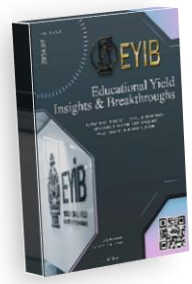
EYIB
EDUCATIONAL YIELD
INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.6 №2
https://eyib.uz



Axborotlarni uzatishda USB qurilmalaridan foydalanish hamda ularni himoyalash usullari

Qaxramonov Elbek Quvondiq o‘g‘li

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, axborot xavfsizligi kafedrasi katta o‘qituvchisi
eljon.mail@gmail.com

Annotatsiya

ushubu maqolada USB qurilmalarni himoyalash undagi ma’lumotlarning xavfsizligini ta’minlash hamda o‘g‘rilash, o‘zgartirish yoki yo‘q qilish xavflarini kamaytirishga qaratilgan harakatlar tahlil etilgan. USB qurilmalardagi kerakli ma’lumotlarni turli xil zararli dasturlar va viruslardan qanday himoyalash kerakligi, ko‘plab foydalanuvchilar uchun muhim amaliyot hisoblanadi. Quyida Windows operatison tizimi misolida USB qurilmalardagi yorliq viruslar va ulardan himoyalanish uchun bir qancha usullarni taklif etilgan.

Kalit so‘zlar: USB yorliq virusi, USB xotira, Internet zararli dasturlari, Antivirus, formatlash, NTFS fayl tizimi, CMD, msconfig.

USB yorliq virusi - bu USB xotira qurilmasini shunday zararlaydiki, uning ichidagi fayllarga kirish imkonsiz bo‘lib qoladi. Bu zararli dastur barcha fayllarni yashirib, ularni xuddi shu nomdagi “yorliq”lar bilan almashtiradi. Bu yorliqlar aslida yolg‘onchi manzil bo‘lib, ishlamaydi va ularga bosish orqali virusni osonlikcha tarqatish mumkin bo‘ladi. Sodda qilib aytganda, USB yorliq virusi - bu bizning fayllarimizni yashiradigan qurt yoki troyan dasturidir. USB qurilmamiz virusga chalinishining ko‘plab sabablari bor. Bu virusning eng yomon tomoni shundaki, uni ikki marta bosganimizdan so‘ng, u ko‘payadi va natijada tizimni jiddiy darajada zararlaydi. Tizim protsessori uzluksiz ishlaydi, bu esa tizimning ish samaradorligini pasaytiradi. Quyidagi ba’zi sabablar orqali USB yorliq virusini yuqtirib olinishi mumkin:

Zararlangan tizimda USB qurilmasining ishlatilishi. Ba’zan USB xotira qurilmasi yorlig‘i virusi bilan zararlangan tizimlar ham uchraydi. Agar siz USBni bunday tizimlardan biriga ulasangiz, u zararlanishi mumkin. USB xotiradagi fayllar yashirinadi, so‘ngra virus boshqa tizimlarga ham tarqaladi. Flesh xotira yorlig‘i virusini olib tashlash uchun siz bu sababni puxta bilishingiz lozim.

Internet zararli dasturlari. Ma’lumki, bu zararli dasturiy ta’minotlar har kuni dunyoning turli burchaklaridagi tizimlarga yuqib bormoqda. Bu USB va boshqa xotira qurilmalarining zararlanishining asosiy sabablaridan biridir. Fleshkadan yorliq virusini

olib tashlashda bu holatni albatta hisobga olish lozim. Ushbu muammoni hal qilish uchun fleshka yorliq viruslarini samarali tozalaydigan sifatli vositaga har doim muhtojdir.

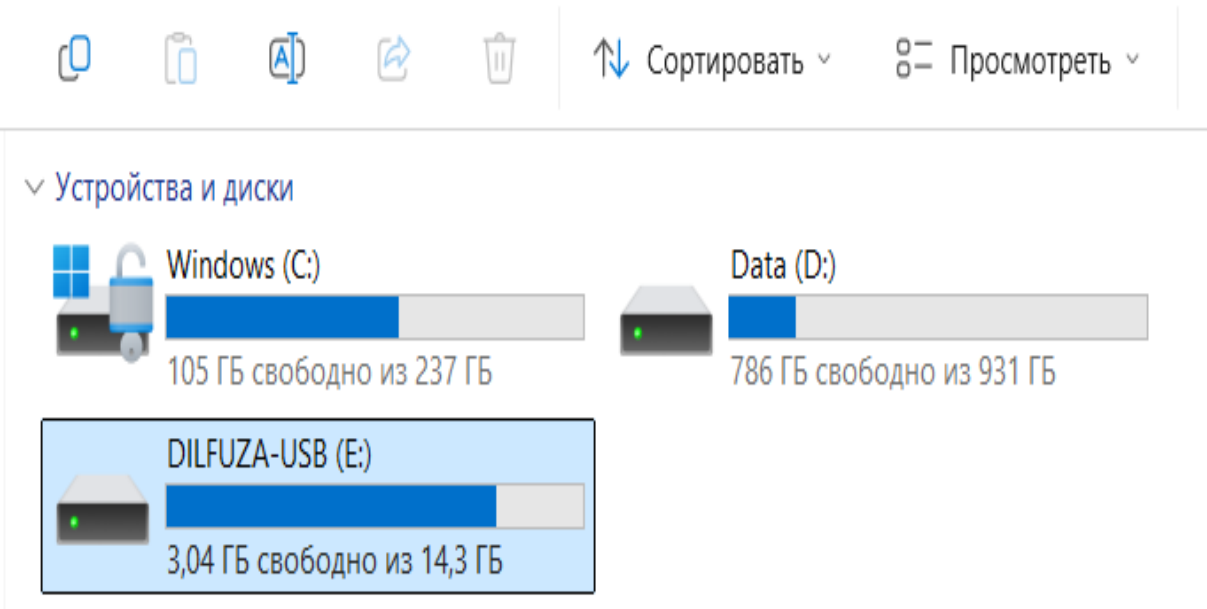
Boshqa zararlangan USB orqali. Agar USB xotira qurilmasini istalgan manbadan oldigan bo‘lsak, virusni aniqlash va yo‘q qilish uchun uni antivirusda tekshirib ko‘rishimiz lozim. Hech qanday muammoga duch kelmaslik uchun boshqa xotira qurilmalaridan juda ehtiyotkorlik bilan foydalanish tavsiya etiladi. Fleshkadagi yorliq virusini o‘chirish uchun ma’lumotlar uzatilishini nazorat qilish kerak.

Antivirusning faol emasligi. Agarda antivirus dasturining bepul versiyasi bizda mavjud bo‘lsa, fleshkadagi yorliq virusini o‘chirish uchun uni yangilashimiz kerak bo‘ladi. Antivirus dasturlarining bepul versiyalari faqat virusni aniqlaydi, lekin uni butunlay o‘chirmaydi. USB yorliq viruslarini o‘chiruvchi dastur sifatida ishlashi uchun kompyuterda to‘g‘ri antivirus o‘rnatilgan bo‘lishini ta’minlashimiz kerak.

Endi esa yorliq viruslarni USB qurilmalaridan qanday qilib o‘chirish yoki yo‘q qilish usullarini ko‘rib chiqamiz. USB qurilmalardan virusning butunlay olib tashlanganligi haqida ishonch hosil qilish uchun bir qancha usullarni qo‘llash mumkin. Bu usullarning bajarilishi oson bo‘lib, 100% natija kafolatini beradi. Shuningdek, bu kabi muammoni hal qilish uchun internetdan USB yorlig‘idagi viruslarni yo‘qotishning boshqa vositalarini ham topish mumkin.

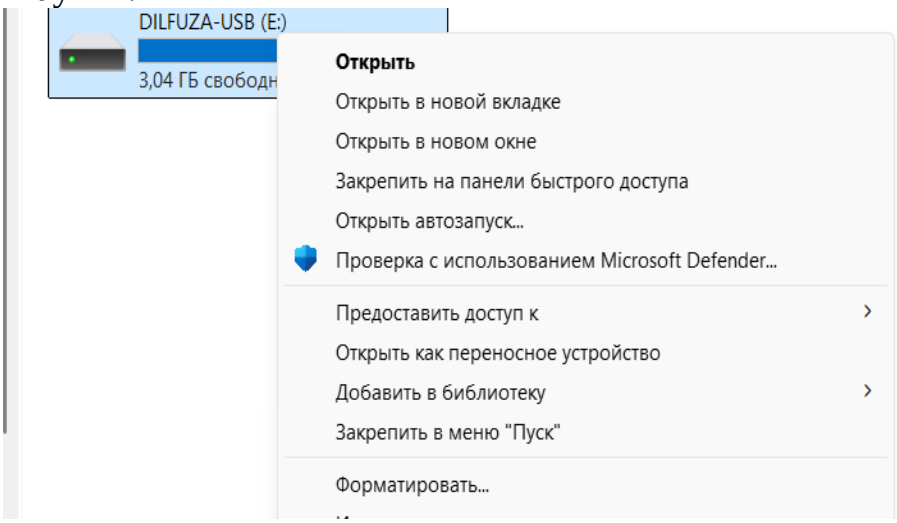
Birinchi usul bu USB qurilmani formatlash. Shubhasiz, bu USBdagi yorliq virusini yo‘q qilishning eng oson usuli. Bu usul sizning talablaringizga mos natija olishingizni kafolatlaydi. Shu maqsadda quyidagi harakatlarni amalga oshirishingiz kerak. Bundan tashqari, u sizga USBda yorliqlar yaratayotgan virus haqida ma’lumot ham beradi.

Demak, Win+E yordamida yoki mening kompyuterim yorlig‘idan fayl boshqaruvchiga kiramiz va bu yerdagi USB qurilmani topamiz:



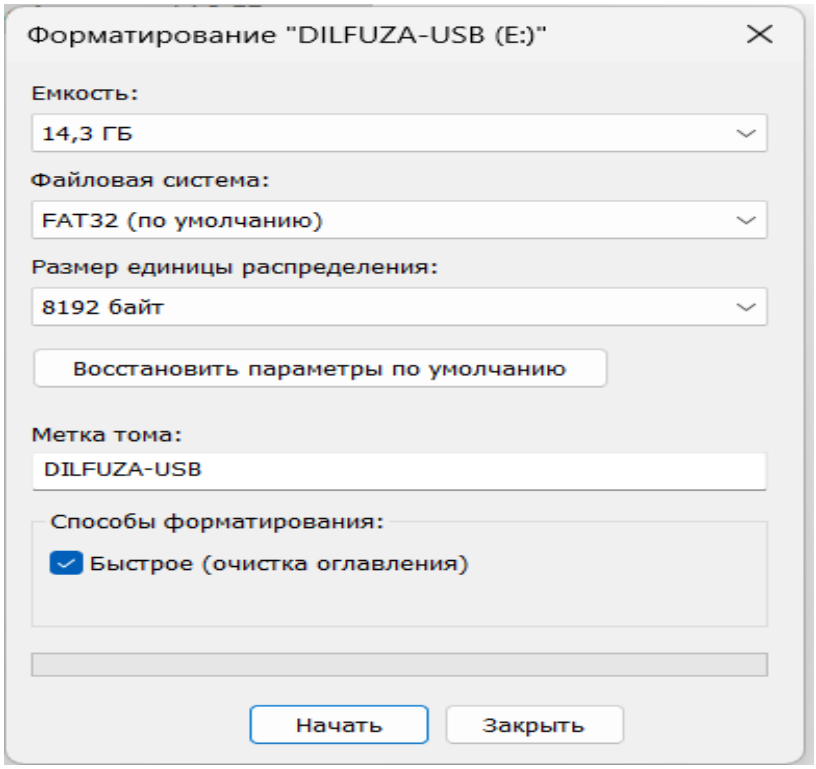
1-rasm. Kompyuterdagi DILFUZA-USB nomli USB qurilmasi

Rasmda ko‘rsatilgan “DILFUZA-USB” deb nomlangan USB qurilmaning ustiga sichqonchaning o‘ng tugmasini bosib, kontekst menyular qatoridan formatlash buyrug‘ini tanlaymiz.



2-rasm. USB qurilmasini formatlashni tanlash

Ushbu amalni bajarayotganda ko‘rsatilgan interfeysda NTFS fayl tizimini tanlab, tezkor formatlash funksiyasini yoqamiz, chunki tezkor formatlash funksiyasi yoqilmasa, formatlashda kechikish bo‘lishi mumkin. Tanlovimizni tasdiqlab, USB qurilmasini formatlash orqali USB qurilmadan yorliq virusini olib tashlash mumkin bo‘ladi.



3-rasm. USB qurilmani formatlashni boshqarish

Ikkinchi usul USB yorlig‘ini viruslardan tozalash vositasidan foydalanish. Virusni to‘liq yo‘q qilish uchun ko‘plab antivirus dasturlaridan foydalanish mumkin. Bu muammoga duch kelgan foydalanuvchilar uchun ishonchli antivirusga ega bo‘lish katta yengillik bo‘lardi. Quyida keltirilgan jarayon USB xotira qurilmasi yorlig‘i virusini o‘chirib tashlash uchun qo‘llanilishi mumkin:

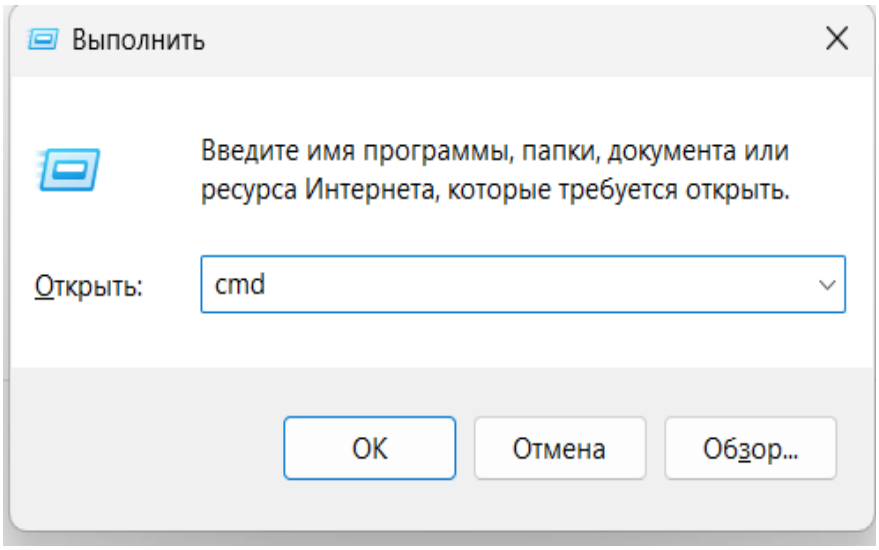
1-qadam. Antivirus dasturini yuklab olish va o‘rnatish.

2-qadam. Dastur o‘rnatilgandan so‘ng uni ishga tushirish va tizimni tekshirishni boshlash.

3-qadam. Antivirus nafaqat yorliq virusini yo‘q qiladi, balki keyingi oynada boshqa viruslarni ham ko‘rsatib beradi.

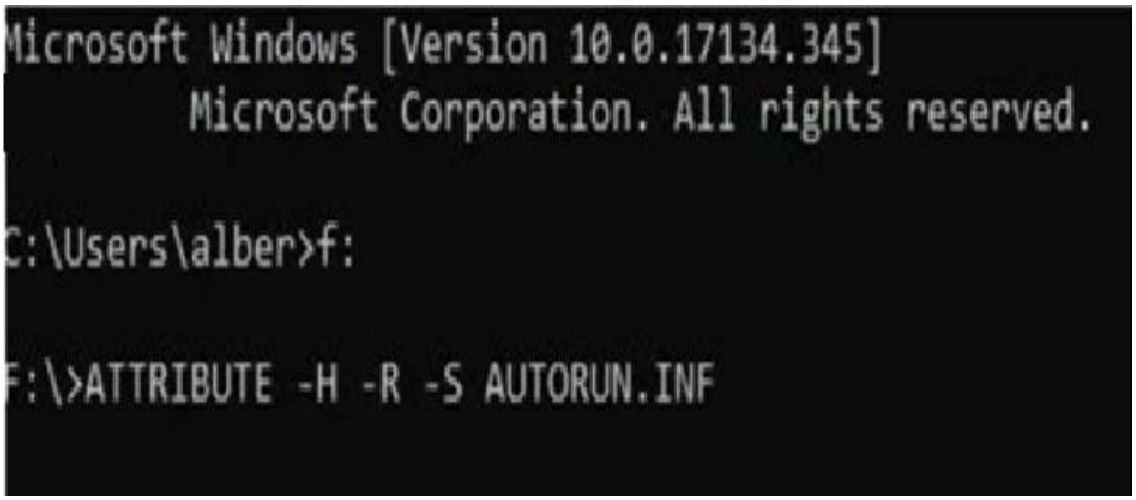
4-qadam. Virusning tizimdan butunlay tozalanganiga ishonch hosil qilish uchun dastur yorliqlarini ham tozalashimiz mumkin.

Uchinchi usul buyurtmalar qatori (CMD) dan foydalanish. Bu CMD yordamida USB yorlig‘i virusini o‘chirishning yana bir muhim va zamonaviy usulidir. Eng quvonarlisi, ushbu jarayon uchun zarur bo‘lgan barcha vositalar USB yorlig‘i virusini o‘chirish uchun tizimga o‘rnatilgan bo‘lib, qo‘shimcha dasturlarni o‘rnatishga hojat yo‘q. Quyida keltirilgan ko‘rsatmalarni bajarish orqali fleshkadagi yorliq virusini CMD yordamida o‘chirib tashlashingiz mumkin. Buning uchun Win+R yordamida CMD ishga tushirib olinadi:



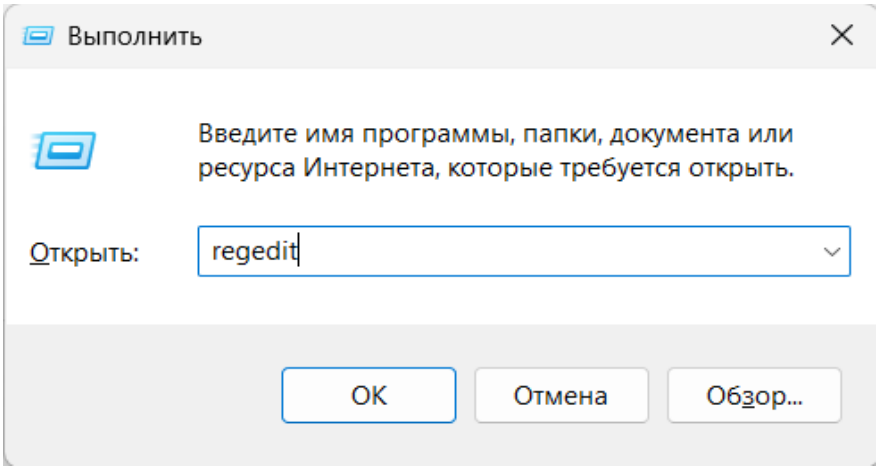
4-rasm. CMD oynasini ochish

Ochilgan CMD oynasining buyruqlar qatoriga kompyuterga ulangan USB qurilmaning manzili ko‘rsatiladi. Masalan, E:, G:, F: vahokazo. Undan keyin esa shu joyga ATTRIBUTE -H -R -S AUTORUN.INF buyrug‘ini kiritib ENTER tugmasini bosamiz va USB qurilma yorliq viruslaridan tozalanadi:



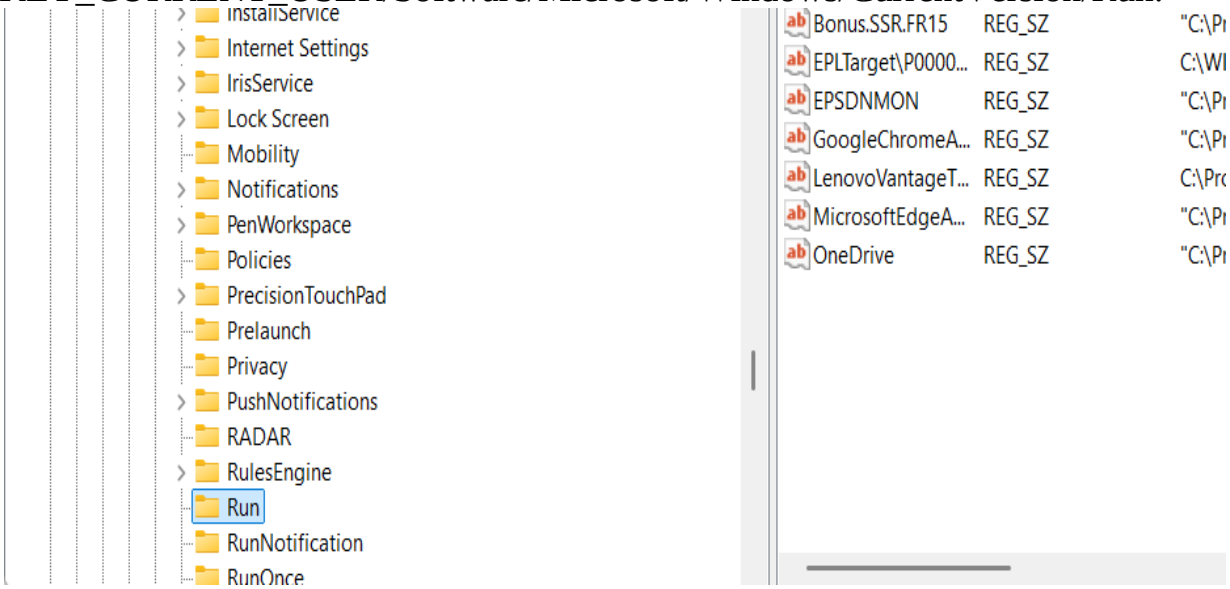
6-rasm. USB ni CMD orqali tozalash usuli

To‘rtinchi usul operatsion tizimning ro‘yxatga olish kitobi muharriri (reestr) dan shubhali kalitlarni olib tashlash orqali amalga oshirish. Bunda Win+R orqali “regedit” buyrug‘i yoziladi:



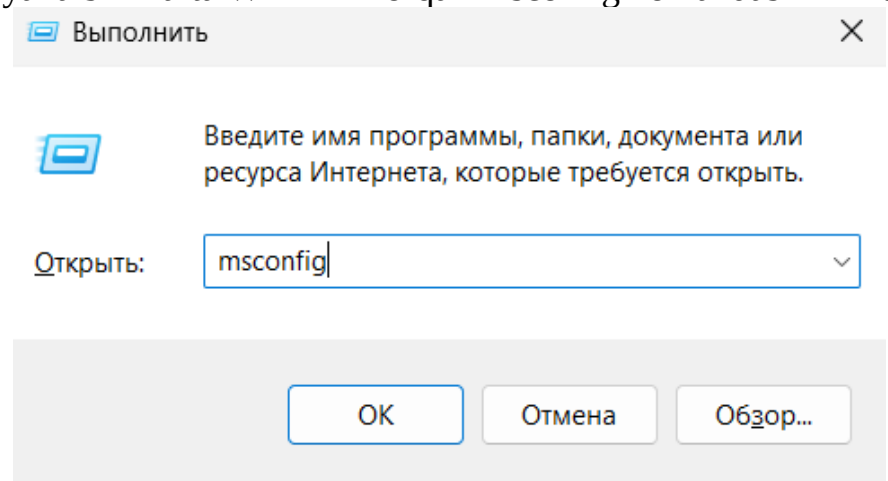
5-rasm. Operatsion tizim reestrini ochish

So‘ngra ochilgan reestr oynasidan quyidagi menyularni tanlaymiz: HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run.



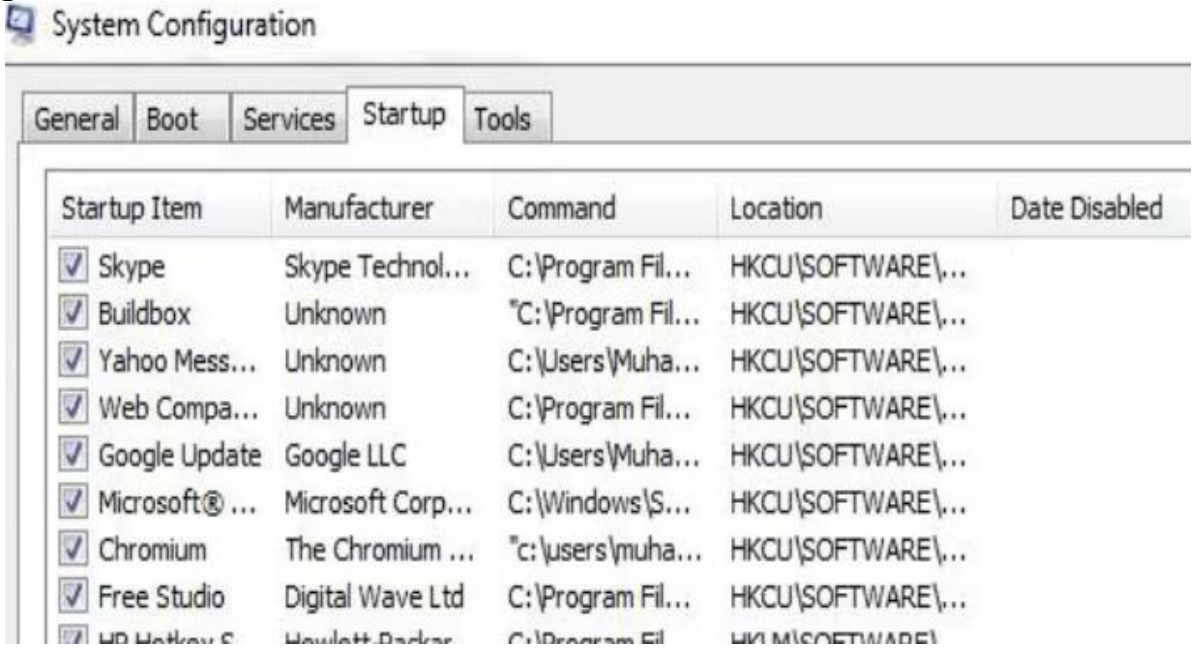
7-rasm. Reestrdan tegishli joyni tanlash.

Keyin yana bir marta Win+R ni orqali msconfig komandasini kiritamiz:



8-rasm. Tizim konfiguratsiyasini ochish

Ushbu oynada ya’ni tizim konfiguratsiyasi oynasidagi avtomatik ishga tushirish qismidan antivirus dasturidan tashqari barcha dasturlarni o‘chirib qo‘yamiz va virusli flesh-diskdan yorliqni olib tashlash uchun OK tugmasini bosib kompyuterni qayta ishga tushiramiz:



9-rasm. Avtomatik ishga tushirish oynasi

Yuqoridagi amallardan keyin agar kerakli ma’lumotlar ham o‘chib ketganligi aniqlansa, qayta tiklovchi dasturlardan foydalangan holda, ularni qayt tiklab foydalanishimiz mumkin bo‘ladi. Masalan Recoverit data recovery dasturi orqali qayta tiklash mumkin.

Foydalanilgan adabiyotlar ro‘yxati

1. G‘aniyev S. K., Karimov M. M., Tashev K. A. Axborot xavfsizligi. Talabalar uchun darslik. Toshkent, 2016.

2. Eshonqulov Sh.U., Qarshiboyev N.A “Axborot xavfsizligi” o‘quv qo‘llanma, Jizzax-2022.

3. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд. 4-е-М: Ленанд, 2015.

4. S.K. G‘aniyev, T.A. Qo‘chqorov Axborot xavfsizligining maxsus vositalari. Ma’ruzalar matni. TATU 2013.

5. Stamp, Mark. Information security: principles and practice / Mark Stamp/ - 2nd ed. ISBN 978-0-4-470-62639-9(hardback)/ QA76.9.A25S69, USA, 2011.

6. Hacking exposed. Web Applications 3. Joel Scambray, Vincent Liu, Caleb Sima. 2010 y.

7. https://hetmanrecovery.com/ru/recovery_news/backup-and-recovery-in-windows-10.htm.

8. https://recoverit.wondershare.com.ru/flashdrive-recovery/usb-shortcut-virus-remover.html.

9. https://www.usbvirus.com/

10. https://www.acronis.com/en-eu/blog/posts/how-to-remove-usb-viruses/

11. https://cyber-star.org/ru/cs-articles/how-to-use-usb-sticks-safely-ru/