AXBOROT XAVFSIZLIGINI TA’MINLASH USULLARI. AXBOROT XAVFSIZLIGI TUSHUNCHASI VA ZARURIYATI.

Toshboltayev Faxriddin O‘rinboyevich
FarDU Axborot texnologiyalari kafedrasi katta o‘qituvchisi (PhD)
To‘ychiyeva Dilnozaxon Qodirjon qizi
Farg‘ona davlat universiteti Chet tillari fakulteti 1-kurs talabasi

Annotatsiya: Ushbu maqolada axborot xavfsizligi tushunchasi, uning jamiyat va tashkilotlar hayotidagi o‘rni hamda bu xavfsizlikni ta’minlashning zamonaviy usullari tahlil qilinadi. Axborot resurslari bugungi raqamli davrda eng muhim boyliklardan biri hisoblanadi. Shu sababli ularni himoyalash, axborotga ruxsatsiz kirish, uni o‘zgartirish yoki yo‘q qilishga qarshi samarali choralar ko‘rish dolzarb masalaga aylangan. Maqolada axborot xavfsizligining asosiy tamoyillari — maxfiylik, yaxlitlik va mavjudlik yoritilgan, shuningdek, shifrlash, autentifikatsiya va tarmoq xavfsizligi kabi usullar ko‘rib chiqilgan.

Kalit so‘zlar: Axborot xavfsizligi, himoya usullari, maxfiylik, yaxlitlik, mavjudlik, shifrlash, autentifikatsiya, kiberxavfsizlik, tarmoq xavfsizligi, axborot texnologiyalari.

Annotation: This article explores the concept of information security, its importance in the lives of societies and organizations, and the modern methods used to ensure it. In today's digital era, information resources are among the most valuable assets. Therefore, protecting data from unauthorized access, alteration, or destruction has become a critical issue. The article highlights the key principles of information security — confidentiality, integrity, and availability — and examines protection methods such as encryption, authentication, and network security.

Keywords: Information security, protection methods, confidentiality, integrity, availability, encryption, authentication, cybersecurity, network security, information technology.

Аннотация: В данной статье рассматриваются понятие информационной безопасности, её роль в жизни общества и организаций, а также современные методы обеспечения этой безопасности. В условиях цифровой эпохи

информационные ресурсы становятся одним из важнейших активов. Поэтому защита информации от несанкционированного доступа, изменений или уничтожения становится актуальной задачей. В статье подробно освещаются основные принципы информационной безопасности — конфиденциальность, целостность и доступность, а также рассматриваются такие методы защиты, как шифрование, аутентификация и сетевая безопасность.

Ключевые слова: Информационная безопасность, методы защиты, конфиденциальность, целостность, доступность, шифрование, аутентификация, кибербезопасность, сетевая безопасность, информационные технологии.

Zamonaviy jamiyatda axborot eng muhim strategik resurslardan biri hisoblanadi. Davlat idoralari, tijorat tashkilotlari, ta’lim muassasalari va oddiy foydalanuvchilar faoliyati to‘liq axborot texnologiyalariga bog‘liq holda rivojlanmoqda. Bu esa axborot xavfsizligining ta'minlanishini muhim masalaga aylantiradi. Axborot xavfsizligi deganda, axborotning ruxsatsiz kirish, o‘zgartirish, tarqatish yoki yo‘q qilinishdan himoyalanish holati tushuniladi. Xususan, raqamli ma'lumotlar, onlayn xizmatlar va tarmoqlar orqali uzatiladigan axborotlar kiberxavf-xatarlar tahdidiga duch keladi.

Bugungi kunda axborotni himoyalash nafaqat texnik vositalar, balki tashkiliy, yuridik va axloqiy yondashuvlarni ham o‘z ichiga oladi. Axborot xavfsizligini ta’minlash, foydalanuvchilar va tashkilotlar uchun xavfsiz muhit yaratish orqali ularning ishonchliligini oshiradi. Shu bois, axborot xavfsizligi nafaqat IT mutaxassislari, balki har bir zamonaviy inson uchun muhim bilim sohasiga aylangan. Ushbu maqolada axborot xavfsizligining mazmuni, uning zaruriyati va himoya qilish usullari atroflicha yoritiladi.

1. Axborot xavfsizligining asosiy tushunchalari

Axborot xavfsizligi — bu axborotni ruxsatsiz kirish, o‘zgartirish, tarqatish yoki yo‘q qilishdan himoya qilishga qaratilgan chora-tadbirlar majmuasidir. Axborot xavfsizligi uchta asosiy prinsipga asoslanadi: maxfiylik (confidentiality), yaxlitlik (integrity) va mavjudlik (availability). Maxfiylik — axborotga faqat ruxsat etilgan shaxslar kirishini ta’minlaydi. Yaxlitlik — axborot buzilmasdan, asl holida saqlanishi kerakligini bildiradi.

Mavjudlik esa axborot zarur bo‘lgan vaqtda mavjud bo‘lishini anglatadi. Ushbu tamoyillar axborot xavfsizligining poydevori hisoblanadi.

2. Axborot xavfsizligining zaruriyati

Raqamli texnologiyalarning keng joriy etilishi bilan axborot oqimi sezilarli darajada oshdi. Ko‘plab jarayonlar — elektron hujjatlar yuritilishi, onlayn to‘lovlar, davlat xizmatlari, ta’lim va tibbiyot tizimlari — barchasi axborot texnologiyalariga tayanmoqda. Shu sababli, ushbu tizimlardagi ma’lumotlarning xavfsizligi milliy xavfsizlik darajasida ahamiyat kasb etmoqda. Axborotni yo‘qotish yoki unga ruxsatsiz kirish korxonalar uchun moliyaviy zarar, davlat uchun esa strategik yo‘qotishlarga olib kelishi mumkin. Shuningdek, shaxsiy ma’lumotlar bilan bog‘liq huquqbuzarliklar jamiyatda ishonchsizlik va ijtimoiy muammolarni yuzaga keltiradi.

3. Axborot xavfsizligiga tahdidlar

Axborot xavfsizligiga tahdidlar juda ko‘p va xilma-xil bo‘lishi mumkin. Ularni quyidagicha tasniflash mumkin:

Ichki tahdidlar: xodimlar tomonidan qasddan yoki bexosdan ma’lumotlarni sizdirish, noto‘g‘ri foydalanish.

Tashqi tahdidlar: xakerlik hujumlari, viruslar, zararli dasturlar, fishing (foydalanuvchi ma’lumotlarini qalbakilashtirish orqali o‘g‘irlash), DDoS hujumlari va boshqalar.

Texnik xatolar: tizimdagi nosozliklar, qurilmalarning ishdan chiqishi, noto‘g‘ri konfiguratsiyalar.

Tabiiy ofatlar: yong‘in, suv toshqini, zilzila va boshqa hodisalar natijasida axborot yo‘qolishi.

Bu tahdidlarning oldini olish uchun kompleks yondashuv talab etiladi.

4. Axborot xavfsizligini ta'minlash usullari

Axborot xavfsizligini ta'minlashda quyidagi asosiy usullar va vositalardan foydalaniladi:

a) Shifrlash (kryptografiya)

Shifrlash axborotni maxfiylashtirish orqali uni faqat belgilangan shaxslar o‘qiy oladigan shaklga keltirishni anglatadi. Simmetrik va assimmetrik shifrlash usullari mavjud. Masalan, RSA, AES, DES kabi algoritmlar keng qo‘llaniladi. Bugungi kunda onlayn aloqa, elektron pochta, internet banking va boshqa xizmatlarda shifrlash texnologiyalari asosiy xavfsizlik vositasi sifatida ishlatiladi.

b) Autentifikatsiya va avtorizatsiya

Autentifikatsiya — foydalanuvchini aniqlash jarayoni. Bu parollar, PIN-kodlar, biometrik ma’lumotlar (barmoq izi, yuz skaneri) yordamida amalga oshiriladi. Avtorizatsiya esa foydalanuvchiga qaysi resurslarga kirish huquqi berilganini aniqlaydi. Ikki bosqichli autentifikatsiya (2FA) xavfsizlikni sezilarli darajada oshiradi.

c) Tarmoq xavfsizligi

Tarmoqlar orqali axborot almashinuvi xavf-xatar bilan kechadi. Shu bois, xavfsiz tarmoq protokollaridan foydalanish (masalan, HTTPS, VPN), xavfsizlik devorlari (firewall), tarmoq monitoringi va tarmoqda harakatlarni filtrlaydigan tizimlar ishlatiladi.

d) Axborot xavfsizligi siyosati

Har qanday tashkilot o‘zining ichki axborot xavfsizligi siyosatiga ega bo‘lishi zarur. Bu siyosatda ma’lumotlardan qanday foydalanish mumkinligi, ruxsatsiz kirishga qanday javob berish, foydalanuvchilar uchun qanday qoidalar mavjudligi aniq ko‘rsatiladi. Bu me’yoriy hujjatlar orqali tashkilot ichida intizom va xavfsizlik madaniyati shakllanadi.

e) Zaxira nusxalar (backup)

Ma’lumotlarning zaxira nusxalarini muntazam yaratish — axborot xavfsizligini ta’minlashdagi muhim choralardan biridir. Zaxiralar tizimdagi nosozlik, hujum yoki tasodifiy yo‘qotishlar yuzaga kelganida axborotni tiklash imkonini beradi.

f) Axborot xavfsizligi bo‘yicha xodimlarni o‘qitish

Xodimlar axborot xavfsizligi haqida yetarlicha bilimga ega bo‘lmasa, eng kuchli texnologiyalar ham foydasiz bo‘lishi mumkin. Shu sababli tashkilotlar axborot xavfsizligi bo‘yicha muntazam treninglar va sinovlar o‘tkazib borishlari kerak. Bu foydalanuvchilarning fishing, zararli ilovalar va boshqa tahdidlarga qarshi hushyorligini oshiradi.

5. Zamonaviy tendensiyalar

So‘nggi yillarda axborot xavfsizligida sun’iy intellekt (AI), mashinali o‘rganish (machine learning) va avtomatlashtirilgan xavfsizlik tizimlari keng qo‘llanilmoqda. AI tizimlari potentsial hujumlarni bashorat qilishi, g‘ayrioddiy xatti-harakatlarni aniqlashi va avtomatik tarzda chora ko‘rishi mumkin. Shuningdek, bulutli texnologiyalar xavfsizligini ta’minlash, mobil qurilmalar xavfsizligi, IoT (Internet of Things) xavfsizligi kabi yangi yo‘nalishlar ham tobora dolzarb bo‘lmoqda.

6. Axborot xavfsizligini tartibga soluvchi qonunchilik

Ko‘plab davlatlarda axborot xavfsizligini tartibga soluvchi qonunlar mavjud. Masalan, O‘zbekiston Respublikasida “Axborotlashtirish to‘g‘risida”gi qonun, “Shaxsga oid ma’lumotlar to‘g‘risida”gi qonunlar bu sohaga oid asosiy huquqiy hujjatlar hisoblanadi. Shuningdek, xalqaro miqyosda ISO/IEC 27001 standarti axborot xavfsizligi boshqaruv tizimini joriy qilishda asosiy vositadir.

Axborot xavfsizligini ta’minlash bugungi raqamli davrda har qanday jamiyat va tashkilot faoliyatining ajralmas va strategik tarkibiy qismiga aylangan. Mavjud tahdidlarning murakkablashuvi, zararli dasturlar va kiberhujumlarning ko‘payib borayotgani, shuningdek, texnologik vositalarga bo‘lgan bog‘liqlikning ortishi axborot xavfsizligini alohida e’tibor talab qiladigan soha sifatida shakllantirdi. Ushbu maqolada ko‘rib chiqilgan chora-tadbirlar va texnologik yondashuvlar orqali nafaqat texnik jihatdan, balki tashkiliy va huquqiy asosda ham himoya mexanizmlarini barpo etish zarurati o‘z isbotini topdi.

Tahlillar shuni ko‘rsatadiki, faqatgina dasturiy himoya vositalari yoki apparat yechimlari bilan cheklanib qolish yetarli emas. Axborot xavfsizligi — bu keng qamrovli tizim bo‘lib, foydalanuvchi madaniyatidan tortib, davlat siyosatigacha bo‘lgan barcha omillarni o‘z ichiga oladi. Ayniqsa, foydalanuvchilarning xabardorlik darajasini oshirish, ularga tahdidlarni tanib olish va to‘g‘ri munosabatda bo‘lish ko‘nikmalarini berish muhim strategiyalardan biridir.

Yakuniy xulosa sifatida aytish mumkinki, axborot xavfsizligi bo‘yicha tizimli yondashuv — bu kelajakda sodir bo‘lishi mumkin bo‘lgan zararli oqibatlarning oldini

olishda eng asosiy kafolatdir. Barcha darajadagi tashkilotlar o‘z faoliyatlarini zamonaviy xavfsizlik tamoyillari asosida tashkil etib, doimiy monitoring va yangilanishga tayyor bo‘lishlari kerak. Faqat shu tarzda barqaror, ishonchli va xavfsiz axborot muhiti vujudga keladi.

Foydalanilgan adabiyotlar:

1. ISO/IEC. (2013*). Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC 27001:2013). International Organization for Standardization.

2. Kshetri, N. (2017). *1 The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns*. Big Data for Development, 1–25. https://doi.org/10.1007/978-3-319-44164-3_1

3. Laudon, K. C., & Laudon, J. P. (2021). *Management Information Systems: Managing the Digital Firm* (17th ed.). Pearson.

4. Mavlonova, R. (2020). *Axborot xavfsizligini ta'minlashning dolzarb masalalari*. Toshkent: TATU nashriyoti.

5. Rahimov, S. (2019). *Axborot texnologiyalari va axborot xavfsizligi asoslari.* Toshkent: Fan va texnologiya nashriyoti.

6. Stallings, W. (2018). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson Education.