ISSN 2181-3187

AXBOROTLARNI HIMOYALASHNING ASOSIY VOSITALARI

Andijon davlat pedagogika instituti "Aniq fanlar"
Fakulteti Matematika va informatika 3-kurs talabasi
Mahammadjonova Muattar Rustamjon qizi
Andijon davlat pedagogika instituti kata o'qituvchisi
Axmedov Shavkatbek Baltabayevich

Annotatsiya: Umumiy axborot kengligining yaratilishi va shaxsiy kompyuterlarning amaliy jihatdan keng qo'llanilishi va kompyuter tizimlari va tarmoqlarining tatbiq etilishi axborotni himoya qilish muammosini yechish zarurligini keltirib chiqaradi.

Kalit so`zlar: Tarmoq xavfsizligi, tarmoqda axborotni himoya qilish, axborotlarni himoyalashning asosiy vositalari, shifrlash haqida malumot.

Axborotni himoya qilish deganda zamonaviy kompyuter tizimlarida va tarmoqlarida uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotning ishonchliligini va butunligini tizimli ta'minlash maqsadida turli xil vositalarni va usullarni ishlatish, choralarni ko'rish va tadbirlarni o'tkazish tushuniladi. Global tarmoqlarning rivojlanishi va axborotlarni olish, qayta ishlash va uzatishning yangi texnologiyalari paydo bo'lishi bilan Internet tarmog'iga har xil shaxs va tashkilotlarning e'tibori qaratildi. Ko'plab tashkilotlar o'z lokal tarmoqlarini global tarmoqlarga ulashga qaror 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 bo'ldi va o'z navbatida, shu axborotlarni himoyalash tizimida malakali mutaxassislarga ehtiyoj tug'ilmoq. Global tarmoqlardan foydalanish bu faqatgina «qiziqarli» axborotlarni izlash emas, balki tijorat maqsadida va boshqa ahamiyatga molik ishlarni bajarishdan iborat.

Kirish. Bugungi kunda axborot texnologiyalari sohasi respublikamizning rivojlanishida muhim o'rin tutib kelmoqda. O'tgan yillar mobaynida O'zbekiston Respublikasi hukumati tomonidan axborot kommunikatsiya texnologiyalarini keng joriy qilish va rivojlantirish borasida olib borgan siyosati hozirgi kunga kelib o'z natijalarini ko'rsatmoqda. Har bir soha faoliyatida kompyuter texnologiyalari va internet tarmog'idan foydalanish ish unumdorligini oshirmoqda. Bizga ma'lumki hayotiy faoliyatimizda ahamiyatli ro'liga ega bo'lgan har qanday yo'nalish borki unga nisbatan tahdidlar, xato va kamchiliklar va albatta o'ziga xos yutuqlardan tashkil topadi. Sohalardagi AKTga talab ortib borgani sari uni himoyalashga, tahdidlarni oldini olishga bo'lgan talab keskin ortdi. Ushbu talablarni amalga oshirish uchun innovatsion usullarini

ISSN 2181-3187

izlab topish, axborotlashtirish jarayoniga har tomonlama ko‘maklashish, ularni hayotga keng joriy etish, xavfsizligini himoya qilishda apparat va dasturiy maxsulotlardan samarali foydalanish sohalar faoliyatining muhim yo‘nalishlaridan biriga aylanmoqda. Zero, axborotlashtirish tizimida davlat siyosatini olib borish masalasi strategik ahamiyatga ega vazifadir.

Axborotlarni himoyalashning asosiy vositalari

Hozirgi kunda axborot-kommunikatsiya tizimlariga bo‘ladigan taxdidlar, ruhsatsiz tizimga kirish holatlari turli xil yo‘llar bilan amalga oshirilishiga javoban xavfsizlikni ta‘minlash turli xil usullar va vositalar yordamida amalga oshirilmoqda.

Axborot xavfsizligi ta‘minlashning birinchi va eng asosiy vositasi bu – foydalanuvchilarni identifikatsiyalash va autentifikatsiyadan o‘tkazishdir.

Identifikatsiya – foydalanuvchining ro‘yxat yozuvi (login) ni kiritishi. Foydalanuvchining tizimdagi logini orqali u haqidagi barcha kerakli axborotlarga: uning shaxsi; tizimdagi ruhsat darajasi; tizimdagi faoliyati tarixi va boshqalar ega bo‘lish mumkin.

Autentifikatsiya – bu foydalanuvchining shaxsini tasdiqlashi. Odatda bu jarayon maxfiy so‘z (parol) orqali amalga oshiriladi. Ya‘ni foydalanuvchi dastlab tizimga o‘zining kalit so‘zini kiritadi va so‘ng shu kalit so‘z rostdan ham unga tegishli ekanligini maxfiy so‘z orqali tasdiqlaydi.

Identifikatsiya va autentitifikatsiya vositalari birlashishi ham mumkin. Bu yerda barchamiz uchun ma‘lum bo‘lgan xizmat guvohnomasini keltirish mumkin. Unda shaxsning identifikatsiyasi uchun ismi, familiyasi, mansabi (va boshqa ma‘lumotlar), autentifikatsiya uchun esa uning surati keltirilganligini aytishimiz mumkin. Shuni alohida ta‘kidlash kerakki autentifikatsiya va identifikatsiya vositalarining o‘zi haqiqiylikni tasdiqlovchi belgilarga ega bo‘lishi mumkin. Misol uchun guvohnomadagi muhr, imzo yoki uning himoyasini saqlovchi boshqa qalbakilashtirishdan himoyalovchi vositalar.

Agar foydalanuvchi bu jarayonlardan muvafaqqiyatli o‘tsa, u axborot tizimiga kirishiga va unga berilgan vakolat darajasida istalgancha foydalanish huquqiga ega bo‘ladi.

Hozirgi vaqtda axborot–hisoblash tizimlarida foydalanuvchilarni autentifikatsiya va identifikatsiyalashning usullarini quyidagi asosiy guruhlarga bo‘lish mumkin:

– foydalanuvchidan qandaydir maxsus axborotni so‘rash (masalan, login yoki parol);

– foydalanuvchidan qandaydir maxsus tavsiyaga yoki xususiyatga ega bo‘lgan ashyoni so‘rash (masalan, smart-karta, USB-token va boshqalar);

– autentifikatsiya qilinayotgan axborot foydalanuvchi tanasining muhim qismi (masalan, barmoq izlari yoki boshqa biometrik ma‘lumotlar).

ISSN 2181-3187

Shifrlash - bu avtorizatsiya qilingan foydalanuvchilarga unga kirish huquqini taqdim etishda ruxsatsiz shaxslardan yashirish uchun ma'lumotni qayta o‘zgartirish. Asosan, shifrlash uzatilayotgan ma'lumotlarning maxfiyligini ta'minlashga xizmat qiladi. Har qanday shifrlash algoritmining muhim xususiyati bu algoritm uchun mumkin bo'lgan to‘plamdan ma'lum bir transformatsiyani tanlashni tasdiqlaydigan kalitdan foydalanish hisoblanadi. Agar foydalanuvchilarda haqiqiy kalit bo‘lsa, ular avtorizatsiya qilinadi. Butun murakkablik va aslida shifrlash vazifasi bu jarayon qanday amalga oshirilganligidadir. Umuman olganda, shifrlash ikkita tarkibiy qismdan iborat - shifrlash va parolni ochish. Shifrlash axborot xavfsizligining uchta holatini ta'minlaydi. Maxfiylik Shifrlash ma'lumot uzatish yoki saqlash paytida ruxsatsiz foydalanuvchilardan ma'lumotlarni yashirish uchun ishlatiladi. Butunlik Shifrlash ma'lumot uzatish yoki saqlash paytida o‘zgartirilishining oldini olish uchun ishlatiladi. Aniqlik shifrlash ma'lumot manbaini autentifikatsiya qilish va ma'lumotni yuboruvchiga unga ma'lumot yuborilganligini rad qilishining oldini olish uchun ishlatiladi. Shifrlangan ma'lumotni o‘qish uchun qabul qiluvchi tomonga kalit va dekolifator kerak (shifrlash algoritmini amalga oshiradigan qurilma). Shifrlash g'oyasi shundan iboratki, buzg'unchi shifrlangan ma'lumotlarni ushlagan va ular uchun kalitga ega bo'lmagan holda uzatilgan ma'lumotni o‘qiy olmaydi va o‘zgartira olmaydi. Bundan tashqari, zamonaviy kriptotizimlarda (ochiq kalit bilan) ma'lumotlarni shifrlash, shifrlash uchun turli xil kalitlardan foydalanish mumkin. Biroq, kriptovalyutaning rivojlanishi bilan siz yopiq 6 matnni kalitsiz shifrlash imkonini beradigan texnikalar paydo bo'ldi. Ular uzatilgan ma'lumotlarning matematik tahliliga asoslangan. Shifrlash dasturlari fayllar xavfsizligini ta’minlashda yoki qattiq disklarda shifrlangan ma’lumotlar xajmini yaratishda ishlatiladi. Bu ma’lumotlarni rasshifrovka qilish uchun, odatda, parolni kiritish yoki shaxsiy kalitlarni ishlatish talab etiladi. Barcha axborotlarni shifrlangan fayllarda yoki arxivlarda saqlanishi kerakli fayllar to‘plamini arxiv uchun nusxalashni yengillashtiradi, chunki ular endi ma’lum joyda joylashgan bo‘ladi. Shifrlashning standart usullari (Milliy yoki xalqaro) shifrlarni yechishga mustaxkamlik darajasini oshirish uchun shifrlashni bir nechta etaplar (qadamlar) amalga oshiradi, bularning har birida tanlangan kalitga (yoki kalitlarga) qarab shifrlashni turli klassik usullari ishlatiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Vishnevskiy V.M. – Kompyuter tarmoqlarini qurishning nazariy asoslari – M.: “ Texnosfera ”, 2020. – 512 b .
2. Olifer V.G., Olifer N.A. – Kompyuter tarmoqlari – Sankt-Peterburg : “ Pyotr”, 2018 yil – 944 b.
3. Shangin V.F. – Kompyuter tizimlari va tarmoqlarida axborotni himoya qilish – M.: “DMK Press”, 2020. – 593 b .

ISSN 2181-3187

4. Tanenbaum E. Kompyuter tarmoqlari. 5-nashr. - Sankt-Peterburg: "Peter", 2019. – 960 b .
5. Tonievich A. – Kompyuter tarmoqlari – M.: “ Aserfan ”, 2018. – 235 b .
6. Stallings V. Kompyuter tarmoqlari, protokollari va internet texnologiyalari - SP b.: "BHV-Peterburg", 2020. - 832 b.

Internet resuslar:

1.https://e-library.namdu.uz
2.http://tatumarkaz.uz
3.https://uz.m.wikipedia.org
4.https://www.ziyouz.com
5.https://allbest.ru
6.https://infourok.ru