19-mavzu. Identifikatsiya va autentifikatsiya

Kompyuter tizimida ro‘yxatga olingan har bir subyekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni birma’noda indentifikatsiyalovchi axborot bog‘liq.

Bu ushbu subyektga nom beruvchi son yoki simvollar satri bo‘1ishi mumkin. Bu axborot subyekt *indentifikatori* deb yuritiladi. Agar foydalanuvchi tarmoqda ro‘yxatga olingan indentifikatorga ega bo‘lsa, u legal (qonuniy), aks holda, legal bo‘lmagan (noqonu- niy) foydalanuvchi hisoblanadi. Kompyuter resurslaridan foydala- nishdan awal foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o‘tishi lozim.

Identifikatsiya (Identification) — foydalanuvchini uning identi- fikatori (nomi) bo‘yicha aniqlash jarayoni. Bu foydalanuvchi tar- moqdan foydalanishga uringanida birinchi galda bajariladigan funk- siyadir. Foydalanuvchi tizimga uning so‘rovi bo‘yicha o‘zining identifikatorini bildiradi, tizim esa o‘zining ma’lumot1ar bazasida uning borligini tekshiradi.

Autentifikatsiya (Authentication) — ma’1um qilingan foydala- nuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqi-qatan aynan o‘zi ekanligiga ishonch hosil qilishiga imkon beradi. Autentifikatsiya o‘tqazishda tekshiruvchi taraf tekshiriluvchi tarafning haqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qat- nashadi. Odatda foydalanuvchi tizimga o‘z xususidagi noyob, bosh- qalarga ma’1um bo‘lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya va autentifikatsiya subyektlarning (foydalanuv- chilarning) haqiqiy ekanligini aniqlash va tekshirishning o‘zaro bog‘1angan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga

bog‘liq. Subyektni identifikatsiyalash va autentifikatsiyalashdan so‘ng uni avtorizatsiyalash boshlanadi.

Avtorizatsiya (Authorization) — subektga tizimda ma’lum va- kolat va resurslami berish muolajasi, ya’ni avtorizatsiya subyekt ha- rakati doirasini va u foydalanadigan resurslami belgilaydi. Agar ti- zim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli olmasa, bu tizimda axborotning konfidensialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma murlash muolajasi uzviy bog‘langan.

ajrata

Ma’murlash (Accounting) — foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishi- ni qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtayi nazaridan tarmoqdagi xavfsizlik hodisalarini oshkor qilish, tahlillash va ularga mos reaksiya ko‘rsatish uchun juda muhimdir.

Ma’1umot1arni uzatish kanallarini himoyalashda *subyektlar- ning o’zaro autentifikatsiyasi,* ya’ni aloqa kanallari orqali bog‘1ana- digan subyektlar haqiqiyligining o‘zaro tasdig‘i bajarilishi shart. Haqiqiylikning tasdig‘i odatda seans boshida, abonentlarning bir- biriga ulanish jarayonida amalga oshiriladi. “Ulash” atamasi orqali tarmoqning ikkita subyekti o‘rtasida mantiqiy bog‘1anish tushu- niladi. Ushbu muolajaning maqsadi — ulash qonuniy subyekt bilan amalga oshirilganligiga va barcha axborot mo‘ljallangan manzilga borishligiga ishonchni ta’minlashdir.

O‘zining haqiqiyligini tasdiqlash uchun subyekt tizimga turli axborotni taqdim etadi. Bunday axborot turi “Autentifikatsiya fak- tori” deb yuritiladi. Autentifikatsiyalashning quyidagi uchta faktori farqlanadi:

- *biror narsani bilish asosida.* Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda “so‘rov javob” xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlami ko‘rsatish mumkin;
- *biror narsaga egaligi asosida.* Odätda bular magnit kartalar, smart-kartalar, sertifikatlar va touch memory qurilmalari;
- *qandaydir daxlsiz xarakteristikalar asosida.* Ushbu faktor o‘z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko‘zining rangdor pardasi va to‘r pardasi, barmoq izlari,
kaft geometriyasi va h.) asoslangan usullari oladi. Bu faktorda kriptografik usullar va vositalar ishlatilmaydi. Beometrik xarakte- ristikalar binodan yoki qandaydir texnikadan foydalanishni nazorat- lashda ishlatiladi.

Subyektning haqiqiyligini tasdiqlash autentifikatsiyaning uchta faktoridan biri yordamida amalga oshirilishi mumkin. Masalan, foy- dalanuvchini autentifikatsiyalash jarayonida undan parol yoki bar- moq izlari so‘ra1ishi mumkin. Autentifikatsiya jarayonida faqat bitta faktor ishlatilsa, bunday autentifikatsiya *bir faktorli* deb yuritiladi.

Autentifikatsiya jarayonida bir necha faktor ishlatilsa, bunday autentifikatsiya *ko p faktorli* deb yuritiladi. Masalan, autentifikat- siya jarayonida foydalanuvchi smart-kartadan va qo‘shimcha parol-dan (yoki PIN-koddan) foydalanishi lozim. Ikki faktorli va uch faktorli autentifikatsiya tushunchalari ham ishlatiladi.

NCSC-TG-017 hujjatda ko‘p faktorli autentifikatsiya turlari uchun 1,2 xilli, 2,3 xilli va 1,2,3 xilli autentifikatsiya atamalari ki- ritilgan. 1,2 xilli autentifikatsiya *{bir ikki xilli autentifikatsiya* deb yuritiladi), lTlaSalan, autentifikatsiyaning ikki faktorini ishlatadi: bi- rinchi (bir narsani bilish asosida) va ikkinchi (bir narsaga egaligi asosida).

1,2,3 xilli autentifikatsiya *(bir ikki uch xilli autentifikatsiya* deb yuritiladi), autentifikatsiyaning uchta faktorining kombinasiyasini ishlatadi (bir narsa bilish asosida, bir narsaga egaligi asosida va qandaydir daxlsiz xarakteristikalar asosida).

Agar autentifikatsiyalashda bir omilli autentifikatsiya ishlatilsa bunday autentifikatsiya zaif hisoblanadi. Shu sababli, xavfsizlikning yuqori darajasini ta’min1ash uchun ko‘p faktorli autentifikatsiyadan foydalanish maqsadga muvofiq hisoblanadi.

Bankomatdan foydalanuvchini haqiqiyligini tasdiqlashda ikki faktorli autentifikatsiya keng tarqalgan. Bu bir vaqtda magnit hoshiyali karta va PIN-kod ishlatiladi.

Parol — foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan narsa. O‘zaro autentifikatsiya uchun foydalanuvchi va uning sherigi o‘rtasida parol almashinishi mumkin. Plastik karta va smart-karta egasini autentifikatsiyasida shaxsiy identifikatsiya nomeri PIN sinalgan usul hisoblanadi. PIN — kodning maxfiy qiymati faqat karla egasiga ma’lum bo‘lishi shart.