

## IDENTIFIKATSIYA VA AUTENTIFIKATSIYANING ASOSIY TUSHUNCHA VA TAMOYILLARI

Jumaboyev Javlonbek Sherqul o'g'li  
Po'latov Doston Normurod o'g'li  
Roziqov Abdug'ani Ilhomjon o'g'li  
Hasanov Murodillo Azim o'g'li

**Annotatsiya:** *Identifikatsiya va autentifikatsiya, ma'lumot tizimlarida shaxslar va obyektlar haqida ma'lumotlarni aniqlash, tasdiqlash va ularga kirishni tartibga solishning muhim aspektlarini ta'minlash uchun ishlatiladigan tamoyillardir.*

*Identifikatsiya ma'lumot tizimida shaxs yoki obyekt haqida unikal identifikator (ID) berish jarayonidir. Identifikatorlar, shaxsning yagona va tanish bilan ajralib turuvchi ma'lumotlarni ta'riflash uchun ishlatiladi. Masalan, foydalanuvchilar uchun foydalanuvchi nomi (username), e-pochta manzili yoki raqamli ID identifikator sifatida ishlatilishi mumkin.*

*Autentifikatsiya esa ma'lumot tizimiga kirish uchun shaxs yoki obyektning to'g'ri va aniq tasdiqlash jarayonidir. Bu jarayon orqali ma'lumot tizimi shaxsning kimlik tasdiqlashini amalga oshiradi. Autentifikatsiya usullari shaxsning identifikatorini (username, ID) bilan birgalikda maxfiylik kalitlarini (parol, asosiy kalit, biometrik ma'lumotlar) ishlatish bilan amalga oshiriladi. Bunday usullar orqali foydalanuvchi, tizimga kirishda o'zi haqida tasdiqlash ma'lumotlarini kiritadi va tizim uni tasdiqlab kirishga imkon beradi.*

*Identifikatsiya va autentifikatsiya ma'lumotlarni himoya qilish va tizimga kirishning maxfiy va xavfsiz bo'lishini ta'minlaydi. Ular, kiberxavfsizlikning asosiy qismi sifatida muhim rol o'ynaydi. Shaxslar va obyektlar identifikatsiya va autentifikatsiya protokollarini ishlatib, ma'lumotlarga kirishni boshqarish, ularga xavfsizlikni ta'minlash va ma'lumot almashish jarayonlarini himoya qilishadi.*

**Kalit so'zlar:** *Identifikatsiya, Autentifikatsiya, Ma'lumot tizimi, Identifikatsiya protokollari, Autentifikatsiya usullari, Maxfiylik.*

**Abstract:** *Identification and authentication are principles used to identify, validate, and regulate access to information about individuals and objects in information systems.*

*Identification is the process of assigning a unique identifier (ID) to a person or object in an information system. Identifiers are used to describe information that uniquely and uniquely identifies an individual. For example, a username, email address, or digital ID can be used as an identifier for users.*

*Authentication is the process of correctly and clearly confirming a person or object for access to an information system. Through this process, the information system performs identity verification of the individual. Authentication methods are implemented using the identity of the person (username, ID) together with the privacy keys (password, master key, biometric data). Through such methods, the user enters authentication information about himself when logging into the system, and the system allows him to log in.*

*Identification and authentication ensure data protection and access to the system is confidential and secure. They play an important role as a key part of cyber security. Individuals and entities use identification and authentication protocols to control access to information, provide security to it, and protect information exchange processes.*

**Keywords:** *Identification, Authentication, Information system, Identification protocols, Authentication methods, Privacy.*

## KIRISH

Kiberxavfsizlik sohasida identifikatsiya va autentifikatsiya tushunchalari muhimlik kazgan holda, ularning afzalliklar va kamchiliklariga o'rtacha qaraydiganicha yodda tutishimiz lozim. Quyidagi afzalliklar va kamchiliklar ma'lumotlarni himoya qilishda identifikatsiya va autentifikatsiya tizimlarining muhimligini belgilaydi:

### AFZALLIKLAR

1. Maxfiylik: Identifikatsiya va autentifikatsiya protokollari maxfiylikni ta'minlashga imkon beradi. Parol, asosiy kalit yoki biometrik ma'lumotlar kabi maxfiylik kalitlari foydalanuvchilarning identifikatsiya va autentifikatsiyasini muhim sifatida saqlashga yordam beradi.

2. Aniq va unikal identifikatsiya: Identifikatsiya tizimi unikal identifikatorlar yaratishga imkon beradi, bu esa foydalanuvchilarni to'g'ri va aniq aniqlashni ta'minlaydi. Bu esa ma'lumotlarni xavfsiz va to'g'ri foydalanishga imkon beradi.

3. Avtomatik tizimlar: Identifikatsiya va autentifikatsiya tizimlari avtomatlashtirilgan bo'lishi, ishga tushish jarayonlarini tezlashtiradi va foydalanuvchilar uchun qulaylik yaratadi. Bu tizimlar yordamida identifikatsiya va autentifikatsiya jarayonlari avtomatik tarzda amalga oshiriladi, hatto biron bir qo'shimcha tasdiqlash ma'lumotlarini ham talab qilmaydi.

### KAMCHILIKLAR

1. Xavfsizlik risklari: Identifikatsiya va autentifikatsiya tizimlari ham xavfsizlik rivojlanishiga raqobat qiladigan xavfsizlik risklari bilan birlashishadi. Parol yoki asosiy kalitning o'zgartirilmay qolishi, biometrik ma'lumotlarining o'zgarishlari yoki identifikatsiya ma'lumotlarining hususiy axborot tarmog'iga kirishi kabi muammo va xavfsizlik og'irliklari mavjud bo'lishi mumkin.

2. Yuqori texnologiyalar: Identifikatsiya va autentifikatsiya tizimlarining yuqori texnologiyalar va yuksek sifatli qurilmalar talab qilishi kamchiliklar bo'lishi mumkin. Bu esa narxlarning oshishi va qurilmalar bilan ishlovchi xodimlar talabini oshirishi mumkin.

3. Foydalanuvchilarning zaruriy tushunmovchiliklari: Identifikatsiya va autentifikatsiya protokollari foydalanuvchilar uchun qulay va foydali bo'lishi kerak, aks holda foydalanuvchilar tizimga kirishda muammo va qiyinchiliklar bilan yuzlashishlari mumkin. Bu esa tizimning ish faoliyatini ta'sir qilishi va tizimdan bo'sh tashqariga tashlanishlarini oshirishi mumkin.

Identifikatsiya va autentifikatsiya tushunchalari kiberxavfsizlikning asosiy qismi bo'lib, ma'lumotlarni himoya qilishda muhim ahamiyatga ega. Bu tushunchalar ma'lumotlarga foydalanuvchilar va obyektlar bilan bog'lanish imkonini beradi va ularga yomon niyatli tashqi shaxslar tomonidan kirishni cheklashga imkon yaratadi. Ular tizimlarda yuqori darajada xavfsizlik, maxfiylik va integritetni ta'minlashda muhim rol o'ynaydi.

Shuningdek, identifikatsiya va autentifikatsiya protokollari foydalanuvchilarga xavfsiz va foydali tizimga kirish imkonini beradi, shaxslarning ma'lumotlarga qayta ulanish va o'zlariga xos axborotlarga kirishni tartibga solishda himoya ta'minlaydi. Bu protokollar tizimlar uchun muhimdir, chunki foydalanuvchilarning ma'lumotlarga xavfsiz kirishlari va ularga to'g'ri va haqiqiy tizimga kirishlari xavf-xatarlarni kamaytiradi.

Identifikatsiya va autentifikatsiya tushunchalari bilan ma'lumotlarni himoya qilishning yuqori darajada muhim asosiy qismlari hisoblanadi. Xavfsizlikni ta'minlash va maxfiylikni saqlash maqsadida, ma'lumotlar to'g'ri inobatga olingan foydalanuvchilarga berilishi, ularga tegishli maxfiylik kalitlari ishlatilishi va identifikatsiya va autentifikatsiya protokollarining yuqori darajada xavfsiz bo'lishi zarur. Bu tushunchalar kiberxavfsizlikning asosiy qismidir va muhimdir, shuning uchun ularga tizimlar va ma'lumotlarni xavfsizlikni ta'minlashda diqqat bilan qarash kerak. muvozanatini ta'minlash uchun foydalanuvchilarning talablariga va tizimning xavfsizlik darajasiga qarab tanlash kerak. Ba'zi usullar oson va ishonchli bo'lishi bilan ajralib turadi, ammo ularning biometrik ma'lumotlarni to'plash uchun mahsulotlarni talab qilishi yoki tizim uchun yuqori darajada xavfsizlikni ta'minlash talab qilishi mumkin. Boshqa usullar esa shaxsiy xavfsizlikka ko'maklashish uchun yoki yurituvchi organlar bilan integratsiya talab etishi mumkin.

Identifikatsiya va autentifikatsiya kiberxavfsizlikning muhim qismlaridir va tizimlarni yomon niyatli tashqariga qarshi himoya qilishda asosiy ahamiyatga ega. Foydalanuvchilar va tizimlar uchun identifikatsiya va autentifikatsiya usullarini to'g'ri va amalga oshirish, shu bilan birga, foydalanuvchilar bilan ma'lumotlar va axborot almashishda o'zlarining xavfsizligini ta'minlash muhimdir. Tizimlarda muvaffaqiyatli identifikatsiya va autentifikatsiya protokollari ishlatish, foydalanuvchilarga xavfsiz va foydali tizimga kirish imkonini beradi, shuningdek, maxfiylik va integritetni ta'minlash imkoniyatini oshiradi. Shu sababli, kiberxavfsizlikning yuqori darajada muhim qismlari sifatida, identifikatsiya va autentifikatsiya usullariga e'tibor berish katta muhimlikka ega.

Kriptografiya sohasida identifikatsiya va autentifikatsiya muhim tushunchalardir. Identifikatsiya, foydalanuvchini, tizimni yoki xizmatni unikal ravishda tanlash jarayonidir, autentifikatsiya esa foydalanuvchi tomonidan bildirilgan ma'lumotlarni tekshirish va tasdiqlash jarayonidir.

Identifikatsiya va autentifikatsiya tizimlari kiberxavfsizlikning muhim qismlarini tashkil etadi. Ular yurituvchi organlar, internet saytlari, banklar va boshqa tizimlar uchun kritik ahamiyatga ega bo'lgan ma'lumotlarni himoya qilishda katta rol o'ynaydi.

Identifikatsiya va autentifikatsiya tizimlarida foydalanuvchilarning identifikatori, parollar, biometrik ma'lumotlar, elektronik sertifikatlar kabi usullar ishlatiladi. Bu usullar tizimlar orasidagi ma'lumot almashishni xavfsiz va ishonchli qilishda yordam beradi.

Boshqa kiber xavfsizlik muammolarini oldini olish uchun identifikatsiya va autentifikatsiya tizimlari ikkilanuvchi autentifikatsiya, fido2 protokollari, kripto kaltaklar kabi yuqori darajadagi xavfsizlikning muhim tamoyillarini ham o'z ichiga oladi.

Shuningdek, identifikatsiya va autentifikatsiya tizimlarining afzalliklari daromad, ishonch, xavfsizlik, foydalanuvchilarning sahifalarga va tizimlarga oson kirishini ta'minlash, foydalanuvchilar va tizimlar orasidagi ma'lumot almashishni to'g'ri va xavfsiz qilish imkoniyatini beradi.

Shu bilan birga, identifikatsiya va autentifikatsiya tizimlarining kamchiliklari ham mavjud. Misol uchun, parollar yodlash muammolari, biometrik ma'lumotlarni falsifikatsiya qilish imkoniyati, sertifikatlar va kalit so'zlar yoki kalitlar yoki ularning boshqa xavfsizlik muammolari bo'lishi mumkin.

Xulosa qilish uchun, identifikatsiya va autentifikatsiya tizimlari tizimlarning xavfsizligini ta'minlashda muhim ahamiyatga ega. Ular foydalanuvchilar uchun oson, ishonchli va foydali tizimga kirish imkonini ta'minlaydi. Shuningdek, ular ma'lumot almashishda xavfsizlik va maxfiylikni ta'minlashga yordam beradi. Bu tizimlar kiberxavfsizlikning muhim asoslari hisoblanadi.

#### **XULOSA**

Identifikatsiya va autentifikatsiya, kiberxavfsizlikning muhim tushunchalari bo'lib, tizimlarda va foydalanuvchilar orasidagi ma'lumot almashishda va kirishlarda xavfsizlikni ta'minlashda ahamiyatga ega.

Identifikatsiya, foydalanuvchini, tizimni yoki xizmatni unikal ravishda tanlash jarayonidir. Bu, bir foydalanuvchining tizimga kirishda o'zining identifikatorini yoki usernameni ko'rsatish orqali amalga oshiriladi. Identifikatsiya jarayoni tizim tomonidan identifikator bilan bog'liq ma'lumotlar bazasida qidiruvni bajaradi va foydalanuvchining kimligini aniqlayadi. Bu usul yordamida foydalanuvchilar bir-biridan ajralib turadigan ma'lumotlarga kirish imkoniyatiga ega bo'ladi.

Autentifikatsiya esa foydalanuvchi tomonidan bildirilgan ma'lumotlarni tekshirish va tasdiqlash jarayonidir. Ushbu jarayonda foydalanuvchi o'zining identifikatorini kiritadi va uni tasdiqlash uchun autentifikatsiya usullaridan foydalaniladi, masalan, parol, biometrik ma'lumotlar yoki elektronik sertifikatlar. Autentifikatsiya jarayoni foydalanuvchining kimligini tasdiqlash va tasdiqlangan foydalanuvchining tizimga kirishga ruhsat berishni ta'minlaydi.

Identifikatsiya va autentifikatsiya tizimlarining afzalliklari o'zlariga xos bo'lib, foydalanuvchilar va tizimlar uchun quyidagi imkoniyatlarni beradi:

1. Xavfsizlik: Identifikatsiya va autentifikatsiya usullari tizimlardagi ma'lumot almashishni xavfsiz va ishonchli qilishda muhim ahamiyatga ega. Ushbu usullar yordamida

faqat tasdiqlangan va ma'lumotlarni to'g'ri identifikatsiya qilingan foydalanuvchilar tizimga kirish imkoniyatiga ega bo'ladi.

2. Foydalanuvchi kirishining osonligi: Identifikatsiya va autentifikatsiya tizimlari foydalanuvchilarga tizimlarga oson kirish imkonini ta'minlaydi. Foydalanuvchilar o'z identifikatorlarini va autentifikatsiya ma'lumotlarini yodlash va unga kirishda qulaylikka ega bo'ladi.

3. Xavfsizlikning muhofazasi: Identifikatsiya va autentifikatsiya tizimlari foydalanuvchilar va tizimlar orasidagi ma'lumot almashishni xavfsiz va shartnoma

#### **FOYDALANILAGAN ADABIYOTLAR:**

«Axborot texnologiyasi. Ma'lumotlarni kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O'zbekiston Davlat standard. O'z DSt 1092:2005.

«Axborot texnologiyasi. Axborotlarni kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi» O'zbekiston Davlat standard. O'zDSt 1105:2006

«Axborot texnologiyasi. Ochiq tizimlar o'zaro bogliqligi. Elektron raqamli imzo ochiq kaliti sertifikatini va atribut sertifikatining tuzilishi» O'zbekiston Davlat standarti. O'zDSt 1108:2006.

С.В. Симонов. Анализ рисков в информационных системах. Практические советы! // Конфидент. -2001. -№2.

S.S.Qosimov. Axborot texnologiyalari. O'quv qo'llanma. - T.: «Aloqachi», 2006.

S.K.G'aniyev, M.M. Karimov. Hisoblash sistemalari va tarmoqlarida informatsiya himoyasi. Oliy o'quv yurti talab uchun o'quv qo'llanma. —Toshkent Davlat texnika universiteti, 2003.

3. Kosimova, A. (2022). MAIN FEATURES OF LANGUAGE LEARNING STRATEGIES. Eurasian Journal of Academic Research, 2(12), 1247-1249.

4. Kosimova, A. (2022). DRABLLAR–KICHIK HAJMLI EPIK JANR. In INTERNATIONAL CONFERENCES (Vol. 1, No. 21, pp. 490-493).

5. Usmonova, D. S., & Muydinova, N. U. Phraseological Units with Proper Nouns in the English and Uzbek Languages. International Journal on Integrated Education, 4(2), 370-374.

6. Muydinova, N. (2020). DYNAMIC ACTIVITIES FOR SONG IN THE EFL CLASSROOM. In НАУКА И ТЕХНИКА. МИРОВЫЕ ИССЛЕДОВАНИЯ (pp. 11-13).

7. Муйдинова, Н. (2020). СОСТОЯНИЕ ВДОХНОВЕНИЯ У СПОРТСМЕНОВ. In Психологическое здоровье населения как важный фактор обеспечения процветания общества (pp. 112-113).