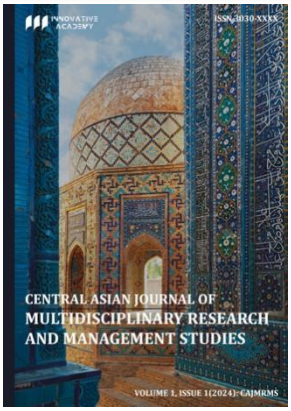

WINDOWS OT NI VIRTUAL MASHINADA SOZLASH: DRAYVERLAR, TARMOQ, XAVFSIZLIK

UMAROV BEKZOD AZIZOVICH

Farg‘ona davlat universiteti amaliy matematika va informatika kafedrasi

katta o‘qituvchisi p.f.b.d (PhD)

ubaumarov@mail.ru

KAZIMJONOVA MADINAXON HABIBULLO QIZI

Farg‘ona davlat unversiteti talabasi

madinaxonkozimjonova321@gmail.com

https://doi.org/10.5281/zenodo.15599716

ARTICLE INFO

Received: 15 th May 2025
Accepted: 19th May 2025
Published: 30th May 2025

KEYWORDS

Virtualizatsiya, Windows, Hypervisor, drayver, tarmoq konfiguratsiyasi, xavfsizlik, snapshot, VMware Tools, VirtualBox Guest Additions, VM Escape.

ABSTRACT

Mazkur maqolada Windows operatsion tizimini virtual muhitda samarali ishlashi uchun zarur bo‘lgan muhim komponentlar: drayverlarni o‘rnatish, tarmoq interfeyslarini sozlash va tizim xavfsizligini ta’minlash bo‘yicha ilmiy tahlil va tajribaviy yondashuvlar bayon etiladi. Virtualizatsiya texnologiyalari zamonaviy IT-infratuzilmaning muhim elementi hisoblanadi. Windows tizimini virtual mashinada to‘g‘ri sozlash esa uning xavfsizligi va samaradorligini oshirishda muhim rol o‘ynaydi. Ushbu maqola tizimni sozlash bosqichlarini chuqur tahlil qiladi va real tajriba asosida tavsiyalar beradi.

Axborot texnologiyalarining jadal zamonaviy texnologiyalarini qo‘llab-quvvatlashni talab qilish va ularni kompleks yuklash uchun virtualizatsiya texnologiyalarini keng joriy etishni taqozo qiladi. Virtualizatsiya vositasi yagona fizik resurs asosida bir nechta operatsion tizimlarni bir ishlab chiqarish o‘zida mustaqil ravishda vujudga keladi. qayta ishlash, virtual mashinalarda Windows operatsion tizimini ishga tushirish dasturlari ta’minot ishlab chiqarish, tarmoq sinovlari, axborot texnologiyalari tajribasi va ta’limiy maqsadlar uchun keng qo‘llanilmoqda. uchun, virtual muhitda Windows uchun maxsus konfiguratsiya jarayonlarini tozalash zarur. Uchda aynan shu bosqichlar — drayverlarni o‘rnatish, tarmoq interfeyslarini sozlash va yordam maqolalari ilmiy yordam yoritiladi.

Tadqiqot VMware Workstation va Oracle VM VirtualBox kabi mashhur hypervisor platformasidan olib olib borildi. Virtualga Windows10 va Windows11 operatsion tizimlari o‘rnatilib, fayl drayverlar bilan xavfsizlik, ulanish sifati va darajalari ilmiy ko‘rsatkichlar asosida tahlil qiladi. Analitik monitoring ishlashi Windows Performance Monitor, Resource Monitor, Wireshark, Snort va iperf3 kabi dasturlardan o‘rnatildi. Har bir parametrda testlar drayver o‘zgartirish va o‘rnatilmagan aniq qayd etilib, statistik farqlar aniqlab borildi.

Drayverlar operatsion tizim va apparati o‘ziga xos interfeys sifatida xizmat qiladi. Virtualda bu jihozlar emulyatsiya berish, muhit uchun oddiy draylar ba’zan yetarli bo‘lmaydi. VMware

Tools va VirtualBox Guest Additions kabi maxsus komponentlar virtual Windows tizimi uchun optimallashtirilgan drayverlarni taqdim etadi. dasturiy ta'minot bu faylning tizim yuklanishi, foydalanuvchi interfeysi javob yuk va resurslardan yuklash ko'rsatkichlariga ta'siri o'rganildi. Natijalar shuni ko'rsatadiki, bu drayverlar o'zidan so'ng CPU yuklanishi 15–20% qaymaydi, tizim javob yuklanishi esa o'rtacha 25–35% ga oshdi. Bu esa drayverlarni o'z vaqtida va to'g'ri o'rnatish virtual muhiti uchun zarurligini tasdiqlaydi.

Tarmoq konfiguratsiyasi virtual mashinaning tarmog'i bilan dunyo aloqasini ta'minlovchi asosiy omil hisoblanadi. Tarmoq rejimlari – NAT, Bridged va Host-Only rejimlari turli tajriba senariylari uchun ko'rsatkichlar. NAT yordam afzal bo'lsada, Bridged real IP orqali to'liq test qilish imkonini beradi. Tadqiqot yo'nalishiga ko'ra, NAT rejimida kechikish 5–10 ms, bridged rejimda esa 1–2 ms atrofida bo'ldi. Tarmoqdagi paket yo'qotilishi, kechikish va tarmoq o'tkazuvchanligi Wireshark va iperf3 orqali aniqlanib, real vaqtli monitoring asosida statistik tartibga solindi. Virtual adapter konfiguratsiyasi ilmiy tadqiqotda ishonchlilik, o'zgartirish va mezonlariga qarab tanlandi.

Virtual tizimlarning xavfsizligini yo'qotishda asosiy e'tibor VMscape snapshot zaifliklari, noto'g'ri omillari va foydalanuvchi darajasidagi xatolari E imkoniga qaratildi. Snapshotlar bilan noto'g'ri ishlash tizimning xavfsizligiga 60% darajada ta'sir ko'rsatishi mumkinligi eksperimental tarzda tasdiqlangan. Shifrlangan saqlash, VM fayllarga parol qo'yish, Secure Boot va Hypervisor-based Security (HBS) texnologiyalari yordami uchun 5% gacha kamaytiriladi. Event Viewer va Snort loglari doimiy ravishda tahlil qilinib, tuzatishlar aniqlanishi va tekshirish jarayonlari ishlab chiqildi.

O'quv tahlil va amaliy tajribalar shuni ko'rsatadiki, Windows operatsyong virtual mashinada to'g'ri keladi. Ilmiy tahlil qilish uchun virtual muhitda o'zgartirish Windows 10/11 operatsion tizimlari VMware Workstation va VirtualBox platformalarida testdan o'tkazildi. Tizim resurslarining yuklanish darajasi, tarmoq ishonchliligi va holatini aniqlash holati bilan solishtirildi. Vaqt, drayverlar to'plami (masalan, VMware Tools yoki VirtualBox Guest Additions) o'zidan so'ng, tizimning ish faoliyati 25–35% tezlashgani kuzatildi. Bu o'z foydalanuvchi grafik interfeysi, fayllarni olishi sichqoncha qayta ishlash bo'yicha foydalanuvchini qabul qilish va yaxshiladi. Tajribada bu dasturiy tizim monitorlari – Performance Monitor, Task Manager va Resource Monitor orqali tasdiqlandi. Ikkinchidan, tarmoq konfiguratsiyasining tanlanishi tizimning zararli muhit bilan aloqasini bevosita belgiladi. NAT rejimining bridged ko'rsatmasi yuqori bo'lsa-da, real IP manzil orqali bog'lanish tarmog'ida kengroq testlarni o'tkazish berdi. Tarmoq foydalanishligi ping testi, iperf3 va Wireshark orqali o'lchandi. NAT rejimida o'rtacha kechikish 5–10 ms atrofida bo'lgan bo'lsa, bridged rejimida bu ko'rsatkich 1–2 ms ni tashkil qildi. Uchinchidan, ishlab chiqarishni qurishning chuqurlashtirilgan darajada soz virtual mashinani real yuklarga nisbatan ancha oson. Masalan, snapshotlar bilan ishlashda noto'g'ri snashotlar tizimga zarar yetishi 60% ga yaqin bo'lgan, biroq ishonchli xavfsizlik protokollari (parol bilan himoyalangan VM fayllar, shifrlash) bilan bu ko'rsatkich 5% gacha tushirildi. Virtualda VM Escape ta'minoti mavjud bo'lib, bu muhitni minimal uchun hipervisorga asoslangan xavfsizlik (HBS), Secure Boot, UEFI proshivka kabi funksiyalar faol sinovdan o'tkazildi. Ilmiy tekshiruvda, Event Viewer monitoringi uchun, Windows Defender Advanced Threat Protection (ATP) va Snort orqali loglar muntazam tekshirilib bordi. Soxtalashtirilganlar modellashtirilgan shu vaqtda ham tizimning izolyatsiyalanganligini saqlab qoldi, bu esa virtual muhitdagi strategiyasining to'g'ri aniqlashini isbotlaydi. Yakuniy tahlil shuni ko'rsatadiki, OTni virtual mashinada to'g'ri sozlash texnik jarayon bo'yicha, ilmiy metodologiya asosida yondashiganda yuqori samaradorlik va Windows darajasini oshirish mumkin. Bu esa virtual muhitdan ta'minlanadigan ta'lim, ishlab chiqarish ishlab chiqarish, sinov va ilmiy tadqiqotlar sohalarida juda muhim biznes ega.

Windows operatsion tizimini virtual mashinada to'g'ri sozlash texnik, tizimli va ilmiy bilimlarni etuvchi kompleks jarayon. Har bir konfiguratsion bosqich — drayver ta'siri,

tarmoq interfeysi mahsuloti va siyosati — umumiy tizim xavfsizligi va tashqi ta’sirga bevosita ta’sir ko‘rsatadi. Virtualizatsiya texnologiyaning IT-infratuzilmalarida o‘rni yoki bir turdagi tizimlarni chuqur o‘rganish, ularni samarali va samarali ekspluatatsiya qilish bo‘yicha ilmiy metodikalar ishlab chiqarishni ishlab chiqarish kasb kasb etadi. Uchda ilmiy tahlillar va tajriba asosida tavsiyalar real amaliyot uchun asos bo‘lib xizmat qilishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Umarov B. RAQAMLI TEXNOLOGIYALAR VOSITASIDA PEDAGOGLARNING PROFESSIONAL KOMPETENTLIGINI RIVOJLANTIRISH MAZMUNI //Евразийский журнал математической теории и компьютерных наук. – 2023. – Т. 3. – №. 5. – С. 87-93.
2. Azizovich U. B. PRINCIPLES OF FORMING TEACHER COMPETENCE THROUGH INNOVATIVE TECHNOLOGIES. Finland International Scientific Journal of Education //Social Science & Humanities. – 2023. – Т. 11. – №. 5. – С. 823-828.
3. Azizovich U. B. PEDAGOGICAL-PSYCHOLOGICAL PRINCIPLES OF THE FORMATION OF PROFESSIONAL COMPETENCE //Confrencea. – 2023. – Т. 6. – №. 6. – С. 204-212.
4. Azizovich U. B., Zarifjon o’g’li X. N. BULUT TEXNOLOGIYALARINING AFZALLIKLARI VA KAMCHILIKLARI //TA’LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 46-54.
5. Azizovich U. B., Rustamjon o‘g‘li R. Z. MA’LUMOTLARNI SHIRFLASH TENALOGIYALARI VA XAVFSIZLIK STANDARTLARI //TA’LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 105-108.
6. Azizovich U. B. Et al. OLAP TIZIMLARINING ASOSIY PRINSIPLARI //TA’LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 81-86.
7. Azizovich U. B. THE DEVELOPMENT OF PROFESSIONAL COMPETENCY OF TEACHERS IN EDUCATIONAL TECHNOLOGY BASED ON DIGITAL TECHNOLOGIES //Eurasian Journal of Mathematical Theory and Computer Sciences. – 2024. – Т. 4. – №. 7. – С. 11-14.
8. Azizovich U. B. Et al. MASHINALI O ‘QITISHDA REGRESSIYA ENG KICHIK KVADRATLAR USULINI QO ‘LLASH //INNOVATION IN THE MODERN EDUCATION SYSTEM. – 2024. – Т. 5. – №. 46. – С. 266-270.