AUTENTIFIKATSIYA VA AVTORIZATSIYA BILAN ISHLASH.

Yusupov Mirsaid Abdulaziz o'g'li
Farg'ona davlat universiteti amaliy matematikavainformatika kafedrasi katta o'qituvchisi
mirsaidbeky@gmail.com
Meliqoziyev Sahobiddin Umidjon o'g'li
Farg'ona davlat universiteti 2-bosqich talabasi
sahobiddinmeliqoziyev1@gmail.com

Anotatsiya: *Ushbu maqolada axborot tizimlari va veb-ilovalarda xavfsizlikni ta'minlashda muhim bo'lgan autentifikatsiya (shaxsni aniqlash) va avtorizatsiya (huquqlarni tekshirish) mexanizmlari haqida batafsil tahlil berilgan. Autentifikatsiya foydalanuvchining haqiqiyligini aniqlashga xizmat qilsa, avtorizatsiya esa unga ruxsat etilgan resurslarga kirish imkoniyatlarini nazorat qiladi. Maqolada ushbu ikki mexanizmning farqlari, ishlash tamoyillari, qo'llaniladigan texnologiyalar (OAuth 2.0, OpenID Connect, JWT, cookie, token-based authentication) va xavfsizlikka ta'siri haqida so'z yuritiladi.*

Kalit so'zlar: *Autentifikatsiya, avtorizatsiya, foydalanuvchi identifikatsiyasi, OAuth 2.0, OpenID Connect, JWT, RBAC, ASP.NET Core Identity, token, cookie, xavfsizlik, identifikatsiya, login, parol, JSON Web Token*

Abstract: *This article provides a detailed analysis of two essential security mechanisms in information systems and web applications: authentication and authorization. While authentication ensures the identification of the user, authorization checks their access rights to resources. The article explores the differences between these two processes, their principles, and the technologies commonly used (OAuth 2.0, OpenID Connect, JWT, cookie, token-based authentication) to implement them.*

Keywords: *Authentication, authorization, user identification, OAuth 2.0, OpenID Connect, JWT, RBAC, ASP.NET Core Identity, token, cookie, security, login, password, JSON Web Token*

Аннотация: *В данной статье проводится подробный анализ двух ключевых механизмов безопасности в информационных системах и веб-приложениях: аутентификация и авторизация. Аутентификация обеспечивает идентификацию пользователя, тогда как авторизация проверяет его права доступа к ресурсам. В статье рассматриваются различия между этими процессами, их принципы и технологии, которые обычно используются для их реализации (OAuth 2.0, OpenID Connect, JWT, cookie, token-based authentication).*

Ключевые слова: *Аутентификация, авторизация, идентификация пользователя, OAuth 2.0, OpenID Connect, JWT, RBAC, ASP.NET Core Identity, токен, cookie, безопасность, вход, пароль, JSON Web*

Autentifikatsiya va avtorizatsiya - zamonaviy axborot tizimlarining eng muhim va asosiy xavfsizlik mexanizmlaridan hisoblanadi. Axborot xavfsizligini ta'minlashda bu ikki jarayon bir-birini to‘ldiruvchi va tizimni himoya qilishda muhim rol o‘ynaydi. Autentifikatsiya, asosan, foydalanuvchining kimligini aniqlash jarayoni bo‘lib, tizimga kirish uchun uning shaxsini tekshiradi. Avtorizatsiya esa, autentifikatsiya jarayoni muvaffaqiyatli yakunlangandan so‘ng, foydalanuvchiga qanday resurslarga kirish huquqi berilishini belgilaydi. Bu ikki jarayonni to‘g‘ri tashkil etish, tizimni xavfsizligini oshirishga yordam beradi va tizimdagi resurslarga ruxsatsiz kirishni oldini oladi. Shuningdek, autentifikatsiya va avtorizatsiya tizimlarda ma'lumotlarning maxfiyligini, yaxlitligini va mavjudligini ta'minlashga xizmat qiladi, bu esa barcha onlayn xizmatlarning asosiy talabidir. Zamonaviy veb-ilovalar, mobil ilovalar va korporativ tizimlarda autentifikatsiya va avtorizatsiyaning turli usullari qo‘llaniladi, masalan, parollar,

ikki faktorli autentifikatsiya, tokenlar va ro‘yxatga olish xizmatlari. Ushbu maqolada autentifikatsiya va avtorizatsiya jarayonlarining o‘ziga xos jihatlari, ishlash tamoyillari va zamonaviy texnologiyalar yordamida xavfsizlikni ta'minlashning samarali usullari yoritiladi. Tizim xavfsizligini ta'minlashda autentifikatsiya va avtorizatsiyaning ahamiyati o‘sib bormoqda, shu bois bu mexanizmlar har bir tizimning mustahkam asosiga aylanishi kerak.

Autentifikatsiya (shaxsni aniqlash) jarayoni foydalanuvchining haqiqiyligini tekshirish uchun amalga oshiriladi. Bu jarayon tizimga kirish yoki unga ma'lumot yuborishdan oldin, foydalanuvchining kimligini tasdiqlashga xizmat qiladi. Autentifikatsiya jarayonining asosiy maqsadi tizimga faqat ruxsat etilgan shaxslarni kirishini ta'minlashdir. Buning uchun turli usullar qo‘llaniladi, masalan, foydalanuvchining identifikatsiya ma'lumotlari (login va parol), biometrik ma'lumotlar (barmoq izi, yuzni tanib olish), yoki xavfsiz tokenlar (masalan, bir martalik parollar yoki SMS orqali yuborilgan kodlar). Autentifikatsiya jarayoni tizimning asosiy xavfsizlik qatlamini tashkil etadi, chunki uning yordamida tizimga kirayotgan har bir foydalanuvchining kimligi tasdiqlanadi. Eng ko‘p qo‘llaniladigan autentifikatsiya usuli login va parol kombinatsiyasidir. Foydalanuvchi tizimga kirish uchun o‘zining maxfiy ma'lumotlarini taqdim etadi, va tizim bu ma'lumotlarni saqlangan ma'lumotlar bilan taqqoslaydi. Shuningdek, ikki faktorli autentifikatsiya (2FA) keng qo‘llanilmoqda, bunda foydalanuvchi faqatgina parolni emas, balki qo‘shimcha xavfsizlik kodini ham kiritishi kerak bo‘ladi. Bu usul xavfsizlikni sezilarli darajada oshiradi, chunki hatto parolni bilgan shaxs ham tizimga kirish uchun ikkinchi bosqichni o‘tishi kerak. Zamonaviy tizimlarda, autentifikatsiya jarayonlari tokenlar orqali amalga oshirilishi mumkin, bu esa foydalanuvchini bir marta tizimga kirgandan so‘ng, biror vaqt davomida tizimga qayta-qayta parol kiritmasdan kirish imkonini beradi. Tokenlar, ayniqsa, mobil ilovalar va veb-ilovalar uchun qulay bo‘lib, ular foydalanuvchining xavfsizligini ta'minlash bilan birga tizimning ishlash samaradorligini oshiradi.

Autentifikatsiya jarayonini to‘g‘ri tashkil etish va xavfsizligini ta'minlash tizimni ruxsatsiz kirishdan himoya qiladi, shu bilan birga foydalanuvchilarga ham oson va xavfsiz ishlash imkoniyatini yaratadi.

Avtorizatsiya (huquqlarni tekshirish) jarayoni autentifikatsiya jarayonidan keyin amalga oshiriladi va foydalanuvchining tizimdagi resurslarga kirish huquqini aniqlashga qaratilgan. Autentifikatsiya foydalanuvchining kimligini tasdiqlaydi, avtorizatsiya esa uning o‘zi tanlagan yoki tizim tomonidan berilgan resurslarga kirish imkoniyatlarini belgilaydi. Bu jarayon tizimning xavfsizligini ta'minlash uchun juda muhim, chunki u faqatgina ruxsat berilgan foydalanuvchilarga ma'lum ma'lumotlar yoki xizmatlarga kirish huquqi beradi. Avtorizatsiya ko‘pincha foydalanuvchining roliga yoki ma'lum huquqlar to‘plamiga asoslanadi. Masalan, ba'zi foydalanuvchilar faqat o‘qish huquqiga ega bo‘lishi mumkin, boshqalari esa ma'lumotlarni tahrirlash, o‘zgartirish yoki o‘chirib tashlash imkoniyatiga ega bo‘ladi. Bu turdagi huquqlarni belgilashda, odatda, ro‘yxatga olish tizimlari (RBAC – Role-Based Access Control) yoki atributga asoslangan kirish nazorati (ABAC – Attribute-Based Access Control) qo‘llaniladi. RBAC tizimida foydalanuvchiga bir yoki bir nechta ro‘l tayinlanadi, va har bir ro‘lni bajarishga ruxsat etilgan faoliyatlar va huquqlar ro‘yxati mavjud bo‘ladi. ABAC esa foydalanuvchining o‘ziga xos atributlariga (masalan, bo‘limi, lavozimi yoki boshqa parametrlariga) asoslanib, unga ma'lum resurslarga kirish imkoniyatlarini beradi. Shuningdek, avtorizatsiya jarayonida tizim ma'lum resurslarga kirish uchun vaqt chegaralari, geolokatsiya, foydalanuvchining faoliyati va boshqa omillarni ham hisobga olishi mumkin. Bu tizimlarga to‘g‘ri kirish huquqlarini ta'minlash, tashkilotning ichki xavfsizlik siyosatini qo‘llash va foydalanuvchilarning ma'lumotlarini himoya qilishni yanada samarali qilish imkonini beradi. Yaxshi tashkil etilgan avtorizatsiya tizimi, foydalanuvchilarga kerakli resurslarga kirish huquqlarini samarali taqdim etish bilan birga, tizimning xavfsizligini yuqori darajada saqlaydi.

Zamonaviy autentifikatsiya va avtorizatsiya jarayonlarini amalga oshirishda turli texnologiyalar va protokollar keng qo‘llaniladi. Bularning orasida OAuth 2.0, OpenID Connect, JWT, SAML, va X.509 kabi mashhur usullar mavjud. OAuth 2.0 — bu autentifikatsiya va avtorizatsiya uchun keng tarqalgan standart bo‘lib, u foydalanuvchi resurslariga kirishni boshqa bir xizmat orqali ruxsat olish imkoniyatini beradi. OAuth 2.0 tizimlarida foydalanuvchi o‘zi istagan xizmatni tanlab, boshqa bir tizimga (masalan, Facebook, Google) o‘zining identifikatsiya ma'lumotlarini taqdim etmasdan, ushbu xizmatning resurslariga kirish imkoniyatiga ega bo‘ladi. OpenID Connect esa OAuth 2.0 asosida qurilgan protokol bo‘lib, foydalanuvchining kimligini autentifikatsiya qilishni ta'minlaydi va foydalanuvchi haqidagi qo‘shimcha ma'lumotlarni (masalan, ismi, email manzili) olish imkonini beradi. Bu ikki protokolni birgalikda ishlatish ko‘plab veb-ilovalar va mobil ilovalarda foydalanuvchilarning kirish jarayonlarini soddalashtiradi va xavfsizligini oshiradi.

JWT (JSON Web Token) esa foydalanuvchi identifikatsiyasi va avtorizatsiya uchun ishlatiladigan ko‘plab ilovalarda qo‘llaniladigan formatdir. JWT tokenlari, foydalanuvchi muvaffaqiyatli autentifikatsiyadan o‘tgandan so‘ng, tizim tomonidan yaratiladi va ular foydalanuvchi haqidagi ma'lumotlarni saqlaydi, shu bilan birga tizimga kirishni davom ettirish uchun tokenni uzatishga imkon beradi. Tokenlar, shuningdek, serverga o‘zgartirilmaydigan tarzda yuboriladi, bu esa xavfsizlikni ta'minlashga yordam beradi. SAML (Security Assertion Markup Language) esa asosan tashkilotlar va kompaniyalar o‘rtasida yagona kirishni ta'minlash uchun ishlatiladi. SAML yordamida foydalanuvchining autentifikatsiyasi tashqi provayder tomonidan amalga oshiriladi, va tizimga kirishda faqatgina foydalanuvchining identifikatsiya ma'lumotlari uzatiladi. X.509 esa shifrlash va autentifikatsiyani amalga oshiradigan sertifikatlar asosidagi texnologiya bo‘lib, ayniqsa tarmoqda xavfsiz aloqa o‘rnatish uchun ishlatiladi.

Bu texnologiyalarni birgalikda qo‘llash orqali tizimlar nafaqat foydalanuvchi identifikatsiyasini samarali va xavfsiz tarzda amalga oshirishi, balki resurslarga kirishni to‘g‘ri boshqarish hamda huquqlarni tekshirishni ta'minlaydi. Xavfsizlikning yuqori darajada saqlanishi uchun autentifikatsiya va avtorizatsiya jarayonlarining to‘g‘ri tashkil etilishi juda muhimdir. Har bir texnologiyaning o‘ziga xos afzalliklari va qo‘llanilish sohalari mavjud bo‘lib, ular tizimning ehtiyojlariga mos ravishda tanlanadi. Bu texnologiyalarni amalga oshirish orqali foydalanuvchilarga maksimal darajada xavfsiz va qulay kirish imkoniyatlari yaratiladi.

Autentifikatsiya va avtorizatsiya jarayonlari zamonaviy axborot tizimlarining xavfsizlikni ta'minlashdagi asosiy elementlaridan biridir. Ushbu jarayonlarning to‘g‘ri tashkil etilishi, foydalanuvchilarni tizimga kirishda va ularning resurslarga kirishini boshqarishda muhim rol o‘ynaydi. Autentifikatsiya orqali foydalanuvchining kimligini tasdiqlash, avtorizatsiya orqali esa unga qanday huquqlar va resurslar taqdim etilishi aniq belgilanadi. Ushbu mexanizmlar tizim xavfsizligini ta'minlashda kuchli himoya qatlamlarini yaratadi, chunki ular faqat ruxsat etilgan foydalanuvchilarga tizimga kirishga va resurslardan foydalanishga imkon beradi. Shuningdek, autentifikatsiya va avtorizatsiyaning zamonaviy texnologiyalar bilan amalga oshirilishi xavfsizlikni yanada kuchaytiradi, masalan, ikki faktorli autentifikatsiya, JWT tokenlari, OAuth 2.0 kabi metodlar foydalanuvchi identifikatsiyasini va huquqlarini tasdiqlashda samarali ishlaydi.

Kelayotgan yillarda autentifikatsiya va avtorizatsiya texnologiyalari yanada rivojlanib, yanada xavfsizroq va samaraliroq bo‘lishi kutilmoqda. Bunday texnologiyalarni amalga oshirishda foydalanuvchilarga qulaylik yaratish bilan birga, tizimlar xavfsizligini ta'minlash va ma'lumotlarni himoya qilishda yangi imkoniyatlar ochiladi. Biroq, xavfsizlikni ta'minlashda bir nechta xavflar va muammolar mavjud. Misol uchun, parolni yo‘qotish yoki noto‘g‘ri autentifikatsiya qilish kabi holatlar tizimning zaif tomonlarini yaratishi mumkin. Shuning uchun,

autentifikatsiya va avtorizatsiya jarayonlarini muntazam ravishda yangilab borish va zamonaviy xavfsizlik metodlarini qo‘llash zarur. Takliflar sifatida, tizimlarga ikki faktorli autentifikatsiya (2FA)ni joriy qilish, foydalanuvchilarning maxfiy ma'lumotlarini saqlashda yuqori darajadagi shifrlash texnologiyalarini qo‘llash va kirish huquqlarini muntazam tekshirib turish muhim ahamiyatga ega. Shuningdek, foydalanuvchi kirishlarini real vaqt rejimida monitoring qilish va tizimga kirishlarni audit qilish uchun ilg‘or vositalardan foydalanish, xavfsizlikni yanada kuchaytiradi. Avtorizatsiya mexanizmlarini optimallashtirish va foydalanuvchilarga moslashtirilgan huquqlarni yaratish tizimlar uchun xavfsizlikni ta'minlashning samarali usulidir. Xavfsizlikni yanada kuchaytirish va tizimlarni yangilab borish orqali axborot tizimlarining ishonchliligini oshirish mumkin.

Foydalanilgan adabiyotlar

1. Microsoft Docs – Authentication and Authorization in ASP.NET Core
2. OAuth 2.0 Authorization Framework – IETF RFC 6749
3. OpenID Connect Core 1.0 – OpenID Foundation
4. "Programming ASP.NET Core" – Dino Esposito
5. "Identity and Access Management" – Graham Williamson
6. Auth0 Blog – Authentication vs. Authorization
7. "ASP.NET Core in Action" – Andrew Lock
8. OWASP Authentication Cheat Sheet – owasp.org
9. "Pro ASP.NET Core Identity" – Adam Freeman
10. JWT.io Documentation – JSON Web Token Introduction
11. Microsoft Learn – Secure ASP.NET Core apps
12. Pluralsight – OAuth2 and OpenID Connect Explained
13. IdentityServer4 Documentation – identityserver.io
14. "Security in Computing" – Pfleeger & Pfleeger

15.Spring Security Documentation – Authentication and Authorization Concepts

16.Raxmatjonova, M. N., & Tojimamatov, I. N. (2023). BIZNESDA SUNIY INTELEKT TEXNOLOGYALARI VA ULARNI AHAMIYATI. Лучшие интеллектуальные исследования, 11(3), 46-52.

17.Nurmamatovich, T. I. (2024, April). BIR QATLAMLI PERCEPTRONNI O ‘QITISH. In " CANADA" INTERNATİONAL CONFERENCE ON DEVELOPMENTS İN EDUCATİON, SCİENCESAND HUMANİTİES (Vol. 17, No. 1).

18.Nurmamatovich, T. I. (2024, April). SUN’IY NEYRONNING MATEMATIK MODELI HAMDA FAOLLASHTIRISH FUNKTSIYALARI. In " USA" INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE TOPICAL ISSUES OF SCIENCE (Vol. 17, No. 1).