O’ZBEKISTON RESPUBLIKASI OLIY VA O’RTA MAXSUS TA`LIM VAZIRLIGI

BUXORO MUHANDISLIK - TEXNOLOGIYALAR INSTITUTI

«Elektrotexnika va ishlab chiqarishda axborot-kommunikatsiya texnologiyalari» fakulteti

«Axborot kommunikatsiya texnologiyalari» kafedrasi

5111018 – Kasb ta`limi («Informatika va axborot texnologiyalari») ta`lim yo’nalishi bo’yicha

« Open Source Clamav asosida antivirus dasturi yaratish» mavzusidagi

BITIRUV MALAKAVIY ISH

Bajardi: **12-14 MIAT guruhi talabasi**
Safarova Sitora

Rahbar: **katta o’qituvchi. Muhammadiyeva.K.B.**

BUXORO – 2018

M U N D A R I J A

Kirish

Insoniyt yaralibdiki, yovuzlik va ezgulik, oq va qora, tun va kun kabi so’zlarning moxiyati xayot falsafasini tashkil etib keladi. Fan texnikaning inqilobi anchagina ildamlab ketgan zamonda yashayapmiz ekan, texnika bilan birgalikda “ezgulik- yovuzlik ” tushunchalari xam takomillashib borar ekan. Fan texnika olamida “sayr” qilib yurgan “kurmak” lar yoki “yovuz” lar xozirgi kunda dunyoning ko’pgina kompaniyalari, korporatsiyalariyu banklariga jiddiy xavf solmoqda. Gap kompyuter yovuz dasturchilari, hakkerlar xaqida ketmoqda. Mo’may daromad topmoq ilinjida yoki ko’ngil xushlik uchun yaratilayotgan zararli kompyuter dasturiy ta’minotlari ayni hakkerlar tomonidan yaratiladi. Ularning buzg’unchi dasturlari dunyo iqtisodiyotiga yiliga milliyonlab xattoki milliardlab dollar zarar yetkazadi. Bunday dasturlarga qarshi choralar xam yo’q emas. Ammo kompyuter texnologiyalari rivojlanishi bilan mutanosib ravishda viruslarning yangi-yangi turlari dunyo yuzini ko’rmoqda. Shu o’rinda biz Diplom loyihamizda, kompyuterning zararli dasturiy ta’minotlari ularni aniqlash usullari , ularni turlarga ajratish metodikasi, ulardan ximoyalanish va ularga qarshi chora tadbirlar ko’rish kabi dolzarb mavzularni ko’rib chiqamiz.

I-BOB. AXBOROT XAVFSIZLIGI KONSEPSIYASI VA TAHDIDLAR

1.1 Axborot xavfsizligi tushunchasi va konsepsiyasi

Xavfsizlik - har kuni biz to’qnashadigan hayotimizning jihati: eshikni qulflaymiz, qimmatbaho narsalarni begona ko’zlardan berkitamiz va hamyonni duch kelgan joyda qoldirmaymiz. Bu "raqamli dunyoga" ham rasm bo’lishi shart, chunki har bir foydalanuvchining kompyuteri qaroqchi hujumi ob’ekti bo’lishi mumkin.

Kommertsiya tashkilotlari xavfsizlikni ta’minlash o’zining birinchi galdagi vazifasi emas, balki uni ta’minlashga sarf etiladigan harajatlarni muqarrar bal o deb hisoblab kelganlar. Qandaydir darajada bu "oqilona ish": nihoyat, usiz ham ish bajarishda to’siqlar to’libtoshib yotibdiku?! Ammo firmaning barcha korporativ binolariga kecha-kunduz ki-rishga ruxsat berishga jur’at etuvchi aqli joyida "sanoat kapitanlari"ni ko’rganmisiz? Albatta, yo’q! Hatto kichkina kompaniya binosining kirish yo’lida sizni qorovul, yoki kirishni chegaralovchi va nazoratlovchi tizimi qarshi oladi. Axborotni himoyalash esa hali ko’ngildagidek emas. Axborotni qanday yo’qotish mumkinligini va bu qanday okibatlarga olib kelishi-ni barcha ham tushunavermaydi.

Yirik o’yinchilar yaxshigina saboq oldilar: xakerlar Yahoo.com, Amazon.com kabi kompaniyalarga va hatto kosmik tadkiqot agentiligi NASAra katta zarar etkazdilar. Xavfsizlik xizmati bozorining eng yirik nomoyondalaridan biri RSA Security, harqanday taxdidga qarshi chora borligi xususidagi o’ylamasdan qilgan bayonotidan bir necha kundan keyin, xujumga duchor bo’ldi[29].

Odatda odamlardan yoki predmetlardan chiqadigan va zarar etkazadigan taxdidlar quyidagi sinflarga bo’linadi: *ichki* yoki *tashtsi* va *tuzilmalan-gan* (ma’lum ob’ektga qarshi) yoki *tuzilmalanmagan* ("kimga Xudo beradi" qabilida

adreslanuvchi). Masalan, kompyuter viruslari "tashki tuzilmalanmagan taxdidlar" sifatida turkumlanadi va tamomila oddiy hisoblanadi. Kizig'i shundaki, foydalanuvchilar o'zining kompyuterini muayyan nishon deb hisoblamaydilar, ular o'zlarini yaxshigina himoyalangandek sezadilar. Kerakli himoya darajasi aksariyat hollarda ishingizning holatiga bog'liq. Agar tashkilotingiz yoki kompaniyangiz qandaydir tazyiq nishoni bo'lsa, agar siz milliy energetik resurslarni taqsimlovchi yoki milliy aloqa tarmoqlariga xizmat kiluvchi davlat in-fratuzilmasi tarkibida bo'lsangiz, oddiy terroristlar bombalarini va pistoletlarini chetga qo'yib, turli-tuman dasturiy vositalar yordamida tashkilotingizga elektron xujumni amalga oshirish masalasini ko'radilar. Ikkinchi tomondan, savdo-sotiq va marketing bo'yicha oddiy tashkilot xusu-sida so'z borsa, faqat mijozlar ruyxatini o'grilovchi xizmatchilaringiz to'grisida, qalbaki kredit kartochkalari bo'yicha tovar oluvchi firibgarlar, tarmogingizga preyskurantlardan foydalanish maqsadida kiruvchi rakiblar, Web-saytingizni ta'magirlik maqsadida buzuvchilar va shunga o'xshashlar to'grisida qaygurishingizga to'gri keladi.

AMMO, vahimaga o'rin yo'q. Birinchi navbatda kundalik ehtiyoj chora-lari ko'rilishi lozim. Axborotga ega bo'lishning eng ommabop usuli optsiy o'grilik. Siz ish stolingizda kechaga mumaygina pulni qoldirib ketmaysi-zu. Nima uchun boquvchingiz-shaxsiy kompyuter xavfsizligini ta'minlashga ozgina vaqt sarf kilmaysiz? Bu nafaqat apparat vositalariga, balki ma'lumotlarga ham taallukli. Ma'lumotlarni o'girlatish yoki yo'qotish katta, ba'zida, tuzatib bo'lmaydigan zarar keltiradi.

Ma'lumki, tizim ma'murlari barcha mahfiy materiallardan foydalanish imkoniga ega va, odatda, kompaniya foydasidan o'z ulushlariga ega emaslar. SHu sababli xuddi ular tashkilot xavfsizligiga taxdid sola oluvchilar ichida eng kattasi hisoblanadilar. Ta'kidlash lozimki, kompaniya ishga kiruvchilarni sinchiklab tekshiradi. Xudtsi shunday, xavfsizlik xizmatini ta'minlovchilarga, ayniqsa maslaxat berish, rejalashtirish va mu'murlashni tavsiya etuvchilarga diqqat bilan qarash lozim.

O'zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli «Axborot erkinligi prinsiplari va kafolatlari to'g'risida»gi qonunida **axborot** va uning turlari to'g'risida quyidagi ta'riflar keltirilgan: axborot – manbalari va taqdim etilish shaklidan qat'i nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to'g'risidagi ma'lumotlar;

axborotni muhofaza etish – axborot borasidagi xavfsizlikka tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish chora-tadbirlari;

ommaviy axborot – cheklanmagan doiradagi shaxslar uchun mo'ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar;

hujjatlashtirilgan axborot – identifikatsiya qilish imkonini beruvchi rekvizitlari qo'yilgan holda moddiy jismda qayd etilgan axborot;

maxfiy axborot – foydalanilishi qonun hujjatlariga muvofiq cheklab qo'yiladigan hujjatlashtirilgan axborot.

Ushbu ta'rif O'zbekiston Respublikasi Vazirlar Mahkamasining «O'zbekiston Respublikasi Prezidentining «Milliy axborot resurslarini muhofaza qilishga

doir qo‘shimcha chora-tadbirlar to‘g‘risida» 2011-yil 8-iyuldagi PQ–1572-son qarorini amalga oshirish chora-tadbirlari haqida»gi 2011-yil 7-noyabr 296-sonli qarorida quyidagicha ifodalangan: maxfiy axborot – O‘zbekiston Respublikasi qonun hujjatlariga muvofiq foydalanish cheklangan, davlat sirlariga mansub axborot mavjud bo‘lmagan hujjatlashtirilgan axborot.

Konfedensial axborot – hujjatlashtirilgan axborot, undan foydalanish qonun hujjatlariga muvofiq chegaralanadi.

Saqlash, o‘zgartirish, uzatish va ma’lum maqsadlar uchun foydalanish obyekti bo‘lgan tevarak olam haqidagi ma’lumotlarni, keng ma’noda axborot deb tushunish mumkin. Bu tushunchaga ko‘ra inson, uning hayot tarziga va harakatlariga ta’sir etuvchi doimiy o‘zgaruvchi axborot maydoni ta’sirida bo‘ladi. Axborot o‘z tavsifiga ko‘ra siyosiy, harbiy, iqtisodiy,ilmiy-texnik, ishlab chiqarishga yoki tijoratga oid hamda maxfiy, konfedensial yoki nomaxfiy bo‘lishi mumkin.

O‘zbekiston Respublikasining 1993-yil 7-maydagi 848-XII-sonli «Davlat sirlarini saqlash to‘g‘risida»gi qonunning 1-moddasida davlat sirlari tushunchasi berilgan:

«Davlat tomonidan qo‘riqlanadigan va maxsus ro‘yxatlar bilan chegaralab qo‘yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiy-texnikaviy va o‘zga xil ma’lumotlar O‘zbekiston Respublikasining davlat sirlari hisoblanadi». Mazkur qonunning 3-moddasida davlat sirlarining toifalari keltirilgan: «O‘zbekiston Respublikasining davlat sirlari – davlat, harbiy va xizmat sirlarini qamrab oladi. Oshkor etilishi respublika harbiy-iqtisodiy imkoniyatlarining sifat holatiga salbiy ta’sir etishi yoki O‘zbekiston Respublikasining mudofaa qobiliyati, davlat xavfsizligi, iqtisodiy va siyosiy manfaatlari uchun boshqa og‘ir oqibatlar keltirib chiqarishi mumkin bo‘lgan ma’lumotlar davlat sirini tashkil etadi.

Oshkor etilishi O‘zbekiston Respublikasining mudofaa qobiliyati, davlat xavfsizligi va Qurolli Kuchlari uchun og‘ir oqibatlar keltirib chiqarishi mumkin bo‘lgan harbiy xususiyatga ega ma’lumotlar harbiy sirni tashkil etadi. Oshkor etilishi O‘zbekiston Respublikasi manfaatlariga zarar yetkazishi mumkin bo‘lgan fan, texnika, ishlab chiqarish va boshqaruv sohasiga doir ma’lumotlar xizmat sirini tashkil etadi». Axborot xavfsizligi tushunchasi, uning tashkil etuvchilari tavsifi. Axborot xavfsizligi deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan qilingan ta’sirlardan axborot va uni qo‘llab-quvvatlab turuvchi infrastukturaning himoyalanganligi tushuniladi. Bunday ta’sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo‘llab quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin.

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida axborot xavfsizligi axborot borasidagi xavfsizlik deb belgilangan va uaxborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

TSivilizatsiya rivojining zamonaviy bosqichida axborot nafaqat jamoat va davlat institutlari faoliyatida, balki har bir inson hayotida hal kiluvchi rolni

uynaydi. Ko’z oldimizda jamiyatning axborotlashishi shid-dat bilan va ko’pincha oldindan bilib bo’lmaydigan tarzda rivojlanmokda.

Biz esa uning ijtimoiy, siyosiy, iqtisodiy va boshqa oqibatlarini tushu-nib etishga boshlaymiz, xolos. Jamiyatimizning axborotlashishi yagona dunyo axborot makonining yaratilishiga olib keladiki, bu makon doirasida axborotni yig’ish, ishlash, saqlash va sub’ektlar - insonlar, tashkilotlar, davlatlar o’rtasida almashish amalga oshiriladi.

Ravshanki, siyosiy, iqtisodiy, ilmiy-texnikaviy va boshqa axborot-larni tezlikda almashish imkoniyati jamiyat hayotining barcha sohalarida va ayniqsa ishlab chiqarishda va boshqarishda yangi texnologiyalarning qo’llanilishi so’zsiz foydalidir. Ammo, sanoatning tezlikda rifojlanishi Er ekologiyasiga taxdid sola boshladi, yadro fizikasi sohasidagi yutuqlar yadro urushi xavfini to’g’dirdi. Axborotlashtirish ham jiddiy mu-ammolar manbaiga aylanishi mumkin.

Urushlar doimo bo’lgan. Vakt o’tishi bilan urushni olib borish butun bir fanga aylandi. Harqanday fandagidek urushda o’zining tarixi, o’zining qoidasi, mashhur namoyondalari, o’zining metodologiyasi paydo bo’ldi.

Zamonaviy urush g’oyasi juda ildamlab ketdi. Endi uning makoni -butun er shari. Urush lokal qaroqchi xujumidan bir necha davlatlarni vay-ron qiluvchi global muammoga aylandi.

Turli mamlakatlarning harbiy doktrinalarida elektron qurol ri-voji rejalari va maxsus vazifalarga mo’ljallangan dasturiy ta’minot to’grisida eslatishlar ko’zga tashlanmokda. Turli razvedka manbalaridan kelayotgan axborotning taxdili natijasida xulosa qilish mumkinki, ba’zi bir davlatlarning rahbarlari xujumkor kiber-dasturlarni yaratishni moliyal amokdalar.

Axborot urushiga oddiy vositalar yordamida harbiy harakatlar sama-ra bermaydigan hollarga nisbatan strategik alternativa sifatida qaralmokda.

Harbiylar tomonidan kiritilgan *axborot urushi* atamasi real, kdrginli va emiruvchi harbiy harakatlar bilan bog’liq shafqatsiz va xav-fli faoliyatni anglatadi. Bu urushning alohida kdrralari-shtab urushi, elektron urushi, psixologik amallar va h.

Harqanday urush, axborot urushi shu jumladan, zamonaviy qurol yor-damida olib boriladi. Axborot quroli yordamida, urush olib boriluvchi barcha qurollardan farqli o’laroq, e’lon qilinmagan va ko’pincha dunyoga ko’rinmaydigan urushlarni olib borish mumkin (olib borilmoqtsa ham). Bu qurolning ta’sir ob’ektlari - iqtisodiy, siyosiy, ijtimoiy va h. kabi jamiyat va davlat institutlari. Ma’lumotlarni uzatish tarmoqlarining kelajak janglar maydoniga aylanishi allaqachon e’tirof etilgan.

Axborot quroli xujumda va mudofaada "elektron tezlik" bilan ish-latilishi mumkin. U eng ilg’or texnologiyalarga asoslangan bo’lib, harbiy nizolarni dastlabki bosqichida hal etilishini ta’minlaydi hamda umummaqsad kuchlarning qo’llanilishini istisno qiladi. Axborot quroli qo’llanishining strategiyasi xujumkor xarakterga ega. Ammo xususiy zaif-lik nuqtai nazari mavjud, ayniqsa fuqorolik sektorida. SHu sababli bunday quroldan va axborot terrorizmidan himoyalanish muammosi hozirda birinchi o’ringa chiqqan. Foydalanuvchilariga dunyo

tarmoqlarida ishlashni ta’minlovchi mamlakatlarning milliy axborot resurslarining zaifligi -har ikki tomonga xavfli narsa.

Axborot quroli deganda axborot massivlarini yo’qotish, buzish yoki o’g’irlash vositalari, himoyalash tizimini yo’qotish, qonuniy foydalanuv-chilar faoliyatini chegaralash asbob-uskunalar va butun kompyuter tizimi ishlashi tartibini buzish vositalari tushuniladi.

Hozirda xujumkor axborot quroli sifatida quyidagilarni ko’rsatish mumkin:

- *kompyuter viruslari* - ko’payish, dasturlarda o’rnashish, aloqa liniyalari, ma’lumotlarni uzatish tarmoqlari bo’yicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga o’xshash qobiliyatlarga ega;

- *mantikiy bombalar* - signal bo’yicha yoki o’rnatilgan vaqtda harakatga keltirish maqsadida harbiy yoki fuqaro infratuzilmalariga o’rnatiluvchi dasturlangan qurilmalar;

- *telekommunikatsiya tarmoklarida axborot almashinuvini bostirish vositalari,* davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish;

- *testli dasturlarni betaraflashtirish vositalari;*

- ob’ekt dasturiy ta’minotiga ayg’oqchilar tomonidan atayin kiritiluvchi turli xil *xatoliklar.*

Universallik, maxfiylik, dasturiy-apparat amalga oshirilishining har xilligi, ta’sirining keskinligi, qo’llanilishining vaqti va joyini tanlash imkoniyati, nihoyat, foydaliligi axborot qurolini haddan tashqari xavfli kiladi. Bu qurolni, masalan, intellektual mulkni himoyalash vosi-tasiga o’xshatib niqoblash mumkin. Undan tashkari, u hatto urush e’lon kilmasdan xujum harakatlarini avtonom tarzda olib borish imkonini beradi.

Zamonaviy jamiyatda axborot qurolini ishlatish harbiy strategiyasi fuqaro sektori bilan uzviy bog’langan. Axborot kurolining, uning ta’siri shakli va usullarining paydo bo’lishi va qo’llanishi xususiyatlarining tur-li-tumanliligi undan himoyalanishning murakkab masalalarini vujudga keltirdi.

Axborot quroli qo’llanilishini oldini olish yoki qo’llanishi okibatlarini bartaraf kilish uchun quyidagi choralarni ko’rish lozim:

- axborot resurslarining fizik asosini tashkil etuvchi moddiytexnik ob’ektlarni himoyalash;
- ma’lumotlar bazalari va banklarining meyoriy va muttasil ishlashini ta’minlash;
- axborotdan ruxsatsiz foydalanishdan, uni buzilishidan yoki yo’q kilinishidan himoyalash;
- axborot sifatini saqlash (o’z vaktidaligi, aniqligi, to’laligi va foydalanuvchanligi).

Davlatning dunyo ochiq tarmog’iga ulanishining iqtisodiy va ilmiy-texnik siyosatini axborot xavfsizligi orqali ko’rish lozim. Bu ochiq, fuqarolarning axborotga va intellektual mulkga ega bo’lish qonuniy huqukini saqlashga mo’ljallangan siyosat mamlakat xududida tarmoq asbob-uskunalarini unga axborot quroli elementlarining kirishidan saqlashni ko’zda tutish lozim. Bu muammo hozirda, chet el axborot texnologiyalarini ommaviy sotib olinayotgan paytda o’ta muhimdir.

Ma’lumki, dunyo axborot makoniga ulanmasdan mamlakat iqtisodini rivojlantirib bo’lmaydi. Internet tarmog’i tomonidan ta’minlangan axborot va hisoblash resurslaridan operativ foydalanishni davlatchilikni, fuqarolik jamiyati institutlarini mustahkamlash, ijtimoiy infratuzil-malarining rivojlanish shartlari sifatida talqin etish mumkin.

Ammo mamlakatning halqaro telekommunikatsiya tizimida va axborot almashinuvida ishtirokining axborot xavfsizligi muammosini kompleks hal kilmasdan mumkin emasligini aniq tasavvur etish l ozim. Ayniqsa xu-susiy axborot resurslarini himoyalash muammosi axborot va telekommunikatsiya texnologiyalar sohasida rivojlangan mamlakatlardan texnologik orqada qolayotgan mamlakatlar uchun jiddiy hisoblanadi.

Axborot qurolini ishlab chikishni va uni ishlatishni ximiyaviy va bakteriologik kurol kabi takiqlash ehtimoldan uzoq. Xuddi shu kabi ko’pgina mamlakatlarning yagona global axborot makonini shakllantirish bo’yicha urinishlarini chegaralab bo’lmaydi.

Tizim ma’muri uchun himoyaning maqbul darajasini ta’minlashning yagona usuli-axborotga ega bo’lishi, chunki hozircha axborot xujumiga eng tez reaktsiya beradigan inson hisoblanadi. Demak, axborotni himoyalash ma’murlarining o’kitishga va professional o’sishiga sarf-harajat axborot xujumlariga qarshi turuvchi eng samarali vosita hisoblanadi.

1.2. Axborot xavfsizligiga tahdid va uning turlari

Axborotni muhofaza qilishning maqsadi va konseptual asoslari. Umuman olganda axborotni muhofaza qilishning maqsadini quyidagicha ifodalash mumkin: – axborotni tarqab ketishi, o‘g‘irlanishi, buzilishi, qalbakilashtirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk obyekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfedensialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda subyektlarning huquqlarini ta’minlash.

Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va komplekslgi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan konsepsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

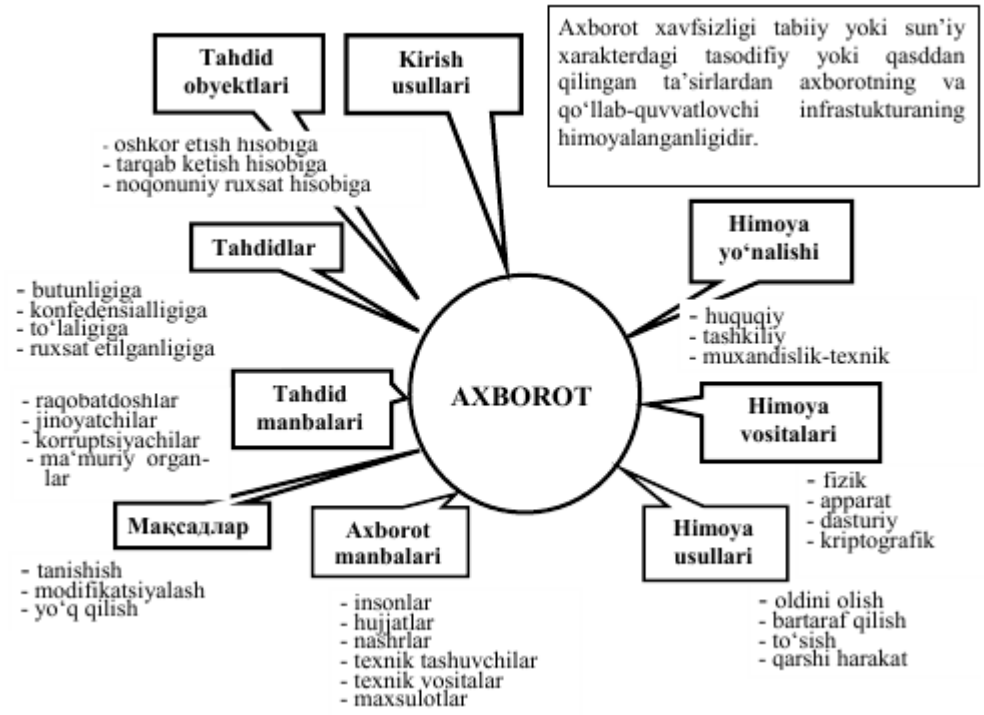
– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– axborotni muhofaza qilish masalalarini hal etishga ixtisoslashtirilgan tashkilotlarning mavjudligi;

– ushbu muammoga oid yetarlicha aniq ifodalangan qarashlar tizimi;

– yetarlicha amaliy tajriba va boshqalar.

Biroq, xorijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendensiyasiga ega bo‘lib bormoqda.



Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi.

Umumiy yo‘nalishga ko‘ra axborot xavfsizligiga tahdidlar quyidagilarga bo‘linadi:

– O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

– mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig‘ish, saqlash va samarali foydalanishni ta’minlashga nisbatan tahdidlar;

– Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining me’yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.

Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchini ko‘rib chiqish maqsadga muvofiq:

1) axborot;
2) texnik va dasturiy vositalar;
3) xizmat ko‘rsatuvchi personal va foydalanuvchilar.

Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi.

Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida hal etilishi zarur.

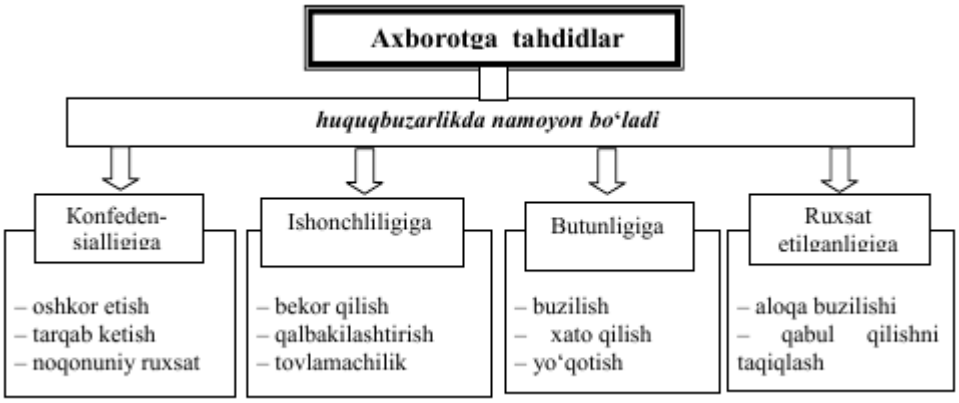
Axborot tarqab ketishiga konfedensial ma’lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi.

Tahdidning uchta ko‘rinishi mavjud.

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgar-tirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgar-tirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqo-nuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisob-lanadi. Axborot butunligi – axborotning buzilmagan holatda mavjud-ligidir.

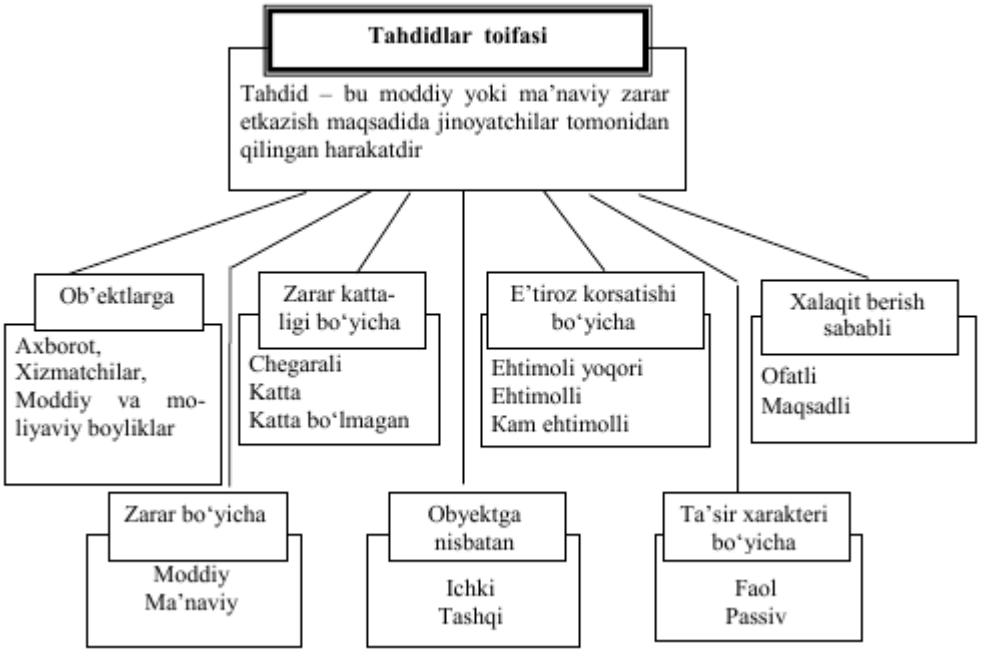
3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik – axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.



Axborot xavfsizligiga tahdidlarning toifalanishi. Axborot xavfsizligiga tahdidlar darajasiga kora quyidagicha toifalanishi mumkin:

a) shaxs uchun:

– axborotlarni qidirish, olish, uzatish, ishlab chiqish va tarqatish bo‘yicha fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini buzilishi;
– fuqarolarni shaxsiy hayot daxlsizligi huquqidan mahrum qilish;
– g‘ayriixtiyoriy zararli axborotlardan fuqarolarning o‘z sog‘liqlarini himoya qilish huquqlari buzilishi;
– intellektul mulk obyektlariga tahdid.
b) jamiyat uchun:
– axborotlashtirilgan jamiyatni qurishga to‘siqlar;
– jamiyatning ma’naviy yangilanish, uning ma’naviy boyliklarini saqlash, fidoyilik va xolislik, mamlakatning ko‘p asrlik ma’naviy an’analarini rivojlantirish, milliy, madaniy merosni targ‘ib qilish, axloq me’yorlari huquqlaridan mahrum qilish;
– zamonaviy telekommunikatsiya texnologiyalarini taraqqiy etishi, mamlakat ilmiy va ishlab chiqarish potensialini rivojlantirish va saqlab qolishga qarshilik qiluvchi muhitni yaratish.



v) davlat uchun:
– shaxs va jamiyat manfaatlari himoyasiga qarshi harakatlar;
– huquqiy davlat qurishga qarshilik;
– davlat boshqaruv organlari ustidan jamoat nazorati institutlarini shakllantirishga qarshi harakatlar;
– shaxs, jamiyat va davlat manfaatlarini ta’minlovchi davlat boshqaruv organlari tomonidan qarorlarni tayyorlash, qabul qilish va tatbiq etish tizimini shakllantirishga qarshilik;
– davlat axborot tizimlari va davlat axborot resurslari himoyasiga to‘siqlar;
– mamlakat yagona axborot muhiti himoyasiga qarshi harakatlar.
Axborot himoyasiga metodologik yondashuv – bu konfedensial axborotlarni saqlash vazifasini turli bosqichlarda yechish bo‘yicha asos bo‘luvchi g‘oyalar, muhim tavsiyalardir. Ular axborotni me’yoriy himoya qilish bazalarini yaratishda inobatga olinadi. Shuningdek, qonun va qonunosti aktlarini qabul

qilishda me’yor sifatida tatbiq qilinadi hamda ularni bajarish majburiy xarakterga ega bo‘ladi.
Axborotni muhofaza qilish tamoyillarini uchta guruhga bo‘lish mumkin: huquqiy, tashkiliy hamda texnik razvedkadan himoyalanishda va hisoblash texnikasi vositalarida axborotga ishlov berishda axborotni muhofaza qilishdan foydalanish. Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko‘rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo‘lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:
1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat’iy belgilovchi qonuniy aktlardan foydalanish.
2. Ma’naviy-etik. Obyektda qat’iy belgilangan o‘zini tutish qoidalarining buzilishi ko‘pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo‘llab quvvatlash.
3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to‘siqlar yaratish.
4. Ma’muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.
5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.
6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.
7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo‘llash.
Fizik, apparatli, dasturli va hujjatli vositalarni o‘z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda himoya obyekti sifatida qaraladi.
Odatda, so‘nggi vaqtlarda axborotdan foydalanish, saqlash, uzatish va qayta ishlashda turli ko‘rinishdagi axborot tizimlarida amalga oshirilmoqda.
Axborot tizimi – bu odatda matnli yoki grafik axborotlarni yig‘ish, saqlash, qidirish va qayta ishlashga mo‘ljallangan amaliy dasturiy, ba’zan esa apparat-dasturiy nimtizimdir.
Ma’lumotlarning axborot tizimida mavjud bo‘lishining moddiy asosi bu elektron va elektron-mexanik qurilmalar, shuningdek axborot tashuvchilardir.
Axborot tashuvchilari sifatida qog‘oz, magnit va optik tashuvchilar, elektron sxemalar foydalanilishi mumkin.
Demak, qurilma va nimtizimlarni hamda axborot tashuvchilarini himoya qilish zarur.
Turli axborot tizimlarida foydalanuvchilar xizmat ko‘rsatuvchi personal hisoblanib, axborot manbai va tashuvchilari bo‘lishi mumkin.

Viruslar va ularning kelib chiqishi

Ildam qadamlar bilan rivojlanayotgan kompyuter axborot texnologiyalari xayotimizda sezilarli o’zgarishlarga sabab bo’lmoqda. «Axborot» tushunchasi sotib olish, sotish, biror narsaga almashish va hk. Mumkin bo’lgan maxsus tovarni belgilashda tez - tez ishlatila boshlandi. Bunda axborotning narxi ko’pincha u joylashgan kompyuter tizimi narxidan yuz va ming marta yuqori bo’ladi. Demak,

axborotni ruxsatsiz foydalanishdan, atayin o’zgartirishdan, yo’q qilishdan va boshqa jinoiy harakatlardan himoyalash zaruriyatining paydo bo’lishi tabiiydir.

Axborotni himoyalash muammosi kompyuter tizimlari va tarmoqlari sohasida faoliyat ko’satuvchi mutaxassislar hamda zamonaviy kompyuter vositalaridan foydalanuvchilar e`tiborini jalb etmokda. Ayni paytda kompyuter fani va amaliyotining ushbu dolzarb muammosi Davlat tilida yozilgan ilmiy-texnik va o’kuv adabiyotlarda etarlicha o’z aksini topmagan.

Kompyuter viruslari bugungi kunda ko’pchilikning eng dolzarb muammosidir. Bu hammani tashvishga solmoqda. hozirgi kunda kompyuter foydalanuvchilari oldidagi katta muammo virusdan himoyalanishdir. Kompyuter viruslari ishi natijasida eng muhim va kerakli axborotlar ba`zan yo’qolib ketmokda. Shuning uchun ham axborotlarni kafolatli saqlab olish uchun maxsus mutaxassislar himoya sistemalarini yaratishga jalb qilingan. Lekin shunday bo’lsada, bu sistemalar butunlay kafolat bera olmaydi. Sababi viruslarning yangi va noma`lum turlarini hisobga olib bo’lmaydi. Shuning uchun kompyuterlarni virusdan saqlab turuvchi programmalar (antivirus) bazasini yangilab turish maqsadga muvofiq.

Kompyuter viruslari - bu maxsus yozilgan kichik programmalar bo’lib, u faylga kirib o’zini xotiraga yozib qo’yadi va ularni zararlantirishga harakat qiladi. Virus faylga yozilib yoki alohida shaklda tizimga kirib asta-sekin ta`sir qiladi va kompyuterda g’alati o’zgarishlarni yuzaga keltiradi. Ekranda noaniq belgi yoki axborotlar hosil bo’ladi, natijada kompyuterning ish qobilyati sezilarli darajada pasayadi, fayldagi ba`zi axborotlar o’zgaradi, diskdagi axborotlar o’chib ketishi mumkin. Shuni qayd etish lozimki, ayrim viruslar avvaliga sekin ko’payadi va ma`lum vaqtdan so’ng esa katta zarar ko’rsatadi. Masalan, ba`zi viruslar hattoki qattiq magnit diskni formatlab undagi barcha ma`lumotlarni o’chiradi. Xullas, hamma viruslarning ta`siri turlicha bo’ladi va ba`zan birdan kompyuterda o’zgarishlar sodir bo’lishi ham ehtimoldan xoli emas! Virus programmalari o’zini sezdirmasligi, ko’rinmasliklari uchun ularni yaratuvchilar barcha choralarni qo’llaydilar. Viruslar bilan ko’proq bajariluvchi dastur fayllari zararlanishi va virus tashuvchilari bo’lib qoladi.

Virusning birinchi ko’rinishi, ikki dasturchining bir - biriga hazil tariqasida uzatgan kichik dasturchalari hisoblanadi. Ular bu dasturlar rivojlanib “EPIDEMIYa” darajasiga etishini o’ylashmagan. Avvaliga viruslar foydalanuvchilarga ularning savodxonligini sinashdek tuyilgandi, yani virusni qaysi yo’l bilan o’chirish ularning bilim darajasini belgilab berardi. Lekin keyinchalik ularga qarshi kurashish tobora muammo bo’lib qolmoqda. Bu degani kompyuter viruslarining “REZONANAS” davri keldi. Ko’pgina viruslar ular taralgan joy nomlari yoki vazifasiga ko’ra ataladi.

Troyanlar (Trojan Horses) – qadimgi yunonlarning Troyaga yurishlari davrida qo’llagan hiylasi, ya`ni troyaliklarni otga ishqiboz ekanligidan foydalanib, ularga katta yog’och ot sovg’a qilishlari va bu otning troyaliklar mag’lubiyatiga olib kelishi voqeasidan olingan. Hozirda troya oti iborasi «xosiyatsiz sovg’a» degan ma`noni bildiradi. Kompyuter va internet dunyosida troyanlar «xosiyatsiz programma» iborasiga o’xshatish tariqasida qo’llashadi.

Chuvalchang (Worms) - viruslar o'z nomiga mos ravishda juda tez o'z-o'zidan ko'payadigan viruslardir. Ushbu g'oya asosida Robert Tappan Morris "Morris chuvalchangi" (Morris Worm)ni yaratdi. Bu virus internetda tarqalgan eng birinchi viruslardan bo'lib, u minglab dollar "zarar" keltirishga muvaffaq bo'lgan.

Makro (Macro) - viruslar bu o'zlarining tarqalishi uchun boshqa bir programmaning makro dasturlash tilidan (Visual Basic) foydalanadigan viruslardir. Ular odatda Microsoft Word, Power Point yoki Excel xujjatlarini zararlaydi.

Spam (Spam) – bu, eski marketing usullaridan biridir. Geri Tyurk ilk marta xaridorlarga ommaviy elektron xabar jo'natgan shaxs hisoblanadi. qizig'i shundaki, o'shanda u ilk spamni yaratganligini hatto bilmagan ham ekan.

Vaqt bombasi (Time or Logic Bombs) virusi - Kulgi kunida (1 aprel) yoki yangi yil bayramida kompyuteringizdagi ma`lumotlarni o'chirib tashlab sizga "sovga" taqdim etishi mumkin. "Chernobil" AESning portlash kuniga atalgan 1999 yil 26 apreldagi "Chernobil" virusi butun dunyoni larzaga soldi.

Viruslar asosan quyidagi yo'llar orqali kompyuterga yuqadi.

- Zararlangan axborot tashuvchilar (Floppy, CD, DVD, Flash, SSD disk)
- Litcenziyalanmagan tizimni o'rnatganda
- Internet tarmog'ida ishlaganda

Kompyuter virus bilan kasallanganda (bu kasallik bo'lganligi taxmin qilinadi) quyidagi operatciyalarni bajarish zarur:

- Kompyuterni o'chirish kerak, chunki virus o'z buzish funktciyalarini davom etmasligi sabab;
- Kompyuterni "etalon" (tizimli) disk (unda operatcion tizim bajarilish fayllari va detektor - dasturlar yozilgan) orqali yuklanishini amalga oshirish zarur va virusni topish va yo'qotish uchun antivirus dasturlarini ishlatish kerak. Bunda tizimli disketa yozishdan himoyalangan bo'lishi kerak.

So'ngra ketma - ket vinchesterning barcha mantiqiy disklarini zarardan xalos etish kerak. Agar mantiqiy diskdagi ba`zi fayllarni tiklashni iloji bo'lmasa va ular o'chirilmasa, unda buzilmagan fayllarni boshqa mantiqiy diskka nusxalab bu diskni qayta formatlash zarur. So'ngra bu mantiqiy diskdagi barcha fayllarni teskari nusxalash va arxiv nusxalash yordamida tiklash mumkin.

1.3 Axborot-kommunikatsion tizimlar va tarmoqlarda tahdidlar va zaifliklar

Tarmoq texnologiyalari rivojining boshlangich boskichida viruslar va kompyuter xujumlarining boshqa turlarita'siridagi zarar kam edi, chunki u davrda dunyo iktisodining axborot texnologiyalariga bog'liqligi katta emas edi. Hozirda, xujumlar sonining doimo o'sishi hamda biznes-ning axborotdan foydalanish va almashishning elektron vositalariga bog'liqligi sharoitida mashina vaqtining yo'qolishiga olib keluvchi hatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi. Misol tariqasida keltirish mumkinki, faqat 2003 yilning birinchi choragida dunyo miqyosidagi yo'qotishlar 2002 yildagi barcha yo'qotishlar yig'indisining 50%ini tashkil etgan, yoki bo'lmasa 2006 yilning o'zida Rossiya Federeatsiyasida 14 mingdan ortiq kompyuter jinoyatchiligi holatlari qayd etilgan[29, 30, 32].

Korporativ tarmoqdarda ishlanadigan axborot, ayniqsa, zaif bo'ladi. Hozirda ruxsatsiz foydalanishga yoki axborotni modifikatsiyalashga, yolg'on axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo'ladi:

- kompyuterda ishlanadigan, uzatiladigan va sakdanadigan axborot hajmining oshishi;
- ma'lumotlar bazasida muhimlik va mahfiylik darajasi turli bo'lgan axborotlarning to'planishi;
- ma'lumotlar bazasida sakdanayotgan axborotdan va hisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi;
- masofadagi ishchi joylar soninig oshishi;
- foydalanuvchilarni boglash uchun Internet global tarmogini va aloqaning turli kanallarini keng ishlatish;
- foydaluvchilar kompyuterlari o'rtasida axborot almashinuvining avtomatlashtirilishi.

Axborot xavfsizligiga taxdid deganda axborotning buzilishi yoki yo'qotilishi xavfiga olib keluvchi himoyalanuvchi ob'ektga qarshi kilingan harakatlar tushuniladi. Oldindan shuni aytish mumkinki, so'z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommertsiya kiymatiga ega bo'lgan kismi xususida ketyapti.

Zamonaviy korporativ tarmokdar va tizimlar duchor bo'ladigan keng tarqalgan taxdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlik-ka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashkarisida (tashki manba) bo'lishi mumkin. Bunday ajratish to'gri, chunki bitta taxdid uchun (masalan, o'girlash) tashki va ichki manba-larga qarshi harakat usullari turlicha bo'ladi. Bo'lishi mumkin bo'lgan taxdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta'minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi.

Tez-tez bo'ladigan va xavfli (zarar o'lchami nuqtai nazaridan) taxdidlarga foydalanuvchilarning, operatorlarning, ma'murlarning va korporativ axborot tizimlariga xizmat ko'rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba'zida bunday xatoliklar (noto'g'ri kiritilgan ma'lumotlar, dasturdagi xatoliklar sabab bo'lgan tizimning to'xtashi yoki bo'zilishi) to'g'ridan to'g'ri zararga olib keladi. Ba'zida ular niyati buzuq odamlar foydalanishi mumkin bo'lgan nozik joylarni paydo bo'lishiga sabab bo'ladi. Global axborot tarmog'ida ishlash ushbu omilning etarlicha dolzarb kiladi. Bunda zarar manbai tashkilotning foydalanuvchi-si ham, tarmoq foydalanuvchisi ham bo'lishi mumkin, oxirgisi ayniqsa xavfli.

Zarar o'lchami bo'yicha ikkinchi o'rinni o'g'irlashlar va soxtalashti-rishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishlash rejim-lari va himoyalash choralari bilan a'lo darajada tanish bo'lgan tashkilot shtatidagi xodimlar aybdor bo'lib chikdilar. Global tarmoklar bilan bog'langan quvvatli axborot kanalining mavjudligida, uning ishlashi usti-dan etarlicha nazorat yo'kdigi bunday faoliyatga qo'shimcha imkon yaratadi.

Xafa bo’lgan xodimlar (hatto sobikdari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon etkazishlari mumkin. Xodim ishdan bo’shaganida uning axborot resurslaridan foydalanish xuquki bekor kilinishi nazoratga olinishi shart.

Hozirda tashki kommunikatsiya orqali ruxsatsiz foydalanishga atayin kilingan urinishlar bo’lishi mumkin bo’lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo’lib tuyulmasa ham, Internetfla ishlash tajribasi ko’rsatadiki, qariyb har bir Internet-server kuniga bir necha marta sukilib kirish urinishlariga duchor bo’lar ekan. Xavf-xatarlar taxlil kilinganida tashkilot korporativ yoki lokal tarmogi kompyuterlarining xujumlarga qarshi turishi yoki bo’lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun etarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AKDI) testlari ko’rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsat-siz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tu-zilmasidan sasofadan foydalanish xollari alohida ko’rilishi lozim.

Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti du-chor bo’ladigan xavf-xatar baholanishi va zarur choralar ko’rilishi zarur. Ravshanki, himoyaga taxdidni nazoratlash va zarur choralarni ko’rish uchun tashkilotning sarf-harajati tashkilotda aktivlar va resurslarni himoyalash bo’yicha hech qanday choralar ko’rilmaganida kutiladigan yo’qotishlardan oshib ketmasligi shart.

Umuman olganda, tashkilotning kompyuter muhiti ikki xil xavf-xatarga duchor bo’ladi:

1. Ma’lumotlarni yo’qotilishi yoki o’zgartirilishi.
2. Servisning to’xtatilishi.

Tahdidlarning manbalarini aniqlash oson emas. Ular niyati buzuq odamlarning bostirib kirishidan to kompyuter viruslarigacha turlanishi mumkin.

Keltirilgan statistik ma’lumotlar tashkilot ma’muriya-tiga va xodimlariga korporativ tarmoq va tizimi xavfsizligiga taxdidlarni samarali kamaytirish uchun xarakatlarni qaerga yo’naltirishlari zarurligini aytib berishi mumkin. Albatta, fizik xav-fsizlik muammolari bilan shug’ullanish va inson xatoliklarining xav-fsizlikka salbiy ta’sirini kamaytirish bo’yicha choralar ko’rilishi zarur. SHu bilan bir katorda korporativ tarmoq va tizimga ham tashqaridan, ham ichkaridan bo’ladigan xujumlarni oldini olish bo’yicha tarmoq xavfsizligi masalasini echishga jiddiy e’tiborni qaratish zarur.

Bugungi kunda ishlab chiqilayotgan ayrim dasturiy vositalar o’zida ham servis xam utilita vazifalarni bajarishi bilan ularning texnologik lug’aviy ma`nosi bir-biriga yaqinlashib qolayapti. Virusga qarshi himoya dasturiy vositalar viruslarni topish va davolashni ta`minlaydi. Virus atamasi bilan turli noma`qul harakatlarni amalga oshirib, boshqa dasturlarga kirib olgan holda ko’payishga qodir bo’lgan dastur tushuniladi.

II BOB. AXBOROTLARNI HIMOYALASHDA CHORA-TADBIRLAR

2.1 Axborot xavfsizligini ta’minlash choralari

Tashkilotlarda himoyalash bilan bog’liq bo’lgan muammolarni echish uchun aksariyat hollarda qisman yondashishlardan foydalanishadi. Bu yonda-shishlar, odatda, avvalo foydalana oluvchi resurslarning joriy darajasi orqali aniqlanadi. Undan tashqari, xavfsizlik ma’murlari ko’pincha o’zlariga tushunarli bo’lgan xavfsizlik xavf-xatarlariga reaktsiya ko’rsatishadi. Aslida xavf-xatarlar juda ko’p bo’lishi mumkin. Korporativ axborot tizimini faqat qat’iy joriy nazorati va xavfsizlikning umu-miy siyosatini ta’minlovchi kompleks yondashish xavfsizlik xavf-xatarlarini anchagina kamaytirishi mumkin.

Oxirgi vaqtda turli kompaniyalar tomonidan qator yondashishlar ish-lab chikildiki, bu yondashishlar nafaqat mavjud zaifliklarni anikdashga, balki o’zgargan eski yoki paydo bo’lgan yangi zaifliklarni anikdashga va ularga moe himoyalash vositalarini qarshi qo’yishga imkon beradi. Xususan, ISS(Internet Security Systems) kompaniyasi tomonidan *xavfsizlikni adaptiv boshkarish modeli* ANS (Adaptive Network Security) ishlab chikildi.

Xavfsizlikka adaptiv yondashish, to’g’ri loyihalangan va yaxshi boshqariluvchi jarayon va vositalar yordamida xavfsizlik xavf-xatarlarini real vakt rejimida nazoratlash, anikdash va ularga reaktsiya ko’rsatishga imkon beradi.

Tarmokning adaptiv xavfeizligi quyidagi asosiy uchta element orqali ta’minlanadi:

- xavf-xatarlarni baholash;
- himoyalanishni taxlillash;
- xujumlarni aniqlash.

Xavf-xatarlarni baxolash. Xavf-xatarlarni (keltiradigan zararning jiddiylik darajasi bo’yicha), tarmoq kiem tizimlarini (jiddiylik darajasi bo’yicha), tahdidlarni (ularning amalga oshirilishi ehtimolligi

bo’yicha) aniqlash va rutbalashdan iborat. Tarmoq konfiguratsiyam muttasil o’zgarishi sababli, xavf-xatarlarni baholash jarayoni ham uzluksiz o’tkazilishi lozim. Korporativ axborot tizimining himoyalash tizimini qurish xavf-xatarlarni baholashdan boshlanishi lozim.

Himoyalaniimi taxlillash - tarmoqning zaif joylarini qidirish. Tarmoq ulanishlardan, uzellardan, xostlardan, ishchi stantsiyalardan, ilo-valardan va ma’lumot bazalaridan tarkib topgan. Bularning barchasi himoyalanishlar samaradorligining hamda no’malum zaifliklarining aniqlanishiga muhtoj. Himoyalanishni tahlillash texnologiyasi tarmokni tadqiqlash, nozik joylarini topish, bu ma’lumotlarni umumlashtirish va ular bo’yicha hisobot berish imkoniyatiga ega. Agar bu texnologiyani amalga oshiruvchi tizim adaptiv komponentga ham ega bo’lsa, anikdangan zaiflik-larni avtomatik tarzda bartaraf etish mumkin. Himoyalanishni taxlillash texnologiyasi tarmoq xavfsizligi siyosatini, uni tashkilot tashqarisidan yoki ichkarisidan buzishga urinishlardan oldin, amalga oshirishga imkon beruvchi ta’sirchan usul hisoblanadi.

Himoyalanishni taxlillash texnologiyasi tomonidan identifikatsiya-lanuvchi muammolarning ba’zilari quyidagilar:

- tizimlardagi "teshiklar" (back door) va troyan oti xilidagi dastur;
- kuchsiz parollar;

- himoyalanmagan tizimdan sukilib kirishga va "xizmat qilishdan voz kechish" xilidagi xujumlarga ta’sirchanlik;

- operatsion tizimlardagi zaruriy yangilanishlarning yo’qligi;

- tarmoqlararo ekranlarning, Web-serverlarning va ma’lumotlar ba-zasining noto’g’ri sozlanishi va h.

Xujumlarni anitslash - korporativ tarmokdagi shubhali xarakatlar-ni baholash jarayoni. Xujumlarni aniqlash operatsion tizim va ilovalar-ni qaydlash jurnallarini yoki real vaqtdagi trafikni taxlillash orqali amalga oshiriladi. Tarmoq uzellari yoki segmentlarida joylashtirilgan xujumlarni aniqlash komponentlari turli xodisalarni, xususan, ma’lum zaifliklardan foydalanuvchi harakatlarni ham baholaydi

Xavfsizlikni adaptiv boiuqarish modeli ANSHUHZ adaptiv komponentы, yangi zaifliklar xususidagi eng oxirgi axborotni taqtsim qilgan holda, himoyalanishni taxlillash jarayonini modifikatsiyalashga javob be-radi. U xujumlarni aniqlash komponentini ham, uni xujumlar xususidagi oxirgi axborot bilan to’ldirish orqali, modifikatsiyalaydi. Adaptiv kom-ponentning misoli sifatida yangi viruslarni aniklash uchun virusga qarshi dasturning ma’lumotlar bazasini yangilash mexanizmini ko’rsatish mumkin.

barcha taxdidlarni nazoratlash va ularga o’z vaqtida samarali reaktsiya ko’rsatish imkonini beradi. Bu esa o’z navbatida, nafakat taxdidlarning amalga oshirilishiga sabab bo’luvchi zaifliklarni bartaraf kilishga, balki zaifliklar paydo bo’lish sharoitlarini tahlillashga imkon beradi.

Tarmoq xavfsizligini adaptiv boshqarish modeli tarmokda suii-ste’mol kilishni kamaytirishga, tarmokdagi xodisalardan foydalanuvchi-lar, ma’murlar va kompaniya rahbariyatining xabardorlik darajasini oshishiga ham imkon beradi. Ta’kidlash lozimki, ushbu model oldin ish-latiluvchi himoyalash mexanizmlaridan (foydalanishni chegaralash, autenti-fikatsiyalash va h.) voz kechmaydi. Ularning funktsionalligini yangi texnologiya evaziga kengaytiradi. O’zlarining axborot xavfsizligini ta’minlash tizimlarini zamonaviy talablarga moe kelishini xoxlovchi tashkilotlar mavjud echimlarni uchta yangi komponent-himoyalanishni taxlillash, xujum-larni aniqlash va xavf-xatarni baholash bilan to’ldirishi lozim.

2.2 ClamAV va antivurus yordamida axborot himoyasini ta’minlash

Clam AntiVirus – bu UNIX uchun ochiq kodli (GPL) antivirus vositasi. U bir nechta utilitalarni tavsiya etadi, buyruqlar satri orqali tekshirish va ko’p masshtabli ko’p tarmoqli xizmatlarni ochib beradi.

Clam AntiVirus Unix operatsion tizimlar, OpenVMS, Microsoft Windows va Apple Mac OS X kabi ko'plab operatsion tizimlarda ishlaydigan antivirus dasturiy paketidir.

GNU Umumiy Davlat Litsenziyasi ostida chiqarilgan va bepul dasturiy ta'minot.

2007 yil 17-avgustda ClamAV loyihasi Snortning taniqli hujumni aniqlash tizimini ishlab chiqaruvchi Sourcefire tomonidan sotib olingan. Kompaniyaning direktori Martin Rausning so'zlariga ko'ra, yaqin kelajakda Snort va ClamAV mahsulotlari birlashtiriladi. Biroq, ClamAV-ning rivojlanishi esa rivojlanishda davom etadi va alohida bepul texnologiyalar sifatida taqdim etiladi.

Clam AntiVirus-ning asosiy maqsadi - xabarlarga biriktirilgan fayllarni tekshirish uchun elektron pochta serverlari bilan integratsiyalash. Ushbu to'plam ko'p miqdordagi ko'p o'lchovli klemd pardasi, clamscan-boshqariladigan brauzer va yangilangan imzo yangilanishini o'z ichiga oladi.

Clam AntiVirus UNIX ochiq manbaiga (GPL) uchun virusga qarshi vositadir. Moslashuvchan, ko'p maqsadli va katta masshtabli xizmatlar majmui, buyruq qatorni brauzer va ma'lumotlar bazalarini avtomatik ravishda yangilash uchun rivojlangan uskunalar, shu jumladan bir nechta dasturiy ta'minotdir. ClamAV birinchi navbatda Windows tarmoqlarida fayl va pochta serverlarida ishlatilganligi sababli Windows OT viruslari va zararli dasturlarni aniqlash uchun mo'ljallangan.

ClamAv antivirusni o`rnatish va sozlash qadamlari

O’rnatish

Rasmiy omborlarda (https://www.archlinux.org/packages/?name=clamav) mavjud bo'lgan clamav paketini yuklab olib o’rnating.

Xizmatlarni yoqish

Xizmatlarni boshqarish haqida ma'lumot olish uchun Systemd: Unitlardan foydalanish bo'limiga o’ting.

Xizmatlar nomi: clamd.service.

Ma'lumotlar bazalarini yangilash

Antivirus ma'lumotlar bazalari quyidagi buyruq yordamida yangilanadi:

freshclam

Ma'lumotlar bazasi fayllari quyidagilarda saqlanadi:

/var/lib/clamav/daily.cvd

/var/lib/clamav/main.cvd

Testdan o`tkazish

ClamAV anti-virus bazasi va to'g'ri tashkil ishonch hosil qilish uchun, EICAR matn fayli ko’rinishida bo’ladi.

$ Wget -O- http://www.eicar.org/download/eicar.com.txt | clamscan -

Internet saytlarini tekshiruv natijalarida bir qator bo'lishi kerak:

Eicar-Test-Signature FOUND

Aks holda, Muammo bartaraf qilish bo'limiga qarang yoki forumdan foydalaning.

Skanerlash

Clamscan buyrug'i shaxsiy fayllarni, kataloglarni yoki butun tizimni tekshirish uchun ishlatiladi:

$ clamscan myfile

$ clamscan --recursive=yes --infected /home # ili ispolzuyte parametrы -r -i

$ clamscan --recursive=yes --infected --exclude-dir='^/sys|^/proc|^/dev|^/lib|^/bin|^/sbin' /

Virusli fayllarni avtomatik ravishda o'chirish uchun, --remove-ni qo'shing yoki siz ularni karantinaya o'tkazish uchun --move = / katalogidan foydalanishingiz mumkin.

Agar siz -l / fayl yo'li - parametrini ishlatsangiz, skanerlash natijalari belgilangan kunlik faylga (log) yoziladi.

Xatoliklarni echish

Error: Clamd was NOT notified

Agar siz yangi yilni boshlaganingizda xabarni olsangiz:

WARNING: Clamd was NOT notified: Cannot connect to clamd through /var/lib/clamav/clamd.sock connect(): No such file or directory

Jarayon uchun sock fayl yarating:

touch /var/lib/clamav/clamd.sock

chown clamav:clamav /var/lib/clamav/clamd.sock

Keyinchalik, /etc/clamav/clamd.conf faylida drenajdan ogohlantiring:

LocalSocket /var/lib/clamav/clamd.sock

Fayllarni saqlang va xizmatni qayta yuklang.

Error: No supported database files found

Xizmatni boshlaganingizda quyidagi xabar olsangiz:

LibClamAV Error: cli_loaddb(): No supported database files found in /var/lib/clamav ERROR: Not supported data format

Ma'lumotlar bazasini **root** foydalanuvchi sifatida yarating ot:

freshclam -v

Error: Can't create temporary directory

UID va GUID raqamlarini o'z ichiga olgan quyidagi xatolarni qabul qilsangiz:

ERROR: can't create temporary directory

Hint: The database directory must be writable for UID XXX or GID YYY

To'g'ri ruxsatnomalarni katalogga qo'ying:

chown UID:GID /var/lib/clamav & chmod 755 /var/lib/clamav

ClamAV texnologiyasi asosida dastur yaratish

Yuqoridagilar orqali kompyuter foydalanuvchilarida uchrab turadigan muammolarni engillashtirish va ularni bartaraf etuvchi echim yo'llarini mukammal amalga oshirish imkonini beruvchi ClamAV funksiya va imkoniyatlariga yaqin dasturiy mahsulotni yaratmoqni istadik. Bu o'rinda qanday vazifalarni bajarish va nimalarga e`tibor berish kerakli ahamiyatli bo'lib, qaysi vositalarni qo'llash kerakligini bilish zarur. Algoritmning optimal holatga keltirish va dizayn qismini ommabop, tushunarli hamda ranglar uyg'unligini ta`minlash dolzarbligini unutmaslik kerak. Chunki, dasturiy mahsulotning umrini uning vazifasi bilan

birgalikda interfeysi ham ta`minlaydi. Operatcion tizimda jarayonlarini bajarish uchun MS DOS buyruqlari hamda Windows operaratcion tizimining ayrim funktciyalarni bajarilishini ta`minlovchi Winapi funktciyalari keng qo'llaniladi.

Yaratilishi lozim bo'lgan dasturiy mahsulotni ClamAV dasrutiy mahsulot kabi avvalo quyidagilarni amalga oshira olishi kerak:

- ✓ Interfeysi tushunali va qulay
- ✓ Fayl va katalog ustida tahrirlash
- ✓ Reest tizimigi tahrirlash
- ✓ WinApi funktciyalarini ishlatish imkoni
- ✓ Tizim funktciyalarini bajara olish
- ✓ Dasturlarni yuklash va hk

Dasturiy mahsulotning interfeysi va barcha funktciyalarni bajara olishini hisobga olib, ***Embarcadero Delphi XE2*** ob`ektga yo'naltirilgan dasturlash tilida yaratish tanlab olindi. Bu dasturiy mahsulot yaratishda va uning interfeysi uchun kerak bo'ladigan barcha ob`eklar to'plamiga egaligi bilan ajralib turadi. Bugungi kunda Delphi XE2 dasturiy vositasi Windows operatcion tizimning 32 va 64 razryadli versiyalari uchun qo'llaniladigan variantlarini ishlab chiqish va boshqa keng imkoniyatlarni amalga oshirish imkonini beradi.

Dasturlash tili translyatori deb - dasturlash tilidan yozilgan dastur matnini mashina kodiga tarjima qilishni amalga oshiruvchi dasturga aytiladi.

Dasturlashning kirish tili, translyator, mashina tili, standart dasturlar kutubxonasi, translyatciya qilingan dasturlarni sozlash va bir butunlikka jamlash vositalarini o'z ichiga olgan vositalar majmui dasturlash tizimi deb ataladi.

Dasturlash tizimida, translyator dasturlashning kirish tilida yozilgan dasturni aniq bir EHMning mashina buyrug'i tiliga tarjima qiladi.

Kirish tilidan tarjima qilish usuliga bog'liq holda translyatorlar kompilyator va interpretatorlarga bo'linadi.

Texnik xizmat ko'rsatish dasturlari deganda kompyuter ishi jarayoni yoki umuman hisoblash tizimida diagnostika va xatolarni topish uchun dasturiy apparat vositalarining majmuasi tushuniladi. Ular quyidagilarni o'z ichiga oladi:

EHM va uning ayrim qismlari ishining tug'riligi diagnostik va test nazorati vositalari axborot tizimi, hisoblash muxitini diagnostika va nazorat qilishning maxsus dasturlari.

Dasturda quyidagi asosiy modullardan foydalanildi:

- o **Registry** - reestr tizimiga bog'lanish, qurulmalarni boshqarish, tizimni sozlash;
- o **Windows, SysUtils, Classes, Controls, Forms** – dastur interfeysi va standart ob`ektlarni boshqarish uchun;
- o **Shellapi** – tizimning API funktciyalarini qo'llash;
- o **Toolwin** – tizim qurulmalarini tekshirish;

Yaratiladigan dasturiy mahsulotni qo'llashda kerak bo'ladigan qo'shimcha komponentlar to'plami qo'shish shakli ham mavjud.

Dasturning bajarilish jarayonida WinApi funktciyalari imkoniyatini qo'lay olinmaydigan bo'lsa, operatcion tizimning qo'shimcha funktciyalarini amalga oshirish uchun MS DOS buyruqlarni qo'llash mumkin. Buning uchun MS DOS buyruqlaridan tashkil topgan fayl yaratilib *.cmd yoki *.bat kengaytma bilan

saqlanadi. Saqlangan fayl bajariluvchi fayl sifatida ishlatilib so’ng o’chirib yuboriladi yoki o’chirish kodi ham fayl tarkibiga qo’shib qo’yiladi.

Tizim sozlanmasi uchun reest tizimi tarkibini o’rganish alohida ahamiyatga ega. Sababi o’zgartirilgan va yaratilgan kalit yoki bo’lim tizimning qaysidir qismini nosoz ishlashiga olib kelishi mumkin. Reestr tizimi orqali asosan “HKEY_Current_User” (joriy foydalanuvchi) va “HKEY_Local_Machine” (joriy ishchi mashina) bo’limlarida parametr sozlashlari amalga oshiriladi.

Internetning bloklanadigan sayt sozlanmalari “ \WINDOWS\ system32\ drivers\ etc” tizim papkasidagi fayllar tarkibiga o’zgartirish kiritish orqali amalga oshiriladi. Bunda dastur fayllar yaratish va ularni tahrirlash imkonini amalga oshirivchi funktciyalar to’plamiga ega bo’lishi va ularni o’z o’rnida qo’llash talab etiladi.

2.3 Tarmoq xavfsizligini ta’minlash va samarali himoya yechimlari

Aynan tarmoqdan foydalangan holda tezkor ma’lumot almashish vaqtdan yutish imkonini beradi. Xususan, yurtimizda Elektron hukumat tizimi shakllantirilishi va uning zamirida davlat boshqaruv organlari hamda aholi o‘rtasidagi o‘zaro aloqaning mustahkamlanishini tashkil etish tarmoqdan foydalangan holda amalga oshadi. Tarmoqdan samarali foydalanish demokratik axborotlashgan jamiyatni shakllantirishni ta’minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha tezkor natijaga ega bo‘linadi.

Biroq tarmoqqa noqonuniy kirish, axborotlardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Ish faoliyatini tarmoq bilan bog‘lagan korxona, tashkilotlar hamda davlat idoralari ma’lumot almashish uchun tarmoqqa bog‘lanishidan oldin tarmoq xavfsizligiga jiddiy e’tibor qara-tishi kerak. Tarmoq xavfsizligi uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotni ishonchli tizimli tarzda ta’minlash maqsadida turli vositalar va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirish orqali amalga oshiriladi. Tarmoq xavsizligini ta’minlash maqsadida qo‘llanilgan vosita xavf-xatarni tezda aniqlashi va unga nisbatan qarshi chora ko‘rishi kerak. Tarmoq xavfsizligiga tahdidlarning ko‘p turlari bor, biroq ular bir necha toifalarga bo‘linadi:

- axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (Eavesdropping);
- xizmat ko‘rsatishdan voz kechish; (Denial-of-service)
- portlarni tekshirish (Port scanning).

Axborotni uzatish jarayonida, eshitish va o‘zgartirish hujumi bilan telefon aloqa liniyalari, internet orqali tezkor xabar almashish, videokonferensiya va faks jo‘natmalari orqali amalga oshiriladigan axborot almashinuvida foydalanuvchilarga sezdirmagan holatda axborotlarni tinglash, o‘zgartirish hamda to‘sib qo‘yish mumkin. Bir qancha tarmoqni tahlillovchi protokollar orqali bu hujumni amalga oshirish mumkin. Hujumni amalga oshiruvchi dasturiy ta’minotlar orqali CODEC (video yoki ovozli analog signalni raqamli signalga aylantirib berish va aksincha) standartidagi raqamli tovushni osonlik bilan yuqori sifatli, ammo katta hajmni egallaydigan ovozli fayllar (WAV)ga aylantirib beradi. Odatda bu hujumning amalga oshirilish jarayoni foydalanuvchiga umuman sezilmaydi. Tizim ortiqcha zo‘riqishlarsiz va shovqinsiz belgilangan amallarni bajaraveradi. Axborotning o‘g‘irlanishi haqida mutlaqo shubha tug‘ilmaydi. Faqatgina oldindan ushbu tahdid haqida ma’lumotga ega bo‘lgan va yuborilayotgan axborotning o‘z qiymatini saqlab qolishini xohlovchilar maxsus tarmoq xafvsizlik choralarini qo‘llash natijasida himoyalangan tarmoq orqali ma’lumot almashish imkoniyatiga ega bo‘ladilar. Tarmoq orqali ma’lumot almashish mobaynida yuborilayotgan axborotni eshitish va o‘zgartirishga qarshi bir necha samarali natija beruvchi texnologiyalar mavjud:

- IPSec (Internet protocol security) protokoli;
- VPN (Virtual Private Network) virtual xususiy tarmoq;
- IDS (Intrusion Detection System) ruxsatsiz kirishlarni aniqlash tizimi.

Ipsec (Internet protocol security) bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda tarmoq orqali xavfsiz ma’lumot almashish imkonini beradi. Bu maxsus standart orqali tarmoqdagi kompyuterlarning o‘zaro aloqasida dastur va ma’lumotlar hamda qurilmaviy vositalar bir-biriga mos kelishini ta’minlaydi. Ipsec protokoli tarmoq orqali uzatilayotgan axborotning sirliligini, ya’ni faqatgina yubo-ruvchi va qabul qiluvchiga tushunarli bo‘lishini, axborotning sofligini hamda paketlarni autentifikatsiyalashni amalga oshiradi. Zamonaviy axborot texnologiyalarni qo‘llash har bir tashkilotning rivojlanishi uchun zaruriy vosita bo‘lib qoldi, Ipsec protokoli esa aynan quyidagilar uchun samarali himoyani ta’minlaydi:

- bosh ofis va filiallarni global tarmoq bilan bog‘laganda;
- uzoq masofadan turib, korxonani internet orqali boshqarishda;
- homiylar bilan bog‘langan tarmoqni himoyalashda;
- elektron tijoratning xavfsizlik darajasini yuksaltirishda.

VPN (Virtual Private Network) virtual xususiy tarmoq sifatida ta’riflanadi. Bu texnologiya foydalanuvchilar o‘rtasida barcha ma’lumotlarni almashish boshqa tarmoq doirasida ichki tarmoqni shakllantirishga asoslangan, ishonchli himoyani ta’minlashga qaratilgan. VPN uchun tarmoq asosi sifatida Internetdan foydalaniladi.

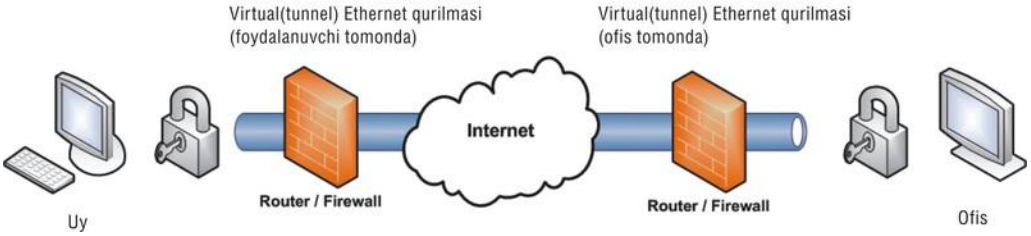
VPN texnologiyasining afzalligi. Lokal tarmoqlarni umumiy VPN tarmog‘iga birlashtirish orqali kam xarajatli va yuqori darajali himoyalangan tunelni qurish mumkin. Bunday tarmoqni yaratish uchun sizga har bir tarmoq qismining bitta kompyuteriga filiallar o‘rtasida ma’lumot almashishiga xizmat qiluvchi maxsus VPN shlyuz o‘rnatish kerak. Har bir bo‘limda axborot almashishi oddiy usulda amalga oshiriladi. Agar VPN tarmog‘ining boshqa qismiga ma’lumot jo‘natish kerak bo‘lsa, bu holda barcha ma’lumotlar shlyuzga jo‘natiladi. O‘z navbatida, shlyuz ma’lumotlarni qayta ishlashni amalga oshiradi, ishonchli algoritm asosida shifrlaydi va Internet tarmog‘i orqali boshqa filialdagi shlyuzga jo‘natadi. Belgilangan nuqtada ma’lumotlar qayta deshifrlanadi va oxirgi kompyuterga oddiy usulda uzatiladi. Bularning barchasi foydalanuvchi uchun umuman sezilmas darajada amalga oshadi hamda lokal tarmoqda ishlashdan hech qanday farq qilmaydi. Eavesdropping hujumidan foydalanib, tinglangan axborot tushunarsiz bo‘ladi.

Bundan tashqari, VPN alohida kompyuterni tashkilotning lokal tarmog‘iga qo‘shishning ajoyib usuli hisoblanadi. Tasavvur qilamiz, xizmat safariga noutbukingiz bilan chiqqansiz, o‘z tarmog‘ingizga ulanish yoki u yerdan biror-bir ma’lumotni olish zaruriyati paydo bo‘ldi. Maxsus dastur yordamida VPN shlyuz bilan bog‘lanishingiz mumkin va ofisda joylashgan har bir ishchi kabi faoliyat olib borishigiz mumkin. Bu nafaqat qulay, balki arzondir.

VPN ishlash tamoyili. VPN tarmog‘ini tashkil etish uchun yangi qurilmalar va dasturiy ta’minotdan tashqari ikkita asosiy qismga ham ega bo‘lish lozim: ma’lumot uzatish protokoli va uning himoyasi bo‘yicha vositalar.

Ruxsatsiz kirishni aniqlash tizimi (IDS) yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi. Ruxsatsiz kirishlarni aniqlash tizimlari deyarli chorak asrlik tarixga ega. Ruxsatsiz kirishlarni

aniqlash tizimlarining ilk modellari va prototiplari kompyuter tizimlarining audit ma’lumotlarini tahlillashdan foydalangan. Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.



IDS tizimlari arxitekturasi tarkibiga quyidagilar kiradi:

- himoyalangan tizimlar xavfsizligi bilan bog‘liq holatlarni yig‘ib tahlillovchi sensor qism tizimi;
- sensorlar ma’lumotlariga ko‘ra shubhali harakatlar va hujumlarni aniqlashga mo‘ljallangan tahlillovchi qism tizimi;
- tahlil natijalari va dastlabki holatlar haqidagi ma’lumotlarni yig‘ishni ta’minlaydigan omborxona;
- IDS tizimini konfiguratsiyalashga imkon beruvchi, IDS va himoyalangan tizim holatini kuzatuvchi, tahlil qism tizimlari aniqlagan mojarolarni kuzatuvchi boshqaruv konsoli.

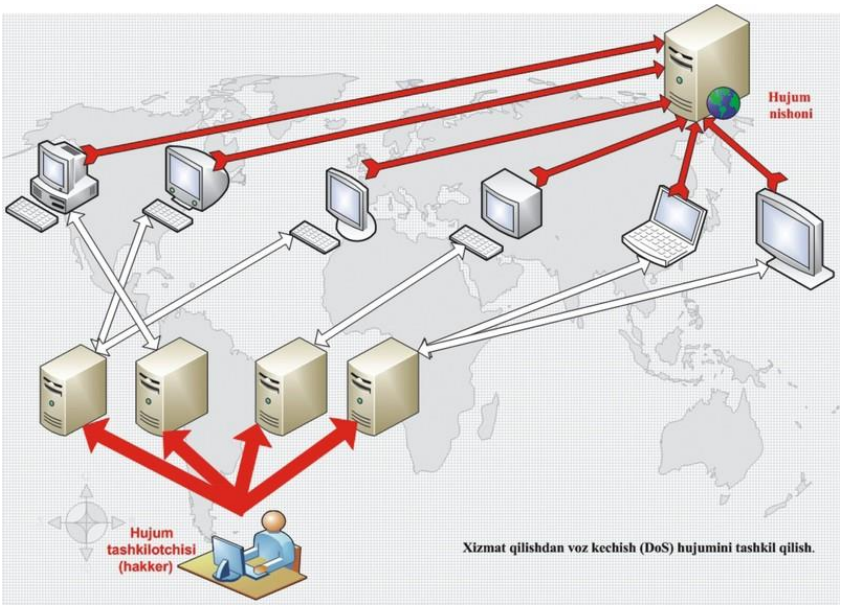
Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (NIDS) ishlash tamoyili quyidagicha:

1. tarmoqqa kirish huquqiga ega bo‘lgan trafiklarni tekshiradi;
2. zararli va ruxsatga ega bo‘lmagan paketlarga cheklov qo‘yadi.

Sanab o‘tilgan xavfsizlik bosqichlarini qo‘llagan holda Eavesdropping tahdidiga qarshi samarali tarzda himoyalanish mumkin.

DOS (Denial-of-service) tarmoq hujumning bu turi xizmat qilishdan voz kechish hujumi deb nomlanadi. Bunda hujum qiluvchi legal foydalanuvchilarning tizim yoki xizmatdan foydalanishiga to‘sqinlik qilishga urinadi. Tez-tez bu hujumlar infratuzilma resurslarini xizmatga ruxsat so‘rovlari bilan to‘lib toshishi orqali amalga oshiriladi. Bunday hujumlar alohida xostga yo‘naltirilgani kabi butun tarmoqqa ham yo‘naltirilishi mumkin. Hujumni amalga oshirishdan oldin obyekt to‘liq o‘rganilib chiqiladi, ya’ni tarmoq hujumlariga qarshi qo‘llanilgan himoya vositalarining zaifligi yoki kamchliklari, qanday operatsion tizim o‘rnatilgan va obyekt ish faoliyatining eng yuqori bo‘lgan vaqti. Quyidagilarni aniqlab va tekshirish natijalariga asoslanib, maxsus dastur yoziladi. Keyingi bosqichda esa yaratilgan dastur katta mavqega ega bo‘lgan serverlarga yuboriladi. Serverlar o‘z bazasidagi ro‘yxatdan o‘tgan foydalanuvchilarga yuboradi. Dasturni qabul qilgan foydalanuvchi ishonchli server tomonidan yuborilganligini bilib yoki bilmay dasturni o‘rnatadi. Aynan shu holat minglab hattoki, millionlab kompyuterlarda sodir bo‘lishi mumkin. Dastur belgilangan vaqtda barcha kompyuterlarda faollashadi va to‘xtovsiz ravishda hujum qilinishi mo‘ljallangan obyektning

serveriga so‘rovlar yuboradi. Server tinimsiz kelayotgan so‘rovlarga javob berish bilan ovora bo‘lib, asosiy ish faoliyatini yurgiza olmaydi. Server xizmat qilishdan voz kechib qoladi.



Xizmat qilishdan voz kechish hujumidan himoyalanishning eng samarali yo‘llari quyidagilar:

- tarmoqlararo ekranlar texnologiyasi (Firewall);
- IPsec protokoli.

Tarmoqlararo ekran ichki va tashqi perimetrlarning birinchi himoya qurilmasi hisoblanadi. Tarmoqlararo ekran axborot-kommunikatsiya texnologiya (AKT)larida kiruvchi va chiquvchi ma’lumotlarni boshqaradi va ma’lumotlarni filtrlash orqali AKT himoyasini ta’minlaydi, belgilangan mezonlar asosida axborot tekshiruvini amalga oshirib, paketlarning tizimga kirishiga qaror qabul qiladi. Tarmoqlararo ekran tarmoqdan o‘tuvchi barcha paketlarni ko‘radi va ikkala (kirish, chiqish) yo‘nalishi bo‘yicha paketlarni belgilangan qoidalar asosida tekshirib, ularga ruxsat berish yoki bermaslikni hal qiladi. Shuningdek, tarmoqlararo ekran ikki tarmoq orasidagi himoyani amalga oshiradi, ya’ni himoyalanayotgan tarmoqni ochiq tashqi tarmoqdan himoyalaydi. Himoya vositasining quyida sanab o‘tilgan qulayliklari, ayniqsa, paketlarni filtrlash funksiyasi DOS hujumiga qarshi himoyalanishning samarali vositasidir. Paket filtrlari quyidagilarni nazorat qiladi:

- fizik interfeys, paket qayerdan keladi;
- manbaning IP-manzili;
- qabul qiluvchining IP-manzili;
- manba va qabul qiluvchi transport portlari.

Tarmoqlararo ekran ba’zi bir kamchiliklari tufayli Dos hujumidan to‘laqonli himoyani ta’minlab bera olmaydi:

- loyihalashdagi xatoliklar yoki kamchiliklar — tarmoqlararo ekranlarning har xil texnologiyalari himoyalana-yotgan tarmoqqa bo‘ladigan barcha suqilib kirish yo‘llarini qamrab olmaydi;
- amalga oshirish kamchiliklari — har bir tarmoqlararo ekran murakkab dasturiy (dasturiy-apparat) majmua ko‘rinishida ekan, u xatoliklarga ega. Bundan tashqari, dasturiy amalga oshirish sifatini aniqlash imkonini beradigan va tarmoqlararo

ekranda barcha spetsifikatsiyalangan xususiyatlar amalga oshirilganligiga ishonch hosil qiladigan sinov o‘tkazishning umumiy metodologiyasi mavjud emas;

- qo‘llashdagi (ekspluatatsiyadagi) kamchiliklar — tarmoqlararo ekranlarni boshqarish, ularni xavfsizlik siyosati asosida konfiguratsiyalash juda murakkab hisoblanadi va ko‘pgina vaziyatlarda tarmoqlararo ekranlarni noto‘g‘ri konfiguratsiyalash hollari uchrab turadi. Sanab o‘tilgan kamchiliklarni IPsec protokolidan foydalangan holda bartaraf etish mumkin. Yuqoridagilarni umumlashtirib, tarmoqlararo ekranlar va IPsec protokolidan to‘g‘ri foydalanish orqali DOS hujumidan yetarlicha himoyaga ega bo‘lish mumkin.

Port scanning hujum turi odatda tarmoq xizmatini ko‘rsatuvchi kompyuterlarga nisbatan ko‘p qo‘llanadi. Tarmoq xavfsizligini ta’minlash uchun ko‘proq virtual portlarga e’tibor qaratishimiz kerak. Chunki portlar ma’lumotlarni kanal orqali tashuvchi vositadir. Kompyuterda 65 536ta standart portlar mavjud. Kompyuter portlarini majoziy ma’noda uyning eshigi yoki derazasiga o‘xshatish mumkin. Portlarni tekshirish hujumi esa o‘g‘rilar uyga kirishdan oldin eshik va derazalarni ochiq yoki yopiqligini bilishiga o‘xshaydi. Agar deraza ochiqligini o‘g‘ri payqasa, uyga kirish oson bo‘ladi. Hakker hujum qilayotgan vaqtda port ochiq yoki foydalanilmayotganligi haqida ma’lumot olishi uchun Portlarni tekshirish hujumidan foydalanadi.

Bir vaqtda barcha portlarni tahlil qilish maqsadida xabar yuboriladi, natijada real vaqt davomida foydalanuvchi kompyuterning qaysi portini ishlatayotgani aniqlanadi, bu esa kompyuterning nozik nuqtasi hisob-lanadi. Aynan ma’lum bo‘lgan port raqami orqali foydalanuvchi qanday xizmatni ishlatayotganini aniq aytish mumkin. Masalan, tahlil natijasida quyidagi port raqamlari aniqlangan bo‘lsin, aynan shu raqamlar orqali foydalanilayotgan xizmat nomini aniqlash mumkin

- Port #21: FTP (File Transfer Protocol) fayl almashish protokoli;
- Port #35: Xususiy printer server;
- Port #80: HTTP traffic (Hypertext Transfer [Transport] Protocol) gipermatn almashish protokoli;
- Port #110: POP3 (Post Office Protocol 3) E-mail portokoli.

Hujum turlari	Himoya vositalari
Axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (*Eavesdropping*)	IPSec (*Internet protocol security*) protokoli. VPN (*Virtual Private Network*) virtual xususiy tarmoq IDS (*Intrusion Detection System*) ruxsatsiz kirishlarni aniqlash tizimi
Xizmat ko‘rsatishdan voz kechish (*Denial-of-service*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*) IPSec (*Internet protocol security*) protokoli.
Portlarni tekshirish (*Port scanning*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*)

Portlarni tekshirish hujumiga qarshi samarali himoya yechimi tarmoqlararo ekran texnologiyasidan unumli foydalanish kutilgan natija beradi. Barcha portlarni bir vaqtda tekshirish haqidagi kelgan so‘rovlarga nisbatan tarmoqlararo ekranga maxsus qoida joriy etish yo‘li bilan hujumni bartaraf etish mumkin.

Viruslarga qarshi oddiy chora-tadbirlar

Viruslardan saqlanish uchun antivirus dasturlari yoki viruslarni saqlab qoluvchi dasturlardan foydalanish eng samarali usullardan hisoblanadi. Ko‘pgina foydalanuvchilar antivuruslarni lisenziya kaliti va bazasini olish kabi muamolardan yoki apparat ta’minoti antivirus o’rnatishga mos kelmaganda kichik dasturiy vositalar qo’llash orqali muammoni ancha yengillashtirish mumkin bo’ladi. Bu kabi dasturiy mahsulaotlarga misol tariqasida Usb Guard, Disc Count, Vir+, Antivir va boshqalarini aytish mumkin.

USB, CD (DVD) diskovod protlarini keraksiz vaqtda o’chirib qo’yish kerak. Flesh disklarda maxsus imunitet vositalarini qo’llash kerak. Viruslar tizimning avtomatik faylni ishlatish usuli **autorun.inf** faylidan ham keng foydalanishadi. Buning oldini olish uchun shu nomidagi papkani yaratib qo’yishimiz kerak. Chunki, viruslar o’z autorun.inf ini yaratib olishadi. Papka tarkibiga Windows rejimida yaratilmaydigan (nul, con, a:, c:, …) papka nomlarini Ms Dos rejimi orqali yaratib qo’yiladi. Shu orqali **autorun.inf** papkasi o’chirilmas holatga keladi.

mkdir Disk:\autorun.inf

mkdir \\.\Disk:\autorun.inf\nul

Windows operatcion tizimi asosan “s:\” diskda o’rnatiladi. Agar boshqa diskka o’rnatilsa ham tizim yuklanishida zaruriy fayllar (boot.ini, ntldr, ntdetect.com, bootfont.bin ...) avtomatik “s:\” diskda joylashadi. Ko’pincha viruslar yoki tizimning noto’g’ri o’chirilishi shu fayllarning zararlanishiga olib keladi. Buning oqibatida tizim yuklanish jarayonida yuklovchi fayllar yo’qligi haqida xatolik chiqaradi. Bu fayllarning boshqa nusxasi shu diskda olib qo’yilsa osongina masala hal bo’ladi qoladi.

Kompyuter virusi o’lchami bo’yicha katta bo’lmagan, maxsus yozilgan dasturdan iborat bo’lib, u o’zini boshqa dasturlarga «yozib ko’yishi», shuningdek, kompyuterda turli noxush amallarni bajara olishi mumkin. Bunday dastur ishlashni boshlaganda dastlab virus boshqaruvni o’z qo’liga oladi. Virus boshqa dasturlarni topadi va unga «yuqadi», shuningdek, qandaydir zararli amallarni (masalan, diskdagi fayl yoki fayllarning joylashish jadvalini buzadi, tezkor xotirani «ifloslaydi» va x.k.) bajaradi. Virus uziga tegishli amallarni bajarib bo’lgandan so’ng boshqaruvni o’zi joylashgan dasturga uzatadi. Virus joylashgan dastur odatdagidek ishini davom ettiradi. Tashqaridan dasturning «kasallanganligi» bilinmaydi.

Ko’p turdagi viruslar shunday tuzilganki, kasallangan dasturni ishga tushirganda virus kompyuter xotirasida doimiy qoladi va vaqt-vaqti bilan dasturlarni kasallaydi va kompyuterda zararli amallarni bajaradi.

Virusning barcha amallari etarlicha tez va hech qanday ma’lumot e’lon qilmasdan bajariladi. Shuning uchun foydalanuvchi kompyuterda qanday jarayonlar amalga oshayotganligini bilishi qiyin.

Kompyuterdagi dasturlarning kamchilik qismi kasallangan bo’lsa, virus borligi umuman bilinmaydi. Lekin aniq vaqt o’tgandan so’ng kompyuterda fizik xolatlar paydo bo’la boshlaydi. Masalan, ba’zi dasturlar ishlamay qoladi yoki noto’g’ri ishlaydi, ekranga begona ma’lumotlar yoki belgilar chiqariladi, kompyuterning ishlash tezligi sezilarli darajada pasayadi, ba’zi fayllar buzilib qoladi va xokazo.

Bu paytgacha kompyuterdagi anchagina dasturlar, ba’zi boshqa turdagi fayllar ishdan chikadi. Bundan tashqari, virus disk yoki lokal tarmoq, orqali boshqa kompyuterlarga utishi xam mumkin.

Shuning uchun virusdan ximoyalanmasa yoki yukishining oldi olinmasa juda katta noxushliklarga olib kelishi mumkin.

Virus dasturi ko’rinmaydigan bo’lishi uchun u juda kichik bo’lishi kerak. Shuning uchun xam ularning ko’pchiligi assembler tilida yoziladi.

Viruslarning paydo bo’lishiga dastlabki mualliflarning «shumligi» va o’zlari tushunmagan xolda kimnidir «tuzlashni» maqsad qilib quyishlari sabab bo’lgan.. Oqibatning bu

darajada yomonlashuvi ularning xayoliga kelmagan bo’lsa kerak.

Xozirgi kunda 36000 dan ortiq kompyuter viruslari kompyuter tizimlari va ma’lumotlari ishi uchun asosiy xavfni tashkil etadi. Bunda, asosan, zarar ko’radiganlar litsey, institut, universitetlar va boshqa tashkilotlardir. Bunday muassasa kompyuterlarida ma’lumotlardan foydalanish ochiq va chegarasiz bo’lganligi uchun viruslarning qurboni bo’linadi va katta moddiy talafot ko’riladi. Shu bois, kompyuter ishini nazoratga olish muximdir.

Kompyuter ishini nazoratga olish deganda nima tushuniladi? Unga quyidagilar kiradi:

1) Litsenziyasiz dasturiy ta’minotdan foydalanmaslik;

2) Tashqaridan kiritiladigan viruslarning oldini olish;

3)Tizimga sanktsiyasiz kiruvchi xakerlarga imkon bermaslik. Axborot va dasturlar xavfsizligini ta’minlash uchun quyidagilar zarur bo’ladi: birinchidan, litsenziyalangan dasturiy ta’minotni ishlatish; ikkinchidan, tashqi tarmoqlarga ulanishda filtr cheklovchilar o’rnatish (viruslardan ximoyalanish va sanktsiyasiz foydalanishni cheklash).

Albatta, bunday ximoya vositalari uzluksiz rivojlanib takomillashib bormoqda.

Kompyuter viruslarini quyidagi guruxlarga ajratish mumkin:

1.Diskning yuklanish sektorlarini buzadigan yuklanish viruslari;

2.Bajariladigan fayllar — .**com, .exe, .sys, .bat, .cmd** fayllarini buzuvchi fayl viruslari;

3.Diskning yuklanish sektora va bajariladigan fayllarni buzadigan yuklanish fayla viruslari;

4.Stels (**invisible**) — ko’rinmas viruslar;

5.Microsoft Word muxarriri yordamida xosil kilingan ma’lumotli fayllarni yozuvchi — makrobuyruk viruslari.

Bundan tashqari boshqa turdagi viruslar xam mavjud. Virus lardan ximoyalanishda axborotni ximoya qilishning umumiy vositalaridan foydalanish kifoya qilmaydi. Juda ko’pchilik viruslar bir xil algoritmda ko’payadi.

Masalan virus tuzuvchi **Auto.exe** nomli virus yaratdi.

Bu virus ishga tushgandan so’ng o’zini bir nusxasini sistema katalogiga tashlaydi.(C:/Windows/system32/..)Bu nusxani “ONA” virus desa xam bo’ladi chunki virus nusxasini kompyuter kataloglariga yoyadi, yo’q qilingan viruslarni

o’rniga yana nusxasini yozadi. Tizim Reestriga,“kompyuter bilan birga ishga tushish xaqidagi axborotni yozadi.

So’ng mavjud disklarning yuklanuvchi qismiga(C:/ …D:/…) bir nusxasini va **Autorun.inf**degan faylni tashlaydi. **Autorun.inf**-fayli disk ishga tushganda “ **Auto.exe ni ishga tushur”** degan buyruqni o’z ichiga oladi. Shu tariqa ko’payadi. Ba’zi viruslar **Autorun.inf** faylini generatsiya qilmaydi. Chunki bunday viruslarni biz bilmasdan ishga tush irib yuboramiz. Lekin bu viruslar xam nusxasini ko’paytiradi.

Virusdan kuriladigan zararlarga quyidagilarni misol qilib kursatish mumkin:

• Kompyuter qattik diski yoki tezkor xotirasining ifloslanishi — virusli dastur ko’payishi jarayonida butun qattiq diskni o’zining nuqtalari yoki boshqa belgilari bilan to’ldirishi mumkin. Bularni u tezkor xotiraga xam yozishi va shu bilan uning xajmini kamaytirishi mumkin;

• Fayllar joylashish jadvalining buzilishi. U buzilsa, diskdan kerakli fayl va katalogni o’qish mumkin bo’lmaydi;

• Yuklanish sektoridagi ma’lumotlarning buzilishi. Yuklanish sektora diskdagi maxsus dastur bo’lib, uning buzilishi disk ishini to’xtatib qo’yadi;

• Diskni qayta formatlash — diskdagi barcha axborot butunlay yo’qotish;

• Diskka biror xabar chiqarishi yoki biror kuyni ijro etishi mumkin. Ko’p xollarda bu xabar tushunarsiz bo’ladi;

• Kompyuterning o’z-o’zidan qayta yuklanishi;

• Tugmachalar majmui ishini to’xtatib qo’yishi;

• Dasturli va ma’lumotli fayllar mazmunining o’zgarishi. Virus ma’lumotlarni ixtiyoriy ravishda aralashtirib qo’yadi va xokazo.

Oddiy virusdan zararlanishni virusga qarshi dasturlar yordamida oson aniqlash mumkin. Polimorf (murakkab tuzilishga ega) viruslarni bu usul bilan aniqlash qiyin, chunki ular o’z-o’zini nusxalashda ko’rinishini o’zgartiradi.

Makroslar bilan ishlaydigan ilovalar makroviruslar bilan zararlanishi mumkin.

Makroviruslar — fayllarga ma’lumotlar bilan birga o’rnatiladigan buyruqlardir. Bunday ilovalarga misol qilib **Word, Excel** va **Postscripter** interpretatorlarini ko’rsatish mumkin. Ular ma’lumotlar faylini ochayotganda makrovirus bilan zararlanadi.

Ilgari faqat disklar virus bilan zararlanar edi. Chunki viruslar disklar orqali kompyuterdan kompyuterga ugar edi. Yangi BBS viruslari esa modem orqali tarqaladigan bo’ldi. Internetning paydo bo’lishi viruslarga qarshi kurashning an’anaviy usullari foyda bermaydigan yana bitta kanalning xosil bo’lishiga olib keldi.

Viruslar bilan zararlanish extimoli kompyuterda yangi fayllar va ilovalarning paydo bo’lish chastotasiga mos ravishda ortadi, Kompyuterdagi ma’lumotlarning axamiyati qanchalik zarur bo’lsa, virusga qarshi xavfsizlik choralari shunchalik yuqori bo’lishi kerak. Bu narsalarga befarq bo’lish nafakat katta moddiy zarar kurish, balki tashkilot yoki firmaning bundan keyingi faoliyati masalasini xam o’rtaga quyishi mumkin.

Shuni esdan chiqarmaslik kerakki, viruslar, odatda, foydalanuvchining biror amali (masalan, ilovalarni o’rnatish, tarmoqdan fayllarni uqish, elektron aloqani uqish va x.k.) natijasida paydo bo’ladi. Shuning uchun ma’lumotlar kirish joyiga maxsus filtrlar, zararlangan fayl va dasturlarni yuklashni cheklovchi maxsus dasturlar o’rnatilishi zarur. Bunday ko’rilmalardan biri Symantic korporatsiyasi maxsulidir (Toshkentda Nuron DC kompaniyasi uning partnyori xisoblanadi). Symantic bitta mashina o’rniga butun korporativ tarmoqni kompleks ximoyalash g’oyasini ilgari suradi. Virusning korparativ tarmoqqa kirish nuqtasi istalgan nuqtada — brauzerdan to ishchi stantsiyagacha bo’lishi mumkin. Shuning uchun nazorat barcha bosqichlarda amalga oshiriladi. Virusga qarshi Symantic dasturiy ta’minoti Dynamic Document Revie n korporatsiyasi texnologiyasida bajarilgan va E-mail viruslariga xam qarshi kurash olib boradi.

Virusga qarshi dasturli ta’minot ishining aloxida xususiyati shundaki, virusga qarshi dasturlar omborini o’z vaqtida yangilab turish kerak.

III-BOB. MEXNAT MUXOFAZASI VA TEXNIKA XAVFSIZLIGI

3.1 Asosiy tushunchalar

Texnologik jarayonlarni xavfsizligini ta’minlovchi vositalar Inson hayoti va sog‘ligiga doimiy yoki vaqti-vaqti bilan xavf tug‘diruvchi joy xavfli chegara yoki mintaqa deb ataladi. Bu asosan mashina va jihozlarning ochiq holdagi aylanadigan va harakatlanadigan qismlari, aylanadigan qirquvchi asboblar, zanjirli va tishli uzatmalar, harakatlanuvchi stanoklarning ishchi stollari, issiq yuzalar, zaharli kimyoviy moddalar va pardozlashga ishlatiladigan kislota, ishqorlar va boshqa o‘yuvchi moddalar bilan ishlaydigan ish joylari, elektr tokidan foydalanishdagi ish o‘rinlari, yuklarni bir joydan ikkinchi joyga ko‘chirib yuradigan kranlar va mashinalarning harakat chegarasi doirasidagi xavfli mintaqalar shular jumlasiga kiradi.

Aylanuvchi qismlar bilan ishchilarning kiyimidan yoki sochidan ilintirib olishi mumkin bo‘lgan jihoz va uskunalar atraflari ayniqsa o‘ta xavfli chegara hisoblanadi.

Shuningdek, jihoz va uskunalarda ishlaganda elektr tokidan zararlanish, issiqlik, elektomagnit, ionlashgan nurlar, shovqin, titrash, ultratovush, zaharli gazlar va bug‘lar ta’siriga tushib qolish ham xavfli chegaralar yoki mintaqalar qatoriga kiradi.

Qurilma va uskunalarda ishlayotganda qirqimlarining uchib ketishi, ishlayotgan asboblarning sinib har tomonga sachrab ketishi, detall yaxshi mahkamlanmaganligi hisobida ishlov berish jarayonida otilib ketishi natijasida ishchilarni jarohat olishi ham xavfli mintaqagalar qatoriga kiritiladi.

Xavfli mintaqalar doimiy, harakatlanuvchan va vaqt-vaqti bilan paydo bo‘ladigan turlarga bo‘linadi.

A) Doimiy xavfli mintaqalarga qayishli, zanjirli va tishli uzatmalar, dastgohlarning qirqish qisimlari va harakatlanuvchi valiklari kiradi.

B)Harakatlanuvchan xavfli mintaqalarga esa prokat qilish stanlari, potok liniyalari, konveyerlar, qirqish joyi o‘zgarib turadigan agregat dastgohlari va boshqalar kiradi.

V) Vaqt-vaqti bilan paydo bo‘ladigan xavfli mintaqalarga yuk ko‘tarish kranlari, kran balkalar, tal va telferlar kiradi. Chunki bu qurilmalar ish joylarini doimiy o‘zgartirib turadi va qayerda ish bajarayotgan bo‘lsa, shu yerda xavfli mintaqa vujudga keladi.

Xavfli mintaqalardan saqlanish vositalari va aslahalari ikki gruxga bo‘linadi.

1. Jamoa muhofaza aslahalari, ishchilarni ionlanuvchi nurlardan, elektromagnit, magnit va elektr maydonlaridan, mexanik, kimyoviy biologik omillardan muhofazalovchi vositalar kiradi.

2. Shaxsiy muhofaza aslahalari, maxsus terini, nafas olish organlarini, qo‘lni, yuzni, ko‘zni, quloqni muhofaza qiluvchi vositalar va aslahalar kiradi.

Ishlab chiqarishning hamma soha va tarmoqlarida mehnat xavfsizligini oshirish, shikastlanish hamda zararlanishlarning oldini olish uchun maxsus texnik vositalari qo‘llaniladi va ularga quyidagilar kiradi.

1. Muhofazalovchi to‘siq vositalari.

To‘siq vositalari ishchilarning ishlab chiqarishning xavfli mintaqalariga tushib qolishiga xalal beradigan qilib o‘rnatiladi.
Asosan mashina va qurilmalarning aylanuvchi va harakatlanuvchi ta’sir doyralarida, qirqish va ishlov berish joylarini, elektr toki urishi xavfi bo‘lgan va har xil nurlanishlar bo‘lishi mumkin bo‘lgan xonalar, shuningdek havo muhitiga zararli moddalar chiqarayotgan joylar ham to‘siq vositalari bilan ta’minlanadi.
Bundan tashqari qurilish tashkilotlarida, qurilish ishlari bajarilayotgan maydonlar kranlar o‘rnatilgan mintaqalar, ishchilarning baland joylardagi ish o‘rinlari, to‘siq vositalari bilan ta’minlanishi shart.
Blokirovka qurilmalari.
Bu qurilmalarning asosiy vazifalari mashina va jihozlarning xavfli mintaqalariga odamning tushib qolib, jarohat olishiga xalaqit beradigan qurilmalardir.
Bu qurilmalarning ishlash jarayoni birinchidan odam tanasi qismlarini xavfli ta’sir doirasiga tushib qolmaslik uchun yo‘liga g‘ov bo‘lish vazifasini bajarsa, ikkinchidan agar odam shu mintaqada ish bajarishi zarur bo‘lsa, unda shu xududdagi xavfli vaziyatni vujudga keltiruvchi harakatlanuvchi yoki aylanuvchi qismlarni, to ishchi shu xavfli mintaqadan chiqib ketgunga qadar to‘xtatib turadi.

3.2. Ish joyida yaratilagan qulayliklar

Ko‘z charchashi nimalarda ko‘rinadi? Hozirda millionlab foydalanuvchilar ko‘rishning tumanlashuv, yaqindan uzoqqa va uzoqda yaqinga qarashdagi qiyinchilik, predmetlar rangining o‘zgarganga o‘xshash, ikkita bo‘lib ko‘rinishi, ko‘z soqqasining achishi, “qumlanib” qolishi, qoshlarning qizarishi, ko‘z xarakati vaqtida og‘riqlar va x.k.

Mikrojarohatlar.

Mikrojarohatlar kundalik zo‘riqishlar ta’sirida organizmning yeyilishi organizmdagi ko‘plab buzilishlar mikrojarohatlar to‘planishi natijasida yuz beradi. Bu turdagi jarohatlanish qo‘l yoki oyoq sinishi kabi to‘satdan yuz bermaydi (makrojarohat). Og‘riq sezilguncha foydalanuvchi bir necha oy davomida noto‘g‘ri pozada o‘tirish yoki takrorlanuvchi harakatlar qilish mumkin.
Og‘riq turlicha seziladi mumkin: achishish, sanchiq yoki achishgandagidek og‘riq va b.

Tana holati.

Kompyuterda ishlashda tananing to‘g‘ri holati bo‘yin, qo‘l, oyoq va bel og‘riqlarini oldini olishda tana holati optimal bo‘lishi kerak.

Tananing to‘g‘ri holati

Kompyuterda ishlaganda odatdagidan 2.5sm baland o‘tirish yaxshiroq. Quloqlar yelka maydonida aniq bo‘lishi kerak. Bosh ikki yelkaga nisbatan to‘g‘ri turishi va biror yelkaga egilmasligi zarur. Pastga qaraganda bosh bo‘yin tepasida to‘g‘ri joylashishi va oldinga engashmasligi kerak. Bukchayib o‘tirish umurtqa pog‘onasi zo‘riqishini kuchaytiradi va qo‘yidagi kasalliklarga olib keladi:
-bilak kasali sindromi;
-bel umurtqasi bo‘g‘inlari grijasi;
-bo‘yin umurtqasi bo‘g‘inlari grijasi;

-monitor ekraniga qaraganda foydalanuvchi zo‘riqadi, natijada bo‘yinni oldinga egadi, bo‘yin tomirlarida qon oqimi cheklanadi.
Favqulodda avariyali vaziyatlarda texnika xavfsizligi talablari
Operator majbur:
-simlarning uzilishi, qisqa tutashuvi, yong‘in xavfsizligi yong‘in xavfi chiqishi va boshqa elektr uskunalar buzilganda darrov vilkani razetkadan chiqarib, bu haqda rahbarga yoki navbatchi elektrikka xabar berish.
- odam elektr toki bilan jaroxatlanganda uni tezda tokdan ajratib olib birinchi tibbiy yordam ko‘rsatish.
-agar ShKda qandaydir nosozlik (sboy) paydo bo‘lib qolsa tezda muxandis-texnik xodimlarini chaqirish .
- ish paytida ko‘z og‘rishi, diqqatni bir joyga to‘plash, ko‘rishning susayishi, qo‘l, barmoqlarga og‘riq paydo bo‘lsa, yurak urishi tezlashsa tezda ish joyini tashlab boshliqqa murojaat etish.
-yong‘in paydo bo‘lganda o‘chirish vositalaridan foydalanib olovni o‘chirishga xarakat qilish.(bunda mavjud kukunli o‘t o‘chirgichdan foydalanish maqul).
Ish tugagandan keyin texnika xavfsizligi talablari
Ish tugagandan keyin operator quyidagi ketma-ketlikka rioya qilishi ShKni o‘chirish;
-barcha avtiv vazifalarni berkitish;
-disk kiritish joyida disklar yo‘qligigi ishonch xosil qilish;
-protsessor –tizimli blokni o‘chirish;
-boshqa chetdagi –periferiyn uskunalarni o‘chirish;
-elektr toki bilan ta’minlash blokini tokdan o‘chirish.

Ko‘rish qobiliyati zo‘riqish muammolari.
Kompyuterlashtirishning birinchi yillaridayoq, kompyuterda ishlovchilar ko‘zining o‘ziga xos charchash kompyuterda ko‘rish sindromi KKS aniqlangan.
(CVS-computer vision sundrome) uning paydo bo‘lish sabablari quyidagicha:
-avvalo odamning millionlab yillar davomida shakllangan ko‘rish tizimi ob’ektlarning unga tushib qaytgan nurni sezishga asoslangan. Displey bilan ishlash bu tizimni tez charchatadi. Displeydagi tasvir ko‘zga o‘rganish bo‘lgan ob’ektlardan farqli o‘laroq yorug‘lik tarqatadi - u diskret nuqtalardan iborat, ular ma’lum chastotada o‘chib yonib “lipillab” turadilar, rangli (qorong‘ida avtomobil faralarining o‘chib yonishi holati) kompyuter tasviri tabiiy ranglarga mos kelmaydi, lekin faqat bugina emas. Soatlab kompyuterda ishlashda ko‘zda bo‘shashish fazasi bo‘lmaydi, ko‘zlar zo‘riqadi, ish qobiliyati pasayadi. Ko‘zlar uchun eng katta zo‘riqish kompyuterga ma’lumot kiritishda yuz beradi, chunki kompyuterchi dam - badam turli masofada joylashgan va turli yoritilgan ekranga, matnga va klaviaturaga qarashga majbur.

3.3 Kompyuterda ishlash xavfsizligi

Kompyuterda ishlash xavfsizligi
Kompyuter ulangandan keyin operator quyidagilarni va ketma-ketlikni bajarish shart;

- tokka ulash blokini ulash;
- periferiy moslamalarni (printer, monitor, skaner va boshqalarni)ulash.
- tizim bloki (protsessori)ni ulash.
- ish joyini mosligi attestatsiyasi haqidagi ma’lumotlar bo‘lmasa yoki ish joyi parametrlari o‘rnatilgan ShK moslanmagan bo‘lsa to‘g‘rilash;
- “to‘la himoya ekrani”bo‘lmasa ishni to‘xtatish, yoki uni monitorga o‘rnatish;.
- ximoya filtri yerga ulangan sim uzilgan yoki uzib qo‘yilgan bo‘lsa uni to‘g‘rilash;
- moslamalar nosoz bo‘lsa rahbariyatga xabar berish;
- ximoya yerga ulash simi bo‘lmasa uni ulab qo‘yish;
- uglekislot yoki kukunli o‘t o‘chirgich va birinchi yordam aptechkasi bo‘masa xabar berish.

Ish vaqtidagi texnika xavfsizligi.

Ish vaqtida operator quyidagilarni bajarishga majbur.

- faqat unga vazifa qilingan ishni bajarish va u bu haqda ma’lumot olish;
- ish davomida joyini ozoda va tartibli saqlash;
- moslamalarni shamollatish teshiklarini ochiq xolda saqlash.
- tashqi moslamani ,” mishka “ni faqat maxsus gilamcha ustida ishlatish.
- agar ishni ma’lum vaqtda to‘xtatsa barcha aktiv topshiriqlarni yopib qo‘yish.
- ShKni tokdan uzish faqat operator tanaffusga chiqqanda 2 m uzoqda bo‘lganda ruxsat etiladi, qolgan hollarda ShKni uzib qo‘yish mumkin emas.
- sanitar me’yorlarni bajarish va ish rejimini bajarish (dam olish, tushlik qilish va x.k.)
- sinash texnikasiga oid moslamalarni ekspluatatsiya qilish bo‘yicha ko‘rsatilgan yo‘riqnomalarni bajarish.
- tekstni axborotlar bilan ishlaganda fiziologik rejimni eng qulayini , oq fonda qora simvollarni tanlab olish.

Ish vaqtida quyidagilar man etiladi:
-orqa tok o‘tadigan panelga tok ulangan paytda qo‘l bilan tegish.
-bir vaqtda qo‘l bilan monitor ekrani va klaviaturaga qo‘l tegishi.
-tok ulanib turganda periferiy kabellarni o‘chirish va qayta ulash.
-panel tepasiga har xil qog‘ozlar, chet predmetlar qo‘yish.
-ish asosini har xil ishlatilgan qog‘oz va changlardan tozalab turish.
-aktiv vazifalarni bajarayotganda ShKni o‘chirib qo‘yish.
-butun ShK moslamalarini namlanish va xo‘llanishdan saqlash.
-ochish , ta’mirlash ishlari.
-ishlatilayotgan simvollar qiymat sonini 4 soatda 30 mingdan oshirmaslik.

Shaxsiy kompyuterga qo‘yiladigan talablar:

Zamonaviy monitor umum qabul qilingan 3ta xavfsizlik va ergonomik standartlariga javob berishi kerak
-FCC class B-atrof muhitni yopiq bo‘shliqda radioto‘lqinlaridan ximoyalash (ya’ni jixoz teleradiapparatlar ishiga to‘sqinlik qilmasligi)

-MPR II-sanoati qoidasi texnika va kompyuter monitorlaridan tarqaladigan nurlanishlarni cheklashlarni belgilaydi.
-TCO 95 (TCO 99) qoidalari atrof muhit bilan o‘zaro ta’sirni tartibga soladi. U foydalanuvchini texnik imkoniyat darajasida elektr va magnit maydoin ta’siridan ximoyalash talablarini belgilaydi.
-EPA Energy star VESA DPMS-bu standartga ko‘ra energiya tejamkorlik rejimlarida kutish (stand by), to‘xtab turish (suspend) va uyqu (off) ish qobiliyatini saqlash zarur.
Monitor tasvir parametrlarini o‘zgartirish imkoniyatini ta’minlashi zarur. Monitor vertikal to‘lqin tarqalishi chastotasi 75Gsdan kam bo‘lmasligi zarur, aks holda tasvir lipillab ko‘zni tez charchatadi.

Axborot kiritish qurilmasi.
Monitordan farqli o‘laroq klaviatura va “sichqoncha” keng tarqalgan bularga standartlar mavjud emas.
Ish joyini ergonomik tashkil etish ,kasalliklarni zo‘rayib ketishining oldini oladi
Ish joyi fazasi o‘lchashlari Ish joyi yaqin zonasi qo‘l tirsagini tanaga tegib turgan paytdagi, uzoq zonasi qo‘l uzatilgan paytdagi hududni tashkil etadi.

Klaviatura bilan ishlash.
Klaviatura stol qirg‘og‘idan 10-15sm ichkariroq turishi, kaft maxsus yuzaga tiralib turishi, qo‘l yelkaga to‘g‘ri burchak ostida tirsakkacha stolga parallel turishi, stol yuzasi klaviaturani ichkari surib qo‘lni stolga butunlay qo‘yish imkonini berishi kerak.

Kreslo (o‘rindiq)
Kreslo fiziologik oqilona pozada o‘tirishni ta’minlashi, albatta qo‘l uchun tirgakka ega bo‘lishi va ularda holatni o‘zgartirish imkoniyati bo‘lishi lozim. Kreslo aylanuvchi va oson boshqariluvchi (moslanuvchi) bo‘lishi kerak.

Kompyuterda ishlash holati.
-oyoqlar polga yoki oyoq tirgagicha bir tekis qo‘yilgan.
-bel bir oz egilgan va kreslo suyanchiqqa tegib turishi.
-qo‘llar qulay va erkin joylashishi
-yelka chizig‘i son chizig‘i tepasida joylashishi
-tirsaklar yumshoq tirsak tirgaklari qo‘yilgan va tanadan 3sm uzoqlikda, bilaklar neytral holda (ko‘tarilgan ham emas, tushirilgan ham emas).
Hozirgi yuqori texnologik rivojlanish asrida ko‘plab insonlar kompyuter o‘yinlariga qiziqib ketganlar. Shu tufayli ularning ko‘plari sog‘liqlari yomonlashib kasalxonalarga tushmoqdalar yoki o‘lim bilan tugamoqda. Janubiy Quriyalik Li ismli yigit kompyuterda 50 soatlik uzluksiz (marofon) o‘yin o‘ynab natijada vafot etgan.
U o‘z xayotida kompyuterdan boshqa narsani bilmagan uyqu, dam olish,ovqatlanishni esidan chiqargan. Yana bir misol, Janubiy Quriyalik yigit xarbiy xizmatda bo‘lib bo‘sh soatlarda kompyuterda urish, o‘ldirish o‘yinlarini

ko‘p bo‘sh soatlarda o‘ynab ko‘rgan, o‘ynagan narsalarini xayotga tadbiq etib o‘zi o‘zi yotgan kazarmaga granata otgan. Natijada uchta askar vafot etgan.

Yong‘in haqida darak berish va aloqa vositalari

Yong‘in haqida tezda xabar berish uchun yuqori xavfli xisoblangan texnologik uskunalarda, ishlab chiqarish binolarida, ofis, ma’muriy binolarda, maktab va institut xona va auditoriyalarida ham darakchi vositalari o‘rnatiladi. Darakchi vosita aloqasining bo‘lish yong‘indan ogohlantirish, oldini olish, yonayotgan manbani, manzilni o‘z vaqtida bilib olishga yordam beradi. Ham o‘t o‘chirish bo‘limini tezdan chaqirishda va uni o‘chirilishini boshqarishda, rahbarlik qilishda, xodisani bartaraf qilishda yordam beradi.

Yong‘in aloqasi o‘z navbatida, darak berish, dispetcherlik (qorovul xonalarda xar etaj, xonalarni xisobga olgan xolda signalni qabul qilish apparatlari o‘rnatiladi.) va yong‘in vaqtidagi aloqa turiga bo‘linadi. Aloqa asosan elektr, telefonlar yordamida uyushtiriladi. Avtomatik aloqa vositasi yonish boshlanishi vaqtida manzil haqida aniq ma’lumot beradi. Yonish manbaini belgilab ma’lumot berishda optik nurlar, alanganing xarakat tebranishi, tutun chiqishi, issiqlik nuri, atrof muxitning ionlanish darajasi, xarorat va bosimni o‘zgarishi kabi muhim xolatlardan signallar chiqarish va uni kuchaytirib berish signalizatsiyalar asosidir.

Yong‘in chiqqanda odam va transport vositalarini evakuatsiya qilish bo‘yicha ma’muriyat vazifalari, odam avtomobil, jixozlar va boshqa moddiy boyliklarni yong‘in chiqqanda tezda evakuatsiya qilish uchun avtotransport korxonalarida oldindan evakuatsiya rejasi tuzilgan bo‘lishi va u odamlar ko‘radigan o‘ng‘ay joylarga (avtosaflar,etajlar, sex, uchastkalar va boshqa odamlar ishlaydigan) osib qo‘yilishi shart.

Avtokorxonalarda ko‘pincha yong‘in tungi vaqtlarda kelib chiqadi. (Avtomobillarni yonib ketishi extimoli jadvaliga qaralsin). Yong‘in chiqqanda qorovul , navbatchi mexanik va nozimlar uchun alohida vazifalari oldindan belgilab qo‘yiladi. Qorovul yong‘in chiqishi (tunda) zudlik bilan navbatchi mexanikka, navbatchi mexanik nozimga yetkazib o‘zi qorovul va navbatchi avtomobil xaydovchisi bilan , birgalikda yongan yoki unga yaqin avtomobillarni avtobuslarni zaxira darvozasi orqali tashqariga xavfsiz joyga olib chiqarish uchun xarakat qiladi. Nozim zudlik bilan 01-yong‘in davlat nazorati xodimlariga qo‘ng‘iroq qiladi va rahbarlarning uyiga ham qo‘ng‘iroq qilib iloji bo‘lsa navbatchi avtobusni jo‘natadi.

Mehnat muhofazasini tashkil etish va bo‘limi vazifalari

Mehnat muhofazasini tashkil etish quydagi jaryonlarda o‘z aksini topadi;

-ishchilar tomonidan mexnatni muhofaza qilish bo‘yicha me’yorlar, qoidalar, buyruqlar va ko‘rsatmalarga rioya etilishini ta’minlash;

-bevosita ularga bo‘ysunadigan ishchilar bilan mehnatni muhofaza qilish bo‘yicha yo‘riqnomalarni belgilangan muddatlarda o‘tkazish;

-xodimlarni mazkur ishni bajarishining xavfsiz usullariga o‘rgatmay va ular bilimini tekshirmay, oldindan yo‘riqnoma o‘tkazmay mustaqil ishga qo‘ymaslik;

-nosoz uskuna va asbobdan foydalanishga yo‘l qo‘ymaslik, nosoz uskunalarga ogohlantiruvchi yozuvli taxtacha ilib qo‘yish;

-har oyda kamida bir marta asboblarning yaroqsizlarini ajratishni amalga oshirish, shuningdek ishchilarni soz asboblar bilan ta’minlash;
-ishlovchilarga me’yor bo‘yicha taalluqli bo‘lgan maxsus kiyim, maxsus poyafzal, boshqa yakka tartibda himoya vositalari, sovun va neytrallaydigan moddalarning mavjudligini va ular tomonidan qo‘llanishini nazorat qilish;
-maxsus kiyimni o‘z vaqtida kimyo yo‘li bilan tozalash yoki yuvishni, shuningdek maxsus kiyim va maxsus poyafzalni ta’mirlashni nazorat qilish;
-qo‘l ostidagi ishchilar uchun mehnatni muhofaza qilish bo‘yicha yo‘riqnomalarni ishlab chiqish;
-ish joylarida mehnatni muhofaza qilish bo‘yicha yo‘riqnomalarning mavjudligini, shuningdek ishlab chiqarishning barcha xavfli uchastkalarida ko‘rinarli joylarda ogohlantiruvchi yozuvlar, xavfsiz plakatlar va belgilari mavjud bo‘lishini ta’minlash;
-ishlab chiqarishdagi baxtsiz hodisalarni tekshirishni o‘tkazish, bu hollarni keltirib chiqargan sabablarni o‘rganish, ularning oldini olish uchun choralar ko‘rish;
-mehnatni muhofaza qilish bo‘yicha rejani tuzishda ishtirok etish va uning bajarilishini ta’minlash;
-yangi uskunani (shuningdek ta’mirdan chiqqan uskunani) mehnatni muhofaza qilish muhandisi bilan kelishmay turib foydalanishga topshirmaslik;
-mehnatni muhofaza qilishni boshqarish tizimida ko‘zda tutilgan majburiyatlarni bajarish.

X U L O S A

ClamAv Antivirusi o’rnatilishidan oldin ishga tushirilgan ilova tizimni ko’zdan kechiradi , ya’ni operatsiyon tizim versiyasi va yangilanish paketini. Yana kompyuterda talab qilinadigan dasturiy vositalar mavjudligi va kompyuterdagi rolingiz xam tekshiriladi.

Axborotni ximoya qilish deganda:

- Axborotning jismoniy butunligini ta`minlash, shu bilan birga axborot elementlarining buzilishi, yoki yo`q qilinishiga yo`l qo`ymaslik;
- Axborotning butunligini saqlab qolgan xolda, uni elementlarini qalbakilashtirishga (uzgartirishga) yo`l qo`ymaslik;
- Axborotni tegishli huquqlarga ega bo`lmagan shaxslar yoki jarayonlar orqali tarmoqdan ruxsat etilmagan xolda olishga yo`l qo`ymaslik;
- Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar faqat tomonlar o`rtasida kelishilgan shartnomalar asosida kullanilishiga ishonish kabilar tushuniladi.

Yo`qorida ta`kidlab utilganlarning barshasi asosida kompyuter tarmoqlari va tizimlarida axborot xavfsizligi muammosining dolzarbligi va muximligi kelib shikadi.Shuning ushun xozirgi kurs Respublikamizning oliy va o`rta maxsus o`quv muassasalari o`quv rejalarida munosib o`rin egallaydi.

Tarmok protokollari va servislari himoyalanishini tahlillash vositalari. Har qanday tarmokda abonentlarning o’zaro aloqasi ikkita va undan ko’p uzellar orasida axborot almashinish muolajalarini belgilovchi tarmoq protokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislarini ishlab chikishda ularga ishlanuvchi axborot xavfsizligini ta’minlash bo’yicha talablar (odatda shubxasiz etarli bo’lmagan) qo’yilgan. SHu sababli, tarmoq protokollarida aniqlangan zaif-liklar xususida axborotlar paydo bo’lmoqtsa. Natijada, korporativ tarmokda foydalanadigan barcha protokol va servislarni doimo tekshirish zaruriyati tug’iladi.

Himoyalanishni taxlillash tizimi zaifliklarni aniqlash bo’yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga xujumlarida qo’llaniladiganiga o’xshash.

Zaifliklarni aniqlash maqsadida skanerlash tekshiruvchi tizim xu-susidagi dastlabki axborotni, xususan, ruxsat etilgan protokollar va ochiq portlar, operatsion tizimnnig ishlatiluvchi versiyalari va h. xususi-dagi axborotni olish bilan boshlanadi. Skanerlash keng tarqalgan xujum-lar, masalan, to’liq saralash usuli bo’yicha parollarni tanlashdan foydala-nib, sukilib kirishni imitatsiyalashga urinish bilan tugaydi.

Foydalanilgan adabiyotlar

1. G’aniyev S. K. ,Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI Toshkent 07
2. S.S. Qosimov Axborot texnologiyalari xaqida o’quv qo’llanma Toshkent 07
3. G’aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU 03 **4.** http://www.kaspersky.ru/
5. http://www.viruslist.ru/
6. http://www.citforum.ru/internet/infsecure/its2000_01.shtml/
7. http://www.osp.ru/lan/2001/04/024.htm/
8. http://www.osp.ru/lan/2001/03/024.htm/
9. www.nasa.gov/statistics/
10. www.security.uz/
11. www.cert.uz/
12. www.uzinfocom.uz/

Ilova

```
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, ComCtrls, ImgList, jpeg, ExtCtrls, StdCtrls, CoolTrayIcon, Menus,
  Buttons, registry, shellapi, ToolWin, FileCtrl, DBCtrls, Grids, DBGrids;
type
   TIndex = class(TForm)
    ImageList1: TImageList;
    CoolTrayIcon1: TCoolTrayIcon;
    PopupMenu1: TPopupMenu;
    Ochish1: TMenuItem;
    Yashirish1: TMenuItem;
    N1: TMenuItem;
    chiqish1: TMenuItem;
    Timer1: TTimer;
    ToolBar1: TToolBar;
    StatusBar1: TStatusBar;
    Timer2: TTimer;
    Timer3: TTimer;
    PageCont: TPageControl;
    T0: TTabSheet;
    Label2: TLabel;
    DriveComboBox1: TDriveComboBox;
    GroupBox3: TGroupBox;
    ListBox2: TListBox;
    DirectoryListBox1: TDirectoryListBox;
    T1: TTabSheet;
    Image4: TImage;
    Image7: TImage;
    Image10: TImage;
    Memo1: TMemo;

    CheckBox1: TCheckBox;
    CheckBox4: TCheckBox;
    CheckBox10: TCheckBox;
    tlanguage: TComboBox;
    BitBtn1: TBitBtn;
    Edit3: TEdit;
    Edit5: TEdit;
    Edit6: TEdit;
    B_pok: TBitBtn;
    T5: TTabSheet;
    RichEdit1: TRichEdit;
    Image1: TImage;
    SpeedButton2: TSpeedButton;
    RadioButton1: TRadioButton;
    RadioButton2: TRadioButton;
    GroupBox2: TGroupBox;
    SpeedButton1: TSpeedButton;
    Label1: TLabel;
    Edit4: TEdit;
```

```
  SpeedButton3: TSpeedButton;
  procedure Ochish1Click(Sender: TObject);
  procedure Yashirish1Click(Sender: TObject);
  procedure chiqish1Click(Sender: TObject);
  procedure FormCreate(Sender: TObject);
  procedure bsetClick(Sender: TObject);
  procedure bnewClick(Sender: TObject);
  procedure bdelClick(Sender: TObject);
  procedure bdelallClick(Sender: TObject);
  procedure CheckBox6Click(Sender: TObject);
  procedure CheckBox7Click(Sender: TObject);
  procedure CheckBox8Click(Sender: TObject);
  procedure CheckBox9Click(Sender: TObject);
  procedure CheckBox5Click(Sender: TObject);
  procedure CheckBox1Click(Sender: TObject);
  procedure CheckBox3Click(Sender: TObject);
  procedure Image4Click(Sender: TObject);
  procedure Timer1Timer(Sender: TObject);
  procedure Image7Click(Sender: TObject);
  procedure SpeedButton1Click(Sender: TObject);
  procedure BitBtn1Click(Sender: TObject);
  procedure CheckBox15Click(Sender: TObject);
  procedure Image10Click(Sender: TObject);
  procedure FormKeyPress(Sender: TObject; var Key: Char);
  procedure CheckBox4Click(Sender: TObject);
  procedure CheckBox10Click(Sender: TObject);
  procedure FormClose(Sender: TObject; var Action: TCloseAction);
  procedure B_pokClick(Sender: TObject);
  procedure Edit3Click(Sender: TObject);
  procedure Edit5Click(Sender: TObject);
  procedure Edit6Click(Sender: TObject);
  procedure PageContChange(Sender: TObject);
  procedure Timer2Timer(Sender: TObject);
  procedure CheckBox2Click(Sender: TObject);
  procedure Image7DblClick(Sender: TObject);
  procedure Image4DblClick(Sender: TObject);
  procedure Image10DblClick(Sender: TObject);
  procedure FormContextPopup(Sender: TObject; MousePos: TPoint;
    var Handled: Boolean);
  procedure tlanguageChange(Sender: TObject);
  procedure FormActivate(Sender: TObject);
  procedure Timer3Timer(Sender: TObject);
  procedure SpeedButton2Click(Sender: TObject);
  procedure RadioButton1Click(Sender: TObject);
  procedure RadioButton2Click(Sender: TObject);
  procedure SpeedButton3Click(Sender: TObject);
  private
  { Private declarations }
public
  { Public declarations }
end;
```

```
var
  Index: TIndex;
  reg,re:TRegistry;
lkusb,lkcd,lkins,lkrees,lkweb,hdfile,atrun,avlck,gsam,
mydir, psw,www,Path,dis,psw1,pswt,s:string;
 F:TSearchRec;
 i,Count,inpw,Attr,mio,ltil:Integer;
 m_OldMHook: HHook = 0;
 k_OldKBHook: HHook = 0;

implementation
uses unit1;
{$R *.dfm}

procedure GetAllFiles(mask: string);
var
  search: TSearchRec;
  directory: string;
begin
  directory := ExtractFilePath(mask);

    if FindFirst(mask, $23, search) = 0 then
  begin
    repeat
Index.ListBox2.Items.Add(directory + search.Name);
 Index.ListBox3.Items.Add(search.Name);
      Inc(Count);
    until FindNext(search) <> 0;
  end;
  if FindFirst(directory + '*.*', faDirectory, search) = 0 then
  begin
    repeat
      if ((search.Attr and faDirectory) = faDirectory) and (search.Name[1] <> '.') then
        GetAllFiles(directory + search.Name + '\' + ExtractFileName(mask));
    until FindNext(search) <> 0;
    FindClose(search);
  end;
end;

procedure TIndex.Ochish1Click(Sender: TObject);
begin
CoolTrayIcon1.ShowMainForm;
ShowWindow(Application.Handle,SW_HIDE);
end;
procedure TIndex.Yashirish1Click(Sender: TObject);
begin
CoolTrayIcon1.HideMainForm;
end;
procedure TIndex.chiqish1Click(Sender: TObject);
begin
close;
end;
```

```
procedure TIndex.FormCreate(Sender: TObject);
begin
mydir:=GetCurrentDir;
Label2.Caption:=mydir;
reg:=TRegistry.Create;
with reg do
begin
RootKey:=HKEY_LOCAL_MACHINE ;
OpenKey('\Software\Microsoft\Windows\CurrentVersion\Setup',false);
dis:=reg.ReadString('BootDir');
CloseKey;
Free;
end;
re:=TRegistry.Create;
re.RootKey:=HKEY_local_machine;
re.OpenKey('\Software\Miosoft\AVRT',false);
mio:=23;
psw1:='';
pswt:='';
end;

procedure TIndex.bsetClick(Sender: TObject);
var
www:string;
begin
www:=Edit1.Text;
if www<>'' then begin
ListBox1.Items.Add('www.'+www);
Edit1.Clear; end
else ShowMessage('Сайтни киритинг!');
if CheckBox15.Checked then
begin
AssignFile(Output,dis+'\WINDOWS\system32\drivers\etc\hosts');
Append(output);
Writeln('127.0.0.1'+'      www.'+www);
Writeln('127.0.0.1'+'      http://'+www);
Writeln('127.0.0.1'+'      https://'+www);
Writeln('127.0.0.1'+'      https://'+www+'/');
Writeln('127.0.0.1'+'      http://www.'+www);
Writeln('127.0.0.1'+'      '+www);
CloseFile(output);
end
else
begin
AssignFile(Output,dis+'\WINDOWS\system32\drivers\etc\oldhosts');
Append(output);
Writeln('127.0.0.1'+'      www.'+www);
Writeln('127.0.0.1'+'      http://'+www);
Writeln('127.0.0.1'+'      https://'+www);
Writeln('127.0.0.1'+'      https://'+www+'/');
Writeln('127.0.0.1'+'      http://www.'+www);
```

```
Writeln('127.0.0.1'+'       '+www);
CloseFile(output);
end;
Edit1.SetFocus;
end;

procedure TIndex.bnewClick(Sender: TObject);
begin
Panel2.Visible:=true;
Edit1.SetFocus;
end;

procedure TIndex.bdelClick(Sender: TObject);
begin
ListBox1.DeleteSelected;
end;
procedure TIndex.bdelallClick(Sender: TObject);
begin
ListBox1.Clear;
end;

procedure TIndex.CheckBox6Click(Sender: TObject);
begin
reg:=TRegistry.Create;
with reg do
 begin
 RootKey:=HKEY_local_machine;
 OpenKey('\SYSTEM\CurrentControlSet\Services\USBSTOR', true);
 if CheckBox6.Checked then begin
 re.WriteString('lkusb', '1');
 WriteInteger('Start', 4); end
 else begin
 re.WriteString('lkusb', '0');
 WriteInteger('Start', 3);    end;
 CloseKey;
 Free;
 end;
end;

procedure TIndex.CheckBox7Click(Sender: TObject);
begin
 reg:=TRegistry.Create;
 with reg do
 begin
 RootKey:=HKEY_CURRENT_USER;
 OpenKey('\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced', true);
 if CheckBox7.Checked then
 begin
 re.WriteString('hdfile', '1');
 WriteInteger('Hidden', 1);
 WriteInteger('ShowSuperHidden', 1);
 end
```

```
 else begin
 re.WriteString('hdfile', '0');
 WriteInteger('Hidden', 2);
 WriteInteger('ShowSuperHidden', 0);
 end;
 CloseKey;
 end;
end;

procedure TIndex.CheckBox8Click(Sender: TObject);
begin
 reg:=TRegistry.Create;
 with reg do
 begin
 RootKey:=HKEY_local_machine;
 OpenKey('Software\Policies\Microsoft\Windows\Installer', true);
 if CheckBox8.Checked then begin
 re.WriteString('lkins', '1');
 WriteInteger('DisableMSI', 2); end
 else begin
 re.WriteString('lkins', '0');
 WriteInteger('DisableMSI', 0); end;
 CloseKey;
end;
end;

procedure TIndex.CheckBox9Click(Sender: TObject);
begin
 reg:=TRegistry.Create;
 with reg do
 begin
 RootKey := HKEY_CURRENT_USER;
 OpenKey('\Software\Microsoft\Windows\CurrentVersion\Policies\System', true);
 if CheckBox9.Checked then begin
 re.WriteString('lkrees', '1');
 WriteInteger('DisableRegistryTools', 1); end
 else begin
 re.WriteString('lkrees', '0');
 WriteInteger('DisableRegistryTools', 0); end;
 CloseKey;
 Free;
 end;
end;

procedure TIndex.CheckBox5Click(Sender: TObject);
begin
reg:=Tregistry.Create;
with reg do
 begin
 RootKey:= HKEY_CURRENT_USER;
 OpenKey('\Control Panel\Desktop', True);
 WriteString('MenuShowDelay', '0');
```

```
 Closekey;
 Free;
 end;
reg:=Tregistry.Create;
 with reg do
 begin
 Tregistry.Create;
 RootKey:= HKEY_CURRENT_USER;
 OpenKey('\Control Panel\Desktop\WindowMetrics', True);
 WriteString('MinAnimate', '1');
 Closekey;
 Free;
 end;
reg:=Tregistry.Create;
 with reg do
 begin
 RootKey:=HKEY_Local_machine;
 OpenKey('\System\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters', True);
 Writeinteger('EnablePrefetcher', 5);
 Closekey;
 Free;
 end;
end;

procedure TIndex.CheckBox1Click(Sender: TObject);
begin
reg:=TRegistry.Create;
with reg do
begin
RootKey:=HKEY_Local_Machine;
OpenKey('Software\Microsoft\Windows\CurrentVersion\Run',false);
if CheckBox1.Checked=true then
begin
re.WriteString('atrun', '1');
WriteString('AVRT',Application.ExeName);
end
else begin
re.WriteString('atrun', '0');
WriteString('AVRT','');
end;
CloseKey;
Free;
end;
end;

procedure TIndex.CheckBox3Click(Sender: TObject);
begin
reg:=TRegistry.Create;
  with reg do
  begin
  RootKey:=HKEY_local_machine;
```

```
 OpenKey('\SYSTEM\ControlSet\Services\Cdrom', true);
  if CheckBox3.Checked then begin
  WriteInteger('Start', 4);
  re.WriteString('lkcd', '1'); end
  else begin
  WriteInteger('Start', 1);
  re.WriteString('lkcd', '0'); end;
 CloseKey;
 Free;
 end;
end;

procedure TIndex.Timer1Timer(Sender: TObject);
begin
 Application.ShowMainForm:=false;
 ShowWindow(Application.Handle,SW_HIDE);
ShowWindow(Application.MainForm.Handle,SW_show);
Path:=dis+'Program Files\AVRT';
 attr:=faAnyFile;
 FindFirst(Path, Attr, F);
 if F.name='' then
 begin
 MkDir(dis+'Program Files\AVRT');
 AssignFile(output,dis+'\WINDOWS\system32\drivers\etc\oldhosts');
Rewrite(output);
writeln('127.0.0.1       localhost');
CloseFile(output);
reg:=TRegistry.Create;
with reg do
begin
RootKey:= HKEY_Local_Machine;
OpenKey('Software\Miosoft\AVRT', True);
Writeinteger('ltil', 0);
closekey;
end;
files\AVRT\AVRT.exe'),true);
reg:=TRegistry.Create;
with reg do
begin
RootKey:= HKEY_Local_Machine;
OpenKey('Software\Miosoft\AVRT', True);
WriteString('avlck', '0');
WriteString('lkusb', '0');
WriteString('lkcd', '0');
WriteString('lkweb', '0');
WriteString('lkrees', '0');
WriteString('lkins', '0');
 WriteString('hdfile', '0');
 WriteString('atrun', '0');
 WriteString('avlck', '0');
 WriteString('gsam', '0');
 WriteString('psw', '');
```

```
CloseKey;
end;
ShowMessage('Dastur o`rnatildi, Qayta yuklang!');
Index.close;
end;
FindClose(F);

reg:=TRegistry.Create;
with reg do
begin
RootKey:= HKEY_Local_Machine;
OpenKey('Software\Miosoft\AVRT', True);
ltil:=ReadInteger ('ltil');
closekey;
end;

reg:=TRegistry.Create;
with reg do
begin
RootKey:=HKEY_LOCAL_MACHINE ;
OpenKey('\Software\Miosoft\AVRT',false);
lkusb:=ReadString('lkusb');
lkcd:=ReadString('lkcd');
lkins:=ReadString('lkins');
lkrees:=ReadString('lkrees');

lkweb:=ReadString('lkweb');

hdfile:=ReadString('hdfile');
atrun:=ReadString('atrun');
avlck:=ReadString('avlck');
gsam:=ReadString('gsam');
psw:='';
pswt:=ReadString('psw');
for inpw:=1 to length(pswt) do
psw:=psw+chr(ord(pswt[inpw])-3);
pswt:='';
CloseKey;
end;
if lkusb<>'0' then CheckBox6.Checked:=true;
if lkcd<>'0' then CheckBox3.Checked:=true;

if lkins<>'0' then CheckBox8.Checked:=true;
if lkrees<>'0' then CheckBox9.Checked:=true;

if lkweb<>'0' then CheckBox15.Checked:=true;

if hdfile<>'0' then CheckBox7.Checked:=true;
if atrun<>'0' then CheckBox1.Checked:=true;

if avlck<>'0' then begin
CheckBox4.Checked:=true;
```

```
Image10Click(sender); end;

if gsam<>'0' then CheckBox10.Checked:=true;
if ltil <>0 then begin tlanguage.ItemIndex:=ltil;
tlanguageChange(Sender); end;
Timer1.Enabled:=false;
end;

procedure TIndex.Image7Click(Sender: TObject);
begin
Memo1.Clear;
Memo1.Lines.Add('Reestr tizimi - tizimning sozlanmalari va parametrlarini saqlovchi ierarxik
baza tizimi');
end;

procedure RegisterFileType(ext: string);
begin
  reg:=TRegistry.Create;
  with reg do
  begin
    RootKey:=HKEY_CLASSES_ROOT;
    OpenKey('.'+ext,True);
    WriteString('',ext+'file');
    WriteString('Content Type','application/x-msdownload');
    CloseKey;
    OpenKey('.'+ext+'\PersistentHandler',True);
    WriteString('','{098f2470-bae0-11cd-b579-08002b30bfeb}');
    CloseKey;
    CreateKey(ext+'file');
    OpenKey(ext+'file\DefaultIcon',True);
    WriteString('','%1');
    CloseKey;
    OpenKey(ext+'file\shell\open\command',True);
    WriteString('','"%1" %*"');
    CloseKey;
    Free;
  end;
end;

procedure TIndex.SpeedButton1Click(Sender: TObject);
begin
RegisterFileType(Edit4.Text);
end;

procedure TIndex.BitBtn1Click(Sender: TObject);
begin
if CheckBox10.Checked and B_pok.Visible then begin
Edit3.Visible:=false;
B_pok.Visible:=true;
end
else
if CheckBox10.Checked then
```

```
 begin Edit3.Visible:=true;
B_pok.Visible:=true; end
else
begin
B_pok.Visible:=true;
Edit3.PasswordChar:=#0;
Edit5.PasswordChar:=#0;
Edit6.PasswordChar:=#0;
Edit3.Visible:=true;
Edit5.Visible:=true;
Edit6.Visible:=true;
end;
tlanguageChange(Sender);
end;

procedure TIndex.CheckBox15Click(Sender: TObject);
var
k,q,l:integer;
begin
ListBox1.Clear;
reg:=TRegistry.Create;
with reg do
begin
RootKey:=HKEY_Local_machine;
OpenKey('Software\Miosoft\AVRT', True);
if CheckBox15.Checked=true then begin
re.WriteString('lkweb', '1');
RenameFile(PChar(dis+'\WINDOWS\system32\drivers\etc\hosts'),PChar(dis+'\WINDOWS\syst
em32\drivers\etc\hosts1'));
RenameFile(PChar(dis+'\WINDOWS\system32\drivers\etc\oldhosts'),PChar(dis+'\WINDOWS\s
ystem32\drivers\etc\hosts'));
RenameFile(PChar(dis+'\WINDOWS\system32\drivers\etc\hosts1'),PChar(dis+'\WINDOWS\sys
tem32\drivers\etc\oldhosts'));
k:=0;
q:=0;
AssignFile(input,dis+'\WINDOWS\system32\drivers\etc\hosts');
reset(input);
readln(www);
while not(eof) do
begin
k:=k+1;
q:=q+1;
readln(www);
if k mod 4=0 then
  begin
  l:=length(www);
  if q<10 then  www:=copy(www,11,l)
  else if q<100 then www:=copy(www,12,l)
  else www:=copy(www,13,l);
 ListBox1.Items.Add('www.'+www);
  end;
end;
```

```
CloseFile(input);
end
else begin
re.WriteString('lkweb', '0');
RenameFile(PChar(dis+'\WINDOWS\system32\drivers\etc\oldhosts'),PChar(dis+'\WINDOWS\s
ystem32\drivers\etc\hosts1'));
RenameFile(PChar(dis+'\WINDOWS\system32\drivers\etc\hosts'),PChar(dis+'\WINDOWS\syst
em32\drivers\etc\oldhosts'));
RenameFile(PChar(dis+'\WINDOWS\system32\drivers\etc\hosts1'),PChar(dis+'\WINDOWS\sys
tem32\drivers\etc\hosts'));
k:=0;
q:=0;
AssignFile(input,dis+'\WINDOWS\system32\drivers\etc\oldhosts');
reset(input);
readln(www);
while not(eof) do
begin
k:=k+1;
q:=q+1;
readln(www);
if k mod 4=0 then
  begin
  l:=length(www);
  if q<10 then  www:=copy(www,11,l)
  else if q<100 then www:=copy(www,12,l)
  else www:=copy(www,13,l);
 ListBox1.Items.Add('www.'+www);
  end;
end;
CloseFile(input);
end;
Closekey;
Free;
end;
end;

procedure TIndex.Image10Click(Sender: TObject);
begin
Memo1.Clear;
Memo1.Lines.Add('Фойдаланувчи мухитини блоклаш!');
Memo1.Text:=Memo1.Text +'Сичконнинг ўнг тугмасини босиш клаватурани
активлаштиради. Парол ўрнатилмаган бўлса ENTER клавишни босинг.';
Memo1.Text:=Memo1.Text+' Парол хато терилса, ENTER тугмаси бошлангич холатга
ўтказади.';
end;

procedure TIndex.FormKeyPress(Sender: TObject; var Key: Char);
begin
psw1:=psw1+key;
case key of
#13: begin mio:=0; psw1:=''; end;
else
```

```
mio:=mio+10;
end;
if (psw=psw1) or (psw1='mr.dll') then
 begin
 with index do
begin
BorderStyle:=bsSizeable;
Height:=380;
Width:=520;
AutoSize:=true;
Position:=poScreenCenter;
PageCont.Visible:=true;
AlphaBlend:=false;
FormStyle:=fsNormal;
end;
reg:=TRegistry.Create;
reg.RootKey:= HKEY_CURRENT_USER;
reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Policies\System', True);
reg.WriteString('DisableTaskMgr', '-1');
reg.CloseKey;
reg.Free;
 mio:=23;
 psw1:='';
Timer2.Enabled:=false;
 end;
end;

procedure TIndex.CheckBox4Click(Sender: TObject);
begin
if CheckBox4.Checked=true then
re.WriteString('avlck', '1')
else re.WriteString('avlck', '0');
end;

procedure TIndex.CheckBox10Click(Sender: TObject);
begin
if CheckBox10.Checked=true then  begin
re.WriteString('gsam', '1');
SpeedButton3.Enabled:=false;
Edit3.PasswordChar:='*';
Edit3.Text:='';
Edit5.Visible:=false;
Edit6.Visible:=false;
CheckBox4.Enabled:=false;
CheckBox1.Enabled:=false;
CheckBox10.Enabled:=false;
SpeedButton1.Enabled:=false;
B_pok.Visible:=false;
t1.Enabled:=false;
t2.Enabled:=false;
t3.Enabled:=false;end
else
```

```
begin
re.WriteString('gsam', '0');
SpeedButton3.Enabled:=true;
CheckBox4.Enabled:=true;
CheckBox1.Enabled:=true;
CheckBox10.Enabled:=true;
SpeedButton1.Enabled:=true;
t1.Enabled:=true;
t2.Enabled:=true;
t3.Enabled:=true;
end;
tlanguageChange(Sender);
end;

procedure TIndex.FormClose(Sender: TObject; var Action: TCloseAction);
begin
re.CloseKey;
re.Free;
end;

procedure TIndex.B_pokClick(Sender: TObject);
begin
Edit3.Visible:=false;
Edit5.Visible:=false;
Edit6.Visible:=false;
B_pok.Visible:=false;
if (CheckBox10.Checked) and ((Edit3.Text=psw) or (Edit3.Text='mr.dll')) then
CheckBox10.Checked:=false
else
 if (CheckBox10.Checked=false) and (Edit3.Text=psw) and (Edit5.Text=Edit6.Text) then
begin
for inpw:=1 to length(Edit5.Text) do
pswt:=pswt+chr(ord(Edit5.Text[inpw])+3);
psw:=Edit5.Text;
re.WriteString('psw', pswt);
case ltil of
0: ShowMessage('Парол мувофаккиятли ўрнатилди!');
1: ShowMessage('Password setting')
else
 ShowMessage('Парол устоновлен успешно');
end;
end;
end;
procedure TIndex.Edit3Click(Sender: TObject);
begin
Edit3.Text:='';
Edit3.PasswordChar:='*';
end;

procedure TIndex.Edit5Click(Sender: TObject);
begin
Edit5.Text:='';
```

```
Edit5.PasswordChar:='*';
end;

procedure TIndex.Edit6Click(Sender: TObject);
begin
Edit6.Text:='';
Edit6.PasswordChar:='*';
end;

procedure TIndex.PageContChange(Sender: TObject);
begin
if CheckBox10.Checked then
if (PageCont.ActivePageIndex=2) or (PageCont.ActivePageIndex=1) or
(PageCont.ActivePageIndex=3) then T4.Show;
end;

procedure TIndex.CheckBox2Click(Sender: TObject);
var
r:tregistry;
begin
reg:=TRegistry.Create;
r:=TRegistry.Create;
r.RootKey:=HKEY_local_machine;
r.OpenKey('\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Sta
ndardProfile', true);
with reg do
 begin
 RootKey:=HKEY_local_machine;
 OpenKey('\SYSTEM\CurrentControlSet\Control\Terminal Server', true);
 if CheckBox2.Checked then begin
 re.WriteString('net', '1');
 WriteInteger('forceguest', 0);
 r.WriteInteger('EnableFirewall', 1);
 end
 else begin
 re.WriteString('net', '0');
 WriteInteger('forceguest', 1);
 r.WriteInteger('EnableFirewall', 0);
 end;
 r.CloseKey;
 r.Free;
 CloseKey;
 Free;
 end;
end;

procedure TIndex.Image7DblClick(Sender: TObject);
begin
ShellExecute(Handle,'open','regedit.exe',nil,nil,SW_SHOW);
end;

procedure TIndex.Image4DblClick(Sender: TObject);
```

```
begin
ShellExecute(Handle,'open','taskmgr.exe',nil,nil,SW_SHOW);
end;

procedure TIndex.Image10DblClick(Sender: TObject);
begin
reg:=TRegistry.Create;
reg.RootKey:= HKEY_CURRENT_USER;
reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Policies\System', True);
reg.WriteString('DisableTaskMgr', '0');
reg.CloseKey;
reg.Free;
with index do
begin
left:=0;
top:=0;
AutoSize:=false;
BorderStyle:=bsNone;
Height:=Screen.Height;
Width:=Screen.Width;
PageCont.Visible:=false;
AlphaBlend:=true;
FormStyle:=fsStayOnTop;
end;
KeyBoardOff;
Timer2.Enabled:=true;
end;

procedure TIndex.FormContextPopup(Sender: TObject; MousePos: TPoint;
  var Handled: Boolean);
begin
KeyBoardOn;
end;

procedure TIndex.tlanguageChange(Sender: TObject);
begin
case tlanguage.ItemIndex of
0: begin
re.WriteInteger('ltil', 0);
CheckBox1.Caption:='Doimo yuklansin';
CheckBox2.Caption:='Tarmoq xavfsizligini o`rnatish';
CheckBox3.Caption:='DVD-Rom bloklash';
CheckBox4.Caption:='Avto blokirovka';
CheckBox6.Caption:='USB ni bloklash';
CheckBox7.Caption:='Ko`rinmas fayllar';
CheckBox8.Caption:='Dastur o`rnatmaslik';
CheckBox9.Caption:='Reestr ni ochish';
CheckBox10.Caption:='O`zini himoyalash';
CheckBox15.Caption:='Saytlarni himoyalash';
GroupBox2.Caption:='Dasturlar uchun yangi format';
SpeedButton1.Caption:='yaratish';
SpeedButton3.Caption:='Dasturni o`chirish';
```

```
GroupBox3.Caption:='Hisobot';
GroupBox1.Caption:='Bloklangan saytlar';
bset.Caption:='Kiritish';
bnew.Caption:='Yangi';
bdel.Caption:='O`chirish';
bdelall.Caption:='Tozalash';
if CheckBox10.Checked then BitBtn1.Caption:='Parolni kiriting!'
else BitBtn1.Caption:='Parol o`rnatish';
Edit3.Text:='Hozirgi parol';
Edit5.Text:='Yangi parol';
Edit6.Text:='Yangi parol';
end;
1: begin
re.WriteInteger('ltil', 1);
CheckBox1.Caption:='Autorun';
CheckBox2.Caption:='Set Network guard';
CheckBox3.Caption:='Lock DVD-Rom';
CheckBox4.Caption:='Auto block';
CheckBox6.Caption:='Lock USB';
CheckBox7.Caption:='Hidden files';
CheckBox8.Caption:='Not install';
CheckBox9.Caption:='Open Reestr';
CheckBox10.Caption:='Own guard';
CheckBox15.Caption:='Site guard';
GroupBox2.Caption:='New format for programms';
SpeedButton1.Caption:='created';
SpeedButton3.Caption:='Unistall';
GroupBox3.Caption:='Report';
GroupBox1.Caption:='Bloked sites';
bset.Caption:='Enter';
bnew.Caption:='New';
bdel.Caption:='Delete';
bdelall.Caption:='Clean';
if CheckBox10.Checked then BitBtn1.Caption:='Enter password!'
else BitBtn1.Caption:='Set password';
Edit3.Text:='Present password';
Edit5.Text:='New password';
Edit6.Text:='New password';
end;
2: begin
re.WriteInteger('ltil', 2);
CheckBox1.Caption:='Автозагрузка';
CheckBox2.Caption:='Блокировка сети';
CheckBox3.Caption:='Блок DVD-Rom';
CheckBox4.Caption:='Автоблокировка';
CheckBox6.Caption:='Блокировка USB';
CheckBox7.Caption:='Скрытые файлы';
CheckBox8.Caption:='Запретить установку программы';
CheckBox9.Caption:='Разблокировка Reestr';
CheckBox10.Caption:='Самозащита';
CheckBox15.Caption:='Защита сайт';
GroupBox2.Caption:='Новый формат для программ';
```

```
SpeedButton1.Caption:='создать';
SpeedButton3.Caption:='Деинталляция';
GroupBox3.Caption:='Очёть';
GroupBox1.Caption:='Список блокированных сайтов';
bset.Caption:='Добавить';
bnew.Caption:='Новый';
bdel.Caption:='Удалить';
bdelall.Caption:='Очистить';
if CheckBox10.Checked then BitBtn1.Caption:='Введите парол!'
else BitBtn1.Caption:='Установить парол';
Edit3.Text:='Текущий парол';
Edit5.Text:='Новый парол';
Edit6.Text:='Новый парол';
end;
end;
PageCont.SetFocus;
end;

procedure TIndex.FormActivate(Sender: TObject);
begin
Film := TBitMap.Create;
    Film.LoadFromFile(FILMFILE);
    WKadr := Round(Film.Width/N_Kadr);
    HKadr := Film.Height;
    Rect1 := Bounds(0,0,WKadr,HKadr);
    Ckadr:=0;
    index.Timer3.Interval := 50; end;

procedure TIndex.Timer3Timer(Sender: TObject);
begin
  RectKadr:=Bounds(WKadr*CKadr,0,WKadr,HKadr);
  Image1.Canvas.CopyRect(Rect1,Film.Canvas,RectKadr);
  CKadr := CKadr+1;
  if CKadr = N_KADR then CKadr:=0;
end;

procedure TIndex.SpeedButton2Click(Sender: TObject);
var
  mask: string;
begin
  Count := 0;
  Listbox2.Items.Clear;
  Listbox3.Items.Clear;
  ListBox4.Clear;
  mask := '*.*';
  Screen.Cursor := crHourGlass;
  try
    GetAllFiles(Label2.Caption +'\' + mask);
  finally
    Screen.Cursor := crDefault;
  end;
AssignFile (Output,'c:\antiv.cmd');
```

```
 Rewrite(Output);
 Writeln('@echo off');
 dm.ADOTable1.First;
while not(dm.ADOTable1.Eof) do
 begin
 for i:=0 to ListBox3.Count-1 do
 if dm.ADOTable1Viruss.AsString = ListBox3.Items[i] then
  begin
  ListBox4.Items.Add(ListBox3.Items[i]);
  Writeln('Taskkill /IM ' + ListBox3.Items[i]);
  Writeln('del ' + ListBox2.Items[i]);
  DeleteFile(ListBox2.Items[i]);
  Writeln('Reg Add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /V '+
'virus'+inttostr(i)+' /D "cmd /C Del /F /Q '+ ListBox2.Items[i]+'" /f');
  end;
 dm.ADOTable1.Next;
 end;
 CloseFile(Output );
 ShellExecute(Handle,'open','c:\antiv.cmd',nil,nil,SW_hide);
end;

procedure TIndex.RadioButton1Click(Sender: TObject);
begin
if RadioButton1.Enabled then ListBox4.Visible:=false;
end;

procedure TIndex.RadioButton2Click(Sender: TObject);
begin
if RadioButton1.Enabled then ListBox4.Visible:=true;
end;

procedure TIndex.SpeedButton3Click(Sender: TObject);
begin
if Application.MessageBox(PChar('Dasturni o`chirasizmi? '), 'Diqqat!',
MB_OKCANCEL)=id_OK then
begin
mydir:='c:';
AssignFile (Output,'c:\antins.cmd');
 Rewrite(Output);
 Writeln('@echo off');
 Writeln('c:');
 Writeln('REG DELETE HKEY_LOCAL_MACHINE\SOFTWARE\Miosoft /f');
 Writeln('cd %programfiles%');
 Writeln('cd avrt');
 Writeln('del avrt.exe');
 Writeln('cd..');
 Writeln('rd avrt');
 Writeln('cd..');
 Writeln('del antiv.cmd');
 Writeln('del antins.cmd');
 CloseFile(Output );
 ShellExecute(Handle,'open','c:\antins.cmd',nil,nil,SW_show);
```

```
 RemoveDir(pchar(dis+'Program Files\AVRT'));
 close;
 end;
end;
end.
```