

ANTIVIRUSLAR VA ULARNING TURLARI. KOMPYUTER VIRUSLARI

Mamatmurotov Rufatbek Sherzod o'g'li,

Termiz davlat pedagogika instituti o'qituvchisi,

rufatmamatmurotov@gmail.com

Saidmurodova Malika

Termiz davlat pedagogika instituti talabasi,

malikasaidmurodova@gmail.com

Shog'dorova Barno

Termiz davlat pedagogika instituti talabasi,

barnoshogdorova@gmail.com

Izoh: kompyuter viruslari – bu zararli dasturlar bo'lib, ular kompyuterga yashirincha kirib, turli xil zarar yetkazadi. masalan, fayllarni buzadi, o'chiradi, kompyuterni sekinlashtiradi yoki maxfiy ma'lumotlarni o'g'iraydi. bu viruslar ko'pincha internet, fleshka, elektron pochta yoki noma'lum dasturlar orqali tarqaladi. shuning uchun kompyuterni himoya qilish juda muhim. antivirus dasturlari aynan shu vazifani bajaradi. ular viruslarni aniqlaydi, zararsizlantiradi yoki karantinga oladi. ba'zi antiviruslar doimiy ravishda kompyuterni nazorat qilib turadi, ba'zilar esa faqat foydalanuvchi tekshiruv o'tkazganda ishga tushadi. Hozirgi kunda ko'plab ishonchli antivirus dasturlari mavjud. masalan: kaspersky, avast, eset nod32, bitdefender va boshqalar. antivirus dasturini doim yangilab turish va ehtiyotkorlik bilan internetdan foydalanish kompyuter xavfsizligini ta'minlaydi.

Kalit so'zlar: kompyuter xavfsizligi, kompyuter viruslari, zararli dasturlar, antivirus dasturlari, fayl virusi, troyan dasturi, makros virusi, boot-sektor virusi, spyware, adware, antivirus turlari, virusdan himoyalalanish, antivirus yangilanishi, real vaqt himoyasi, antivirus skaneri, kaspersky, eset nod32, avast, bitdefender, internet xavfsizligi, kompyuter himoyasi, shaxsiy ma'lumotlar xavfsizligi, karantin funksiyasi, zararli fayllarni aniqlash.

Annotation: Computer viruses are malicious programs that secretly enter a computer and cause various types of damage. For example, they can corrupt or delete files, slow down the computer, or steal confidential information. These viruses often spread through the internet, USB drives, email, or unknown software. Therefore, protecting the computer is very important. Antivirus programs perform exactly this function. They detect viruses, neutralize them, or quarantine them. Some antivirus programs continuously monitor the computer, while others only run scans when the user initiates them. Nowadays, many reliable antivirus programs exist, such as Kaspersky, Avast, ESET NOD32, Bitdefender, and others. Regularly updating the antivirus software and using the internet cautiously ensures computer security.

Keywords: computer security, computer viruses, malicious programs, antivirus programs, file virus, trojan virus, macro virus, boot-sector virus, spyware, adware, types of antivirus, virus protection, antivirus updates, real-time protection, antivirus scanner, Kaspersky, ESET NOD32, Avast, Bitdefender, internet security, computer protection, personal data security, quarantine function, detecting malicious files.

Аннотация: компьютерные вирусы — это вредоносные программы, которые тайно проникают в компьютер и наносят различные виды ущерба. например, они могут повредить или удалить файлы, замедлить работу компьютера или украсть конфиденциальную информацию. эти вирусы часто распространяются через интернет, usb-накопители, электронную почту или неизвестное программное обеспечение. поэтому защита компьютера очень важна. антивирусные программы выполняют именно эту функцию. они обнаруживают вирусы, нейтрализуют их или помещают заражённые файлы в карантин. некоторые антивирусы постоянно контролируют компьютер, а другие запускаются для проверки только по инициативе пользователя. в настоящее время существует много надёжных антивирусных программ, таких как kaspersky, avast, eset nod32, bitdefender и другие. регулярное обновление антивируса и осторожное использование интернета обеспечивают безопасность компьютера.

ключевые слова: компьютерная безопасность, компьютерные вирусы, вредоносные программы, антивирусные программы, файловый вирус, троянский вирус, макровирус, вирус загрузочного сектора, шпионское ПО, рекламное ПО, виды антивирусов, защита от вирусов, обновление антивируса, защита в реальном времени, антивирусный сканер, kaspersky, eset nod32, avast, bitdefender, интернет-безопасность, защита компьютера, безопасность персональных данных, функция карантина, обнаружение вредоносных файлов

Kirish

Axborotning muhimlik darajasi qadim zamonlardan ma'lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo'llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o'qiy olmagan. Asrlar davomida bu san'at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixonasi rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o'n yil oldin hamma narsa tubdan o'zgardi, ya'ni axborot o'z qiymatiga ega bo'ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o'g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug'iladi. Axborotni qayta ishlash sanoatining paydo bo'lishi axborotni himoyalash sanoatining paydo bo'lishiga olib keladi. Xavfsizlikning asosiy yo'nalishlari. Axborot xavfsizligi. Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo'llanilmoqda (iqtisod, fan, ta'lim, xarbiy ish, turli texnologiyalarni boshqarish va x.k.) Iqtisodiy xavfsizlik. Milliy iqtisodda axborotlarni yaratish, tarqatish, qayta ishlash va foydalanish jarayoni hamda vositalarini qamrab olgan Yangi tarmoq vujudga keldi. «Milliy axborot resursi» tushunchasi Yangi iqtisodiy kategoriya bo'lib xizmat qilmoqda. Davlatning axborot resurslariga

keltirilayotgan zarar axborot xavfsizligiga xam ta'sir ko'rsatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakllantirish va uning asosida jahon yagona axborot maydoniga kirib borish natijasida milliy iqtisodimizga turli xildagi zararlar keltirish xavfi paydo bo'lmoqda. Mudofaa xavfsizligi. Mudofaa sohasida xavfsizlikning asosiy ob'ektlaridan bo'lib, mamlakatning mudofaa potentsialining axborot tarkibi va axborot resurslari hisoblanmoqda. Hozirgi kunda barcha zamonaviy qurollar va harbiy texnikalar juda ham kompyuterlashtirilib yuborildi. Shuning uchun ham ularga axborot qurollarini qo'llash ehtimoli katta. Ijtimoiy xavfsizlik. Zamonaviy axborot-kommunikatsiyalar texnologiyalarining milliy iqtisod barcha tarmoqlarida keng qo'llanishi inson psixologiyasi va jamoa ongiga «yashirin» ta'sir ko'rsatish vositalarining samaradorligini yuksaltirib yubordi.

Hozirgi zamonda axborot texnologiyalari hayotimizning barcha sohalariga chuqur kirib bordi. Kompyuter va internet biz uchun ish faoliyatidan tortib, ta'lim, sog'liqni saqlash, hatto kundalik muloqotlarimizgacha juda muhim vositalarga aylandi. Biroq, shu bilan birga raqamli dunyoda yangi tahdidlar ham paydo bo'lmoqda. Kompyuter viruslari va zararli dasturlar global muammo sifatida yuzaga kelib, foydalanuvchilarning shaxsiy ma'lumotlari, tashkilotlarning faoliyati xavf ostida qolmoqda.

Kompyuter viruslari — bu maxfiy va zararli dasturlar bo'lib, ular tizimga kirib, kompyuterning ishlashiga salbiy ta'sir ko'rsatadi, ma'lumotlarni buzadi, o'chiradi yoki o'g'iraydi. Ularning tarqalishi ko'pincha internet, tashqi xotira vositalari (fleshka, DVD), elektron pochta xabarlarini orqali sodir bo'ladi. Viruslar kompyuterni ishdan chiqarishi, ma'lumotlar yo'qolishi yoki maxfiylik buzilishi kabi jiddiy oqibatlariga olib keladi. Shu bois, kompyuterlarni viruslardan himoyalash, ularning zararli ta'siridan saqlanish uchun antivirus dasturlariga ehtiyoj tug'iladi. Antiviruslar zararli dasturlarni aniqlash, bloklash va yo'q qilish uchun mo'ljallangan dasturiy ta'minotdir. Ularning yordamida foydalanuvchilar o'z tizimlarini xavfsiz saqlashi mumkin.

Asosiy qism

Kompyuter viruslari haqida umumiy ma'lumot:

Kompyuter viruslari — bu zararli dasturlar bo‘lib, ular kompyuterga yashirincha kirib, tizim resurslariga zarar yetkazadi. Viruslar o‘zini ko‘paytirish xususiyatiga ega bo‘lib, boshqa fayllarga yoki qurilmalarga o‘tadi. Ularning asosiy maqsadi — foydalanuvchining kompyuteri ishlashini buzish, ma’lumotlarni o‘g‘irlash yoki o‘chirish, tizimni sekinlashtirishdir. Viruslar turli shakllarda bo‘lishi mumkin: fayl viruslari, boot-sektor viruslari, makros viruslari, troyanlar, chervlar, spyware va boshqalar.

Viruslarning tarqalish usullari ham turlicha bo‘lib, eng keng tarqalganlari internetdan yuklab olinadigan noma’lum dasturlar, elektron pochta orqali yuborilgan zararli fayllar, fleshka va boshqa tashqi xotira vositalaridir. Shu sababli, kompyuter foydalanuvchilari ehtiyotkor bo‘lishlari kerak.

Kompyuter viruslarining turlari:

- **Fayl viruslari** — bu viruslar dastur fayllariga birikib, ularni ishga tushirish paytida faollashadi. Ular fayllarni buzishi yoki o‘zgartirishi mumkin.
- **Boot-sektor viruslari** — kompyuterning yuklanish sektorini (boot sector) zararlaydi, natijada tizim ishga tushmasligi mumkin.
- **Makros viruslari** — Microsoft Office kabi dasturlarda ishlaydigan makros funksiyalari orqali tarqaladi va hujjatlarga zarar yetkazadi.
- **Troyan dasturlari** — foydalanuvchini aldash uchun foydali dastur sifatida ko‘rsatiladi, ammo aslida zararli kodlarni o‘z ichiga oladi.
- **Cherv (worm) viruslari** — tarmoqlar orqali o‘z-o‘zini ko‘paytirib, tez tarqaladi va tarmoq resurslarini band qiladi.
- **Spyware va Adware** — foydalanuvchining ma’lumotlarini yig‘ish, maxfiylikni buzish yoki reklama dasturlarini ko‘rsatish uchun mo‘ljallangan.

Antivirus dasturlari va ularning turlari:

Antivirus dasturlari zararli dasturlarni aniqlash, ularni karantinga olish yoki tizimdan tozalash vazifasini bajaradi. Ularning asosiy turlari quyidagilardir:

- **Real vaqt antiviruslari:** doimiy ravishda kompyuterni nazorat qilib, yangi zararli dasturlar paydo bo'lishi bilan ularni bloklaydi.
- **Skaner antiviruslari:** foydalanuvchi talabiga binoan fayllarni va tizimni tekshiradi.
- **Onlayn antiviruslar:** internet orqali ishlaydi va viruslarni aniqlaydi.
- **Oflayn antiviruslar:** internetga ulanmasdan ishlaydigan antiviruslar.
- **Kompleks xavfsizlik paketlari:** antivirusdan tashqari, firewall, spam-filtr va boshqa xavfsizlik vositalarini o'z ichiga oladi.

Antiviruslarning vazifalari va ahamiyati: Antivirus dasturlari viruslarni aniqlash, ularni tizimdan olib tashlash, karantinga olish va yangi viruslarga qarshi himoya qilish uchun mo'ljallangan. Zamonaviy antiviruslar viruslar bazasini doimiy yangilab boradi, shuningdek, noma'lum zararli dasturlarni xatti-harakatlari asosida aniqlash imkoniyatiga ega. Antiviruslar yordamida kompyuter foydalanuvchilari o'z tizimlarini himoya qilib, muhim ma'lumotlarni yo'qotishdan, shaxsiy ma'lumotlarning o'g'irlanishidan va tizim ish faoliyatining buzilishidan saqlanishlari mumkin.

- Viruslardan himoyalaniish bo'yicha tavsiyalar:
- Antivirus dasturini doimiy ravishda yangilab borish.
- Noma'lum manbalardan fayl va dasturlarni yuklab olmaslik.
- Internet va elektron pochtdan keladigan noma'lum fayllarga ehtiyotkorlik bilan yondashish.
- Tashqi xotira vositalarini tekshirish.
- Ishonchsiz saytlar va dasturlardan foydalanmaslik.

Taklif va Tavsiyalar

1. **Ishonchli antivirus dasturlaridan foydalanish**-Kompyuteringizni viruslardan himoya qilish uchun ishonchli va keng tarqalgan antivirus dasturlarini o'rnatish muhimdir. Kasperskiy, Avast, ESET Nod32, Bitdefender kabi antiviruslar muntazam yangilanishi va samarali himoya ta'minlashi bilan mashhurdir.

2. **Antivirusni doimiy yangilab boorish**-Viruslar va zararli dasturlar tez o'zgarib, yangilanadi. Shu sababli antivirus dasturining viruslar bazasini doimiy yangilab borish zarur, bu yangi tahdidlarga qarshi himoyani kuchaytiradi.

3. **Internet xavfsizligi qoidalariga rioya qilish**-Noma'lum manbalardan fayl yoki dastur yuklab olmang, elektron pochta orqali kelgan shubhali xabarlardagi havolalarni bosmang. Bu virus va zararli dasturlar tarqalishini oldini oladi.

4. **Tashqi qurilmalarni tekshirish**-Fleshka, tashqi qattiq disk kabi qurilmalarni kompyuterga ulashdan oldin antivirus orqali skanerlash tavsiya etiladi, chunki ular virus tarqatuvchi manba bo'lishi mumkin.

5. **Ma'lumotlarni zaxiralash (backup)**-Muhim fayllar va ma'lumotlarni muntazam ravishda zaxiralash — viruslar, ayniqsa shifrovchi viruslardan (ransomware) himoyalanişda muhim choradir.

6. **Kompyuter va dasturlarni yangilab boorish**-Operatsion tizim va dasturlarni yangilab borish xavfsizlik zaifliklarini bartaraf etadi va viruslarning kirib kelish imkoniyatini kamaytiradi.

7. **Xavfsizlik haqida xabardorlikni oshirish**-Foydalanuvchilarni viruslar va ularning tarqalishi, himoya vositalari haqida muntazam ravishda ma'lumot berish, o'qitish ularning ehtiyotkorligini oshiradi.

Foydalangan adabiyotlar

1. Abramson, M. (2019). *Introduction to Computer Security*. Pearson Education.
2. Skoudis, E., & Zeltser, L. (2011). *Malware: Fighting Malicious Code*. Prentice Hall.
3. Kaspersky Lab. (2023). *Kaspersky Security Bulletin 2023*. <https://www.kaspersky.com>
4. ESET. (2023). *ESET Threat Report*. <https://www.eset.com>
5. Avast. (2023). *Avast Security Reports*. <https://www.avast.com>
6. Bitdefender. (2023). *Bitdefender Annual Threat Report*. <https://www.bitdefender.com>

7. Tanenbaum, A. S., & Bos, H. (2015). *Modern Operating Systems*. Pearson.
8. Microsoft. (2023). *Security Intelligence Reports*.
<https://www.microsoft.com/security>
9. Wikipedia contributors. (2024). *Computer virus*. Wikipedia.
https://en.wikipedia.org/wiki/Computer_virus
10. O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. (2022). *Axborot xavfsizligi haqida qo'llanma*.