N.N. ZARIPOV Yu.T.HAMROYEVA

INFORMATIKA VA AXBOROT TEXNOLOGIYALARI

Internetda axborot xavfsizligini ta’minlash

BUXORO - 2016

Ushbu uslubiy qo’llanma oliy o’quv yurtlari, akademik litsey va kasb – hunar kollejlari talabalari uchun mo’ljallangan bo’lib, bunda internetdan unumli foydalanish yo’llari yoritib berilgan.

Tuzuvchilar: **Zaripov N.N.** Buxoro Davlar Universiteti Fizika-matematika fakulteti “Axborot texnologiyalari” kafedra o’qituvchisi
Hamroyeva Yu.T. Buxoro Madaniyat kolleji informatika fani o‘qituvchisi

Taqrizchilar: **Nurulloyev F.N.** Buxoro Davlar Universiteti Fizika-matematika fakulteti “Axborot texnologiyalari” kafedra o’qituvchisi
G‘aniyeva A. A. Buxoro Madaniyat kolleji o‘qituvchisi

Bilimdan qudratliroq kuch yo'q: bilim bilan qurollangan odam yengilmasdir.

M.GORKIY

KIRISH.

Ma'lumki, har qanday davlatning axborot resurslari uning iqtisodiy va harbiy salohiyatini belgilovchi omillaridan biri hisoblanadi. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirilishini ta'minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot-kommunikatsiyalar texnologiyalarini qo'llash keng ko'lamda amalga oshiriladi. Axborotlashgan jamiyat tezlik bilan shakllanib bormoqda. Axborot dunyosida davlat chegaralari degan tushuncha yo'qolib bormoqda. 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.

«Axborot erkinligi prinsiplari va kafolatlari to'g'risida»gi Qonunning qabul qilinishi har kimning axborotni erkin va moneliksiz olish hamda foydalanish huquqlarini amalga oshirishda, shuningdek, axborotning muhofaza qilinishi, shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta'minlashda muhim ahamiyat kasb etdi». Darhaqiqat, 2002-yil 12-dekabrda qabul qilingan bu qonunda axborot xavfsizligini ta'minlash sohasidagi davlat siyosati axborot sohasidagi ijtimoiy munosabatlarni tartibga solishga qaratilgan bo'ladi hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta'minlash sohasida davlat hokimiyati va boshqaruv organlarining asosiy vazifalari hamda faoliyat yo'nalishlarini belgilaydi deb belgilangan. Kompyuter tizimlari va tarmoqlarida axborotni muhofaza qilishi deganda, uzatilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta'minlash maqsadida turli vosita va usullarni qo'llash, choralarni ko'rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Internetda axborotlar xavfsizligini ta’minlash.

Umumiy axborot kengligining yaratilishi va shaxsiy kompyuterlarning amaliy jihatdan keng qo’llanilishi va kompyuter tizimlari va tarmoqlarining tatbiq etilishi axborotni himoya qilish muammosini yechish zarurligini keltirib chiqaradi.

Axborotni himoya qilish deganda zamonaviy kompyuter tizimlarida va tarmoqlarida uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotning ishonchliligini va butunligini tizimli ta’minlash maqsadida turli xil vositalarni va usullarni ishlatish, choralarni ko’rish va tadbirlarni o’tkazish tushuniladi.

Axborotni himoya qilish - bu:

- ► axborotning fizik butunligini ta’minlash, ya’ni axborot elementlarini to’siqlarga uc1hrashiga va yo’qolishiga yul qo’ymaslik;
- ► axborot butunligini saqlashda uning elementlarini almashtirishga (modifikasiyaga) yo’l qo’ymaslik;
- ► mos vakolatlarga ega bo’lmagan shaxslar yoki jarayonlar tomonidan taqiqlangan axborotni olinishiga yo’l qo’ymaslik;
- ► egalariga uzatilayotgan resurslar faqatgina tomonlar kelishgan shartlarga mos ravishda ishlatilishiga ishonch hosil qilinishi kerak.

Internetda ruxsatsiz kirish usullarining tasnifi

Global tarmoqlarning rivojlanishi va axborotlarni olish, qayta ishlash va uzatishning yangi texnologiyalari paydo bo‘lishi bilan Internet tarmog’iga har xil shaxs va tashkilotlarning e’tibori qaratildi. Ko‘plab tashkilotlar o’z lokal tarmoqlarini global tarmoqlarga ulashga qaror qilishgan va hozirgi paytda WWW, FTP, Gophes va boshqa serverlardan foydalanishmoqda. Tijorat maqsadida ishlatiluvchi yoki davlat siri bo‘lgan axborotlarning global tarmoqlar bo’yicha joylarga uzatish imkoni paydo bo’ldi va o’z navbatida, shu axborotlarni himoyalash tizimida malakali mutaxassislarga ehtiyoj tug’ilmoqda.

Global tarmoqlardan foydalanish bu faqatgina «qiziqarli» axborotlarni izlash emas, balki tijorat maqsadida va boshqa ahamiyatga molik ishlarni bajarishdan iborat. Bunday faoliyat vaqtida axborotlarni himoyalash vositalarining yo’qligi tufayli ko‘plab talofotlarga duch kelish mumkin.

Har qanday tashkilot Intenetga ulanganidan so’ng, hosil bo’ladigan quyidagi muammolarni hal etishlari shart:

• tashkilotning kompyuter tizimini xakerlar tomonidan buzilishi:

• Internet orqali jo’natilgan ma’lumotlarning yovuz niyatli shaxslar tomonidan o‘qib olinishi;

• tashkilot faoliyatiga zarar etkazilishi.

Internet loyixalash davrida bevosita himoyalangan tarmoq sifatida ishlab chiqilmagan. Bu sohada hozirgi kunda mavjud bo‘lgan quyidagi muammolarni keltirish mumkin:

• ma’lumotlarni yengillik bilan qo’lga kiritish;

• tarmoqdagi kompyuterlar manzilini sohtalashtirish;

• TCP/IP vositalarining zaifligi;

• ko‘pchilik saytlarning noto’g’ri konfiguratsiyalanishi;

• konfiguratsiyalashning murakkabligi.

Global tarmoqlarning chegarasiz keng rivojlanishi undan foydalanuvchilar sonining oshib borishiga sabab bo’lmoqda, bu esa o’z navbatida axborotlar xavfsizligiga taxdid solish ehtimolining oshishiga olib kelmoqda. Uzoq, masofalar bilan axborot almashish zaruriyati axborotlarni olishning qat’iy chegaralanishini talab etadi. Shu maqsadda tarmoqlarning segmentlarini har xil darajadagi himoyalash usullari taklif etilgan:

• erkin kirish (masalan: WWW-server);

• chegaralangan kirishlar segmenti (uzok masofada joylashgan ish joyiga xizmatchilarning kirishi);

• ixtiyoriy kirishlarni man etish (masalan, tashkilotlarning moliyaviy lokal tarmoqlari).

Internet global axborot tarmogi uzida nixoyatda katta hajmga ega bo‘lgan axborot resurslaridan milliy iqtisodning turli tarmoqlarida samarali foydanishga imkoniyat tug’dirishiga qaramasdan axborotlarga bo‘lgan xavfsizlik darajasini oshirmoqda. Shuning uchun ham Internetga ulangan har bir korxona uzining axborot xavfsizligini ta’minlash masalalariga katta e’tibor berishi kerak. Ushbu

tarmoqda axborotlar xavfsizligining yo’lga qo’yilishi yondashuvi quyida keltirilgan:

Lokal tarmoqlarning global tarmoqga qo’shilishi uchun tarmoqlar himoyasi administratori quyidagi masalalarni hal qilishi lozim:

— lokal tarmoqlarga global tarmoq, tomonidan mavjud xavflarga nisbatan himoyaning yaratilishi;

— global tarmoq fondalanuvchisi uchun axborotlarni yashirish imkoniyatining yaratilishi;

Bunda quyidagi usullar mavjud:

— kirish mumkin bo’lmagan tarmoq manzili orqali;

— Ping dasturi yordamida tarmoq paketlarini to’ldirish;

— ruxsat etilgan tarmoq manzili bilan taqiqlangan tarmoq manzili bo’yicha birlashtirish;

— ta’qiqlangan tarmoq protakoli bo’yicha birlashtirish;

— tarmoq bo’yicha foydalanuvchiga parol tanlash;

— REDIREST turidagi ICMP paketi yordamida marshrutlar jadvalini modifikatsiyalash;

— RIR standart bo’lmagan paketi yordamida marshrutlar jadvalini o’zgartirish;

— DNS spoofingdan foydalangan holda ulanish.

Internetda mavjud elektron to’lovlar xavfsizligini ta’minlash

Hozirgi kunda Internetda ko‘pgina axborot markazlari mavjud, masalan, kutubxonalar, ko‘p sohali ma’lumotlar bazalari, davlat va tijorat tashkilotlari, birjalar, banklar va boshqalar.

Internetda bajariladigan elektron savdo katta ahamiyat kasb etmokda. Buyurtmalar tizimining ko‘payishi bilan ushbu faoliyat yana keskin rivojlanadi. Natijada, haridorlar bevosita uydan yoki ofisdan turib, buyurtmalar berish imkoniga ega bo‘lishadi. Shu bois ham, dasturiy ta’minotlar va apparat vositalar ishlab chiqaruvchilar, savdo va moliyaviy tashkilotlar ushbu yo’nalishni rivojlantirishga faol kirishishgan.

Elektron savdo — global axborot tarmoqlari orqali maxsulotlarni sotish va pulli xizmatlar ko’rsatish demakdir.

Elektron savdoning asosiy turlari quyidagilardir:

• axborotlar sotuvi;

• elektron dukonlar;

• elektron banklar.

Axborotlar sotuvi asosan ma’lumotlar bazasidan On-line rejimda foydalanish uchun takdim etilishi mumkin.

Elektron dukonlar Internetda Web-site orqali tashkillashtiriladi. Bunda tovarlar ro’yxati, to’lov vositalari va boshqalar keltiriladi. Harid qilingan maxsulotlar oddiy pochta orqali jo’natilishi yoki agar ular elektron maxsulot bulsa, bevosita internetdan manzilga etkazilishi mumkin.

Elektron banklarni tashkil etishdan asosiy maqsad bankning doimiy harajatlarini kamaytirish va keng ommani qamrab olishdir. Shu bois, elektron banklar uz mijozlariga yukori foiz stavkalarini taklif qilishlari mumkin.

Elektron pochtaga ruxsatsiz kirish.

Internet tizimidagi elektron pochta juda ko‘p ishlatilayotgan axborot almashish kanallaridan biri hisoblanadi. Elektron pochta yordamida axborot almashuvi tarmoqdagi axborot almashuvining 40%ini tashkil etadi. Bunda axborot almashuvi bor-yo‘g‘i ikkita protokol: SMTP (Simple Mail Transfer Protocol) va ROR-3 (Post Office Rgolosol)larni ishlatish yordamida amalga oshiriladi. ROR-3 multimedia texnologiyalarining rivojini aks ettiradi, SMTP eca Appranet proyekti darajasida tashkil etilgan edi. Shuning uchun ham bu protokollarning hammaga ochiqligi sababli, elektron pochta resurslariga ruxsatsiz kirishga imkoniyatlar yaratilib berilmoqda:

SMTP server — dasturlarining nokorrekt o‘rnatilishi tufayli bu serverlardan ruxsatsiz foydalanilmoqda va bu texnologiya «spam» texnologiyasi nomi bilan ma’lum;

elektron pochta xabarlariga ruxsatsiz egalik qilish uchun oddiygina va samarali usullardan foydalanilmokda, ya’ni quyi qatlamlarda vinchesterdagi ma’lumotlarni o‘qish, pochta resurslariga kirish parolini o‘qib olish va xokazolar.

Elektron pochtadan foydalanish jarayonning asosiy maqsadi muhim xujjatlar bilan ishlashni to‘g‘ri yo‘lga qo‘yish hisoblanadi.

Bu yerda quyidagi yunalishlar bo‘yicha takliflarni e’tiborga olish zarur:

E-mail tizimidan tashkilot faoliyati maqsadlarida foydalanish;

shaxsiy maqsadda foydalanish;

maxfiy axborotlarni saqlash va ularga kirish:

elektron xatlarni saqlash va ularni boshqarish.

E-mail asoslari

Internetda asosiy pochta protokollariga quyidagilar kiradi:

SMTP (Simple Mail Transfer Protocol);

POP (Post Office Protocol);

IMAP (Internet Mail Access Protocol);

MIME (Multi purpose Internet Mail Extensions).

Bular bilan birma-bir tanishib chiqamiz:

SMTP — ushbu protokol asosida server boshqa tizimlardan xatlarni qabo‘l qiladi va ularni foydalanuvchining pochta ko‘tisida saqlaydi. Pochta serveriga interaktiv kirish xuquqiga ega bo‘lgan foydalanuvchilar o‘z kompyuterlaridan bevosita xatlarni o‘qiy oladilar. Boshqa tizimdagi foydalanuvchilar esa o‘z xatlarini ROR-3 va IMAP protokollari orqali o‘qib olishlari mumkin;

POP — eng keng tarkalgan protokol bo‘lib, serverdagi xatlarni, boshqa serverlardan qabul qilingan bo‘lsa-da, bevosita foydalanuvchi tomonidan o‘qib olinishiga imkoniyat yaratadi. Foydalanuvchilar barcha xatlarni yoki xozirgacha o‘qilmagan xatlarni ko‘rishi mumkin. Xozirgi kunda POP ning 3-versiyasi ishlab chiqilgan bo‘lib va autentifikatsiyalash usullari bilan boyitilgan;

IMAP — yangi va shu bois ham keng tarqalmagan protokol sanaladi.

Ushbu protokol quyidagi imkoniyatlarga ega:

pochta qutilarini yaratish, o‘chirish va nomini o‘zgartirish;

yangi xatlarning kelishi;

xatlarni tezkor o‘chirish;

xatlarni qidirish;

xatlarni tanlab olish.

IMAR sayoxatda bo‘lgan foydalanuvchilar uchun RORga nisbatan qulay bo‘lib hisoblanadi;

MIME — Internet pochtasining ko‘p maqsadli kengaytmasi so’zlari qisqartmasi bo‘lib, u xatlarning formatini aniqlash imkonini beradi, ya’ni:

matnlarni har xil kodlashtirishda jo‘natish;

xar xil formatdagi nomatn axborotlarni jo‘natish;

xabarning bir necha qismdan iborat bo‘lishi;

xat sarlavhasida har xil kodlashtirishdagi ma’lumotni joylashtirish.

Ushbu protokol elektron raqamli imzo va ma’lumotlarni shifrlash vositalaridan iborat bo‘lib, bundan tashqari uning yordamida pochta orqali bajariluvchi fayllarni xam jo‘natish mumkin. Natijada, fayllar bilan birga viruslarni xam tarqatish imkoniyati tug‘iladi.

E-maildagi mavjud muammolar

Elektron pochta bilan ishlash jarayonida quyidagi xatolarga yo‘l quyish mumkin:

xatni tasodifan jo‘natish;

xatning noto‘g‘ri manzil bo‘yicha jo‘natilishi;

xatlar arxivining keskin oshib ketishi oqibatida tizimning ishdan chiqishi;

yangiliklarga noto‘g‘ri obuna bo‘lish;

xatni tarqatish ro‘yxatida xatoga yo‘l quyish.

Agar tashkilotning pochta tizimi bevosita Internetga ulangan bo‘lsa, yo‘l qo‘yilgan xatolar oqibati keskin oshib ketadi.

Ushbu xatolarning oldini olish usullarining ba’zi birlari quyidagilar:

- foydalanuvchilarni o‘qitish;
- elektron pochta dasturlarini to‘g‘ri konfiguratsiyalash;
- Internetdagi protokollarga to‘liq amal qiluvchi dasturlarni qo‘llash.

Bundan tashqari elektron pochtaning shaxsiy maqsadda ishlatilishi tashkilot raxbariyati uchun ba’zi bir muammolarni keltirib chiqarishi mumkin, chunki E-mail manzilida tashkilot nomlari aks ettirilgan bo‘lishi extimoldan xoli emas. Natijada, shaxs jo‘natayotgan xat tashkilot nomidan deb qabul qilinishi mumkin. Shu bois, telefonlar kabi YE-maildan shaxsiy ishlar uchun foydalanishni cheklab quyish zarur bo‘ladi. Albatta, buni joriy qilish qiyin masala.

Elektron pochtada mavjud xavflar.

Elektron pochta bilan ishlash jarayonida quyidagi xavflar mavjud:

1. Jo‘natuvchining kalbaki manzili. Qabul qilingan xatni E-mail manzili aniqligiga to‘liq ishonch xosil qilish qiyin, chunki xat jo‘natuvchi o‘z manzilini qalbakilashtirishi mumkin.

2. Xatni qo‘lga kiritish. Elektron xat va uning sarlavhasi o‘zgartirilmasdan, shifrlanmasdan jo‘natiladi. Shu bois, uni yo‘lda qo‘lga kiritish va mazmunini o‘zgartirishi mumkin.

3. Pochta «bomba»si. Pochga tizimiga ko‘plab elektron xatlar jo‘natiladi, natijada tizim ishdan chiqadi. Pochta serverining ishdan chiqish xolatlari quyidagilardir:

disk to‘lib qoladi va keyingi xatlar qabul qilinmaydi. Agar disk tizimli bo‘lsa, u xolda tizim tamomila ishdan chiqishi mumkin;

kirishdagi navbatda turgan xatlar sonining oshib ketishi natijasida keyingi xatlar umuman navbatga quyilmaydi;

• olinadigan xatlarning maksimal sonini o‘zgartirish natijasida keyingi xatlar qabul qilinmaydi yoki o‘chiriladi;

foydalanuvchiga ajratilgan diskning to‘ldirilishi natijasida keyingi xatlar qabul qilinmaydi va diskni tozalab bo‘lmaydi.

4. «Qo‘rqinchli» (noxush) xat. Internet orqali olinadigan elektron xatlarning umuman noma’lum shaxslar tomonidan jo‘natilishi va bu xatda foydalanuvchilarning shaxsiyatiga teguvchi so‘zlar bo‘lishi mumkin.

Elektron pochtani himoyalash

Yuqorida keltirilgan xavflarga nisbatan quyidagi himoyalanish usullari ishlab chiqilgan:

- qalbaki manzildan himoyalanish, bu holda shifrlangan elektron imzolarni qo‘llash taklif qilinadi;

- xatni qo‘lga qiritishdan himoyalanish, bu xolda xabarni yoki jo‘natish kanalini shifrlash taklif qilinadi.

Ushbu himoyalash usullari bevosita kolgan xavflarning ulushini kamaytiradi.

Har qanday tashkilot Intenetga ulanganidan so‘ng, hosil bo‘ladigan quyidagi muammolarni hal etishlari shart:

tashkilotning kompyuter tizimini xakerlar tomonidan buzilishi:

Internet orqali jo‘natilgan ma’lumotlarning yovuz niyatli shaxslar tomonidan o‘qib olinishi;

tashkilot faoliyatiga zarar yetkazilishi.

Internet loyihalash davrida bevosita himoyalangan tarmoq sifatida ishlab chiqilmagan. Bu sohada xozirgi kunda mavjud bo‘lgan quyidagi muammolarni keltirish mumkin:

ma’lumotlarni yengillik bilan qo‘lga kiritish;

tarmoqdagi kompyuterlar manzilini soxtalashtirish;

TCP/IP vositalarining zaifligi;

ko‘pchilik saytlarning noto‘g‘ri konfiguratsiyalanishi;

konfiguratsiyalashning murakkabligi.

Global tarmoqlarning chegarasiz keng rivojlanishi undan foydalanuvchilar sonining oshib borishiga sabab bo‘lmokda, bu esa o‘z navbatida axborotlar xavfsizligiga taxdid solish ehtimolining oshishiga olib kelmoqda. Uzoq, masofalar bilan axborot almashish zaruriyati axborotlarni olishning qat’iy chegaralanishini talab etadi. Shu maqsadda tarmoqlarning segmentlarini xap xil darajadagi himoyalash usullari taklif etilgan:

erkin kirish (masalan: WWW-server);

chegaralangan kirishlar segmenti (uzok masofada joylashgan ish joyiga xizmatchilarning kirishi);

ixtiyoriy kirishlarni man etish (masalan, tashkilotlarning moliyaviy lokal tarmoqlari).

Internet global axborot tarmog‘i o‘zida nihoyatda katta xajmga ega bo‘lgan axborot resurslaridan milliy iqtisodning turli tarmoqlarida samarali foydanishga imkoniyat tug‘dirishiga qaramasdan axborotlarga bo‘lgan xavfsizlik darajasini oshirmokda. Shuning uchun xam Internetga ulangan xar bir korxona o‘zining axborot xavfsizligini ta’minlash masalalariga katta e’tibor berishi kerak.

Lokal tarmoqlarning global tarmoqarga qo‘shilishi uchun tarmoqlar himoyasi administratori quyidagi masalalarni xal qilishi lozim:

lokal tarmoqlarga global tarmoq, tomonidan mavjud xavflarga nisbatan himoyaning yaratilishi;

global tarmoq foydalanuvchisi uchun axborotlarni yashirish imkoniyatining yaratilishi;

Bunda quyidagi usullar mavjud:

— kirish mumkin bo‘lmagan tarmoq manzili orqali;

— Ping dasturi yordamida tarmoq paketlarini to‘ldirish;

— ruxsat etilgan tarmoq manzili bilan taqiqlangan tarmoq manzili bo‘yicha birlashtirish;

— ta’qiqlangan tarmoq protakoli bo‘yicha birlashtirish;

— tarmoq bo‘yicha foydalanuvchiga parol tanlash;

— REDIREST turidagi ICMP paketi yordamida marshrutlar jadvalini modifikatsiyalash;

— RIR standart bo‘lmagan paketi yordamida marshrutlar jadvalini o‘zgartirish;

— DNS spoofingdan foydalangan xolda ulanish.

Ishchi stansiyalarga xujumning asosiy maqsadi, asosan, qayta ishlanayotgan ma’lumotlarni yoki lokal saqlanayotgan axborotlarni olishdir. Bunday xujumlarnint asosiy vositasi «Troyan» dasturlar sanaladi. Bu dastur o‘z tuzilishi bo‘yicha kompyuter viruslaridan farq qilmaydi va kompyuterga tushishi bilan

o‘zini bilintirmasdan turadi. Boshqacha aytganda, bu dasturning asosiy maqsadi — tarmoq stansiyasidagi himoya tizimini ichki tomondan buzishdan iborat.

Bu xolatda masalani xal qilish ma’lum qiyinchilikka olib keladi, ya’ni maxsus tayyorlangan mutaxassis lozim yoki boshqa choralar qabo‘l qilish kerak bo‘ladi. Boshqa bir oddiy himoya usullaridan biri har qaysi ishchi stansiyadagi tizimli fayllar va xizmat sohasidagi ma’lumotlarning o‘zgarishini tekshirib turuvchi revizor (ingl. advizer— qiruvchi) o‘rnatish sanaladi.

Axborotlarni himoyalashning asosiy vosatalari

Haridor, kredit kartasi sohibi, bevosita tarmoq orqali to’lovlarni bajarish uchun ishonchli va himoyalangan vositalarga ega bo‘lishi lozim.

Hozirgi kunda SSL (Secure Socket Layer) va SET (Secure Electronic Transactions) protokollari ishlab chikilgan:

• SSL protokoli ma’lumotlarni kanal darajasida shifrlashda qo’llaniladi;

• SET xavfsiz elektron tranzaktsiyalari protokoli yakinda ishlab chikilgan bo‘lib, faqatgina moliyaviy ma’lumotlarni shifrlashda qo’llaniladi.

SET protokolining joriy etilishi bevosita Internetda kredit kartalar bilan to’lovlar sonining keskin oshishiga olib keladi.

SET protokoli quyidagilarni ta’minlashga kafolat beradi:

• axborotlarning to’liq maxfiyligi, chunki foydalanuvchi to’lov ma’lumotlarining himoyalanganligiga to’liq ishonch hosil qilishi kerak;

• ma’lumotlarning to’liq saqlanishi, ya’ni ma’lumotlarni uzatish jarayonida buzilmasligini kafolatlash. Buni bajarish omillaridan biri rakamli imzoni qo‘llashdir;

• kredit karta soxibining hisob rakamini audentifikatsiyalash, ya’ni elektron (raqamli) imzo va sertifikatlar hisob rakamini audentifikatsiyalash va kredit karta sohibi ushbu hisob rakamining haqiqiy egasi ekanligini tasdiqlash;

• tijoratchini uz faoliyati bilan shugullanishini kafolatlash, chunki kredit karta soxibi tijoratchining haqiqiyligini, ya’ni moliyaviy operatsiyalar bajarishini bilishi shart. Bunda tijoratchining rakamli imzosini va sertifikatini qo‘llash elektron to’lovlarning amalga oshirilishini kafolatlaydi.

Ma’lumki internet tarmoqlararo informatsiya almashinuvini ta’minlavchi magistiraldir. Uning yordamida dunyo bilimlar manba’iga kirish, qisqa vaqt ichida ko‘plab ma’lumotlar yig‘ish ishlab chiqarishning va uning texnik vositalarini masofadan turib boshqarish mumkin. SHu bilan bir qatorda internetning ushbu imkoniyatlaridan foydalanib turmoqdagi begona kompyuterlarni boshqarish ularning ma’lumotlar bazasiga kirish, nusxa ko‘chirish g‘arazli maqsadda turli xil viruslar tarqatish kabi noqonuniy ishlarni amalga oshirsh mumkin. Internetda mavjud bo‘lgan ushbu xavf, axborot xavfsizlik muammolari bevosita tarmoqlarning xususiyatlaridan kelib chiqadi. Bizning oldingi paragraflarda qayd etib o‘tganimizdek ixtiyoriy tarmoq xizmatini o‘zaro kelishilgan qoida (protokol) asosida ishlovchi juftlik «Server» va «Mijoz» dastur ta’minoti bajaradi. Ushbu protokollar miqyosida ham «Server», ham «Mijoz» dasturlari ruxsat etilgan amallarini (operatsiya) bajarish vositalariga ega. Masalan, NTTR protokoldagi formatlash komandalari Web sahifalarida joylashtirilgan tovush, vidio animatsiyalar va har xil aktiv ob’ektlar ko‘rinishidagi mikrodasturlar. Xuddi shunday ruxsat etilgan operatsiyalar, aktiv ob’ektlardan foydalanib internetda ba’zi bir noqonuniy harakatlarni oshirish tarmoqdagi kompyuterlarga va ma’lumotlar ba’zasiga kirish hamda ularga tahdid solish mumkin bo‘ladi.

Bundan tashqari axborot xavfsizlikni ta’minlash borasida internet foydalanuvchilari orasida o‘rnatilmagan tartib qoidalar mavjud. Ulardan ba’zi birlarini keltiramiz:

- ► Hech qachon hech kimga internetdagi o‘z nomingiz va parolingizni aytmang.
- ► Hech qachon hech kimga o‘zingiz va oila a’zolaringiz haqidagi shaxsiy hamda ishxonangizga oid ma’lumotlarni internet orqali yubormang.
- ► Elektron manzilingiz (E-mail)dan maqsadli foydalaning.
- ► Internet orqali dasturlar almashmang.
- ► Internetda tarqatilayotgan duch kelgan dasturlardan foydalanmang. Dasturlarni faqat ishonchli egasi ma’lum bo‘lgan serverlardan ko‘chiring.

- ► Elektron pochta orqali yuborilgan «aktiv ob’ektlar» va dasturlarni ishlatmang, yoki qo‘shimchali o‘z-o‘zidan ochiluvchi sizga noma’lum arxiv holidagi ma’lumotlarni ochmang.
- ► Elektron pochta xizmatidan foydalanayotganingizda ma’lumotlarni shifrlash zarur, ya’ni kriptografiya usullaridan foydalaning.
- ► Egasi siz uchun noma’lum bo‘lgan xatlarni ochmang.
- ► Egasi ma’lum bo‘lgan va uning sifatiga kafolat beruvchi antivirus dasturlardan foydalaning va ularni muntazam yangilab boring.
- ► Internetda mavjud bo‘lgan axborot resurslar va dasturlardan ularning mualliflari ruxsatisiz foydalanmang.

Axborot xavfsizligini ta’minlash.

Axborot xavfsizligini ta’minlash – bu foydalanuvchining axborotlarini himoyalashga quyilgan me’yor va talablarni bajarishidir. Axborot xavfsizligi esa bu axborot foydalanuvchilariga va ko‘plab axborot tizimlariga zarar keltiruvchi tabiiy yoki sun’iy xarakterga ega tasodifiy va uyushtirilgan ta’sirlardan axborotlarni va axborot kommunikatsiya tizim obyektlarining himoyalanganligidir.

Login tushunchasi. Login – shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi hisoblanadi.

Parol tushunchasi. Parol – uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi. U kompyuter bilan muloqot boshlashdan oldin, unga klaviatura yoki identifikatsiya kartasi yordamida kiritiladigan harfli, raqamli yoki harfli-raqamli kod shaklidagi mahfiy so‘zdan iborat.

Avtorizatsiya tushunchasi. Avtorizatsiya – foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni. Bunda foydalanuvchiga hisoblash tizimida ba’zi ishlarni bajarish uchun muayyan huquqlar beriladi. Avtorizatsiya shaxs harakati doirasini va u foydalanadigan resurslarni belgilaydi.

Ro‘yxatdan o‘tish tartibi. Ro‘yxatdan o‘tish – foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni. Ayrim veb-saytlar foydalanuvchilarga qo‘shimcha xizmatlarni olish va pullik xizmatlarga obuna bo‘lish uchun ro‘yxatdan o‘tishni, ya’ni o‘zi haqida ayrim ma’lumotlarni kiritishni (anketa to‘ldirishni) hamda login va parol olishni taklif qiladilar. Foydalanuvchi ro‘yxatdan o‘tgandan so‘ng tizimda unga qayd yozuvi (account) yaratiladi va unda foydalanuvchiga tegishli axborotlar saqlanadi.

Login va parolga ega bo‘lish shartlari. Biror shaxs o‘zining login va paroliga ega bo‘lishi uchun u birinchidan axborot kommunikatsiya tizimida ruyxatdan o‘tgan bo‘lishi kerak va shundan so‘ng u o‘z logini va parolini o‘zi hosil qilishi yoki tizim tomonidan berilgan login parolga ega bo‘lishi mumkin. Login va parollar ma’lum uzunlikdagi belgilar ketma-ketligidan tashkil topadi. Login va parollarning uzunligi va qiyinligi uning qanchalik xavfsizligini ya’ni buzib bo‘lmasligini ta’minlaydi.

Login va parolni buzish. Login va parolni buzish – bu buzg‘unchining biror bir maqsad yo‘lida axborot kommunikatsiya tizimi obyektlaridan foydalanish uchun qonuniy tarzda foydalanuvchilarga tegishli login va parollarini buzishdir. Bunda maxsus dastur yordamida login va parollar generatsiya qilib topiladi. Login va parollarning uzunligi bu jarayonning uzoq vaqt davom etishiga yoki generatsiya qilaolmasiligiga ishora bo‘ladi.

Login va parolni o‘g‘irlash. Login va parolni o‘g‘irlash – bu foydalanuvchilarning mahfiy ma’lumotlari bo‘lgan login va parollarga ega bo‘lish maqsadida amalga oshiriladigan internet firibgarligining bir turidir. Bu mashhur brendlar, masalan, ijtimoiy tarmoqlar, banklar va boshqa servislar nomidan elektron xatlarni ommaviy jo‘natish yo‘li orqali amalga oshiriladi. Xatda odatda tashqi ko‘rinishi asl saytdan farq qilmaydigan saytga to‘g‘ri ishorat mavjud bo‘ladi. Bunday saytga tashrif buyurgan foydalanuvchi firibgarga akkauntlar va bank hisob raqamlariga kira olishga ega bo‘lishga imkon beruvchi muhim ma’lumotlarni bildirishi mumkin. Fishing – ijtimoiy injeneriyaning bir turi bo‘lib, foydalanuvchilarning tarmoq xavfsizligi asoslarini bilmasligiga asoslangan.

Jumladan, ko‘pchilik oddiy faktni bilishmaydi: servislar qayd yozuvingiz ma’lumotlari, parol va shu kabi ma’lumotlarni yuborishni so‘rab hech qachon xat yubormaydi.

Resurslardan ruxsatsiz foydalanish va uning oqibatlari. Axborot-kommunikatsiya tizimining ixtiyoriy tarkibiy qismlaridan biri bo‘lgan hamda axborot tizimi taqdim etadigan imkoniyat mavjud bo‘lgan resurslardan belgilangan qoidalarga muvofiq bo‘lmagan holda foydalanishni cheklash qoidalariga rioya qilmasdan foydalanish – bu resurslardan ruxsatsiz foydalanish toifasiga kiradi. Bunday foydalanish natijasida quyidagi oqibatlar yuzaga kelishi mumkin:

axborotning o‘g‘irlanishi;

axborotni o‘zgartirish;

axborotning yo‘qotilishi;

yolg‘on axborotni kiritish;

axborotni qalbakilashtirish va h.k.

Kompyuter virusi. Kompyuter virusi – bu o‘z-o‘zidan ko‘payuvchi, kompyuter tarmoqlari va axborot tashuvchilari orqali erkin tarqaluvchi, hamda kompyuter va unda saqlanayotgan axborot va dasturlarga zarar yetkazuvchi dastur kodi yoki komandalar ketma-ketligi hisoblanadi. Kompyuter viruslari quyidagi xossalarga ega: o‘zidan nusxa ko‘chirish, axborotdan ruxsatsiz foydalanishni amalga oshirish. U o‘zining nusxalarini kompyuterlarda yoki kompyuter tarmoqlarida qayta ko‘paytirib va tarqatib, hamda qonuniy foydalanuvchilar uchun nomaqbul harakatlarni bajaradi. Virus, aksariyat hollarda nosozlik va buzilishlarga sabab bo‘ladi va biror hodisa yuz berishi bilan, masalan, aniq kunning kelishi bilan ishga tushirilishi mumkin.

Viruslarning turlari va vazifalari. Viruslarni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

yashash makoni;

operatsion tizim;

ishlash algoritmi xususiyati.

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

Fayl viruslar turli usullar bilan bajariluvchi fayllarga kiritiladi (eng ko‘p tarqalgan viruslar xili), yoki fayl yo‘ldoshlar (kompanon viruslar) yaratadi yoki faylli sistemalarni (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 vazifalari, odatda, to‘rt bosqichni o‘z ichiga oladi:

virusni xotiraga yuklash;

qurbonni qidirish;

topilgan qurbonni zaharlash;

destruktiv funksiyalarni bajarish.

Viruslarga qarshi kurashish usullari. Hozirgi kunda 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 yoki antiviruslar deb yuritiladi. Antivirus dasturlariga AVP, Doctorweb, Nod32 dasturlarini kiritish mumkin. Umuman barcha virusga qarshi dasturlar zaharlangan dasturlar va yuklama sektorlarning avtomatik tarzda tiklanishini ta’minlaydi.

Viruslarga qarshi kurashishning asosan quyidagi usullari mavjud:
Muntazam profilaktika ishlarini, ya’ni virusga tekshiruv ishlarini olib borish.

Taniqli virusni zararsizlantirish.

Taniqli bo‘lmagan virusni zarasizlantirish.

Hujum tushunchasi. Xujum tushunchasi – buzg‘unchining biror bir maqsad yo‘lida axborot kommunikatsiya tizimlarining mavjud himoyalash tizimlarini buzishga qaratilgan harakati.

Axborot xujumlari va undan saklanish qoidalari. Axborot hujumlari odatda 3 ga bo‘linadi:

Obyekt haqida ma’lumotlar yig‘ish (razvedkalash) hujumi.

Obyektdan foydalanishga ruxsat olish hujumi.

Xizmat ko‘rsatishdan voz kechish xujumi.

Axborot xujumlaridan saqlanishda birinchi navbatda axborot kommunikatsiya tizimi obyektlariga qilinayotgan hujumlarni topib olishda qo‘llaniladigan mexanizm va vositalarni qo‘llash kerak. Bularga tarmoqlararo ekran (FIREWALL) va xujumlarni aniqlash (IDS) vositalarini misol tariqasida keltirish mumkin.

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga yetarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Viruslarning ta’sir mexanizmlarini, ularga qarshi kurash usullari va vositalarini bilish viruslanishga qarshi harakatlarni samarali tashkil etish, ularning ta’siridan zararlanish ehtimolligini va talafatlarni minimumga keltirish imkonini beradi.

Kompyuter viruslari – bu KTda tarqalish va o‘zini o‘zi ishlab chiqish xususiyatiga ega bo‘lgan kichik hajmdagi bajariluvchi dasturlar. Viruslar KTda saqlanayotgan dasturiy vositalar yoki ma’lumotlarni yo‘q qilishi yoki o‘chirib yuborishi mumkin. Tarqalish jarayonida viruslar o‘zini modifikatsiyalashi mumkin. Viruslarning ommaviy tarqalib ketishi va ularning KT resurslariga ta’siri oqibatlarining jiddiyligi, maxsus antivirus vositalarini

va ularni qo‘llash usullarini yaratish va foydalanish zaruriyatini keltirib chiqardi.

Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:

– KTda viruslarni topish;

– virus – dasturlar ishini blokirovka qilish;

– viruslar ta’sirining oqibatlarini bartaraf qilish.

Viruslarni topishni, ularni joylashib olish bosqichida yoki hech bo‘lmaganda virusning buzg‘unchilik funksiyalarini boshlagunga qadar amalga oshirgan maqsadga muvofiq. Shuni ta’kidlash joizki, barcha turdagi viruslarni topishni kafolatlovchi antivirus vositalar mavjud emas. Virus topilgan holatda, uning tizimga keltirishi mumkin bo‘lgan zararli ta’sirini minimallashtirish maqsadida darhol virus-dasturning ishini to‘xtatilish lozim.

Virusning ta’sir oqibatlarini bartaraf qilish ikki yo‘nalishda olib boriladi:

– virusni o‘chirish;

– fayllarni, xotira sohalarini tiklash.

Tizimni qayta tiklash virus turiga, uni aniqlangan hamda zararlovchi ta’sirini boshlagan vaqtiga bog‘liq. Viruslar tizimga kirish jarayonida, o‘zini saqlaydigan joydagi ma’lumotlarni o‘chirib yuborsa hamda zararlovchi ta’siri natijasida ma’lumotlarni o‘zgartirish nazarda tutilgan bo‘lsa, zaxiraga olingan ma’lumotlarsiz yo‘qolgan ma’lumotlarni tiklab bo‘lmaydi. Viruslarga qarshi kurashda aniq bir ketma-ketlik va kombinatsiyada qo‘llaniluvchi, viruslarga qarshi kurashish usullarini hosil qiluvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi. KTning xavfsiz ishlashining asosiy shartlaridan biri, amalda sinovdan o‘tkazilgan va o‘zining yuqori samara berishini ko‘rsatgan bir qator qoidalarga rioya qilish hisoblanadi.

Birinchi qoida – qonuniy rasmiy yo‘l bilan olingan dasturiy mahsulotlardan foydalanish. Dasturiy ta’minotning qaroqchilik yo‘li bilan ko‘paytirilgan nusxalarida, rasmiy yo‘l bilan olinganlariga nisbatan viruslarning mavjudlik ehtimoli juda yuqori.

Ikkinchi qoida – axborotlar zaxirasini hosil qilish. Avvalo dasturiy ta’minotning distributivlari yozilgan tashuvchilarni saqlash zarur. Bunda tashuvchilarga ma’lumotlarni yozish imkoni berilgan bo‘lsa, imkon qadar uni blokirovka qilish zarur. Ishga taalluqli ma’lumotlarni saqlanishiga jiddiy yondashishi zarur. Muntazam ishga taalluqli fayllarning zaxira nusxalarini yaratib borish va ularni yozishdan himoyalangan yechib olinuvchi tashuvchilarda saqlash kerak. Agar bunday nusxalar yechib olinmaydigan tashuvchilarda yaratilayotgan bo‘lsa, ularni butunlay boshqa kompyuterning doimiy xotirasida yaratish maqsadga muvofiq. Bunda yoki faylning to‘liq nusxasi yoki kiritilayotgan o‘zgarishlarning nusxalari saqlanadi.

Uchinchi qoida – antivirus vositalaridan muntazam foydalanish. Antivirus vositalari muntazam yangilanib turilishi lozim.

To‘rtinchi qoida – yangi yechib olinadigan axborot tashuvchilardan va yangi fayllardan foydalanilganda ehtiyotkorlikka rioya qilish. Yangi yechib olinadigan tashuvchilar olinganda, albatta, yuklanuvchi va fayl viruslari mavjudligiga, olingan fayllar esa fayl viruslari mavjudligiga tekshirilishi lozim. Tekshiruv, skanerlovchi – dasturlar va evristik tahlilni amalga oshiruvchi dasturlar yordamida amalga oshirilishi kerak. Olingan hujjatlar va jadvallar bilan ishlashda, ushbu fayllar to‘liq tekshirilgunga qadar, matn va jadval muharrirlariga o‘rnatilgan makrokomandalarning bajarilishini taqiqlash zarur.

Beshinchi qoida – tizimga, ayniqsa taqsimlangan tizimlarga yoki jamoa bo‘lib foydalaniladigan tizimlarga, kiritilayotgan fayllarni va yechiladigan axborot tashuvchilarni maxsus ajratilgan kompyuterlarda tekshirish. Uni tizim administratori yoki ma’lumotlar xavfsizligiga mas’ul bo‘lgan shaxsning avtomatlashtirilgan ish joyidan amalga oshirilishi maqsadga muvofiq. Disk va fayllarni har tomonlama antivirus tekshiruvidan o‘tkaziluvidan so‘ng ularni tizimdan foydalanuvchilarga taqdim etish mumkin.

Oltinchi qoida – agar axborotlarni tashuvchilarga yozish nazarda tutilmagan bo‘lsa, bunday amallarni bajarilishini blokirovka qilish. Yuqorida keltirilgan tavsiyalarga doimiy rioya qilinishi virus dasturlar bilan zararlanish

ehtimolini ancha kamaytiradi va foydalanuvchini axborotlarni qaytib tiklab bo‘lmaydigan yo‘qotishlardan saqlaydi.

Texnik vositalar bilan himoyalanadigan axborotlarning turlari.

Axborotlarni muhofaza qilishning texnik vositalari – obyektning niqoblovchi (maskirovkalovchi) belgilari ochilishini bartaraf etish yoki kamaytirish, yolg‘on alomatlarni yaratish hamda texnik vositalar orqali axborotga ruxsatsiz kirishga to‘sqinlik qilishga mo‘ljallangan texnik vositalardir.

Ma’lumotlarni ruxsatsiz olishning obyektlari, usullari va vositalari quyidagilar bo‘lishi mumkin:

– bino, inshoat va qurilish konstruksiyalari (devorlar, tomlar, pollar, deraza va eshiklar, deraza oynalari, isitish va suv bilan ta’minlash tizimlari, havo tozalash quvurlari); konfedensial muzokara va majlislarni o‘tkazishda akustik tebranish kanallari bo‘yicha ma’lumotlarni ruxsatsiz olish;

– harakatlanuvchi obyektlar (avtomobil, temir yo‘l, suv va havo yo‘llari transportlari); konfedensial suhbatlar olib borishda – akustik tebranish kanallari bo‘yicha;

– kuchsiz tok texnika vositalari (aloqa qurilmalari, ovoz kuchaytirgichlar, audio- va telequrilmalar, elektr soatlar, radio eshittirishlar, yong‘in va qo‘riqlash signalizatsiya qurilmalari, elektr yozuv mashinkalari, konditsionerlar va ulardan foydalanilganda hamda bu vositalar yopiq tasnifli tadbirlarni o‘tkazishga mo‘ljallangan binoga joylashganda – elektroakustik o‘zgarishlar bo‘yicha va yondosh elektromagnit nurlanishlar va navodkalar hisobiga;

– hisoblash texnikasi vositalari (monitordagi tasvir efir orqali ma’lum bir masofaga uzatiladi);

– elektr manbasi va yerga ulangan o‘tkazgichlar tizimi (bu zanjir orqali ovoz kuchaytirish, kompyuterda kotiba bilan aloqa va shu kabilarni amalga oshiruvchi qurilmalarda qayta ishlanadigan ma’lumotlarni tutib olish mumkin);

– bino, avtomashina va boshqalardagi akustika (so‘z, tovushlar) – radiokanal va simlarda akustik radiomikrofonlar bo‘yicha hamda lazer qurilmalari orqali qo‘lga kiritish hisobiga;

– telefonda so‘zlashuvlar – radiokanal va simlar orqali telefon «juchoklar» hisobiga;

– faks orqali ma’lumotlar – yondosh nurlanishlar va navodkalar hamda aloqa liniyasi orqali qo‘lga kiritish hisobiga;

– yo‘naltirilgan mikrofonlar yordamida masofadagi shaxs akustikasi (so‘zi);

– uyali aloqa tarmog‘i orqali radioso‘zlashuvlar.

Himoyaning texnik vositalari – bu texnik qurilmalar, komplekslar yoki tizimlar yordamida obyektni himoyalashdir. Texnik vositalarning afzalligi keng ko‘lamdagi masalalarni hal etilishda, yuqori ishonchlilikda, kompleks rivojlangan himoya tizimini yaratish imkoniyatida, ruxsatsiz foydalanishga urinishlarga mos munosabat bildirishda va himoyalash amallarini bajarish usullaridan foydalanishning an’anaviyligida namoyon bo‘ladi.

Niqoblovchi belgilarning ochilishi (demaskirovka belgilari) deganda obyektning boshqa obyektlardan biron-bir tavsifi bilan farq qiladigan xususiyati tushuniladi. Farqlovchi tavsiflar son yoki sifatda baholanishi mumkin. Obyektning demaskirovka belgilari – bu himoya obyektiga xos xususiyat bo‘lib, undan texnik razvedka obyektni topishi yoki aniqlashi hamda obyekt haqida kerakli ma’lumotlarni olish uchun foydalanilishi mumkin. Axborotga egalik demaskirovka belgilarini tahlil etish orqali amalga oshiriladi. Demak, bu belgilar axborotni o‘ziga xos chiqib ketish kanali hisoblanadi. Demaskirovka belgilarni tarqatuvchilar bo‘lib to‘g‘ridan-to‘g‘ri bu belgilar bilan bog‘liq bo‘lgan fizik maydonlar hisoblanadi.

Obyektni topishda texnik razvedka vositalarining faoliyat ko‘rsatish jarayonida obyektning texnik demaskirovka belgilari aniqlanadi va uning mavjudligi haqida xulosa qilinadi. Demaskirovka belgilari quyidagilar bilan farq qiladi:

– joylashuvi – boshqa obyektlar va atrofdagi predmetlar orasida obyekt joylashuvini aniqlab beradigan belgi;

– tarkibiy ko‘rinish – obyektning tuzilishi va to‘laligicha ko‘rinishini aks ettiradigan kattaliklarini (tarkibi, soni va alohida obyektlarning joylashuvi, shakli va geometrik o‘lchamlari) aniqlovchi belgilar;

– faoliyati – obyektning fizik faoliyat yuritishi orqali uni ochib beruvchi belgilar.

Texnik demaskirovka belgilarini ikki toifaga bo‘lish mumkin:

– to‘g‘ridan-to‘g‘ri demaskirovka belgilari – himoya obyektining faoliyati va uning fizik maydonlari (elektromagnit, akustik, radiatsion va boshqalar) bilan bog‘liq bo‘lgan, himoya qilinadigan axborotga bog‘liq bo‘lmagan atrof-muhitning fizik maydoni fonidan farq qiladigan belgilar;

– bilvosita demaskirovka belgilari – obyektning faoliyat ko‘rsatishi natijasida atrof-muhitdagi o‘zgarishlar natijasida yuzaga keladigan belgilar (faoliyatning optik-vizual belgilari, geometrik o‘lchamlar, yoritilganlikning keskin farq qilinishi, ishlab chiqarish faoliyatidan qolgan izlar va hokazo).

Axborotni muhofaza qilishning samaradorlik ko‘rsatkichi himoya obyektining texnik demaskirovka belgilari kattaligi bo‘lib, unga nisbatan axborotni muhofaza qilish samaradorligining me’yorlari belgilanadi.

Kodlashtirish va kriptografiya usullari.

Axborotni himoyalash uchun **kodlashtirish** va **kriptografiya** usullari qo‘llaniladi.

Kodlashtirish deb axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoniga aytiladi.

Kriptografiya deb maxfiy xabar mazmunini shifrlash, ya’ni malumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq qo‘yish usuliga aytiladi.

Stenografiyaning kriptografiyadan boshqa o‘zgacha farqi ham bor. YA’ni uning maqsadi — maxfiy xabarning mavjudligini yashirishdir. Bu ikkala usul birlashtirilishi mumkin va natijada axborotni himoyalash samaradorligini oshirish

uchun ishlatilishi imkoni paydo bo‘ladi (masalan, kriptografik kalitlarni uzatish uchun). Kompyuter texnologiyalari stenografiyaning rivojlanishi va mukammallashuviga yangi turtki berdi. Natijada axborotni himoyalash sohasida yangi yo‘nalish — kompyuter stenogryafiyasi paydo bo‘ldi.

Kompyuter stenografiyasi rivojlanishi tendensiyasining tahlili shuni ko‘rsatadiki, keyingi yillarda kompyuter stenografiyasi usullarini rivojlantirishga qiziqish kuchayib bormoqda. Jumladan, ma’lumki, axborot xavfsizligi muammosining dolzarbligi doim kuchayib bormoqda va axborotni himoyalashning yangi usullarini qidirishga rag‘batlantirilayapti. Boshqa tomondan, axborot-kommunikatsiyalar texnologiyalarining jadal rivojlanishi ushbu axborotni himoyalashning yangi usullarini joriy qilish imkoniyatlari bilan ta’minlayapti va albatta, bu jarayonning kuchli katalizatori bo‘lib umumfoydalaniladigan Internet kompyuter tarmog‘ining juda kuchli rivojlanishi hisoblanadi.

Hozirgi vaqtda axborotni himoyalash eng ko‘p qo‘llanilayotgan soha bu — kriptografik usullardir. Lekin, bu yo‘lda kompyuter viruslari, «mantiqiy bomba»lar kabi axborotiy qurollarning kriptovositalarni buzadigan ta’siriga bog‘liq ko‘p yechilmagan muammolar mavjud. Boshqa tomondan, kriptografik usullarni ishlatishda kalitlarni taqsimlash muammosi ham bugungi kunda oxirigacha yechilmay turibdi. Kompyuter steganografiyasi va kriptografiyalarining birlashtirilishi paydo bo‘lgan sharoitdan qutulishning yaxshi bir yo‘li bo‘lar edi, chunki, bu holda axborotni himoyalash usullarining zaif tomonlarini yo‘qotish mumkin.

Kriptografiya nuqtai – nazaridan shifr — bu kalit demakdir va ochiq ma’lumotlar to‘plamini yopiq (shifrlangan) ma’lumotlarga o‘zgartirish kriptografiya o‘zgartirishlar algoritmlari majmuasi hisoblanadi.

Kalit — kriptografiya o‘zgartirishlar algoritmining ba’zi-bir parametrlarining maxfiy holati bo‘lib, barcha algoritmlardan yagona variantini tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy ko‘rsatkich bo‘lib kriptomustahkamlik hisoblanadi.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar quyiladi:

yetarli darajada kriptomustaxkamlik;

shifrlash va qaytarish jarayonining oddiyligi;

axborotlarni shifrlash oqibatida ular hajmining ortib ketmasligi;

shifrlashdagi kichik xatolarga tasirchan bo‘lmasligi.

Ushbu talablarga quyidagi tizimlar javob beradi:

o‘rinlarini almashtirish;

almashtirish;

gammalashtirish;

analitik o‘zgartirish.

O‘rinlarini almashtirish shifrlash usuli bo‘yicha boshlang‘ich matn belgilarining matnning ma’lum bir qismi doirasida maxsus qoidalar yordamida o‘rinlari almashtiriladi.

Almashtirish shifrlash usuli bo‘yicha boshlangich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtirilali.

Gammalashtirish usuli bo‘yicha boshlang‘ich matn belgilari shifrlash gammasi belgilari, ya’ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

Taxliliy o‘zgartirish usuli bo‘yicha boshlang‘ich matn belgilari analitik formulalar yordamida o‘zgartiriladi, masalan, vektorni matritsaga ko‘paytirish yordamida. Bu yerda vektor matndagi belgilar ketma-ketligi bo‘lsa, matritsa esa kalit sifatida xizmat qiladi.

O‘rinlarni almashtirish usullari

Ushbu usul eng oddiy va eng kadimiy usuldir. O‘rinlarni almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin:

— shifrlovchi jadval;

— sehrli kvadrat.

Shifrlovchi jadval usulida kalit sifatida quyidagilar qo‘llaniladi:

— jadval o‘lchovlari;

— so‘z yoki so‘zlar ketma-ketligi;

— jadval tarkibi xususiyatlari.

Antivirus dasturlarni o`rganish

Kompyuter viruslaridan himoyalanish uchun ikki shartni bajarish: kompyuter gigiyena talablariga rioya etish, antivirus dasturlaridan foydalanish kerak.

Kompyuter gigiyena talablari.

Notanish kishilardan elektron pochta orqali kelgan fayllarni hech kachon ochmang. Tanish manzil bo`yicha xat kelgan taqdirda ham juda eqtiyot bo`ling - tanishlaringiz va hamkasblaringiz kompyuterlarida virus borligidan bexabar virus ulardan o`z nusxasini yuborayotgan bo`lishi mumkin.

Skanerli antivirusda hamma disketalar, kompakt-disklar va boshqa axborot tashuvchilarni, shuningdek Internet hamda boshqa tarmoqlardan olinadigan fayllarni har doim yaxshilab tekshiring.

Begona foydalanuvchilarni kompyuteringizga qo`yishda ehtiyot bo`ling.

Ma'lumotlaringizning saqlanish ishonchliligini oshirish uchun, vaqt-vaqti bilan axborot tashuvchilarda ma'lumotlarni zaxiraviy arxivlab turing.

Bugungi kunda antivirus xavfsizligini ta'minlashni 5 asosiy tarmoqqa ajratish mumkin.

Antivirus skanerlari. Skanerlarning ishlash tarzi hamma fayllar, yuklanuvchi sektorlar va xotirani virusning noyob dastur kodi bor-yo`sligini tekshirishga asoslangan.

Antivirus monitorlari. U skanerlarning bir ko`rinishi bo`lib, monitorlar har doim kompyuter xotirasida aniq vaqt ko`lamida fayllar, yuklanuvchi sektor va xotirani fonli tekshiradi.

**O`zgarish taftishchilari.** Bu turdagi antivirus dasturlarining vazifasi fayl va tizimli sektorlardan original tamra olishdan iborat. Bu tamralar ma'lumot omborida saqlanadi. Keyingi yuklanganda tekshiruvchi tamrani original bilan solishtiradi va foydalanuvchiga qodir bo`lgan o`zgarishlar qaqida xabar beradi.

Immunizatorlar. Antivirusli immunizator dasturlari ikki turga bo`linadi: zararlanganlik qaqida xabar beruvchi immunizatorlar va zararlanishni virusning biron turi bilan blokirovkalovchi immunizatorlar.

Birinchi turi, odatda, faylning oxiriga yozilib, faylning har bir yuklanishida uning o`zgargan-o`zgarmaganligini tekshiradi. Bunday immunizatorlar zararlangan faylda berkinib yotgan ko`rinmas viruslarni aniqlay olmaydi.

Ikkinchi turi esa tizimni virusning aniq bir turi bilan zararlanishdan qimoya qiladi. Buning uchun fayllarga shunday bir shakl beriladiki, virus ularni zararlangan deb hisoblashi kerak bo`ladi. Rezident virusdan qimoyalanish uchun esa kompyuter xotirasiga virus nusxasiga o`xshatma dastur kiritiladi. Virus yuklanib, unga tuknashganda tizim zararlanganligini paysaydi.

Albatta, fayllarni barcha viruslardan saqlash mumkin emas: ulardan xar birining zararlanganligini aniqlash usuli mavjud. Shuning uchun xam immunizatorlar keng tarqalmadi, hozirgi vaqtda ular deyarli qo`llanmaydi.

Axloq blokiratorlari. Yuqorida aytib o`tilgan antiviruslarning qech biri asosiy muammo - noma'lum viruslardan qimoyalanishni qal etmaydi. Binobarin, kompyuter tizimlari antiviruschilar virusga harshi "vosita" ishlab chisargunga qadar qimoyasiz qolyapti.

Bu masalani qal etishda axloq, blokiratorlari istiqbolli yo`nalishlardan hisoblanadi. Bu dastur har doim kompyuter operativ xotirasida bo`lib, tizimdagi turli qodisalarni tutib oladi. Shubqali virus yoki zararli dastur qilishi mumkin bo`lgan harakatni sezganda blokirator bu harakatni man etadi yoki foydalanuvchidan izm so`raydi.

Hozirgi vaqtda respublikamizda keng tarqalgan antiviruslar, asosan AVP, NAV, Dr.Web.

Ma'lumki, Kasperskiy laboratoriyasi dunyodagi barcha antivirus ishlab chiharuvchilari orasida yetakchi o`rinlardan birini egallaydi. Uning ruscha va inglizcha versiyalari mavjud. Antiviral ToolKitPro antivirusida viruslardan qimoyalanishning skaner va monitorli usulidan foydalanilgan, bugungi kunda 55 845 (2002 yil 2 iyul xolatiga) virusdan davolaydi.

Antivirus dasturlarni o`rnatish

Hozirgi vaqtda viruslarni yo’qotish uchun ko’pgina usullar ishlab chiqilgan va bu usullar bilan ishlaydigan dasturlarni antiviruslar deb atashadi.

Antiviruslarni, qo’llanish usuliga ko’ra, quyidagilarga ajratishimiz mumkin: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar.

Detektorlar — virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo’yicha tezkor xotira va fayllarni ko’rish natijasida ma`lum viruslarni topadi va xabar beradi. YAngi viruslarni aniqlab olmasligi detektorlarning kamchiligi hisoblanadi.

Faglar — yoki doktorlar, detektorlarga xos bo’lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oldingi xolatiga qaytaradi.

Vaktsinalar — yuqoridagilardan farqli ravishda himoyalanayotgan dasturga o’rnatiladi. Natijada dastur zararlangan deb hisoblanib, virus tomonidan o’zgartirilmaydi. Faqatgina ma`lum viruslarga nisbatan vaktsina qilinishi uning kamchiligi hisoblanadi. Shu bois ham, ushbu antivirus dasturlari keng tarqalmagan.

Privivka — fayllarda xuddi virus zararlagandek iz qoldiradi. Buning natijasida viruslar «privivka qilingan» faylga yopishmaydi.

Filtrlar — qo’riqlovchi dasturlar ko’rinishida bo’lib, rezident holatda ishlab turadi va viruslarga xos jarayonlar bajarilganda, bu haqda foydalanuvchiga xabar beradi.

Revizorlar — eng ishonchli himoyalovchi vosita bo’lib, diskning birinchi holatini xotirasida saqlab, undagi keyingi o’zgarishlarni doimiy ravishda nazorat qilib boradi.

Detektor dasturlar kompyuter xotirasidan, fayllardan viruslarni qidiradi va aniqlangan viruslar xaqida xabar beradi.

Doktor dasturlari nafaqat virus bilan kasallangan fayllarni topadi, balki ularni davolab, dastlabki holatiga qaytaradi. Bunday dasturlarga Aidstest, Doctor Web dasturlarini misol kilib keltirish mumkin. Yangi viruslarning to’xtovsiz paydo bo’lib turishini hisobga olib, doktor dasturlarini ham yangi versiyalari bilan almashtirib turish lozim.

Filtr dasturlar kompyuter ishlash jarayonida viruslarga xos bo’lgan shubhali harakatlarni topish uchun ishlatiladi.

Bu harakatlar quyidagicha bo’lishi mumkin:

- fayllar atributlarining o’zgarishi;
- disklarga doimiy manzillarda ma`lumotlarni yozish;
- diskning ishga yuklovchi sektorlariga ma`lumotlarni yozib yuborish.

Tekshiruvchi (revizor) dasturlari virusdan himoyalanishning eng ishonchli vositasi bo’lib, kompyuter zararlanmagan holatidagi dasturlar, kataloglar va diskning tizim maydoni holatini xotirada saqlab, doimiy ravishda yoki foydalanuvchi ixtiyori bilan kompyuterning joriy va boshlangach holatlarini bir-biri bilan solishtiradi. Bunga ADINF dasturini misol qilib keltirish mumkin.

Viruslarga qarshi chora-tadbirlar

Kompyuterni viruslar bilan zararlanishidan saqlash va axborotlarni ishonchli saqlash uchun quyidagi qoidalarga amal qilish lozim:

- kompyuterni zamonaviy antivirus dasturlar bilan ta`minlash;
- disketalarni ishlatishdan oldin har doim virusga qarshi tekshirish;
- qimmatli axborotlarning nusxasini har doim arxiv fayl ko’rinishida saqlash.

Kompyuter viruslariga qarshi kurashning quyidagi turlari mavjud:

- viruslar kompyuterga kirib buzgan fayllarni o’z holiga qaytaruvchi dasturlarning mavjudligi;
- kompyuterga parol bilan kirish, disk yurituvchilarning yopiq turishi;
- disklarni yozishdan himoyalash;
- litsenzion dasturiy ta`minotlardan foydalanish va o’g’irlangan dasturlarni qo’llamaslik;
- kompyuterga kiritalayotgan dasturlarning viruslarning mavjudligini tekshirish;
- antivirus dasturlaridan keng foydalanish;
- davriy ravishda kompyuterlarni antivirus dasturlari yordamida viruslarga qarshi tekshirish.

Antivirus dasturlaridan DrWeb, Adinf, AVP, VootCHK va Norton Antivirus, Kaspersky Security , Symantek Antivirus kabilar keng foylalaniladi.

Antivirus dasturini o’rnatish

Hozirda kompyuterlarni viruslardan himoya qilish uchun turli antivirus dasturlari va yordamchi vositalari mavjuddir. Bunday dasturlar ichida Kasperskiy antivirusi mashhur. Ushbu dasturni bugungi kunda bir nechta versiyalari mavjud.

Kasperskiy 5.0, Kasperskiy 6.0, Kasperskiy 7.0, Kasperskiy 2009 lar bunga misoldir. Kasperskiy antivirusini 6.0 versiyasini o'rnatish, bazasini yangilash va ishlatishni ko'rib chiqamiz.

Tarmoqlararo ekran va uning vazifalari

Tarmoqlararo ekran — himoyalash vositasi bo'lib, ishonchli tarmoq, va ishonchsiz tarmoq orasida ma'lumotlarga kirishni boshqarishda qo'llaniladi.

Tarmoqlararo ekran ko'p komponentli bo'lib, u internetdan tashkilotning axborot zaxiralarini himoyalash strategiyasi sanaladi ya'ni tashkilot tarmog'i va internet orasida qo'riqlash vazifasini bajaradi.

Tarmoqlararo ekranning asosiy funksiyasi — ma'lumotlarga egalik qilishni markazlashtirilgan boshqaruvini ta'minlashdan iborat.

Tarmoqlararo ekran quyidagi himoyalarni amalga oshiradi:

• o'rinsiz trafiklar, ya'ni tarmoqda uzatiladigan xabarlar oqimini taqiqlash;

• qabul qilingan trafikni ichki tizimlarga yo'naltirish;

• ichki tizimning zaif qismlarini yashirish bilan internet tomonidan uyushtiriladigan hujumlardan himoyalash;

• barcha trafiklarni bayonlashtirish;

• ichki ma'lumotlarni, masalan tarmoq topologiyasini, tizim nomlarini, tarmoq uskunalarini va foydalanuvchilarning identifikatorlarini Internetdan yashirish;

• ishonchli autentifikatsiyani ta'minlash.

Ko'pgina adabiyotlarda **tarmoqlararo ekran** tushunchasi **brandmauer** yoki **Fire Wall** deb yuritilgan. Umuman bularning hammasi yagona tushunchadir.

Tarmoqlararo ekran — bu tizim, umumiy tarmoqni ikki qismga ajratib, tarmoqlararo himoya vazifasini o'taydi va ma'lumotlar paketining chegaradan o'tish shartlarini amalga oshiradigan qoidalar to'plami hisoblanadi.

Odatda tarmoqlararo ekran ichki tarmoqlarni global tarmoqlardan, ya'ni internetdan himoya qiladi. Shuni aytish kerakki, tarmoqlararo ekran nafaqat Internetdan, balki korporativ tarmoqlardan ham himoya qilish qobiliyatiga egadir.

Har qanday tarmoqlararo ekran ichki tarmoqlarni to’liq himoya qila oladi deb bo’lmaydi.

Internet xizmati va hamma protokollarning amaliy jihatdan axborotlarga nisbatan himoyasining to’liq bulmaganligi muammosi bor. Bu muammolar kelib chikishining asosiy sababi Internetning UNIX operatsion tizim bilan borlikligida.

TCR/IR (Transtnission Control Protokol/lnternet Protocol) Internetning global tarmog’ida kommunikatsiyani ta’minlaydi va tarmoqlarda ommaviy ravishda qo’llaniladi, lekin ular ham himoyani etarlicha ta’minlay olmaydi, chunki TCP/IP paketining boshida xaker hujumi uchun qulay ma’lumot ko’rsatiladi.

Internetda elektron pochtani jo’natishni oddiy protokol pochta transport xizmati amalga oshiradi (SMTP - Simple Mail Transfer Protocol). Bu protokolda mavjud bo‘lgan himoyalashning muhim muammolaridan biri - foydalanuvchi junatuvchining maizilini qura olmasligidir. Bundan foydalanib xaker katta miqdorda pochta xabarlarini junatishi mumkin, bu esa ishchi pochta serverni haddan tashkari band bo‘lishiga olib keladi.

Internetda ommaviy tus olgan dastur bu Sendmail elektron pochtasidir. Sendmail tomonidan jo’natilgan xabarlar bosqinchi xaker axborot shaklida foydalanishi mumkin.

Tarmoq nomlari xizmati (Domain Name System — DNS) foydalanuvchilar nomi va xost-kompyuterini - manzilini ko’rsatadi. DNS kompaniyaning tarmoq tuzilishi haqida ma’lumotlarni saqlaydi. DNSning muammolaridan biri shundaki, bundagi ma’lumotlar bazasini mualliflashtirilmagan foylalanuvchilardan yashirish ancha qiyin. Buning natijasida, xakerlar DNS ni ko‘pincha xost-kompyuterlarning ishonchli nomlari haqida ma’lumotlar manbasidan foydalanish uchun ishlatishi mumkin.

Uzoq, terminallar emulyatsiyasi ximati uzoq, tizimlarni bir-biriga ulash uchun xizmat qiladi. Bu serverdan foydalanuvchilar TELNET serveridan ro’yxatdan o’tish va uz nomi va parolini olishi lozim. TELNET serveriga ulangan xaker dasturni shunday urnatishi mumkinki, buning natijasida u foydalanuvchining nomi va parolini yozib olish imkoniga ega bo’ladi.

World Wide Web — WWW bu tizim Internet yoki intratarmoqlardagi har xil serverlar ichidagi ma’lumotlarni ko’rish uchun xizmat qiladi. WWW ning acosiy xossalaridan biri — Tarmoqlararo ekran orqali aniq protokol va manzillarni fil’trlash zarurligini tarmoqning himoyalash siyosati qarori bilan hal etilishidir.

Har qanday tashkilotning **tarmoq xavsizligi siyosati** ikki qismdan iborat buladi: tarmoq servislaridan foydalanish tarmoqlararo ekranni qo‘llash.

Tarmoq servislaridan foydalanish siyosatiga mos ravishda Internetda servislar ruyxati aniqlanadi. Bu servislarga foydalanuvchilar cheklangan kirish bilan ta’minlanadi.

Kirish usullarining cheklanilishi — foydalanuvchilar tomonidan Internet servislariga chet yo’llar orqali ruxsatsiz kirishni taqiqlash ma’nosini bildiradi.

Tarmoq servislariga kirish siyosati, odatda, quyidagi prinsiplarga moyil bo’ladi:

- Internetdan ichki tarmoqka kirishni taqiqlash, lekin ichki tarmoqdan internetga kirishga ruxsat berish;

- vakolatlangan tizimlarga Internetdan ichki tarmoqqa cheklanilgan kirishga ruxsat berish.

Tarmoqlararo ekranlarga kuyiladigan vazifaviy talablar quyidagilardan iborat.

• tarmoq darajasida fil’trlashga talab;

• amaliy darajada fil’trlashga talab;

• administratsiyalash va fil’trlash koidalarini urnatish bo’yicha talab;

• tarmoqli autentifikatsiyalash vositalariga talab;

• ishlarni qayd qilish va hisobni olib borish bo’yicha talab.

Tarmoqlararo ekranning asosiy komponentlari

Tarmoqlararo ekranlarning komponentlari sifatida quyidagilarni keltirish mumkin: fil’trlovchi –yo’llovchi; tarmoq, darajasidagi shlyuzlar; amaliy darajadagi shlyuzlar.

Fil’trlovchi-yullovchi — yo’llovchi, ya’ni kompyuter tarmog’ida ma’lumotlarni manzilga etkazuvchi dasturlar paketi yoki serverdagi dastur bo‘lib, u kiradigan va chiqadigan paketlarni fil’trlaydi. Paketlarni fil’trlash, ya’ni ularni

aniq to’plamga tegishliligini tekshirish, TCP/IP sarlavxasidagi ma’lumotlar bo’yicha amalga oshiriladi.

Fil’trlashni anik xost-kompyuter, ya’ni tarmoqdagi fayl va kompyuter zaxiralariga kirishni amalga oshiruvchi kompyuter yoki port, ya’ni xabarlarni jo’natish yoki qabul qilish maqsadida mijoz va server tomonidan ishlatiladigan va odatda 16 bitli son bilan nomlanadigan dastur bilan ulanishda amalga oshirish mumkin. Masalan, foydalanuvchiga keraksiz yoki ishonchsiz xost-kompyuter va tarmoqlar bilan ulanishda taqiqlash.

Fil’trlash qoidalarini ifodalash qiyin jarayon bo‘lib, ularni testlash vositalari mavjud emas.

Birinchi qoida bo’yicha, Internetdan keladigan TCP paketi jo’natuvchining porti 1023 dan katta bulsa, 123.4.5.6 manzilli kabul qiluvchiga 23-portga o’tkaziladi (23-port TELNET serveri bilan boglangan).

Ikkinchi koida ham xuddi shunday bo‘lib, faqatgina 25-port SMTP bilan bog’langan.

Tarmoq darajasidagi shlyuzlar ishonchli mijozlardan aniq xizmatlarga so’rovnomasini qabul qiladi va ushbu aloqaning qonuniyligini tekshirgandan so’ng ularni tashki xost-kompyuter bilan ulaydi. SHundan sung shlyuz ikkala tomonga ham paketlarni fil’trlamay junatadi.

Bundan tashqari, tarmoq darajasida shlyuzlar bevosiga **server-dallol** vazifasini bajaradi, ya’ni, ichki tarmoqdan keladigan IP manzillar o’zgartirilib, tashqariga faqatgina bitta IP manzil uzatiladi. Natijada, ichki tarmoqdan tashqi tarmoq bilan to’g’ridan-to’g’ri bog’lamaydi va shu yul bilan ichki tarmoqni himoyalash vazifasini utaydi.

Amaliy darajadagi shlyuzlar fil’trlovchi-yo’llovchilarga mansub bo‘lgan kamchiliklarni bartaraf etish maqsadida ishlab chiqilgan. Ushbu dasturiy vosita **vakolatlangan server,** deb nomlanadi va u bajarilayotgan xost-kompyuter esa amaliy darajadagi shlyuz deb ataladi.

Amaliy darajadagi shlyuzlar mijoz va tashqi xost-kompyuter bilan to’g’ridan-to’g’ri aloqa o’rnatishga yo’l qo’ymaydi. Shlyuz keladigan va

junatiladigan paketlarni amaliy darajada fil’trlaydi. Server-dallollap shlyuz orqali aniq server tomonidan ishlab chiqilgan ma’lumotlarni qaytadan yo’naltiradi.

Amaliy darajadagi shlyuzlar nafaqat paketlarni fil’trlash, balki serverning barcha ishlarini qayd qilish va tarmoq adminstratorini noxush ishlardan xabar qilish imkoniyatiga ham ega.

Amaliy darajadagi shlyuzlarning afzalliklari quyidagilardan iborat:

• global tarmoq tomonidan ichki tarmoq tarkibi ko’rinmaydi;

• ishonchli autentifikatsiya va qayd qilish;

• fil’trlash koidalarining engilligi;

• ko‘p tamoyilli nazoratlarni amalga oshirish mumkinligi.

Fil’trlovchi-yo’llovchilarga nisbatan amaliy darajadagi shlyuzlarning kamchiliklari quyidagilardan iborat samaradorligining pastligi; narxining qimmat bo‘lishi.

Amaliy darajadagi shlyuzlar sifatida quyidagilarni misol qilib keltirish mumkin:

• Border Ware Fire Wall Server — jo’natuvchining va qabul qiluvchining manzillarini, vaqtini va foydalanilgan protokollarni qayd qiladi;

• Black Hole — serverning barcha ishlarini qayd qiladi va tarmoq administratoriga kutilayotgan buzilish haqida xabar jo’natadi.

Bulardan tashqari quyidagi shlyuzlar ham qo’llaniladi:

Gauntlet Internel FirewaU, Alta Visla FireWali, ANS Interlock va boshqalar.

Zero, axborot xavfsizligi sohasida davlat siyosatini amalga oshirishga imkon beruvchi sharoitlarni yaratish, mamlakatni iqtisodiy va ilmiy-texnik taraqqiyotiga ko‘maklashish, axborotni muhofaza qilishning usul va vositalarini yaratish dolzarb masalalardan biridir. Amaliyot shuni ko‘rsatadiki, axborotni muhofaza qilishda yetarli darajadagi yutuqlarga erishish uchun huquqiy, tashkiliy va texnik choralarni birgalikda amalga oshirish zarur. Bu himoyalanadigan axborotning konfedensialligi, tahdidning tasnifi va himoya

vositalarining mavjudligi bilan belgilanadi. Umumiy holda xavfsizlikni ta’minlashning kompleks choralariga:

– ruxsatsiz foydalanishdan kompleks himoya qilish vositalari;
– apparat-dasturiy vositalar;
– kriptografik muhofaza qilishning kompleks vositalari;
– injener-texnik tadbirlar;
– texnik kanallarni blokirovkalash kompleks vositalari;
– obyektlarni jismoniy qo‘riqlashni kiritish mumkin.

Bu choralarning har biri boshqasini to‘ldiradi, bironta usulning yo‘qligi yoki yetishmasligi yetarli darajadagi himoyaning buzilishiga sabab bo‘lishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI.

1. R.X. Alimov, B.YU. Xodiev, K.A. Alimov, S.U. Usmonov, B.A. Begalov, N.R. Zaynalov, A.A. Musaliev, F. Fayzieva, «Milliy iqtisodda axborot tizimlari va texnologiyalari», O'quv qo'llanma, T. Sharq, 2004 yil.
2. M.T. Gafurova, D.CH. Dursunov, V.I. Rapoport, B.YU. Xodiev. Proektirovanie sovremennых informatsionnых texnologiy. Uchebnoe posobie.-Toshkent, TDIU, 1994.-96 s.
3. G'ulomov S.S. va boshq. Iqtisodiy informatika: Oliy o'quv yurtlarining iqtisodiy mutaxassisliklari uchun darslik.
4. G'ulomov S.S., SHermuhammedov A.T., Begalov B.A.; S.S. G'ulomovning umumiy tahriri ostida. —T.: «O'zbekiston», 1999. —528 b.
5. www.intuit.ru
6. www.it-study.ru
7. www.informatika.ru
8. www.ziyonet.uz

Mundarija.