6 –TOM 2 – SON / 2023 - YIL / 15 - FEVRAL

AXBOROT XAVFSIZLIGINI TA'MINLASHNING DOLZARB MASALALARI VA MUAMMOLARI

Axmedova Nigora Orifjonovna
O'zbekiston Respublikasi

Annotatsiya: *Axborot xavfsizligi jamiyatda axborotdan keng foydalanishda muhim ahamiyatga ega hisoblanadi. Ijtimoiy tarmoqlar, internet kabi tushunchlar bilan birga jamiyatga spam, feyk,kompyuter viruslari kabi juda jo'plab tushunchlar ham kirib kelmoqda. Albatta har bir narsanining old va orqa tarafi bor. Demak axborotdan foydalanish jarayonida ham uning qanchalik xavfli va xavfsiz ekanligiga ahamiyat berish muhim hisoblanadi. Hozirgi paytda juda ko'plab bunday misollarni keltirish mumkin. Shunday ekan axborotdan foydalanish madaniyatiga ham kata e'tibor berish kerak bo'ladi.*

Kalit so'zlar: *Axborot xavfsizligi, SMM, kiberjinoyat, konfidentsial xabarlar, axborot ximoyasi.*

Bugungi kunda jamiyatni axborotlashtirish muhim ahamiyatga ega bo'lmoqda.Axborotdan foydalanish qanchalik ko'p bo'lsa, uni himoyalash shunchalik muammoga aylanib boraveradi. Kiberjinoyatlardan saqlanish uchun axborotni muxofazalash muhim ahamiyat kasb etadi. Hozirda SMM dan foydalanish jarayonida ham axborot xavfsizligiga oid juda ko'plab muammolar kelib chiqmoqda.

Axborotning muximlik darajasi qadim zamonlardan ma'lum. Shuning uchun xam qadimda axborotni himoyalash uchun turli xil usullar qo'llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o'qiy olmagan. Asrlar davomida bu san'at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o'n yil oldin hamma narsa tubdan o'zgardi, ya'ni axborot o'z qiymatiga ega bo'ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o'g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug'iladi. Axborotni qayta ishlash sanoatining paydo bo'lishi axborotni himoyalash sanoatining paydo bo'lishiga olib keladi.

Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo'llanilmoqda (iqtisod, fan, ta'lim, xarbiy ish, turli texnologiyalarni boshqarish va x.k.).

Axborot xavfsizligi deb, ma'lumotlarni yo'qotish va o'zgartirishga yo'naltirilgan tabiiy yoki sun'iy xossali tasodifiy va qasddan ta'sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi..

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va xujjatlarni o'g'irlash yoki nusxa olishdan iborat bo'lsa, hozirgi paytdagi xavf esa kompyuter ma'lumotlari to'plami, elektron ma'lumotlar, elektron massivlardan ularning egasidan ruxsat so'ramasdan foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta'minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta'minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar yetkazmokchi bo'lgan nohuquqiy muomaladan xar qanday xujjatlashtirilgan, ya'ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo'yilgan xolda moddiy jismda qayd etilgan axborot ximoyalanishi kerak.

Axborotni ximoyalashning maqsadlari kuyidagilardan iborat:

- axborotning kelishuvsiz chikib ketishi, ugirlanishi, yo'qotilishi, o'zgartirilishi, soxtalashtirilishlarning oldini olish;

- shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf – xatarning oldini olish;

- axborotni yo'q qilish, o'zgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish;

- xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta'minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish;

- axborot tizimida mavjud bulgan shaxsiy ma'lumotlarning shaxsiy maxfiyligini va konfidentsialligini saklovchi fukarolarning konstitutsion xukuklarini ximoyalash;

- davlat sirini, konunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saklash;

- axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chikish va kullashda sub'ektlarning xukuklarini ta'minlash.

Internet tizimi orqali tarmoqlararo ma'lumot almashinuvini ta'minlash, butun dunyodagi bilimlar manbalariga kirish, qisqa vaqt ichida ko‘plab ma'lumotlar yig‘ish, ishlab chiqarishning va uning texnik vositalarini masofadan turib boshqarish mumkin. Shu bilan bir qatorda internetning ushbu imkoniyatlaridan foydalanib tarmoqdagi begona kompyuterlarni boshqarish ularning ma'lumotlar bazasiga kirish, nusxa ko‘chirish g‘arazli maqsadda turli xil viruslar tarqatish kabi noqonuniy ishlarni amalga oshirsh mumkin. Internetda mavjud bo‘lgan ushbu xavf, axborot xavfsizlik muammolari bevosita tarmoqlarning xususiyatlaridan kelib chiqadi. Ixtiyoriy tarmoq xizmatini o‘zaro kelishilgan qoida (protokol) asosida ishlovchi juftlik «Server» va

«Mijoz» dastur ta’minoti bajaradi. Ushbu protokollar miqyosida ham «Server», ham «Mijoz» dasturlari ruxsat etilgan amallarini (operatsiya) bajarish vositalariga ega. Ruxsat etilgan operatsiyalar, faol ob’ektlardan foydalanib internetda ba’zi bir noqonuniy harakatlarni amalga oshirish tarmoqdagi kompyuterlarga va ma’lumotlar ba’zasiga kirish hamda ularga tahdid solish mumkin bo‘ladi. Bu xavf va tahdid nimalardan iborat:

• Tarmoqdagi kompyuterlarga ruxsatsiz kirish va uni masofadan turib boshqarish. Ularga sizning manfaatingizga zid bo‘lgan dasturlarni joylashtirish mumkin.

• Web sahifalarida joylashtirilgan «faol ob’ektlar» agressiv dastur kodlari bo‘lib, siz uchun xavfli virus yoki josus dastur vazifasini o‘tashi mumkin.

• Internetda uzatilayotgan ma’lumotlar yo‘l yo‘lakay aloqa kanallari yoki tarmoq tugunlarida tutib olinishi ulardan nusxa ko‘chirilishi, almashtirilishi mumkin.

• Davlat muassasasi, korxona faoliyati, moliyaviy ahvoli va uning xodimlari haqidagi ma’lumotlarni razvedka qilinishi o‘g‘irlashi va shu orqali sizning shaxsiy hayotingizga, korxona rivojiga tahdid solishi mumkin.

• Internetda e’lon qilinayotgan har qanday ma’lumot ham jamiyat uchun foydali bo‘lmasligi mumkin, ya’ni internet orqali bizning ma’naviyatimizga, madaniyatimizga va e’tiqodimizga zid bo‘lgan informatsiyalarni kirib kelishi ehtimoli ham mavjud.

Internet foydalanuvchisi ushbu xavflarni oldini olish uchun quyidagi texnik yechim va tashkiliy ishlarni amalga oshirishi zarur:

• Shaxsiy kompyuterga va mahalliy kompyuter tarmog‘iga hamda unda mavjud bo‘lgan axborot resurslarga tashqaridan internet orqali kirishni cheklovchi va ushbu jarayonni nazorat qilish imkonini beruvchi texnik va dasturviy usullardan foydalanish.

• Tarmoqdagi axborot muloqot ishtirokchilari va ular kuzatayotgan ma’lumotlarni asl nusxasiga mosligini tekshirish.

• Ma’lumotlarni uzatish va qabul qilishda kriptografiya usullaridan foydalanish

• Viruslarga qarshi nazoratchi va davolovchi dasturlardan foydalanish.

• Shaxsiy kompyuter va mahalliy kompyuter tarmog‘iga begona shaxslarni qo‘ymaslik va ularda mavjud bo‘lgan ma’lumotlardan nusxa olish imkoniyatlarini cheklovchi tashkiliy ishlarni amalga oshirish.

Bundan tashqari axborot xavfsizlikni ta’minlash borasida internet foydalanuvchilari orasida o‘rnatilmagan tartib qoidalar mavjud. Ulardan ba’zi birlarini keltiramiz:

Hech qachon hech kimga internetdagi o‘z nomingiz va parolingizni aytmang.

Hech qachon hech kimga o‘zingiz va oila a’zolaringiz haqidagi shaxsiy hamda ishxonangizga oid ma’lumotlarni internet orqali yubormang.

Elektron manzilingiz (E-mail)dan maqsadli foydalaning. Internet orqali dasturlar almashmang.

♣ Internetda tarqatilayotgan duch kelgan dasturlardan foydalanmang. Dasturlarni faqat ishonchli egasi ma’lum bo‘lgan serverlardan ko‘chiring.

♣ Elektron pochta orqali yuborilgan «aktiv ob'ektlar» va dasturlarni ishlatmang, yoki qo'shimchali o'z-o'zidan ochiluvchi sizga noma'lum arxiv holidagi ma'lumotlarni ochmang.

♣ Elektron pochta xizmatidan foydalanayotganingizda ma'lumotlarni shifrlash zarur, ya'ni kriptografiya usullaridan foydalaning.

♣ Egasi siz uchun noma'lum bo'lgan xatlarni ochmang.

♣ Egasi ma'lum bo'lgan va uning sifatiga kafolat beruvchi antivirus dasturlardan foydalaning va ularni muntazam yangilab boring.

♣ Internetda mavjud bo'lgan axborot resurslar va dasturlardan ularning mualliflari ruxsatisiz foydalanmang.

♣ Tarmoqdagi begona kompyuter va serverlarning IP manzillarini aniqlash va shu orqali ruxsat etilmagan serverlar va axborot resurslarga kirish nusxa ko'chirish, viruslar tarqatish kabi noqonuniy dasturlashtirish ishlari bilan shug'ullanmang, bu jinoyatdir.

Internet bilan ishlaganda tizimning ixtiyoriy qismidan unga kirish imkoniyati mavjud bo'ladi. Shu sababli, axborot xavfsizligini ta'minlash uchun foydalanuvchilarni identifikatsiyalash, autentifikatsiyalash va autorizatsiyalash zarur bo'ladi.

Kompyuter tizimida ro'yxatga olingan har bir sub'ekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma'noda indentifikatsiyalovchi axborot bog'liq.

Bu ushbu sub'ektga nom beruvchi son yoki simvollar satri bo'lishi mumkin. Bu axborot sub'ekt indentifikatori deb yuritiladi. Agar foydalanuvchi tarmoqda ro'yxatga olingan indentifikatorga ega bo'lsa u legal (qonuniy), aks holda legal bo'lmagan (noqonuniy) foydalanuvchi hisoblanadi. Kompyuter resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o'tishi lozim.

Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo'lishi mumkin bo'lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo'lib tuyulmasa ham, Internetda ishlash tajribasi ko'rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga duchor bo'lar ekan. Xavfxatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog'i kompyuterlarining xujumlarga qarshi turishi yoki bo'lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko'rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan sasofadan foydalanish xollari alohida ko'rilishi lozim.

Xulosa qilib shuni aytish mumkinki, xar qanday axborotdan foydalanishda uning ishonchli va xavfsiz ekanligiga alohida e'tibor berish kerak. Axborot xavfsizligini ta'minlashda esa ishonchli shifrlash usllaridan foydalanish, turli viruslardan himoyalanganligiga ahamiyat berish kerak bo'ladi.

ADABIYOTLAR:

1. Turdiqulov A.M. – Axborot xavfsiligi. O'quv qo'llanma. Toshkent – 2015.
2. Kadirova, O. K. (2022). Use of the Neurolinguistic Programming Method to Achieve the Goals of the Educational Process. International Scientific Journal Theoretical & Applied Science, 10(12), 188-192.
3. Mirxalilova, N. A., & Davlatova, M. A. (2022). TIMSS xalqaro baholash dasturida miqdor tushunchasi va uning turlari. *Academic research in educational sciences*, *3*(9), 282-285.
4. Seitniyazov, K. M., Baltabayev, O. O. (2020). Methods for toponymical research of objects. Fan va jamiyat, 1(1), 28-29.
5. Turdimambetov, I. R., Seitniyazov, K. M., Baltabayev, O. O. (2020). Methods of toponymic researches of peoples geographical terms in the Republic of Karakalpakstan. Science and Education in Karakalpakstan, 1(2), 109-111.
6. Abdullaev PhD, A., & Ochilov, O. (2021). ACCOUNTING AND ANALYSIS OF INVESTMENTS UNDER ACTIVE INVESTMENT POLICY: NECESSITY, PURPOSE AND OBJECTIVES. *International Finance and Accounting*, *2021*(2), 29.
7.