kerakki, ishlab chiquvchilar, komponentlar va boshqa omillarga qarab, keng ko'lamli yangilanishlar paytida veb-sayt qisman yoki butunlay ishlamay qolishi mumkin. Shuning uchun, avvalo, saytning zaxira nusxalari mavjudligiga e'tibor qaratish lozim, shunda avvalgi versiyani qayta tiklash va texnik qo'llab-quvvatlash yordamida yangilash imkoniyati bo'ladi.

Zaxira nusxalash — buzg'unchilik kabi noxush hodisalardan so'ng tizimni tez va to'liq tiklashning asosiy vositasidir. Hatto eng mukammal himoya ham yetarli bo'lmasligi mumkin, masalan, platforma dasturchilari hali bexabar bo'lgan zero-day (nolinchi kun zaifliklari) mavjud bo'lgan hollarda. Bunday zaifliklardan hatto to'liq yangilangan tizimlarda ham foydalanish mumkin. Bunday vaziyatda ziyonkor kod mavjudligini istisno qilish uchun eng yaxshi usul — tizimni zaxira nusxasidan tiklashdir. Agar buzg'unchilik qachon sodir bo'lgani aniq bo'lmasa, tizimni avvalroq yaratilgan nusxadan tiklashga to'g'ri kelishi mumkin. Xosting-provayderingiz muntazam ravishda zaxira nusxalarini yaratib, ularning turli versiyalarini saqlashiga ishonch hosil qiling. Agar tashkilotda texnik mutaxassis bo'lsa, zaxira nusxalarini yaratish va ularning versiyalarini saqlab borish uning vazifalariga kirishi lozim. Zaxira nusxalarini yaratish davriyligi resursning yangilanish tezligiga bog'liq. Odatda, o'zingizga savol berishingiz kerak: tiklash ishlari imkon qadar kam vaqt va kuch talab qilishi uchun nusxalar qanchalik tez-tez olinishi kerak?

Tashqi himoya xizmatlari — buzib kirish ehtimolini kamaytirish uchun, shu jumladan zero-day (nolinchi kun zaifliklaridan) foydalangan holda, WAF (Web Application Firewall) kabi qoʻshimcha xizmatlar qoʻllanilishi mumkin, bu himoya mexanizmi boʻlib, aksariyat buzib kirish urinishlarini veb-resursga yetib bormasdan turib toʻxtatadi. Odatda, bunday funksiyani taqdim etuvchi xizmatlar bitta tugma bilan texnik tafsilotlarga e'tibor bermasdan asosiy toʻplamni yoqish imkoniyatiga ega. Masalan, yuqorida tilga olingan Cloudflare kompaniyasining Project Galileo loyihasi asosiy sozlamalar toʻplamini oddiy yoqish imkoniyatiga ega boʻlgan korporativ darajadagi WAFni oʻz ichiga oladi. CMS uchun WAF plaginlari ham mavjud, masalan, Wordpress uchun Wordfence va Joomla uchun Akeeba Admin Tools, ammo ular uchun funksionallikning katta qismi pullik.

DDoS hujumlariga qarshi choralar

Hozirgi vaqtda DDoS hujumlari kichik bir mamlakatning internet iste'moli bilan taqqoslanadigan ulkan miqdorlarga yetishi mumkin. Qayd etilgan eng muhim hujumlardan biri 2025-yilda sodir boʻlgan va 29,7 Tbit/s ni tashkil etgan. Bu bir soniyada saytdan taxminan 7000 ta filmni HD sifatda yuklab olish bilan barobar. Taxminlarga koʻra, hujumda 1 milliondan ortiq zararlangan qurilmalar ishtirok etgan. Katta resurslarga ega boʻlmasdan turib, bunday hujumlarni, hatto kamroq kuchga ega boʻlganlarini ham yengish deyarli imkonsiz, shuning uchun eng samarali usul — zarbani oʻz zimmasiga oladigan ixtisoslashgan vositachi xizmatlardan foydalanishdir. Yuqorida tilga olingan Cloudflare Project Galileo, VirtualRoad.org, eQualitie kabi tashkilotlar fuqarolik jamiyati uchun DDoS-hujumlardan himoyani taqdim etadi.

Huquqiy va ma'muriy tazyiqqa qarshi kurashish choralari

Ushbu turdagi tahdidlardan himoyalanish asosan huquqiy va protsessual jihatdan, xususan, qonunchilikka rioya qilish, huquqshunoslar bilan maslahatlashish va malakali tahririyat siyosatining mavjudligi bilan bogʻliq. Shu bilan birga, tayyorgarlik ishlarini olib borish va bunday tahdidlar amalga oshirilganda ishni davom ettirish imkonini beruvchi texnik jihatlar mavjud.

Birinchi navbatda, bu mamlakat ichidagi resurslarning mavjudligini minimallashtirishni oʻz ichiga oladi, masalan, mamlakat ichidagi resursni joylashtirish va mamlakat zonasidagi domen nomi. Hosting provayderi yoki domen hududi administratoriga ma'muriy bosim oʻtkazilganda, resursingiz oʻchirilishi yoki olib tashlanishi, domen nomi esa olib qoʻyilishi mumkin. Buning oldini olish uchun mamlakatdan tashqarida ishonchli hostingni ta'minlang va umumiy domen nomidan foydalaning (masalan, .org, ,info, .ngo). Shuningdek, koʻzgu saytlarining (mirror sites) mavjudligini va Cloudflare yoki Akamai kabi kontent tarqatish tarmoqlaridan (CDN) foydalanishni ham hisobga oling. Va, albatta, zaxira nusxa olishni unutmang.

Shaxsiyat va ishonchga qarshi hujumlarga qarshi choralar

Ushbu toifadagi tahdidlarning aksariyati yomon nazorat qilinadi, shuning uchun ular odatda sizning nazoratingiz doirasidan tashqarida boʻladi. Ammo avval aytib oʻtilganidek, tahdidlar haqidagi bilim bizga ularga javob berish imkonini beradi, shuning uchun raqamli muhitni kuzatishni oʻzingizga odat qiling, vaqti-vaqti bilan sizning nomingizga oʻxshash saytlarni qidiring, bu ijtimoiy tarmoqlardagi sahifalarga ham tegishli. Soxta hisoblar haqidagi barcha xabarlarni tekshiring. Soxta klon saytlarni aniqlaganingizda, ularning xosting provayderi va domen registratoriga shikoyat bilan murojaat qiling, ijtimoiy tarmoqlar holatida rasmiy shikoyat kanallaridan foydalaning, shuningdek, barcha mavjud kanallar orqali auditoriyangizni ogohlantiring. Oʻz tomoningizdan saytingizning domen nomini himoya qilishingiz kerak. U qayerda va kimga roʻyxatdan oʻtkazilganini hamda uning sozlamalariga qanday kirishni bilishingizga ishonch hosil qilishingiz kerak. Koʻpincha bu bilan veb-sayt ishlab chiquvchilari shugʻullanadilar, uni oʻzlariga rasmiylashtiradilar va mavjud xavfsizlik imkoniyatlaridan (murakkab parol, ikki bosqichli autentifikatsiya, domenni koʻchirishni taqiqlash) foydalanmaydilar. Natijada, domen nomi bilan bogʻliq muammolar yuzaga kelganda, masalan, domen oʻgʻirlanganda, tashkilot uni qaytarib olishi juda qiyin yoki imkonsiz boʻlishi mumkin. Shuningdek, veb-resursingizning haqiqiy xavfsizlik sertifikatiga ega ekanligiga ishonch hosil qilish muhimdir. Bunday sertifikatning yoʻqligi auditoriyaning saytingizga boʻlgan ishonchini pasaytirishi mumkin, chunki ulanish shifrlanmagan boʻladi va trafik ushlab qolinishi yoki oʻzgartirilishi mumkin, shuningdek, baʼzi antivirus dasturlari hozirda bunday saytlarga kirishni bloklaydi. Aksariyat ishonchli xostinglar bunday imkoniyatni sukut boʻyicha taqdim etadi. Agar bunday imkoniyat boʻlmasa, Let's Encrypt (letsencrypt.org) yordamida bepul sertifikat olish mumkin, bu esa baʼzi texnik koʻnikmalarni talab qiladi.

Hodisalarni tergov qilish va tahdidlarga javob qaytarish

Xavfsizlik hodisasi yuz berganda — bu saytning buzilishi, xodimga tahdidlar yoki muvofiqlashtirilgan hujum boʻladimi — birinchi reaksiya deyarli har doim tartibsizlik va vahima, tizimsiz muvofiqlashtirilmagan harakatlar boʻlib, bu koʻpincha vaziyatning yomonlashishiga, tergov uchun izlarning yoʻqolishiga va boshqa tegishli yoʻqotishlarga olib keladi. Shuning uchun, har qanday hodisa yuz berganda, aniq, bosqichma-bosqich harakat rejasiga amal qilish kerak. Samarali javob nafaqat zararni kamaytiradi, balki kelajakda hodisa yoki uning oqibatlarini kamaytirish va tezroq tiklanish uchun saboq olishga yordam beradi.

Aniqlash, dastlabki chora-tadbirlar va hujjatlashtirish

Hodisa aniqlangandan keyingi dastlabki daqiqalar va soatlar juda muhimdir. Ushbu bosqichdagi asosiy vazifa — hodisada jabrlangan tashkilot va resurslar uchun masʼul shaxslarni ogohlantirishdir. Birinchi navbatda, bu tashkilot direktori, IT mutaxassisi, agar u boʻlsa, tegishli yoʻnalish rahbarlari (saytni buzib kirish holatlarida sayt yoki ijtimoiy tarmoqlar administratori, tahdidlar paytida HR mutaxassisi, maʼlumot sizib chiqqanda loyiha rahbari va boshqalar). Axborot sizib chiqishining oldini olish uchun zudlik bilan javob qaytarish guruhini tuzish va hodisa yuzasidan barcha muloqotlarni, masalan, Signal kabi himoyalangan kanallar orqali olib borish lozim. Sodir boʻlayotgan barcha voqealarni: vaqti, alomatlari, koʻrilgan choralarni qayd etib, hodisa jurnalini yuritishni boshlash juda muhim. Bu hujjatlar keyingi tahlil uchun asos boʻlib xizmat qiladi. Hech qanday holatda hujum izlarini darhol yoʻqotish mumkin emas; bu bilan muammoni hal qila olmaysiz, aksincha, muhim dalillarni yoʻq qilasiz, xolos. Buning oʻrniga skrinshotlar qilib, log fayllarining nusxalarini saqlab qoʻyish kerak, chunki bu maʼlumotlar keyingi tekshiruv uchun muhim boʻlishi mumkin. Agar hodisadan zarar koʻrgan qurilma faol ishlatilayotgan boʻlsa (spam tarqatayotgan, unda qandaydir harakatlar sodir boʻlayotgan boʻlsa), uni darhol tarmoqdan uzish kerak (tarmoq kabelini jismonan sugʻurib olish yoki Wi-Fiʼni oʻchirish lozim). Qurilmani butunlay oʻchirish yaramaydi, chunki bu muhim izlarni yoʻqotib yuborishi mumkin. Sayt buzilgan taqdirda, uni texnik xizmat koʻrsatish rejimiga oʻtkazsa boʻladi. Vaziyatni baholashda professional koʻmak beradigan Access Now (https://www.accessnow.org/) kabi ixtisoslashgan tashkilotlarning Digital Security Helpline (help@accessnow.org) xizmatiga tashqi ekspert yordami uchun zudlik bilan murojaat qilish zarur. Shuni yodda tutish kerakki, Access Now birinchi murojaatingizda maqomingizni tasdiqlash uchun sizni ishonchli hamkorlar orqali tekshirishi lozim va bu jarayon biroz vaqt talab qilishi mumkin. Shu sababli, hodisalarga oldindan tayyorgarlik koʻrgan maʼqul: hodisa yuz berganda zudlik bilan yordam olish uchun tashkilotning elektron pochtasidan

Access Now’ga keyingi murojaatlar uchun tekshiruvdan o‘tkazishni so‘rab, oldindan xat yozib qo‘ying. Digital Security Helpline ijtimoiy tarmoqlar va boshqa tashkilotlar bilan o‘zaro aloqa kabi keng qamrovli masalalarga ixtisoslashgan. Veb-resurslarga qilingan hujumlar va dezinformatsiya kampaniyalarini tekshirish bo‘yicha Qurium — The Media Foundation (https://www.qurium.org/rapid-response/request/) tashkilotiga ham murojaat qilish mumkin.

Zararni tahlil qilish va baholash

Keyinchalik, texnik mutaxassislar bilan birgalikda hujum yo‘nalishini aniqlash uchun tahlil o‘tkazish kerak: bu buzilgan parol, dasturiy ta’minotdagi zaiflik yoki fishing natijasi bo‘lganmi. Hujumchi tizimga qanday qilib kirganini tushunish ushbu zaiflikni bartaraf etishning kalitidir. Zararni baholash hodisa tergovi bilan parallel ravishda amalga oshiriladi: ma’lumotlar o‘g‘irlanganmi yoki o‘zgartirilganmi, resurs boshqalarga hujum qilish uchun ishlatilganmi va hodisa qanchalik keng tarqalishi (boshqa qurilmalarga yoki boshqa odamlarga ta’sir qilishi) mumkin.

Oqibatlarni bartaraf etish, tiklash va aloqa

Bu bosqichda bevosita oqibatlar bartaraf etiladi va normal ishlashga qaytiladi. Buzib kirilgan sayt uchun eng ishonchli usul uni zararli kodlardan «tozalashga» urinish emas, balki ataylab toza zaxira nusxasidan to‘liq tiklashdir. Har qanday akkauntni buzish zudlik bilan buzilgan tizim bilan bog‘liq barcha parollarni o‘zgartirish va ikki bosqichli autentifikatsiyani yoqish bilan birga amalga oshirilishi kerak. Oshkor etilgan qurilmalar holatida, tizimni to‘liq qayta o‘rnatish yoki zavod sozlamalariga qaytarish to‘g‘ri bo‘ladi. Ta’sirlangan tomonlar bilan muloqot qilish muhim qadamdir. Agar foydalanuvchilarning shaxsiy ma’lumotlari sizib chiqsa, ularni bu haqda xabardor qilish va kerakli ma’lumotlarni qanday taqdim etish bo‘yicha huquqshunoslar bilan maslahatlashish lozim.

Hodisadan keyingi xulosalar

Vaziyat barqarorlashgandan so‘ng, voqeani ichki tahlil qilish zarur. Ushbu tahlilning maqsadi aybdorlarni topish emas, balki jarayonlar va texnologiyalardagi zaif nuqtalarni aniqlashdir. Xulosalarga asoslanib, ichki xavfsizlik siyosatlarini yangilash, hodisalarga javob berish tartib-qoidalarini yaratish yoki yangilash, jamoa uchun qo‘shimcha treninglar o‘tkazish va yangi texnik himoya vositalarini joriy etish lozim. Bunday yondashuv har bir hodisani kelajakda tashkilotni yanada barqaror qiladigan saboqqa aylantiradi.

Huquqni muhofaza qilish organlariga murojaat qilish

Politsiyaga rasmiy ariza berish masalasi NNT uchun ancha murakkab va xavfli hisoblanadi. Bir tomondan, rasmiy bayonot hodisa faktini qayd etadi, bu esa o‘g‘irlangan ma’lumotlar yoki buzilgan resurs sizning nomingizdan noqonuniy faoliyat uchun ishlatilsa, huquqiy himoya vazifasini o‘tashi mumkin. Boshqa tomondan, “jabrlanuvchining gumonlanuvchiga aylanishi” kabi jiddiy xavf ham bor: tergov doirasida huquq-tartibot idoralari butun texnikangizni olib qo‘yishi va shu orqali faoliyatingiz, benefitsiarlaringiz va hamkorlaringizga oid maxfiy ma’lumotlarga qonuniy kirish imkoniyatiga ega bo‘lishi mumkin.

Bu qaror faqat mamlakatdagi siyosiy vaziyatni, huquqiy tizimga bo‘lgan ishonch darajasini va oshkor etilishi mumkin bo‘lgan ma’lumotlarning nozikligini hisobga olgan holda xavflarni sinchkovlik bilan baholagandan so‘ng qabul qilinishi kerak. Huquqni muhofaza qilish organlari bilan har qanday aloqadan oldin faollarni himoya qilishga ixtisoslashgan ishonchli advokatdan maslahat olish oltin qoidadir.

Xulosa

Raqamli muhit notijorat tashkilotlar faoliyatining ajralmas qismiga aylandi. U muloqot, ma’lumotlarga kirish, loyihalarni amalga oshirish va auditoriya bilan muloqot qilish uchun yangi imkoniyatlar ochadi. Shu bilan birga, raqamlashtirish mas’uliyat, huquqiy savodxonlik va xavflarni boshqarishga bo‘lgan talablarni kuchaytiradi.

Ushbu qo‘llanmada ko‘rsatilganidek, raqamli huquqlar mavhum kategoriya emas, balki NNTlarning kundalik faoliyatiga bevosita ta’sir ko‘rsatuvchi amaliy vositadir. Ma’lumotlarga kirish, shaxsiy ma’lumotlarni himoya qilish, kontentni e’lon qilish qoidalari, davlat organlari va onlayn platformalar bilan hamkorlik — bu masalalarning barchasi ongli va tizimli yondashuvni talab qiladi.

Shuni hisobga olish muhimki, huquqlarning rasmiy kafolatlari har doim ham ularni amalda avtomatik ravishda amalga oshirishni anglatmaydi. NNTlar bir vaqtning o‘zida milliy qonunchilik, xalqaro standartlar va raqamli platformalar qoidalari amal qiladigan muhitda faoliyat yuritadi. Bu tartibga solishning bir necha darajalarida mo‘ljal olish va huquqiy hamda obro‘-e’tibor oqibatlarini hisobga olgan holda puxta o‘ylangan qarorlar qabul qilish qobiliyatini talab etadi.

Risklarni boshqarish alohida ahamiyat kasb etadi. Nozik ma’lumotlar bilan ishlash, kontent nashr etish, auditoriya va hamkorlar bilan muloqot qilish — bularning barchasi tashkilotning o‘ziga ham, uning benefitsiarlariga ham ta’sir qilishi mumkin bo‘lgan potensial tahdidlar bilan bog‘liq. Bunday sharoitda ma’lumotlarni, axborot manbalarini himoya qilish va aloqa barqarorligini ta’minlashga qaratilgan ichki siyosat, tartib-qoidalar va amaliyotlarni ishlab chiqish muhim ahamiyatga ega.

Qo‘llanma barcha mumkin bo‘lgan vaziyatlarga universal javob berish maqsadini ko‘zlamaydi. Uning vazifasi o‘quvchida raqamli huquqlar mantiqini tushunish, asosiy xavf-xatarlarni ko‘rsatish va muayyan sharoitlarda qaror qabul qilish vositalarini taklif etishdan iborat.

Shunday qilib, bugungi kunda nodavlat notijorat tashkilotlarining raqamli muhitda samarali faoliyat yuritishi huquqiy xabardorlik, amaliy ko‘nikmalar hamda kommunikatsiya va xavfsizlikka strategik yondashuvni uyg‘unlashtirmasdan mumkin emas. Aynan shu uyg‘unlik nafaqat xavf-xatarlarni kamaytirish, balki raqamli vositalardan jamiyat manfaatlari yo‘lida maksimal darajada samarali foydalanish imkonini beradi.

ILOVALAR

1-ilova

O‘zbekiston Respublikasining shaxsiy ma’lumotlar to‘g‘risidagi qonunchiligining asosiy talablarini bajarish bo‘yicha nazorat ro‘yxati

Manba: https://www.itts.uz/contacts

	Talab	Korxonada talab qanday amalga oshirilgan? Oddiyroq — Bor/Yo‘q yoki +/- Yaxshiroq — mas’ul shaxslar ismlari, buyruq raqamlari, hujjat nomlari va boshqalarni ko‘rsatish	Manba normativ-huquqiy hujjat	URL, NHH bandiga havola
1	Korxonada shaxsga doir ma’lumotlarni qayta ishlash uchun huquqiy asoslar belgilanganmi? Qanday asoslar? (yozma rozilik, shartnoma ijrosi, NHH talablari)		O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 18-modda	https://lex.uz/docs/4396428#4398418
2	Shaxsiy ma’lumotlarni qayta ishlashga rozilikning namunaviy shakllari ishlab chiqilganmi?			
3	Shartnomalarning namunaviy shakllariga shaxsga doir ma’lumotlarni qayta ishlash to‘g‘risidagi bandlar kiritilganmi?			
4	Subyekt bilan tuzilgan shartnoma muddati tugaganidan keyin shaxsiy ma’lumotlar qayta ishlanadimi? Ha bo‘lsa, qanday asosda?			
5	Shaxsiy ma’lumotlarni qayta ishlashga rozilik shakli qonunchilik talablariga javob beradimi, unga barcha majburiy maydonlar kiritilganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘i, 11-band	https://lex.uz/docs/6663967#6664336
6	Barcha tegishli shaxsiy ma’lumotlar bazalari davlat reyestrida ro‘yxatdan o‘tkazilganmi?		O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 31-modda	https://lex.uz/docs/4396428#4398788

7	Shaxsiy ma’lumotlarni qayta ishlashga subyektning roziligi qanday qayd etiladi? Rozilik berilgan sana/ vaqt/qurilma identifikatori/IP-manzil saqlanadimi?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 21-modda	https://lex.uz/ docs/4396428#4398514
8	Rozilik berilgan shaklda uni qaytarib olish		
9	imkoniyati mavjudmi? Rozilikni qaytarib olishni elektron hujjat shaklida yuborish imkoniyati bormi?		
10	Subyektlarning so‘rovlari bo‘yicha shaxsiy ma’lumotlarga ishlov berish to‘g‘risidagi ma’lumotlarni qaysi bo‘linma taqdim etadi?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 22-modda	https://lex.uz/ docs/4396428#4398536
11	Shaxsga doir ma’lumotlar subyektining murojaati asosida shaxsga doir ma’lumotlarni bloklash va yo‘q qilish tartibi belgilanganmi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘ining 30.13-bandi	https://lex.uz/ docs/6663967#6664487
12	Shaxsga doir ma’lumotlarga bir-biriga mos kelmaydigan maqsadlarda ishlov berilayotgan bo‘lsa, ma’lumotlar bazalari ajratilganmi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘ining 5-bandi	https://lex.uz/ docs/6663967#6664304
13	Subyekt uning shaxsiy ma’lumotlari shaxsiy ma’lumotlar bazasiga kiritilgani to‘g‘risida qanday xabardor qilinadi?	O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 23-modda	https://lex.uz/ docs/4396428#4398628
14	Subyektning shaxsiy ma’lumotlari uchinchi shaxslarga berilganda u qanday xabardor qilinadi?		
15	Uchinchi shaxslar ro‘yxati shakllantirilganmi? Uni kim va qanday qilib dolzarblashtiradi?		
16	Korxonada shaxsiy ma’lumotlarga to‘liq avtomatlashtirilgan ishlov berish, masalan, skoring amalga oshiriladimi?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 24-modda	https://lex.uz/ docs/4396428#4398652
17	Subyektning shaxsiy ma’lumotlarini to‘liq avtomatlashtirilgan holda qayta ishlashga roziligini qanday olish mumkin? Bunday qayta ishlashning huquqiy asosi qanday?		

18	Maxsus shaxsiy ma'lumotlar (sog'lig'i, oila tarkibi, millati haqidagi ma'lumotlar) qayta ishlanadimi?* *Maxsus shaxsiy ma'lumotlarga ishlov berish taqiqlanadi, cheklangan holatlar bundan mustasno.	O'zbekiston Respublikasining «Shaxsiy ma'lumotlar to'g'risida»gi Qonuni, 25-modda	https://lex.uz/docs/4396428#4398682
19	Korxonada biometrik shaxsiy ma'lumotlar (fotosuratlar, barmoq izlari va boshqalar) qayta ishlanadimi?	O'zbekiston Respublikasining «Shaxsiy ma'lumotlar to'g'risida»gi Qonuni, 26-modda	https://lex.uz/docs/4396428#4398727
20	Bunday ishlov berishning huquqiy asoslari qanday? Subyekt/xodim bunday ishlov berishga rozilik berganmi?		
21	Korxonada biometrik KNBT mavjudmi? Uning ma'lumotlar bazasi shaxsiy ma'lumotlar bazalari davlat reestrida ro'yxatdan o'tkazilganmi? KNBT bazasiga kiritilgan barcha shaxslarning yozma roziligi olinganmi?		
22	Biometrik/genetik ma'lumotlarni o'z ichiga olgan moddiy manbalarni hisobga olish qanday amalga oshiriladi?	5.10.2022-yildagi 570-son VMQga 2-ilovaning 5-bandi	https://lex.uz/ru/docs/6225462#6227477
23	Biometrik ma'lumotlarni shifrlash va kriptografik himoyalash talabi qanday amalga oshirilgan?	5.10.2022-yildagi 570-son VMQga 2-ilovaning 4-bandi	https://lex.uz/ru/docs/6225462#6227475
24	Biometrik ma'lumotlar tashuvchilarga grif qo'yilganmi? Tashuvchilarning jismoniy xavfsizligini ta'minlash uchun qanday aniq majburiy choralar qo'llaniladi? Biometrik ma'lumotlarga kirish huquqiga ega bo'lgan qurilmalarning IP va MAC manzillari qayd etiladimi?	05.10.2022-yildagi 570-son VMQga 2-ilovaning 2-bobi.	https://lex.uz/ru/docs/6225462#6227469
25	O'zbekiston fuqarolarining shaxsga doir ma'lumotlariga (ShDMa) qayerda va qanday ishlov beriladi? Ishlov beriladigan uskunalar jismonan qayerda joylashgan? Yurisdiksiya ma'lumotlarni yetarli darajada himoya qiladigan mamlakatlar ro'yxatiga kiritilganmi? Operatorning standart shartnoma shartlari va korporativ qoidalari vakolatli davlat organi talablariga javob beradimi? Operator shaxsga doir ma'lumotlarni boshqarish va saqlash sohasidagi xalqaro standartlarga rioya qiladimi?	O'zbekiston Respublikasining «Shaxsiy ma'lumotlar to'g'risida»gi Qonuni, 27.1-modda	https://lex.uz/docs/4396428#5271076

26	Shaxsiy ma’lumotlarning boshqa davlatlarga uzatiladimi? (transchegaraviy uzatish) Qaysi mamlakatlar hududiga?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 15-modda	https://lex.uz/docs/4396428#4398348
27	Korxona vazifalarini bajarish uchun zarur va yetarli bo‘lgan shaxsiy ma’lumotlarning tasdiqlangan tarkibi?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 31-modda	https://lex.uz/docs/4396428#4398788
28	Shaxsiy ma’lumotlarni qayta ishlash va himoya qilish bilan bog‘liq ishlar uchun mas’ul bo‘lgan tarkibiy bo‘linma yoki mansabdor shaxs belgilanganmi?		
29	Shaxsga doir ma’lumotlarga ishlov berish muddatlari belgilanganmi (har bir toifa, har bir baza bo‘yicha)? Bu muddatlar qanday?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 10 va 19-moddalar	https://lex.uz/docs/4396428#4398106
30	Korxonada shaxsiy ma’lumotlar bilan tarixiy, statistik, sotsiologik yoki ilmiy tadqiqotlar o‘tkaziladimi? Bunda ushbu shaxsiy ma’lumotlar majburiy ravishda shaxssizlashtiriladimi?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 16-modda	https://lex.uz/docs/4396428#4398378
31	Shaxsiy ma’lumotlar yo‘q qilinadimi? Kim, qanday? Buni qaysi hujjat tartibga soladi?	O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 17-modda	https://lex.uz/docs/4396428#4398388
32	Har bir shaxsiy ma’lumotlar bazasi uchun dolzarb bo‘lgan tahdid turlari aniqlanganmi? Har bir bazaga himoya darajalari belgilanganmi?	5.10.2022-yildagi 570-son VMQning 2-bandi	https://lex.uz/uz/docs/6225462#6227189
33	Shaxsiy ma’lumotlar bazalarining har biri uchun ularga berilgan himoya darajasi asosida axborot xavfsizligi talablari bajarilayaptimi? Muayyan bazaga qanday aniq choralar qo‘llaniladi?	O‘zbekiston Respublikasi VM2022-yil 5-oktyabrdagi 570-son qarori, 10-bob	https://lex.uz/uz/docs/6225462#6227279
34	Shaxsiy ma’lumotlar himoyasini ta’minlash uchun mas’ul bo‘linma bevosita korxona rahbariga bo‘ysunadimi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3477-son buyrug‘I, 3-band	https://lex.uz/docs/6663969#6668986

35	Shaxsiy ma’lumotlar bazasi vaqti-vaqti bilan tekshirib turiladimi? Ro‘yxatga olish ma’lumotlarining dolzarbligi oxirgi marta qachon tekshirilgan?	Adliya vazirligining 2023-yil 15-noyabrdagi 3477-sonli buyrug‘I, 8-band	https://lex.uz/docs/6663969#6669029
36	Korxonaning shaxsga doir ma’lumotlar bazalari bilan ishlash huquqiga ega bo‘lgan xodimlari ro‘yxati shakllantirilganmi?		
37	Shaxsiy ma’lumotlar bilan ishlovchilar (jurnalistlar, IT, kadrlar, huquqshunoslar) uchun seminarlar yoki treninglar o‘tkaziladimi?		
38	Ruxsatsiz kirish natijasida yo‘q qilingan yoki shikastlangan shaxsiy ma’lumotlarni tiklash imkoniyati ta’minlanganmi?		
39	Agar shaxsiy ma’lumotlarga ishlov berish oferta asosida amalga oshirilayotgan bo‘lsa, unda ishlov berishning aniq maqsadlari ko‘rsatilganmi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘I, 9-band	https://lex.uz/docs/6663967#6664327
40	Korxonada videokuzatuv amalga oshiriladimi? Nima maqsadda? Qanday shaxsiy ma’lumotlar qayta ishlanadi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘I, 12-band	https://lex.uz/docs/6663967#6664354
41	Shaxsiy ma’lumotlarni qayta ishlash va himoya qilish bo‘yicha mulkdor/operator siyosatini belgilovchi ichki hujjatlar tasdiqlanganmi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘I, 30.12-bandi	https://lex.uz/docs/6663967#6664485
42	Kadrlar ishini yuritishda xodimning shaxsiy ma’lumotlarini himoya qilish bo‘yicha O‘zbekiston Respublikasining yangi Mehnat kodeksi talablari inobatga olinadimi?	6-§. O‘zbekiston Respublikasi Mehnat kodeksining xodimning shaxsiy ma’lumotlarini himoya qilish	https://lex.uz/ru/docs/6257291#6262031
43	Agar xodimning shaxsiy ma’lumotlari uchinchi shaxslardan olinayotgan bo‘lsa (sudlanganlik, dispanserlarda hisobda turish), xodim bu haqda oldindan yozma ravishda xabardor qilinadimi va undan yozma rozilik olinganmi?	O‘zbekiston Respublikasi Mehnat kodeksi, 176-modda	https://lex.uz/ru/docs/6257291#6262106

44	Xodim ish beruvchida saqlanayotgan barcha shaxsiy ma’lumotlaridan to‘liq foydalana oladimi? Ulardan nusxa ko‘chirishi mumkinmi?	O‘zbekiston Respublikasi Mehnat kodeksi, 179-modda	https://lex.uz/ru/docs/6257291#6262129
45	*Rozilik shakllari va takliflarda «dark patterns» mavjud emas: • ishlov berishga rozilik belgisi va bayroqchalar shaxsiy ma’lumotlar avtomatik tarzda kiritilmagan bo‘lsa; • shartlarga rozilik tugmasi faqat subyekt taklif etilayotgan shartnoma (oferta) ning barcha sahifalarini to‘liq ko‘rib chiqqandan so‘ng bosilishi mumkin; • belgilar qo‘yish va shartlar bilan tasdiqlash tugmasini bosish fakti sana, vaqt, IP-manzil va mijoz identifikatorini ko‘rsatgan holda qayd etilishi shart * talablar faqat tijorat banklariga taalluqli	O‘zR MBning 2018-yil 2-iyuldagi 3030-sonli Qarori, 28-bandi	https://lex.uz/docs/3804290#3805017
46	Axborot xavfsizligini boshqarish tizimiga (AXBT) shaxsiy ma’lumotlarni himoya qilish joriy etilganmi?	Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘ining 31-bandi A.5.34 ISO/IEC 27001:2022 A.18.1.4 O‘z DSt ISO/IEC 27001:2020	https://lex.uz/docs/6663967#6664488 https://stt2.unicon.uz/#/post/772

2-ilova

Shaxsiy ma’lumotlarga ishlov berish tartib-taomillarining universal nazorat ro‘yxati

A. Shaxsiy ma’lumotlarni qayta ishlash jarayonlari va shaxsiy ma’lumotlar bazalari reestri
- Shaxsiy ma’lumotlarni qayta ishlash jarayonlari reestri tuzildi (maqsadlar, asoslar, subyektlar toifalari, ma’lumotlar tarkibi, qabul qiluvchilar, saqlash muddatlari).
- Shaxsiy ma’lumotlar bazalari reestri tuzildi.
- Shaxsiy ma’lumotlar bazalari ro‘yxatga olindi.
- Har bir jarayonning egasi tayinlandi.
- Tahdidlar baholandi va baholash dalolatnomasi tuzildi
- Shaxsiy ma’lumotlarni qayta ishlash siyosati tasdiqlandi

B. Shaxsiy ma’lumotlarni yig‘ish va xabardor qilish tartibi
- Для каждого канала сбора определены цели и основания.
- Подготовлен текст уведомления субъекту при включении в базу.
- Настроены формы/скрипты (веб-сайт, анкеты, договоры, HR-формы).
- Исключены лишние поля («на всякий случай» не считается основанием).

C. Rozilik berish tartibi
- Rozilik olinganlik faktini tasdiqlash imkonini beradigan shaklda qayd etiladi.
- Maxsus ma’lumotlar uchun — yozma rozilik (shu jumladan elektron hujjat).
- Rozilik isboti (log, imzolangan hujjat, yozuvli chek-boks) saqlanadi.
- Fikr-mulohaza o‘sha shaklda yoki yozma ravishda (shu jumladan elektron shaklda) qabul qilinadi.

D. Kirish va ichki foydalanish tartibi
- Kirish matritsasi (role-based) kiritildi.
- Foydalanish huquqi talabnoma bo‘yicha va zaruriyat prinsipiga ko‘ra beriladi.
- Kirish va operatsiyalar jurnallari yuritiladi.
- Nusxalash, tushirish, olinadigan tashuvchilar tartibga solingan.
- Olinadigan tashuvchilarni saqlash joylari reglamentlangan.

E. Ma’lumotlarni o‘zgartirish tartibi va sifati
- Tasdiqlovchi hujjatlar bo‘yicha ma’lumotlarni tuzatish/aniqlashtirish uchun kanal mavjud.
- Agar tuzatish imkoni bo‘lmasa, yo‘q qilish ko‘zda tutilgan.
- Muhim ma’lumotlarni (aloqalar, hujjatlar) yangilash muddatlari belgilandi.

F. Shaxsiy ma’lumotlar subyektlarining so‘rovlari bilan ishlash tartibi
- Shaxsiy ma’lumotlar subyektiga ularning ma’lumotlariga ishlov berish to‘g‘risida taqdim etiladigan axborot tarkibi tavsiflangan.
- Ariza beruvchini identifikatsiya qilish yolga qo‘yilgan.
- Hujjatlarni to‘xtatib turish/yo‘q qilish uchun elektron shaklda yuborish imkoniyati ta’minlangan.

- Shaxsiy ma’lumotlar so‘rovlariga javob berishning ichki muddatlari va shablonlari belgilangan.

G. Uchinchi shaxslarga berish tartibi

- Berishga faqat asos mavjud bo‘lgandagina yo‘l qo‘yiladi (shu jumladan rozilik/shartnoma/qonun).
- Himoya va maxfiylik majburiyatlari bilan shartnoma tuzilgan.
- Subyekt, agar istisno bo‘lmasa, uchinchi shaxsga berilganligi to‘g‘risida 3 kun ichida xabardor qilinadi.
- Uchinchi shaxslar va beriladigan shaxsiy ma’lumotlar toifalari reyestri yuritiladi.

H. Tarqatish (e’lon qilish) tartibi

- E’lon qilingan maqsadlardan tashqari har qanday tarqatish faqat subyektning roziligi bilan amalga oshiriladi. ([LEX.UZ][1])
- Sayt, ijtimoiy tarmoqlar, keyslar, foto/video, sharhlar uchun alohida qoidalar.
- Ma’lumotlarning «ommaviyligi» va kirish asoslarini tekshirish.

I. Transchegaraviy uzatish tartibi

- Mamlakat aniqlanadi va «yetarlicha himoya» baholanadi (qonunchilikning mavjudligi, maxfiylik to‘g‘risidagi shartnoma, ichki siyosat, texnik himoya choralari)
- «Noadekvat» mamlakatlar uchun asos (masalan, rozilik) qayd etiladi.
- Transchegaraviy o‘tkazmalar reyestri yuritiladi (tizim, provayder, sana, asos).
- Transchegaraviy o‘tkazish to‘g‘risida regulyatorni xabardor qilish tartibi

J. Mahalliylashtirish va ro‘yxatdan o‘tkazish (O‘zR fuqarolari ma’lumotlari uchun)

- O‘zbekiston Respublikasida texnik vositalarda yig‘ish/tizimlash/saqlash ta’minlangan.
- Ma’lumotlar bazasi davlat reyestrida ro‘yxatga olingan.
- Bulutli xizmatlar, zaxiralash va tashqi xizmatlarni boshqarish.

K. Saqlash, o‘chirish va yo‘q qilish tartibi

- Qayta ishlash maqsadlariga ko‘ra saqlash muddatlari belgilangan.
- Yo‘q qilish asoslari: maqsadga erishilgan, rozilik qaytarib olingan, qayta ishlash muddati tugagan, sud qarori.
- Yo‘q qilish dalolatnoma bilan rasmiylashtiriladi.
- Nusxalar va zaxiralarning reglament bo‘yicha o‘chirilishi tekshiriladi.

L. Insidentlarga (ma’lumotlarning sizib chiqishi/buzilishlarga) javob qaytarish tartibi

- Hodisalar toifalari va javob berish guruhi aniqlandi.
- Qayta ishlash shartlari buzilganligi to‘g‘risida ma’lumot mavjud bo‘lgan taqdirda, qayta ishlashni to‘xtatib turish yoki yo‘q qilish nazarda tutilgan.
- Ta’minlangan: lokalizatsiya, hodisalarni tekshirish, sabablarini bartaraf etish, hujjatlashtirish.
- Bildirishnoma shablonlari va aloqa protokoli kiritildi.

https://lex.uz/docs/4396428 «Shaxsga doir ma’lumotlar to‘g‘risida»gi O‘RQ-547-sonli Qonuni, 02.07.2019

3-ilova

Shaxsiy ma’lumotlarga ishlov berish va ularni himoya qilish siyosatining tuzilmasi

1. Umumiy qoidalar
    1.1. Siyosatning maqsadi.
    1.2. Qo‘llanish sohasi (xodimlar, nomzodlar, mijozlar, kontragentlar, kontragentlar vakillari).
    1.3. Atamalar va ta’riflar (subyekt, operator/mulkdor, uchinchi shaxs, Shaxsiy ma’lumotlar bazasi, tarqatish, transchegaraviy uzatish).
    1.4. Ishlov berish tamoyillari.
2. Rollar va mas’uliyat
    2.1. Mulkdor va (yoki) operator.
    2.2. Shaxsiy ma’lumotlar bo‘yicha mas’ul bo‘linma/mansabdor shaxs (vazifasi va funksiyalari).
    2.3. Foydalanuvchilar va jarayonlar egalarining vakolatlari.
3. Qayta ishlashning huquqiy asoslari va maqsadlari
    3.1. Qayta ishlash shartlari (asoslari) (rozilik, shartnoma, qonun, qonuniy manfaatlar, ijtimoiy ahamiyatga ega maqsadlar, egasizlantirilganda o‘tkaziladigan tadqiqotlar, hamma foydalanishi mumkin bo‘lgan manbalar).
    3.2. Ichki hujjatlarda ishlov berish maqsadlarini belgilash va ularning yig‘ishda ilgari e’lon qilingan maqsadlarga muvofiqligi.
4. Ma’lumotlar toifalari va subyektlar
    4.1. Subyektlarning toifalari.
    4.2. Ma’lumotlar toifalari (oddiy, maxsus; mavjud bo‘lsa — biometrik/genetik).
    4.3. Ma’lumotlar tarkibini minimallashtirish (zarurligi va yetarliligi).
5. Ishlov berishning hayotiy davri
    5.1. Yig‘ish, tizimlashtirish, saqlash.
    5.2. Foydalanish.
    5.3. Kompaniya ichida taqdim etish va foydalanish.
    5.4. Uchinchi shaxslarga berish.
    5.5. Tarqatish (nashr, sayt, OAV).
    5.6. Transchegaraviy uzatish.
    5.7. Egasizlantirish (agar qo‘llanilsa).
    5.8. Yo‘q qilish (olib tashlash).
6. Rozilik va roziliklarni boshqarish
    6.1. Rozilik shakli va uning olinganligini isbotlash.
    6.2. Maxsus ma’lumotlarga uchun rozilik (yozma shaklda, shu jumladan elektron hujjat shaklida).
    6.3. Rozilikni qaytarib olish va uni qayd etish.

7. Subyektlarning huquqlari va ularni amalga oshirish tartibi
   7.1. Qayta ishlash haqida ma’lumot olish huquqi va taqdim etiladigan ma’lumot tarkibi.
   7.2. Ma’lumotlarning sifati/qonuniyligi/zaruriyati bilan bog‘liq muammolar yuzaga kelganda, ularni qayta ishlashni vaqtincha to‘xtatib turishni talab qilish huquqi.
   7.3. So‘rovlarni yuborish kanallari va ichki ko‘rib chiqish muddatlari (ichki SLA).
   7.4. Ariza beruvchini identifikasiya qilish.

8. Subyektlarni xabardor qilish
   8.1. Ma’lumotlarni bazaga kiritishda xabardor qilish (maqsadlar va huquqlar).
   8.2. Ma’lumotlarni uchinchi shaxsga uzatishda xabardor qilish (3 kun, istisnolar).

9. Maxfiylik va ochiq ma’lumotlar
   9.1. Maxfiylik rejimi.
   9.2. Hamma foydalanishi mumkin bo‘lgan shaxsiy ma’lumotlar va ular bilan ishlash qoidalari.

10. Bazalarni mahalliylashtirish va ro‘yxatdan o‘tkazish
   10.1. O‘zbekiston Respublikasi fuqarolari ma’lumotlarini AT/Internetdan foydalangan holda qayta ishlash shartlari (mahalliylashtirish + davlat reyestrida ro‘yxatdan o‘tkazish).
   10.2. Bazalarni ro‘yxatga olish va ro‘yxatga olish uchun ma’lumotlar o‘zgarganligi to‘g‘risida xabardor qilish.

11. Himoya choralari
   11.1. Huquqiy, tashkiliy va texnik choralar.
   11.2. Foydalanishni boshqarish, hisob qaydnomalari, jurnallar, tashuvchilar, xonalar.
   11.3. Pudratchilar va uchinchi shaxslar nazorati.

12. Amaliy ma’noda o‘chirish, yo‘q qilish va «unutilish huquqi»
   12.1. Yo‘q qilish/o‘chirish asoslari asoslari (maqsadga erishilganligi, rozilikni qaytarib olish, muddatning tugashi, sud qarori).
   12.2. Cheklash/to‘xtatish talablarini qayta ishlash.
   12.3. Yo‘q qilishni hujjatlashtirish (dalolatnomalar, loglar).

13. Hodisalar va sizib chiqishlarga munosabat bildirish
   13.1. Ma’lumotlarni qayta ishlash shartlari buzilganligi haqida ma’lumot mavjud bo‘lganda, ularni qayta ishlashni to‘xtatish yoki yo‘q qilish majburiyati.
   13.2. Tekshirish, lokalizatsiya, tuzatish va hisobot berish tartibi.

14. Transchegaraviy uzatish
   14.1. «Muvofiq himoya» mezonlari.
   14.2. «Nomuvofiq» mamlakatlarga o‘tkazish va ruxsat etilgan asoslar (shu jumladan rozilik).
   14.3. Transchegaraviy uzatishlar reyestri va oqimlar nazorati.

15. Yakuniy qoidalar
   15.1. Xodimlarni o‘qitish va javobgarlik.
   15.2. Siyosatni audit qilish va qayta ko‘rib chiqish.
   15.3. Mas’ul shaxs kontaktlari.

Yevropa Ittifoqi tomonidan moliyalashtiriladi

ZAMONAVIY JURNALISTIKANI RIVOJLANTIRISH MARKAZI

LPRC LEGAL POLICY RESEARCH CENTRE

UDRMI O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI