

WINDOWS OPERATSION TIZIMIDA ISHLASH ASOSLARI

Suyarov Akram Musayevich

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrası PHD, dotsenti

akramsuyarov@gamil.ru

Zokirova Fariza Fozilovna

Samarqand Iqtisodiyot va servis instituti

Buxgalteriya hisobi va menejment fakulteti talabasi

Annotatsiya

Ushbu maqolada Microsoft Windows operatsion tizimining arxitekturasi, ichki komponentlari, fayl tizimi, xavfsizlik mexanizmlari va foydalanuvchi interfeysi batafsil ko‘rib chiqiladi. Shuningdek, zamonaviy Windows versiyalarida (masalan, Windows 10 / Windows 11) ishlash samaradorligi, qulayliklari va xatarlarini baholash uchun SWOT tahlil jadvali keltiriladi. Maqola oliy ta‘lim talabalariga mo‘ljallangan bo‘lib, operatsion tizimlar nazariyasi va amaliy kompyuter bilimlari nuqtai nazaridan ahamiyatga ega.

Kalit so‘zlar: Microsoft Windows, operatsion tizim, yadroviy arxitektura, kernel-mode, user-mode, fayl tizimi, NTFS, ReFS, EFS, xavfsizlik, foydalanuvchi interfeysi, grafik interfeys (GUI), multitasking, resurs boshqaruvi, disk shifrlash, tizim xizmatlari, Windows 11, yangilanishlar, operatsion muhit, tizim konfiguratsiyasi, tarmoq integratsiyasi.

Kirish

Microsoft Windows operatsion tizimi — shaxsiy kompyuterlar, noutbuklar va boshqa ko‘plab qurilmalar uchun yaratilgan global darajada mashhur operatsion muhitdir. Windows turli versiyalari (masalan, Windows 10, Windows 11) davomida o‘zgarish va rivojlanishlardan o‘tib, foydalanuvchi ehtiyojlari va zamonaviy texnologiyalar talabiga

mos ravishda takomillashgan. Bu tizim kompyuter resurslarini boshqarish, dasturlarni bajarish, fayllarni tashkil qilish va foydalanuvchi bilan interaktiv aloqani ta'minlashda markaziy rol o'ynaydi. Ushbu maqolaning maqsadi — Windows operatsion tizimining asosiy arxitekturasi, funksiyalari va xavfsizlik jihatlarini chuqur tahlil qilish, shuningdek, uning ijobiy va salbiy tomonlarini ko'rsatish orqali tizimni samarali foydalanish bo'yicha tavsiyalar berishdir.

Asosiy qism

Microsoft Windows arxitekturasi ichida bir nechta qatlam va komponentlar mavjud bo'lib, ularning har biri tizimning ishlashini ta'minlaydi. Eng markaziy qism — yadroviy modul (kernel) bo'lib, u apparat resurslari (protessor, xotira, disk va h.k.) bilan bevosita aloqada bo'ladi. Windows kernel-mode (yadro rejimi) va user-mode (foydalanuvchi rejimi) tartibini qo'llaydi: ko'p hollarda boshqaruv, drayverlar va tizim xizmatlari kernel rejimida ishlaydi, foydalanuvchiga ko'rinadigan dasturlar esa user rejimida.

Windows tizimida fayl va papkalar bilan ishlash uchun NTFS (New Technology File System) asosiy fayl tizimi hisoblanadi. NTFS keng imkoniyatlarga ega: katta hajmli bo'limlarni qo'llab-quvvatlash, faylga ruxsatlar belgilash, disk kvotalari, jurnal yuritish, shuningdek fayl darajasida shifrlash imkonini beruvchi EFS (Encrypting File System) funksiyasini taqdim etadi. Bundan tashqari, zamonaviy server muhitlarida (masalan, server versiyalarida) ReFS (Resilient File System) kabi fayl tizimlari ham qo'llaniladi, ular katta hajmdagi ma'lumotlarni boshqarish va ma'lumotlarni himoya qilishda qulaylik beradi.

Foydalanuvchi interfeysi (GUI) orqali Windows o'zining qulayligi bilan ajralib turadi: ish stoli, oynalar, Windows Explorer orqali papka va fayllarni boshqarish, vazifalar paneli va menyular tizimi foydalanuvchiga intuitiv va tezkor ishlash imkonini beradi. Bu GUI yondashuvi kompyuter bilimlari bo'yicha ta'lim olayotgan yoshlar va keng foydalanuvchilar uchun tushunarli va qulay muhit yaratadi.

Xavfsizlik masalasida Windows bir qancha birliklarni taklif qiladi. Masalan, EFS orqali fayllar shifrlanishi, foydalanuvchi hisoblari (turli ruxsat darajalari), tizim xizmatlari va avtomatik yangilanishlar orqali himoya choralari ko‘riladi. Biroq, texnik jihatdan ochiqligi va keng qo‘llanilishi tufayli Windows tizimlari kiber tahdidlarga, zararli dasturlar, rootkitlar yoki apparat darajasidagi hujumlarga moyil bo‘lishi mumkin. Masalan, yadroviy darajadagi xotira boshqaruvi va kernel objektlariga hujumlar xavfi doimo mavjud.

Zamonaviy Windows versiyalari (Windows 10, Windows 11) foydalanuvchilar uchun moslashuvchanlik va yangilanishlar bilan ta‘minlangan.

Biroq, masalan, 2025-yilda Microsoft Windows 10 ga bo‘lgan qo‘llab-quvvatlashni to‘xtatganini e‘lon qildi, bu esa eski versiyalardan foydalanayotgan foydalanuvchilar uchun xavfsizlik yangilanishlari yo‘qligini anglatadi, ya‘ni operatsion tizim xavfsizlik jihatdan zaiflashi mumkin.

Shu jihatlar asosida, Windows operatsion tizimi talaba, muhandis yoki oddiy foydalanuvchi uchun qulay va keng imkoniyatli platforma bo‘lishiga qaramay, tizimning to‘liq xavfsizligini ta‘minlash foydalanuvchining o‘ziga ham bog‘liq — zamonaviy versiyalardan foydalanish, antivirus va shifrlash funksiyalaridan foydalanish, va muhim ma‘lumotlarni muntazam zaxira qilish lozim.

Imkoniyatlar (O) hamda Tahdidlar (T): Tizimning keng qo‘llanilishi, yangi xizmatlar va bulut infratuzilmalari bilan integratsiya — imkoniyatdir. Biroq kiberxavfsizlik xatarlari, eski versiyalarni yangilamaslik — tahdiddir.

SWOT TAHLILI

Kuchli tomonlar (S)	Zaif tomonlar (W)

Keng qo‘llaniladigan va tanilgan interfeys, ko‘p dasturiy ta‘minot (kompatibilnost)	Resurs talabchanligi — eski yoki kam quvvatli kompyuterlarda sekin ishlashi mumkin
NTFS/EFS kabi rivojlangan fayl tizimlari, fayl shifrlash va ruxsatlar tizimi bilan yuqori darajadagi ma‘lumotlar himoyasi	Agar tizim yangilanmasa — xavfsizlik hujumlari va malware xavfi mavjud
Multitasking, keng apparat va qurilmalar bilan moslik, tarmoq va server imkoniyatlari	Ayrim eski versiyalar endi yangilanmaydi, yangilanishlar tugashi bilan qo‘llab-quvvatlash to‘xtaydi
Zamonaviy GUI va qulay foydalanuvchi tajribasi, ta‘lim va kundalik foydalanish uchun moslik	Foydalanuvchining noto‘g‘ri sozlamalari yoki ehtiyotkorlik qilmasligi tufayli ma‘lumotlar xavfsizligi buzilishi mumkin

Xulosa

Microsoft Windows operatsion tizimi zamonaviy kompyuterlar va foydalanuvchilar uchun qulay, mos va kuchli platforma hisoblanadi. Uning arxitekturasi, kernel-mode va user-mode tizimi, NTFS/ReFS fayl tizimlari, fayl shifrlash va keng dasturiy qo‘llab-quvvatlash kabi imkoniyatlari tizimni keng qamrovli va ishonchli qiladi. Biroq, operatsion tizimdan maksimal foyda olish va xavfsizlikni ta‘minlash uchun foydalanuvchi zamonaviy versiyalardan foydalanishi, xavfsizlik choralari ko‘rishi hamda ma‘lumotlarni muntazam zaxiralashi lozim.

Windows tizimi — nafaqat kundalik foydalanish, balki ilmiy, ta‘limiy va professional darajadagi kompyuter ishlari uchun mos va kuchli muhit. Agar talaba yoki dasturchi bo‘lsangiz, uning imkoniyatlaridan to‘liq foydalanish uchun tizim arxitekturasi, fayl tizimlari va xavfsizlik xususiyatlarini chuqur o‘rganishingiz tavsiya qilinadi.

Foydalanilgan adabiyotlar va manbalar

1. Adabiyotlar: SWIFT. Understanding SWIFT: An Introduction to the Global Payment System. SWIFT Publishing, 2022.
2. Bank for International Settlements. Cross-border Payment Systems and SWIFT: Efficiency and Challenges // BIS Working Papers No. 876. – 2021.
3. Raximov A. Xalqaro to'lov tizimlari va ularning iqtisodiy samaradorligi. – Toshkent: Iqtisodiyot, 2020. – 145 b.
4. Xudoyberdiyev S., Karimova N. SWIFT tizimi va O'zbekiston moliya sektoridagi roli // Moliyaviy tahlil jurnali. – 2021. – №4. – B. 78-85.
5. Karimov M. Xalqaro to'lov tizimlarining samaradorligini oshirishda SWIFTning o'rni // Iqtisodiyot va moliya. – 2022. – №6. – B. 120-127.
6. Toshmurodov Sh., Yuldasheva G. SWIFT tizimida raqamli texnologiyalar va ularning xalqaro savdodagi ahamiyati // O'zbekiston moliyaviy sharhi. – 2023. – №3. – B. 95-103.
7. Usmonov O. O'zbekiston bank tizimida SWIFT tizimining joriy etilishi va samaradorligi // Bank ishi va moliyaviy texnologiyalar. – 2021. – №2. – B. 66-72.
8. Qodirov B. Xalqaro moliyaviy operatsiyalarda SWIFT tizimi orqali amalga oshiriladigan o'tkazmalarning xususiyatlari. – Toshkent: Moliya va iqtisodiyot nashriyoti, 2022. – 132 b.