KOMPYUTER VIRUSLARI. ANTIVIRUSLAR. ANTIVIRUSLARNI TO‘G‘RI TANLASH. ANTIVIRUSLAR BILAN ISHLASH

Farg‘ona viloyati Qo‘shtepa tumani 2-son Texnikumi Informatika va axborot texnalogiyalari fani o‘qituvchisi
Dadajonova Matluba Shodiyor qizi

Reja:

1. Virus nima?
2. Kompyuter viruslari qanday hosil bo’ladi?
3. Yashash makoni bo’yicha Kompyuter viruslarining turkumlanishi

Kompyuter viruslariga qarshi minglab professional mutaxassislar ko’lab kompaniyalarda ish olib borishmoqda. Bu mavzu o’ta qiyin va muhimki ko’p e`tiborni talab qilmoqda. Kompyuter virusi ma`lumotni yo’qotish sabablaridan biri va asosiysi bo’lib qolmoqda. Viruslar ko’’lab tashkilot va kom’aniyalarni ishlarini buzishga olib kelganligi ma`lum. Shunday ma`lumotlar mavjudki, Niderlandiya gos’itallaridan birida bemorga Kompyuter qo’ygan tashxis bo’yicha iste`mol qilingan dori oqibatida bemor olamdan o’tgan. Bu Kompyuter virusining ishi bo’lgan.

E`tiborsizlik bilan qilingan ishdan Kompyuter tezda virus bilan zararlanadi. Inson kasallik virusi bilan zararlansa issiqligi o’zgarishi, vazni o’zgarishi, xolsizlanish va og’riqning paydo bo’lishi ko’zda tutiladi. Kompyuter virusi bilan zararlangan Kompyuterlarda quyidagilar kuzatiladi: dasturlarning ishlashining sekinlashishi, fayllarni hajmi o’zgaradi, g’ayritabiiy va ba`zi bir noma`lum xatoliklar, ma`lumotlar va sistema fayllari yo’qotilishi. Ba`zi viruslar zararsiz ko’’ayadi, lekin qo’rqinchli emas. Bu viruslar ekranga xato ma`lumot chiqaradi. Ammo, bir turdagi viruslar hujum qiluvchi, ya`ni, yomon asoratlar qoldiruvchi hisoblanadi. Masalan, viruslar qattik diskdagi ma`lumotlarni o’chirib tashlaydi.

Virus nima?

Virus(Virus) inglizcha “yuqumli boshlanish”, “yomon boshlanish – buzuvchi boshlanish”, “yuqumli kasal” degan ma`nolarni anglatadi.

Mashxur «doktor» lardan biri D.N.Lozinskiy virusni kotibaga o’xshatadi. Tartibli kotibani faraz qilsak, u ishga keladi va stolidagi bir kunda qilishi kerak bo’lgan ishlarni - qog’ozlar qatlamini ko’radi. U bir varog’ni ko’’aytirib bir nusxasini o’ziga ikkinchisini keyingi qo’shni stolga qo’yadi. Keyingi stoldagi kotiba ham kamida ikki nusxada ko’’aytirib, yana bir kotibaga o’tkazadi. Natijada kontoradagi birinchi nusxa bir necha nusxalarga aylanadi. Ba`zi nusxalar yana ko’’ayib boshqa stollarga ham o’tishi mumkin.

Kompyuter viruslari taxminan shunday ishlaydi, Faqat qog’ozlar o’rnida endi dasturlar, kotiba bu - Kompyuter. Birinchi buyruq «ko’chirish-nusxa olish» bo’lsa, Kompyuter buni bajaradi va virus boshqa dasturlarga o’tib oladi. Agar Kompyuter biror zararlangan dasturni ishga tushirsa virus boshqa dasturlarga tarqalib borib butun Kompyuterni egallashi mumkin.

Agar bir dona virusning ko’payishiga 30 sekund vaqt ketsa, bir soatdan keyin bu 1000000000 dan ortib ketishi mumkin. Aniqrog’i Kompyuter xotirasidagi bo’sh joylarni band qilishi mumkin.

Xuddi shunday voqea 1988 yili Amerikada sodir bo’lgan. Global tarmoq orqali uzatilayotgan ma`lumot orqali virus bir Kompyuterdan boshqasiga o’tib yurgan. Bu virus Morris virusi deb atalgan.

Ma`lumotlarni virus qanday yo’q qilishi mumkin degan savolga shunday javob berish mumkin:

Virus nusxalari boshqa dasturlarga tez ko’’ayib o’tib oladi;

Kalendar bo’yicha 13-sana juma kunga to’g’ri kelsa hamma xujjatlarni yo’q qiladi.

Buni hammaga ma`lum «Jerusalem» («Time» virusi ham deb ataladi) virusi juda «yaxshi» amalga oshiradi.

Ko’’ xollarda bilib bo’lmaydi, virus qayerdan paydo bo’ldi.

Virusni aniqlanishi shundaki, u Kompyuter sistemasida joylashib va ko’’ayib borishiga bog’lik. Misol uchun, nazariy jihatdan o’eratsion sistemada virus davolab bo’lmaydi. Bajaruvchi kodning sohasini tuzish va o’zgartirish ta`qiqlangan sistema misol bo’lishi mumkin.

Virus hosil bo’lishi uchun bajariluvchi kodlar ketma-ketligi ma`lum bir sharoitda shakllanishi kerak. Kompyuter virusining xossalaridan biri o’z nusxalarini Kompyuter tarmoqlari orqali bajariluvchi obyektlarga ko’chiradi. Bu nusxalar ham o’z-o’zidan ko’’ayish imkoniyatiga ega.

Kompyuter viruslari qanday hosil bo’ladi?

Biologik viruslardan farqli o’laroq, Kompyuter viruslarini inson tomonidan tuziladi. Viruslar Kompyuter foydalanuvchilariga katta zarar yetkazadi. Ular Kompyuter ishini to’xtatadi yoki qattiq diskdagi ma`lumotlarni o’chiradi. Virus sistemaga bir necha yo’llar bilan tushishi mumkin: ma’lumot tashuvchi qurilmalar, dasturiy ta`minot yuklangan CD-ROM, tarmoq interfeysi yoki modemli bog’lanish, global Internet; tarmog’idagi elektron pochta.

Ma’lumot tashuvchi qurilma virusdan zararlanishi oson. Zararlangan Kompyuterga ma’lumot tashuvchi qurilmani solib o’qitilganda diskning bosh sektoriga virus tushadi.

Internet ma`lumotlar almashinishiga katta imkoniyat yaratadi. Lekin, Kompyuter viruslari va zararli dasturlar tarqalishi uchun yaxshi muhit yaratadi. Albatta Internetdan olingan barcha ma`lumotlarda virus bor deb bo’lmaydi. Kompyuterda ishlovchi ko’’chilik mutaxassislar va o’eratorlar qabul qilinadigan ma`lumotlarni viruslardan tekshirishni doimo bajaradi. Internet da ishlayotgan har bir kishi uchun yaxshi antivirus himoya zarur. «Kas’erskiy laboratoriyasi» texnik ta`minot xizmati statistikasiga ko’ra, viruslardan zararlangan xolatlarning 85% i elektron pochta orqali sodir bo’lgan. 1999 yilga nisbatan xozirgi kunda bu ko’rsatkich 70 % tashkil etadi. «Kas’erskiy laboratoriyasi» elektron pochtalarga yaxshi antivirus himoyasi kerakligini ta`kidlaydi.

Virus tuzuvchilarga elektron pochta juda qulay. Amaliyot shuni ko’rsatadiki, ommabo’ dasturlar, o’eratsion sistemalar, ma`lumotlarni uzatish texnologiyalari uchun viruslar ko’’lab

tuzilmoqda. Xozirda elektron pochta biznes va boshqa sohalarda muloqot uchun asosiy vosita bo’lib qolmoqda. Shuning uchun virus tuzuvchilari elektron pochtaga diqqatini qaratmoqda.

Kompyuter virusining ko’’ ta’riflari mavjud. Birinchi ta’rifni 1984 yili Fred Koen bergan: "Kompyuter virusi - boshqa dasturlarni, ularga o’zini yoki o’zgartirilgan nusxasini kiritish orqali, ularni modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko’’ayish qobiliyatini saqlaydi". Virusning o’z-o’zidan ko’’ayishi va hisoblash jarayonini modifikatsiyalash qobiliyati bu ta’rifdagi tayanch tushunchalar hisoblanadi. Kompyuter virusining ushbu xususiyatlari tirik tabiat organizmlarida biologik viruslarning parazitlanishiga o’hshash.

Hozirda Kompyuter virusi deganda quyidagi xususiyatlarga ega bo’lgan dasturiy kod tushuniladi:

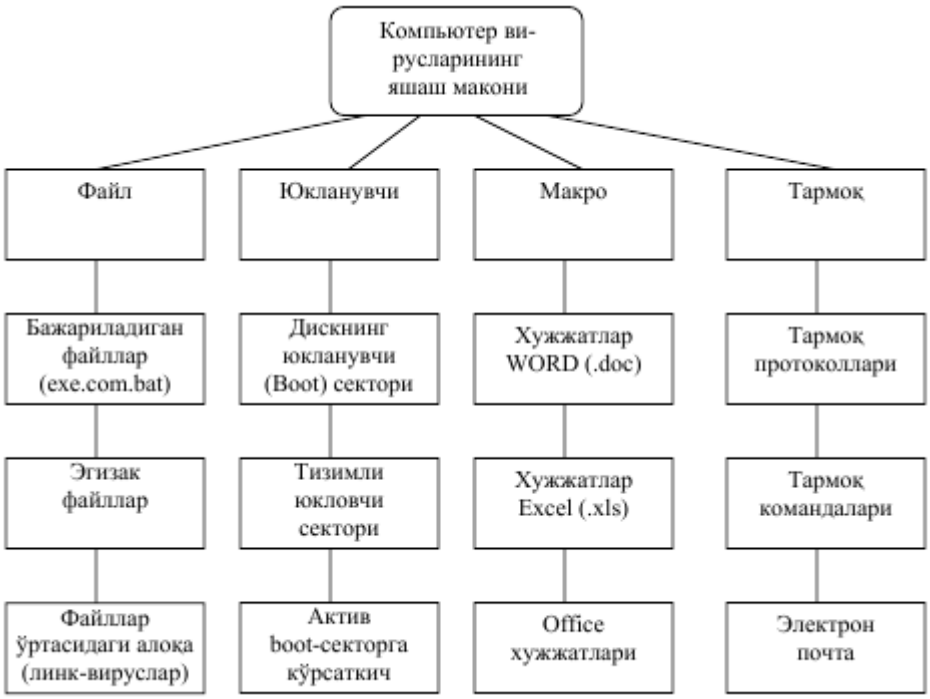
- asliga mos kelishi shart bo’lmagan, ammo aslining xususiyatlariga (o’z-o’zini tiklash) ega bo’lgan nusxalarni yaratish qobiliyati;
- hisoblash tizimining bajariluvchi ob’ektlariga yaratiluvchi nusxalarning kiritilishini ta’minlovchi mexanizmlarning mavjudligi.

Ta’kidlash lozimki, bu xususiyatlar zaruriy, ammo yetarli emas. Ko’rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta’sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to’ldirish lozim.

Viruslarni quyidagi asosiy alomatlari bo’yicha turkumlash mumkin:

- yashash makoni;
- o’eratsion tizim;
- ishlash algoritmi xususiyati;
- destruktiv imkoniyatlari.

Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi Kompyuter tizimi obyektlarining xili bo’yicha turkumlash asosiy va keng tarqalgan turkumlash hisoblanadi.



Yashash makoni bo'yicha Kompyuter viruslarining turkumlanishi.

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko'' tarqalgan viruslar xili), yoki fayl-yo'ldoshlarni (kom'anon viruslar) yaratadi yoki faylli tizimlarni (link-viruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o'zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (Master Boot Record) bo'lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan MicroSoft Word, MicroSoft Excel va h. kabi ommaviy muharrirlarning fayl-xujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o'zini tarqatishda Kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba'zida tarmoq viruslarini "qurt" xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo'yicha tarqaladi), IRC-qurtlarga (chatlar, Internet Relay Chat) bo'linadi.

Kompyuter viruslarining bajarilish davri, odatda, beshta bosqichni o'z ichiga oladi:

1. Virusni xotiraga yuklash.
2. Qurbonni qidirish.
3. To'ilgan qurbonni zaharlash.
4. Destruktiv funktsiyalarni bajarish.
5. Boshqarishni virus dastur-eltuvchisiga o'tkazish.

Virusni xotiraga yuklash. Virusni xotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi ob'ekt bilan bir vaqtda amalga oshiriladi.

Qurbonni qidirish. Qurbonni qidirish usuli bo'yicha viruslar ikkita sinfga bo'linadi. Birinchi sinfga o'eratsion tizim funktsiyalaridan foydalanib faol qidirishni amalga oshiruvchi

viruslar kiradi. Ikkinchi sinfga qidirishning passiv mexanizmlarini amalga oshiruvchi, ya’ni dasturiy fayllarga tuzoq qo’yuvchi viruslar taalluqli.

Topilgan qurbonni zaharlash. Oddiy holda zaharlash deganda qurbon sifatida tanlangan ob’ektda virus kodining o’z-o’zini nusxalashi tushuniladi.

Destruktiv funktsiyalarni bajarish. Destruktiv imkoniyatlari bo’yicha beziyon, xavfsiz, xavfli va juda xavfli viruslar farqlanadi.

Beziyon viruslar - o’z-o’zidan tarqalish mexanizmi amalga oshiriluvchi viruslar. Ular tizimga zarar keltirmaydi, faqat diskdagi bo’sh xotirani sarflaydi xolos.

Xavfsiz viruslar - tizimda mavjudligi turli taassurot (ovoz, video) bilan bog’liq viruslar, bo’sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydi.

Xavfli viruslar - Kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar. Natijada dastur va ma’lumotlar buzilishi mumkin.

Juda xavfli viruslar - dastur va ma’lumotlarni buzilishiga hamda Kompyuter ishlashiga zarur axborotni o’chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar.

Boshqarishni virus dastur — eltuvchisiga o’tkazish. Ta’kidlash lozimki, viruslar buzuvchilar va buzmaydiganlarga bo’linadi. Buzuvchi viruslar dasturlar zaharlanganida ularning ishga layoqatligini saqlash xususida qayg’urmaydilar, shu sababli ularga ushbu bosqichning ma’nosi yo’q.

Buzmaydigan viruslar uchun ushbu bosqich xotirada dasturni korrekt ishlanishi shart bo’lgan ko’rinishda tiklash va boshqarishni virus dastur-eltuvchisiga o’tqazish bilan bog’liq.

Virus paydo bo’lish belgilari.

Zararlangan Kompyuterda eng muhimi virusni aniqlash. Buning uchun virusni asosiy belgilarini bilish kerak:

1.Funktsional dasturlarni ishini to’xtatish yoki noto’g’ri ishlashi;
2.Kompyuterni sekin ishlashi;
3.OS ni yuklanmasligi;
4.Fayl va kataloglarni yo’qolishi yoki ulardagi ma`lumotlarni buzilishi;
5.Fayllar modifikatsiyasining sana va vaqtining o’zgarishi;
6.Fayl hajmining o’zgarishi;
7.Diskdagi fayllar miqdorining keskin ko’’ayishi;
8.Bo’sh o’erativ xotira hajmining keskin kamayishi;
9.Kutilmagan ma`lumotlar va tasvirlarning ekranga chiqishi;
10.Kutilmagan tovushlarning paydo bo’lishi;
11 .Kompyuterning tez-tez osilib kolishi.

Yuqoridagi belgilar boshqa sabablarga ko’ra ham bo’lishi mumkinligini eslatib o’tamiz.

Virusga qarshi dasturlar

Kompyuter viruslarini aniqlash va ulardan himoyalanish uchun maxsus dasturlarning bir necha xillari ishlab chiqilgan bo'lib, bu dasturlar Kompyuter viruslarini aniqlash va yo'qotishga imkon beradi. Bunday dasturlar virusga qarshi dasturlar deb yuritiladi. Umuman, barcha virusga qarshi dasturlar zaharlangan dasturlarning va yuklama sektorlarning avtomatik tarzda tiklanishini ta'minlaydi.

Viruslarga qarshi dasturlar foydalanadigan viruslarni aniqlashning asosiy usullari quyidagilar:

- etalon bilan taqqoslash usuli;
- evristik taxlil;
- virusga qarshi monitoring;
- o'zgarishlarni aniqlovchi usul;
- Kompyuterning kiritish/chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o'rnatish va h.

Etalon bilan taqqoslash usuli eng oddiy usul bo'lib, ma'lum viruslarni qidirishda niqoblardan foydalanadi. Virusning niqobi-mana shu muayyan virusga xos kodning qandaydir o'zgarmas ketma-ketligidir. Virusga qarshi dastur ma'lum virus niqoblarini qidirishda tekshiriluvchi fayllarni ketma-ket ko'rib chiqadi (skanerlaydi).

Evristik tahlil. Kompyuter virusi ko''ayishi uchun xotirada nusxalanish, sektorga yozilish kabi qandaydir muayyan xarakatlarni amalga oshirishi lozim.

Virusga qarshi monitoring. Ushbu usulning mohiyati shundan iboratki, Kompyuter xotirasida boshqa dasturlar tomonidan bajariluvchi shubhali harakatlarni monitoringlovchi virusga qarshi dastur doimo bo'ladi. Virusga qarshi monitoring barcha ishga tushiriluvchi dasturlarni, yaratiluvchi, ochiluvchi va saqlanuvchi xujjatlarni, Internet orqali olingan yoki disketdan yoki har qanday kom'akt-diskdan nushalangan dastur va xujjatlarning fayllarini tekshirishga imkon beradi. Agar qandaydir dastur xavfli harakatni qilishga urinmoqchi bo'lsa, virusga qarshi monitor foydalanuvchiga xabar beradi.

O'zgarishlarni aniqlovchi usul. Diskni taftish qiluvchi deb ataluvchi ushbu usulni amalga oshirishda virusga qarshi dastur diskning xujumga duchor bo'lishi mumkin bo'lgan barcha sohalarini oldindan xotirlaydi, so'ngra ularni vaqti-vaqti bilan tekshiradi. Virus Kompyuterlarni zaharlaganida qattiq disk tarkibini o'zgartiradi: masalan, dastur yoki xujjat fayliga o'zining kodini qo'shib qo'yadi, Autoexec.bat fayliga dastur-virusni chaqirishni qo'shadi, yuklama sektorni o'zgartiradi, faylyo'ldosh yaratadi. Disk sohalari xarakteristikalarining qiymatlari solishtirilganida virusga qarshi dastur ma'lum va no'malum viruslar tomonidan qilingan o'zgarishlarni aniqlashi mumkin.

Kompyuterlarning kiritish/chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o'rnatish. Kompyuterlarning tizimli platasiga viruslardan himoyalashning oddiy vositalari o'rnatiladi. Bu vositalar qattiq disklarning bosh yuklama yozuviga hamda disklar va disketlarning yuklama sektorlariga barcha murojaatlarni nazoratlashga imkon beradi. Agar qandaydir dastur yuklama sektorlar tarkibini o'zgartirishga urinsa, himoya ishga tushadi va foydalanuvchi ogohlantiriladi. Ammo bu himoya juda ham ishonchli emas.

Virusga qarshi dasturlarning xillari. Virusga qarshi dasturlarning quyidagi xillari farqlanadi:

- dastur-faglar (virusga qarshi skanerlar);
- dastur-taftishchilar (CRC-skanerlar);
- dastur-blokirovka qiluvchilar;
- dastur-immunizatorlar.

Dr.Web — Rossiyaning virusga qarshi ommaviy dasturi, Windows 9x/NT/2000/X'/7/8 uchun mo'ljallangan bo'lib, faylli, yuklama, va fayl-yuklama viruslarni qidiradi va zararsizlantiradi.

AV' (Antivirus Kas'erskogo personal) — Rossiyaning virusga qarshi paketi.

Eset Nod32 Antivirus

Symantec Antivirus — Symantec kom'aniyasining kor'orativ foydalanuvchilarga taklif etgan virusga qarshi mahsuloti to''lami.

FOYDALANILGAN ADABIYOTLAR:

1. To'lqin Eshbek. Mediata'lim: yangi ta'lim usuli sifatida. http://sharh.uz/munosabat/item/17008–mediatalim–axborot–tv–radio–internet

2. Mamatova Ya., Sulaymanova S. O'zbekiston mediata'lim taraqqiyoti yo'lida. O'quv qo'llanma. -T.: «Extremum-rress», 2015. -94 b.

3. Martineau, M. (Ed.) (1988). L'enseignement du cinema et de l'audiovisuel. Paris: CinemAction, 299 p.

4. Freinet, C. (1927). L'imprimerie a l'ecole. Boulogne: Ferrary.

5. Sanobar Djumanova. International scientific-practical conference on the topic of "Problems and perspectives of modern technology in teaching foreign languages" VOLUME 2 | SPECIAL ISSUE 20 ISSN 2181-1784 SJIF 2022: 5.947 | ASI Factor = 1.7 48 w February 2022

6. Fedorov, A. (2001). Media Education: History, Theory and Methods. (in Russian). Rostov: CVVR, 708 p.