Kompyuter tarmoqlarida axborotlarni himoyalash

Butun jahon axborot makoninig yaratilishi, shaxsiy kompyuterlarning ommaviy ishlatilishi hamda kompyuter tizimlarining rivojlanishi axborotlarni himoyalashning kompleks muammolarini keltirib chiqaradi. Bu tizimlarda ishonchli himoyani tashkil etish katta moddiy va moliyaviy xarajatlarni, murakkab tadqiqotlarni talab etadi. Shuningdek, axborotlarning qimmatligiga qarab, himoya xarajatlarining optimal, maqsadga muvofiq darajasini ishlab chiqish zaruriyati tug`iladi. Yuqori darajada axborotlar xavfsizligini ta'minlovchi xarajatlarni hisoblash – mumkin bo`lgan tajovuzlarni to`liq o`rganish, ular har birining xavflilik darajasini aniqlashni taqozo etadi.

«Detektorlashtirilgan obyektlar». Zarar ketiruvchi dasturlarni kim va nima uchun yaratadi?

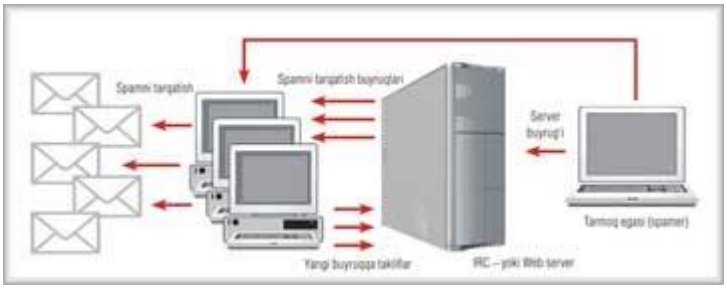
Avvalo - eng asosiy savolga javob beraylik. Bu kimga kerak? Nima uchun kompyuterlar, tarmoqlar, mobil telefonlari faqat foydali axborotlarnigina emas, balki turli xil zararli dasturlarni ham tarqatuvchi maskanga aylanib qoldi? Bu savolga javob berish qiyin emas. Barcha (yoki deyarli barcha) kashfiyotlar, ommaviy foydalanish texnologiyalari — ertami-kechmi bezorilar, qalloblar, firibgarlar va boshqa jinoyatchilar vositalariga aylangan.

Biror narsadan bezorilik yoki jinoyatchilik maqsadida foydalanish imkoniyati paydo bo'lishi bilanoq — albatta, mazkur yangi texnologiyalardan kashfiyotchi mo'ljallagan maqsadlarda emas, balki aksincha g'arazli niyatlarda yoki atrofdagilarga o'z shaxsiyatini namoyon etish uchun foydalanadiganlar paydo bo'ladi. Afsuski, bu qismatdan — kompyuterlar, tarmoqlar, mobil telefonlari, kompyuter va mobil telefonlari tarmoqlari ham chetda qolmadi. Bu texnologiyalardan ommaviy foydalanila boshlanishi bilanoq — ular yomon niyatlilar qo'liga tushdi. Biroq yangilikning «jinoiylashishi» asta-sekin sodir bo'ldi: Kompyuter bezoriligi - Mayda o'g'rilik - Jinoiy biznes - Yarim maxfiy biznes ko'rinishida paydo bo'ldi.

Kompyuter bezoriligi. Virus va troyan dasturlarining asosiy qismi ilgari endigina dasturlashtirish tilini o'rganib olgan hamda bu sohada o'z kuchlarini sinab ko'rmoqchi bo'lgan, biroq foydalanishda bundan yaxshiroq yo'lini topolmagan talaba va o'quvchilar tomonidan yaratilgan. Bunday viruslar faqatgina ularning mualliflari o'zlarini namoyon etishlari uchun yaratilgan va yaratilmoqda. Shunisi quvonarliki, mazkur viruslarning ko'pgina qismi mualliflari tomonidan tarqatilmagan, viruslar esa biroz vaqtdan so'ng o'z-o'zidan saqlanayotgan disklari bilan nobud bo'lgan yoki ularning mualliflari ularni hech qachon boshqa joylarga tarqatmaslik haqidagi xabarlari bilan antivirus (virusga qarshi kurashuvchi) kompaniyalariga jo'natganlar.

Virus yaratuvchilarning ikkkinchi guruhini dasturlashtirish san'atini to'liq o'zlashtirib ulgurmagan yoshlar (ko'pincha talabalar) tashkil etadi. Virus yaratishlariga undovchi yagona sabab, bu o'z xususiyatlaridan ko'ngli to'lmaganlik holati bo'lib, uni kompyuter bezoriligi bilan to'ldirishga intilishdir. Bunday «ustasi faranglar» qalamiga juda sodda va katta xatolarga yo'l qo'yib yaratilgan viruslar («talabalar» viruslari) mansubdir.

Internet rivojlanishi va kompyuter viruslarini yaratishga-o'rgatishga yo'naltirilgan ko'plab veb-saytlarning paydo bo'lishi bilan shunday virus yaratuvchilarining hayoti ancha yengillashdi. Mana shunday veb-resurslarda tizimga kirish metodlari, antivirus dasturlarini ochish uslublari, virusni tarqatish bo'yicha batafsil tavsiyalarni topish mumkin. Ko'pincha bu yerda faqatgina biroz «mualliflik» o'zgartirishlarini kiritish va tavsiya etiladigan usul bilan kompilyatsiya (qurama asar yozish) kerak bo'ladigan tayyor dastlabki matnlarni topish mumkin.



Yosh jihatdan ulg‘ayib va tajriba orttirgan mazkur, virus yaratuvchilarining ko‘pchiligi, «professional» viruslar yaratib, ularni jahonga tarqatuvchi eng xavfli uchinchi guruhga kiradilar. Mana shu puxta o‘ylangan va yo‘lga qo‘yilgan dasturlarni malakali, juda ko‘p hollarda iste’dodli dasturchilar yaratadilar. Bunday viruslarda ma’lumotlarning tizimli muhitiga buzib kirishning yetarli darajada original algoritmlari, operatsion muhitlar xavfsizlik tizimlaridagi xatolar, ijtimoiy injiniring va boshqa ayyorliklardan foydalanadi.
Virus mualliflari to‘rtinchi guruhi alohida o‘rinda turadi — bu «tadqiqotchilar» ancha idrokli dasturchilardir, ular zararlantirish, ochish, antiviruslarga qarshilik ko‘rsatish va shu kabi umuman yangi metodlarni ixtiro qilish bilan shug‘ullanadilar. Ular yangi operatsion tizimlarga kiritish usullarini o‘ylab topadilar. Bu dasturchilar viruslarni shunchaki viruslar uchun emas, balki «kompyuter olami» imkoniyatlarini o‘rganish maqsadida «konseptual» («Proof of Concept» — PoC) deb ataluvchi viruslarni yaratadilar. Ko‘pincha bunday virus yaratuvchilar o‘z ijodlarini tarqatmaydilar, biroq viruslar yaratishga bag‘ishlangan ko‘p sonli internet-resurslar orqali o‘zlarining g‘oyalarini targ‘ib etadilar. Shu bilan birga, mana shunday «tadqiqotchilik» viruslaridan ham katta xavflar kelib chiqadi — avvalgi guruh «professionallari» qo‘liga tushgan bu g‘oyalar tezlikda yangi viruslarda paydo bo‘ladi.
Yuqorida ko‘rsatib o‘tilgan viruslarning yaratuvchi guruhlari tomonidan yaratiladigan «an’anaviy» viruslar hozirgi kunda ham paydo bo‘lishda davom etmoqda — ulg‘aygan tineyjer-bezorilar o‘rniga har gal tineyjerlar yangi avlodi kelib qo‘shiladi. So‘nggi yillarda «bezorilik» viruslari borgan sari o‘z ahamiyatini yo‘qotib borishi holati kuzatilmoqda, faqat global tarmoq va pochta epidemiyalarini keltirib chiqaruvchi zarar keltiruvchi dasturlar bundan mustasno. Yangi «an’anaviy» viruslar soni sezilarli darajada kamayib bormoqda — 2005-2006 yillarda ular 1990-yillar o‘rtalari va oxiriga qaraganda, bir necha bor kamaydi. Maktab o‘quvchilari va talabalarning viruslar yaratishga qiziqishlari yo‘qolishiga sabab quyidagicha bo‘lishi mumkin:

- 1990-yillarda MS-DOS operatsion tizimi uchun virusli dasturlarni yaratish texnik jihatdan ancha murakkab, Windows dasturi uchun yaratishga qaraganda, bir necha bor oson bo‘lgan.
- Ko‘plab mamlakatlar amaldagi qonun hujjatlarida maxsus kompyuter jinoyatchiligiga oid moddalar paydo bo‘ldi, virus yaratuvchilarining jazoga tortish holatlari keng yoritildi — bu holat, albatta ko‘plab talaba va o‘quvchilarning viruslarga qiziqishlarini susaytirdi.
- Bundan tashqari, ularda o‘zlarini namoyon etish uchun tarmoq o‘yinlari kabi yangi imkoniyatlar paydo bo‘ldi. Aftidan aynan zamonaviy o‘yinlar qiziqishlar yo‘nalishini o‘zgartirdi va kompyuterlarga qiziquvchi yoshlarni o‘ziga jalb etdi.

Shunday qilib, hozirgi kunda «an’anaviy» bezorilik viruslari va troyan dasturlarining ulushi antivirus ma’lumotlar bazasiga kiritiladigan «materiallarning» 5 foizini tashkil etadi. Qolgan 95 foizi shunchaki viruslardan ko‘ra ancha xavfli bo‘lib, ular quyida ko‘rsatilgan maqsadlarda yaratiladi.
Mayda o‘g‘rilik. Pullik internet-servislar (pochta, veb, xosting) paydo bo‘lishi va ommaviylashib borishi bilan (o‘yinchi) kompyuter andegraundi boshqalar hisobiga tarmoqdan foydalanishga, ya’ni maxsus ishlab chiqilgan troyan dasturlari yordamida kimningdir logini hamda parolini (yoki turli zararlangan kompyuterlardan bir necha login va parollarni) o‘g‘irlashga katta qiziqish ko‘rsatila boshlandi.
1997-yil boshida AOL (internet-provayder America Online) tizimidan foydalana olish

parollarini o‘g‘irlovchi troyan dasturlarini yaratish va tarqatishning birinchi holatlari qayd etildi. 1998-yili, internet-xizmatlarining yanada keng tarqalishi bilan, boshqa internet-servislari uchun ham shunday Troyan dasturlari paydo bo‘ldi. Shu turdagi Troyan dasturlari, viruslar kabi odatda internet-xizmatlari uchun haq to‘lash imkoniyati bo‘lmagan yoshlar tomonidan yaratiladi. Internet-servislar arzonlashib borishi bilan shunday troyan dasturlarining soni ham kamayib borish dalili o‘ziga xos xislatdir. Ammo dial-up, AOL tizimlariga parollarni, ICQ, boshqa servislardan foydalanish kodlarini o‘g‘irlovchi troyanlar butun jahon antivirus kompaniyalari laboratoriyalariga «kelib tushuvchilar»ning katta qismini tashkil etmoqda.
«Mayda o‘g‘rilar» tomonidan boshqa turdagi Troyan dasturlari ham yaratiladi. Ular: o‘z «egasi» manfaatlari yo‘lida zararlangan kompyuterlar resurslaridan foydalanuvchi turli dasturiy mahsulotlarni qayd etish ma’lumotlarini va asosiy fayllarni o‘g‘irlovchi dasturlardir.
So‘nggi yillarda noqonuniy foydalanish yoki sotish maqsadida tarmoq o‘yinlaridan shaxsiy axborotlarni (o‘yinlar kabi virtual mulkni) o‘g‘irlovchi troyan dasturlari soni doimiy o‘sib borishi kuzatilmoqda. Shunday troyanlar Osiyo davlatlarida, ayniqsa, Xitoy, Koreya va Yaponiyada keng tarqalgan.
Demak, aytish joizki, shaxsiy kompyuterlardan foydalanishning boshlang`ich yillarida ko`proq xakerlar, «elektron bosqinchilar» xavf solishgan bo`lsa, keyingi yillarda axborotlar mustahkamligiga programma vositalari – kompyuter viruslari, Internet tarmog`i sabab bo`lmoqda. Natijada axborotlar butunligi buzilmoqda. Bu jarayon ikki xil holatda amalga oshirilishi mumkin:

- tasodifan;
- g`arazli maqsadda (qasddan).

Birinchi holatda axborotlarning buzilishiga kishilar tomonidan tasodifan yo`l qo`yilgan xatolar, texnik nosozliklar sabab bo`lishi mumkin.
Ikkinchisiga esa kishilar tomonidan g`arazli maqsadlarni ko`zlab olib borilgan harakatlar turtki bo`ladi.
Axborot butunligi buzilishining sabablari qanday bo`lishidan qat'iy nazar, u ko`zda tutilmagan har qanday natijalarni keltirib chiqarishi mumkin. Amaliyot shuni ko`rsatadiki, axborotlar ularni kiritish, saqlash, qayta ishlash, chop etish hamda uzatish jarayonida turli xil tasodifiy tashqi ta'sirlarga uchraydi. Oqibatda axborotlarda signal shaklida jismoniy o`zgarishlar kuzatiladi. Masalan, raqamli kodning biror - bir razryadida ikkilik belgisining invertatsiyasi vujudga kelsa hamda bu xato funktsional nazorat vositalari tomonidan aniqlanmasa, yolg`on ma'lumot olinadi yoki ma'lumot noto`g`ri manzil bo`yicha jo`natiladi va boshqa noxush holatlar vujudga kelishi mumkin.
Kompyuter tizimlari faoliyatiga tasodifiy ta'sirlar tufayli quyidagi buzilishlar bo`lishi mumkin:

- apparatlarning sifatsizligi, eskirishi natijasida buzilishi;
- tashqi muhit ta'sirida aloqa kanallari va tarmoqlarida axborotlarning o`zgarishi;
- avariya holatlari (yong`in, suv toshqini, zilzila va hokazo)
- kompyuter ishlab chiqaruvchilar hamda loyixalashtiruvchilarning sxema va sistemotexnik xatolari;
- algoritmik va dasturiy xatolar;
- kishilarning kompyuterlarda ishlayotganda yo`l qo`yadigan nuqsonlari.

Ikkinchi, ya'ni g`arazli maqsadlardagi buzilishlarni «axborot quroli» deb atashimiz mumkin.
Axborot quroli radioelektron klassli qurol, dushmanning axborot imkoniyatlarini yo`q qilish uchun yaratilgan dasturli- axborot vositalar kompleksidan iborat. Bu tushunchaga aniqlik kiritamiz. Jahonda qadimiy tarixga ega bo`lgan «dezinformatsiya» nomi bilan

hammaga ma'lum bo`lgan «oddiy» tashviqot – psixologik axborot quroli ham mavjud. Harbiy tarixiy adabiyotlarda urush davrida ham, tinchlik davrida ham muvaffaqiyatli amalga oshirilgan dezinformatsiyalarning ko`plab misollari ko`rsatilgan. «DEZA» hozir ham maxsus xizmat quroli sifatida saqlanib kelinmoqda.
«Oddiy» axborot quroliga 60-70 yillar davrida «sun'iy intellekt» kirib keladi, axborot tizimlarini, kompyuter va mikrokompyuterni jihozlash sodir bo`ladi. Natijada axborot quroli faqatgina uni qo`llash doirasini cheksiz kengaytirishga imkon beruvchi emas, balki G`arbda aytishlaricha, u ommaviy hujum vositalarining ham o`rnini bosa oladigan xususiyatga ega bo`ladi.
Endi rossiyalik ekspertlar bergan «axborot quroli»ning aniq tushunchasini keltiramiz. Axborot quroli «axborot massivlarini yo`q qilish, buzish yoki o`g`irlash vositasi, himoya tizimini buzib kirgandan keyin ulardan kerakli ma'lumotlarni bilib olishdir. Ularga qonuniy foydalanuvchilarning kirishini taqiqlash yoki cheklash, texnik vositalarining ishlarini buzish, telekommunikatsion tarmoqlarni ishdan chiqarish, kompyuter tizimlarini, jamiyat hayotini yuqori texnologik ta'minlashni va davlat faoliyatining barcha bo`g`inlarini yo`ldan chiqarishdir».
Axborotlashtirish yagona jahon axborot muhitini yaratishga olib keladi, uning doirasida ma'lumotlardan foydalanish, yaratish, o`zgartirish, saqlash va eng asosiysi, bu muhit sub'ektlari, ya'ni odamlar, tashkilotlar, davlatlar o`rtasida ma'lumotlar almashish amalga oshiriladi.
Hujum qiluvchi axborot quroli deb quyidagilarni hisoblash mumkin:

- kompyuter viruslari;
- mantiqiy bombalar (dasturli to`siqlar);
- telekommunikatsion tarmoqlarda axborot almashish vositalarini yo`q qilish, davlat boshqaruv kanallarida axborotlarni qalbakilashtirish;
- test dasturlarini buzish, ishdan chiqarish;
- ob'ektni dasturli ta'minlashga atayin kiritiladigan turli xil xatolar.

Hujum qiluvchi axborot quroli «Kompyuter viruslari» (KV) boshqalarning «Elektron muhitiga» tadbiq etiladigan (kiritiladigan) dastur. KV aloqa tarmoqlari orqali yuboriladi, elektron telefon stantsiyalari va boshqaruv tizimlariga kirib boradi. Ko`rsatilgan, belgilangan vaqtda yoki KV signallari bo`yicha EHM xotirasida saqlanadigan axborotlarni o`chirib yuboradi yoki o`zgartiradi, shu bilan birga o`zgartirish ixtiyoriy yoki aniq maqsadli bo`lishi mumkin. Masalan, bank kompyuteriga kiritilgan KV o`z muallifi foydasiga mablag` hisobini o`zgartirishi yoki bir hisobdan ikkinchi hisobga pul o`tkazishi mumkin. Bunday virus kompyuterning butun xotirasini boshqa ma'lumotlar bilan to`ldirishi va oxir-oqibat uni buzib qo`yishi mumkin. Hujum qiluvchi axborot qurolining yana bir turi bu «Mantiqiy bomba» bo`lib, u fuqarolik infrastrukturalarining ob'ektlarini boshqarishni ta'minlaydigan axborot tizimlar va tarmoqlarga oldindan kiritib qo`yiladigan dasturli qo`shimchalardir (dasturli to`siqlardir). Bomba signal bo`yicha yoki belgilangan vaqtda ishga tushiriladi, zararlangan kompyuterdagi ma'lumotlarni o`chiradi yoki buzadi, oqibatda uni ishdan chiqaradi. «Troyan oti» mantiqiy bombaning bir turi. Bu yashirin ma'lumotlar olish uchun kompyuter foydalanuvchisining axborot muhitiga yashirin, ruxsatsiz kirishni amalga oshirishga imkon beruvchi dasturdir.
Ob'ektlarga Internet tarmog`i orqali o`zboshimchalik bilan ulanish xavfi haqida G`arb matbuotlarida keltirilayotgan ko`plab misollar dalil bo`la oladi. Misol uchun, 1994 yili 16 yoshlik Londonlik maktab o`quvchisi Internet orqali AQShning havo hujumidan himoyalanish tizimlari kompyuter tarmog`iga kirgan, so`ngra «qonun buzar» xuddi shunday Nyu-York yaqinida joylashgan Amerika yadro tadqiqot markazi tarmog`iga ham ulangan. «Axborot qaroqchisini» aniqlash operatsiyasi Amerika va ingliz maxsus xizmatlari uchun 400 ming dollarga tushgan.
Jinoiy (kriminal) biznes. G`arazli maqsadlarda atayin zararli dasturlar yaratuvchi yakka-xaker yoki xakerlar guruhlari virus yaratuvchilarining eng xavfli toyifasi

hisoblanadi. Buning uchun ular bank hisoblariga kirish kodlarini o‘g‘irlovchi virusli va Troyan dasturlarini yaratadilar. Qandaydir mahsulot yoki xizmatlarni yolg‘on reklama qiladilar, zararlangan kompyuter resurslaridan noqonuniy (yana pul uchun —spam-biznesni yo‘lga qo‘yish yoki tovlamachilik qilish maqsadida taqsimlangan tarmoq hujumini tashkil qilish uchun) foydalanadilar. Shu toifa fuqarolar faoliyatlari miqyosi juda keng. Tarmoqda jinoiy biznesning asosiy turlari haqida to‘xtalib o‘taylik.

Spam-biznesga xizmat ko‘rsatish. Spamlarni tarqatish uchun troyan proksi-serverlaridan (proxy server — tarmoqda maxfiy ishlash uchun utilita, odatda ajratilgan kompyuterga o‘rnatiladi) yoki proksi-server funksiyasi bilan ko‘p maqsadli troyan dasturlaridan ixtisoslashtirilgan «zombi-tarmoqlar» yaratiladi. Shundan so‘ng troyan proksi-serverlar «egasidan» spam namunasi va ushbu spamlar tarqatiladigan adreslarni oladi. Spamni minglab (yoki o‘n minglab) zararlangan kompyuterlar orqali tarqatilishi natijasida spamchilar bir necha maqsadlarga erishadilar: Birinchidan tarqatish anonim amalga oshiriladi — xat sarlavhalari va xatdagi boshqa xizmat axborotlaridan spamerning haqiqiy manzilini aniqlash mumkin emas; Ikkinchidan, spam-tarqatishning katta tezligiga erishiladi, chunki bu ishda ko‘p sonli «zombi»-kompyuterlardan foydalaniladi; Uchinchidan, zararlangan mashinalar manzillari «qora ro‘yxatini» yuritish texnologiyasi ishlamaydi — spam tarqatuvchi barcha kompyuterlarni «uzib qo‘yish» mumkin emas, chunki ular juda ko‘p.

Taqsimlangan tarmoq hujumlari. Bundan tashqari, DDoS-hujumlar (Distributed Denial of Service - xizmat ko‘rsatishda taqsimlangan rad etish) deb ham ataladi. Tarmoq resurslari (misol uchun, veb-serverlar) murojaatlarga bir vaqtda xizmat ko‘rsatish soni bo‘yicha cheklangan imkoniyatlarga ega — ushbu sonlar server o‘zining quvvati kabi, u internetga ulangan kanal kengligi bilan ham cheklanadi. Agar murojaatlar soni mumkin bo‘lganidan ortiq bo‘lsa, unda server bilan ishlash ancha qiyinlashadi yoki foydalanuvchilarning murojaatlari umuman javobsiz qoladi.

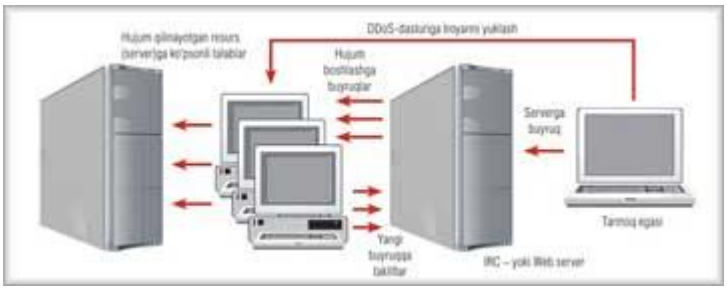
Shu dalildan foydalanib, g‘araz niyatli kompyuter foydalanuvchilari hujum qilinayotgan resursga «keraksiz» talablarni ustun qo‘yadi, bunday murojaatlarning soni zararlanuvchi-jabrlanuvchi resurs imkoniyatidan bir necha bor ortiq bo‘ladi. Yetarlicha kattalikdagi «zombi-tarmoq» yordamida tarmoqning hujum qilinagan usullari rad javobiga sabab bo‘luvchi bir yoki bir necha internet-resurslarga keng DDoS-hujumi tashkil etiladi, natijada oddiy foydalanuvchilar hujum qilingan resurslardan foydalana olmaydilar. Odatda, internet-do‘konlar, internet-kazino(qimorxona), bukmekerlik idoralari, bizneslari to‘g‘ridan-to‘g‘ri o‘z internet-servislariga ishlash qobiliyatlariga bog‘liq bo‘lgan boshqa kompaniyalarga hujum qilinadi. Ko‘pchilik hollarda taqsimlangan hujumlar yoki raqobatchisi biznesini «sindirish» yoki hujum qilishni to‘xtatish uchun mukofot sifatida mablag‘ talab etish maqsadida — qandaydir internet-reket maqsadlarida amalga oshiriladi.

2002-2004 yillarda jinoiy faoliyat ushbu turi juda keng tarqalgan edi. Shundan keyin ushbu faoliyat turi kamaydi, aftidan bunga jinoyatchilarni muvaffaqiyatli aniqlash (ushbu jinoyat turi bo‘yicha jahonda kamida bir necha o‘nlab fuqarolar jazoda tortilgan) hamda shunga o‘xshash hujumlarga qarshi muvaffaqiyatli texnik choralar bunga sabab bo‘ldi.

«Zombi-mashinalar» tarmoqlarini yaratish. Bunday tarmoqlarni hosil qilish uchun uzoq masofadagi «egasi» tomonidan markazlashtirilgan boshqariladigan maxsus troyan dasturlari - «botlar» («robot» so‘zidan) yordamida yaratiladi. Ushbu Troyan minglab, o‘n minglab yoki hatto millionlab kompyuterlarga tatbiq etiladi. Natijada «zombi-tarmoq egasi» (yoki «bot-tarmoq») barcha zararlangan kompyuterlar resurslaridan foydalanish imkoniga ega bo‘ladi va ulardan o‘z manfaatlari yo‘lida foydalanadi. Bazan shunday «zombi-mashinalar» yashirin noqonuniy internet-bozorlarda paydo bo‘ladi, ularni spamerlar sotib oladilar yoki ularga ijaraga beriladi.

Pullik telefon raqamlariga qo‘ng‘iroqlar yoki pullik SMS-xabarlarni yuborish. Dastavval jinoyatchi (yoki bir necha) mobil telefonlardan foydalanuvchi

tomonidan noqonuniy telefon qo‘ng‘iroqlari yoki SMS-xabarlar tarqatishni amalga oshiruvchi maxsus dastur yaratiladi va tarqatiladi. Bunday ishlardan oldin yoki bir vaqtda ushbu shaxslar kompaniyani ro‘yxatdan o‘tkazib, uning nomidan mahalliy telefon provayderi bilan pullik telefon xizmati ko‘rsatishga shartnoma tuziladi. Provayder esa tabiiyki, qo‘ng‘iroqlar foydalanuvchi ruxsatisiz amalga oshirilishi haqida xabardor qilinmaydi. Shundan so‘ng troyanchi pullik telefon raqamiga qo‘ng‘iroq qiladi, telefon kompaniyasi ushbu raqamlarga haq hisoblaydi va jinoyatchiga shartnomada ko‘rsatilgan mablag‘ni o‘tkazadi.



Internet-pullarni o‘g‘irlash. Xususan — Shaxsiy «elektron hamyonlardan» (e-gold, WebMoney kabi) pul mablag‘larini o‘g‘irlashga qaratilgan troyan josus-dasturlarini yaratish, tarqatish va xizmat ko‘rsatish. Ushbu turdagi troyan dasturlari hisoblardan foydalanish kodlari haqidagi axborotlarni to‘playdi va ularni o‘z «egasiga» jo‘natadi. Odatda axborotlarni to‘plash hisob egasi shaxsiy ma’lumotlari saqlanadigan fayllarni izlash va ochish bilan amalga oshiriladi.
Bank axborotlarini o‘g‘irlash. Bank axborotlarini o‘g‘irlash — hozirgi kunda, internetda eng keng tarqalgan jinoiy faoliyat turlaridan biridir. Bank kredit kartalari raqamlari va internet orqali xizmat ko‘rsatiladigan shaxsiy («omad kelsa» kelib qolsa — unda korporativ ham) bank hisob-varaqlaridan («internet-benking») foydalanish kodlari xavf ostida qoladi. Bunday hujumlarni amalga oshirishda troyanchi-josuslar turli metodlardan foydalanadilar. Masalan, dialog oynasini chiqaradilar yoki bank veb-sahifasi bilan mos keladigan tasvirli oynani ko‘rsatadilar — shundan so‘ng foydalanuvchidan hisobiga yoki kredit kartasidan foydalanish login va parolni so‘raydilar (shu kabi metodlar fishingda — bankdan yoki boshqa internet-servisdan axborot xabariga o‘xshash qalbaki matn bilan spamlarni tarqatishda qo‘llaniladi).
Foydalanuvchini shaxsiy ma’lumotlarini kiritishga majbur qilish uchun turli psixologik nayranglarni qo‘llaydilar, odatda — agar o‘z kodingizni kiritmasangiz, biror-bir yomon holat (misol uchun, internet-bank hisob bo‘yicha xizmat ko‘rsatishni to‘xtatishi) yoki qandaydir juda yaxshi imkoniyat taqdim etilishi («Sizning hisobingizga katta miqdorda pul o‘tkazishmoqchiligi — iltimos, o‘z rekvizitlaringizni tasdiqlang») haqida xabar yoki matn yuboriladi.
Foydalanuvchi bankning haqiqiy veb-sahifasiga ulanishini kutib turib, shundan so‘ng klaviaturadan kiritilgan belgilarni (ya’ni, login va parolni) qo‘lga tushirib oluvchi troyan dasturlari («klaviatura josuslari») juda ko‘p uchraydi. Buning uchun ular ilovalarning ishga tushirilishi va faolligini kuzatib boradilar. Agar foydalanuvchi internet-brauzerda ishlayotgan bo‘lsa, veb-sayt nomini troyan kodiga «biriktirilgan» banklar ro‘yxati bilan solishtiradilar. Agar veb-sayt ro‘yxatdan topilsa, unda klaviatura josusi ishga kirishadi, shundan so‘ng qo‘lga olingan axborot (bosilgan tugmalar ketma-ketligi) jinoyatchiga jo‘natiladi. Ushbu Troyan dasturlari (boshqa bank troyanlaridan farqli ravishda) tizimda mavjudligini umuman namoyon etmaydi.
Boshqa konfidensial axborotlarni o‘g‘irlash. Jinoyatchilarni nafaqat moliyaviy yoki bank axborotlari, balki biror-bir qimmatga ega bo‘lgan — ma’lumotlar bazasi, texnik hujjatlar va shunga o‘xshash boshqa ma’lumotlar ham qiziqtirishi mumkin. Shunday axborotlardan foydalanish va o‘g‘irlash uchun kompyuterlarga maxsus ishlab chiqilgan troyan-josuslari kiritiladi.

Hujum uyushtirish uchun qonuniy tarmoq ilovalaridan foydalanilgan holatlar ham kuzatilgan. Misol uchun, tizimga yashirin ravishda FTP-server kiritiladi yoki shunday yashirin fayllar almashish («Peer-to-Peer» — P2P) dasturiy ta'minoti o'rnatiladi. Natijada kompyuterning fayllar resurslari tashqaridan foydalanish uchun ochiq bo'lib qoladi. P2P-tarmoqlaridan jinoiy maqsadlarda foydalanish bilan bog'liq ko'plab sonli holatlar sababli 2006-yilda ular Fransiya va Yaponiyada rasman taqiqlab qo'yilgan.
Kiber-tovlamachilik. Jinoyatchilar tomonidan foydalanuvchining shaxsiy fayllarini shifrlovchi troyan dasturi ishlab chiqiladi. Troyan biror-bir usul bilan tizimga kiritiladi, foydalanuvchining ma'lumotlarini izlaydi va shifrlaydi, ishni yakunlagandan keyin esa fayllarni tiklash mumkin emasligi, rasshifrovkachi-dasturni xabarda ko'rsatilgan manzilda sotib olish mumkinligi haqida xabar qiladi.
Kiber-tovlamachilikning yana bir mashhur metodi — foydalanuvchining fayllarini juda uzun parol bilan shifrlangan arxivga arxivlashtirish hisoblanadi. Arxivlashtirilgandan so'ng haqiqiy fayllar o'chiriladi va shundan keyin arxivga parol uchun ma'lum miqdorda pul mablag'i o'tkazilishi talab etiladi.
Kiber-jinoyatning ushbu usuli (ma'lumotlarni shifrlash) texnik nuqtai nazardan juda xavfli hisoblanadi, chunki boshqa holatlarda troyan dasturi ta'siri oqibatlaridan himoyalanish mumkin bo'lsa, bu erda shifrlash mustahkam algoritmlariga duch kelamiz. Mana shunday algoritmlar va yetarlicha uzunlikdagi kalitlardan (parollar) foydalanilganda fayllarni jinoyatchidan tegishli axborotni olmasdan-qayta tiklash texnik jihatdan bajarib bo'lmaydigan amal bo'lib qoladi.
«Yetkazish vositalarini» ishlab chiqish. Kiber-jinoyatchilarning internetdagi yuqorida ko'rsatilgan jinoiy faoliyatlari turlarini amalga oshirish uchun ko'plab internet-epidemiyalar sababchisi bo'lib qoladigan tarmoq qurt (chervi)lari ishlab chiqiladi va tarqatiladi. Shunday qurtilarning asosiy vazifasi global tarmoqda iloji boricha, ko'p sonli kompyuterlarda jinoiy troyan dasturlarini o'rnatish hisoblanadi. Katta shov-shuvlarga sabab bo'lgan 2004-yildagi Mydoom va Bagle, 2006-yilda esa - Warezov pochta qurtlari mana shunday zararkunanda (chervi)larga misol bo'la oladi.
Ba'zi hollarda «maksimal qoplab olish» vazifasi qo'yilmaydi - aksincha, zararlangan mashinalar soni majburiy ravishda cheklanadi, aftidan, huquqni himoya qilish organlari e'tiborlarini ortiqcha jalb qilmaslik uchun bo'lsa kerak. Bunday hollarda kompyuter-jabrlanuvchilarga kiritish tarmoq qurti nazoratsiz epidemiyasi yordamida emas, balki misol uchun zararlangan veb-sahifa orqali sodir bo'ladi. Jinoyatchilar sahifaga tashrif buyuruvchilar, muvaffaqiyatli zararlantirishlar sonini qayd etishlari va zararlangan mashinalar kerakli soniga erishganda troyan kodini bartaraf qilishlari mumkin.
Mo'ljalli hujumlar. Iloji boricha, ko'proq sonli kompyuterlarni zararlantirishga qaratilgan ommaviy hujumlardan farqli ravishda, mo'ljalli hujumlar umuman boshqa - aniq bir kompaniya yoki tashkilot tarmog'ini zararlashni yoki hatto maxsus ishlab chiqilgan troyan-agentni tarmoq infrastrukturasi yagona qismiga (serverga) kiritish maqsadlarini ko'zlaydi. Juda qimmatli axborotlarga ega kompaniyalarga - banklar, billing kompaniyalariga (misol uchun, telefon kompaniyalari) hujumlar uyushtirilishi mumkin.
Bank serverlari yoki tarmoqlariga hujumlar uyushtirilishi sabablari aniq: bank axborotlaridan foydalanish, pul mablag'larini hisob raqamlariga yoki jinoyatchilar hisob raqamlariga noqonuniy ravishda o'tkazishdan iborat. Billing kompaniyalariga hujumlar uyushtirlganida mijozlar hisoblaridan foydalanish maqsadlari ko'zlanadi. Serverlarda saqlanadigan har qanday qimmatli axborotlar — mijozlar ma'lumot bazalari, moliyaviy va texnik hujjatlar, jinoyatchilarni qiziqtirishi mumkin bo'lgan har qanday axborotlarga aniq mo'ljalli hujumlar uyushtirilishi mumkin.
Ko'pincha juda muhim va qimmatli axborotlarga ega yirik kompaniyalarga hujum uyushtiriladi. Bunday kompaniyalarning tarmoq infratuzilmalari tashqi hujumlardan ancha yaxshi himoyalangan va kompaniyaning ichidan yordamsiz ularga kirish deyarli mumkin emas. Shu sababli ko'pchilik hollarda shu kabi hujumlar tashkilot xodimlari

(insayderlar) tomonidan, yoki bevosita ularning ishtiroklarida amalga oshiriladi.
Boshqa jinoiy faoliyat turlari. Jinoiy kompyuter biznesi boshqa turlari ham mavjud, ular hozircha keng tarqalmagan. Misol uchun, zararlangan mashinalardan aniqlangan elektron pochta manzillarini o‘g‘irlash (to‘plash) va ularni spamerlarga sotish. Bu operatsion tizimlar va ilovalar zaif tomonlarini izlash va boshqa kompyuter jinoyatchilariga sotish. Bunga troyan dasturlarini «buyurtma» bo‘yicha ishlab chiqish hamda sotish va shu kabilar kiradi. Mavjud internet-servislarning rivojlanib borishi va yangilarining paydo bo‘lishi bilan internet-jinoyatlar sodir etishning yangi metodlari ham paydo bo‘lishi ehtimoldan xoli emas.
Yarim qonuniy biznes. Talabalar — virus yaratuvchilari va yaqqol jinoiy biznesdan tashqari internetda qonunni buzish chegarasida faoliyat yurituvchilar — «yarim qonuniy» biznes ham mavjud. Vaqti-vaqti bilan pullik veb-resurslarga tashrif buyurishga taklif etuvchi elektron reklamalarni majburlab kirituvchi tizimlar, utilitlar, boshqa yoqmaydigan dasturiy ta’minotlar — ularning barchasi ham dasturchi-xakerlar tomonidan texnik qo‘llab-quvvatlashni talab etadi. Ushbu qo‘llab-quvvatlash tizimga yashirin kirish mexanizmini amalga oshirish, vaqti-vaqti bilan o‘z komponentlarini yangilab turish, turli xil niqoblash (tizimdan chiqarib tashlashdan o‘zlarini himoya qilish maqsadida) — antivirus dasturlarga qarshilik ko‘rsatish uchun kerak bo‘ladi — ko‘rsatib o‘tilgan vazifalar turli xildagi troyan dasturlari vazifalari bilan deyarli mos tushadi.
Majburiy reklama (Adware). Tizimga maxsus reklama komponentlarini kiritish amalga oshiriladi, ular vaqti-vaqti bilan alohida serverlardan reklama axborotlarini ko‘chirib olib va uni foydalanuvchiga ko‘rsatadi. Ko‘pchilik hollarda (ammo har doim emas) foydalanuvchi uchun sezdirmay, tizimga kirish amalga oshiriladi, reklama oynalari esa faqatgina internet-brauzer ishlagandagina (shu usulda reklama tizimlari go‘yo veb-saytlar reklama bannerlari kabi) paydo bo‘ladi.
AQSh’ning bir necha shtatlari tomonidan reklamalarga qarshi qonunlar qabul qilinganidan so‘ng Adware loyihachilari amalda noqonuniy bo‘lib qoldi (bu kompaniyalarning deyarli barchasi — Amerika kompaniyalaridir). Natijada, ulardan ba’zilari o‘z loyihalarini maksimal ravishda qonuniylashtirdilar: endi Adware installyatori bilan taqdim etiladi, tizim panelida belgisi ko‘rinib turadi va uning deinstallyatori ham mavjud. Ammo aqli joyida va xotirasi mustahkam inson o‘z kompyuteriga ixtiyoriy ravishda reklama tizimini o‘rnatishini tasavvur qilish qiyin va shuning uchun qonuniy Adware’larni biror-bir bepul soft bilan birgalikda taqdim eta boshladilar. Shunday qilib, Adware installyatsiyasi ushbu soft installyatsiyasi bilan birgalikda sodir bo‘ladi: ko‘pchilik foydalanuvchilar ekrandagi matnga e’tibor bermay, «OK» tugmasini bosaveradilar va o‘rnatilayotgan dastur bilan birgalikda reklamalarni ham yozib oladilar. Ko‘pincha ish stolining va tizim panelining yarmi turli suratlar bilan band bo‘lganligi sababli reklama dasturi suratini ular orasida payqash qiyin bo‘ladi. Natijada yarim qonuniy Adware foydalanuvchidan yashirin o‘rnatiladi va tizimda ko‘rinmaydi.
Ba’zi hollarda asosiy soft ishlashiga zarar keltirmasdan, qonuniy reklama tizimini bartaraf qilish mumkin emasligini ham aytib o‘tish zarur. Shunday usulda Adware ishlab chiqaruvchilari deinstallyatsiyadan himoyalanadilar.
Pornografik (axloqsizlik) biznesi, pullik veb-resurslar. Foydalanuvchilarni pullik veb-saytlarga jalb qilish uchun ko‘pincha ma’lum darajada zararlilar qatoriga kirmaydigan turli dasturlardan foydalaniladi, chunki ular o‘zlarining mavjudliklarini yashirmaydilar, pullik resursga esa foydalanuvchi tegishli savolga ijobiy javob qilgani holda kirishi mumkin. Ammo bunday dasturlar ko‘pincha foydalanuvchining ixtiyorisiz, misol uchun, shubhali mazmundagi veb-saytlarga kirganda tizimga o‘rnatiladi. Shundan so‘ng ular tinmay biror-bir pullik resursga tashrif buyurishni qat’iy taklif etadilar.
Soxta josuslikka qarshi (Anti-Spyware) yoki viruslarga qarshi utilitalar. Bu biznesning ancha yangi turi. Foydalanuvchiga kichik bir dastur yashirin kiritiladi, ushbu dastur kompyuterda josus dasturiy ta’minot yoki virus aniqlanganligini xabar qiladi. Haqiqiy vaziyatning qandayligidan qat’iy nazar, hatto kompyuterda OS Windows

dasturidan boshqa narsa bo`lmasa ham baribir, har qanday holatda xabar qilinadi. Shu bilan birga, foydalanuvchiga arzon narxda «dorisini» sotib olish taklif etiladi, ular aslida deyarli hech narsadan davolamaydi.
Hozirgacha ko`pgina adabiyotlarda kompyuter viruslarining insonga ta'siri yo`q deb e'tirof etib kelindi. Internetdan olingan xabarlarga qaraganda, insonlarga psixologik ta'sir ko`rsata oluvchi, ko`z qamashtiradigan viruslar paydo bo`lgan. Xususan,

- «VIRUS № 666» deb ataluvchi virus EHM operatorining «psixologik holatiga» ta'sir ko`rsatib, uni o`limga olib kelishi mumkin. Bu «qotil - virus» ekranda alohida maxsus ranglar kombinatsiyasini chiqaradi, u insonni o`ziga xos gipnoz qilib, ya'ni gipnotik karaxt holatga tushiradi va uni ongsiz qabul qilish holatiga keltirib qo`yadi. Yurak - qon tomir tizimining ishlashini keskin buzadi va bosh miya tomirlarini ishlatmay qo`yadi.
- «Ko`z qamashtiradigan viruslar» (VRCD – virtual reality control device) ishlatgan foydalanuvchilarning orasida vaqtinchalik ko`z ojizligi qayd qilindi. Etakchi ekspertlar fikricha, bu muammoni echishda oxirgi paytda on-layn ekstremist jinoyatchilar orasida keng tarqalgan «ko`z qamashtiradigan» virusga qarshi maxsus ishlab chiqilgan kuchli himoya vositasi yordam bera oladi.
- Shuni aytib o`tish kerakki, I. Blazer nomli virus on-layn o`yinlar o`ynaydigan Internet foydalanuvchilar orasida vaqtinchalik ko`z ojizlik epidemiyasini keltirgan. «Ko`z nur» virusi lyuminatsiya mikromonitorlarning zaifligi sababli o`z ta'sirini ko`rsata oladi, zamonaviy 3D vizuallashtirish qurilmalari esa aynan shu monitorlar bilan jihozlangan.

Demak, axborot xavfsizligi qoidasiga jiddiy amal qilish iqtisodiy va ilmiy texnik ahamiyatga ega. Bu qoidalarni aniq tizimlashtirish va aniqlashtirish lozim. Shu bilan birga, xorijiy axborot vositalaridan foydalanuvchilar ularning buzilmay ishlashi va ishonchliligiga asosiy e'tiborni qaratishlari talab qilinadi.
INTERNETda informasion xavfsizlik. Ma'lumki internet tarmoqlararo informatsiyalar almashinuvini ta'minlovchi magistraldir. Uning yordamida dunyo bilimlari manbaiga kirish, qisqa vaqt ichida ko`plab ma'lumotlarni yig`ish, ishlab chiqarishni va uning texnik vositalarini masofadan turib boshqarish mumkin. Shu bilan bir qatorda internetning ushbu imkoniyatlaridan foydalanib yuqorida aytib o’tganimizdek, tarmoqdagi begona kompyuterlarni boshqarish, ularning ma'lumotlar bazasiga kirish, nusxa ko`chirish, g`arazli maqsadda turli xil viruslar tarqatish kabi noqulay ishlarni amalga oshirish ham mumkin. Internetda mavjud bo`lgan ushbu xavf, informatsion xavfsizlik muammolari bevosita tarmoqning xususiyatlaridan kelib chiqadi. Ixtiyoriy tarmoq xizmatini o`zaro kelishilgan qoida ("protokol") asosida ishlovchi juftlik "server" va "mijoz" programma ta'minoti bajaradi. Ushbu protokollar miqyosida ham "server", ham "mijoz" programmalari ruxsat etilgan amallarni (operatsiyalarni) bajarish vositalariga ega (masalan, HTTP protokolidagi formatlash komandalari, Web sahifalarda joylashtirilgan tovush, videoanimatsiyalar va har xil aktiv ob'ektlar ko`rinishidagi mikroprogrammalar). Xuddi shunday ruxsat etilgan operatsiyalar, aktiv ob'ektlardan foydalanib internetda ba'zi bir noqonuniy harakatlarni amalga oshirish, tarmoqdagi kompyuterlarga va ma'lumotlar bazasiga kirish, hamda ularga tahdid solish mumkin bo`ladi.
Bu xavf va tahdidlar quyidagilardan iborat:

- Tarmoqdagi kompyuterlarga ruxsatsiz kirish va uni masofadan turib boshqarish, ularga sizning manfaatingizga zid bo`lgan programmalarni joylashtirish mumkin.
- Web saxifalarda joylashtirilgan "aktiv ob'ekt" lar agressiv programma kodlari bo`lib, siz uchun xavfli "virus" yoki josus programma vazifasini o`tashi mumkin.
- Internetda uzatilayotgan ma'lumotlar yo`l-yo`lakay aloqa kanallari yoki tarmoq tugunlarida tutib olinishi, ulardan nusxa ko`chirilishi, almashtirilishi mumkin.
- Davlat muassasasi, korxona (firma) faoliyati, moliyaviy axvoli va uning xodimlari haqidagi ma'lumotlarni razvedka qilishi, o’g’irlashi va shu orqali sizning shaxsiy hayotingizga, korxona rivojiga taxdid solishi mumkin.
- Internetda e'lon qilinayotgan har qanday ma'lumot ham jamiyat uchun foydali bo`lmasligi mumkin. Ya'ni, internet orqali bizning ma'naviyatimizga, madaniyatimizga va e'tiqodimizga zid bo`lgan informatsiyalarni kirib kelish ehtimoli ham mavjud.

Internet foydalanuvchisi, ushbu xavflarni oldini olish uchun quyidagi texnik echim va tashkiliy ishlarni amalga oshirishi zarur:

- Shaxsiy kompyuterga va mahalliy kompyuter tarmog`iga, hamda unda mavjud bo`lgan informatsion resurslarga tashqaridan internet orqali kirishni cheklovchi va ushbu jarayonni nazorat qilish imkonini beruvchi texnik va dasturiy usullardan foydalanish;
- Tarmoqdagi informatsion muloqat ishtirokchilari va ular uzatayotgan ma'lumotlarni asl nusxasi mosligini tekshirish;
- Ma'lumotlarni uzatish va qabul qilishda "kriptografiya" usullaridan foydalanish;
- Viruslarga qarshi nazoratchi va davolovchi programmalardan foydalanish;
- Shaxsiy kompyuter va mahalliy kompyuter tarmog`iga begona shaxslarni qo`ymaslik va ularda mavjud bo`lgan ma'lumotlardan nusxa olish imkoniyatlarini cheklovchi tashkiliy ishlarni amalga oshirish.

Bundan tashqari informatsion xavfsizlikni ta'minlash borasida **internet foydalanuvchilari orasida o`rnatilmagan tartib-qoidalar** mavjud. Ulardan ba'zi-birlarini keltiramiz:

- Hich qachon hich kimga internetdagi o`z nomingiz va parolingizni aytmang;
- Hich qachon hich kimga o`zingiz va oila a'zolaringiz haqidagi shaxsiy, hamda ishxonangizga oid ma'lumotlarni (ismi sharifingiz, uy adresingiz, bankdagi hisob raqamingiz, ish joyingiz va uning xodimlari haqida ma'lumotlarni va hokazo) internet orqali yubormang;
- Elektron adresingizdan (e-mail) maqsadli foydalaning, internet orqali programmalar almashmang;
- Internetda tarqatilayotgan duch kelgan programmalardan foydalanmang. Programmalarni faqat ishonchli, egasi ma'lum bo`lgan serverlardan ko`chiring.
- Elektron pochta orqali yuborilgan "aktiv ob'ekt"lar va programmalarni ishlatmang, .exe qo`shimchali o`z-o`zidan ochiluvchi sizga noma'lum arxiv ko'rinishidagi materiallarni ochmang;
- Elektron pochta xizmatidan foydalanayotganingizda ma'lumotlarni shifrlash zarur, ya'ni "kriptografiya" usullaridan albatta foydalaning;
- Egasi siz uchun noma'lum bo`lgan xatlarni ochmang;
- Egasi ma'lum bo`lgan va uning sifatiga kafolat beruvchi antivirus programmalaridan foydalaning va ularni muntazam yangilab boring;
- Internetda mavjud bo`lgan informatsion resurslar va programmalardan ularning avtorlari ruxsatisiz foydalanmang;
- Tarmoqdagi begona kompyuter va serverlarning IP adreslarini aniqlash va shu orqali ruxsat etilmagan serverlar va informatsion resurslarga kirish, nusxa ko`chirish, viruslar tarqatish kabi noqonuniy programmalashtirish ishlari bilan shug`ullanmang, bu jinoyatdir.

Axborot xavfsizligini ta'minlashning biometrik usullari. Hozirgi vaqtga kelib, kompyuter-kommunikatsiya texnologiyalari kundan-kunga tez rivojlanib bormoqda. Shu sababli ham kompyuter texnologiyalari kirib bormagan sohaning o'zi qolmadi, desak xato bo'lmaydi. Ayniqsa ta'lim, bank, moliya tizimlarida ushbu zamonaviy texnologiyalarni qo'llash yuqori samara bermoqda. Shu bilan birga axborot havfsizligiga bo'lgan tahdid ham tobora kuchayib borayotgani hech kimga sir emas. Demak, hozirgi davrning eng dolzarb muammolardan biri axborot havfsizligini ta'minlashdan iborat. Hozirga qadar tizimga ruxsatsiz kirishni taqiqlashning eng keng tarqalgan usuli sifatida «parol» qo'yish printsipi hisoblanib kelmoqda. Chunki ushbu usul juda sodda, foydalanish uchun qulay va kam harajat talab etadi. Lekin, hozirga kelib «parol» tizimi to'laqonli o'zini oqlay olmayapti. Ya'ni ushbu usulning bir qator kamchiliklari ko'zga tashlanib qoldi.

Birinchidan, ko'pchilik foydalanuvchilar sodda va tez esga tushadigan parollarni qo'llaydilar. Masalan, foydalanuvchi o'z shaxsiga oid sanalar, nomlardan kelib chiqqan holda parol qo'yadilar. Bunday parollarni buzish esa, foydalanuvchi bilan tanish bo'lgan ixtiyoriy shaxs uchun unchalik qiyinchilik tug'dirmaydi.

Ikkinchidan, foydalanuvchi parolni kiritishi jarayonida, kuzatish orqali ham kiritilayotgan belgilarni ilg'ab olish mumkin.

Uchinchidan, agar foydalanuvchi parol qo'yishda murakkab, uzundan-uzoq belgilardan foydalanadigan bo'lsa, uning o'zi ham ushbu parolni esidan chiqarib qo'yishi extimoldan holi emas.

Va nihoyat, hozirda ixtiyoriy parollarni buzuvchi dasturlarning mavjudligi ko’zga tashlanib qoldi.
Yuqoridagi kamchiliklardan kelib chiqqan holda aytish mumkinki, axborotni himoyalashning parolli printsipidan foydalanish to’la samara bermayapti. Shu sababli ham hozirda axborotlardan ruxsatsiz foydalanishni cheklashning biometrik usullarini qo’llash dunyo bo’yicha ommaviylashib bormoqda va ushbu yo’nalish biometriya nomi bilan yuritilmoqda.
Biometriya – bu insonning o’zgarmaydigan biologik belgilariga asosan aynan o’xshashlikka tekshirishdir (identifikatsiya). Hozirda biometrik tizimlar eng ishonchli himoya vositasi hisoblanadi va turli xil maxfiy ob'ektlarda, muhim tijorat axborotlarini himoyalashda samarali qo’llanilmoqda.
Hozirda biometrik texnologiyalar insonning quyidagi o’zgarmas biologik belgilariga asoslangan: barmoqning papillyar chiziqlari, qo’l kaftining tuzilishi, ko’zning kamalak qobig’i chiziqlari, ovoz parametrlari, yuz tuzilishi, yuz termogrammasi (qon tomirlarining joylashishi), yozish formasi va usuli, genetik kodi fragmentlari. Insonning ushbu biologik belgilaridan foydalanish turli xil aniqliklarga erishishga imkon beradi. Biz ushbu maqolada hozirda keng qo’llanilayotgan barmoq izlari va qo’l kaftining tuzilishi bo’yicha insonni tanish masalalariga to’xtalib o’tishni lozim topdik.
“Barmoq izlari buyicha insonni idetifikatsiyalash” hozirda eng keng tarqalgan usul bo’lib, axborotni himoyalash biometrik tizimlarida keng qo’llanilmoqda. Bu usul o’tgan asrlarda ham keng qo’llanilganligi xech kimga yangilik emas. Hozirgi kunga kelib barmoq izlari bo’yicha identifikatsiyalashning uchta asosiy texnologiyasi mavjud. Ularning birinchisi ko’pchilikka ma'lum optik skanerlardan foydalanishdir. Ushbu qurilmadan foydalanish printsipi odatiy skanerdan foydalanish bilan bir xil. Bu erda asosiy ishni ichki nur manbai, bir nechta prizma va linzalar amalga oshiradi. Optik skanerlarni qo’llashning e'tiborli tomoni uning arzonligidir. Lekin, kamchilik tomonlari bir muncha ko’p. Ushbu qurilmalar tez ishdan chiquvchi hisoblanadi. Shu sababli foydalanuvchidan avaylab ishlatish talab etiladi. Ushbu qurilmaga tushgan chang, turli xil chiziqlar shaxsni aniqlashda xatolikka olib keladi, ya'ni foydalanuvchining tizimga kirishiga to’sqinlik qiladi. Bundan tashqari, optik skanerda tasviri olingan barmoq izi foydalanuvchi terisining holatiga bog’liq. Ya'ni, foydalanuvchi terisining yog’liligi yoki quruqligi shaxsni aniqlashga xalaqit beradi.
Barmoq izlari bo’yicha identifikatsiyalashning ikkinchi texnologiyasi elektron skanerlarni qo’llashdir. Ushbu qurilmadan foydalanish uchun foydalanuvchi 90 ming kondensator plastinkalaridan tashkil topgan, kremniy moddasi bilan qoplangan mahsus plastinkaga barmog’ini qo’yadi. Bunda o’ziga xos kondensator hosil qilinadi. Kondensator ichidagi elektr maydon potentsiali plastinkalar orasidagi masofaga bog’liq. Ushbu maydon kartasi barmoqning papillyar chizmasini takrorlaydi. Elektron maydon hisoblanadi, olingan ma'lumotlar esa, katta aniqlikka ega sakkiz bitli rastrli tasvirga aylantiriladi. Ushbu texnologiyaning e'tiborli tomoni shundaki, foydalanuvchi terisining har qanday holatida ham barmoq izi tasviri yuqori aniqlikda hosil qilinadi. Ushbu tizim foydalanuvchi barmog’i kirlangan taqdirda ham tasvirni aniq oladi. Bundan tashqari qurilma hajmining kichikligi sababli, ushbu qurilmani hamma joyda ishlatish mumkin. Ushbu qurilmaning kamchilik tomonlari sifatida quyidagilarni keltirish mumkin: 90 ming kondensatorli plastinkani ishlab chiqarish ko’p harajat talab etadi, skanerning asosi bo’lgan kremniy kristali germetik (zich yopiladigan) qobiqni talab etadi. Bu esa, qurilmani ishlatishda turli xil cheklanishlarni yuzaga keltiradi. Nihoyat, kuchli elektromagnit nurlanishi vujudga kelganda elektron sensor ishlamaydi.
Barmoq izi buyicha identifikatsiyalashning uchinchi texnologiyasi Who Vision Sustems kompaniyasi tomonidan ishlab chiqarilgan Tactile Sense skanerlaridir. Ushbu skanerlarda maxsus polimer material ishlatilgan bo’lib, terining bo’rtib chiqqan chiziqlari va botiqlari orasida hosil bo’lgan elektr maydonni sezish orqali tasvir hosil qilinadi. Umuman olganda ushbu skanerlarning ishlash printsipi elektron skanerlar ishlash

printsipi bilan deyarli bir xil. Faqat ushbu qurilmalarning quyidagi afzalliklarini sanab o'tishimiz mumkin: qurilmani ishlab chiqarish bir necha yuz barobar kam harajat talab etadi, qurilma avvalgi qurilmadan mustahkam va foydalanishda hech qanday cheklanishlar yuzaga kelmaydi.

"Insonining qo'l kafti tuzilishiga ko'ra identifikatsiyalash"ning ikki xil usuli mavjud. **Birinchi usulda** qo'l kaftining tuzilishidan foydalaniladi. Buning uchun maxsus qurilmalar ishlab chiqarilgan bo'lib, ushbu qurilma kamera va bir nechta yorituvchi diodlardan tashkil topgan. Ushbu qurilmaning vazifasi qo'l kaftining uch o'lchovli tasvirini hosil qilishdan iborat. Keyinchalik ushbu hosil qilingan tasvir ma'lumotlar bazasiga kiritilgan tasvir bilan solishtiriladi. Ushbu qurilma yordamida identifikatsiyalash yuqori aniqlikda amalga oshiriladi. Lekin kaft tasvirini oluvchi skaner o'ta nozik ishlangan bo'lib, ushbu qurilmadan foydalanish noqulayliklar tug'diradi.
Qo'l kafti tuzilishiga ko'ra identifikatsiyalashning **ikkinchi texnologiyasi** esa, kaftning termogrammasini aniqlashga asoslangan. Qo'l kaftida juda ko'p qon tomirlari mavjud bo'lib, ushbu qon tomirlari har bir insonda, hattoki egizaklarda ham turlicha joylashadi. Ushbu qon tomirlarining joylashish tasvirini olish uchun maxsus infraqizil nurli fotokameradan foydalaniladi. Ushbu hosil bo'lgan tasvir kaft termogrammasi deb ataladi. Ushbu usulning ishonchliligi juda ham yuqori. Bu usulning vujudga kelganiga ko'p vaqt bo'lmaganligi sababli hali keng tarqalib ulgurmagan.
Keltirib o'tilgan barcha biometrik usullar axborotni himoya qilishda keng qo'llanilmoqda. Ushbu himoya tizimining ishonchliligi shundaki, tizimda foydalanilayotgan insonning biologik belgilari hech qachon o'zgarmaydi, biron-bir jaroxat etgan taqdirda ham qayta tiklanadi.
Yuqorida biz insonning biologik belgilariga asosan shaxsni tanish maqsadida barmoq izi va qo'l kaftining tasvirini hosil qilish texnologiyalari bilan tanishib chiqdik. Endigi masala hosil qilingan tasvirni ma'lumotlar bazasida saqlanayotgan tasvir bilan taqqoslash va shaxsni aniqlash algoritmi bilan bog'liq. Biz ushbu masalada hosil qilingan barmoq izidan foydalangan holda shaxsni aniqlash algoritmini keltirib o'tishga harakat qilamiz. Yuqorida ta'kidlaganimizdek, birinchi navbatda ixtiyoriy qurilma orqali barmoq izi tasviri hosil qilinadi. Qolgan bosqichlarni quyidagi ketma-ketlik orqali bayon qilishga harakat qilamiz:

1. **Tasvirga boshlang'ich ishlov berish** – bunda hosil qilingan tasvir Binar tasvirga o'tkaziladi, ya'ni, tasvirdagi faqat barmoq izining chiziqlari olib qolinadi va tasvirning markazi (og'irlik markazi) aniqlanadi;
2. **Tasvirdagi o'ziga xos belgilarni aniqlash** – bunda tasvirning markazidan turli xil radiusli bir nechta aylanalar chiziladi (aylanalar qanchalik ko'p bo'lsa, aniqlik shunchalik ortadi). Natijada aylanalar hosil qilingan tasvir chiziqlarining bir nechta nuqtalarida kesishadi. Ushbu kesishish nuqtalari shartli ravishda $A_1, A_2, ..., A_n$ (birinchi aylana), $B_1, B_2, ..., B_m$ (ikkinchi aylana), $C_1, C_2, ..., C_k$ (uchinchi aylana) harflari yordamida belgilanadi. Har bir aylanadagi kesishish nuqtalarini birlashtirish orqali $A_1A_2...A_n$, $B_1B_2...B_m$, $C_1C_2...C_k$ ko'pburchaklar hosil qilinadi. Ushbu hosil qilingan ko'pburchaklar perimetrlari (P_1, P_2>, P_3) hisoblanadi.
3. **Olingan tasvirni ma'lumotlar bazasida saqlanayotgan tasvir bilan solishtirish** – bunda yuqoridagi bosqichda olingan natijalar: R_1, R_2, R_3 radiusli aylanalardagi kesishishlar soni n, m, k; aylanalarda hosil qilingan ko'pburchaklar perimetri
P_1,P_2, P_3 lar ma'lumotlar bazasida saqlanayotgan ushbu kattaliklar bilan taqqoslanadi. Ushbu kattaliklar o'zaro mos tushsagina shaxs tasdiqlanadi.