RAQAMLI TEXNOLOGIYALARI DAVRIDA SOHADA AXBOROT XAVFSIZLIK

Marg‘ilon 1-son kasb-hunar maktabi
Maxsus fan o‘qituvchisi
Kamolova Muqaddamxon Sohibjonovna

Annotatsiya. *Raqamli texnologiyalari davrida sohada axborot xavfsizlik xaqida ma’lumotlar berilgan.*

Kalit so‘zlar: *GDPR, infoetika, AI neoretorika, ritorika, qora ritorika, axborot xavfsizligi etikasi.*

KIRISH

Raqamli texnologiyalar davrida axborot xavfsizligi juda muhim masala bo‘lib, bu nafaqat kompaniyalar va tashkilotlar, balki har bir shaxs uchun ham dolzarbdir. Axborot xavfsizligi — bu ma'lumotlarni himoya qilish, ularni ruxsatsiz kirishdan, o‘zgartirishdan yoki yo‘qotishdan saqlash jarayonidir.

Raqamli tarmoqlarning rivojlanishi bilan "axborot xavfsizligi" tushunchasi dunyoda tobora dolzarb bo‘lib bormoqda. Iqtisodiyot va ijtimoiy sohani raqamlashtirishga yo‘l olgan O‘zbekiston uchun ham bu masala ustuvor ahamiyatga ega. O‘zbekiston Respublikasi Prezidenti tashabbusi bilan iyun oyi oxirida Toshkentda MDH davlatlarining axborot xavfsizligi masalalari bo‘yicha xalqaro ekspertlar forumi o‘tkazilgani bejiz emas.

Ko‘pincha tibbiy va davlat muassasalari yoki chakana sektordagi tashkilotlar kiberhujumlarga duchor bo‘ladi. Aksariyat hollarda sabab jinoyatchilarning harakatlaridir. Har qanday kompaniya, tashkilot yoki moliya instituti maqsad bo‘lishi mumkin. Mutaxassislarning qayd etishicha, 2020 yilda dunyoda 1120 ta yirik kiberhujumlar qayd etilgan. Hammasi bo‘lib, 20 milliard yozuv buzilgan. Global axborot texnologiyalari va telekommunikatsiya bozorini o‘rganuvchi International Data Corporation xalqaro tadqiqot va konsalting kompaniyasi prognozlariga ko‘ra, agar kiberxavflar soni o‘sishda davom etsa, 2022-yilga borib kiberxavfsizlik yechimlari uchun global xarajatlar 133,7 milliard dollarga etadi. Ko‘pgina hukumatlar kiberxavfsizlikning samarali amaliyotlarini amalga oshirishda tashkilotlarga yordam berish orqali kiberjinoyatchilarga qarshi kurashmoqda.

Axborot xavfsizligining asosiy jihatlari:

1.Bu ma'lumotlarning maxfiyligini, yaxlitligini va mavjudligini ta'minlashni o‘z ichiga oladi. Masalan, shifrlash texnologiyalari yordamida ma'lumotlar ruxsatsiz kirishdan himoyalanadi.

2. Kiberhujumlar (masalan, viruslar, trojanlar va phishing) raqamli axborot xavfsizligiga jiddiy tahdid solishi mumkin. Shuning uchun antivirus dasturlari va kiberxavfsizlik protokollari muhim ahamiyatga ega.

3. Foydalanuvchilarning identifikatsiyasini ta'minlash uchun kuchli parollar, ikki faktorli autentifikatsiya kabi usullar qo‘llaniladi.

4. Tarmoq xavfsizligi: Tarmoqni himoya qilish uchun devorlar (firewalls), tarmoq monitoringi va boshqa texnologiyalar foydalaniladi.

5.Xavf-xatarlarni aniqlash va ularga tezda javob berish jarayonlari muhimdir. Bu bilan kiberhujumlarning oqibatlarini kamaytirishga imkon beriladi.

6. Foydalanuvchilarni axborot xavfsizligi bo‘yicha o‘qitish va xabardor qilish muhimdir, chunki ko‘p hollarda inson omili kiberxavflarning paydo bo‘lishida asosiy sabab bo‘ladi.

7.Axborotni himoya qilishda turli xil qonunlar (masalan, GDPR) va standartlarga amal qilish zarur.

Kelajakdagi tendensiyalar:

- Sun’iy intellekt (AI) yordamida kiberhujumlarni aniqlash va ularga qarshi kurashish.
- Bulutli texnologiyalarda axborot xavfsizligini ta'minlash.
- IoT qurilmalarining xavfsizligi, chunki ularning soni ortib bormoqda.

Xavf-xatarlarni oldini olish strategiyalari, masalan, doimiy monitoring tizimlari orqali real vaqt rejimida javob berish imkoniyatlari.Ayni vaqtda butun dunyoda axborot xavfsizligi masalasiga dolzarb vazifa sifatida qaralayapti. Jumladan, mamlakatimizda ham axborot xavfsizligini ta'minlash, uning huquqiy bazasini yaratish borasida qator chora-tadbirlar amalga oshirib kelinmoqda. Xususan, kiber tahdidlarga qarshi kurashda barcha davlat organlari harakatlari muvofiqlashtirilayapti. E’tiborlisi, O‘zbekiston Markaziy Osiyoda birinchilardan bo‘lib axborot va kommunikasiya texnologiyalari sohasidagi xalqaro xavfsizlik tizimiga qo‘shildi. Shuningdek, respublikamizda axborot xavfsizligi sohasiga ixtisoslashtirilgan xizmatlar va kompleks texnik echimlarni taqdim etadigan kompaniyalar faoliyat yuritayapti. Ta’kidlash joiz, hukumatimizning tegishli qarorlariga muvofiq, Axborot texnologiyalari va kommunikasiyalarini rivojlantirish vazirligi huzurida Axborot xavfsizligini ta'minlash markazi tashkil etilgan. Markaz kompyuter hodisalari bo‘yicha axborotni yig‘ish va tahlil qilish, axborot xavfsizligini ta'minlashga texnik va konsultativ yordam berish bo‘yicha O‘zbekistonda yagona davlat muassasasi sanaladi. Mazkur faoliyatdan ko‘zda tutilgan asosiy maqsad iqtisodiyotning barcha tarmoqlari va sohalarida axborotni himoya qilishning zamonaviy vositalarini yanada rivojlantirish va keng joriy qilishni ta'minlashdan iborat.

Bugungi kunda axborot-kommunikatsiya texnologiyalari iqtisodiyotning barcha sohalarida zamonaviy boshqaruv tizimlarining ajralmas qismidir. Iqtisodiyot tarmoqlarining o‘zgarishi, bu jarayonning raqamlashuvi, mobillashuvi, sohaga sun’iy intellektning joriy etilishi bilan bog‘liq muhim davrni boshdan kechirmoqda. Xususan, 2020 — 2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiyani, “Kiberxavfsizlik to‘g‘risida” gi qonun loyihasini hamda O‘zbekiston Respublikasi

yagona axborot siyosati konsepsiyasi ishlab chiqish belgilandi.[1] Prezidentning 2018 yil 21 noyabrdagi PQ-4024-son Qarori bilan davlat unitar korxonasi shaklida Kiberxavfsizligi markazi tashkil etildi. Ta'kidlash joizki kiberxavfsizlik sohasiga tegishli bo'lgan 17 ta qonun hujjati, 9 ta Prezident Farmon va Qarorlari, 14 ta Vazirlar Mahkamasining Qarori, shuningdek tegishli normalar va ko'plab idoralararo me'yoriy-huquqiy hujjatlar qabul qilingan.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Raqamli texnologiyalar davrida axborot xavfsizligi muhim ahamiyatga ega. Quyidagi asosiy nuqtalarni ko'rib chiqish mumkin:

Axborot xavfsizligi muhim jihatlari

- Ma'lumotlar faqat ruxsat etilgan shaxslar tomonidan ko'rilishi kerak.
- Ma'lumotlar o'zgartirilmasligi yoki buzilmasligi kerak.
- Foydalanuvchilar kerakli ma'lumotlarga o'z vaqtida va xavfsiz ravishda kirish imkoniyatiga ega bo'lishi kerak.

Xavflar va tahdidlar

- Xakerlik, fishing va boshqa internet orqali amalga oshiriladigan xavflar.
- Viruslar, troyanlar va boshqa zararli dasturlar tizimlarni buzishi mumkin.
- Xodimlar tomonidan ma'lumotlarning noto'g'ri ishlatilishi yoki o'g'irlanishi.

Himoya choralari

- Ma'lumotlarni shifrlash orqali ularning maxfiyligini ta'minlash.
- Murakkab va muntazam yangilanadigan parollarni ishlatish.
- Antivirüs dasturlari va xavfsizlik devorlari o'rnatish.
- Xodimlarni muntazam ravishda xavfsizlik qoidalari bo'yicha o'qitish.

Bu chora-tadbirlar axborot xavfsizligini ta'minlashda yordam beradi va raqamli texnologiyalar davrida muhim ahamiyatga ega.

MUHOKAMA VA NATIJALAR:

Bu borada amalga oshirilayotgan ishlarning samaradorligini oshirish va takomillashtirish uchun yana quyidagi ishlarni taklif qilmoqchimiz:

1) Axborot xavfsizligini ta'minlashga qaratilgan milliy qonunchilik bazasini takomillashtirish, xususan, alohida qonun hujjati qabul qilish masalasini ko'rib chiqish;

2) milliy axborot makonimizni aholining qiziqishini inobatga olgan holda jarayonlarni ob'ektiv va pozitiv yorituvchi mahalliy va xorijiy axborotlar bilan muntazam to'ldirib borish;

3) xalqimizning, xususan, yoshlarning internetdan foydalanish madaniyatini o'stirish, undagi har qanday axborotni tafakkur va tahlil qilib, so'ng xulosa chiqarishga o'rgatishimiz zarur;

[1] Barakayevich, Q. S., & Baxtiyorovna, A. S. (2021). Xalqaro dastur talabalari asosida innovatsion ta'lim muhitini yaratish. Integration of science, education and practice. scientific-methodical journal, 1(02), 132-137.

4) mamlakatimiz to‘g‘risida noto‘g‘ri, bir taraflama axborot tarqatuvchi har qanday xorijiy axborot vositalari faoliyatiga qonun doirasida chek qo‘yish, bu kabi axborotlari uchun ularning javobgaligini oshirish va tarqatilgan axborotlarning bir taraflama yoki noto‘g‘ri ekanligini mutaxassislar ishtirokida xalqimizga o‘z vaqtida yetkazish;

5) o‘rta maxsus va professional ta'lim, shuningdek, oliy ta'lim muassasalarida axborot xavfsizligini ta'minlash, xususan, axborot xurujlari, uning shakl va ko‘rinishlari, maqsadi va salbiy oqibatlari borasida maxsus kurslar o‘tilishini ta'minlash;

Xulosa. Raqamli texnologiyalar rivojlanishi bilan birga axborot xavfsizlikka e'tibor qaratish yanada zarur bo‘ladi. Har bir shaxs hamda tashkilot o‘z ma'lumotlarini himoya qilishi kerak.

FOYDALANGAN ADABIYOTLAR:

1. Qonun hujjatlari ma'lumotlari milliy bazasi, 03.07.2019-y., 03/19/547/3363-son, 4 - modda.

2.Barakayevich, Q. S., & Baxtiyorovna, A. S. (2021). Xalqaro dastur talabalari asosida innovatsion ta'lim muhitini yaratish. Integration of science, education and practice. scientific-methodical journal, 1(02), 132-137.

3. Elmurzaeva, N. K., & Qorayev, S. B. (2021). Pedagogical Requirements for the Organization of the Educational Process in Specialized State Educational Institutions. Psychology and Education Journal, 58(1), 1078-1084.

4. Эрназаровой, Г. О. (2017). Подготовка учащихся к профессиональной деятельности на основе акмеологического подхода. Традиционная и инновационная наука: история, современное состояние, перспективы: сборник статей, 115.

5. O‘tayev A. Zamonaviy ta'limda bo‘lajak boshlang‘ich sinf o‘qituvchilarining siyosiy tarbiyasi.Science and Education Volume 1, Special Issue 4, December 2020.135-143b.

5. RAQAMLI TEXNOLOGIYALAR DAVRIDA SHAXSIY MA’LUMOTLARNI MUHOFAZA QILISHNING HUQUQIY ASOSLARI – тема научной статьи по психологическим наукам читайте бесплатно текст научно-исследовательской работы в электронной библиотеке КиберЛенинка (cyberleninka.ru)