**O‘zbekiston Respublikasi Raqamli texnologiyalari vazirligi**

**Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti**

**Foydalanishlarni boshqarish fanidan**

**Amaliy ishi 1**

Mavzu: Tashkilot uchun axborot xavfsizligi siyosatining foydalanishlarni

boshqarish bandini ishlab chiqish.

Bajardi:AXF 710-21 guruh

Eshboboyev Diyorbek

Tekshirdi: Bozorov Suhrobjon Mumin o‘g‘li

Toshkent-2024

**Nazariy qism**

Axborotni muhofaza qilish axborotni ixtiyoriy ko‘rinishda yo‘qotishda

ko‘riladigan zararning oldini olishni ta’minlashi lozim. Axborotni muhofaza qilish

choralari axborot xavfsizligiga oid amaldagi qonun va me’yoriy hujjatlar asosida

va axborotdan foydalanuvchilarning manfaatlariga ko‘ra tashkil etilishi zarur.

Yuqori darajada axborotni mufofaza qilishni kafolatlash uchun muntazam ravishda

murakkab ilmiy – texnik vazifalarni hal etish va himoya vositalarini

takomillashtirish talab etiladi. Axborot xavfsizligi siyosati maxfiylikni to‘plash,

yig'ish va oshirishga qaratilgan texnik vositalardan tizimli foydalanishni nazarda

tutadi

**8-variant**

Ichki Ishlar

Axborot Xavfsizligi Siyosati

1.1-jadval. Shartnoma varaqasi

|  |  |  |  |
| --- | --- | --- | --- |
| N | Lavozimi | Ism va Familiyasi | Imzo |
| 1 | Ichki ishlar vaziri | Qodirov A. |  |
| 2 | Mijozlar bilan ishlash bo‘limi boshlig'i | Tashkentova B. |  |
| 3 | Xavfsizlik bo‘limi boshlig’i | Murodov. S |  |
| 4 | Axborot xavfsizligi bo‘limi boshlig’i | Karimov D. |  |
| 5 | Yuridik bo‘lim rahbari | Sultonov E. |  |

**MUNDARIJA**

1. Umumiy tushunchalar

2. Atama va ta’riflar

3. Belgilar va qisqartmalar

4. Axborot xavfsizligini ta'minlashning dastlabki kontseptual sxemasi

5. Axborot xavfsizligining maqsad va vazifalari

6. Ichki ishlar ma'lumotlarini himoyalash

7. Axborot xavfsizligini buzuvchi tahdidlar

8. Axborot xavfsizligi tizimi

9. Axborot xavfsizligini boshqarish tizimi

10. Axborot xavfsizligi siyosatini amalga oshirish va qayta ko‘rib chiqish tartibi

11. Mas'ullar

### 1. Umumiy tushunchalar

1. Ichki ishlar axborot xavfsizligi siyosati, davlat va fuqarolarga xizmat ko'rsatish bilan bog‘liq axborotlarni himoya qilishga qaratilgan.

2. Siyosat, ichki ishlar organining maqsadlari va vazifalarini belgilab, axborot xavfsizligini ta'minlash jarayonlarini tartibga soladi. Bu, shuningdek, xizmatning ishonchliligini oshirishga yordam beradi.

3. Axborot xavfsizligi siyosati, ichki ishlar xodimlariga axborot xavfsizligi masalalarida yo'riqnoma beradi va ularning javobgarligini belgilaydi.

### 2. Atama va ta’riflar

- Ichki ishlar – davlat xavfsizligini ta'minlash va fuqarolarning huquqlarini himoya qilish bilan bog‘liq organlar.

- Axborot xavfsizligi – axborotlarni himoya qilish va muhofaza qilish holati.

- Ichki ishlar ma'lumotlari – xizmatlar, hujjatlar va fuqarolar haqida tegishli axborot.

- Tahdid – axborot xavfsizligiga zarar yetkazishi mumkin bo‘lgan har qanday holat yoki voqea.

### 3. Belgilar va qisqartmalar

- II – Ichki Ishlar

- AX – Axborot Xavfsizligi

- AT – Axborot Texnologiyalari

- IMZ – Ichki Ishlar Ma'lumotlari Zahiralar Obyektlari

- HZO – Hujjatlar Zahiralar Obyektlari

### 4. Axborot xavfsizligini ta'minlashning dastlabki kontseptual sxemasi

1. Axborot xavfsizligining kontseptual sxemasi ichki ishlar ma'lumotlarini himoya qilish, tahdidlarni kamaytirish va potentsial zararni minimallashtirishga qaratilgan.

2. Ichki ishlar xodimlarini tayyorlash va ularga xavfsizlik choralarini tushuntirish muhim ahamiyatga ega.

3. Axborot xavfsizligi siyosati doimiy ravishda yangilanadi va zamonaviy tahdidlarga moslashadi.

### 5. Axborot xavfsizligining maqsad va vazifalari

1. Maqsad – ichki ishlar organining faoliyatini to‘g‘ri va xavfsiz o'tkazish, axborotlarni himoya qilish.

2. Vazifalar:

- Fuqarolar va xodimlar haqida shaxsiy ma'lumotlarni himoya qilish.

- Ichki ishlar ma'lumotlari haqida to‘g‘ri ma'lumotlarni saqlash.

- Axborotlar oqimini boshqarish va nazorat qilish.

- Huquqbuzarliklarni aniqlash va oldini olish.

### 6. Ichki ishlar ma'lumotlarini himoyalash

- Ichki ishlar ma'lumotlari, shuningdek, fuqarolarning shaxsiy ma'lumotlari va hujjatlarga tegishli axborot himoya qilinadi.

- Xodimlarga axborot xavfsizligi bo‘yicha ta'lim va treninglar o'tkaziladi, shuningdek, xavfsizlik bo'yicha ichki nazorat tizimi yo'lga qo'yiladi.

### 7. Axborot xavfsizligini buzuvchi tahdidlar

- Ichki va tashqi tahdidlar, shuningdek, texnik nosozliklar va xodimlarning noto‘g‘ri harakatlari.

- Axborot xavfsizligini buzish ehtimoli va uning oqibatlari doimiy ravishda baholanadi.

- Fuqarolar va hamkorlar bilan axborot almashinuvi jarayonida xavfsizlik choralarini kuchaytirish.

### 8. Axborot xavfsizligi tizimi

- Axborot xavfsizligini ta'minlash uchun zarur bo‘lgan chora-tadbirlar, uslublar va mexanizmlar ishlab chiqiladi.

- Ichki ishlar xodimlari axborot xavfsizligi tizimiga rioya qilishga majbur.

- Axborot xavfsizligi monitoringi va audit jarayonlari muntazam ravishda amalga oshiriladi.

### 9. Axborot xavfsizligini boshqarish tizimi

- Boshqaruv jarayonlari, axborot xavfsizligini ta'minlash va monitoring tizimlarini o‘z ichiga oladi.

- Xodimlarga ishonchni ta'minlash, rollarni tayinlash va tarqatishda axborot xavfsizligini ta'minlash.

### 10. Axborot xavfsizligi siyosatini amalga oshirish va qayta ko‘rib chiqish tartibi

- Siyosat ichki ishlar vaziri tomonidan tasdiqlanadi va har uch yilda bir marta ko‘rib chiqiladi.

- Har qanday o‘zgarishlar va yangi talablar siyosatga kiritilishi lozim.

- Xodimlar o‘rtasida siyosatning mohiyati va ahamiyati bo‘yicha seminarlar o'tkaziladi.

### 11. Mas'ullar

- Axborot xavfsizligi sohasida mas'ul xodimlar va rahbarlar belgilangan.

- Har bir xodim axborot xavfsizligi siyosatiga rioya qilish va uning joriy etilishiga javobgardir.

- Ichki ishlar organida axborot xavfsizligini ta'minlash uchun mas'uliyatni bo‘lishish tizimi o‘rnatiladi.