

KORPORATIV MUHITDA AXBOROT XAVFSIZLIGI SIYOSATINING NAZARIY ASOSLARI VA AMALIY AHAMIYATI

Temurbek Bahromov

Urganch davlat universiteti Axborot xavfsizligi mutaxassisligi bo'yicha magistrant.

temurbekbaxramov150@gmail.com

<https://doi.org/10.5281/zenodo.18340762>

Annotatsiya. Mazkur tezisdan korporativ muhitda axborot xavfsizligi siyosatining nazariy asoslari va uning amaliy ahamiyati tahlil qilinadi. Axborot xavfsizligining asosiy tamoyillari — maxfiylik, yaxlitlik va mavjudlik (CIA triadasi) yoritilib, ularning korporativ boshqaruv tizimidagi o'rni ochib beriladi. Xalqaro standartlar, xususan ISO/IEC 27001 va ISO/IEC 27002 talablari asosida axborot xavfsizligi siyosatini shakllantirish, joriy etish va boshqarish masalalari ko'rib chiqiladi. Shuningdek, inson omilining axborot xavfsizligiga ta'siri hamda O'zbekiston Respublikasida axborot xavfsizligini ta'minlash bo'yicha yaratilgan me'yoriy-huquqiy baza tahlil qilinadi. Tadqiqot natijalari axborot xavfsizligi siyosatini korporativ strategiya ajralmas qismi sifatida shakllantirish zarurligini ko'rsatadi.

Kalit so'zlar: axborot xavfsizligi, korporativ xavfsizlik, xavfsizlik siyosati, ISO/IEC 27001, risklarni boshqarish, inson omili.

Annotation. This paper analyzes the theoretical foundations and practical significance of information security policy in a corporate environment. The core principles of information security — confidentiality, integrity, and availability (CIA triad) — are examined, along with their role in corporate governance systems. Based on international standards such as ISO/IEC 27001 and ISO/IEC 27002, the study explores the development, implementation, and management of information security policies. Special attention is given to the impact of the human factor on information security and the regulatory framework established in the Republic of Uzbekistan. The results emphasize that information security policy should be considered an integral part of corporate strategy.

Keywords: information security, corporate security, security policy, ISO/IEC 27001, risk management, human factor.

1. Axborot xavfsizligi tushunchasi va uning korporativ boshqaruvdagi o'rni

Zamonaviy raqamli iqtisodiyot sharoitida axborot tashkilotlar faoliyatining eng muhim strategik resurslaridan biriga aylandi. Moliyaviy operatsiyalar, boshqaruv qarorlari va mijozlar ma'lumotlarining raqamli shaklda yuritilishi axborot tizimlarining ishonchliligiga bo'lgan talabni oshirmoqda. Shu sababli axborot xavfsizligi masalasi korporativ boshqaruvning muhim yo'nalishlaridan biri sifatida qaraladi.

Axborot xavfsizligi axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga qaratilgan kompleks chora-tadbirlar majmuasidir. Ushbu uchlik xalqaro amaliyotda CIA triadasi deb ataladi va axborot xavfsizligi siyosatining konseptual asosini tashkil etadi [4]. Axborot xavfsizligining asosiy tamoyillari o'rtasidagi o'zaro bog'liqlik 1-rasmda aks ettirilgan.



1-rasm. Axborot xavfsizligi tamoyillari.

Korporativ muhitda ushbu tamoyillarning buzilishi moliyaviy zarar, huquqiy javobgarlik va obro‘-e’tibor yo‘qotilishiga olib kelishi mumkin.

2. Axborot xavfsizligi siyosati va xalqaro standartlar

Axborot xavfsizligi siyosati tashkilotda axborot resurslarini himoya qilish bo‘yicha yagona qoidalar va tamoyillarni belgilovchi asosiy hujjat hisoblanadi. ISO/IEC 27001:2022 standarti axborot xavfsizligi menejment tizimini (ISMS) tashkilotning umumiy boshqaruv tizimiga integratsiya qilishni nazarda tutadi [4]. Ushbu standart riskga asoslangan yondashuvni qo‘llab, xavfsizlik choralari rejallashtirish, joriy etish, monitoring qilish va doimiy takomillashtirishni talab etadi.

ISO/IEC 27002:2022 esa axborot xavfsizligini ta’minlash bo‘yicha amaliy nazorat choralari belgilab beradi. Mazkur standart siyosatni real jarayonlarga tatbiq etishda tashkiliy, texnik va inson omiliga oid choralarni tizimli tarzda joriy etishga yordam beradi [5]. Shu sababli ushbu ikki standart birgalikda qo‘llanilishi korporativ xavfsizlikni mustahkamlashda muhim ahamiyat kasb etadi. Axborot xavfsizligi siyosatining asosiy tarkibiy elementlari 1-jadvalda keltirilgan.

1-jadval. Axborot xavfsizligi siyosatining asosiy tarkibiy elementlari

No	Element	Tavsifi
1	Xavfsizlik siyosati	Axborot resurslarini himoyalash bo‘yicha umumiy qoidalar
2	Risklarni boshqarish	Tahdidlarni aniqlash va kamaytirish jarayoni
3	Kirishni nazorat qilish	Foydalanuvchi huquqlarini belgilash
4	Texnik himoya choralari	Shifrlash, autentifikatsiya, zaxiralash
5	Inson omili	Xodimlarni o‘qitish va xavfsizlik madaniyati
6	Audit va monitoring	Nazorat va doimiy baholash

3. Inson omili va tashkiliy chora-tadbirlarning ahamiyati

Tadqiqotlar shuni ko‘rsatadiki, axborot xavfsizligi hodisalarining katta qismi inson omili bilan bog‘liq. Xodimlarning e’tiborsizligi, yetarli bilimga ega emasligi yoki ataylab qilgan harakatlari xavfsizlik tizimining zaiflashishiga olib keladi [6]. Shu bois zamonaviy axborot xavfsizligi siyosati faqat texnik vositalarga emas, balki xodimlarning xabardorligi va xavfsizlik madaniyatiga ham tayanishi lozim.

ISO/IEC 27001 va 27002 standartlari doirasida xodimlarni muntazam o‘qitish, ichki nazorat mexanizmlarini joriy etish va audit jarayonlarini kuchaytirish inson omilidan kelib chiqadigan xavflarni kamaytirishga xizmat qiladi [5]. Bunday yondashuv axborot xavfsizligini tashkilot madaniyatining ajralmas qismiga aylantiradi.

4. O‘zbekiston amaliyoti va me‘yoriy-huquqiy asoslar

O‘zbekiston Respublikasida axborot xavfsizligini ta’minlash bo‘yicha me’yoriy-huquqiy baza izchil rivojlanmoqda. “Axborot xavfsizligi to‘g‘risida”gi Qonun (2022-yil) va Prezidentning PQ–4562-son qarori davlat hamda xususiy sektorda axborot xavfsizligini kuchaytirishga qaratilgan [1], [3]. Shuningdek, O‘zDST 1105:2021 va 1106:2021 standartlarining joriy etilishi xalqaro tajribani milliy sharoitga moslashtirish imkonini berdi [2].

Mazkur hujjatlar asosida korxonalarda axborot xavfsizligi siyosatini shakllantirish va ISO/IEC 27001 talablariga muvofiq boshqarish amaliyoti kengayib bormoqda. Bu esa raqamli iqtisodiyot sharoitida korporativ barqarorlikni ta’minlashning muhim omili hisoblanadi.

Xulosa

Xulosa qilib aytganda, axborot xavfsizligi siyosati korporativ boshqaruvning ajralmas qismi bo‘lib, u tashkilotning strategik barqarorligi va raqobatbardoshligini ta’minlaydi. Texnik, tashkiliy va inson omiliga oid chora-tadbirlarni uyg‘unlashtirish orqali axborot xavfsizligini samarali boshqarish mumkin. Xalqaro standartlarga asoslangan va milliy qonunchilikka moslashtirilgan yondashuv O‘zbekiston korxonalari uchun ham muhim va istiqbolli yo‘nalish hisoblanadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi “Axborot xavfsizligi to‘g‘risida”gi Qonuni, 2022-yil.
2. O‘zDST 1105:2021. Axborot xavfsizligi menejmenti tizimi. Talablar.
3. O‘zbekiston Respublikasi Prezidentining PQ–4562-son qarori, 2020-yil.
4. ISO/IEC 27001:2022. Information Security Management Systems - Requirements.
5. ISO/IEC 27002:2022. Code of practice for information security controls.
6. ISO 31000:2018. Risk management — Guidelines.