

## KOMPYUTER VIRUSLARI VA ULARNING AXBOROT XAVFSIZLIGIDAGI O‘RNI

*Murtazova Marjona Davrbek qizi*

*Mirzo Ulug‘bek nomidagi*

*O‘zbekiston Milliy universiteti Jizzax filiali*

*Axborot tizimlari va texnologiyalari talabasi*

**Annotatsiya.** Axborot texnologiyalarining rivojlanishi bilan birga kiberxavfsizlikka bo‘lgan tahdidlar ham sezilarli darajada ortib bormoqda. Kompyuter viruslari axborot tizimlarining ishonchliligi, yaxlitligi va maxfiyligiga jiddiy zarar yetkazuvchi omillardan biri hisoblanadi. Ushbu ishda kompyuter viruslarining kelib chiqish tarixi, tasnifi, aniqlash usullari, zamonaviy zararli dasturlar va ularga qarshi qo‘llanilayotgan himoya texnologiyalari keng yoritilgan.

**Kalit so‘zlar:** kompyuter virusi, zararli dastur (malware), kiberxavfsizlik, axborot xavfsizligi, troyan dastur, tarmoq qurti (worm), ransomware, spyware, phishing, antivirus dasturi, signatura tahlili, hevristik tahlil, xulq-atvor monitoringi, sun‘iy intellekt, mashinali o‘rganish, tarmoq xavfsizligi, ma‘lumotlarni shifrlash, kiberhujum, zararli kod, operatsion tizim xavfsizligi, firewall, autentifikatsiya, ma‘lumotlarni himoyalash, kiberjinoyatchilik, raqamli xavfsizlik, DDoS hujum, zararli skript, internet xavfsizligi, axborot resurslari himoyasi.

Kompyuter viruslari ilk bor XX asrning 1970-yillarida paydo bo‘lgan. Dastlab ular ilmiy tajriba sifatida yaratilgan bo‘lsa, keyinchalik zarar yetkazish maqsadida qo‘llanila boshlandi. Eng birinchi mashhur viruslardan biri **Creep**er bo‘lib, u ARPANET tarmog‘i orqali tarqalgan. Ushbu virusga qarshi yaratilgan dastur **Reaper** tarixdagi birinchi antivirus hisoblanadi.

Bugungi kunda kompyuter viruslari umumiy **Malware** tushunchasi ostida birlashtiriladi. Malware — bu foydalanuvchiga zarar yetkazish maqsadida yaratilgan barcha turdagi dasturlarni anglatadi.

Ransomware foydalanuvchi fayllarini shifrlab, ularni ochish uchun pul talab qiladi. Bu turdagi viruslar ayniqsa banklar va yirik tashkilotlar uchun xavflidir.

#### Spyware (Josus dasturlar)

Spyware foydalanuvchining parollari, klaviatura bosishlari va shaxsiy ma'lumotlarini yashirin tarzda yig'adi.

#### Adware (Reklama viruslari)

Adware tizimda keraksiz reklama oynalarini chiqarib, kompyuter ish faoliyatini sekinlashtiradi.

#### Signatura asosida aniqlash

Bu usul antivirus bazasida mavjud bo'lgan virus kodlari bilan solishtirish orqali ishlaydi. Eng keng tarqalgan va samarali usullardan biri hisoblanadi.

#### Evristik tahlil

Evristik tahlil virusning xatti-harakatlarini kuzatish orqali aniqlaydi. Bu yangi va noma'lum viruslarni aniqlashda muhim ahamiyatga ega.

#### Sun'iy intellekt asosida aniqlash

Zamonaviy antiviruslar sun'iy intellekt va mashinaviy o'rganish texnologiyalaridan foydalanib, zararli dasturlarni yuqori aniqlikda aniqlaydi.

Antivirus dasturlari real vaqt rejimida tizimni tekshiradi, shubhali fayllarni karantinga oladi va viruslarni o'chiradi. Mashhur antivirus dasturlariga quyidagilar kiradi:

Kompyuter viruslari natijasida har yili milliardlab dollar zarar yetkaziladi. Katta kompaniyalar faoliyatining to'xtashi, foydalanuvchi ma'lumotlarining tarqalishi va kiberjinoyatchilikning oshishi jamiyatga salbiy ta'sir ko'rsatadi.

Litsenziyalangan dasturlardan foydalanish

Kuchli parollar yaratish

Ikki bosqichli autentifikatsiyani yoqish

Internet xavfsizligi qoidalariga rioya qilish

Axborot xavfsizligi bo'yicha foydalanuvchilarni muntazam o'qitish

So'nggi yillarda smartfon va planshetlardan foydalanish kengaygani sababli mobil qurilmalar ham zararli dasturlar hujumiga ko'proq uchramoqda. Mobil viruslar asosan Android operatsion tizimida keng tarqalgan bo'lib, ular foydalanuvchi ruxsatisiz ilovalar o'rnatish, SMS yuborish, bank ma'lumotlarini o'g'irlash kabi zararli harakatlarni amalga oshiradi. Mobil viruslar ko'pincha rasmiy bo'lmagan ilovalar do'konlari orqali tarqaladi.

Mobil qurilmalarda viruslardan himoyalani uchun faqat ishonchli manbalardan ilova yuklab olish, ilovalarga berilayotgan ruxsatlarni tekshirish va mobil antiviruslardan foydalanish muhim ahamiyatga ega.

Bulutli hisoblash texnologiyalari (Cloud Computing) zamonaviy IT infratuzilmaning ajralmas qismiga aylangan. Biroq ma'lumotlarning masofaviy serverlarda saqlanishi yangi xavfsizlik muammolarini yuzaga keltiradi. Bulutli tizimlarda zararli dasturlar noto'g'ri sozlangan autentifikatsiya, zaif parollar yoki phishing hujumlari orqali tarqaladi.

Bulutli muhitda viruslardan himoyalani uchun ko'p bosqichli autentifikatsiya, ma'lumotlarni shifrlash va foydalanuvchi faoliyatini doimiy monitoring qilish tavsiya etiladi.

Kompyuter viruslarini yaratish, tarqatish va ulardan foydalanish ko'pgina davlatlarda jinoyat hisoblanadi. Axborot xavfsizligini buzish bilan bog'liq jinoyatlar uchun ma'muriy

va jinoiy javobgarlik belgilangan. O'zbekiston Respublikasida ham axborot tizimlariga noqonuniy kirish va zarar yetkazish holatlari qonun bilan tartibga solinadi.

Ushbu jihatlarni maqolada yoritish ishning ilmiy va ijtimoiy ahamiyatini yanada oshiradi.

Ta'lim muassasalarida elektron jurnal, masofaviy ta'lim platformalari va raqamli resurslardan keng foydalanilmoqda. Viruslar ushbu tizimlarga zarar yetkazib, o'quv jarayonining to'xtab qolishiga sabab bo'lishi mumkin. Shu bois ta'lim muassasalarida axborot xavfsizligi bo'yicha alohida siyosat yuritilishi zarur.

Talabalar va o'qituvchilar uchun kiberxavfsizlik bo'yicha treninglar tashkil etish muhim hisoblanadi.

Sun'iy intellekt texnologiyalari viruslarni aniqlash va ularga qarshi kurashishda samarali vosita bo'lib xizmat qilmoqda. Mashinaviy o'rganish algoritmlari zararli dasturlarning xatti-harakatlarini tahlil qilib, ilgari noma'lum bo'lgan viruslarni ham aniqlay oladi. Shu bilan birga, sun'iy intellektdan foydalangan holda yaratilayotgan murakkab viruslar ham paydo bo'lmoqda.

Xulosa qilib aytganda kompyuter viruslari zamonaviy axborot tizimlari uchun jiddiy xavf manbai hisoblanadi. Ularning turli shakllari ma'lumotlarning yo'qolishiga, maxfiy axborotlarning oshkor bo'lishiga hamda moliyaviy zararlarning yuzaga kelishiga sabab bo'lmoqda. Raqamli texnologiyalarning keng qo'llanilishi viruslar tarqalish tezligini oshirib, kiberxavfsizlik masalasining dolzarbligini yanada kuchaytirmoqda.

Axborot xavfsizligini ta'minlashda zamonaviy antivirus dasturlaridan foydalanish, tizimlarni muntazam yangilash, zaxira nusxalar yaratish hamda foydalanuvchilarning kiberxavfsizlik bo'yicha bilim va ko'nikmalarini oshirish muhim ahamiyat kasb etadi. Kompleks yondashuv asosida amalga oshirilgan himoya choralarigina kompyuter viruslarining salbiy ta'sirini kamaytirishga xizmat qiladi.

### Foydalanilgan adabiyotlar:

1. Tanenbaum A.S. *Computer Networks*. — Pearson Education, 2011.
2. Stallings W. *Network Security Essentials: Applications and Standards*. — Pearson, 2017.
3. Skoudis E., Liston T. *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. — Prentice Hall, 2006.
4. Ayubov R.X., Karimov S.S. **Axborot xavfsizligi asoslari**. — Toshkent: O‘zbekiston, 2019.
5. Kaspersky Lab. **Malware va antivirus texnologiyalari bo‘yicha ilmiy-tahliliy materiallar**.
6. ESET Research. **Zamonaviy kiberxavfsizlik tahdidlari va ularni aniqlash usullari**.
7. Cisco Networking Academy. *Introduction to Cybersecurity*.
8. Microsoft Corporation. **Security Documentation and Windows Security Architecture**.
9. ISO/IEC 27001. **Information Security Management Systems — Requirements**.