Mavzu: Antivirus dasturiy vositalar: kompyuter viruslarining xarakteristikalari, viruslarni aniqlash va ulardan himoya qilish dasturlari.

23.11.2015

Reja:

1. Virus va uning turlari.
2. Kompyuter viruslaridan himoyalash.
3. Antivirus dasturlari.

1. Virus va uning turlari.

«Kompyuter virusi» atamasi 80-yillarning o‘rtalarida kiritilgan. Biologik viruslarga tegishli o‘lchamlarning kichikligi, o‘z-o‘zidan ko'payib va obyektlarga singib (ularni zaharlab), tez tarqalish qobiliyati, sistemaga salbiy ta’siri kabi alomatlar zararkunanda dasturlarga ham xosdir. Kompyuter viruslari bilan ish ko‘rilganda, «virus» atamasi bilan bir qatorda, «zaharlanish», «yashash muhiti», «profilaktika» kabi tibbiyot atamalaridan ham foydalaniladi.

«Kompyuter viruslari» — kompyuter sistemalarida tarqalish va o‘z-o‘zidan qaytadan tiklanish (replikatsiya) xususiyatlariga ega bo‘lgan bajariluvchi yoki sharhlanuvchi kichik dasturlardir. Viruslar kompyuter sistemalarida saqlanuvchi dasturiy ta’minotni o'zgartirishi yoki yo‘qotishi mumkin.

Barcha kompyuter viruslari quyidagi alomatlariga ko‘ra tasniflanishi mumkin:

— yashash muhiti bo‘yicha;

— yashash muhitining zaharlanishi bo‘yicha;

— zararli ta’sirining xavflilik darajasi bo'yicha;

— ishlash algoritmi bo'yicha.

Yashash muhitiga ko‘ra kompyuter viruslari quyidagilarga bo'linadi:

— tarmoq viruslari;

— fayl viruslari;

— yuklama viruslar;

— kombinatsiyalangan viruslar.

Tarmoq viruslarining yashash muhiti kompyuter tarmoqlarining elementlaridir. Fayl viruslar bajariluvchi fayllarda joylashadi. Fayl viruslar ichida makroviruslar alohida o‘rin tutadi. Makroviruslar — makrotillarda yozilgan zararkunanda dasturlar, elektron jadvallar va h.k. Yuklama viruslar tashqi xotira qurilmalarining yuklama sektorlarida (boot-sektorlarda) bo‘ladi. Kombinatsiyalangan viruslar bir necha yashash muhitida joylashgan bo'ladi. Misol tariqasida yuklama fayl viruslarni ko‘rsatish mumkin.

Yashash muhitining zaharlanishi usuli bo'yicha kompyuter viruslari:

— rezident;

— rezident bo'lmagan viruslarga bo‘linadi.

Rezident viruslar faollashganlaridan so‘ng to‘laligicha yoki qisman yashash muhitidan (tarmoq, yuklama sektori, fayl) hisoblash mashinasining asosiy xotirasiga ko‘chadi. Bu viruslar, odatda, faqat operatsion sistemaga ruxsat etilgan imtiyozli rejimlardan foydalanib yashash muhitini zaharlaydi va ma’lum sharoitlarda zararkunandalik vazifasini bajaradi.

Rezident bo’lmagan viruslar faqat faollashgan vaqtlarida hisoblash mashinasining asosiy xotirasiga tushib, zaharlash va zararkunandalik vazifalarini bajaradi. Keyin bu viruslar asosiy xotirani butunlay tark etib yashash muhitida qoladi. Agar virus yashash muhitini zaharlamaydigan dasturni asosiy xotiraga joylashtirsa, bunday virus rezident bo'lmagan virus hisoblanadi.

Kompyuter viruslarini foydalanuvchining axborot resurslari uchun xavflilik darajasi bo'yicha quyidagilarga ajratish mumkin:

- beziyon viruslar;
- xavfli viruslar;
- juda xavfli viruslar.

Beziyon kompyuter viruslari kompyuter sistemasi resurslariga qandaydir shikast yetkazishni maqsad qilmagan mualliflar tomonidan yaratiladi. Ularning maqsadi, odatda, o‘zlarining dasturchilik imkoniyatlarini ko‘z-ko‘z qilishdir. Bunday viruslarning zararkunandaligi monitorda aybsiz matnlarni va rasmlarning, musiqiy parchalarning ijro etilishiga olib keladi va h.k.

Xavfli viruslarga kompyuter sistemalari samaradorligi jiddiy pasayishiga olib keluvchi, ammo xotirlovchi qurilmalarda saqlanuvchi axborotning yaxlitligini va maxfiyligini buzmaydigan viruslar kiradi. Bunday viruslar ta’siri oqibatlarini unchalik katta bo'lmagan moddiy va vaqt resurslari sarfi evaziga yo‘qotish mumkin.

Juda xavfli viruslarga axborotning maxfiyligi buzilishiga, yo‘q qilinishiga, takrorlanmaydigan turlanishga (shifrlash ham shu qatorda) hamda axborotdan foydalanishga to‘sqinlik qiluvchi va natijada apparat vositalaming ishdan chiqishiga hamda foydalanuvchilar sog‘lig‘iga shikast yetishiga sabab bo’luvchi viruslar kiradi.

Ishlash algoritmining xususiyatlari bo‘yicha viruslarni:

• tarqalishida yashash makonini o'zgartirmaydigan;

• tarqalishida yashash makonini o‘zgartiradigan sinflarga ajratish mumkin.

Yashash makonini o'zgartirmaydigan viruslar, o‘z navbatida:

- «yo‘ldosh» viruslar (companion),
- «qurt» viruslar (worm) dan iborat ikki guruhga ajratilishi mumkin.

«Yo‘ldosh» viruslar fayllarni o'zgartirmaydi. Uning ta’sir mexanizmi bajariluvchi fayllarning nusxalarini yaratishdan iboratdir.

«Qurt» viruslar tarmoq orqali ishchi stansiyaga tushadi, tarmoqning boshqa abonentlari bo‘yicha virusni jo'natish adreslarini hisoblaydi va virusni uzatadi. Virus fayllarni o'zgartirmaydi va disklaming yuklama sektorlariga yozilmaydi.

Algoritmlarning murakkabligi, mukammallik darajasi va yashirinish xususiyatlari bo‘yicha **yashash makonini o'zgartiradigart viruslar**:

- talaba viruslar;
- «stels» viruslar (ko'rinmaydigan viruslar);
- polimorf viruslarga bo‘linadi.

- **Talaba viruslar** malakasi past yaratuvchilar tomonidan yaratiladi.
- Bunday viruslar, odatda, rezident bo'lmagan viruslar qatoriga kiradi, ularda ko'pincha xatoliklar mavjud bo‘ladi, osongina taniladi va yo‘qotiladi.
- **«Stels»** viruslar malakali mutaxassislar tomonidan yaratiladi. «Stels» viruslar operatsion sistemaning shikastlangan fayllarga murojaatlarini ushlab qolish yo‘li bilan o'zining yashash makonida ekanligini yashiradi va operatsion sistemani axborotning shikastlanmagan qismiga yo'naltiradi.
- **Polimorf** viruslar ham malakali mutaxassislar tomonidan yaratiladi va doimiy tanituvchi guruhlar — signaturalarga ega bo‘lmaydi. Oddiy viruslar yashash makonining zaharlanganligini aniqlash uchun zaharlangan obyektga maxsus tanituvchi ikkili ketma-ketlikni yoki simvollar ketma-ketligini (signaturani) joylashtiradi.

2. Kompyuter viruslaridan himoyalash.

Virusga qarshi vositalar yordamida quyidagi masalalar yechiladi:
kompyuter sistemalaridagi viruslar aniqlanadi;
viruslar ta’siri oqibatlari yo'qotiladi.

Kompyuter sistemalarida viruslarni aniqlashning quyidagi metodlari mavjud:

- skanerlash;
- o’zgarishlarni bilib qolish;
- evristik tahlil;
- rezident qorovullardan foydalanish;
- dasturni vaksinasiyalash;
- viruslardan apparat-dasturiy himoyalanish.

Skanerlash viruslarni aniqlashning eng oddiy metodlaridan hisoblanadi. Skanerlash skaner-dastur tomonidan amalga oshiriladi. Bu skaner dastur viruslarning tanituvchi qismini — signaturani qidirish maqsadida fayllarni ko‘rib chiqadi. Ko‘pincha skaner-dasturlar aniqlangan viruslarni yo‘qotishi mumkin. Bunday dasturlar polifaglar deb ataladi. Skanerlash metodi signaturalari ajratilgan va doimiy bo‘lgan viruslarni aniqlashda qo‘llanadi.

O‘zgarishlarni bilib olish metodi dasturiy taftishchidan foydalanishga asoslangan. Bunday dasturlar, odatda, virus joylashadigan diskning barcha qismlari tavsifini aniqlaydi va eslab qoladi. Dasturtaftishchining davriy bajarilish jarayonida saqlanuvchi tavsiflari bilan disk qismlarini nazoratlash natijasidagi xarakteristikalar taqqoslanadi. Taftish natijasida dasturiy viruslar borligi xususida taxminga asoslangan axborotni beradi.

Evristik tahlil metodi ham, o‘zgarishlarni bilib olish metodlari kabi, noma’lum viruslarni aniqlash imkonini beradi. Ammo bu metod fayl sistemasi xususidagi axborotni oldindan yig‘ish, ishlash va saqlashni talab etmaydi. Evristik tahlilning mohiyati viruslar yashashi ehtimol tutilgan makonlarni tekshirish va ulardagi viruslarga xos buyruqlarni (buyruqlar guruhini) aniqlashdan iboratdir.

Rezident qorovullardan foydalanish metodi hisoblash mashinasining asosiy xotirasida doimo saqlanuvchi va boshqa dasturlar harakatini kuzatuvchi dasturlarga asoslangan. Bu metodning jiddiy kamchiligi unda yolg'ondakam trevogalar foizining yuqoriligidir.

Dasturni vaksinatsiyalash deganda, uning yaxlitligini nazorat qilish maqsadida maxsus modulning yaratilishi tushuniladi. Fayl yaxlitligining tavsifi sifatida, odatda, nazorat yig'indisidan foydalaniladi.Vaksinatsiyalangan fayl zaharlansa, nazorat moduli nazorat yig‘indisining o‘zgarishini aniqlaydi va foydalanuvchini bu xususda ogohlantiradi.

Viruslarga qarshi apparat-dasturiy vositalardan foydalanish viruslardan himoyalanishning eng ishonchli metodi hisoblanadi. Hozir shaxsiy kompyuterlarni himoyalashda maxsus nazoratchilar va ularning dasturiy ta’minotidan foydalaniladi. Nazoratchi umumiy shinadan foydalana oladi va shu sababli disk sistemasiga bo'lgan barcha murojaatlarni nazorat qila oladi. Nazoratchining dasturiy ta’minotida ishlashning oddiy rejimida diskning o‘zgartirilishi mumkin bo‘lmagan qismlari xotirlanadi.

Viruslarga qarshi apparat-dasturiy vositalar quyidagi afzalliklarga ega:

- doimo ishlaydi;
- ta’sir mexanizmidan qat’i nazar barcha viruslarni aniqlaydi;
- virus ta’siri yoki malakasiz foydalanuvchi ishi natijasidagi ruxsatsiz harakatlarni to'xtadi.

3. Antivirus dasturlari .

Kompyuterdagi ma'lumotlarni viruslardan himoya etish uchun antivirus dasturlar ishlab chiqarilgan. Antivirus dasturlar AQSh, Kanada, Rossiyaning bir qator firmalari tomonidan ishlab chiqarilmoqda. Antivirus dasturlar rezident va norezident turlarga bo'linadi: rezident antivirus dasturi kompyuter yoqilganidan o'chirilguncha qadar operativ xotira, aktiv (joriy) dasturlarni, fayllarni virusga tekshirib turadi. Rezident antivirus dasturi o'zining ishini foydalanuvchiga bildirmasdan olib boradi, faqat ayrim hollarda foydalanuvchidan virusi mavjud faylni davolashga ruxsat so'raydi. Norezident antivirus dasturlar esa faqat foydalanuvchining o'zi ko'rsatgan joylarni va belgilangan vaqtda tekshiradi va davolaydi.

Hozirgi kunda quyidagi antivirus dasturlar keng tarqalgan:

1. DrWeb for DOS;
2. DrWeb for Windows;
3. Antiviral Tool Kit Pro;
4. AVP Platinium;
5. Norton Antivirus;
6. McAfee;
7. Aidstest;

Doctor Web, AVP, Aidstest antivirus dasturlari Rossiyaning "Kasperskiy" laboratoriyasi tomonidan ishlab chiqarilgan va u MDH davlatlarida ko'p uchraydigan viruslardan xabari bor. Norton Antivirus mashhur Symantec firmasi tomonidan ishlab chiqarilgan bo'lib, u topa oladigan viruslar soni 100000 dan ortiq. AVP dasturi virusdan himoyalaydigan eng ishonchli antivirus dasturi hisoblanadi. DrWeb dasturining rezident tekshiruv dasturi Spider - Windows rejimida tekshiruvni olib boradi. Bitta kompyuterda bir nechta turdagi antivirus dasturlar o'rnatmagan ma'qul, chunki ularning virusni topish usullari (algoritmlari) har xil hamda ular ham o’zlarini viruslar kabi tutadilar va bu holda ular o'zaro "kelisha olmay qolishlari" mumkin.