INTERNET TARMOG‘IDA SAQLANAYOTGAN AXBOROTLAR RESURSLARI XAVFSIZLIGI TA’MINLASH USUL VA VOSITALARI

Bahromova Aziza Bahrom qizi
Koson tuman 1 son kasb hunar maktabi Informatika fani o‘qituvchisi

Annotatsiya: *Ushbu maqolada Internet tarmog‘ida saqlanayotgan axborotlar resurslari xavfsizligi ta’minlash usul va vositalari xususida so‘z yuritildi.*

Kalit so‘zlar: *axborot, internet, kriptotizim, shifrlash kaliti, kriptografiya, aloqa*

Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun ham 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.

Internet texnologiyalarining yaratilishi turli manbalardan tez va oson yo'l bilan axborot olish imkoniyatlarini hamma uchun-oddiy fuqarodan tortib yirik tashkilotlargacha misli ko'rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta'lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib-saqlay boshladilar. Bu muhit avvalgi fizikaviy saqlashga nisbatan katta qulayliklar tug'diradi: saqlash juda ixcham, uzatish esa bir onda yuz beradi va tarmoq orqali boy ma'lumotlar bazalariga murojaat qilish imkoniyatlari juda keng. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko'payishiga olib keldi. Biznes qator tijorat sohalarida bugun axborotni o'zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo'lgan axborot haqida gap borganda o'ta ijobiy hodisa. Lekin pinhona(konfidentsial) va maxfiy axborot oqimlari uchun Internet texnologiyalari qulayliklar bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi:

-Axborot o'g'irlash

-Axborot mazmunini buzib qo'yish, egasidan iznsiz o'zgartirib qo'yish

-Tarmoqqa va serverlarga o'g'rincha suqulib kirish

Bugungi kunda axborot xavfsizligini ta'minlashda an'anaviy qo'llanilib kelingan yondoshuvlar va vositalar yetarli bo'lmay qoldi. Bunday sharoitda axborot himoyasining eng ishonchli va sinalgan usuli bo'lgan kriptografiyaning ahamiyati yanada oshdi. Quyida Internet va Intranetda axborot himoyasining kriptologiya yo'nalishi haqida batafsil to'xtalamiz.

Kriptografik tizim, yo qisqacha, kriptotizim shifrlash ham shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shu kalitlarni boshqaruv tizimi hamda shifrlanadigan va shifrlangan matnlarning o'zaro bog'langan majmuasidir.

Kriptotizimdan foydalanishda matn egasi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o'giradi. Matn egasi uni o'zi foydalanishi uchun shifrlagan bo'lsa (bunda kalitlarni boshqaruv tizimiga hojat ham bo'lmaydi) saqlab qo'yadi va kerakli vaqtda shifrlangan matnni ochadi. Ochilgan matn asli (dastlabki matn)ga aynan bo'lsa saqlab qo'yilgan axborotning butunligiga ishonch hosil bo'ladi. Aks holda axborot butunligi buzilgan bo'lib chiqadi. Agar shifrlangan matn undan qonuniy foydalanuvchiga(oluvchiga) mo'ljallangan bo'lsa u tegishli manzilga jo'natiladi. So'ngra shifrlangan matn oluvchi tomonidan unga avvaldan ma'lum bo'lgan shifr ochish kaliti va algoritmi vositasida dastlabki matnga aylantiriladi.

Bunda kalitni qanday hosil qilish, aloqa qatnashchilariga bu kalitni maxfiyligi saqlangan holda yetkazish, va umuman, ishtirokchilar orasida kalit uzatilgunga qadar xavfsiz aloqa kanalini hosil qilish asosiy muammo bo'lib turadi. Bunda yana boshqa bir muammo – autentifikatsiya muammosi ham ko'ndalang bo'ladi. Chunki:

Dastlabki matn(xabar) shifrlash kalitiga ega bo'lgan kimsa tomonidan shifrlanadi. Bu kimsa kalitning haqiqiy egasi bo'lishi ham, begona (mabodo kriptotizimning siri ochilgan bo'lsa) bo'lishi ham mumkin.

Aloqa ishtirokchilari shifrlash kalitini olishganda u chindan ham shu kalitni yaratishga vakolatli kimsa tomonidan yo tajovuzkor tomonidan yuborilgan bo'lishi ham mumkin.

Bu muammolarni turli kriptotizimlar turlicha hal qilib beradi.

Kriptotizimda axborotni shifrlash va uning shifrini ochishda ishlatiladigan kalitlarning bir-biriga munosabatiga ko'ra ular bir kalitli va ikki kalitli tizimlarga farqlanadilar. Odatda barcha kriptotizimlarda shifrlash algoritmi shifr ochish algoritmi bilan aynan yo biroz farqli bo'ladi. Kriptotizimning ta'bir joiz bo'lsa "qulfning" bardoshliligi algoritm ma'lum bo'lgan holda faqat kalitning himoya xossalariga, asosan kalit axborot miqdori(bitlar soni)ning kattaligiga bog'liq deb qabul qilingan.

Shifrlash kaliti shifr ochish kaliti bilan aynan yo ulardan biri asosida ikkinchisi oson topilishi mumkin bo'lgan kriptotizimlar simmetrik(sinonimlari: maxfiy kalitli, bir kalitli) kriptotizim deb ataladi.

Bunday kriptotizimda kalit aloqaning ikkala tomoni uchun bir xil maxfiy va ikkovlaridan boshqa hech kimga oshkor bo'lmasligi shart.

Bunday tizimning xavfsizligi asosan yagona maxfiy kalitning himoya xossalariga bog'liq.

Simmetrik kriptotizimlar uzoq o'tmishga ega bo'lsa-da, ular asosida olingan algoritmlar kompyuterlardagi axborotlarni himoyalash zarurati tufayli ba'zi davlatlarda standart maqomiga ko'tarildilar. Masalan, AQSHda ma'lumotlarni shifrlash standarti sifatida 56 bitli kalit bilan ishlaydigan DES(Data Encryption Standart) algoritmi 1977 yilda qabul qilingan. Rossiya(sobiq SSSR)da unga o'xshash standart (GOST 28147-89) sifatida 128 bitli kalit bilan ishlaydigan algoritm 1989 yilda tasdiqlangan. Bular dastlabki axborotni 64 bitli bloklarga bo'lib alohida yoki bir-biriga bog'liq holda shifrlashga asoslanganlar. Algoritmlarning matematikaviy asosida axborot bitlarini aralashtirish, o'rniga qo'yish, o'rin almashtirish va modul bo'yicha qo'shish amallari yotadi. Unda kirish va chiqishdagi matnlarning axborot miqdorlari deyarli bir xil bo'ladi.

Xulosa o‘rnida shuni aytish kerakki, global tarmoqlarning rivojlanishi va axborotlarni olish, kayta ishlash va uzatishning yangi texnologiyalari paydo bo‘lishi bilan Internet tarmogiga har xil shaxs va tashkilotlarning e’tibori karatildi. Ko‘plab tashkilotlar o‘z lokal tarmoqlarini global tarmoqlarga ulashga karor qilishgan va hozirgi paytda WWW, FTP, Gophes va boshqa serverlardan foydalanishmoqda. Tijorat maqsadida ishlatiluvchi yoki davlat siri bo‘lgan axborotlarning global tarmoqlar bo‘yicha joylarga uzatish imkoni paydo buldi va uz navbatida, shu axborotlarni himoyalash tizimida malakali mutaxassislarga ehtiyoj tug‘ilmoqda.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. R.X. Alimov, B.YU. Xodiev, K.A. Alimov, S.U. Usmonov, B.A. Begalov, N.R. Zaynalov, A.A. Musaliev, F. Fayzieva, «Milliy iqtisodda axborot tizimlari va texnologiyalari», O‘quv qo‘llanma, T. Sharq, 2004 yil.
2. M.T. Gafurova, D.CH. Dursunov, V.I. Rapoport, B.YU. Xodiev. Proektirovanie sovremennых informatsionnых texnologiy. Uchebnoe posobie.-Toshkent, TDIU, 1994.-96 s.
3. Informatsionnые sistemы v ekonomike: Uchebnik/Pod red. prof. V.V. Dika.-M.:Finansы i statistika,1996.-272 s.
4. Informatika: Uchebnik/Pod red. N.V. Makarovoy. -M.: Finansы i statistika, 1997.-768s.
5. G‘ulomov S.S. va boshq. Iqtisodiy informatika: Oliy o‘quv yurtlarining iqtisodiy mutaxassisliklari uchun darslik.
6. G‘ulomov S.S., SHermuhammedov A.T., Begalov B.A.; S.S. G‘ulomovning umumiy tahriri ostida. —T.: «O‘zbekiston», 1999. —528 b.
7. Kozыrev A.A. Informatsionnые texnologii v ekonomike i upravlenii: Uchebnik, 2-e izd. .—SPb.: Izd-vo Mixaylova V.A., 2001. —360 s.

8. Xodiev B.YU., Musaliev A.A., Begalov B.A. Vvedenie v informatsionnыe sistemы i texnologii. Uchebnoe posobie /Pod red. akad. S.S. Gulyamova. —T.:TGEU, 2002. —156 s