## 12-amaliy mashg‘ulot: Texnik tizimlarda axborot xavfsizligini ta’minlash

12.1. Axborot xavfsizligi muammolari. Axborotlarni himoyalashning tarkibiy qismlari va usullari.

12.2. Parolli himoya va ularning zamonaviy turlari. Parollar asosida autentifikatsiyalash.

12.3. Axborot havfsizligini ta’minlashda biometrik usullardan foydalanish.

12.4. Kompyuter viruslari va ulardan himoyalanish usullari.

### 12.1 Axborot xavfsizligi muammolari. Axborotlarni himoyalashning tarkibiy qismlari va usullari.

XXI asming birinchi o‘n yilligiga kelib axborotning ahamiyati keskin oshib ketdi. Ma’lumotning qimmatbaholigi faqat davlat sirlarini qo‘riqlash nuqtai nazaridangina emas, balki tijorat rivoji sababli ham oshib bormoqda, chunki axborotga ega bo‘lgan mamlakat jahonni boshqaradi.

Yangi innovatsion texnologiyalami loyihalashtirish jarayoniga sarf qili- nayotgan vaqt iqtisodi, telekommunikatsion tizimlar va qurilmalar bozori- dagi sobitqadam sifat o‘zgarishi natijasida raqobatbardoshlik talablari oshib bormoqda. Demak, har qanday tashkilot o‘zini “chaqirilmagan kuzatuvchilardan xalos qilishi zarur bo‘ladi.

Axborot xavfsizligi tahdidlari turli belgilar orqali tavsiflanishi mumkin

• axborot yashirinligini buzish, asosan inson omili yoki muhofaza apparat ta’minoti faoliyatini izdan chiqarish;

• ma’lumotlar mazmunini o‘zgartirishga doir ruxsatsiz faoliyatlar orqali axborot yaxlitligiga zarar yetkazish;

• axborot foydalanuvchilariga kompyuter viruslari orqali tahdidlar;

• axborot xavfsizligiga ichki va tashqi tahdidlar;

• axborot xavfsizligi buzilishida global, hududiy va lokal tarmoqlar tahdidlari.

Axborotlami himoyalashda awalo tashqi tahdidga e’tibor qaratilishi kerak. Quyidagi rasmda axborotdan beruxsat foydalanish mumkin bo‘lgan kanallar ko‘rsatilgan:

Axborot xavfsizligini ta’minlash uchun tashkiliy, texnik va dasturiy vositalardan foydalaniladi.

Tashkiliy vositalar tarkibiga texnik-tashkiliy va huquqiy-tashkiliy tadbir- lami kiritishimiz mumkin. Texnik-tashkiliy tadbirlarda xavfsizlik choralarini ta’minlash uchun ofis xonasidagi kompyuter, telefon, televizor, radio, signa- lizatsiya va shunga o‘xshash axborot chiqish ehtimoli bo‘lgan barcha vositalar ro‘yxatdan o‘tkaziladi.

Texnik vositalar elektron, elektromexanik va boshqa qurilmalardan iborat bo’lib, tizimlami texnik himoyalashda bevosita foydalaniladi. Keng im- koniyatli (0,01 - 1000 MHz) elektromagnit generatorlari kompyuter va boshqa uskunalardan chiquvchi qo‘shimcha to‘lqinlarini sezdirmaslik vazifasini o‘taydi.

Axborotni yashirin olishga mo‘ljallangan mobil aloqa telefonlarini aloqa- dan uzish, elektr tarmog‘idan ma’lumot chiqmasligini ta’minlovchi filtrlar, diktofonlami kuchli elektromagnit to‘lqinlar bilan ishdan chiqaruvchi vositalar qo‘llaniladi

Dasturiy vositalar tarkibiga axborot xavfsizligi, foydalanuvchilar shaxsini identifikatsiyalash, kirish nazorai n o‘matish, ma’lumotlarni yashirin ko‘ri- nishga keltirish kabi vazifalami bajarishga mo‘ljallangan maxsus dasturiy vositalar tizimi kiradi.

Axborotni himoyalovchi dasturiy vositalaming tarkibi quyidagilardan iborat:

• bir necha fayl yoki jildlami yig‘ish orqali ulaming hajmini keskin ka- maytiiib tashqi ta’sirlardan himoyalash dasturlari;

• kompyuter tizimiga beruxsat kirishdan himoyalash dasturlari;

• tizimni viruslardan himoyalashga mo‘ljallangan antivims dasturlari;

• ma’lumotlar yashirinligini ta’minlovchi kdptografik dasturlar.

### 10.2. Parolli himoya va ularning zamonaviy turlari. Parollar asosida autentifikatsiyalash

Login tushunchasi. Login – shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot kommunikatsiya

tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi hisoblanadi.

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

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

Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiyalash bo‘lib, u an’anaviy ko‘p martali parollarni ishlatishi-ga asoslangan. Tarmoqdagi foydalanuvchini oddiy autentifikatsiyalash muolajasini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan foydalanuvchi kompyuter klaviaturasida o‘zining identifiqatori va parolini teradi. Bu ma’lumotlar autentifikatsiya serveriga ishlanish uchun tushadi. Autentifikatsiya serverida saqlanayotgan foydalanuvchi identifiqatori bo‘yicha ma’lumotlar bazasidan mos yozuv topiladi, undan parolni topib foydalanuvchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikatsiya muvaffaqiyatli o‘tgan hisoblanadi va foydalanuvchi legal (qonuniy) maqomini va avtorizatsiya tizimi orqali uning maqomi uchun aniqlangan xuquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Eng keng tarqalgan usul - foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o‘qish va yozishdan himoyalash atributlari o‘rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ro‘yxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir. Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul - foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o‘qish va yozishdan himoyalash atributlari o‘rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ro‘yxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funksiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli urniga uning bir tomonlama funksiyadan foydalanib olingan tasvirini yuborishi shart. Bu o‘zgartirish anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki anim echilmaydigan sonli masalaga duch keladi.

Ko‘p martali parollarga asoslangan oddiy autentifikatsiyalash tizimining bardoshligi past, chunki ularda autentifikatsiyalovchi axborot ma’noli so‘zlarning nisbatan katta bo‘lmagan to‘plamidan jamlanadi. Ko‘p martali parollarning ta’sir muddati tashkilotning xavfsizligi siyosatida belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular luatda bo‘lmasin va ularni topish qiyin bo‘lsin.

Bir martali parollarga asoslangan autentifikatsiyalashda foydalanishga har bir so‘rov uchun turli parollar ishlatiladi. Bir martali dinamik parol faqat tizimdan
bir marta foydalanishga yaroqli. Agar, hatto kimdir uni ushlab qolsa ham parol
foyda bermaydi. Odatda bir martali parollarga asoslangan autentfikatsiyalash tizimi masofadagi foydalanuvchilarni tekshirishda qo‘llaniladi.

Bir martali parollarni generatsiyalash apparat yoki dasturiy usul oqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to‘lov plastik kartochkalariga o‘xshash mikroprotsessor o‘rnatilgan miniatyur qurilmalar ko‘rinishda amalga oshiradi. Odatda kalitlar deb ataluvchi bunday kartalar klaviaturaga va katta bo‘lmagan displey darchasiga ega. Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni
qo‘llashning quyidagi usullari ma’lum:
1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.
2. Legal foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro‘yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish.
3. Foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki
qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

Birinchi usulni amalga oshirish misoli sifatida SecurID autentikatsiyalash texnologiyasini ko‘rsatish mumkin. Bu texnologiya Securitiy Dynamiss kompaniyasi tomonidan ishlab chiqilgan bo‘lib, qator kompaniyalarning, xususan Cusco Systems kompaniyasining serverlarida amalga oshirilgan.

Vaqt sinxronizatsiyasidan foydalanib autentifikatsiyalash sxemasi tasodifiy sonlarni vaqtning ma’lum oraliidan so‘ng generatsiyalash algoritmiga asoslangan. Autentifikatsiya sxemasi quyidagi ikkita parametrdan foydalanadi:

• har bir foydalanuvchiga atalgan va autentifikatsiya serverida hamda foydalanuvchining apparat kalitida saqlanuvchi noyob 64-bitli sondan iborat maxfiy kalit; joriy vaqt qiymati.

Autentifikatsiyaning bu sxemasi bilan yana bir muammo boliq. Apparat kalit generatsiyalagan tasodifiy son katta bo‘lmagan vaqt oralii mobaynida haqiqiy parol hisoblanadi. SHu sababli, umuman, qisqa muddatli vaziyat sodir bo‘lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga
ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya
sxemasining eng zaif joyi hisoblanadi.

Bir martali paroldan foydalanuvchi autentifikatsiyalashni amalga oshiruvchi yana bir variant-«so‘rov-javob» sxemasi bo‘yicha autentifikatsiyalash.

Foydalanuvchi tarmoqdan foydalanishga uringanida server unga tasodifiy son ko‘rinishidagi so‘rovni uzatadi. Foydalanuvchining apparat kaliti bu tasodifiy sonni, masalan DES algoritmi va foydalanuvchining apparat kaliti xotirasida va serverning ma’lumotlar bazasida saqlanuvchi maxfiy kaliti yordamida rasshifrovka qiladi. Tasodifiy son - so‘rov shifrlangan ko‘rinishda serverga qaytariladi. Server ham o‘z navbatida o‘sha DES algoritmi va serverning ma’lumotlar bazasidan olingan foydalanuvchining maxfiy kaliti yordamida o‘zi generatsiyalagan tasodifiy sonni shifrlaydi. So‘ngra server shifrlash natijasini apparat kalitidan kelgan son bilan taqqoslaydi. Bu sonlar mos kelganida foydalanuvchi tarmoqdan foydalanishga ruxsat oladi. Ta’kidlash lozimki, «so‘rov-javob» autentifikatsiyalash sxemasi ishlatishda vaqt sinxronizatsiyasidan foydalanuvchi autentifikatsiya sxemasiga qaraganda murakkabroq.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro‘yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo‘linuvchi ro‘yxati maxfiy parollar ketma-ketligi yoki to‘plami bo‘lib, har bir parol faqat bir marta ishlatiladi. Ushbu ro‘yxat autentifikatsion almashinuv taraflar o‘rtasida oldindan taqsimlanishi shart. Ushbu usulning bir variantiga binoan so‘rov-javob jadvali ishlatiladi. Bu jadvalda autentifikatsilash uchun taraflar tomonidan ishlatiluvchi so‘rovlar va javoblar mavjud bo‘lib, har bir juft faqat bir marta ishlatilishi shart.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan
foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari
mavjud:

• o‘zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;
• bir tomonlama funksiyaga asoslangan parollar ketma-ketligi. Ushbu usulning mohiyatini bir tomonlama funksiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o‘zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.


Axborot havfsizligini ta’minlashda biometrik usullardan foydalanish.
Hozirgi vaqtga kelib, kompyuter-kommunikatsiya texnologiyalari kundan-kunga tez rivojlanib bormoqda. SHu sababli ham kompyuter texnologiyalari kirib bormagan sohaning o‘zi qolmadi, desak xato bo‘lmaydi. Ayniqsa ta’lim, bank, moliya tizimlarida ushbu zamonaviy texnologiyalarni qo‘llash yuqori samara bermoqda. SHu bilan birga axborot havfsizligiga bo‘lgan tahdid ham tobora kuchayib borayotgani hech kimga sir emas. Demak, hozirgi davrning eng dolzarb muammolardan biri axborot havfsizligini ta’minlashdan iborat.

Hozirga qadar tizimga ruxsatsiz kirishni taqiqlashning eng keng tarqalgan usuli sifatida «parol» qo‘yish prinsipi hisoblanib kelmoqda. CHunki ushbu usul juda sodda, foydalanish uchun qulay va kam harajat talab etadi. LMaxsulot, hozirga kelib «parol» tizimi to‘laqonli o‘zini oqlay olmayapti. YA’ni ushbu usulning bir qator kamchiliklari ko‘zga tashlanib qoldi.

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

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

Uchinchidan, agar foydalanuvchi parol qo‘yishda murakkab, uzundan-uzoq belgilardan foydalanadigan bo‘lsa, uning o‘zi ham ushbu parolni esidan chiqarib qo‘yishi extimoldan holi emas va nihoyat, hozirda ixtiyoriy parollarni buzuvchi dasturlarning mavjudligi ko‘zga tashlanib qoldi.

Yuqoridagi kamchiliklardan kelib chiqqan holda aytish mumkinki, axborotni himoyalashning parolli prinsipidan foydalanish to‘la samara bermayapti. SHu sababli ham hozirda axborotlardan ruxsatsiz foydalanishni cheklashning biometrik usullarini qo‘llash dunyo bo‘yicha ommaviylashib bormoqda va ushbu yo‘nalish biometriya nomi bilan yuritilmoqda.

Biometriya - bu insonning o‘zgarmaydigan biologik belgilariga asosan aynan o‘xshashlikka tekshirishdir. Hozirda biometrik tizimlar eng ishonchli himoya vositasi hisoblanadi va turli xil maxfiy ob’ektlarda, muhim tijorat axborotlarini himoyalashda samarali qo‘llanilmoqda.

Hozirda biometrik texnologiyalar insonning quyidagi o‘zgarmas biologik belgilariga asoslangan: barmoqning papillyar chiziqlari, qo‘l kaftining tuzilishi, ko‘zning kamalak qobig‘i chiziqlari, ovoz parametrlari, yuz tuzilishi, yuz termogrammasi (qon tomirlarining joylashishi), yozish formasi va usuli, genetik kodi fragmentlari. Insonning ushbu biologik belgilaridan foydalanish turli xil aniqliklarga erishishga imkon beradi. Biz ushbu maqolada hozirda keng qo‘llanilayotgan barmoq izlari va qo‘l kaftining tuzilishi bo‘yicha insonni tanish masalalariga to‘xtalib o‘tishni lozim topdik.

Ushbu qurilmalar tez ishdan chiquvchi hisoblanadi. SHu sababli foydalanuvchidan avaylab ishlatish talab etiladi. Ushbu qurilmaga tushgan chang, turli xil chiziqlar shaxsni aniqlashda xatolikka olib keladi, ya’ni foydalanuvchining tizimga kirishiga to‘sqinlik qiladi. Bundan tashqari, optik skanerda tasviri olingan barmoq izi foydalanuvchi terisining holatiga bog‘liq. YA’ni, foydalanuvchi terisining yog‘liligi yoki quruqligi shaxsni aniqlashga xalaqit beradi. Barmoq izlari bo‘yicha identifikatsiyalashning ikkinchi texnologiyasi elektron skanerlarni qo‘llashdir.

Ushbu qurilmadan foydalanish uchun foydalanuvchi 90 ming kondensator plastinkalaridan tashkil topgan, kremniy moddasi bilan qoplangan mahsus plastinkaga barmog‘ini qo‘yadi. Bunda o‘ziga xos kondensator hosil qilinadi. Kondensator ichidagi elektr maydon potensiali plastinkalar orasidagi masofaga bog‘liq. Ushbu maydon kartasi barmoqning papillyar chizmasini takrorlaydi. Elektron maydon hisoblanadi, olingan ma’lumotlar esa, katta aniqlikka ega sakkiz bitli rastrli tasvirga aylantiriladi.

Ushbu texnologiyaning e’tiborli tomoni shundaki, foydalanuvchi terisining har qanday holatida ham barmoq izi tasviri yuqori aniqlikda hosil qilinadi. Ushbu tizim foydalanuvchi barmog‘i kirlangan taqdirda ham tasvirni aniq oladi. Bundan tashqari qurilma hajmining kichikligi sababli, ushbu qurilmani hamma joyda ishlatish mumkin. Ushbu qurilmaning kamchilik tomonlari sifatida quyidagilarni keltirish mumkin: 90 ming kondensatorli plastinkani ishlab chiqarish ko‘p harajat talab etadi, skanerning asosi bo‘lgan kremniy kristali germetik (zich yopiladigan) qobiqni talab etadi. Bu esa, qurilmani ishlatishda turli xil cheklanishlarni yuzaga keltiradi. Nihoyat, kuchli elektromagnit nurlanishi vujudga kelganda elektron sensor ishlamaydi.

Barmoq izi buyicha identifikatsiyalashning uchinchi texnologiyasi WhoVisionSustems kompaniyasi tomonidan ishlab chiqarilgan TactileSense skanerlaridir. Ushbu skanerlarda maxsus polimer material ishlatilgan bo‘lib, terining bo‘rtib chiqqan chiziqlari

va botiqlari orasida hosil bo‘lgan elektr maydonni sezish orqali tasvir hosil qilinadi. Umuman olganda ushbu skanerlarning ishlash prinsipi elektron skanerlar ishlash prinsipi bilan deyarli bir xil. Faqat ushbu qurilmalarning quyidagi afzalliklarini sanab o‘tishimiz mumkin: qurilmani ishlab chikarish bir necha yuz barobar kam harajat talab etadi, qurilma avvalgi qurilmadan mustahkam va foydalanishda hech qanday cheklanishlar yuzaga kelmaydi.

Insonining qo‘l kafti tuzilishiga ko‘ra identifikatsiyalashning ikki xil usuli mavjud. Birinchi usulda qo‘l kaftining tuzilishidan foydalaniladi. Buning uchun maxsus qurilmalar ishlab chiqarilgan bo‘lib, ushbu qurilma kamera va bir nechta yorituvchi diodlardan tashkil topgan. Ushbu qurilmaning vazifasi qo‘l kaftining uch o‘lchovli tasvirini hosil qilishdan iborat. Keyinchalik ushbu hosil qilingan tasvir ma’lumotlar bazasiga kiritilgan tasvir bilan solishtiriladi. Ushbu qurilma yordamida identifikatsiyalash yuqori aniqlikda amalga oshiriladi. LMaxsulot kaft tasvirini oluvchi skaner o‘ta nozik ishlangan bo‘lib, ushbu qurilmadan foydalanish noqulayliklar tug‘diradi.

Qo‘l kafti tuzilishiga ko‘ra identifikatsiyalashning ikkinchi texnologiyasi esa, kaftning termogrammasini aniqlashga asoslangan. Qo‘l kaftida juda ko‘p qon tomirlari mavjud bo‘lib, ushbu qon tomirlari har bir insonda, hattoki egizaklarda ham turlicha joylashadi. Ushbu qon tomirlarining joylashish tasvirini olish uchun maxsus infraqizil nurli fotokameradan foydalaniladi. Ushbu hosil bo‘lgan tasvir kaft termogrammasi deb ataladi. Ushbu usulning ishonchliligi juda ham yuqori. Bu usulning vujudga kelganiga ko‘p vaqt bo‘lmaganligi sababli hali keng tarqalib ulgurmagan.

Keltirib o‘tilgan barcha biometrik usullar axborotni himoya qilishda keng qo‘llanilmoqda. Ushbu himoya tizimining ishonchliligi shundaki, tizimda foydalanilayotgan insonning biologik belgilari hech qachon o‘zgarmaydi, biron-bir jaroxat etgan taqdirda ham qayta tiklanadi.

YUqorida biz insonning biologik belgilariga asosan shaxsni tanish maqsadida barmoq izi va qo‘l kaftining tasvirini hosil qilish texnologiyalari bilan tanishib chiqdik. Endigi masala hosil qilingan tasvirni ma’lumotlar bazasida saqlanayotgan tasvir bilan taqqoslash va shaxsni aniqlash algoritmi bilan bog‘liq.

Biz ushbu masalada hosil qilingan barmoq izidan foydalangan holda shaxsni aniqlash algoritmini keltirib o‘tishga harakat qilamiz.

Yuqorida ta’kidlaganimizdek, birinchi navbatda ixtiyoriy qurilma orqali barmoq izi tasviri hosil qilinadi. Qolgan bosqichlarni quyidagi ketma-ketlik orqali bayon qilishga harakat qilamiz:

1) Tasvirga boshlang‘ich ishlov berish – bunda hosil qilingan tasvir Binar tasvirga o‘tkaziladi, ya’ni, tasvirdagi faqat barmoq izining chiziqlari olib qolinadi va tasvirning markazi (og‘irlik markazi) aniqlanadi;

2) Tasvirdagi o‘ziga xos belgilarni aniqlash – bunda tasvirning markazidan turli xil radiusli bir nechta aylanalar chiziladi (aylanalar qanchalik ko‘p bo‘lsa, aniqlik shunchalik ortadi). Natijada aylanalar hosil qilingan tasvir chiziqlarining bir nechta nuqtalarida kesishadi. Ushbu kesishish nuqtalari shartli ravishda A1, A2, ..., An (birinchi aylana), B1, B2, ..., Bm (ikkinchi aylana), C1, C2, ..., Ck (uchinchi aylana) harflari yordamida belgilanadi. Har bir aylanadagi kesishish nuqtalarini birlashtirish orqali A1,A2,...An, B1,B2...Bm, C1,C2...Ck ko‘pburchaklar hosil qilinadi. Ushbu hosil qilingan ko‘pburchaklar perimetrlari (P1, P2, P3) hisoblanadi.

3) Olingan tasvirni ma’lumotlar bazasida saqlanayotgan tasvir bilan solishtirish – bunda yuqoridagi bosqichda olingan natijalar: R1, R2, R3 radiusli aylanalardagi kesishishlar soni n, m, k; aylanalarda hosil qilingan ko‘pburchaklar perimetri P1, P2, P3 lar ma’lumotlar bazasida saqlanayotgan ushbu kattaliklar bilan taqqoslanadi. Ushbu kattaliklar o‘zaro mos tushsagina shaxs tasdiqlanadi.

Ushbu keltirilgan shaxsni tanish algoritmi ustida respublikamizdagi bir nechta olimlar guruhi ish olib bormoqdalar va ushbu sohada ijobiy natijalarga erishilmoqda.

## 10.4. Kompyuter viruslari va ulardan himoyalanish usullari.

Virus tushunchasi. Virus(virus) inglizcha “yuqumli boshlanish”, “yomon boshlanish – buzuvchi boshlanish”, “yuqumli kasal” degan manolarni anglatadi.

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

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

Agar bir dona virusning ko‘payishiga 30 sekund vaqt ketsa, bir soatdan keyin bu 1000000000 dan ortib ketishi mumkin. Aniqroi kompyuter xotirasidagi bo‘sh joylarni band qilishi mumkin.

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

Malumotlarni virus qanday yo‘q qilishi mumkin degan savolga shunday javob berish mumkin:

Virus nusxalari boshqa dasturlarga tez ko‘payib o‘tib oladi;

Kalendar bo‘yicha 13-sana juma kunga to‘g‘ri kelsa hamma hujjatlarni yo‘q qiladi. Buni hammaga ma’lum «Jerusalem» («Time» virusi ham deb ataladi) virusi juda «yaxshi» amalga oshiradi. Ko‘p xollarda bilib bo‘lmaydi, virus qaerdan paydo bo‘ldi.

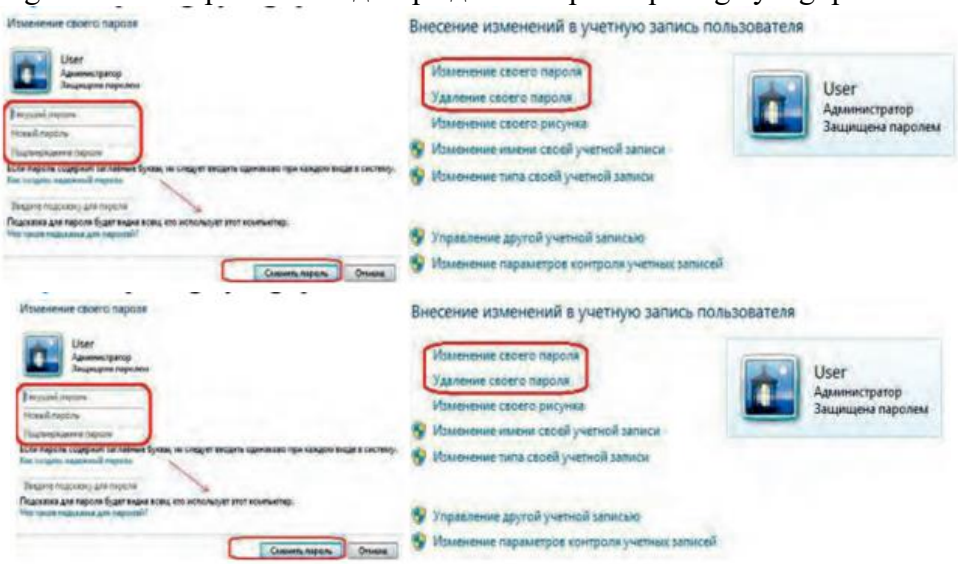
Virusni aniqlanishi shundaki, u kompyuter sistemasida joylashib va ko‘payib borishiga bog‘liq. Misol uchun, nazariy jihatdan operatsion sistemada virus davolab bo‘lmaydi. Bajaruvchi kodning sohasini tuzish va o‘zgartirish ta`qiqlangan sistema misol bo‘lishi mumkin.

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

**Amaliy ishlar bajarish.**

**1-mashq. Windows 7 operatsion tizimini himoyalash.**

1. Пуск tugmasini faollashtirish orqali Панель управления bo‘limi- dan Учетные записы пользователей и сем... qismiga kiriladi va u yerdan Учетные записы пользователей bandi faollashtiriladi;
2. Внесение изменений в учетную запись пользователя oynasidan Изменение своего пароля muloqot darchasiga kiriladi;
3. Agar kompyuterga oldin parol qo‘yilgan bo'Isa, Текущей пароль qa- toriga oldingi parol kiritilib, so‘ngra Новый пароль va Подтверждение пароля qatoriga yangi parol kiritiladi:

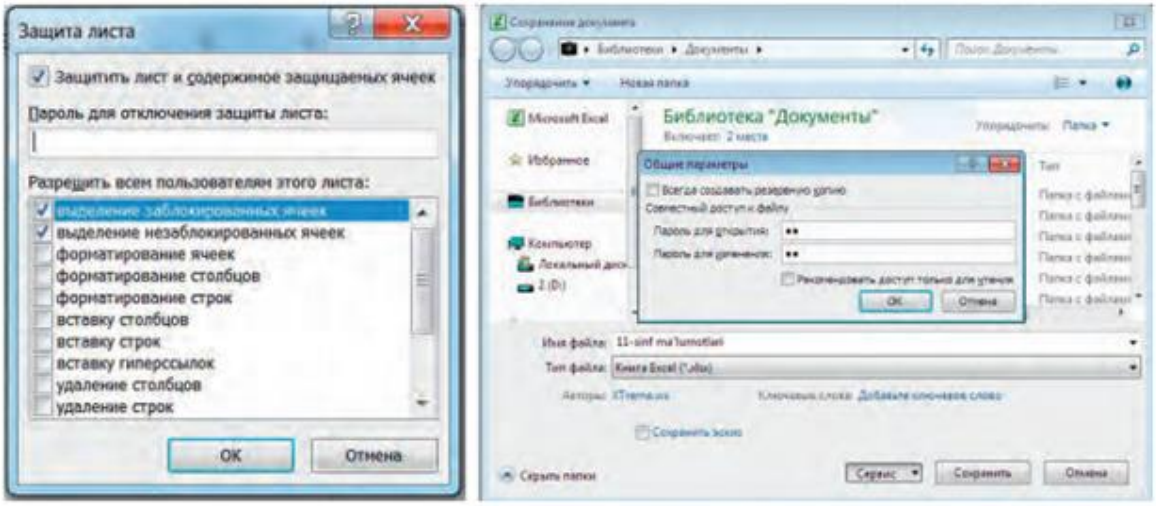


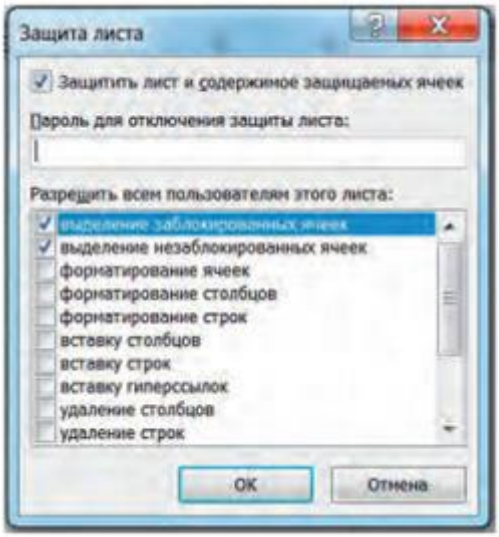

Ushbu ketma-ketlik bajarilgandan so‘ng, kompyuter ishga tushirilganda yangi parol bilan kirish zarur bo‘ladi.

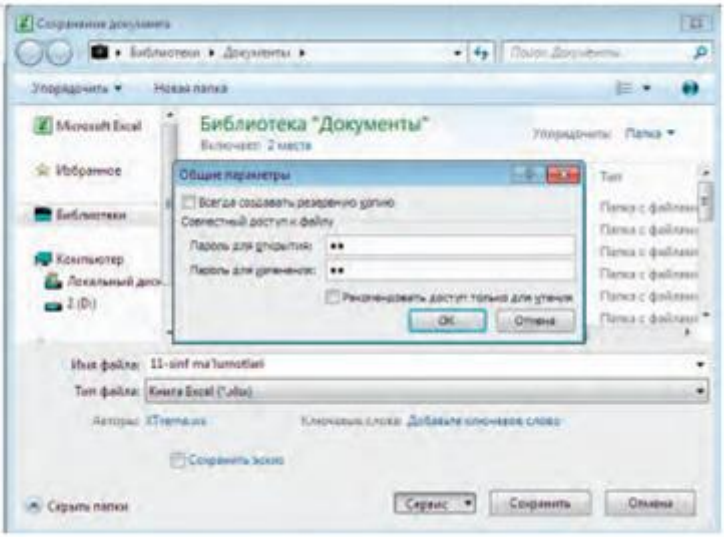
**2- mashq. MS Excel 2010 elektron jadvalida ma’lumotlami himoyalash.**

1. MS Excel 2010 ning menyusida Рецензирование tasmasi faollashtiriladi;
2. Tasmaning Защитить лист bandi bosiladi. Natijada ekranda Защита листа muloqot oynasi paydo bo'ladi. Hosil bo‘lgan oynaning Пароль для отключения защиты листа qatoriga parol kiritiladi;

Himoyalangan varaqdagi ma’lumotlami o‘zgartirish uchun MS Excel 2010ning menyusidan ецензирование tasmasi faollashtiriladi. Tasmaning Изменение qismidan Снять Защитить листа bandi tanlanadi. Natijada Снять Защитить листа muloqot oynasi paydo bo‘ladi. Ushbu hosil bo‘lgan oynaning ma’lumot kiritish qatoriga oldin himoyalangan parol kiritiladi.






**Topshiriqlar.**

1. Axborot xavfsizligiga asosiy tahdidlar nimalardan iborat?
2. MS Power Pointda yaratilgan taqdimotlami himoyalang.
3. Kompyuterni zararlovchi virus turlari haqida ma’lumot bering.
4. Hozirda qўllanilayotgan antiviruslar haqida ma’lumot bering.
5. Viruslarni kompyuterga tushish yўllarini tushuntirib bering.
6. Antivirus dasturlari turlarini bir-biridan farqini tushuntiring.
7. Fayl va disklarda kompyuter viruslari mavjudligini tekshirish.
8. Elementlarni, uzel(tugun) va qurilmalarda kompyuter viruslari mavjudligini tekshirish.
9. Virus nima va uning bajaradigan vazifasi?
10. Viruslar kompyuterda qanday paydo bo‘ladi?
11. Viruslarning qanday turlarini bilasiz?
12. Kompyuterda viruslar mavjudligi qanday aniqlanadi?
13. Antivirus dasturlarining qanday turlarini bilasiz?
14. Kompyuter viruslaridan himoyalanishda ehtiyotkorlik choralari nimalardan iborat?