FOYDALANUVCHILAR BOSHQARUVI
УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ
USER MANAGEMENT

Behzod Sobirjonov
FarDU Axborot texnologiyalari kafedrasi o'qituvchisi
behzodbekqahramonovich@gmail.com
+998905268738
Sharofiddinov Shahobiddin Norinboy o'g'li
Farg'ona davlat universiteti Axborot tizimlari va texnologiyalari yo'nalishi 2-bosqich talabalari
sharofiddinovshahobiddin062@gmail.com

Annotatsiya: *Foydalanuvchilar boshqaruvi (User Management) — axborot tizimlarida foydalanuvchilarni identifikatsiya qilish, autentifikatsiya jarayonini amalga oshirish va ularga tizim resurslaridan foydalanish bo'yicha tegishli ruxsatlarni belgilashga qaratilgan kompleks mexanizmlar majmuasidir. Ushbu jarayon axborot xavfsizligining strategik elementi hisoblanadi va himoyalangan muhitda faqat vakolatli foydalanuvchilarning faoliyat yuritishini ta'minlaydi.*

Zamonaviy korporativ tizimlarda foydalanuvchilar boshqaruvida RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control) va IAM (Identity and Access Management) kabi standartlar keng qo'llaniladi. Gartner tadqiqotlariga ko'ra, kuchli identifikatsiya va ruxsat boshqaruvi siyosati yo'qligi tashkilotlardagi xavfsizlik buzilishlarining 50–70% hollarda asosiy omil sifatida qayd etilgan.

Аннотация: *Управление пользователями представляет собой комплекс механизмов, направленных на идентификацию пользователей информационных систем, выполнение процессов аутентификации и предоставление соответствующих прав доступа к ресурсам системы. Данный процесс является ключевым элементом информационной безопасности, обеспечивая функционирование только уполномоченных субъектов в защищенной среде.*

В современных организациях широко внедряются такие модели как RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control) и IAM (Identity and Access Management), которые обеспечивают структурированное и масштабируемое управление доступом. По данным Gartner, отсутствие корректной политики управления идентификацией и доступом становится причиной 50–70% нарушений безопасности в компаниях по всему миру.

Annotation: *User management is a comprehensive set of mechanisms designed to identify users within information systems, authenticate their identities, and manage their permissions in accessing system resources. As a core pillar of information security, it ensures that only authorized individuals interact with sensitive data and internal infrastructures.*

Modern organizations implement advanced frameworks such as RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), and IAM (Identity and Access Management) to establish structured and scalable access governance. According to Gartner, insufficient identity and access control policies account for 50–70% of organizational security breaches globally.

Kalit so‘zlar: *Foydalanuvchilar boshqaruvi, autentifikatsiya, avtorizatsiya, identifikatsiya, RBAC, ABAC, IAM, MFA, axborot xavfsizligi, ruxsat boshqaruvi, kiberxavfsizlik*

Ключевые слова: *Управление пользователями, аутентификация, авторизация, идентификация, RBAC, ABAC, IAM, MFA, информационная безопасность, контроль доступа, кибербезопасность*

Keywords: *User management, authentication, authorization, identification, RBAC, ABAC, IAM, MFA, information security, access control, cybersecurity*

Kirish

Raqamli texnologiyalar jadal rivojlanib borayotgan XXI asrda axborot tizimlarining xavfsizligi davlatlar, korxonalar va global tashkilotlar oldida turgan eng muhim masalalardan biriga aylandi. Jahon miqyosida har kuni 300 mingdan ortiq kiberhujumlar qayd etilayotgani, yirik kompaniyalar hamda davlat tizimlaridagi ma’lumotlar tarqoqligi yoki himoyaning yetarli bo‘lmasligi natijasida milliardlab dollarlik zararlar yuzaga kelayotgani foydalanuvchilar boshqaruvi (User Management) tizimlarining naqadar zarur ekanini yaqqol ko‘rsatadi.

Axborot tizimlarining asosiy xavf nuqtalaridan biri — bu foydalanuvchilarning identifikatsiyasi va ularga berilgan ruxsatlarning noto‘g‘ri boshqarilishidir. Gartner va Cybersecurity Ventures kabi xalqaro tadqiqot agentliklari bergan ma’lumotlarga ko‘ra, tashkilotlarda sodir bo‘ladigan xavfsizlik buzilishlarining 50–70% holatlari aynan noto‘g‘ri sozlangan foydalanuvchi huquqlari, parollarni boshqarishdagi zaifliklar va autentifikatsiya jarayonining sustligi bilan bog‘liq. Bu esa har qanday axborot tizimida foydalanuvchilar boshqaruvi mexanizmlarini to‘g‘ri joriy etish va muntazam takomillashtirish zarurligini ta’kidlaydi.

Zamonaviy tashkilotlar foydalanuvchi faoliyatini nazorat qilishda RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), IAM (Identity and Access

Management) kabi global standartlardan foydalanmoqda. Ushbu modellarning amaliy samarasini AQSh, Yevropa va Osiyodagi yirik IT korporatsiyalari o‘z tajribalarida tasdiqlagan. Masalan, role-based boshqaruv tizimining joriy etilishi katta korporatsiyalarda ma’lumotlarga noqonuniy kirish hollari miqdorini sezilarli kamaytirgani, audit jarayonlarining tezlashishiga va iqtisodiy sarf-xarajatlarning optimallashuviga olib kelgani qayd etilgan.

Shuningdek, so‘nggi yillarda ko‘p bosqichli autentifikatsiya (MFA), biometrik identifikatsiya, avtomatlashtirilgan sessiya boshqaruvi va foydalanuvchilar faoliyatini real vaqtda monitoring qilish kabi ilg‘or texnologiyalar keng qo‘llanilmoqda. Microsoft hamda Google tomonidan e’lon qilingan statistik ma’lumotlarda MFA qo‘llanilishi hisob buzilish xavfini 99% gacha kamaytirishi amaliy jihatdan tasdiqlangan. Bu esa oddiy parol tizimining zamonaviy tahdidlar oldida yetarli emasligini yana bir bor isbotlaydi.

Asosiy qism

Foydalanuvchilar boshqaruvi — axborot tizimlarida foydalanuvchilarni identifikatsiya qilish, autentifikatsiya jarayonini amalga oshirish, ularga tizim doirasida turli darajadagi huquqlarni belgilash, monitoring qilish hamda ularning tizimdan foydalanish faoliyatini nazorat qilishni o‘z ichiga oladigan kompleks boshqaruv tizimidir. Ushbu mexanizmlar axborot xavfsizligining muhim qismi bo‘lib, davlat tashkilotlaridan tortib yirik korporatsiyalargacha bo‘lgan barcha infratuzilmalarda qo‘llaniladi. Axborot xavfsizligi bo‘yicha xalqaro standart ISO/IEC 27001:2022 da identifikatsiya va ruxsatlarni boshqarish bo‘yicha qat’iy talablar belgilab qo‘yilgan. Har bir foydalanuvchi uchun alohida identitet mavjud bo‘lishi, parol siyosati muntazam yangilanib borishi, huquqlar rollarga asoslanishi va audit jarayonlari avtomatlashtirilgan bo‘lishi lozim. Dunyo miqyosida har kuni yuz minglab yangi kiberhujumlar qayd etilayotgani, ulardan ko‘pchiligi noto‘g‘ri ruxsatlar yoki eskirgan autentifikatsiya jarayonlari tufayli sodir bo‘layotgani foydalanuvchilar boshqaruvi qanchalik muhim ekanini ko‘rsatadi.

Foydalanuvchilar boshqaruvi jarayonida identifikatsiya foydalanuvchini tizimda tanib olishni, autentifikatsiya esa foydalanuvchi haqiqatdan ham tizimga kirishga haqli ekanini tasdiqlashni o‘z ichiga oladi. Autentifikatsiya usullari sifatida parol tizimi, ko‘p bosqichli autentifikatsiya, biometrik identifikatsiya va tokenlar asosida autentifikatsiya keng qo‘llaniladi. Multi-Factor Authentication texnologiyasi hisoblar buzilishi xavfini sezilarli darajada kamaytiradi. Avtorizatsiya foydalanuvchiga qaysi ma’lumotlar, funksiyalar va resurslardan foydalanishga ruxsat berilishini belgilaydi va ko‘plab korporativ tizimlarda RBAC, ABAC va PBAC kabi modellardan foydalaniladi. Rollarga asoslangan boshqaruv modeli foydalanuvchining roliga qarab huquqlarni belgilaydi, atributlarga asoslangan boshqaruv modeli esa foydalanuvchi atributlari orqali ruxsatlarni boshqaradi. Identity and Access Management tizimi esa identifikatsiya va ruxsatlarni markazlashtirilgan

boshqarishni ta’minlaydi, foydalanuvchi hayotiy siklini avtomatlashtiradi, rollar va ruxsatlarni taqsimlaydi hamda audit jarayonlarini soddalashtiradi.

Xulosa

Foydalanuvchilar boshqaruvi axborot tizimlarida xavfsizlikni ta’minlash, tizim resurslarini samarali boshqarish va ma’lumotlarning yaxlitligini saqlashda asosiy vazifani bajaradi. Ushbu boshqaruv tizimi foydalanuvchilarning identifikatsiyasi, autentifikatsiyasi va avtorizatsiyasini tizimli tarzda nazorat qiladi, shu bilan birga ruxsatlarni markazlashtirilgan boshqarish, audit jarayonlarini soddalashtirish va kiberhujumlar xavfini sezilarli darajada kamaytirish imkonini beradi. Zamonaviy tashkilotlarda RBAC, ABAC va IAM kabi boshqaruv modellari qo‘llanilib, foydalanuvchilarning rollari va atributlariga qarab resurslarga kirish huquqlari belgilangan. Bu esa nafaqat tizim xavfsizligini oshiradi, balki foydalanuvchilar faoliyatini tartibga solish, resurslardan samarali foydalanish va jarayonlarni optimallashtirish imkonini ham beradi.

Ko‘p bosqichli autentifikatsiya (MFA), biometrik identifikatsiya va sessiya boshqaruvi kabi ilg‘or texnologiyalar foydalanuvchi hisoblarining buzilish xavfini sezilarli darajada kamaytiradi, shuningdek, tashkilot ichidagi ma’lumotlar oqimini nazorat qilish va noxush kirishlarning oldini olishga yordam beradi. Foydalanuvchilar boshqaruvi tizimi shuningdek audit jarayonlarini osonlashtiradi, xodimlarning faoliyatini kuzatish va tizimdagi nojo‘ya harakatlarni tez aniqlash imkonini beradi.

Shu bilan birga, foydalanuvchilar boshqaruvi nafaqat xavfsizlikni ta’minlash vositasi, balki tashkilotning umumiy samaradorligini oshirish, ish jarayonlarini avtomatlashtirish va axborot resurslarini oqilona boshqarish uchun ham muhim vositadir. Global kiberhujumlar va ma’lumotlarning buzilishi xavfi ortib borayotgan zamonaviy raqamli muhitda foydalanuvchilar boshqaruvini samarali tashkil etish va uni muntazam yangilab borish har bir tashkilot uchun strategik ahamiyatga ega. Umuman olganda, foydalanuvchilar boshqaruvi — bu xavfsiz, samarali va nazorat qilinadigan axborot tizimini yaratishning ajralmas qismi bo‘lib, zamonaviy tashkilotlar faoliyatida ajralmas element sifatida qaraladi. Tizimning barqarorligi va ma’lumotlar xavfsizligini ta’minlash, shuningdek, kiberhujumlarga qarshi samarali choralarni qo‘llash foydalanuvchilar boshqaruvining to‘g‘ri tashkil etilishiga bog‘liq.

FOYDALANILGAN ADABIYOTLAR

1. ISO/IEC 27001:2022 — Information Security Management Standards
2. NIST Special Publication 800-63 — Digital Identity Guidelines
3. Gartner Research Report, 2023–2024

4. Cybersecurity Ventures — Annual Cybercrime Report, 2023
5. Microsoft Security Blog, MFA Security Statistics, 2022–2023