Xulosa. Elektron hujjat aylanish tizimi “Elektron hukumat” ning asosiy elementlaridan biri hisoblanadi. Chunki, ushbu tizimning muvaffaqiyatli yo`lga qo`yilishi nafaqat davlat hukumati va boshqaruvi organlari, xususiy sektor va aholi o`rtasidagi samarali hamkorlikni ta’minlaydi, balki mamlakatda axborot jamiyatini shakllantirishga yordam beradi. Yuqorida bayon qilingan dasturdagi o`zgartirishlar dasturning bundan keyingi qo`llanish sohasida effektivlikni oshirishga yordam beradi. Tashkilot yoki muassasalarda hujjat almashinuvi monitoringini olib borish jarayonida katta ahamiyat ko`rsatadi.

ADABIYOTLAR

1. 2011-yil 4-maydagi «Vazirlar Mahkamasining ijro etuvchi apparati bilan davlat va xo`jalik boshqaruvi organlari, mahalliy ijro etuvchi hokimiyat organlari o`rtasida himoyalangan yagona korporativ elektron pochtani va elektron hujjat aylanish tizimini joriy etish choralari to`g`risida»gi 126-son qarori //Uzinfocom jurnali. – № 6. 2011.
2. Mrs. C.Y., Munasinghe B.Sc. (OUSL); M.Sc.(Colombo), Open University of Sri Lanka, 2013. – 232 p.
3. www.buxdu.uz
4. http://cuteflow.org

УДК 004:681.124

XXI ASR – AXBOROT TEXNOLOGIYALARI ASRIDA “AXBORIY IMMUNITET” TUSHUNCHASI VA UNING DOLZARBLIGI

Muxlisov Sodiqjon Saidjonovich
BuxDU Axborot texnologiyalari kafedrasi o`qituvchisi

Tayanch so’zlar: immunitet, axborot, axborot xavfsizligi, axboriy immunitet, operatsion tizim, virus, atribut, fayl, sahifa, papka, tarmoq.
Ключевые слова: иммунитет, информация, информационная безопасность, информационный иммунитет, операционная система, вирус, атрибут, файл, страница, папка, сеть.
Key words: immunity, information, information security, information immunity, operation system, virus, attribute, file, page, net.

Ushbu maqolada hozirgi vaqtda dolzarb bo`lgan, kompyuter va axborot xavfsizligida asosiy o`rin tutadigan “Axboriy immunitet” haqida keng ma’lumot keltirilgan. Kompyuter va boshqa axborotni saqlovchi qurilmalarda saqlanadigan axborotlarning xavfsizligini ta’minlash to`g`risidagi savollar va ularning yechimi ko`rsatilgan. Bundan tashqari kompyuterlardagi zararli fayllarni o`chirish hamda antivirus dasturlari yordamida ulardan himoyalanish haqida mulohazalar keltirilgan.

В данной статье речь идёт об «информационном иммунитете», который необходим при использовании компьютеров и информационных технологий. Изучены вопросы защиты информации на компьютерах и других устройствах хранения данных. Также перечислены способы удаления вредоносных файлов на компьютере и защиты от них с помощью антивирусных программ.

The article deals with the term “Information security”, that has become important nowadays and which plays a significant role in the sphere computer and information security. The problems regarding the security of information in information storing devises and their solutions have been given in the article. Furthermore, the reflection on deleting harmful files and protecting the information from them with the help of antivirus programs have also been presented.

Kirish. Axborotlashgan jamiyat tezlik bilan shakllanib bormoqda. Axborot dunyosida davlat chegaralari degan tushuncha yo`qolib bormoqda. Jahon kompyuter tarmog`i davlat boshqaruvini tubdan o‘zgartirmoqda. Hududiy joylashishidan qat’i nazar, kundalik hayotimizga turli xildagi axborotlar Internet xalqaro kompyuter tarmog`i orqali kirib keldi. Shuning uchun ham mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va o‘zgartirish, yo`qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi.

Immunitet – ko`pchilikka tanish atama. Lotin tilida “ozod bo‘lish”, “qutulish” ma’nolarini anglatadi. Tibbiy nuqtayi nazardan organizmning kasalliklarga va viruslarga qarshi kurasha olish

qobiliyatini tushunamiz va aksar hollarda buni yagona ta'rif sifatida talqin qilamiz. Globallashuv jarayonida "mafkuraviy immunitet" tushunchasi hayotimizga kirib keldi. XXI asr axborot asrida, ya'ni axborotlashuv jarayonida bu atamani yangicha talqin qilishga arzirli sabablar mavjudligi "axborot immuniteti" termini shakllanishiga olib kelmoqda.

"Axboriy immunitet" atamasi qaysidir adabiyot yoki internet sahifalari orqali topilgani yo`q. Dars jarayonlarida kompyuter viruslari, buzg`unchi dasturlarga qarshi "qo'lbola" usullar yordamida kurashish haqidagi fikrlar ko`p marta muhokama qilinadi [1].

Axboriy immunitet – keraksiz axborotlarni qabul qilishga qarshilik ko`rsata olish qobiliyatimiz va kerakli axborotlarni buzilishlardan himoya qila olish ko`nikmalarimiz majmui.

Hozirda ko`pchilgimizning hayotiy faoliyatimiz kompyuter, internet kabi zamonaviy texnologiyalar bilan bog`liq. Shu jarayonda istasak, istamasak turli mazmun va maqsadga ega axborotlarga murojaat qilamiz yoki e'tiborimizga "taqdim etiladi". Axborotlar hozirda shu darajada ko`pki, ularni texnik yoki dasturiy vositalar yordamida oq-qoraga ajratish, saralash yoki filtrlash ancha mushkul bo'lib qoldi. *Ular bizni shu qadar o'z domiga tortmoqdaki, ba'zan foydali bo'lsa-da axborotlar oqimidan chiqa olmaslik holatlari mavjudligini inkor eta olmaymiz.* Bu masalaning bir tomoni.

Masalaning ikkinchi tomoni – kundalik hayotimizda shaxsiy yordamchimizga aylanib qolgan kompyuter nafaqat texnik vosita, balki virtual dunyomizni o'zida mujassam etgan, o'z o`rnida ajoyib kutubxonamiz; foto, audio va video albomlarimiz hamda turli repititorlar jamlangan darsxonamiz yoki ishxonamiz sifatida ham qadrlidir. Bu shaxsiy yordamchimizning yildan yilga ahamiyati ortib borishi bilan birga unga bo'lgan tahdidlar ham ko`payib bormoqda. Ayniqsa, universal xotira qurilmalari – fleshkalar ommalashgandan so`ng ma'lumotlar va fayllar almashish tezkor va qulay bo'lishi bilan birga kompyuter viruslarining erkin tarqalishiga olib keldi [2,3].

Albatta, ularga qarshi samarali kurashuvchi dasturiy vositalar juda ko`p va kompyuter xavfsizligini ta'minlay oladi. Lekin, ishonchli antivirus dasturlari samarali va muntazam ishlashi uchun ularni litsenzion sotib olish va ishlatishni, ma'lum muddatda bazalarini yangilab turishni talab etadi. Bu o'z yo'liga. Ish va o`qish faoliyatida har doim ham bunga imkon bo'lmaydi. Demakki, buzg`unchi dasturlar, viruslarga qarshi kurashishda nafaqat antivirus dasturlarda, balki o'zimizda ham ma'lum ma'noda "baza" shakllangan bo'lishi kerak.

Zararli bo'lmasa-da keraksiz axborotlarni rad eta olish, "beminnat tortiq etilayotgan" ba'zi axborotlarga qarshi reaksiya bera olish ko`nikmalarimiz hamda kompyuterda xavfsiz ishlash, viruslarga qarshi kurasha olish bilim va tajribalarimizni yuqorida tilga olgan "axboriy immunitet" atamasi bilan atashga yaqinroq kelib qoldik, fikrimizcha.

Masalaning birinchi tomonini batafsil yoritish va muammo yechimining muqobil yo'llarini taklif etish ancha vaqt, bilim va tajriba talab qiladi. Buni o'z sohasining fidoiy mutaxassislariga ishonib topshirgan holda masalaning ikkinchi tomoni – kompyuterda xavfsizroq ishlash, kompyuter viruslariga qarshi kurashishda oid ba'zi tajribalarimiz bilan o`rtoqlashmoqchiman.

Hozirgi zamonda viruslar asosan Windows operatsion tizimi (OT)da mavjud bo'lgan qulayliklardan "unumli" foydalanib o'z faoliyatini osongina amalga oshirmoqdalar. Masalan, Windows OT da tizim registri, ya`ni tizimning barcha parametrlarini saqlovchi va ularni sozlovchi baza bo`lib, u orqali foydalanuvchidan berkitilgan ko`pgina amallarni bajarsa bo`ladi: fayllarni avtomatik yuklash, "ko`rinmas" (скрытый, hidden) va tizimli (системный, system) atributli fayllarni eksplorer (проводник, explorer) orqali ko`rib bo`ladigan rejimga o`tishni taqiqlash, topshiriqlar dispetcheri (диспетчер задач, task manager) va register tahrirlovchisi – regedit dasturini ishlatishni taqiqlab qo`yish kabi "maqsadli" amallarni viruslar osongina bajarishadi. Buzg`unchi, hazilkash dasturlar esa Пуск tugmasini yo`qotish, Windows ning standart oynalari ko`rinishi va undagi yozuvlarni o`zgartirish kabi ishlarni shu registerdagi ma`lum parametrlarni o`zgartirish orqali bajara oladi [2].

Antivirus dasturlar bu viruslarni topishi va o`chirishi mumkin, lekin ular keltirgan zararlarni qayta tiklab bera olmaydi. Agarda ozgina qiziqish va bilimga ega bo`lsak, ularni o`zimiz ham bemalol to`g`rilay olamiz. Ko`pgina zamonaviy viruslar Windowsning avtoyuklash xizmati orqali o`zini-o`zi operativ xotiraga yuklashga asoslangan. Bu turdagi ko`pchilik viruslar worm.win32*.* nomlari bilan tasnif qilinadi, hammasida maqsad turlicha bo`lsa-da, ishlash uslubi deyarli bir xil.

Ular xotira qurilmalari (fleshkalar, lokal disklar) ning ildiz katalogi (корневая папка, root directory) ga o`zini avtomatik yuklovchi autorun.inf faylni yozib qo`yadi va asl virus qaysidir

“ko`rinmas” atributli katalog, Windows ning tizimli kataloglari, vaqtinchalik kataloglar (временные папки, temporary folders) ichida yashirinib olgan bo`ladi. Agarda shu disklarga “Мой компьютер” da 2 marta sichqoncha orqali bosib kirsangiz, ular avtomatik tarzda ishga tushadi. Xo`sh, unda avtoranning borligi yoki yo`qligi, virus ishga tushgan yoki tushmaganligining simptomlari qanday?

Bular:

– fleshkalar va lokal disklarni *Мой компьютер* orqali ochsangiz, ular mavjud oynada emas, balki yangi oynada ochiladi;

– “ko`rinmas” va “tizimli” atributli fayllarni namoyish etish uchun ko`rish rejimiga o`tib bo`lmaydi;

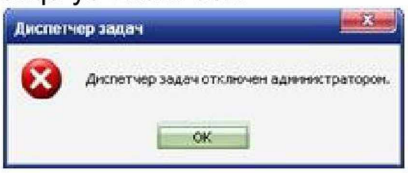
– ildiz kataloglarda bizga notanish nomdagi va *.exe, *.bat, *.com, *.sys, *.vbs kengaytmali fayllar hamda autorun.inf fayli hosil bo`ladi;

– topshiriqlar dispetcheri va register tahrirlovchisini http://www.pedagog.uz/distan/Dem_jam/10_mavzu/1m.htm siz ishga tushira olmaymiz;

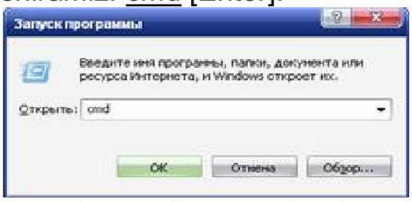
– kompyuter odatdagidan juda sekin ishlaydi, ya`ni operativ xotira va prosessor o`nlab ishga tushib ketgan viruslarning buzg`unchi amallari bilan band bo`ladi.

Keling, ishni ildiz katalogdan boshlaymiz (Tushunarli bo`lishi uchun quyidagi belgilashlarni kiritdik: to`rtburchak qavs [] ichida klaviaturada bosishimiz kerak bo`lgan tugma yoki tugmalar kombinatsiyasi + bilan, yozadigan buyruqlarimiz tagiga chizilgan, Win – Windows (Пуск) tugmasi, > belgi amallar ketma-ketligini ajratish uchun). Ildiz katalogni ochish uchun *Мой компьютер* orqali uning *Проводник* buyrug`i yoki oynaning adres qatoriga shu disk nomini yozgan holda oching. Aks holda unda virus mavjud bo`lsa, ishga tushish xavfi bor. Lekin, virus shunda ham ishga tushgan yoki bu maslahatga amal qilmay uni ishga tushirib yuborgan bo`lasiz.

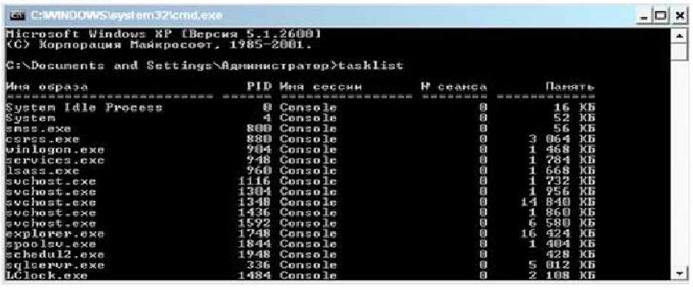
Endigi vazifa uni yoki u zararlagan dasturni operativ xotiradan “olib tashlash” bo`ladi. Buning uchun “*Диспетчер задач*”dan foydalanamiz: [Ctrl+Alt+Del]. Uni ishga tushirib *Процессы* bo`limidagi ayni vaqtda kompyuterda ishlab turgan dasturlar ro`yxatini ko`zdan kechiramiz. Unda shubhali va biz uchun noma`lum, nomi tasodifiy belgi va sonlar ketma-ketligidan iborat dasturlar bo`lsa, tezda ularni o`chiring. Iloji bo`lsa, hamma *.exe fayllarni bu ro`yxatdan o`chirish kerak (winlogon.exe, svchost.exe, system.exe, smss.exe, services.exe, lsass.exe, csrss.exe xizmatlardan tashqari), hatto explorer.exe ni ham. Agar *Диспетчер задач* ishlamasa, (virus uni ishlatishni “taqiqlab” qo`ygan) boshqa yo`l ham bor.



– [Win+R] tugmani bosamiz. *Выполнить* oynasi orqali *cmd.exe* (Cmd bu – buyruq protsessori bo`lib ko`pgina buyruqlarni yozish orqali tizimga ma`lum bir funksiyalarni bajartirishimiz mumkin.) ni ishga tushiramiz: cmd [Enter].

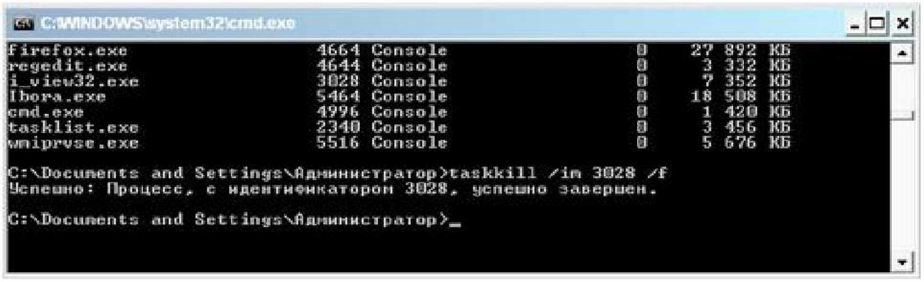


– *Cmd* ga ushbu buyruqni yozamiz: tasklist [Enter], ekranda operativ xotiradagi mavjud dasturlar ro`yxati hosil bo`ladi:



– Endi ularni o`chiramiz:

– Taskkill /im xxxx /f [Enter] bunda xxxx – ro`yxatda qaysidir dasturning identifikatsion raqami (PID – process ID)

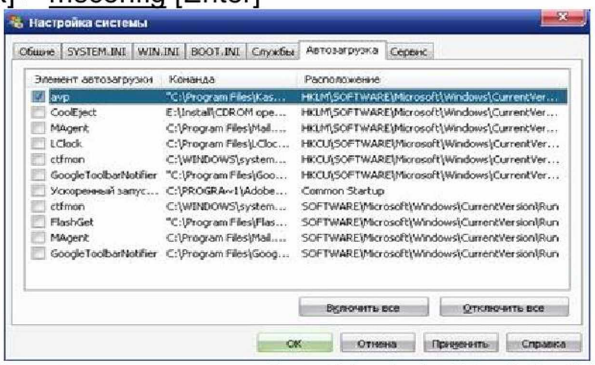


– *Успешно: Процесс, с идентификатором xxxx, успешно завершен* xabari beriladi.

– Taskkill /im xxxx /f [Enter] buyrug`i orqali yuqorida sanab o`tilgan barcha dasturlarni operativ xotiradan olib tashlaymiz.

Endigi vazifa avtoyuklanishga qo`yilgan dasturlarni registerdan o`chirib tashlash.

– Buning uchun: [Win+R] > msconfig [Enter]



– Hosil bo`lgan oynaning *автозагрузка* ro`yxatidagi shubhali fayllardan galochkalarni olib tashlaymiz.

Endigi vazifa virusga ko`rsatilgan yorliqlar va shubhali fayllarning o`zini kompyuter doimiy xotirasidan o`chiramiz. *Корзина*ni hamda quyidagi kataloglarni “chiqindi” fayllardan tozalaymiz:

–C:\Documents and Settings\[foydalanuvchi nomi]\Главное меню\ Програм-мы\Автозагрузка;

– C:\Documents and Settings\All Users\Главное меню\ Программы\ Автозагрузка;

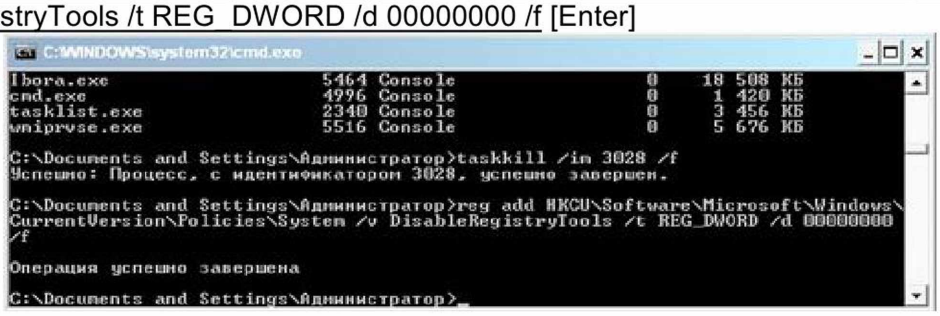
– C:\Documents and Settings\[foydalanuvchi nomi]\Local Settings\Temp;

– C:\WINDOWS\Temp.

Agar *Автозагрузка* papkasida o`zingiz bilgan ishonchli dasturlar yorlig`i bo`lsa, ular qolishi mumkin. Bunda C:\ — operatsion tizim o`rnatilgan disk. Sizda operatsion tizim qaysi diskka o`rnatilgan bo`lsa, yuqoridagi kataloglar shu disk ichida joylashgan bo`ladi.

Endi kompyuterni qayta yuklaymiz. Menimcha, operatsion tizim viruslardan xoli. Keling, endi viruslar operatsion tizimga yetkazgan ba`zi zararlarni (ular yuqorida keltirib o`tildi) sozlab chiqamiz. Buning uchun bizga albatta register tahrirlovchisi regedit kerak bo`ladi. Agar u o`chirilgan bo`lsa, uni *cmd* orqali yoqamiz: [Win+R]>cmd [Enter] va *cmd* ga quyidagi buyruqni kiritamiz:

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 00000000 /f [Enter]



Register tahrirlovchisini ishga tushiramiz: [Win+R] regedit [Enter] bo`limlar ro`yxatidan ushbu parametrlarni topib ularni o`zgartiramiz:

* Agar “ko`rinmas” atributli fayllarni ko`rish rejimiga o`tib bo`lmasa: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced] bo`limida quyidagilarni o`zgartiramiz:

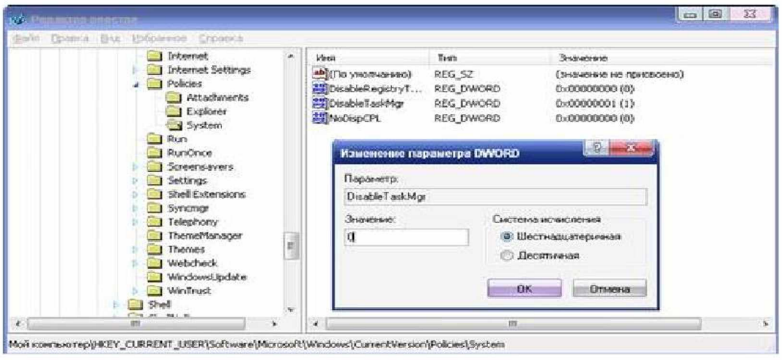
– Hidden=1

– ShowSuperHidden=1

* Agar *dispeycher zadach* ishlamasa:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System] bo`limida quyidagicha o`zgartirish qilamiz:

– DisableTaskMgr=0



Yuqorida ba`zi bir “qo`lbola” usullarni ko`rib o`tdik. Agar quyidagilarni kunaro amalga oshirib tursangiz, kompyuteringizning viruslardan xoli ishlash ehtimolligi yanada oshadi:

– *Avtoyuklanishlar* ro`yxatini nazorat qilib boring: [Win+R]> msconfig [Enter] > Автозагрузка;

– Operativ xotiradagi dasturlar ro`yxatini nazorat qilib turing [Ctrl+Alt+Del] > процессы;

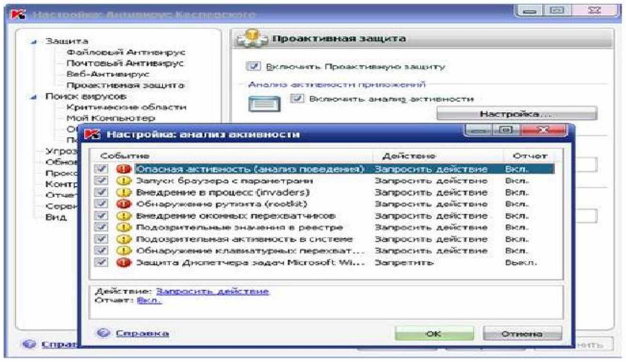
– *Корзина* va vaqtinchalik papkalarni tozalab turing;

– Disk yoki fleshkaning ildiz katalogiga *Мой компьютер* adres qatoriga disk yoki fleshka nomini yozib kiring: d:\ [Enter], f:\ [Enter] va hokazo yoki *проводник* buyrug`i orqali;

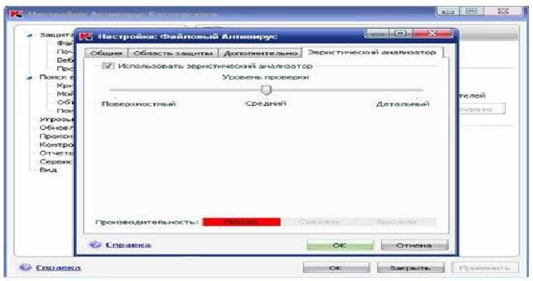
– Yuqorida berilgan simptomlar mavjud bo`lsa va ularni bartaraf etishga, antivirus dasturlar yordamida kompyuterni butunlay virusga tekshirishga harakat qiling.

Endi hozirda ko`pchilik foydalanuvchilar tomonidan ishlatiladigan *Антивирус Касперского* dasturida ishlash bo`yicha bir-ikki tavsiyalarni keltiraman:

– Agar dastur bazasi eski bo`lsa, *Проактивная защита* modulini to`liq ishga tushirib qo`ying;



– Agar dastur bazasini doimiy yangilash imkoni bo`lmasa dasturning barcha modullari uchun evristik tahlil (Эвристический анализатор)ni ishga tushiring. Shunda dastur viruslarga xos harakatlar (masalan, o`zini o`zi ko`paytirish, avtoyuklanishga fayl qo`shish, tizimli fayl va dasturlarga o`z kodini “yozib qo`yish”, tizimga yashirin patchlar kiritish kabilar) bajarayotgan dasturlarni virus sifatida gumon qilib sizga xabar beradi.



– Dasturda *iSwift* va *iChecker* texnologiyalarini ishga tushirib qo`ysangiz, antivirus diskdagi fayllarni signaturasi bo`yicha tez va qulay tekshirib chiqadi.

Maqola so`ngida e`tiboringizga *Windows*dagi “ayyorliklar”dan biri asosida lokal disklar, fleshkalar ildiz katalogiga viruslarni avtomatik yuklovchi autorun.inf fayliga qarshi immunitet yaratishni keltirib o`tamiz.

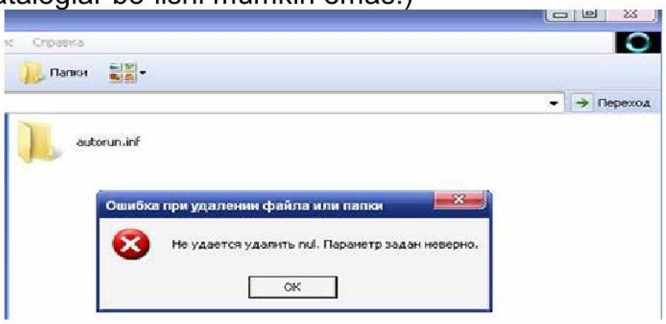
– *Cmd* ni ishga tushiramiz:[Win+R]> cmd [Enter];

– Immunitet qo`yilishi kerak bo`lgan katalogga o`tamiz (f:\ fleshka uchun immunitet yaratsak):Cd f: [Enter]

– Ildiz katalogda Autorun.inf nomli papka yaratamiz:Mkdir autorun.inf [Enter]

– Bu papka ichida Windows ruhsat bermaydigan papka (masalan nul nomli papka) yaratamiz: (ularni *Мой компьютер* orqali yaratib bo`lmaydi) Mkdir \\.\f:\autorun.inf\nul [Enter]

Immunitet tayyor. Xo`sh, endi uni o`chirib ko`ring-chi, o`charmikin? Yo`q, albatta! Demak, autorun.inf fayli bilan ishlovchi viruslar bu ildiz katalogga o`zini yuklovchi autorun.inf faylini yoza olmaydi. Sabab, bu yerda siz yaratgan immunitet katalog turibdi. (*Windows*da bir direktoryada bir xil nomdagi fayl yoki kataloglar bo`lishi mumkin emas!)



Xulosa: Maqolamizni axborot immuniteti tushunchasi haqida boshlagan edik. Yakunida esa xotira qurilmalari uchun immunitet katalog yaratish yo`llaridan birini keltirib o`tdik. O`ylaymizki, keraksiz va mentalitetimizga mos bo`lmagan axborotlarni qabul qilishga qarshilik ko`rsata olish qobiliyatimiz va kerakli axborotlarni buzilishlardan himoya qila olish ko`nikmalarimiz axborot asrida har bir kompyuter foydalanuvchilari uchun suv va havodek zarur.

ADABIYOTLAR

1. Muhammadiyev J.O`. Axborot xavfsizligi: muammo va yechimlar. Monografiya. – T., 2011. – B. 7-20.

2. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. – М., 2008. – С. 54-56.

3. Семененко В.А. Информационная безопасность: Учебное пособие. – М., 2008. – С. 48-53.