ELEKTRON HUKUMAT TIZIMIDA ELEKTRON RAQAMLI IMZOLARDAN FOYDALANISHNING ASOSIY AFZALLIKLARI TAHLILI

Seytniyazov Davronbek Bayramovich, *tayanch doktorant*
Atamuratova Shaxsanem Turdimuratovna, *talaba*
Dauletmuratova Juldiz Ayapbergenovna, *talaba*
Jumaniyazova Ulbosin Polatbay qizi, *talaba*

Axborotni avtomatlashgan ravishda qayta ishlash va boshqarishda kompyuter tizimlaridan kengdan foydalanish ushbu tarmoqlardagi mavjud ma’lumotlarga ruxsatsiz kirish muammosini keltirib chiqardi. Ma’lumki ma’lumotlar faqat toshuvchilar bilan bevosita bog’lanib qolmasdan, aloqa kanallari yordamida osongina ko’chirilishi va uzatilishi mumkin. Hozirgi vaqtga kelib bunday aloqa kanallari yordamida ma’lumotlarga tashqaridan va ichkaridan qo’poruvchilar tomonidan oshirilayotgan taxdidlar soni oshmoqda.

Elektron ma’lumotlarni himoya qilishning radikal usullaridan biri kriptografik usullar yordamida amalga oshirilishi mumkin. Kriptografik usullar ma’lumotlarni avtomatlashgan ravishda qayta ishlash va uzatish tizimlarini himoya qilish masalalarini ijobiy hal qilishi mumkin. Shu bilan birga kriptografik turlantirishning hozirgi zamon tezkor usullari astomatlashgan tizimning unimdorligini saqlab qolishga imkon beradi. Ma’lumotlarning maxfiyligi, butunligi va haqiqiyligini ta’minlashda kriptografik turlantirishlarning o’rni katta. Bunday turlantirishlarni zarur texnik vositalar bilan birgalikda qo’llashgina tizimni ko’plagan taxdidlardan asrashga yordam beradi. Bazi hollarda, masalan vaziyat taqozasi bilan ayrim shahslar kelishilgan shartlardan voz kechishi mumkin. Shu sababli bunday vaziyatlarning oldini oladigan qandayda bir mexanizmning mavjud bo’lishi zarurdir.

Yuqoridagi vaziyatda tomonlar bir biriga ishonmaydi deb fazaz qilinadi. Demak bunday hollarda ushbu muamoni yechishda mahfiy kalttan foydalanish foydasiz. Jo’natuvchi ma’lumotni jo’natganini rad etib, bu ma’luotni qabul qiluvchining o’zi yaratgan degan fikrni ilgari surishi mumkin (mualliflikdan voz kechish). Qabul qiluvchi esa o’z navbatida olingan ma’lumotlarga o’zgarttirishlar kiritishi yoki umuman yangi ma’lumotni kiritib, ushbu ma’lumotni jo’natuvchi jo’natdi deb turub olishi mumkin (mualliflikni o’zlashtirish).

Tabiiyki bunday hollarda hakam bu baxsli muammoni yechish imkoniyatiga ega bo’lmaydi.

Bunday muammoni yechishning asosiy mexanizmi – raqamli imzodir.

Raqamli algoritm sxemasi o’zida ikkita algoritmni mujassam qilgan, birinchisi – hisoblash uchun, ikinchisi – imzoni tekshirish uchun. Imzoni hisoblash faqat imzo muallifi tomonidan bajarilishi mumkin. Imzoning to’g’riligini tekshirish maqsadida tekshirish algoritmiga umumiy foydalanish (dostup) imkoniyati mavjud bo’lishi kerak.

Raqamli imzo sxemasini yaratish uchun simmetrik shifrotizimlar foydalanlishi mumkin. Bunday hollarda imzo vazifasini mahfiy kaltta shifrlangan ma’lumot bajarish mumkin. Lekin bunday imzolarning asosiy kamchiligi – bunday imzolardan faqat bir marta foydalanish hisoblanadi, chunki har bir tekshirish sung mhfiy kalt mahfiylik xusussiyatini yo’qotadi. Simmetrik shifrlarni foydalanish doirasidagi ushbu holdan chiqishnig yagona usuli - ikki tomon ham ishonch bildiradigan va o’lar orasida vositachi vazifasini bajaradigan uchinchi

tomonni kiritish hisoblanadi. Bunday hollarda barcha ma’lumotlar vositachi orqali jo’natiladi va u ma’lumotlarni abonentlarning birisining kaltidan ikkinchisining kaltiga shifrlaydi. Tabiiyki, bunday sxemadan foydalanish noqo’layliklarni to’g’diradi.

Ochiq kaltili shifrotizimlarni foydalanishda raqamli imzo tizimini tashkil qilishning asosiy ikki tamoyili quyidagilardan iborat:

1. Ma’lumotni qandayda bir shaklga turlantirib, ushbu shakl asosida ma’lumotni tiklash. va shuning bilan «imzoning» to’g’riligini tekshirish. Bunday hollarda imzolangan ma’lumotning uzunligi berilgan ma’lumot uzunligiga teng bo’ladi. «Imzolongan ma’lumotni» tuzish uchun berilgan ma’lumotni imzo muallifining mahfiy kaltida bajarish mumkin. Shunda har kim ma’lumotning to’g’riligini imzo muallifning ochiq kaltida shifrdan ochish yordamida tekshirisha oladi;

2. Imzo berilgan ma’lumot bilan jo’natiladi va tekshiriladi. Imzoni hisoblash ma’lumotni raqamlarning bazi kombinatsiyasiga (bu imzo bo’ladi) turlantirishdan iborat. Imzoni hisoblashning algoritmi foydalanuvchining mahfiy kaltiga bog’liq bo’lishi kerak. Bunga sabab, imzodan faqat kalt egasi foydalana olishdir. O’z navbatida imzo to’g’riligini tekshirishning algoritmidan hamma foydalan olishi kerak. SHuning uchun ushbu algoritm foydalanuvchining ochiq kaltiga bog’liq bo’ladi. Mazkur holda imzo uzunligi imzolanayotgan ma’lumotning uzunligiga bog’liq bo’lmaydi.

Raqamli imzo muammosidan kaltsiz kriptografik hesh funktsiyalarni qurish muammosi kelib chiqdi. Gap shundaki, raqamli imzoni hisoblashda avval xesh funktsiyani amalga oshirish, ya’ni berilgan matnni tayinlanagn uzunliudagi kanday bir kombinatsiyaga o’tkazib, so’ng olingan kombinatsiyani mahfiy kalt yordamida imzolash qo’lay ekan. SHu bilan birga xesh funktsiya ochik va kaltga bog’liq bo’lmagani bilan u «kriptografik» bo’lishi kerak. Bu bilan biz ushbu funktsyaining bir tomonlilik xusussiyatini nazarda tutamiz: to’rlantrilgan (svertka) – kombinatsiya qiymati bo’yicha hech kim mos ma’lumotni ola olmasligi kerak.

Hozirgi vaktda kriptografik xesh funktsiyalar uchun standdartlar mavjud bo’lib, ular kriptografik algoritmlar va raqamli imzo sxemasi standartlaridan mustaqil ravishda tastiqlanadi.

Autentifikatsiya jarayoni ma’lumot almashayotgan ikki shaxsni uchinchi shaxsning ta’siridan himoya qiladi. Lekin oddiy autentifikatsiya ma’lumot almashayotgan ikki shaxsni himoya qila olmaydi va natijada ularning orasida kelishmovchilikning ma’lum bir ko’rinishi vujudga keladi. Masalan faraz qilaylik Anvar, Sarvarga autentifikatsiyalangan ma’lumot jo’natib va autentifikatsiya ularning umumiy kelishilgan mahfiy kombinatsiyasi yordamida amalga oshsin. Bu jarayon natijasida hosil bo’ladigan kelishmovchiliklarni ko’rib o’taylik:

• Sarvar ma’lumotni qalbakilashtirib, bu ma’lumot Anvardan keldi deb aytishi mumkin. Buning uchun Sarvar ma’lumotni tuzib va Anvar bilan foydalanayotgan kalit yordamida autentifikatsiya kodini qo’shib qo’yishi mumkin. Anvar bu ma’lumotni Sarvarga jo’natmaganligini rad etish mumkin, lekin buni isbotlash imkoniyati yo’q.

Ikki tomon bir – biriga ishomagan hollarida umuiy mahfiylikka asoslangan autentifikatsiyadan tashqari Yana mir mexanizm zarur bo’ladi. Bunday muammoni yechish raqamli imzo asosida amalga oshirilishi mumkin. Raqamli imzo quyidagi xossalarga ega:

1. Imzo muallifini, imzo yaratilga sana va vaqtni aniqlay olishi;

2. Imzoni yaratish vaqtida ma’lumot tarkibini autentifikatsiyalash;

3. Kelishmovchiliklarni hal qilish uchun imzo uchinchi tomonning imzoni tekshira olishi.

Shunday qilib raqamli imzo autentifikatsiya qilish funktsiyasini o’zida mujassam qiladi.

Yuqoridagi xusussiyatlar asosida raqamli imzo uchun quyidagi talablarni qo’yish mumkin:

1. Imzo imzolanayotgan ma’lumotga bog’liq bitli na’muna bo’lishi kerak.

2. Imzo rad etilmasligi va qalbakilashtirilmasligi uchun jo’natuvchining bazi bir unikal axborotlaridan foydalanishi kerak.

3. Raqamli imzoni yaratish yetarlicha yengil bo’lishi kerak.

4. Raqamli imzoni qalbakilashtirish mumkin bo’lmasligi kerak.

5. Raqamli imzo yetarlicha kompakt bo’lib, hotirada ko’p joyni egallamasligi lozim.

Xulosa qilib aytadigan bo’lsak elektron raqamli imzo elektron hukumat tizimining ajralmas elementidan biri bo’lib hisoblanadi va u axborotlarni himoyalashda muhim ahamiyat kasb etadi. ERI yordamida axborotlarni himoyalashda asosiy usul bu ochiq va yopiq kalitlar asosida shifrlashdan foydalanishni nazarda tutadi. Shuning uchun ham ushbu himoya turi ishonchli bo’lib hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1. Atadjanov D.Yu. va boshqalar. Elektron hukumat bo’yicha eslatma: O’zbekiston Respublikasida elektron hukumatni rivojlantirish bo’yicha davlat organlarining asosiy vazifalari. Toshkent. 2016. 32 b.

2. Zaynidinov H., Yakubov M., Qoraboev J. Elektron hukumat // To’ldirilgan 2-nashr. O’zR Prezidenta xuzuridagi Davlat boshkaruvi akademiyasi, T.: Akademiya. 2014. 273 b.

3. Барбаков Г.О., Устинова О.В. К проблеме внедрения «Электронного правителства» Вестник Челябинского государственного университета №26(381), 2015. S.109-113.

4. Бестолкова Г.В. Государственные электронные услуги: виды и особенности. Государственноэ управление. Электронный вестник. №65. 2017. С.23-44.