ISSN 2181-3187

AXBOROT XAVFSIZLIGI TUSHUNCHASI

Rasulova Feruzaxon Uktambek qizi
Izboskan tuman 2-son politexnikumi
Informatika va AT fani o‘qituvchisi.

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

Kalit so’zlar: Axborot xavfsizligi, kibertahdid, IoT xavfsizligi, kiberjinoyat, GDPR, CCPA, HIPAA, sun’iy intellect(AI).

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 ta’sir ko‘rsatishi mumkin. Axborot xavfsizligini ta’minlashning ko‘plab usullari va sohalari mavjud. Bugungi maqolamizda tashkilotda axborot xavfsizligini ta’minlashning asosiy hujjati sanalmish axborot xavfsizligi hujjati to‘g‘risida so‘z yuritiladi. Axborot xavfsizligi ma’lumotlar bazasiga ruxsatsiz kirish, oshkor qilish, o’zgartirish yoki yo’q qilishdan himoya qilish uchun amalga oshirilgan amaliyotlar, texnologiyalar va siyosatlarni o’z ichiga oladi. Bu axborot aktivlarining maxfiyligi, yaxlitligi va mavjudligini saqlash uchun zarurdir. Kibertahdidlar katta bo’lgan dunyoda axborot xavfsizligini ta’minlashning mustahkam choralari xavflarni kamaytirish va biznes uzluksizligini ta’minlash uchun juda muhimdir.

ISSN 2181-3187

MUHOKAMA

Axborot xavfsizligining ahamiyati shaxsiy daxlsizlik va milliy xavfsizlikni qamrab olish uchun tashkiliy chegaralardan tashqariga chiqadi. Ma'lumotlarning buzilishi jiddiy oqibatlarga olib kelishi mumkin, jumladan moliyaviy yo'qotishlar, obro'ga putur etkazish va yuridik javobgarlik. Bundan tashqari, bir-biriga uzviy bog'langan dunyoda nozik ma'lumotlarda muammolar yuzaga kelishi nafaqat tashkilotga, balki uning hamkorlari, mijozlari va manfaatdor tomonlariga ham ta'sir qiladigan jiddiy oqibatlarga olib kelishi mumkin.

Axborot xavfsizligining hozirgi tendensiyalari :

Axborot xavfsizligi landshafti dinamik bo'lib, yangi tahdidlar paydo bo'ladi va mavjudlari ham tez rivojlanmoqda. Axborot xavfsizligining hozirgi holatini bir qancha tendentsiyalar shakllantirmoqda:

1. Kiberjinoyatlarning kuchayishi: Kiberjinoyatchilar tizimlarga kirish va maxfiy ma'lumotlarni o'g'irlash uchun to'lov dasturi, fishing va ijtimoiy muhandislik kabi ilg'or usullardan foydalanib, tobora murakkablashib bormoqda.

2. IoT xavfsizligi muammolari: Internet of Things (IoT) qurilmalarining tarqalishi yangi xavfsizlik zaifliklarini keltirib chiqaradi, chunki bu qurilmalarning aksariyati mustahkam xavfsizlik xususiyatlariga ega emas va ko'pincha xavfsiz tarmoqlarga ulanadi.

3. Bulutli xavfsizlik xavotirlari: Bulutli hisoblash ko'plab afzalliklarni, jumladan, masshtablilik va iqtisodiy samaradorlikni taqdim etsa-da, u ma'lumotlar xavfsizligi va maxfiyligi bilan bog'liq xavotirlarni ham keltirib chiqaradi. Tashkilotlar bulutda saqlanadigan va qayta ishlanadigan ma'lumotlarni himoya qilish uchun mustahkam bulut xavfsizligi choralarini qo'llashlari kerak.

4. Zero Trust Architecture: An'anaviy perimetrga asoslangan xavfsizlik modeli bugungi dinamik va taqsimlangan hisoblash muhitida endi etarli emas. Nolinchi ishonch arxitekturasi tarmoq ichida yoki tashqarisida hech qanday ob'ekt sukut bo'yicha ishonchli bo'lmagan modelni yoqlaydi va identifikator, qurilma va boshqa kontekst omillari asosida qattiq kirish nazorati amalga oshiriladi.

ISSN 2181-3187

5. Xavfsizlik sohasida sun’iy intellekt (AI) va Machine Learning (ML): AI va ML texnologiyalari tahdidlarni aniqlash, anomaliyalarni aniqlash va kiberxavfsizlikda avtomatlashtirilgan javob berish uchun tobora ko’proq foydalanilmoqda. Biroq, raqiblar AIdan yanada murakkab hujumlarni amalga oshirish uchun foydalanmoqdalar va xavfsizlik mutaxassislari va kiber jinoyatchilar o’rtasida mushuk va sichqoncha o’yinini yaratadilar.

Axborot xavfsizligidagi muammolar Texnologiyalar va kiberxavfsizlik amaliyotidagi yutuqlarga qaramay, tashkilotlar o’zlarining raqamli aktivlarini himoya qilishda ko’plab muammolarga duch kelishadi:

1. Kiberxavfsizlik bo’yicha ko’nikmalar etishmasligi: Kiberxavfsizlik bo’yicha mutaxassislarning global tanqisligi tashkilotlar uchun malakali iste’dodlarni topish va saqlab qolishni qiyinlashtiradi. Ushbu ko’nikmalardagi bo’shliq ularning kiber tahdidlarni samarali aniqlash, oldini olish va ularga javob berish qobiliyatiga to’sqinlik qiladi.

2. AT muhitlarining murakkabligi: zamonaviy IT muhitlari mahalliy infratuzilma, bulut xizmatlari va IoT qurilmalari bog’liqligi bilan tobora murakkablashib bormoqda. Ushbu xilma-xil muhitlarda xavfsizlikni boshqarish, ayniqsa, ko’rish va nazorat qilish nuqtai nazaridan muhim muammolarni keltirib chiqaradi.

3. . Muvofiqlik va me’yoriy talablar: Tashkilotlar GDPR, CCPA, HIPAA va PCI DSS kabi ma’lumotlarni himoya qilish qoidalari va sanoat standartlarining murakkab landshaftini boshqarishi kerak. Operatsion samaradorlikni saqlagan holda muvofiqlikka erishish ko’plab tashkilotlar uchun qiyin vazifa bo’lishi mumkin.

4. Insayder tahdidlar: qasddan yoki qasddan bo’lmagan ichki tahdidlar axborot xavfsizligi uchun katta xavf tug’diradi. Yovuz niyatli insayderlar ma’lumotlarni o‘g‘irlash yoki operatsiyalarni to‘xtatish uchun o‘zlarining kirish huquqlaridan noto’g’ri yolda foydalanishlari mumkin, beparvo insayderlar esa ehtiyotsiz harakatlar orqali nozik ma’lumotlarni beixtiyor fosh qilishlari mumkin.

5. Rivojlanayotgan texnologiyalar va tahdidlar: AI, IoT va blokcheyn kabi rivojlanayotgan texnologiyalarning tez o’zlashtirilishi yangi xavfsizlik muammolari va

ISSN 2181-3187

hujum vektorlarini keltirib chiqaradi. Xavfsizlik bo'yicha mutaxassislar paydo bo'ladigan tahdidlarni samarali tarzda oldindan bilish va yumshatish uchun ushbu o'zgarishlardan xabardor bo'lishlari kerak.

Axborotlarni himoya qilish strategiyalari :

Kiber tahdidlar keltirib chiqaradigan ko'p sonli muammolarni hal qilish uchun tashkilotlar axborot xavfsizligiga ko'p qirrali yondashuvni qo'llashlari kerak:

1. Risklarni boshqarish: kiberxavfsizlik risklarini aniqlash, baholash va ustuvorliklarini belgilash uchun keng qamrovli risklarni boshqarish tizimini joriy etish. Bu xavflarni muntazam ravishda baholash, xavflarni kamaytirish strategiyalarini ishlab chiqish va nazorat samaradorligini monitoring qilishni o'z ichiga oladi.

2. Xavfsizlik bo'yicha treninglar: xodimlarni kiberxavfsizlik bo'yicha ilg'or amaliyotlar va maxfiy ma'lumotlarni himoya qilish muhimligi haqida o'rgatish uchun xavfsizlik bo'yicha o'quv dasturlariga mablag sarflash lozim. Axborotli va hushyor ishchi kuchi kiber tahdidlardan himoyalanishning muhim chizig'i hisoblanadi.

3. Kuchli autentifikatsiya mexanizmlarini amalga oshirish: tizimlar va ma'lumotlarga ruxsatsiz kirishning oldini olish uchun ko'p faktorli autentifikatsiya (MFA) kabi kuchli autentifikatsiya mexanizmlarini qo'llash talab etiladi. Bu hisob ma'lumotlarini o'g'irlash va hisob qaydnomasiga ruxsatsiz kirish xavfini kamaytirishga yordam beradi.

4. Ma'lumotlarni shifrlash: ruxsatsiz kirishdan himoya qilish uchun maxfiy ma'lumotlarni dam olishda ham, tranzitda ham shifrlang. Shifrlash ma'lumotlar noqonuniy o'zlashtirilgan yoki buzilgan taqdirda ham tegishli shifrni ochish kalitlarisiz o'qilmasligini ta'minlaydi.

5. Muntazam xavfsizlik tekshiruvlari va baholashlari: Zaifliklar, noto'g'ri konfiguratsiyalar va muvofiqlik bo'shliqlarini aniqlash uchun muntazam xavfsizlik auditlari va baholashlarini o'tkazish lozim. Bu tashkilotlarga xavfsizlik masalalarini zararli shaxslar tomonidan foydalanishdan oldin faol ravishda hal qilish imkonini beradi.

ISSN 2181-3187

6. Hodisalarga javob berishni rejalashtirish: Ma’lumotlarning buzilishi, zararli dasturlarning infeksiyalari va xizmat ko’rsatishni rad etish hujumlari kabi kiberxavfsizlik hodisalariga samarali javob berish uchun kuchli hodisalarga javob berish rejasini ishlab chiqish va qo’llab-quvvatlash talab etiladi. Rejada voqealar ta’sirini minimallashtirish uchun rol va mas’uliyat, aloqa protokollari va kuchayish tartib-qoidalari belgilanishi kerak.

7. Hamkorlik va axborot almashish: Rivojlanayotgan tahdidlar va ilg’or tajribalardan xabardor bo’lish uchun sohadagi tengdoshlar, davlat idoralari va kiberxavfsizlik tashkilotlari o’rtasida hamkorlik va axborot almashishni rivojlantirish kerak. Tahdid ma’lumotlari va olingan saboqlarni almashish tashkilotlarga kiberhujumlardan yaxshiroq himoyalanishiga yordam beradi.

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 yilllarda O‘zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini rivojlantirishni muvofiqlashtirish bo‘yicha Respublika komissiyasining 2016 yil 23 fevraldagi 7 bayonini bilan tasdiqlangan.

Foydalanilgan adabiyotlar:

1. “O’zbekistonda Axborot xavfsizligi to’g’risida yangi qonun qabul qilindi” – O’zbekistonning AQShdagi elchixonasi rasmiy saytida chop etilgan maqola (https://uzbekistan.org/article/uzbekistan-adopts-new-law-information-security)

ISSN 2181-3187

2. “O’zbekistonning beshta asosiy yo’nalish bo’yicha Harakatlar strategiyasi va “Kiberxavfsizlik to’g’risida”gi qonun” – maqola O’zbekiston Respublikasi Mudofaa vazirligi rasmiy saytida (https://mud.uz/en/news/6445)

3. “O’zbekistonda kiberxavfsizlik: qiyosiy tahlil” – Xalqaro kiber urush va terrorizm jurnali (https://www.igi-global.com/article/cybersecurity-in-uzbekistan/224129) saytida chop etilgan tadqiqot ishi.

4. “2019-2021 yillarda O’zbekiston Respublikasining axborot-Ta'limning zamonaviy transformatsiyasi kommunikatsiya texnologiyalarini rivojlantirish Davlat dasturi” – O’zbekiston hukumati tomonidan tarqatilgan rasmiy hujjat.

5. “Axborot xavfsizligi to‘g‘risidagi O‘zbekiston qonuni” – O‘zbekiston Adliya vazirligi tomonidan e’lon qilingan rasmiy huquqiy hujjat.