53–54-darslar. AXBOROT XAVFSIZLIGI VA UNI TA'MINLASH

Umumjahon axborot globallashuvi jarayonlari axborot-kommunikatsiya texnologiyalarini nafaqat mamalakatlar iqtisodiyoti va boshqa sohalarida joriy etishni, balki axborot tizimlari xavfsizligini ta'minlashni ham taqazo etmoqda. Kompyuter va axborot texnologiyalarining rivojlanishi, ularning hayotimiz har bir jabhasiga kirib borishi insonlarda axborotga bo'lgan talabning ortishi hamda axborot muhimlik darajasining o'sishiga olib kelmoqda. Natijada, axborotni qo'lga kiritish bo'yicha xatti-harakatlar miqdori ortib bormoqda.

Kompyuter texnologiyalarining rivojlanishi bilan parallel ravishda kompyuter tizim va tarmoqlari buzg'unchi, yomon niyatli shaxslar qurboniga aylanmoqda. Qasddan qilingan bunday tahdidlardan tashqari, bilmasdan qilingan (yo'l qoyilgan) xatti-harakat (xatolik)lar ham kerakli ma'lumotning yo'qolishi, buzilishiga sabab bo'lmoqda.

TAYANCH TUSHUNCHALAR

Xavf – nojo'ya harakat yuz berishi ehtimolligi, ya'ni bevosita yoki bilvosita zarar yetkazadigan ko'ngilsiz hodisa.

Tahdid – mavjud xafv natijasida yuz berishi mumkin bo'lgan hujum turi. U, asosan, tizim kamchiliklarini o'rganish natijasida kelib chiqadi.

Hujum – buzg'unchining qandaydir maqsad yo'lida mavjud himoyalash tizimlarini buzishga qaratilgan harakati. Bunda kutilgan tahdid amalga oshiriladi.

Xavfsizlik – xavfdan holi, turli hujum va baxtsiz hodisalar tufayli buzilishdan himoyalangan holat.

Bugungi kunda insonlar barcha xatti-harakatlari kompyuter texnologiyalari bilan chambarchas bog'liqligi sababli ham biz har doim axborot xavfsizligi qoidalariga qat'iy rioya qilishimiz zarur. Eng muhim vazifalardan biri – bu davlat, harbiy, huquqiy va tibbiy sohalarga oid sirlarni, inson shaxsini tasdiqlovchi hujjatlar, ulardagi ma'lumotlarni, turli saytlarda ro'yxatdan o'tish vaqtida qo'lga kiritilgan login va parollarni himoya qilishdir.

Siz *xavf, tahdid, hujum, xavfsizlik* kabi tushunchalarni eshitgandirsiz, lekin ularning axborotga nisbatan asl mohiyatini anglamagan bo'lishingiz mumkin.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

Bugungi kunda axborot xavfsizligi bilan bog'liq tahdidlar kelajakda sodir bo'lishi mumkin bo'lgan xavflardan keladigan zararni kamaytirishga yo'naltirilgan.

Xavflarni boshqarish 3 bosqichdan iborat:

1) ehtimoli mavjud xavflarni aniqlash;

2) xavfni kamaytirish bo'yicha chora-tadbirlarni tanlash va qo'llash;

3) ikkala bosqichni tekshirish maqsadida tajribada xavfni amalga oshirish va xavf zararini baholash.

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 u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatishi ta'kidlangan.

Bunday nojo'ya ta'sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalari, uning foydalanuvchilari hamda axborotni muhofaza qilishni qo'llab-quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin.

Bundan bir necha yil avval xavf faqat maxfiy (konfidensial) xabar va hujjatlarni o'g'irlash yoki nusxa olishdangina iborat bo'lgan bo'lsa, hozirgi zamonaviy xavf esa kompyuter ma'lumotlari to'plami, elektron ma'lumotlar, elektron resurslardan ularning egasidan ruxsat so'ramasdan foydalanishni tashkil etmoqda. Bulardan tashqari, bu harakatlardan moddiy foyda olishga intilish ham rivojlanib bormoqda.

Axborot xavfsizligiga:

- axborotni o'g'irlash;
- axborot mazmunini buzish;
- axborotni egasi iznisiz o'zgartirib olish;
- tarmoq va serverlardan beruxsat foydalanish;
- tarmoqqa tajovuz qilish;
- avval qo'lga kiritilgan uzatmalarni qayta uzatish;
- axborotga daxldorlikdan bo'yin tovlash;
- jo'natmalarni ruxsat etilmagan yo'l orqali jo'natish;
- xotiraning viruslanishi kabilarni kiritish mumkin.

TAYANCH TUSHUNCHALAR

Axborot xavfsizligi — ma'lumotlarning buzilishi, o'zgartirilishi yoki yo'qotilishiga sabab bo'luvchi har qanday xatti-harakatlardan axborotlarni himoya qilish va axborot foydalanuvchilariga yetkazilishi mumkin bo'lgan zararning oldini olish

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

Axborot xavfsizligi xususiyatlari

Virtual makonda axborot xavfsizligini ta'minlashning 3 ta jihati uchun axborotni himoyalashning turli usullaridan foydalaniladi. Tasavvur qiling, siz virtual makonni faqat veb-sahifalarni ko'rish maqsadida ishlatyapsiz. U holda siz antivirus dasturlaridan axborotlarni himoyalash maqsadida foydalanishingiz, shu bilan Internetda ishlash qoidalariga to'liq amal qilishingiz kerak bo'ladi.

TAYANCH TUSHUNCHALAR

Axborot xavfsizligini ta'minlash – foydalanuvchi axborotlarini himoyalashga qo'yilgan me'yor va talablarning bajarilishi.

Axborotlarni muhofaza qilish – axborot xavfsizligini, ya'ni ma'lumotlarni o'g'irlash, yo'qotish, soxtalashtirish, qalbakilashtirsh, ulardan ruxsatsiz foydalanish va ko'paytirishning oldini olishni ta'minlashga qaratilgan chora-tadbirlar majmuasi.

Amaliyotda axborotni muhofaza qilish axborotlarni kiritish, saqlash, tahrirlash va uzatish jarayonida foydalaniladigan ma'lumotlar maxfiyligi, yaxlitligi va mavjudligi ta'minlash bilan izohlanadi. Axborot xavfsizligini ta'minlovchi har bir element (har qanday xavfsizlik nazorati) birgalikda *CIA Triad* deb nomlanuvchi ***maxfiylik*** (confidentiality), ***yaxlitlik*** (integrity) va ***mavjudlik*** (availability) shartlaridan biriga yoki bir nechtasiga erishish uchun ishlab chiqilishi lozim.

Maxfiylik choralari ma'lumotlarning ruxsatsiz oshkor qilinishidan himoya qilishga mo'ljallangan. Shaxsiy ma'lumotlar maxfiyligi, ularni faqat ish vazifalarini bajarish uchun ushbu ma'lumotlarga muhtoj shaxslargina ko'rishi yoki olishining ta'minlanishi maxfiylik prinsipining asosiy maqsadi sanaladi.

Axborotning maxfiyligi (konfidensialligi – ruxsatsiz o'qishning mumkin emasligi). Maxfiy yoki sirli axborotning taqdim etilishi, oshkor bo'lishi yoki unga murojaat qilinishi mumkin bo'lmagan shaxslarga ruxsatsiz tarqalishi natijasida buziladi.

Axborotning maxfiyligi kriptografik himoya usullaridan biri bo'lmish shifrlash usullari asosida amalga oshiriladi. Shifrlash usullari yordamida ochiq ma'lumot yashiringan ko'rinishdagi shifrmatn holatiga aylanadi. Bu esa uni ruxsatsiz foydalanishdan asraydi. Masalan, noutbukni o'g'irlash va undagi fayl yoki dasturlardan noqonuniy nusxa ko'chirish, parolni o'g'irlash, elektron pochta xabarlarini noto'g'ri (yuborilishi kerak bo'lmagan) shaxslarga yuborish.

Yaxlitlik (butunlik) ma'lumotlarni ruxsatsiz o'zgartirishlar (masalan, qo'shish, o'chirish yoki o'zgartirish)dan himoya qilish uchun mo'ljallangan. Axborotning yaxlitligi ma'lumotni uzatish davomida unga o'zgartirish kiritilgan yoki kiritilmaganligi bilan aniqlanadi. Ya'ni ma'lumot yomon niyatli (buzg'unchi) shaxs tomonidan ataylab o'zgartirilishi (almashtirish, o'chirib tashlash) natijasida buzilishi mumkin. Bunday xavf, ayniqsa, axborotni uzatish tizimlari, kompyuter tarmoqlari, radiotexnika tizimlari uchun dolzarbdir. Masalan, elektron pochta xabarlari yoki boshqa elektron hujjatlar mazmunini o'zgartirib yuborish.

> Axborotning yaxlitligi (butunligi – ruxsatsiz yozishning mumkin emasligi)
>
> uning sifati va ishonchliligi buzilishiga, to'liq yo'qotilishiga yoki axborotning o'zgarishiga yo'naltirilgan ta'sirlar natijasida buziladi.

Mavjudlik choralari qo'llab-quvvatlash tizimlari ishini himoya qilish, foydalanuvchilarga kerak bo'lgan vaqt (yoki davr)da ma'lumotlarning to'liq mavjudligini ta'minlashga mo'ljallangan. Qaror qabul qilish uchun zarur bo'lgan vaqtda ma'lumotlarning ishlashini, ya'ni ulardan foydalanish mumkinligini ta'minlash mavjudlik prinsipining asosiy maqsadi sanaladi. Masalan, kompyuterning buzilishi yoki Internet orqali zararli dasturlarning ommaviy hujumga uchrashi natijasida veb-sayt foydalanuvchilari so'rovlarga javob berilmasligi yoki axborotlardan istalgan vaqtda foydalanish imkoniyatining mavjud bo'lmasligi. Deylik, 1-foydalanuvchi tizimning qaysidir xizmatidan foydalanish uchun so'rov yuborsa, 2-foydalanuvchi esa bu xizmatdan foydalanishni bloklab qo'ygan bo'lsa, 1-foydalanuvchi tizimdan o'sha xizmat uchun rad javobini oladi.

Xavfsizlik uchligi (triadasi)ning mazkur 3 ta prinsip (qoida)larini samarali bajarish axborot xavfsizligi nuqtayi nazaridan ideal natijani yaratadi.

Birorta tashkilot o'z biznes operatsiyalari davomida foydalanadigan maxfiy ma'lumotlarni oladi yoki yaratadi. Ma'lumotlar maxfiy bo'lganligi sababli ular tashkilot xodimi uchun faqat o'z vakolat doirasidagi topshiriqlar (xizmat vazifalari)ni bajarish vaqtidagina mavjud bo'lishi, unga ruxsatsiz kirishdan himoyalangan bo'lishi kerak. Bunday holat maxfiylik xususiyatiga rioya qilishga misol bo'la oladi.

Topshiriqlarni bajarish vaqtida xodim tashkilot maxfiy ma'lumotlariga murojaat qilishi zarurati tug'iladi. Topshiriq o'z vaqtida bajarilishi, kompaniya ma'lumot ustida yana qayta ishlashni davom ettira olishi uchun xodim maxfiy ma'lumotga o'sha paytning o'zida tez (onlayn) va oson kirishi, undan foydalana olishi ta'minlangan bo'lishi kerak. Buni mavjudlik xususiyatining ta'minlanishiga misol tariqasida ko'rsatish mumkin.

Ko'pincha tashkilotlar biznes qarorlarni qabul qilish yoki investitsiyalarga ta'sir etuvchi hisob-kitoblarni amalga oshirishda maxfiy ma'lumotlardan foydalanadi. Bunday vaqtlarda to'g'ri, aniq hisob-kitob va natijalarga asoslangan ma'lumotlarga tayanib qaror qabul qilish juda

muhim sanaladi. Ma'lumotlar o'zgartirilmaganligi uchun hisob-kitoblarni amalga oshirish va qarorlarni qabul qilishda ularga ishonchni ta'minlash yaxlitlik xususiyatiga mos keladi.

Ushbu 3 ta xususiyat axborotni himoyalashning asosiy tashkil etuvchilari sanaladi. ***Axborotni himoyalash*** deganda, asosan, shu uchta xususiyatni ta'minlash tushuniladi. Ammo ular to'liq bajarilishi uchun bir nechta ishlarni bajarish talab etiladi. Boshqacha aytganda, ushbu uchta xususiyatni bajarishdan avval ayrim amaliyotlarni bajarishga to'g'ri keladi.

IDENTIFIKATSIYA → **AUTENTIFIKATSIYA** → **AVTORIZATSIYA**

1-rasm. Foydalanishni boshqarish

IDENTIFIKATSIYA

- foydalanuvchi tizimga o'zini tanitish jarayoni bo'lib, unda foydalanuvchi nomi (login), maxsus shaxsiy karta yoki biometrik xususiyatlardan foydalanishi mumkin.

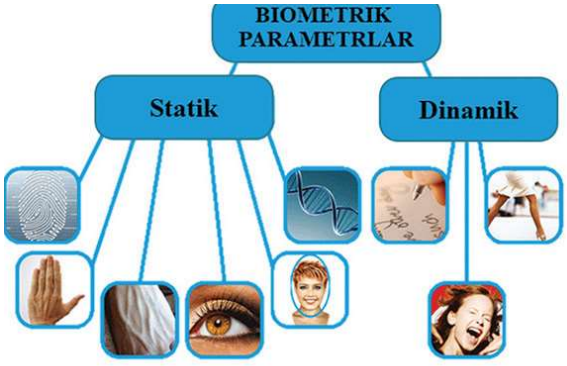
AUTENTIFIKATSIYA

- foydalanuvchi haqiqiyligini tekshirish jarayoni bo'lib, jarayon natijasida foydalanuvchi tizimdan foydalanish uchun ruxsat oladi yoki olmaydi.

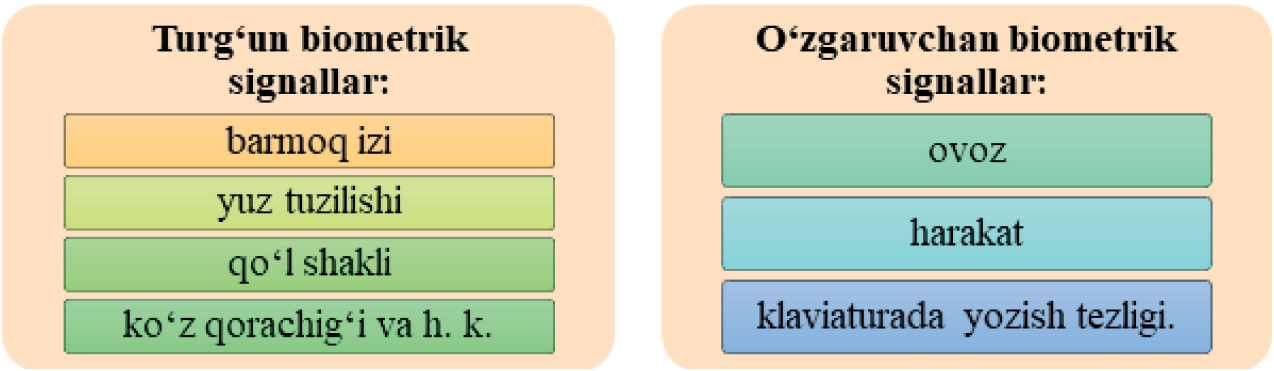
AVTORIZATSIYA

- foydalanuvchiga tizim tomonidan berilgan huquqlar to'plami bo'lib, foydalanuvchi tizim doirasida bajarishi mumkin bo'lgan vazifalarni belgilaydi.

Biometrik ma'lumotlar deb ataluvchi xavfsizlik tizimlari ham mavjud. Bu tizimda ishlatiluvchi ma'lumotlar insonning o'zgarmas xususiyatlariga asoslanganligi sababli biometrik ma'lumotlarni yo'qotib yoki soxtalashtirib bo'lmaydi. Biometrik ma'lumotlar asosida autentifikatsiyalash usuli eng ishonchli usullardan sanaladi.



Biometrik ma'lumotlar autentifikatsiya vositasi bo'lib, u foydalanuvchi barmoq izlarini aniqlash, ko'zining yoy va to'r pardasi orqali tanish, nutq xususiyatlariga ko'ra tanish, yuz shaklini aniqlash, kafti xususiyatlariga ko'ra tanish kabi shaxsiy va farqli alomatlarini o'z ichiga oladi. Biometrik ma'lumotlarning asl nusxalari raqamli ko'rinishda kompyuter yoki mobil qurilmalar xotirasida saqlanadi.



2-rasm. Biometrik ma'lumot turlari

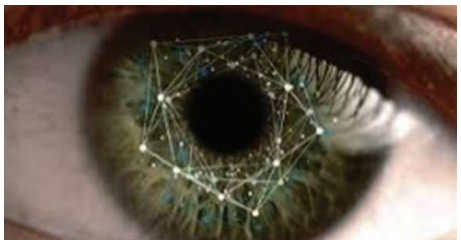
Barmoq izlari (daktiloskopiya) orqali identifikatsiyalash

Hozirda identifikatsiyalashning eng keng qo'llanilayotgan biometrik usuli – barmoq izlarini aniqlashdir. Mazkur usul sud ekspertizasida keng qo'llaniladi, chunki har bir kishining barmoq izlari o'zigagina xos jihatlarga ega. Optik barmoq izlari skanerlari noutbuk, mobil telefon, sichqoncha, klaviatura, flesh-disklarga, shuningdek, alohida tashqi qurilma yoki terminallarga (masalan, aeroport, bank, ta'lim muassasalarida) o'rnatiladi.

Skaner yordamida olingan barmoq izlari raqamli kodga aylantirilib, ma'lumotlar bazasida saqlanadi, so'ngra ilgari kiritilgan yoki o'zgartirilgan barmoq izlari kodlari bilan solishtiriladi. Har bir shaxs barmoq izlari, ya'ni *papiller chiziqlari* o'ziga xos bo'lib, hatto egizaklarda ham ular bir-biridan farq qiladi. Agar barmoqlardan biri shikastlangan bo'lsa, identifikatsiya qilish uchun zaxira barmoq izlaridan foydalanish mumkin (foydalanuvchini ro'yxatdan o'tkazish vaqtida zaxira barmoq izlari biometrik tizimga kiritiladi).

Agar skaner qilingan barmoq izlari namunasi ma'lumotlardan foydalanishga vakolatli shaxslar barmoq izlari "naqshi"ga mos kelmasa, bu ma'lumotga kirishning imkoni bo'lmaydi.

Ko‘zning yoy va to‘r pardasi (irisi) orqali identifikatsiyalash



Identifikatsiya uchun ishlatiladigan noyob biometrik xususiyatlardan biri – ko‘z gavharining yoy pardasi. Ko‘zning yoy va to‘r pardasi har bir insonning noyob biometrik xususiyatlaridan hisoblanadi. U odamda bolalikdan shakllanadi va hayoti davomida o‘zgarmaydi. Ko‘z tasviri olinganidan keyin unga maxsus shtrix-kod niqobi qo‘yiladi. Natijada, har bir kishi uchun individual matritsa olinadi. Ko‘z irisini aniqlash uchun maxsus skanerlar ishlatiladi. Tasdiqlash paytida taxminan 260 ta asosiy nuqta ishlatiladi (taqqoslash uchun barmoq izini tekshirishda 16 ta ga yaqin asosiy nuqtalardan foydalaniladi). Har bir shaxs ko‘zining to‘r pardasi noyob va umr bo‘yi bir xilligicha qoladi. Bu esa ko‘z to‘r pardasini skanerlashni kichik va katta obyektlar uchun eng aniq va tezkor yechimga aylantiradi. Boshqa biometrik parametrlar (barmoq izlari, qo‘l chiziqlari, ovoz, yuz) vaqt o‘tishi bilan o‘zgarishi yoki faqat ma’lum cheklovlar bilan ishlatilishi mumkin.

Nutq xususiyatlari orqali identifikatsiyalash

Shaxsning nutq xususiyatlariga ko‘ra tan olinishi ham biometrik autentifikatsiya usullaridan biri hisoblanadi. Telefonda tanish odamingizni ko‘rmasdan ham ovozidan oson taniy olasiz. Odam psixologik holatini uning ovozi hissiy ohangidan ham bilish mumkin. Ovozni aniqlash nutq chastotasini tahlil qilishga asoslangan. Shaxs ovozining tovush balandligi, ohangi kabi akustik xususiyatlari har bir kishida farq qiladi. Ovozli biometrik autentifikatsiya qilishda ovoz raqamlangan va ilgari yozilgan shablon bilan solishtiriladi. Ishlash prinsipiga ko‘ra, ovozni aniqlash tizimlari matnli shablon (masalan, foydalanuvchidan sevimli rangi yoki ma’lum bir raqamlar ketma-ketligi so‘raladi va ilgari o‘qilgan matn namunasi bilan taqqoslanadi) va ovoz (ovoz xususiyatlari ixtiyoriy matn orqali solishtiriladi) bilan ishlaydigan turlarga bo‘linadi. Ovozli identifikatsiya bilan bog‘liq biometrik yondashuvdan foydalanish oson, lekin ovozning pastligini uning kamchiligi sifatida e’tirof etish lozim. Masalan, shamollash yoki laringit bilan og‘rigan shaxsni identifikatsiyalash qiyin kechishi aniq. Bunday tizimlar aniq olish natijalariga salbiy ta’sir etuvchi quyidagi omillarni o‘z ichiga oladi: boshqa mikrofon, atrof-muhitning tanib olish natijalariga ta’siri (shovqin), talaffuzdagi xatolar, ro‘yxatga olish vaqti va autentifikatsiyalash vaqtidagi shaxs turli xil hissiy holatlari va h. k.).

Yuz tuzilishi orqali identifikatsiyalash

Yuzni identifikatsiya qilish usuli biometrik texnologiyalar orasida eng ko'p tarqalgan va ommabop usul hisoblanadi. Usul odamni bezovta qilmaydi, chunki uning tan olinishi uzoqdan amalga oshiriladi (odam daxlsiz, harakat erkinligi cheklanmagan). Bu texnologiya, odatda, boshqa biometrik usullarga yordamchi usul sifatida ishlatiladi. Insonning yuz xususiyatlari uning tarixi, yoqtirgan va yoqtirmaganlari, kasalliklari, hissiy holati, atrofdagilarga bo'lgan his-tuyg'ulari va ularga nisbatan niyatlarini aytib berishi mumkin. Bularning barchasi, masalan, potensial jinoyatchilarni aniqlash uchun alohida qiziqish uyg'otadi. Identifikatsiya paytida biometrik tizim yuz xususiyatlari (burun, lablar, qoshlar, ular orasidagi masofa, yuzning shakli va rangi, soch rangi va boshqalar) ni tavsiflovchi ma'lumotlarni avtomatik ravishda tanlaydi va qayta ishlaydi. Yuz kontrasti o'zgaradigan joylarning koordinatalari muhim xususiyatlarga kiradi (qosh, ko'z, burun, quloq, og'iz va boshqalar). Ushbu ma'lumotlarga asoslanib, identifikatorlarning raqamli modellari shakllantiriladi, so'ngra ular bir-biri bilan taqqoslanadi. Hozirgda berilayotgan chet el pasportlaridagi chiplarda pasport egasining raqamli fotosurati joy olgan.

Qo'l (kaft) orqali identifikatsiyalash

Biometrikada tanib olish uchun qo'lning o'lchami va shakli, shuningdek, qo'ldagi barmoq suyaklari burmalari, qon tomirlari "naqsh"lari, barmoqlar uzunligi, qalinligi va egriligi, qo'lning umumiy tuzilishi, bo'g'inlar orasidagi masofa, kaftning kengligi va qalinligi kabi xususiyatlar qo'llaniladi. Infraqizil kamera qo'lning tashqi yoki ichki qismini suratga oladi. Tomirlarning shakli qondagi gemoglobin infraqizil nurlanishni yutishi tufayli hosil bo'ladi. Natijada, aks ettirish darajasi pasayadi va kamerada tomirlar qora chiziqlar sifatida ko'rinadi. Qabul qilingan ma'lumotlarga asoslangan maxsus dastur raqamli kodni yaratadi. Qo'l bilan tanib olish skanerlari aeroport, bank, atom elektr stantsiyalari kabilarda o'rnatiladi.

BU QIZIQ!

Shaxsni aniqlash uchun juda kichik, juda eski "genetik izlar" ham yetarli. Pochta markasining orqa tomonida qolgan bitta soch, terining kichik bo'lagi, hatto tupuk izlari jinoyatchi shaxsini aniqlash imkonini beradi. Genlar kombinatsiyasi o'ziga xos bo'lganligi sababli, har bir shaxsda DNK fragmentlarining "namunasi" alohida saqlanadi.

AMALIY FAOLIYAT

№	Topshiriqlar
1-topshiriq. Test savollariga javob bering.	
1.	**Axborot xavfsizligi – … .** a) nojo'ya harakat yuz berishi ehtimolligi; b) mavjud xafv natijasida bo'lishi mumkin bo'lgan hujum turi; c) buzg'unchining biror yomon niyat yo'lidagi harakati; d) axborot foydalanuvchilariga yetkazilishi mumkin bo'lgan zararning oldini olish.
2.	**Axborot xavfsizligini ta'minlash – … .** a) foydalanuvchi axborotlarini himoyalashga qo'yilgan me'yor va talablarning bajarilishi; b) foydalanuvchi axborotlarini himoyalashga qo'yilgan me'yor va talablarning bajarilmasligi; c) xavfdan holi, turli hujum va baxtsiz hodisalar tufayli buzilishdan himoyalash; d) mavjud xafv natijasida bo'lishi mumkin bo'lgan hujum turi.
3.	"Shaxsiy ma'lumotlarni so'roqsiz olish va tarqatish qonuniy jazo olishga sabab bo'la olmaydi." Fikr to'g'ri yoki noto'g'ri ekanligini asoslang.
2-topshiriq. Axborot xavfsizligi sohasida maxfiylik, yaxlitlik va mavjudlikni ta'minlash muammolari o'rganiladi.	
	a) maxfiylik prinsipi yaxlitlikka nisbatan muhim sanalgan aniq misol keltiring; b) yaxlitlik prinsipi maxfiylikka nisbatan muhim sanalgan biror misol keltiring; c) mavjudlik prinsipi qolgan prinsiplarga nisbatan muhim sanalgan aniq hayotiy misol keltiring.
3-topshiriq. Kichik guruhlarda bajaring. Axborotlashtirish va axborot xavfsizligiga oid qonun hujjatlarini yozing:	

№	Nomi	Qabul (e'lon) qilingan vaqti	Tuzilishi (bo'lim, bob, modda)	Maqsad va vazifalari	Tushunchalar	Manbasi
1.						
…						

4-topshiriq. Biometrik shaxsni tasdiqlovchi hujjatlar haqida ma'lumot to'plang va savollarga javob bering:	
	• Biometrik shaxsni tasdiqlovchi qanday hujjatlar mavjud va ular nima uchun joriy qilindi? • Biometrik shaxsni tasdiqlovchi hujjatlarning qanday afzalliklari va kamchiliklari mavjud? • Biometrik shaxsni tasdiqlovchi hujjatlarni qalbakilashtirish mumkinmi?

SAVOL VA TOPSHIRIQLAR

1. Xavf, tahdid va hujum deganda nimani tushunasiz? Ularga oid hayotiy misollar keltiring.
2. Xavflarni boshqarish necha bosqichdan iborat?
3. Biometrik autentifikatsiyalash usullarini sanab bering.
4. Deylik, eng yaqin o'rtog'ingiz kompyuter yoki mobil telefoningizdan sizga tegishli axborotni ruxsatsiz o'z qurilmasiga o'tkazib oldi. Holatga o'z munosabatingizni bildiring.
5. Axborotni qonun bilan himoya qilishning asosiy maqsadlari nimalardan iborat?
6. Axborotni himoya qilish uchun qanday biometrik xavfsizlik usullari mavjud?

UYGA VAZIFA

1. Deylik, siz bank mijozisiz. Bank nuqtayi nazaridan mijoz sifatida sizning ma'lumotlaringiz maxfiyligi muhimmi yoki butunligi? Bank mijozi nuqtayi nazaridan-chi? Fikringizni misollar orqali asoslashga harakat qiling.

2. Jadvalni to'ldiring:

Biometrik identifikatsiyalash usullari	**Afzalliklari**	**Kamchiliklari**
Barmoq izlari (daktiloskopiya) orqali identifikatsiyalash		
Ko'z to'r pardasi orqali identifikatsiyalash		
Nutq xususiyatlari orqali identifikatsiyalash		
Yuz tuzilishi orqali identifikatsiyalash		
Qo'l (kaft) orqali identifikatsiyalash		

3. "Axborot xavfsizligiga tahdidlar" mavzusida diagramma tayyorlash. Muammoni imkon qadar xalqaro miqyosda o'rganib chiqib tayyorlang.