

## IDENTIFIKATSIYA, AUTENTIFIKATSIYA VA AVTORIZATSIYA JARAYONLARINING TAHLILI

**Kalmuratova Sapura Mirzamuratovna**

Qoraqalpoq davlat universiteti

E-mail: [kalmuratova.sapura@mail.ru](mailto:kalmuratova.sapura@mail.ru)

### ANNOTATSIYA

Ushbu maqolada identifikatsiya, autentifikatsiya va avtorizatsiya jarayonlarining bir-biridan farqi va ularning ishlash jarayonlari keltirilgan.

**Kalit sózlar:** Identifikatsiya, autentifikatsiya, avtorizatsiya, tizim, parol, PIN-kod, smart karta, barmoq izi, kaft taftologiyasi.

### ANALYSIS OF IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION PROCESSES

#### ABSTRACT

This article presents the difference between identification, authentication and authorization processes and how they work.

**Keywords:** Identification, authentication, authorization, system, password, PIN code, smart card, fingerprint, palm taftology.

Kirish nazorati va boshqaruvi haqida gap ketganda, autentifikatsiya, avtorizatsiya va identifikatsiya atamaları deyarli darhol paydo bo‘ladi.

Dunyo tobora onlayn harakatlanar ekan, foydalanuvchilar doimo identifikatsiya qilinmoqda, autentifikatsiya qilinmoqda va avtorizatsiya qilinmoqda. Bu atamalar ko‘pincha bir-birining o‘rnida ishlatiladi. Ammo, ular bir xil emas va muayyan vazifalarga erishish uchun boshqacha ishlaydi.

Identifikatsiya - sub'ektning o'z shaxsiga oid da'vosi. Bunga foydalanuvchi identifikatori, jarayon identifikatori, smart-karta va boshqalar orqali erishish mumkin. Tizimdagi turli sub'ektlarni farqlash uchun tasdiqlangan hisobga olish ma'lumotlari noyob bo'lishi juda muhimdir. Identifikatsiya ko'pgina onlayn tranzaksiyalarda birinchi qadam bo'lib, foydalanuvchi odatda ism, elektron pochta manzili, telefon raqami yoki foydalanuvchi nomini ko'rsatish orqali o'zini "identifikatsiyalash" ni talab qiladi. Bu kimdir o'zini ma'lum bir shaxs deb aytish jarayonidir. [1,106]

Onlayn muhitda esa, shaxsning haqiqiy shaxsini ko'rsatayotganini va u o'zi aytganidek ekanligini tekshirish qiyin bo'lishi mumkin.

Shaxslarni ko'proq ma'lumot, ko'pincha davlat tomonidan berilgan identifikatsiya shaklini taqdim etish orqali tekshirish mumkin. Tasdiqlash jarayoni odatda birinchi marta hisob yaratganingizda yoki saytga kirganingizda sodir bo'ladi. Shundan so'ng, sizning shaxsingiz autentifikatsiya qilinadi, ko'pincha foydalanuvchi nomingiz bilan birga parol yaratish orqali. [3]

Tizimga, xizmatga yoki kompaniyaga dastlab ro'yxatdan o'tishda, unga kirishda yoki ishga kirishda — shaxsingizni tasdiqlaganingizdan so'ng — autentifikatsiya shakli o'rnatiladi.

Autentifikatsiya bu foydalanuvchi identifikatorining isboti bo'lib, u odatda parol kiritish orqali boshqariladi. Mavzu o'zini identifikatsiya qilgandan so'ng, u autentifikatsiya qilinishi kerak, ya'ni sub'ekt o'zini kim deb da'vo qilayotganini isbotlashi kerak. Ushbu shaxsni tasdiqlash kirishni boshqarish mexanizmiga hisob ma'lumotlarini taqdim etish orqali erishiladi. Keyinchalik kirishni boshqarish mexanizmlari autentifikatsiya so'rovini tasdiqlashdan oldin taqdim etilgan hisob ma'lumotlarining haqiqiylikini tekshiradi. Boshqacha qilib aytganda, autentifikatsiya sub'ekt taqdim etilgan hisobga olish ma'lumotlariga (autentifikatorlarga) ega ekanligini va nazorat qilishini ishonch darajasini belgilaydi. Shaxsni tasdiqlash uchun ishlatilishi mumkin bo'lgan hisob ma'lumotlariga misol sifatida parollar, PIN-kodlar, raqamli imzolar, biometrik ma'lumotlar va boshqalarni keltirish mumkin. [4]

Faqatgina foydalanuvchi to‘g‘ri identifikatsiya qilingan va autentifikatsiya qilinganidan so‘ng unga tizimlar yoki imtiyozlarga ruxsat berilishi mumkin.

Autentifikatsiya qilish uchun foydalaniladigan hisob ma‘lumotlarini to‘rt xil guruhga bo‘lish mumkin, ular autentifikatsiya usullari ya‘ni turlari deb ham ataladi.

Qisqasi, ular:

- Parol, shaxsiy identifikatsiya raqami (PIN).
- Smart-karta, xotira kartasi yoki token.
- Barmoq izi, kaft topologiyasi, qo‘l geometriyasi, ko‘z to‘r pardasini skanerlash yoki fazani aniqlash.
- Siz qiladigan biror narsa (xulq-atvor biometrikasi), masalan, yozish namunasi (klavishlarni bosish dinamikasi), imzo namunasi (imzo dinamikasi) yoki ovoz namunasi.

Agar autentifikatsiya tizimi turli autentifikatsiya toifalarida bo‘lgan kamida ikkita hisob ma‘lumotlarini talab qilsa, bu ko‘p faktorli autentifikatsiya deyiladi. Masalan, autentifikatsiya qilish uchun paroldan ham, barmoq izingizdan ham foydalanish ko‘p faktorli autentifikatsiya hisoblanadi.

Avtorizatsiya - bu foydalanuvchiga xizmatlar yoki tizimga kirish huquqini berish - allaqachon taqdim etilgan identifikatsiya va autentifikatsiyaga asoslangan huquq va imtiyozlarga ruxsat berish. Identifikatsiya va autentifikatsiya o‘ziga xos maqsadlarga ega va ma‘lumotlar xavfsizligining zarur komponentlari hisoblanadi. Mavzu autentifikatsiya qilingandan so‘ng, autentifikatsiya mexanizmi ob‘ektga kirishni istagan sub‘ekt kimligini biladi. Keyin avtorizatsiya sub‘ektning ob‘ektga kirish darajasini belgilaydi. Boshqacha qilib aytganda, avtorizatsiya sub‘ektning imtiyozlari nima ekanligini va sub‘ektning ob‘ekt bilan qanday munosabatda bo‘lishini belgilaydi. [2,142]

Avtorizatsiya jihati shaxsning o‘zi da‘vo qilgan shaxs ekanligini ta‘minlashga yordam beradi va ular muayyan xizmatlarga kirish huquqiga ega va muayyan imtiyozlarga ega. Avtorizatsiya samarali bo‘lishi uchun identifikatsiya va autentifikatsiyadan keyin kelishi kerak.

Identifikatsiya, autentifikatsiya va avtorizatsiyadan qanday foydalaniladi?

Misol sifatida quyidagilarni o‘z ichiga oladi:

1. Foydalanuvchi identifikatsiya ma’lumotlarini taqdim etish orqali tizimga kiradi.
2. Foydalanuvchi kelajakda kirish uchun parol kabi autentifikatsiya faktorini o‘rnatadi.
3. Foydalanuvchi loginga qaytadi va tizim identifikatsiya (foydalanuvchi nomi) va autentifikatsiya faktorini (parol) so‘raydi.
4. Tizim ma’lumotlarning to‘g‘riligini va saqlangan narsaga mos kelishini tekshirish orqali foydalanuvchini autentifikatsiya qiladi.
5. Foydalanuvchiga administrator ruxsat bergan tizim va resurslarga kirish huquqi beriladi. [3]

Xulosa qilib aytganda, identifikatsiya, autentifikatsiya va avtorizatsiya nima ekanligini umumlashtiradigan bo‘lsak: Identifikatsiya sub’ekt o‘z shaxsini da’vo qilganda sodir bo‘ladi va autentifikatsiya bu sub’ekt hisob ma’lumotlarini taqdim etganda sodir bo‘ladi. Subyektga ruxsat berilgandan so‘ng, ushbu sub’ektning kirish darajalari va imtiyozlari avtorizatsiya mexanizmi orqali boshqariladi.

#### **FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)**

1. S.G‘aniev, M.Karimov, K.Toshev: Axborot xavfsizligi (Axborot-kommunikatsion tizimlar xavfsizligi). Toshkent, «ALOQACHI»-2008. 362 bet.
2. В.Ф.Шаньгин: Информационная безопасность компьютерных систем и сетей. Москва, ИД «ФОРУМ»-ИНФРА-М 2011. 416 ст.
3. <https://imageware.io/identification-authentication-authorization-difference/>
4. <https://cybersophia.net/articles/what-is/what-is-iaa/>