

AXBOROT XAVFSIZLIGI VA U HAQIDA TUSHUNCHALAR!*Husan Sharofiddinov**Muhammad al-Xorazmiy nomidagi TATU Samarqand filiali talabasi*

Annotatsiya: Ushbu maqolada asosan, bugungi kunda jamiyat, insoniyat ijtimoiy hayotida va dunyo siyosiy maydonida global muammoga aylanib ulgurgan axborot xavfsizligi tushunchasi xususida soʻz yuritiladi. Bugungi kunda axborot xavfsizligi, axboriy-siyosiy xavfsizlik jamiyat va xalqaro siyosiy maydondagi, shu bilan birga, insoniyat hayotidagi barqarorlikni saqlashning eng asosiy faktori tarzida boʻy koʻrsatmoqda. Shuningdek, dunyo siyosiy sahnasidagi tez-tez koʻzga tashlanayotgan turli informatsion xurujlar global muammoga aylanib ulgurdi. Bu esa axborot xavfsizligi masalasi va u bilan bogʻliq muammolar hamda jarayonlarni ilmiy va amaliy tadqiq etishni taqozo etmoqda.

Kalit soʻzlar: axboriy-siyosiy xavfsizlik, axboriy-siyosiy xavfsizlik, axborot tahdidi, axborot urushi.

Kirish

Axborot texnologiyalari asrida axborotning muhimligini inobatga olsak, uni himoyalash bugungi kunda har bir tashkilotning dolzarb vazifasi hisoblanadi. Axborot xavfsizligi hodisalari tufayli keladigan zarar tashkilot taqdiriga sezilarli taʼsir koʻrsatishi mumkin. Axborot xavfsizligini taʼminlashning koʻplab usullari va sohalari mavjud. Bugungi maqolamizda tashkilotda axborot xavfsizligini taʼminlashning asosiy hujjati sanalmish axborot xavfsizligi hujjati toʻgʻrisida soʻz yuritiladi.

Asosiy qism

Axborot xavfsizligi siyosati — bu tashkilot yoki tashkilot xodimlari axborot resurslarini himoya qilish uchun kundalik amaliyotida amal qiladigan chora-tadbirlar, qoidalar va tamoyillar toʻplami. Axboriy-siyosiy xavfsizlik deganda fuqarolar, davlat va jamiyatning muhim hayotiy manfaatlarini siyosiy sohada ichki va tashqi axborot tahdidlaridan himoya qilish bilan bogʻliq kompleks muammolar tushuniladi.

Uni yanada yaqqolroq ifodalaydigan boʻlsak, ular quyidagilardir:

-birinchidan, fuqarolar, jamiyat va davlatning manfaatlarini umum qabul qilingan xavfsizliklarini taʼminlashga qaratiladi;

-ikkinchidan, axborotlarning tezlik bilan rivojlanib borishi siyosiy sohada tashqi va ichki tahdidlarga qarshi axborotlardan foydalanish imkoniyatlarini izlash va topish majburiyatini yuklaydi.

Axborot xavfsizligini quyidagicha taʼriflash mumkin: bu sotsium holati boʻlib, bunda davlat, jamiyat va shaxsga nisbatan axborot makonidagi tartibli va stixiyali ravishda vujudga keladigan axborot okimlari orqali boʻladigan tahdiddir. Axborot

xavfsizligi deganda – shaxs, jamiyat va davlat hayotiy muhim manfaatlarining axborot urushi, intervensiya hamda dezinformatsiya tazyiqlaridan himoyalanganligi tushuniladi. Axborot xavfsizligining mohiyati davlatning axborot resurslarini saqlash, axborot sohasida shaxs va jamiyatning qonuniy huquqlarini himoyalashdan iboratdir.

Axborot xavfsizligi ob'ektlariga axborot resurslari, ularning shakllanish, tarqalish va foydalanish tizimi, infrastrukturasi, tizim faoliyatini ta'minlovchi tashkiliy va iqtisodiy mexanizmlar kiradi. Axborot xavfsizligi resurslari davlatning hujjatlar shaklidagi (kutubxona, arxiv, fond) axborotlari, kompyuter dasturlari, bilim va axborot manbalari hamda boshqa tashkilot turlaridan iborat.

Axborot xavfsizligiga tahdid deganda esa, shaxs, jamiyat va davlatning axborot sohasidagi manfaatlari yig'indisi sifatida milliy manfaatlarni amalga oshirishga to'siq bo'layotgan, shuningdek, jamiyat axborot muhitining faoliyatiga, saqlanishiga va taraqqiyotiga zarar yetkazishga bevosita imkon yaratuvchi omil yoki omillar majmui tushuniladi. Uning quyidagi turlari mavjud: Axborot – axborot almashuv reglamentining buzilishi (axborotni noqonuniy to'plash va undan foydalanish; axborotni ataylab noto'g'ri tarqatish; axborotni noqonuniy ravishda axborot tizimidan ko'chirish; axborotni o'g'irlash). Matematik-dasturiy: virus dasturlarini qo'llash; axborot tizimidan ma'lumotni yo'qotish va modifikatsiya qilish. Jismoniy: axborot va aloqalarni qayta ishlash vositalarini yo'qotish hamda axborot texnologiyalarini izdan chiqarish; apparat va dastur ochqich kalitlarini o'g'irlash; jismoniy, matematik-dasturiy va axborot xavf solish maqsadida shaxsga bo'lgan tazyiq.

Radioelektron: axborot va ma'lumotlar tarqatish tarmoqlaridan axborotlarni to'xtatib qolish; boshqaruv tizimi va aloqa tarmoqlarini radioelektron usul bilan izdan chiqarish. Davlat, jamiyat va shaxs manfaatlarini bunday tahdidlardan himoya qilish aynan axborot xavfsizligini ta'minlash orqali amalga oshiriladi.

Axborot xavfsizligining tarkibiy qismlari sifatida quyidagilarni ko'rsatsa bo'ladi:

1) axborot makonining xavfsizligi holati, bu holatda u davlat, jamiyat va fuqarolarning manfaatlari yo'lida shakllanadi va rivojlanadi;

2) axborot infrastrukturasi xavfsizligi holati, bu holatda axborot o'z maqsadiga binoan aniq ishlatiladi va ishlatilish chog'ida tizimga salbiy ta'sir ko'rsatmaydi;

«Davlatning axborot borasidagi xavfsizligi» quyidagi yo'llar bilan ta'minlanadi:

axborot sohasidagi xavfsizlikka tahdidlarga qarshi harakatlar yuzasidan iqtisodiy, siyosiy, tashkiliy va boshqa tushadagi chora tadbirlarni amalga oshirish;

davlat sirlarini saqlash va davlat axborot resurslarini ulardan ruxsatsiz tarzda foydalanilishidan muhofaza qilish;

O'zbekiston Respublikasining jahon axborot makoniga va zamonaviy telekommunikatsiyalar tizimlariga integratsiyalashuvi;

Ta'kidlaganimizdek, tashkilotda axborot xavfsizligini ta'minlashning samarali tashkil etish vositalaridan biri bu axborot xavfsizligi siyosatini joriy etishdir. Xo'sh

axborot xavfsizligi siyosati nima, u qanday joriy etiladi va joriy qilishdan maqsad nimalardan iborat?

Axborot xavfsizligi siyosatining ko‘plab ta‘riflari turli xujjatlarda keltirilgan, shulardan davlat organlari uchun mos keluvchi ta‘rifni quyida keltirib o‘tamiz:

Axborot xavfsizligi siyosati birinchi navbatda, tashkilotda axborot xavfsizligini ta‘minlashning maqsad va vazifalarini faoliyatga singdirish uchun zarurdir. Faoliyat yuritayotgan har bir xodim shuni tushunishi kerakki, xavfsizlik xodimi nafaqat ma‘lumotlar chiqib ketishini tekshiruvchi xodim, balki kompaniya xatarlarini minimallashtirish va shu sababli kompaniya rentabelligini oshirishda yordamlashuvchidir.

Yurtimizda elektron hukumatni qurish, davlat organlari faoliyatini raqamlashtirish bilan bog‘liq harakatlar jadal suratlar bilan amalga oshirilmoqda. Hukumatning tegishli qarorlari va axborot xavfsizligi sohasidagi standartlarga (O‘z DSt ISO/IEC 270XX) muvofiqlik bilan har bir tashkilotda axborot xavfsizligi siyosatini ishlab chiqish va joriy qilinishi lozimligi yuzasidan talablar keltirilgan.

Bunday foydalanish natijasida quyidagi oqibatlar yuzaga kelishi mumkin:

- axborotning o‘g‘irlanishi;
- axborotni o‘zgartirish;
- axborotning yo‘qotilishi;
- yolg‘on axborotni kiritish;
- axborotni qalbakilashtirish va h.k

Uslubiy qo‘llanma tashkilotda xavfsizlikni boshqarish bo‘yicha amaliy choralarini tanlash, shuningdek, tashkilotlar o‘rtasida ma‘lumotlar almashishda ularning yaxlitligi, qulayligi va maxfiyligini ta‘minlash uchun asosdir.

Login – shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi hisoblanadi.

Parol – uning egasi haqiqiylikni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z). U kompyuter bilan muloqot boshlashdan oldin, unga klaviatura yoki identifikatsiya kartasi yordamida kiritiladigan harfli, raqamli yoki harfli-raqamli kod shaklidagi maxfiy so‘zdan iborat.

Xulosa

Axborot-kommunikatsiya tizimining ixtiyoriy tarkibiy qismlaridan biri bo‘lgan, hamda axborot tizimi taqdim etadigan imkoniyat mavjud bo‘lgan resurslardan belgilangan qoidalarga muvofiq bo‘lmagan holda, foydalanishni cheklash qoidalariga rioya qilmasdan foydalanish – bu resurslardan ruxsatsiz foydalanish toifasiga kiradi.

O‘zbekiston Respublikasi hududida davlat va xo‘jalik boshqaruvi organlarida, shuningdek mahalliy davlat hokimiyati organlarida (bundan buyon matnda tashkilotlar deb yuritiladi) axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishning asosiy tamoyillari va tartibini belgilovchi — “O‘zbekiston Respublikasi hududida axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha uslubiy qo‘llanmalar” ham 2013-2020 yillarda O‘zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini rivojlantirishni muvofiqlashtirish bo‘yicha Respublika komissiyasining 2016 yil 23 fevraldagi 7 bayonini bilan tasdiqlangan.

Foydalanilgan adabiyotlar:

1. GOST R 50922-2006. Natsionalnyy standart Rossiyskoy Federatsii: Zashchita informatsii. Osnovnye terminy i opredeleniya.// <https://docs.cntd.ru/document/1200058320>.
2. Plagiatni kidirish usullarini ishlab chikish. Muallif: Abrarov Rinat Dinarovich. Sarlavxa: Maxsus son. Tomonidan nashr etilgan: "Yosh olim" da 12-son (116) 5-7-betlar. Iyun-22016
3. Matnning uziga xosligini tekshirish. [Elektron resurs]. - Kirish tartibi: <https://etxt.ru/antiplagiat/>
4. Antiplagiatni kandy aldash kerak. Antiplagiatni aldashning ishlash usullari. [Elektron resurs]. - Kirish rejimi.
5. Gosudarstvennaya informatsionnaya politika// Osnovy informatsionnoy bezopasnosti v telekommunikatsiyax.
6. Ponyatie «gosudarstvennaya informatsionnaya politika». sistema informatsionnoy bezopasnosti v obshchestve// <https://www.historyjournal.ru/index.php?request=full&id=78>.
7. Tulenova G.J. O‘zbekistonda axborot xavfsizligini ta‘minlash sohasida davlat siyosatining huquqiy asoslari// https://drive.google.com/file/d/0Bxwxnt_0wPHqVzRFY2l0czUzSXc/view?resourcekey=0-02FZLSJk6D1SXAACjN5dqw.
8. O‘zbekiston Respublikasining “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun 2012 yil 12 dekabr.// <https://parliament.gov.uz/uz/laws/adopted/99/3283/>