

DOI: <https://doi.org/10.5281/zenodo.11245208>

AXBOROTNI KIRISH DARAJALARIGA BO'LIH TAMOYILLARI

Ramazonova Madina Shavkatovna

Ilmiy rahbar

Tojmuratov Shuxratbek Dilmurodjon o'g'li

Mirzayev Bekzod Toxirboy o'g'li

Babajanov Jaloliddin Umidjon o'g'li

Toshkent axborot texnologiyalar universiteti talabalari

abdujabbor.madina.1989@gmail.com

***Annotatsiya:** Biznes ma'lumotlarining xavfsizligi zamonaviy tijorat korxonalarini uchun muhim muammolardan biridir. Kompaniyalar raqobatbardosh razvedka bo'linmalarini tashkil etish orqali raqobatchilarning maxfiy ma'lumotlarini olishga harakat qilishadi. Shu sababli, korxonalar o'z ma'lumotlarining xavfsizligini ta'minlash uchun tashkiliy va texnik choralar ishlab chiqishmoqda. Tadqiqotlar shuni ko'rsatadiki, kompaniyalar o'z axborot xavfsizligi siyosatiga ega bo'lish uchun IT bo'limlariga tayanadi. Ma'lumotlarni muhimligiga qarab tasniflash va himoya choralarini belgilash orqali xavfsizlikni ta'minlash kerak. Ushbu maqolada Yevropa va O'zbekiston standartlariga muvofiq ma'lumotlarning tasnifi va himoya qilish tamoyillari haqida ma'lumot beriladi*

***Kalit so'zlar:** Biznes ma'lumotlari xavfsizligi, Axborot xavfsizligi siyosati, Yevropa standartlari, Tijorat siri, Maxfiylik darajasi, Ma'lumotlarni tasniflash, Raqobatbardosh razvedka*

Hozirgi vaqtda biznes ma'lumotlarini himoya qilish muammosi tobora ko'proq paydo bo'lmoqda. Bozorda munosib o'rin egallashni istagan kompaniya qattiq, ham ichki, ham tashqi raqobat sharoitida ishlashga majbur.

Ko'pgina kompaniyalarda raqobatbardosh razvedka bo'linmalari (va ba'zi hollarda, hatto iqtisodiy yoki sanoat josusligi) tashkil etilgan bo'lib, ularning maqsadi raqobatdosh korxonalarining maxfiy ma'lumotlarini olishdir.

Zamonaviy tijorat korxonalarida ma'lumotlarining xavfsizligini ta'minlash uchun tashkiliy va texnik choralar allaqachon ishlab chiqilgan bo'lib, ular tashkilotning himoya vositalari bilan jihozlanganligiga va uning rahbariyati va xodimlari tomonidan muammoni tushunish darajasiga qarab amalga oshiriladi. Masalan, LogicaCMG

mutaxassislari tomonidan 350 ta kompaniya vakillari o'rtasida o'tkazilgan so'rov natijalariga ko'ra, firmalarning yarmida axborot xavfsizligini ta'minlash bo'yicha aniq belgilangan strategiya mavjud emas. *So'rovda qatnashgan kompaniyalarning 71 foizi kompaniyaning axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishda o'z IT bo'limlariga tayanadi.*

Shu bilan birga, birinchilardan bo'lib korxonada va undan tashqarida aylanib yuradigan ma'lumotlarni qanday ajratish va ushbu ma'lumot hajmidan eng muhim va natijada maxsus himoya choralarini talab qiladigan ma'lumotni qanday ajratish kerakligi haqida savol tug'iladi. Natijada, ma'lumotni kirish darajalariga bo'lish zarurati paydo bo'ladi.

Ko'pincha, bu jarayon xaotik, tizimsiz va irratsionaldir, bu jarayonning ahamiyatini yetarli darajada tushunmaslik va ushbu masalalar bilan shug'ullanadigan shaxslarning malakasizligi tufayli yuzaga keladi. Ushbu jarayonga harakatlarning yagona algoritmini va aniq, izchil tizimni ishlab chiqish uchun ma'lumotni uning mazmuni, qiymati va ahamiyatiga qarab tegishli darajalarga bo'lish kerak.

Yevropa standartlariga (masalan, ISO 17799) muvofiq quyidagi tasnifdan foydalanish tavsiya qilinadi:

- ochiq axborot;
- konfidensial axborot;
- maxfiy axborot.

Biroq, amaliyotda kirish darajalarining biroz boshqacha tasnifi ishlab chiqilgan bo'lib, u quyidagicha taqdim etiladi:

- ochiq axborot (OA);
- xizmatda (rasmiy) foydalanish uchun (XFU) axborot;
- tijorat siri.

Shuni ta'kidlash kerakki, ba'zi manbalarda tijorat sirlariga nisbatan "maxfiy ma'lumotlar" atamasi qo'llaniladi, bu "davlat siri to'g'risidagi qonun" ning 3-moddasi 11-bandiga binoan davlat siriga kiritilmagan ma'lumotlarga nisbatan yo'l qo'yilmaydi. Shuni ta'kidlash kerakki, ma'lumotni har qanday kirish darajasiga kiritish va bunday ma'lumotlarning ro'yxati va tarkibini aniqlash huquqi uning egasiga tegishli.

Axborotni kirish darajalariga bo'lish tamoyillari (Tamoyil fundamental normalar yoki xulq-atvor qoidalarini bildiradi.) Axborotni himoya qilishning barcha faoliyati ma'lum tamoyillarga asoslanadi, ular axborotni himoya qilish jarayonida ishtirok etuvchilarni qat'iy boshqaradi. Korxonada axborotni taqsimlashning asosiy tamoyillari quyidagilardan iborat:

1. **Qonuniylik** - axborot almashish amaldagi qonunchilik va qonun hujjatlarida belgilangan tartiblarga muvofiq amalga oshiriladi. Axborotni kirish darajalariga ajratuvchi sub'yekt ma'lum bir yuridik shaxs doirasida ushbu jarayonni tartibga

soluvchi mahalliy ichki normativ hujjatni qabul qiladi. Qonunga ko'ra, ayrim ma'lumotlarni tasniflashni taqiqlovchi ba'zi cheklovlar mavjud.

2. **Mutaxassislik** - axborotni kirish darajalariga bo'lish axborot xavfsizligi sohasida zarur ko'nikma va bilimlarga ega bo'lgan malakali mutaxassislarni jalb qilgan holda amalga oshiriladi. Qoida tariqasida, ushbu mutaxassislar tashkiliy jihatdan korxonada xavfsizlik xizmati, xavfsizlik va axborotni muhofaza qilish bo'limlari yoki boshqa bo'limlarning bir qismidir. Shuningdek, zarur hollarda jarayonga zarur bilimga ega bo'lgan boshqa shaxslar ham jalb etilishi mumkin.

3. **Majmuaviylik (komplekslik)** - axborotni ajratish jarayoni barcha mavjud kuch va vositalardan foydalangan holda yagona kompleksda amalga oshiriladi va korxonaning barcha bo'linmalariga taalluqlidir.

4. **Uzluksizlik** - bu jarayon bir martalik hodisa sifatida amalga oshirilmaydi, balki doimiy ravishda amalga oshiriladi, chunki korxonada axborot aylanishi to'xtatilmaydi va u yoki bu ma'lumotni vaqt va mavjud sharoitga qarab doimiy ravishda qayta baholash mavjud.

5. **Markazlashtirish** - axborotni kirish darajalariga bo'lish jarayonini tashkil etish va boshqarish korxonaning barcha bo'linmalari bo'ysunadigan tegishli vakolatlarga ega bo'lgan yagona markazdan amalga oshiriladi.

Ochiq axborot axborotdan foydalanishning ochiqligi bo'yicha birinchi darajasidir. Uning asosiy maqsadi korxonada faoliyati to'g'risida xabardor qilish uchun uni uchinchi shaxslarga berishdir. Foydalanish ma'lum bir shaxslar doirasi bilan cheklangan ichki (xizmatda) foydalanish ma'lumotlari va tijorat sirlaridan farqli o'laroq, ochiq ma'lumotlarga kirish cheklanmaydi va hatto, aksincha, asosiy maqsad ushbu ma'lumotni maksimal darajada katta doiradagi shaxslarga tanitish bo'lishi mumkin.

Ochiq axborot quyidagilarni o'z ichiga oladi:

- amaldagi qonun hujjatlariga muvofiq foydalanishni cheklash mumkin bo'lmagan ma'lumotlar;
- jamoatchilik bilan aloqalar (PR) xizmatlari tomonidan yaratilgan, tashqariga uzatish uchun mo'ljallangan ma'lumotlar;
- reklama va axborot xabarlari;
- tashqi, ochiq manbalardan olingan ma'lumotlar;
- veb-saytda ochiq bo'lgan ma'lumotlar.

Ommaviy axborotni himoya qilishning hojati yo'qligiga qat'iy ishonch bor. Biroq, bu nuqtai nazar shubhali va bahsli. Ommaviy axborot ham muayyan xavfsizlik choralariga bo'ysunishi kerak. Xususan, noto'g'ri yoki nолоyiq xatti-harakatlar natijasida rasmiy foydalanish uchun ma'lumotlar yoki konfidensial axborotlar bilan

ruxsat etilmagan shaxslarning tanish bo‘lishiga yo‘l qo‘ymaslik uchun qanday ma‘lumotlar jamoat mulkiga o‘tkazilishini diqqat bilan nazorat qilish kerak .

Xususan, noto‘g‘ri yoki malakasiz harakatlar natijasida begonalarining xizmatda foydalanadigan ma‘lumoti yoki konfideksial ma‘lumotlarni ochiq qilib e‘lon qilinishini istisno qilish uchun qanday ma‘lumotni ochiq foydalanish huquqiga o‘tkazish kerakligini diqqat bilan kuzatib borish kerak.

Bundan tashqari, ochiq ma‘lumotlarga nisbatan ham moddiy zarar, ham korxonaning ishchanlik obro‘sigga putur yetkazishi mumkin bo‘holatlar yuzaga kelishini oldini olish uchun zarur himoya choralari ko‘riladi.

Xizmatda foydalanish uchun axborot (xizmatda foydalanish uchun - bundan keyin XFU (yoki ichki foydalanish uchun – IFU) deb yuritiladi) foydalanishning ikkinchi darajasi bo‘lib, unga nisbatan ochiq ma‘lumotlardan farqli o‘laroq, muayyan cheklovchi choralar qo‘llaniladi. Ta‘rifning o‘zidan ko‘rinib turibdiki, ushbu axborotlar ma‘lum ma‘lumotlar va ma‘lumotlar to‘plamini o‘z ichiga oladi, ularning aylanishi faqat korxonaning ushbu ma‘lumotlar bilan biznes ehtiyojlari bo‘yicha o‘zaro aloqada bo‘lgan bir qator xodimlari o‘rtasida amalga oshiriladi. Qoida tariqasida, XFU uchun quyidagi talablar qo‘llaniladi:

- ushbu ma‘lumotlar xizmatlar, bo‘limlar va bo‘limlar o‘rtasidagi ichki muomalaga kiritiladi va ularning normal ishlashi uchun zarurdir;
- ochiq manbalardan olingan ma‘lumotlar bilan ishlashning yakuniy natijasi (analitik eslatma, tijorat xulosasi, prognoz gipotezasi);
- davlat siri bo‘lgan ma‘lumotlarga taalluqli emas;
- tijorat siri bo‘lgan ma‘lumotlarga taalluqli emas;
- ochiq axborotga taalluqli emas;
- unga kirish muayyan tartib-qoidalar va xavfsizlik choralariga bog‘liq.

Ya‘ni, XFU kompaniya tarmog‘ida aylanayotgan barcha ichki ma‘lumotlarni o‘z ichiga olishi mumkin, ularning yo‘qolishi uning faoliyati uchun jiddiy salbiy oqibatlarga olib kelmaydi, biroq ayrim hollarda jiddiy moddiy zarar yoki kompaniyaning ishbilarmonlik obro‘sigga putur yetkazishi mumkin.

Tijorat siri — axborotga kirishning uchinchi, eng yuqori darajasi, ya‘ni O‘zbekiston Respublikasi qonunchiligiga muvofiq foydalanishi cheklangan hujjatlashtirilgan ma‘lumotlar.

Tijorat siri deganda xo‘jalik yurituvchi sub‘ektning ishlab chiqarish, texnologiyasi, boshqaruvi, moliyaviy va boshqa faoliyati bilan bog‘liq bo‘lmagan, oshkor etilishi (uzatilishi, oqishi) uning manfaatlariga zarar yetkazishi mumkin bo‘lgan davlat siri bo‘lmagan ma‘lumotlar tushuniladi.

Tijorat sirini tashkil etuvchi ma'lumotlar xo'jalik yurituvchi sub'yektning mulki hisoblanadi yoki qonun hujjatlariga muvofiq o'zi belgilagan doirada uning egaligida, foydalanishida yoki tasarrufida bo'ladi.

Tijorat sirini tashkil etuvchi ma'lumotlar quyidagi talablarga javob berishi kerak:

a) tadbirkorlik sub'yekti uchun haqiqiy yoki potentsial qiymatga ega bo'lishi;
b) qonun bo'yicha hammaga ma'lum yoki ommaga ochiq bo'lmasligi;
c) tadbirkorlik subyektlari tomonidan ushbu ma'lumotlarni tasniflash tizimi orqali ularning maxfiyligini saqlash bo'yicha tegishli choralar ko'rilishi, ularni maxfiylashtirishning ichki qoidalari ishlab chiqilishi, hujjatlar va boshqa axborot tashuvchilarning tegishli markirovkasi joriy etilishi, maxfiy ish yuritishni tashkil etilishi zarur;

d) davlat sirini tashkil etmasligi va mualliflik va patent huquqlari bilan himoyalanganligi;

e) davlat manfaatlariga zarar yetkazishi mumkin bo'lgan salbiy faoliyati to'g'risidagi ma'lumotlarni o'z ichiga olmasligi.

"Tijorat siri to'g'risida"gi Qonunning 5-moddasi 4-qismiga muvofiq, tijorat siri ob'yektlari quyidagilardan iborat bo'lishi mumkin emas:

– davlat ro'yxatidan o'tkazilishi lozim bo'lgan mol-mulkka doir huquqlar va bu huquqlar bo'yicha bitimlar to'g'risidagi;

– yuridik shaxsning ta'sis hujjatlaridagi, yuridik shaxslar, yakka tartibdagi tadbirkorlar va yuridik shaxs tashkil etmagan dehqon xo'jaliklari haqidagi yozuvlar tegishli davlat reyestrlariga kiritilganligi faktini tasdiqlaydigan hujjatlardagi;

– tadbirkorlik faoliyatini amalga oshirish huquqini beruvchi hujjatlardagi;

– davlat unitar korxonasi, davlat muassasasi, davlat muassasasi tarkibi to'g'risidagi va ular tomonidan tegishli budjet mablag'laridan foydalanilishi haqidagi;

– atrof muhitning ifloslanishi, yong'in xavfsizligining holati, sanitariya-epidemiologik va radiatsiyaviy vaziyat, oziq-ovqat mahsulotlari xavfsizligi hamda ishlab chiqarish obyektlarining xavfsiz faoliyat ko'rsatishini, har bir fuqaroning va butun aholining xavfsizligini ta'minlashga salbiy ta'sir ko'rsatuvchi boshqa omillar haqidagi;

– xodimlarning soni va tarkibi, mehnatga haq to'lash tizimi va mehnat sharoitlari to'g'risidagi, shu jumladan mehnatni muhofaza qilish, ishlab chiqarishdagi jarohatlanishlar va kasb kasalliklari ko'rsatkichlari, shuningdek bo'sh ish o'rinlari bor-yo'qligi haqidagi;

– ish beruvchilarning ish haqi to'lash va ijtimoiy to'lovlar bo'yicha qarzdorligi to'g'risidagi; qonunchilik buzilishlari va bunday buzilishlarni sodir etganlik uchun javobgarlikka tortish faktlari to'g'risidagi;

– davlat mulki obyektlarini xususiylashtirish bo'yicha tanlovlarning yoki kimoshdi savdolarining shartlari haqidagi;

– notijorat tashkilotlar daromadlarining miqdorlari va tuzilishi, ushbu tashkilotlarning mol-mulki miqdorlari va tarkibi haqidagi, ularning xarajatlari, bu tashkilotlar xodimlarining (a'zolarining) soni va mehnatiga haq to'lash, notijorat tashkilotning faoliyatida fuqarolarning tekin mehnatidan foydalanilishi to'g'risidagi;

– yuridik shaxs nomidan ishonchnomasiz ish yuritish huquqiga ega bo'lgan shaxslarning ro'yxati haqidagi;

– davlat statistika hisoboti sifatida taqdim etilishi lozim bo'lgan ma'lumotlar.

Maxfiylik darajasi bo'yicha tasniflash

Axborotning maxfiyligi darajasi muayyan institutsional xavfsizlik siyosatini yaratishda e'tiborga olinadigan eng muhim toifalardan biridir. Axborotni maxfiylik darajasiga ko'ra 4 toifaga bo'lish uchun quyidagi sxema taklif etiladi.

sinf	Axborot turi	Tavsif	Misollar
0	ochiq ma'lumot	ommaviy axborot	axborot risolalari, ommaviy axborot vositalarida chop etilgan ma'lumotlar
1	ichki ma'lumotlar (XFU)	ochiq shaklda mavjud bo'lmagan, ammo oshkor qilingan taqdirda hech qanday xavf tug'dirmaydigan ma'lumotlar	moliyaviy hisobotlar va avvalgi faoliyat ma'lumotlari, muntazam yig'ilishlar va uchrashuvlar hisobotlari, firmaning ichki telefon ma'lumotnomasi
2	konfidensial axborotlar (shu jumladan tijorat siri)	ma'lumotlarning oshkor etilishi bozorda katta yo'qotishlarga olib keladi	haqiqiy moliyaviy ma'lumotlar, rejalar, loyihalar, mijozlar to'g'risidagi ma'lumotlarning to'liq to'plami, axloqiy me'yorlarni buzgan sobiq va joriy loyihalar to'g'risidagi ma'lumotlar
3	maxfiy ma'lumotlar	ma'lumotlarning oshkor etilishi kompaniyaning moliyaviy halokatiga olib keladi	(vaziyatga bog'liq)

Maxfiylik darajasi 1-sinfga kiritiladigan axborotlar bilan ishlashda quyidagi talablarga rioya qilish tavsiya etiladi:

- xodimlarni ushbu ma'lumotlarning maxfiyligi to'g'risida xabardor qilish;
- xodimlarni ma'lumotlarga hujum qilishning asosiy mumkin bo'lgan usullari bilan umumiy tanishtirish;
- jismoniy kirishni cheklash;
- ushbu ma'lumotlar bilan operatsiyalarni bajarish qoidalari bo'yicha to'liq hujjatlar to'plami.

2-sinfga oid axborot bilan ishlashda yuqoridagi talablarga quyidagi talablar qo'shiladi:

- axborotga hujum qilish xavfini hisoblash;
- ushbu ma'lumotlarga kirish huquqiga ega bo'lgan shaxslar ro'yxatini yuritish;
- iloji bo'lsa, bunday ma'lumotni tilhat orqali berish (shu jumladan elektron shakldagilarini ham)
- tizimning yaxlitligini va uning xavfsizlik xususiyatlarini tekshirish uchun avtomatik tizim mavjudligi;
- jismoniy transportirovkaning ishonchli bo'lishi;
- aloqa liniyalari orqali uzatishda majburiy shifrlash;
- kompyuterning uzluksiz quvvat manbai bo'lishi.

Maxfiylik darajasi 3-sinfga oid axborotlar bilan ishlashda yuqoridagi barcha talablarga quyidagi talablar qo'shiladi:

- favqulodda vaziyatlarda (yong'in, suv toshqini, portlash) qutqarish yoki ma'lumotlarni ishonchli yo'q qilishning batafsil rejasi mavjudligi;
- kompyuterlarni yoki saqlash vositalarini suv va yuqori harorat ta'siridan himoya qilish;

XULOSA

Biznes ma'lumotlarini himoya qilish zamonaviy tijorat korxonalarini uchun muhim ahamiyatga ega. Kompaniyalar raqobat sharoitida o'z ma'lumotlarini himoya qilish uchun turli tashkiliy va texnik choralarni ko'rishlari kerak. Tadqiqotlar shuni ko'rsatadiki, ko'plab kompaniyalarda axborot xavfsizligini ta'minlash uchun aniq strategiya mavjud emas va aksariyat hollarda bu mas'uliyat IT bo'limlariga yuklatiladi. Ma'lumotlarni kirish darajalariga bo'lish va ularni himoya qilish uchun aniq tamoyillar asosida ish olib borish zarur. Yevropa standartlari va O'zbekiston qonunchiligiga ko'ra, ma'lumotlar ochiq, konfidensial va tijorat siri kabi kategoriyalarga bo'linadi. Har bir kategoriya uchun tegishli himoya choralari belgilanishi lozim. Ma'lumotlarni to'g'ri tasniflash va himoya qilish orqali kompaniyalar raqobatbardoshligini saqlab qolishi va muhim ma'lumotlarning xavfsizligini ta'minlashi mumkin.

ADABIYOTLAR

1. O‘zbekiston Respublikasi Konstitutsiyasi.
2. O‘zbekiston Respublikasi Fuqarolik kodeksi. 01.03.1997. Qayta taxrirlangan versiyasi (21.04.2022y).
3. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. 16.04.2019 y.
4. O‘zbekiston Respublikasining «Axborot olish kafolatlari va erkinligi to‘g‘risida» Qonuni. 24.04.1997 y.
5. Yevropa Kengashining 1981 yil 28 yanvardagi “Shaxsiy ma’lumotlarni avtomatik qayta ishlash bo‘yicha jismoniy shaxslarni himoya qilish to‘g‘risida”gi konventsiyasi. Elektron resurs: lexdigital.ru/2012/052/ (Murojaat sanasi: 12.11.2015).
6. Yevropa Parlamenti va Kengashning 1996 yil 11 martdagi “Ma’lumotlar bazalarini huquqiy himoya qilish to‘g‘risida”gi 96/6/EC direktivasi. Elektron resurs
7. Yevropa Parlamentining 2001 yil 22 maydagi “Axborot jamiyatida mualliflik huquqi va turdosh huquqlarning ayrim jihatlarini uyg‘unlashtirish to‘g‘risida”gi 2001/29/EC direktivasi. Elektron resurs: http://www.wipo.int/wipolex/ru/text.jsp?file_id=126976 (Murojaat sanasi: 09.12.2015).
8. 2000 yil 8 iyundagi 2000/31/EC-sonli “Ichki bozorda axborot xizmatlarining ayrim huquqiy jihatlarini to‘g‘risida”gi Yevropa Ittifoqi Direktivasi №2000/31/EC. Elektron resurs: http://www.wipo.int/wipolex/ru/text.jsp?file_id=181678 (Murojaat sanasi: 15.10.2015).
9. 1996 yil 20 dekabrda “BIMTning Mualliflik huquqi to‘g‘risida”gi Shartnomasi. - Jeneva: BIMT. – 2000. - № 226(R).
10. A.Sokolov, O.Stepanyuk. Защита от компьютерного терроризма. О‘quv qo‘llanma. BXV-Peterburg. Arlit, 2002.