# KOMPYUTER VIRUSLARI VA ULARGA QARSHI KURASHISH USULLARI

***Abdullayev Ilhom Xo'jayorovich***
*O'zbekiston-Finlandiya pedagogika instituti*
*Informatika kafedrasi assistent o'qituvchi*
***Gulhayo Berdiyeva Sabir qizi***
*Matematika va informatika yo'nalishi*
***Intizor Mamadova Emonjon qizi***
*Matematika va informatika yo'nalishi*

**Annotatsiya:**Ushbu maqola kompyuter viruslari, ularning qanday ishlashi,viruslarning boshqa zararli dasturlardan farqi hamda ular bilan qanday kurashish haqida, viruslarga qarshi kurashish usullari hamda antivirus dasturlaridan foydalanish, xavfsizlik choralariga amal qilish, ma'lumotlarni zaxiralash va foydalanuvchi madaniyatining ahamiyati muhokama qilinadi. Kompyuter xavfsizligini ta'minlash bugungi kunda nafaqat texnik, balki ijtimoiy va iqtisodiy jihatdan ham dolzarb masala ekanligi ta'kidlanadi. Bundan maqsad foydalanuvchilarda raqamli xavfsizlik bo'yicha ongni shakllantirish va viruslarga qarshi samarali kurashish yo'llarini ko'rsatishdir.

**Kalit so'zlar:**kompyuter viruslari, antivirus, zararli dasturlar, kiberxavfsizlik, himoya usullari.

**Kirish**

Kompyuter virusi – o'lchami bo'yicha katta bo'lmagan, maxsus yozilgan dasturdan iborat bo'lib, u o'zini boshqa dasturlarga «yozib qo'yishi», shuningdek, kompyuterda turli noxush amallarni bajara olishi mumkin. Bunday dastur ishlashni boshlaganda dastlab boshqaruvni virus oladi. Virus boshqa dasturlarni topadi va unga «yuqadi», shuningdek, qandaydir zararli amallarni (masalan, diskdagi fayl yoki fayllarning joylashish jadvalini buzadi, tezkor xotirani «ifloslaydi» va h.k.) bajaradi. Virus o'ziga tegishli amallarni bajarib bo'lgandan

so’ng boshqaruvni o’zi joylashgan dasturga uzatadi. Virus joylashgan dastur odatdagidek ishini davom ettiradi. Tashqaridan dasturning «kasallanganligi» bilinmaydi.

Kompyuter viruslari kompyuter egasini ogohlantirmay va uning istagiga qarshi uning dasturiga “joylashtiriladi” va zaryadlangan faylni navbatdagi qo’yishda ko’payadi.Kompyuter virusi kompyuterning risoladagi ish me’yorini buzadi, ma’lumotlarni o’chirib yuboradi, display (monitor) ekranidagi tasvirni buzadi,hisoblash jarayonini sekinlashtiradi.

Kompyuter virusi — internet orqali suzib yuradigan, kompyuter programmalarini yo‘q qilib, ishlamay qolishiga sabab bo‘ladigan programma. Hozirgi kunda bu viruslarga qarshi Antiviruslar ishlab chiqarilgan. Viruslar haqida dastlabki ma’lumotlar amerikalik T. J. Raynning 1977-yilgi fantastik asarida uchraydi. Bu asarda 7000 kompyuter virusdan zararlanganligi haqida so‘z boradi. Virus ham tuzilishiga ko‘ra dastur, lekin zararli. Hozirda viruslar juda keng klassifikatsiya ega. Ular keng qamrovda faoliyat olib bormoqda. Dunyodagi birinchi virus dasturi 1988-yili Karnell Universiteti aspiranti Robert Moris tomonidan Internet tarmog‘iga joylashtirilgan. Bu virus o‘z faoliyatini Unix operatsion tizimi xato-kamchiliklaridan g‘arazli maqsadlarda foydalanish bilan amalga oshirgan. Robert Moris tuzgan virus juda katta ko‘lamli zarar keltirdi. Robert moris esa uzoq muddatli qamoq jazosiga mahkum etildi, lekin uning nomi bir umrga tarixda qoldi.

Viruslar kompyuterlarda o'zini har xil tutadi. Ba'zi birlari kompyuteringizni kerakmas fayllar bilan to'latsa, yana ba'zilari operativ xotirani ko'p qismini ishlatib, kompyuteringizni qotirib qo'yadi, viruslarning bir qismi esa, kerakli fayllaringizni yoki tizim fayllarini o'chirib sizga zarar yetkazadi. Shulardan saqlanish uchun viruslarning turini bilib olish lozim, ya'ni qaysi virus nima ish qiladi va bundan saqlanish o'z o'zidan kelib chiqadi.

Zararli dasturlarning ko‘p turlari mavjud. Kompyuter viruslari,) qurtlar, troyan otlari, to‘lov dasturi, josuslik dasturlari, reklama dasturlari va o‘chiruvchi dasturlar shular jumlasidandir. Zararli dasturlardan himoya qilish strategiyala ularning turiga qarab farqlanadi, lekin ularning aksariyatini antivirus dasturlari, xavfsizlik devorlarinio‘rnatish, kunlik hujumlarni kamaytirish uchun muntazam himoyalarni qo‘llash, tarmoqlarni bosqindan himoya qilish, muntazam zahira nusxalariga ega bo‘lish va zararlangan tizimlarni izolyatsiya qilish orqali oldini olish mumkin. Zararli dasturlar antivirus dasturlarini aniqlash algoritmlaridan qochish qobilyatiga ega qilib dasaturlanishga harakat qilishmoqda.

Troyanlar (Trojan Horses) – Troyanlar odatda internet orqali tarqaladi. Troyanlar kompyuteringizga o'rnashib olib, dastlab foydali dastur sifatida o'zlarini tanishtiradilar, lekin ularning asl vazifasi foydalanuvchiga noma'lumligicha qoladi. Yashirin ravishda ular o'zlarining yaratuvchisi (cracker – yovuz haker) tomonidan belgilangan harakatlarni amalga oshiradilar. Troyanlar o'z-o'zidan ko'paymaydi, lekin kompyuteringiz xavfsizligini ishdan chiqaradi: troyanlar kerakli ma'lumotlaringizni o'chirib yuborishi, kompyuterdagi ma'lumotlarni kerakli manzilga jo'natishi, kompyuteringizga internetdan ruxsatsiz ulanishlarni amalga oshirishi mumkin.

Chuvalchang viruslar (Worms) – Chuvalchang viruslar o'z nomiga mos ravishda juda tez o'z-o'zidan ko'payadigan viruslardir. Odatda bu viruslar internet yo'li intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xatlar yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular haqiqatan ham kompyuteringizdagi ma'lumotlar va kompyuter xavfsizligiga katta ziyon yetkazadi. Chuvalchang viruslar operatsion tizimning nozik joylaridan foydalanish yoki zararlangan elektron xatlarni ochish yo'li bilan kompyuteringizga o'rnashib olishi mumkin.

Boot sektor viruslari (Bootsector viruses) – Bu viruslar kompyuterning ishlay boshlashi (загрузка) uchun foydalaniladigan qattiq diskning maxsus qismini ishdan

chiqaradi. Bu virus kompyuteringizni zararlaganidan keyin, kompyuter ishlamay qolishi mumkin. Odatda floppy disklar orqali tarqaladi.

Makro viruslar (Macro viruses) – O'zlarining tarqalishi uchun boshqa bir dasturning makro dasturlash tilidan foydalanadigan viruslardir. Ular odatda Microsoft Word yoki Excel hujjatlarini zararlaydi.

Operativ xotirada yashovchi viruslar ( Memory Resident Viruses ) — Bu viruslar kompyuteringizning operativ xotirasida (RAM) yashaydi va zararli harakatini amalga oshiradi. Odatda ularni ishga tushirish uchun boshqa virusdan foydalaniladi. Ular o'zlarining ishga tushishga yordam bergan virus yopilgan bo'lsa ham kompyuter xotirasida qoladi, shuning uchun ham ularga yuqoridagi nom berilgan.

Rootkit viruslari (Rootkit viruses) – Rootkitlar viruslar orasida o'zlarining eng xavfliligi va yashirinishga ustaligi bilan alohida ajralib turadi. Rootkitlar kompyuteringizni yovuz hakerlar tomonidan qo'lga olinishi uchun foydalaniladi.

Ba'zi rootkitlarni antivirus dasturlari ham aniqlay olmaydi, chunki ular o'zlarini operativ tizim fayllari sifatida ko'rsatishadi. Rootkitlar odatda troyanlar tomonidan kompyuteringizga o'rnatiladi.

Antivirus dasturlar o’zidan-o’zi ishlamay qoladi, ya’ni bloklanib qolishi mumkin, kompyuter ishlashi sezilarli darajada sekinlashadi, protsessor(CPU) yoki tezkor xotira(RAM) maksimal darajada ishlashga harakat qiladi, har xil reklamali banerlar, video roliklar o’zidan-o’zi paydo bo’lishni boshlaydi, doimiy ishlab turiladigan fayllar ochilmay qoladi, fayl tiplari o’zgarib qolishi mumkin, siz o’rnatmagan dasturlar o’rnatib qolinadi, fayllar yo’q bo’lib qoladi, internetga ulanishda muammolar paydo bo’ladi yoki internet ishlashi ancha sekinlashadi, kompyuter o’zidan-o’zi o’chib qolishi, qayta yuklanishi yoki o’chirish buyrug’ini bersangiz, o’chmasligi ham mumkin, fayl va papkalar shiflranib qoladi.

Himoyalanishning asosiy texnologik sxemasi. Himoyalanishning bunday sxemasi quyidagi bosqichlardan iborat:

- yangi dasturiy mahsulotning dastlabki nazorati;

- qattiq diskni bir necha mantiqiy disklarga ajratish;

- rezident revizor (taftishchi) dasturlar bilan davriy ravishda axborot butligini tekshirib turish;

- arxivlashtirish.

Ko'pchilik mashhur fayl va boot-viruslar mavjudligini kirish nazoratining o'zidayoq aniqlash mumkin. Bu jarayon bor-yo'g'i bir necha daqiqani oladi, xolos. Aks holda ko'p vaqt axborotlarni viruslardan tozalashga ketib qoladi. Kirish nazoratini bir nechta marta saralab, maxsus tanlab olingan detektor va fagalardan o'tkazgan ma'qul.

Kompyuterdagi ma'lumotlar va dasturlar ma'lum virus dasturi tomonidan o'chirilib yuborilishi yoki shikastlanishi mumkin. Virus-dasturlari dasturchilar tomonidan tajriba uchun yoki yomon niyatlarda yaratilib, asosan ular quyidagi vositalar orqali Sizning kompyuteringizga kirishi mumkin:

- noma'lum disketadagi ma'lumotlarni o'qish natijasida (hujjat, o'yin va boshqalar);

- internet tarmog'idan ba'zi xil dasturlarni yuklash natijasida;

- elektron-pochta orqali;

- lokal tarmoq orqali;

- noqonuniy ko'chirilgan va tarqatilayotgan dasturlardan foydalanish oqibatida;

Virus dasturlari asosan Assembler dasturlash tilida tuziladi va ular salbiy ta'siri bo'yicha bir nechta guruhga bo'linadi:

1. Sodda viruslar - operativ xotirani band qilib, kompyuterning ishlashi sekinlashtiradi.

2. Maxsus "stels" viruslari, ular joylashishini o'zgartirib turadi va ularni topish ancha murakkab.

3. Ma'lumotlarga o'zgartirish kiritadigan viruslar.

4. Ma'lumotlarni o'chiradigan viruslar.

5. Foydalanuvchining ayrim bir (mahfiy) ma'lumotlarini Internet tarmog'i orqali virusni yaratgan shaxsga yuboradigan viruslar.

Talabalar kundalik hayotda kompyuter xavfsizligini ta’minlash uchun quyidagi oddiy, lekin samarali qoidalarga amal qilishlari lozim.

1. Kuchli va maxfiy parollar ishlatish

• Har bir akkaunt uchun alohida va murakkab parol qo‘llang (harflar, raqamlar va belgilar aralashgan).

• “123456”, “password” yoki tug‘ilgan sanani ishlatishdan saqlaning.

• Iloji bo‘lsa, ikki bosqichli autentifikatsiya (2FA) yoqing.

2. Antiviral dasturdan foydalanish

• Ishonchli antivirus (kabi: Kaspersky, Bitdefender, Windows Defender) o‘rnating.

• Antivirusni doim yangilab boring va vaqti-vaqti bilan tizimni to‘liq skanerlashni unutmang.

3. Yangilanishlarni e’tibordan chetda qoldirmaslik

• Windows, Mac yoki boshqa OS yangilanishlarini doimiy o‘rnatish zarur. Ular ko‘pincha xavfsizlik yamoqlarini o‘z ichiga oladi.

4. Shubhali havolalar va fayllardan ehtiyot bo‘lish

• Email, Telegram, Instagram yoki boshqa joylarda berilgan noma’lum havolalarni bosmang.

• Fayl yuklab olayotganda, uning manbasi ishonchli ekaniga ishonch hosil qiling.

5. Ommaviy Wi-Fi tarmoqlarida ehtiyot bo‘lish

• Ochiq Wi-Fi (kafe, universitet) orqali shaxsiy ma’lumotlar yubormang.

• Iloji bo‘lsa, VPN (virtual private network) foydalaning.

6. Zaxira nusxalar qilish

• Muhim hujjat va fayllarni USB fleshka, Google Drive, OneDrive yoki boshqa bulut xizmatlarida saqlang.

• Bu virus, texnik nosozlik yoki qurilma yo‘qolishiga qarshi kafolat bo‘ladi.

7. Qurilmani qulflashni odat qiling

• Kompyuterni tashlab ketayotganda uni qulflang (Windows: Win+L).

• Maxfiy hujjatlar saqlanayotgan bo‘lsa, shaxsiy papkalarni parol bilan himoyalang.

8. Noaniq dasturlarni o‘rnatmaslik

• Torrent yoki noma’lum saytlar orqali olingan dasturlar virus tashuvchi bo‘lishi mumkin.

• Faqat ruxsat etilgan, litsenziyalangan dasturlarni o‘rnating.

9. Brauzer xavfsizligiga e’tibor

• Brauzer kengaytmalarini tekshirib turing, keraksiz yoki noma’lumlarini o‘chirib tashlang.

• HTTPS bo‘lmagan saytlar orqali shaxsiy ma’lumot kiritmang.

10. Axborot xabardorligini oshirish

• O‘zingizni va do‘stlaringizni kiberxavfsizlik haqida xabardor qilish — eng kuchli himoya. Kompyuter viruslari bugungi kunda juda muhim va dolzarb muammo hisoblanadi. Raqamli texnologiyalar keng ommalashgan sari, kiberxavfsizlik tahdidlari, xususan viruslar ham ko‘payib bormoqda. Quyida bu muammo nechog‘lik jiddiy ekanini ko‘rsatadigan asosiy jihatlar keltirilgan:

1. Shaxsiy ma’lumotlar xavfi

• Viruslar yordamida xakerlar parollar, bank kartalari ma’lumotlari, shaxsiy fayllar va hattoki kamerani nazorat qilish imkoniga ega bo‘lishi mumkin.

• Ayniqsa, talabalar va yosh foydalanuvchilar oddiy firibgarliklarga tezda uchrashi mumkin.

2. Tashkilot va davlat darajasidagi xatar

• Katta korxonalar va davlat idoralari ham viruslar sabab millionlab dollar zarar ko‘radi.

• Masalan, ransomware (fidyega olingan fayllar) viruslari butun tizimlarni ishdan chiqaradi va foydalanuvchidan pul talab qiladi.

3. Viruslar tobora aqlli va murakkab bo‘lmoqda

• Zamonaviy viruslar sun’iy intellekt, avto-yashirish va o‘zini yangilab olish kabi imkoniyatlarga ega.

• Ular ko‘pincha foydalanuvchi sezmaydigan tarzda ishlaydi.

4. Ommaviy tarqalish tezligi

• Internet, fleshka, elektron pochta va ijtimoiy tarmoqlar orqali viruslar bir necha soniyada butun tizimlarga tarqalishi mumkin.

• Masalan, USB orqali tarqaladigan viruslar hamon eng keng tarqalganlardan biri.

5. Ijtimoiy muhitga ta’siri

• Viruslar nafaqat texnik zarar, balki ta’lim, sog‘liqni saqlash, moliya tizimi kabi sohalarga ham tahdid soladi.

• Dars materiallari, tibbiy yozuvlar yoki moliyaviy hisob-kitoblar o‘chib ketishi jiddiy oqibatlarga olib keladi.

**Xulosa:**

Kompyuter viruslari – bu shunchaki texnik nosozlik emas, balki jamiyat, iqtisodiyot va shaxsiy xavfsizlikka tahdid soluvchi muammo. Shu sababli har bir foydalanuvchi, ayniqsa talabalar, kiberxavfsizlik qoidalariga rioya qilishni o‘rganishi shart.Kompyuter viruslari zamonaviy axborot texnologiyalari davrida eng dolzarb va xavfli muammolardan biri hisoblanadi. Ular foydalanuvchi ma’lumotlarini yo‘qotish, shaxsiy hayotga aralashish, moliyaviy zarar yetkazish va butun tizimlarni ishdan chiqarish kabi salbiy oqibatlarga olib kelishi mumkin. Viruslar tobora murakkab va aqlli shakllarga ega bo‘lib, ular bilan samarali kurashish uchun har bir foydalanuvchi kompyuter xavfsizligi qoidalariga amal

qilishi zarur.Viruslarga qarshi kurashishda ishonchli antivirus dasturlaridan foydalanish, operatsion tizim va dasturlarni muntazam yangilab borish, shubhali fayllar va havolalardan ehtiyot bo‘lish muhim rol o‘ynaydi. Shuningdek, muhim ma’lumotlarni zaxiralash va foydalanuvchi madaniyatini oshirish virus tahdidlariga qarshi samarali himoya vositasidir.Umuman olganda, kompyuter xavfsizligini ta’minlash — bu har bir foydalanuvchining mas’uliyatli yondashuvi va texnologiyalar bilan ongli ishlash madaniyatiga bog‘liq. Faqat shunda biz viruslar bilan samarali kurasha olamiz.

## FOYDALANILGAN ADABIYOTLAR:

1. Andreyev A. V. “Kompyuter xavfsizligi asoslari”, Toshkent, 2020.
2. Kasperskiy laboratoriyasi. “Antivirus texnologiyalari va kiberxavfsizlik”, Moskva, 2022. www.kaspersky.ru
3. Stallings W. “Computer Security: Principles and Practice”, Pearson Education, 4th Edition, 2020.
4. Tanenbaum A. S. “Modern Operating Systems”, Prentice Hall, 4th Edition, 2015.
5. Abdullaev I. H., Anarbaevna E. K. The Role of Computers in Modern Education //Journal of science, research and teaching. – 2024. – T. 3. – №. 2. – C. 51-53.
6. T. J. Ryan. “The Adolescence of P-1”, Science Fiction Novel, 1977.
7. Microsoft Support Center. “Windowsda xavfsizlik sozlamalari”. support.microsoft.com
8. Norton by Symantec. “Cyber Threats and Antivirus Protection Overview”, 2021. www.norton.com
9. Dr.Web Antivirus. “Zararli dasturlar haqida ma'lumot”, Doctor Web Ltd., 2023. www.drweb.com.
10. McAfee. “Understanding and Fighting Malware Threats”, McAfee Security White Papers, 2022.