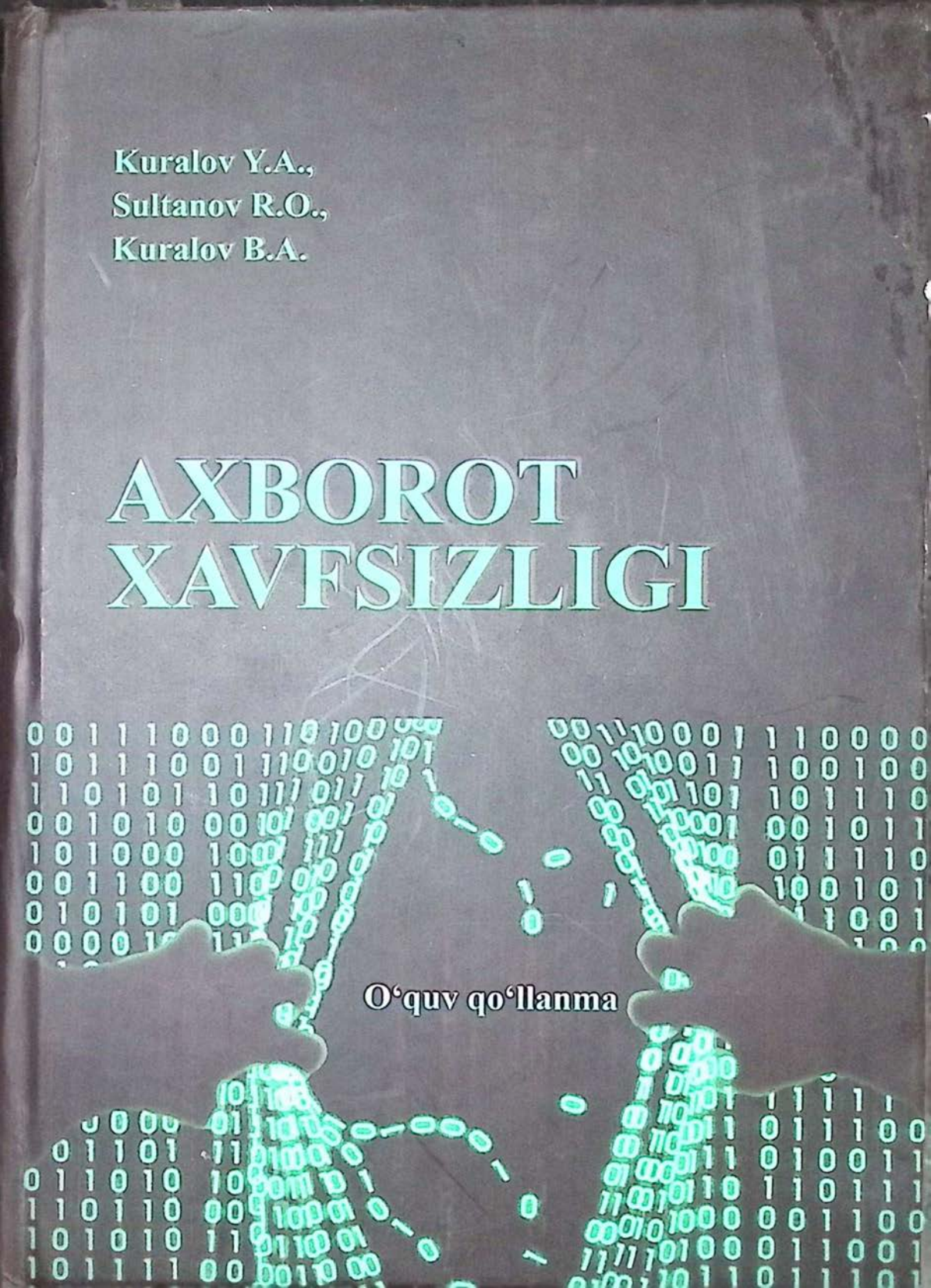


Kuralov Y.A.,
Sultanov R.O.,
Kuralov B.A.

AXBOROT XAVFSIZLIGI

O'quv qo'llanma



004.
K. 79.

O'ZBEKISTON RESPUBLIKASI OLIY TA'LIM, FAN VA
INNOVATSIYALAR VAZIRLIGI
CHIRCHIQ DAVLAT PEDAGOGIKA UNIVERSITETI

Kuralov Y.A., Sultanov R.O., Kuralov B.A.

AXBOROT XAVFSIZLIGI

O'quv qo'llanma

O'ZBEKISTON RESPUBLIKASI MAKTABGACHA
VA MAKTAB TA'LIMI VAZIRLIGI
CHIRCHIQ DAVLAT PEDAGOGIKA UNIVERSITETI
AXBOROT RESURS MARKAZI
1-FILIALI

Chirchiq – 2025

O'ZBEKISTON RESPUBLIKASI OLIY TA'LIM,
FAN VA INNOVATSIYALAR VAZIRLIGI
CHIRCHIQ DAVLAT PEDAGOGIKA UNIVERSITETI
AXBOROT RESURS MARKAZI

-14632/171-

Kuralov Y.A., Sultanov R.O., Kuralov B.A. /Axborot xavfsizligi/ O'quv qo'llanma. – Toshkent: "City of book", 2025. – 196 bet

Ushbu o'quv qo'llanma amaldagi "Axborot xavfsizligi" fani bo'yicha namunaviy dasturlar asosida tayyorlangan bo'lib, 60110600 – Matematika va informatika ta'lim yo'nalishida tahsil olayotgan talabalar uchun mo'ljallangan.

O'quv qo'llanmada "Axborot xavfsizligi" fanining mazmuni, axborot xavfsizligining predmeti, audit mohiyati, uning maqsadi va vazifalari, axborot xavfsizligini ta'minlashning asosiy tushunchalari, taxdidlar, himoya usullari, axborot xavfsizligini ta'minlashning asosiy dasturiy va texnik vositalari haqida yozilgan.

Настоящее учебное пособие подготовлено на основе действующих типовых программ по предмету «Информационная безопасность» и предназначено для студентов, обучающихся по направлению образования 60110600 – Математика и информатика.

Содержание науки «Информационная безопасность», предмет информационной безопасности, сущность аудита, его цели и задачи, основные понятия информационной безопасности, угрозы, методы защиты, основные программные и технические средства информационной безопасности изложены в учебное пособие.

This textbook has been prepared on the basis of current standard programs on the subject "Information Security" and is intended for students studying in the field of education 60110600 – Mathematics and Computer Science.

The content of the science "Information security", the subject of information security, the essence of the audit, its goals and objectives, the basic concepts of information security, threats, methods of protection, the main software and hardware of information security are presented in the textbook.

Taqrizchilar:

1. **D.G.Axmedjonov** - t.f.d. dotsent, CHDPU

2. **N.V.Jurayeva** - t.f.n. dotsent, GFU.

O'zbekiston Respublikasi oliy ta'lim, fan va innovatsiyalar vazirligining 2023 yil 22 dekabrda 537 – sonli buyrug'iga asosan 60110600 - Matematika va informatika ta'lim yo'nalishlari bo'yicha tahsil olayotgan talabalar va professor o'qituvchilari uchun o'quv qo'llanma sifatida nashr qilishga tavsiya etilgan.

ISBN 978-9910-780-02-8

© Kuralov Y.A. va b., 2025
© "City of book", 2025

KIRISH

Har qanday taraqqiy etgan jamiyat hayotida axborotning ahamiyati uzluksiz ortib bormoqda. Uzoq o'tmishdan davlatning harbiy-strategik ahamiyatiga molik bo'lgan ma'lumotlar qat'iy sir tutilgan va himoyalangan. Hozirgi vaqtda ishlab chiqarish texnologiyalariga va mahsulotlarni sotishga tegishli axborot tovar ko'rinishiga ega bo'lib, ichki va tashqi bozorda unga bo'lgan talab ortib bormoqda. Axborot texnologiyalari avtomatlashtirish va axborotni muhofaza qilish yo'nalishlarida muntazam mukammallashib bormoqda.

Zamonaviy axborot texnologiyalarining taraqqiyoti sanoat shpionaji, kompyuter jinoyatchiligi, konfidentsial ma'lumotlarga ruqsatsiz kirish, o'zgartirish, yo'qotish kabi salbiy hodisalar bilan birgalikda kuzatilmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi hisoblanadi. O'zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimi yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o'z ifodasini topmoqda.

«Axborotlashtirish to'g'risida», «Davlat sirlarini saqlash to'g'risida», «Elektron hisoblash mashinalari dasturlari va ma'lumotlar bazalarini huquqiy himoya qilish to'g'risida» va boshqa qonunlar hamda bir qator hukumat qarorlari qabul qilindi va amalga tatbiq etildi.

Axborotni muhofaza qilish axborotni ixtiyoriy ko'rinishda yo'qotishda (o'g'irlash, buzish, qalbakilashtirish) ko'riladigan zararining oldini olishni ta'minlashi lozim. Axborotni muhofaza qilish choralari axborot xavfsizligiga oid amaldagi qonun va me'yoriy hujjatlar asosida va axborotdan foydalanuvchilarning manfaatlariga ko'ra tashkil etilishi zarur. Yuqori darajada axborotni muhofaza qilishni kafolatlash uchun muntazam ravishda murakkab ilmiy-texnik vazifalarni hal etish va himoya vositalarini takomillashtirish talab etiladi.

I-Bob. AXBOROTNI XAVFSIZLIGI, KIBER JINOYATCHILIK VA AXBOROTGA TAHDIDLAR.

1-Mavzu: Axborotni muhofaza qilish, axborot xavfsizligi va uning zamonaviy konsepsiyasi.

Tayanch iboralar: axborot, axborot xavfsizligi, ommaviy axborot, maxfiy axborot, hujjatlashtirilgan axborot, konfedensial axborot.

Axborot xavfsizligi – tasodifiy va atayin qilingan hujumlardan himoyalaniish. Axborot xavfsizligi ko'p qirrali faoliyat sohasi bo'lib, unga faqat tizimli va kompleks yondashuv muvaffaqiyat keltirishi mumkin

O'zbekiston Respublikasining 2002-yil 12-dekabrda №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'iy 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 choratadbirlari;

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.

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 infrastruktura jiddiy zararyetkazishi mumkin.

O'zbekiston Respublikasining 2002-yil 12-dekabrda №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 anglatadi.

Axborot sohasida shaxs manfaatlari fuqarolarning axborotdan foydalanishga doir konstitutsiyaviy huquqlarini amalga oshishida, qonunda taqiqlanmagan faoliyat bilan shug'ullanishida hamda jismoniy, ma'naviy va intellektual rivojlanishda axborotlardan foydalanishlarida, shaxsiy xavfsizlikni ta'minlovchi axborot himoyasida namoyon bo'ladi.

Axborot sohasida jamiyat manfaatlari bu sohada shaxs manfaatlarini ta'minlashda, demokratiyani mustahkamlashda, ijtimoiy huquqiy davlatni qurishda, ijtimoiy hamjihatlikni qo'llab-quvvatlashda o'z aksini topadi.

Axborot sohasida davlat manfaatlarini milliy axborot infrastrukturasi rivojlanishiga sharoitlar yaratishda, axborot olish sohasida shaxs va fuqarolarning konstitutsiyaviy huquq va erkinliklarini amalga oshirishda, O'zbekistonning hududiy birligini, suverenitetini va konstitutsiyaviy tuzumining mustahkamligini, siyosiy, iqtisodiy va ijtimoiy barqarorligini ta'minlash maqsadida axborotdan foydalanishda, qonuniylik va huquq tartibotni qat'iy amalga oshirishda, o'zaro tenglik va o'zaro manfaatdorlikdagi xalqaro hamkorlikni rivojlantirishda ifodalanadi.

Axborot xavfsizligi – ko'p qirrali faoliyat sohasi bo'lib, unga faqat tizimli, kompleks yondashuv muvaffaqiyat keltirishi mumkin. Ushbu muammoni hal etishda huquqiy, ma'muriy, protsedurali va dasturiy-texnik choralarini qo'llaniladi.

Bugungi kunda axborot xavfsizligini ta'minlaydigan uchta asosiy tamoyil mavjud:

ma'lumotlar butunligi – axborotni yo'qotilishiga olib keluvchibuzilishlardan, shuningdek ma'lumotlarni mualliflik huquqi bo'lmagan holda hosil qilish yoki yo'q qilishdan himoya qilish;

axborotning konfidentsialligi. Axborot va uning tashuvchisining holatini belgilaydi va unda axborot bilan ruxsatsiz tanishishning yoki uni ruxsatsiz hujjatlashtirishning (nusxa ko'chirishning) oldini olish ta'minlangan bo'ladi;

foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari.

Ta'kidlash joizki, ayrim faoliyat sohalari (bank va moliya institutlari, axborot tarmoqlari, davlat boshqaruv tizimlari, mudofaa va maxsus tuzilmalar) ularda ko'riladigan masalalarning muhimligi va xarakteriga ko'ra, ularning axborot tizimlari faoliyati ishonchililigiga nisbatan yuqori talablar va xavfsizlik bo'yicha maxsus choralar ko'rilishini talab etadi.

Axborot xavfsizligining milliy xavfsizlik tizimidagi o'rni. XXI asrda shaxs, jamiyat va davlat taraqqiyotida axborot resurslari va texnologiyalarining rolini o'rnatish natijasida O'zbekistonda fuqarolik jamiyatini axborotlashtirilgan jamiyat

sifatida qurish masalasini hal etish bilan birga quyidagi omillar milliy xavfsizlikni ta'minlash tizimida axborot xavfsizligining yetakchi o'rin egallashini belgilaydi:

— milliy manfaatlar, ularga tajovuz va ularni bu tajovuzlardan himoyalash axborot va axborot sohasi orqali ifodalanadi, amalga oshiriladi.

— inson va uning huquqlari, axborot va axborot tizimlari hamda ularga egalik qilish – bu nafaqat axborot xavfsizligining asosiy obyektlari, balki xavfsizlik sohasidagi barcha xavfsizlik obyektlarining asosiy elementlari hamdir;

— axborot yondashuvidan asosiy ilmiy-amaliy usul sifatida foydalanish orqali milliy xavfsizlik masalalarini hal etish mumkin;

— milliy xavfsizlik muammosi yaqqol ajralib turuvchi axborot tavsifiga ega.

Axborot xavfsizligi tizimi davlatning axborot sohasidagi siyosatini mamlakatda milliy xavfsizlikni ta'minlash davlat siyosati bilan chambarchas bog'laydi. Bunda axborot xavfsizligi tizimi davlat siyosatining asosiy tashkil etuvchilarini yaxlit bir butunlikka biriktiradi. Bu esa axborot xavfsizligining roli va uning mamlakat milliy xavfsizligi tizimidagi mavqeini belgilaydi. Axborot sohasidagi O'zbekistonning milliy manfaatlarini, ularga erishishning strategik yo'nalishlarini va ularni amalga oshirish tizimlarini o'zida aks ettiruvchi maqsadlar yaxlitligi davlat axborot siyosatini anglatadi. Shu bilan birga davlat axborot siyosati mamlakatning tashqi va ichki siyosatining asosiy tashkil etuvchisi hisoblanadi hamda jamiyatning barcha jabhalarini qamrab oladi.

Axborot xavfsizligining zamonaviy konsepsiyasi axborot xavfsizligini ta'minlovchi maqsadlar, vazifalar, tamoyillar va asosiy yo'nalishlar bo'yicha rasmiy nuqtai nazarlar majmuini bildiradi.

Quyida axborot xavfsizligining asosiy tashkil etuvchilari va jihatlari keltirilgan:

— axborotni muhofaza qilish (shaxsiy ma'lumotlarni, davlat va xizmat sirlarini va boshqa turdagi tarqatilishi chegaralangan ma'lumotlarni qo'riqlash ma'nosida);

– kompyuter xavfsizligi yoki ma'lumotlar xavfsizligi – kompyuter tarmoqlarida ma'lumotlarning saqlanishini, foydalanishga ruxsat etilganligini va konfedensialligini ta'minlovchi apparat va dasturiy vositalar to'plami, axborotdan ruxsatsiz foydalanishdan himoya qilish choralari;

– axborot egalriga yoki axborotdan foydalanuvchilarga hamda uni qo'llab quvvatlovchi infratuzilmaga zarar yetkazishi mumkin bo'lgan tabiiy yoki sun'iy xarakterdagi tasodifiy yoki qasddan ta'sir etishlardan axborot va uni qo'llab quvvatlovchi infratuzilmaning himoyalanganligi;

– fuqarolar, alohida guruhlar va ijtimoiy qatlamlar, umuman olganda aholining yashash faoliyati, ta'lim olish va rivojlanishlari uchun zarur bo'lgan sifatli axborotga bo'lgan talablarining himoyalanganligi.

Axborotni muhofaza qilish – axborot xavfsizligining (ma'lumotlarning butunligi, foydalana olish va zarur bo'lganda, ma'lumotlarni kiritish, saqlash, qayta ishlash va uzatishda foydalaniluvchi axborot va uning zaxiralari konfedensialligi) muhim jihatlarini ta'minlashga yo'naltirilgan tadbirlar majmuidir.

Xavfsiz tizimda tegishli apparat va dasturiy vositalardan foydalanib, axborotni o'qish, yozish, hosil qilish va o'chirish huquqiga ega shaxslar yoki ular nomidan amalga oshiradigan jarayonlar orqali axborotdan foydalana olish boshqariladi.

Ma'lumki, absolut xavfsiz tizimlar mavjud emas, lekin «ishonish mumkin bo'lgan tizim» ma'nosidagi ishonchli tizimlardan foydalaniladi. Yetarlicha apparat va dasturiy vositalardan foydalanib, bir vaqtning o'zida turli maxfiylik darajasidagi ma'lumotlarni foydalanuvchilar guruhi tomonidan foydalanish huquqlarini buzmaganda qayta ishlash imkonini beruvchi tizim ishonchli hisoblanadi.

Ishonchlilikni baholovchi asosiy mezonlar – bu xavfsizlik siyosati va kafolatlanganlik.

Xavfsizlik siyosati – xavfsizlik obyektlari va subyektlarining berilgan ko'pligining xavfsizligini ta'minlash protseduralari va mexanizmlarini belgilovchi qoidalar to'plami. Tizim xavfsizligini ta'minlashning aniq mexanizmlarini tanlash

qabul qilingan xavfsizlik siyosatiga muvofiq amalga oshiriladi.

Kafolatlanganlik himoyaning passiv qismi bo'lib, tizimdan foydalanishda unga bo'lgan ishonch darajasini ifodalaydi.

Ishonchli tizimda xavfsizlikka taalluqli barcha jarayonlar ro'yxatga olib borilishi kerak.

Axborotni muhofaza qilish tushunchasi axborot xavfsizligi tushunchasi bilan chambarchas bog'liq.

Tor ma'noda axborotni muhofaza qilish deganda axborotni yig'ish, uzatish, qayta ishlash va saqlash jarayonida uning xavfsizligi (konfedensialligi va butunligi)ni ta'minlashga qaratilgan tadbirlar va harakatlar majmui tushuniladi. Bu ta'rif axborotni muhofaza qilish va axborot xavfsizligi tushunchalarining bir-biriga yaqin ekanligini bildiradi.

Axborot xavfsizligi – bu uzatiluvchi, yig'iluvchi va saqlanuvchi axborotning xususiyati (holati) bo'lib, uning tashqi muhit (inson va tabiat) va ichkitahdidlardan himoyalanganlik darajasini xarakterlaydi.

Axborotni muhofaza qilish keng ma'noda axborot xavfsizligiga tahdidni oldini olish va ularning asoratlarini yo'q qilishga qaratilgan tashkiliy, huquqiy va texnik choralar kompleksini bildiradi.

Axborotni muhofaza qilish axborotga bo'lgan salbiy ta'sir manbalarini hamda sabab va sharoitlarni aniqlash va bartaraf etish ma'nosini anglatadi.

Bu manbalar axborot xavfsizligiga tahdidlarni tashkil etadi. Axborotni muhofaza qilish quyidagilarga yo'naltirilgan:

axborot xavfsizligini ta'minlash bo'yicha tahdidlarning oldini olish;
tizimli tahlil va nazorat orqali real va ehtimoli katta bo'lgan tahdidlarni aniqlash va ularni o'z vaqtida oldini olish choralari;

aniq tahdidlar va jinoiy harakatlarni aniqlash maqsadida tahdidlarni topish;
jinoiy harakatlarni bartaraf etish, shuningdek aniq jinoiy harakatlarni hamda tahdidlarni yo'q qilish bo'yicha choralar ko'rish;

tahdid va jinoiy harakatlarning oqibatlarini yo'q qilish va mavqeinisaqlash.

Ushbu barcha usullarning maqsadi axborot resurslarini noqonuniy tahdidlardan himoya qilish va quyidagilarni ta'minlashdan iborat:

konfedensial axborotlarning tarqab ketishini oldini olish;
konfedensial axborot manbalariga noqonuniy kirishni taqiqlash;
axborotning butunligi, to'liqligi va undan foydalana olishni saqlash;
axborot konfedensialligiga rioya qilish;
mualliflik huquqlarini ta'minlash.

Yuqoridagilarni e'tiborga olib, axborotni muhofaza qilish deganda davlat, jamiyat va shaxslarning axborot xavfsizligini ta'minlashga yo'naltirilgan usul, vosita va choralar majmuini tushunish mumkin.

Axborot ximoyasi konsepsiyasini ishlab chiqish bosqichlari.

Konsepsiya – axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yo'llari.

Konsepsiyada ifodalangan maqsadlar, masalalar va ularni bo'lishi mumkin bo'lgan yechish yo'llari asosida axborot xavfsizligini ta'minlashning muayyan rejaları shakllantiriladi.

Konsepsiyani ishlab chiqishni uch bosqichda amalga oshirish tavsiya etiladi.

Bosqichlar	Bosqich nomi	Izoh
I bosqich	Himoyalanuvchi ob'ekt qiymatini aniqlash	Himoyalanishi kerak bo'lgan ob'ekt yoki ma'lumot qiymatini aniqlash va tasniflash.
II bosqich	Buzg'unchining bo'lishi mumkin bo'lgan harakatlarini tahlilash	Potensial xavflarni aniqlash va buzg'unchi tomonidan amalga oshirilishi mumkin bo'lgan harakatlarni tahlil qilish.
III bosqich	Axborotni himoyalash vositalarining ishonchligini baholash	Himoya vositalarining ishonchligi va samaradorligini baholash orqali xavfsizlik darajasini oshirish.

1.1-rasm. Axborot ximoyasi konsepsiyasini ishlab chiqish bosqichlari.

Birinchi bosqichda himoyaning maqsadli ko'rsatmasi, ya'ni qanday real boyliklar, ishlab chiqarish jarayonlari, dasturlar, ma'lumotlar bazasi himoyalanishi zarurligi aniqlanishi shart. Ushbu bosqichda himoyalanuvchi alohida obyektlarni ahamiyati bo'yicha tabaqalashtirish maqsadga muvofiq hisoblanadi.

Ikkinchi bosqichda himoyalanuvchi obyektga nisbatan bo'lishi mumkin bo'lgan jinoiy harakatlar tahlillanishi lozim. Iqtisodiy josuslik, terrorizm, sabotaj, buzish orqali o'g'irlash kabi keng tarqalgan jinoyatchiliklarning real xavf-xatarlik darajasini aniqlash muhim hisoblanadi. So'ngra, niyati buzuvchi odamlarning himoyaga muhtoj asosiy obyektlarga nisbatan harakatlarining ehtimolligini tahlillash lozim.

Uchinchi bosqichning bosh masalasi–vaziyatni, xususan o'ziga xos mahalliy sharoitni, ishlab chiqarish jarayonlarini, o'rnatib qo'yilgan himoyaning texnik vositalarini tahlillashdan iborat.

Nazorat savollari

1. Axborot xavfsizligi tushunchasi nimani anglatadi?
2. Axborot xavfsizligining qanday tashkil etuvchilari mavjud?
3. Axborot xavfsizligi milliy xavfsizlik tizimida qanday o'rin tutadi?
4. Axborot xavfsizligining zamonaviy konsepsiyasi nima?

2-Mavzu: Kiberjinoyatchilik, kiberhuquq va kiberetika.

Tayanch iboralar: kiberjinoyatchilik, kiber huquq, kiberetika.

Ijtimoiy-iqtisodiy manfaatlardan tashqari, kompyuter texnologiyalari va Internet ham, odamlar o'rtasidagi o'zaro munosabatlarning imkoniyatlarini kengaytiruvchi boshqa vositalar kabi, jinoyatlarni sodir etishda ishlatilishi mumkin. Kompyuter jinoyati yoki kompyuter jinoyatlarining nisbatan uzoq vaqtdan beri davom etayotgan hodisani tashkil etsa-da, global tarmoqqa ulanish o'sib borishi zamonaviy kiber jinoyatlarning rivojlanishi bilan uzviy bog'liqdir.

1960 yildan buyon kompyuter tizimlariga jismoniy zarar yetkazish va saqlangan ma'lumotlar, kompyuter tizimlaridan ruxsatsiz foydalanish va elektron ma'lumotlarning manipulyatsiyasi, kompyuterda firibgarlik va dasturiy ta'minotning qaroqchiliklari kabi huquq buzarlilar jinoyat deb topildi.

Ustunlik buzg'unchi-jinoyatchilar tomonida. Qidiruv tizimi bilan mashhur Google korporatsiyasi yaqinda u yuritadigan sistemalar nishonga olingani haqida xabar topdi. Jinoyat Xitoydan turib amalga oshirilgan.

Gap intellektual mulk, mualliflik huquqi va uni o'zlashtirishga urinish haqida ketmoqda. Google qatorida Yahoo, Dow Chemical va Northrop Grumman kabi 20 dan oshiq boshqa yirik kompaniyalar ham xurujlardan shikoyat qiladi. Internetda biznes yuritish xavfli bo'lib qolgan, deydi mo'taxassislar. "Masalani qay jihatidan olib qaramang, ustunlik buzg'unchi-jinoyatchilar tomonida", - deydi ekspert Larri Klinton. "Qonunlar sust. Sohoni yaxshi biladigan mo'taxassislar kam. Xurujlarni uyushtirish oson va arzon. Qo'lidan kelgan odam katta mukofot oladi".

Buning ustiga, o'tgan yillar ichida himoya texnologiyalari bobida uncha yangilik bo'lgani yo'q. Internet - xakerlar uchun cheksiz imkoniyatlar dunyosi.

Kiberjinoyatchiliklarning klassifikatsiyasi.

Moliyaviy yo'naltirilgan kiber jinoyat.

Hech shubhasizki, ko'plab kiber jinoyatchilar Internetdan quyidagi tijoriy hujumlar amalga oshirib, tijorat maqsadlarida foydalanadilar:

Phishing.

Kiber firibgarlar gumonsiragan jabrdiydalarning kompyuterlarini yuqtirish imkoniyati berilganda pastroq osilgan mevalarni to'plashni yoqtirishadi. Bunday sxemalarda elektron pochta - tajovuzkorlarning sevimli vositasi. Usulning mohiyati, oluvchini xatni qonuniy tashkilot nomidan (bank, soliq xizmati, mashhur onlayn-do'kon va boshqalar) amalga oshirishga majbur qilishdir. Bunday hollarda, odatda, bank ma'lumotlarini o'zlashtirishga qaratilgan.

Kiber zo'ravonlik.

Moliyaviy yo'naltirilgan kiber jinoyatchilikka qarshi kurashning yana bir mashhur usuli - bu zo'ravonlik. Odatda foydalanuvchini yoki kompaniyani zararli kodni tushirgandan so'ng, fayllar shifrlanadi va undan keyin naqd pul mukofotiga almashtirish taklifi olinadi (odatda bitcoins yoki boshqa shifrlangan valyuta shaklida). Hukumat pullari kuzatilishi mumkin va kriptovalyutasini kuzatib borish qiyinligi sababli (kriptovalyuta nima, biz ilgari aytgan edik).

Moliyaviy firibgarlik.

Murakkab moliyaviy firibgarliklarning aksariyati mijozlar haqidagi bank ma'lumotlarini (maqsadli hujumlar) yoki olingan ma'lumotlarning keyinchalik manipulyatsiyasini olish uchun chakana operatorlarining kompyuter tizimlariga tajovuz qilish bilan bog'liq. Moliyaviy firibgarlikning ayrim turlari aniqlash juda qiyin.

Kiberjinoyatdan asosiy maqsad nima?

pul, qimmatli krgozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, kuchmas mulk, yoqilgi xom ashyosi, energiya manbalari va strategik xom ashyolarni nokrununiy olish;

- soliq va turli yigimlarni tulashdan bosh tortish;
- jinoiy daromadlarni legallashtirish;
- qalbaki xujjatlar, shtamplar, muxrlar, blankalar, shaxsiy yutuklaruchuy kassa chiptalarini kalbaqilashtirish yoki tayyorlash;
- shaxsiy yoki siyosiy maqsadlarda maxfiy ma'lumotlarni olish;

- ma'muriyat yoki ishdagi xamkasblar bilan shaxsiy dushmanlikmunosabatlari asosida kasos olish;
- shaxsiy yoki siyosiy maqsadlar uchuy mamlakat pul tizimini buzish;
- mamlakatdagi vaziyatni, xududii ma'murii tuzulishni oyekarorlashtirish yoki siyosiy maqsadlar uchun tartibga solish;
- talonchilik, rakibni yo'q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ishini tartibga solmasliq
- boshka jinoyatlarni yashirish uchun;
- tadjikrt masalalarida;
- shaxsiy intelektual kribiliyat yoki ustunlikni namoyish qilish.

Mualliflik huquqini himoyalashning texnik vositalari

Mualiflik xuquqini ta'minlashda turli himoya usullaridan foydalaniladi. Bular CD/DVD diskardagi ma'lumotlarni ruxsatsiz ko'chirishdan himoyalashdan tortib, oddiy RDF fayllarni taxrirlash imkoniyatini cheklash kabi jarayonlarni oz ichiga olishi mumkin.

Biroq, boshqa toifadagi insonlar agar men litsenziyaga ega CD diskni sotib olsam, undan ko'chirish imkoniyatiga xam egabo'lishim kerak deb fikrlaydilar.

Xavfsizlik

Internet tarmog'idagi axborotdan foydalanganda xavfsizlik anchadan beri axloqiy munozaralar mavzusi bo'lib kelgan. Bu birinchi navbatda jamoat faravonligini himoya qilish yoki shaxs xuquqini himoya qilish degan savolni o'rta qo'yadi. Internet tarmog'ida foydalanuvchilar sonini ortishi, shaxsiy ma'lumotlarni ko'payishi natijasida ularning o'g'irlanishi va kiberjinoyatlar soni ortmoqda.

Aniqlik

Internetning mavjudligi va ba'zi bir shaxs yoki jamoalar tabiatitufayli ma'lumotlarning aniqligini bilan shugullanish muammoga aylanmoqda.

Boshqa so'z bilan aytganda Internetdagi

ma'lumotlarning aniqligiga kim javob beradi? Bundan tashqari Internetdagi ma'lumotlarni kim to'ldirib boradi, undagi xatolar va kamchiliklar uchun kim javobgar bo'lishi kerakligi tug'risidagi tortishuvlar mavjud.

Foydalanuvchanlik, senzura va filterlash

Foydalanuvchanlik, senzura va axborotni filterlash mavzulari kiberetika bilan bogliq ko'plab axloqiy masalalarni ko'taradi.

Ushbu masalalarning mavjudligi bizning maxfiylik va shaxsiylikni tushunishimizga va jamiyatdagi ishtirokimizga shubxa tug'diradi.

Agar biror qonun koidaga asosan ma'lumotlardan foydalanishni cheklash yokifilterlash asosida ushbu ma'lumotni tarkalishi yoki foydalanuvchanligiga ta'sir qilish mumkin.

Xozirda ushbu xolatlar amalda keng ko'llanilmokda.

Senzura xam past darajada (masalan, kompaniya o'z xodimlari uchun) yoki yuqori darajada (hukumat tomonidan xavfsizlikni ta'minlash uchun amalga oshirilgan) bo'lishi mumkin.

Mamlakatga kiruvchi ma'lumotlarni boshkarishning eng yaxshi misollaridan biri bu "Buyuk Xitoy Fayrvoli" nomi bilan mashxur bo'lgan loyihadir.

Taqiqlangan kontentlar (pornografiya)

Internet tarmog'ida mavjud bo'lgan taqiqlangan kontentlardan voyaga yetmaganlar tomonidan foydalanish doim axloqiy munozaralargasabab bo'lmoqda. Ayrim davlatlarda bunday kontentlardan foydalanish qattiq taqiqlansa, ayrim davlatlarda bunga ruxsat berilgan.

Qimor o'yinlari

Bu muammo ham etnik masaladagi munozaralardan biri bo'lib uni kimlardir zarar deb hisoblasa, yana kimlardir ularga qonun aralashuvini yoqlamaydilar. O'znavbatida ushbu tomonlar orasidagi munozaralar qaysi turdagi uyinlarga ruxsat berish kerak? Ular qayyerda o'tkazilishi kerak? degan savollar keng muzokaralarga sabab bo'lmoqda. Xozirda aksariyat davlatlarda bu turdagi uyinlarga qonuniy ruxsat berilgan bo'lsa, qolganlariga qat'iy cheklovlar mavjud.

Kompyuterlan foydalanish etikalari

Kompyuter etikasi instituti notijoriy tashqilot bo'lib, vazifasi texnologiyani axloqiy nuqtai nazardan targ'ib qilishdir. Ushbu tashqilot tomonidan quyidagi 10 ta etika qoidalarini keltirib o'tilgan:

1. Shaxsiy kompyuteringizdan boshqalarning zarariga foydalanmang.
2. Boshqa foydalanuvchilarning kompyuter ishlariga xalaqit bermang.
3. Boshqa odamlarning kompyuter fayllariga qaramang.
4. O'g'irlik uchun kompyuterdan foydalanmang.
5. Yomonlik uchun kompyuterdan foydalanmang.
6. O'zingiz pul to'lab sotib olmagan dasturdan foydalanmang va nusxa kuchirmang.
7. Birovni kompyuterini ruxsatsiz foydalanmang.
8. Birovlarni intellektual mexnati samarasiga zarar yetkazmang.
9. Siz yaratgan dasturni ijtimoiy okibati xakida uylang.
10. O'z kompyuteringizdan boshqalarga nisbatan ongli va hurmat bilan foydalaning.

Axborotdan oqilona foydalanish kodeksi

Axborotdan oqilona foydalanish kodeksi buxgalteriya tizimiga quyiladigan talablarni ta'kidlaydigan besh tamoiilga asoslanadi. Ushbu talablar AQSH soglikni sakdash va insonlarga xizmat kursatish vazirligi tomonidan 1973 yilda kiritilgan:

1. Shaxsiy ma'lumotlarni tuplaydigan tizimlar bo'lmasligi kerak. Biroq, bu haqiqat sirdir.
2. Har bir kishi tizimda u to'g'risida kandy ma'lumotlar sakdanishini va undan kandy foydalanilishini boshqarishi kerak.
3. Har bir kishi u to'g'risida to'plangan ma'lumotlardan bitta maqsadda, boshqa maqsadlarda foydalanilishini oldini olish imkoniyatiga ega bo'lishi kerak.
4. Har kim o'zi xakidagi ma'lumotlarni to'g'irlashi kerak.
5. Shaxsiy ma'lumotlar sirasiga kiruvchi ma'lumotlar tuplamini yaratish, sakdash, ishlatish yoki tarqatish bilan shug'ullanadigan har bir tashqilot ushbu

ma'lumotlardan faqat ular belgilangan maqsadlar uchun foydalanilishini ta'minlash va ulardan boshqa maqsadlarda foydalanilishiga qarshi choralar ko'rishi kerak.

Milliy qonunlar

2002 yil 12 dekabrda O'zbekiston Respublikasining 439-P - sonli

"Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi qonuni qabul qilindi. Ushbu qonun 16 moddadan iborat. Xususan unda quyidagilar belgilangan:

1-modda. Ushbu qonunning asosiy vazifalari

Ushbu qonunning asosiy vazifalari axborot erkinligi prinsiplari va kafolatlarga rioya etilishini, xar kimning axborotni erkin va moneliksiz izlash, olish, tekshirish, tarqatish, foydalanish va saqdash huquqdari ruyobga chikarilishini, shuningdek axborotning muxrfaza qilinishini xamda shaxe, jamiyat va davlatning axborot borasidagi xavfeizligini ta'minlashdan iborat.

4-modda. Axborot erkinligi

O'zbekiston Respublikasining Konstitutsiyasiga muvofiq xar kim axborotni moneliksiz izlash, olish, tekshirish, tarqatish, undan foydalanish va uni saklash huquqiga ega.

Axborot olish faqat qonunga muvofiq xamda inson xukuq va erkinliklari, konstitutsiyaviy tuzum asoslari, jamiyatning axlokiy kadriyatlarini, mamlakatning ma'naviy, madaniy va ilmiy salohiyatini muhofaza qilish, xavfeizligini ta'minlash maqsadida cheklanishi mumkin.

6-modda. Axborotning ochiqligi va oshkoraligi

Axborot ochiq va oshkora bo'lishi kerak, maxfiy axborot bundan mustasno. Maxfiy axborotga quyidagilar kirmaydi:

- fukarolarning xukuq va erkinliklari, ularni ruyobga chikarish tartibi to'g'risidagi, shuningdek davlat xokimiyati va boshkaruv organlari, fukarolarning o'zini uzi boshkarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashqilotlarining huquqiy makomini belgilovchi qonun xujjatlarini;

- ekologik, meteorologik, demografik, sanitariya-epidemiologik, favkulodda vaziyatlar to'g'risidagi ma'lumotlar hamda axolining axoli punktlarining ishlab

O'ZBEKISTON RESPUBLIKASI OLIY TA'LIM,
CHIRCHIQ DAVLAT PEDAGOGIKA UNIVERSITETI
AXBOROT RESURS MARKAZI

chikarish obyektlari va kommunikatsiyalarning xavfsizligini ta'minlash uchun zarur bo'lgan boshqa axborotlar;

- axborot-kutubxona muassasalarining, arxivlarning, idoraviy arxivlarning va O'zbekiston Respublikasi hududida faoliyat ko'rsatayotgan yuridik shaxslarga tegishli axborot tizimlarining ochiq fondlaridagi mavjud ma'lumotlar.

Davlat xokimiyati va boshqaruv organlari, fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashqilotlari jamiyat manfaatlariga taalluqli voqealar, faktlar, hodisalar va jarayonlar to'g'risida qonun xujjatlarida belgilangan tartibda ommaviy axborot vositalariga xabar berishi shart.

10-modda. Axborot berishni rad etish

Agar so'ralayotgan axborot maxfiy bo'lsa yoki uni oshkor etish natijasida shaxsning huquqlari va qonuniy manfaatlariga, jamiyat va davlat manfaatlarigazarar yetishi mumkin bo'lsa, axborotni berish rad etilishi mumkin.

So'ralayotgan axborotni berish rad etilganligi to'g'risidagi xabar so'rov bilan murojaat etgan shaxsga so'rov olingan sanadan e'tiboran besh kunlik muddatichida yuboriladi.

Rad etish to'g'risidagi xabarda so'ralayotgan axborotni berish mumkin emasligi sababi kursatilishi kerak.

Maxfiy axborot mulkdori, egasi axborotni so'rayotgan shaxslarni bu axborotni olishning amaldagi cheklovlari to'g'risida xabardor etishi shart

Axborot berilishi qonunga xilof ravishda rad etilgan shaxslar, shuningdek o'z so'roviga haqqoniy bo'lmagan axborot olgan shaxslar o'zlariga yetkazilgan moddiy zararining o'zni qonunda belgilangan tartibda qoplanishi yoki ma'naviy ziyon kompensatsiya qilinishi hukuqiga ega.

11-modda. Axborotni muhofaza etish

Har qanday axborot, agar u bilan qonunga xilof ravishda muomalada bo'lish axborot mulkdori, egasi, axborotdan foydalanuvchi va bopsha shaxsga zarar yetkazishi mumkin bo'lsa, muhofaza etilmog'i kerak.

Axborotni muhofaza etish:

shaxs, jamiyat va davlatning axborot sohasidagi xavfsizligiga taadidlarning oldini olish;

axborotning maxfiyligini ta'minlash, tarqalishi, o'g'irlanishi, yo'qotilishining oldini olish;

axborotning buzib talqin etilishi va soxtalashtirilishining oldini olish maqsadida amalga oshiriladi.

13-modda. Shaxsning axborot borasidagi xavfsizligi

Shaxsning axborot borasidagi xavfsizligi uning axborotdan erkin foydalanishi zarur sharoitlari va kafolatlarini yaratish, shaxsiy xayotiga taalluqli sirlarini saqdash, axborot vositasida qonunga xilof ravishda ruxiy ta'sir ko'rsatilishidan himoya qilish yuli bilan ta'minlanadi.

Jismoniy shaxslarga taalluqli shaxsiy ma'lumotlar maxfiy axborot toifasiga kiradi.

Jismoniy shaxsning rozilgisiz uning shaxsiy xayotiga taalluqli axborotni, xuddi shuningdek shaxsiy xayotiga taallukli sirini, yozishmalar, telefondagi so'zlashuvlar, pochta, telegraf va boshqa muloqot sirlarini buzuvchi axborotni tuplashga, sakdashga, kayta ishlashga, tarqatishga va undan foydalanishga yul ko'yilmaydi, qonun xujjatlarida belgilangan hollar bundan mustasno.

Jismoniy shaxslar to'g'risidagi axborotdan ularga moddiy zarar va ma'naviy ziyon yetkazish, shuningdek ularning huquqdari, erkinliklari va qonuniy manfaatlari ro'yobga chikarilishiga to'sqinlik qilish maqsadida foydalanish taqiqlanadi.

Fukarolar to'g'risida axborot oluvchi, bunday axborotga egalik qiluvchi xamda undan foydalanuvchi yuridik va jismoniy shaxslar bu axborotdan foydalanish tartibini buzganlik uchun qonunda nazarda tutilgan tarzda javobgar bo'ladilar.

Ommaviy axborot vositalari axborot manbaini yoki taxallusini qo'ygan muallifni ularning rozilgisiz oshkor etishga xakdi emas. Axborot manbai yoki muallif nomi faqat sud qarori bilan oshkor etilishi mumkin.

14-modda. Jamiyatning axborot borasidagi xavfsizligi

Jamiyatning axborot borasidagi xavfsizligiga quyidagi yo'llar bilan erishiladi:

- demokratik fuqarolik jamiyati
- asoslari rivojlantirilishini, ommaviy axborot erkinligini ta'minlash;
- qonunga xilof ravishda ijtimoiy ongga axborot vositasida ruhiy ta'sir kursatishga, uni chalgitishga yul quymasliq;
- jamiyatning ma'naviy, madaniy va tarixiy boyliklarini, mamlakatning ilmiy va ilmiy-texnikaviy salohiyatini asrash xamda rivojlantirish;
- milliy o'zlikni anglashni izdan chiqarishga, jamiyatni tarixiy va milliy an'analar xpmda urf-odatlaridan uzoqlashtirishga, ijtimoiy-siyosiy vaziyatni beqarorlashtirishga, millatlararo va konfessiyalararo totuvlikni buzishga qaratilgan axborot ekspansiyasiga qarshi xarakat tizimini barpo etish.

15-modda. Davlatning axborot borasidagi xavfsizligi

Davlatning axborot borasidagi xavfsizligi quyidagi yullar bilan ta'minlanadi:

- axborot soxasidagi xavfsizlikka taxdidlarga qarshi harakatlar yuzasidan iktisodiy, siyosiy, tashqiliy va boshka tUSDagi chora-tadbirlarni amalga oshirish;
- davlat sirlarini savlash va davlat axborot reso'rsalarini ulardan ruxsatsiztarzda foydalanilishidan muxofaza qilish;
- O'zbekiston Respublikasining jaxon axborot makoniga va zamonaviy telekommunikatsiyalar tizimlariga integratsiyalashuvi;
- O'zbekiston Respublikasining konstitutsiyaviy tuzumini zo'rlik bilan o'zgartirishga, xududiy yaxlitligini, suverenitetini buzishga, hokimiyatni bosib olishga yoki qonuniy ravishda saylab ko'yilgan yoxud tayinlangan xokimiyat vaqillarini xokimiyatdan chetlatishga va davlat tuzumiga qarshi boshkacha tajovuz qilishga ochiqdan-ochiq da'vat etishni o'z ichiga olgan axborot tarqatilishidan himoya qilish;
- urushni va zo'ravonlikni, shafqatsizlikni targ'ib qilishni, ijtimoiy, milliy, irqiy va diniy adovat uyg'otishga qaratilgan terrorizm va diniy ekstremizm g'oyalarini yoyishni o'z ichiga olgan axborot tarqatilishiga qarshi harakatlar qilish.

16-modda. Axborot erkinligi prinsiplari va kafolatlari to'g'risidagi qonun hujjatlarini buzganlik uchun javobgarlik

Axborot erkinligi prinsiplari va kafolatlari to'g'risidagi qonun hujjatlarini buzganlikda aybdor shaxslar belgilangan tartibda javobgar bo'ladilar.

Nazorat savollari

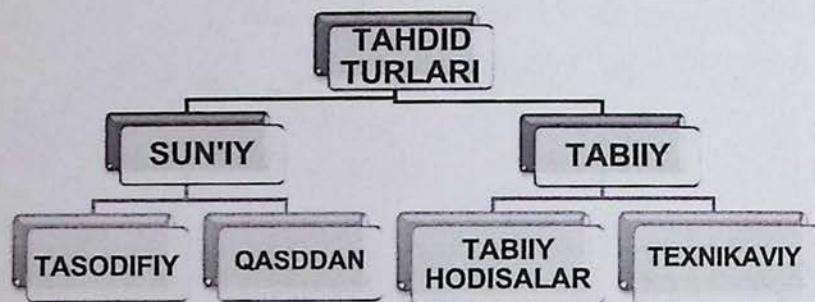
1. Kiberjinoyatchilik va uning turlari?
2. Kiberjinoyatchilikdan maqsad nima?
3. Mualliflik huquqini himoyalashning texnik vositalari .
4. Axborot to'g'risidagi milliy qonunlar.

3-Mavzu: Axborot xavfsizligiga tahdid va uning turlari

Tayanch iboralar: tahdid, sun'iy tahdid, tabiiy tahdid, tasodifiy tahdidlar, Qasddan qilingan tahdidlar, tabiiy hodisalar, texnikaviy hodisalar

Axborot xavfsizligiga tahdid – bu buzg'unchining biror bir maqsad yo'lida mavjud himoyalash tizimlarini buzishga qaratilgan harakati.

Axborotga tahdidlarning turlari



1.1-rasm. Axborotga tahdidlarning turlari.

Tabiiy xarakterdagi tahdidlarning turlari:

Tabiiy hodisalar:

- Yong'in
- Suv bosishi
- Yer qimirlashi
- Magnitli dovul
- Radioaktiv nurlanishlar

Texnikaviy hodisalar:

- Axborot tizimlarning mustahkamligi
- Ta'minot tizimlari

Sun'iy xarakterdagi tahdidlarning turlari:

Tasodifiy tahdidlar:

- Foydalanuvchilarning xatoliklari
- Foydalanuvchilarning uquvsizligi va mas'uliyatsizligi
- Axborot tizimlaridagi xatoliklar

Qasddan qilingan tahdidlar:

- Axborot tizimlariga fizik ta'sir etish
- Axborotlarni o'g'irlash
- Xakerlik hujumlari

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 maxfiylikini va konfidentsialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

— davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfidentsialligini 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 kompleksligi 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 kanalibutun 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.

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 konfidentsialligini saqlash hisoblanadi. Bunda axborot bilan ta'minlash vazifasi tashqi va ichki ruxsat etilmagan ta'sirlardan himoyalash asosida hal etilishi zarur.

Axborot tarqab ketishiga konfedsial 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. Konfedsiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo'lmaganlarga ma'lum bo'ladi. Bu holat konfedsial 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'zgartirishni o'zida mujassamlaydi. Jinoyatchilar axborotni qasddan o'zgartirganda, bu axborotbutunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqonuniy o'zgarishlar kiritilganda ham axborot butunligi buzilgan hisoblanadi. Axborot butunligi – axborotning buzilmagan holatda mavjudligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlikni blokirovka bo'lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlik – axborot aylanuvchi, subyektlarga ularni qiziqitiruvchi 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.



1.2-rasm. Axborotga tahdidlar.

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'ayri ixtiyoriy zararli axborotlardan fuqarolarning o'z sog'liqlarini himoya qilish huquqlari buzilishi; – intellektual 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'alarini 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.

c) 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 konfidentsial 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 himoyalashda 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 nimitzimidir.

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 nimitizimlarni hamda axborot tashuvchilarini himoya qilish zarur.

Turli axborot tizimlarida foydalanuvchilar xizmat ko'rsatuvchi personal hisoblanib, axborot manbai va tashuvchilari bo'lishi mumkin.

Tahdidlarni boshqarish jarayonini quyidagi bosqichlarga bo'lish mumkin:

1. Tahlil qilinuvchi obyektlarni tanlash va ularni ko'rib chiqishdabatafsillik darajasi.
2. Tahdidlarni baholash metodologiyasini tanlash.
3. Aktivlarni identifikatsiyalash.
4. Tahdid va uning oqibatlari tahlili, himoyaning zaifliklarini aniqlash.
5. Tahdidlarni baholash.
6. Himoya choralarini tanlash.
7. Tanlangan choralarni qo'llash va tekshirish.
8. Qoldiq tahdidni baholash.

Ushbu munosabatlarni huquqiy boshqarish avvalo, axborot tahdidlaridan sug'urta qilish orqali amalga oshirilishi mumkin va zarur.

Nazorat savollari

1. Axborot xavfsizligiga tahdid deganda nima tushuniladi?
2. Axborotni muhofaza qilishning qanday usullari va turlari mavjud?
3. Axborotni muhofaza qilish qanday obyektlarga ega?
4. Axborotni muhofaza qilish vositalariga nimalar kiradi?
5. Axborotni muhofaza qilish tizimlari qanday vazifani bajaradi?
6. Axborot xavfsizligi va ma'lumotlarni himoyalash bo'yicha qandayme'yoriy-huquqiy hujjatlar mavjud?
7. Axborotni muhofaza qilish sohasida qanday xalqaro standartlar mavjud?

II-Bob. AXBOROTLARNI FIZIK, KRIPTOGRAFIK VA STEGANOGRAFIK HIMOYALASH.

4-Mavzu: Axborot infratuzulmasini fizik hemoyasini ta'minlash.

Tayanch iboralar: Fizik xavfsizlik, fxborot fizik hemoyalash, OSI modeli.

Axborot xavfsizligini ta'minlashda amalga oshiriladigan dastlabki choralardan biri bu – fizik xavfsizlik hisoblanadi. Ruksat etilmagan fizik boshqarishni, shaxs tomonidan amalga oshiriladigan tahdidlarni va muhitga bog'liq tahdidlarni oldini olish uchun tashkilotlar mos fizik xavfsizlik boshqaruvini sharoitida bo'lishi shart. Tizim administratori fizik xavfsizlikga qaratilgan tahdidlardan saqlanish uchun fizik xavfsizlik choralari o'rnatilgani va to'g'ri ishlayotganini kafolatlashi shart.

Fizik xavfsizlik fizik qurilmalarni, shaxslarni, tarmoq va ma'lumotni hujumlardan himoyalash bilan shug'ullanadi. Ma'lumot, tarmoqlar va qurilmalar xavfsizligi o'zida tabiiy va sun'iy (inson tomonidan qilingan) tahdidlardan himoyalashni mujassamlashtiradi. Tashkilotlar fizik xavfsizlikni ta'minlash uchun mos himoya vositalaridan foydalanishlari zarur. Bunda, tashkilotlar o'z infratuzilmasi va axborot tizimlarining fizik xavfsizligiga ta'sir qiluvchi barcha yo'llarni inobatga olishi shart.

Fizik xavfsizlik – tashkilot axborot xavfsizligi dasturining muhim qismlaridan biri. O'tgan davrda, insonlar fizik xavfsizlik bilan kalitlar, qo'riqchilar, to'siqlar, eshiklar va hak. orqali tushunchaga egalar. Hozirgi kunda, fizik xavfsizlikning ko'rinishi esa tamomila o'zgardi va tashkilotlardan ishchi kuchlar, aktivlar va ko'chmas mulklar nazoratini talab etmoqda. Mazkur aktivlarning fizik xavfsizligini ta'minlash tashkilot uchun muhim vazifalardan biriga aylanmoqda. Tashkilot uchun fizik xavfsizlikni loyihalashda binoning qurilishini rejalashtirishga, jixozlarni sotib olishga, ishchi kuchini jalb etishga, tabiiy hodisalarga, quvvat manbaiga, haroratni nazoratlashga va hak.larga e'tibor qaratish talab etiladi.

Fizik xavfsizlining zaruriyati

Kiber xujumlarning murakkablashishi natijasida hujumchilar tashkilot fizik xavfsizligini buzishda turli usullardan foydalanmoqda. Hujumchilar tashkilotning fizik xavfsizlik tizimidagi bo'shliqlardan foydalangan holda o'z harakatlarini amalga oshirishadi. AQShning Department of Health and Human Services Breach Portal tashkiloti tomonidan 2015 yilda tashkilotlarda eng ko'p yuzaga kelgan xavfsizlik insidentlari fizik xavfsizlikni buzishga uringani aniqlangan (1-rasm).

Fizik himoya tarmoq, ilova yoki ma'lumotlar bazasi xavfsizligi sohalariga o'xshash amallarni bajarmaydi. Ya'ni, fizik xavfsizlik OSI modelining fizik sathida himoyani ta'minlash bilan shug'ullanadi.

Fizik sath quyidagilarni o'z ichiga oladi:

- barcha kabel va tarmoq tizimlari;
- tizim va kabellarni fizik nazoratlash;
- tizim va kabel uchun quvvat manbai;
- tizimni madadlash muhiti.

Fizik xavfsizlikka ta'sir qiluvchi faktorlar

Fizik xavfsizlik buzilishiga ta'sir qiluvchi faktorlarni ikki guruhga ajratish mumkin: tabiiy/ muhit tahdidlari va inson tomonidan (sun'iy) amalga oshiriluvchi tahdidlar.

Tabiiy tahdidlar:

Toshqinlar. Toshqinlar odatda kuchli yomg'ir va muzlarning erishinatisida yuzaga keladi. Toshqinlar natijasida tashkilotning elektr quvvatiga va server xonalariga zarar etishi mumkin. Odatda tashkilotda server xonalari tashkilot binosining podvalida joylashganligi sababli, toshqin yanada ko'proq zarar etkazishi mumkin.

Yong'inlar. Yong'inlar odatda qisqa tutashuvlar va eski bino materiallari sababli yuzaga keladi. Yong'in natijasida tashkilotning kompyuter xonalari va ishchi binolariga zarar etkazilishi mumkin. Yong'in qurilmalar, kabellar va boshqa muhim tashkil etuvchilarga to'liq zarar yetkazishi mumkin.

Zilzila. Zilzila Yer qobig'ida seysmik terbanishni yaratuvchi kuchli energiya natijasida to'satdan yuzaga keladi. U tashkiloning fizik infratuzilmasiga ta'sir qiladi. Zilzila natijasida tashkilot ichidagi xavfsiz muhitda saqlangan kompyuter qurilmalari, boshqa qurilmalar va hujjatlarga jiddiy ziyon yetadi.

Chaqmoq va momaqaldiroq. Chaqmoq va momaqaldiroq muhitning o'zgarishi natijasida yuzaga keladi. Buning natijasida barcha tashqi faoliyat to'xtatiladi. Chaqmoq va momaqaldiroq natijida elektr quvvati o'zgaradi va bu ish faoliyatiga tasir qiladi. Bu esa, o'z navbatida tashkilotdagi qurilmalarning xotira qismlariga tasir qiladi. Bundan tashqari, chaqmoq va momaqaldiroq natijasida kabellarda va boshqa ulanish tizimlarda qisqa tutashuvlar yuzaga kelishi mumkin.

Harorat va namlik. Hisoblash qurilmalari ishlashi uchun ularni ma'lum haroratli muhitda bo'lishi talab etiladi. Kompyuter vositalari yuqori haroratga ishlashga mo'ljallanmagan. Kompyuterlarda sovutish tizimlari mavjud bo'lsada, tashqi harorat ularning ish faoliyatiga salbiy ta'sir ko'rsatadi. Tashkilotdagi elektr va elektron jixozlar namlikni o'zgarishiga ta'sir ko'rsatadi. Yuqori namlik o'z navbatida karroziyaga, qisqa tutashuvlarga sababchi bo'ladi yoki magnetik va optik saqlovchilarga jiddiy ta'sir qiladi.

Sun'iy tahdidlar. Fizik komponentlarga va tarmoqqa bo'ladigan eng katta ta'sir insonlar xatosi natijasida yuzaga keladi. Bu xatolik insonlar tomonidan bilmasdan yoki ataylabdan amalga oshirilishi mumkin. Insonlar tomonidan amalga oshiriluvchi fizik xavfsizlik tizimiga bo'ladigan quyidagi tahdidlar mavjud:

Vandalizim. Norozi xodimlar yoki eski ishchilar tizim komponentlarini buzish yoki zarar etkazish orqali tizimni obro'sizlantirishga harakat qiladi.

Qurilmaning yo'qolishi. Ruksat etilmagan nazoratlash muhim axborot yoki qurilmani yo'qolishiga sababchi bo'ladi. Agar qurilma himoyasi to'g'ri amalga oshirilmagan bo'lsa, uning o'g'irlanishiga sababchi bo'ladi.

Fizik qurilmalarni buzulishi. Qurilmaning noto'g'ri ishlashi, masalan, qurilmani yoki ma'lumotni qanday tutib turilganligi, zararlangan qurilmalarni almashtirilmaganligi va zaif kabellar natijasida fizik qurilmalarga jiddiy zarar

yetkazilishi mumkin.

O'g'irlash. Xavfsizlik tizimidagi kamchilik natijasida jixozlar o'g'irlanishi mumkin.

Terrorizm. Tashkilot yaqinidagi yoki uning ichidagi terrorchilik harakatlari, masalan, mashinada qo'yilgan bomba, shaxs mavjud bo'lgan bomba yoki masofadan turib boshqariluvchi bomba natijasida tashkilot fizik xavfsizligiga turlicha zarar etkazilishi mumkin.

Sotsial injineriya. Sotsial injineriya shaxsiy axborotni boshqa shaxslar tomonidan noqonuniy qo'lga kiritish harakati sifatida qaraladi. Hujumchi tashkilot xodimlaridan sotsial injineriya orqali ruksat etilmagan fiziknazoratlashdan daromad ko'radi.

Tizimlarni ruksat etilmagan nazoratlash. Har ikkala, ichki va tashki foydalanuvchilar ham tashkilot haqidagi axborot yoki tizimni ruksatsiz boshqarishga harakat qilib ko'radi.

Fizik xavfsizlikni nazoratlash

Mos xavfsizlik nazoratisiz, biror fizik xavfsizlikni amalga oshirish qiyin. Fizik xavfsizlik nazorati bardoshli fizik xavfsizlik muhitini yaratishi uchun turli darajalarda amalga oshirilishini talab etadi. Fizik xavfsizlik nazoratini qaysi darajada amalga oshirilishiga qarab, ular quyidagicha tasniflanadi:

Ma'muriy nazorat. Ushbu nazorat turi xavfsizlikni nazoratlashda inson faktorini mujassamlashtiradi. Xodimlarning barcha darajalari ma'muriy nazoratni qurishda inobatga olinishi kerak. Ma'muriy nazorat har bir foydalanuvchi boshqarishi mumkin bo'lgan resurslar va axborotga asoslanadi. Ma'muriy nazorat boshqaruv cheklanishlarini, amaliy muolajalarni, qayd yozuvini amalga oshirish muolajalari va axborot tizimi uchun mos himoya darajasini o'z ichiga oladi. U asosan insonni boshqarish uchun shaxsga qaratilgan usullarni amalga oshiradi.

Fizik nazorat. Fizik nazorat tashkilotdagi fizik tizimlarga zarar yetishini oldini olish bilan shug'ullanadi. U o'z ichiga qurilmalarni, bino yoki biror maxfiy muhitni ruksatsiz boshqarishdan himoyalashni qamrab olgan. Bundan tashqari, fizik

xavfsizlikni nazoratlash fizik tahdidlar: qurilmaning yo'qolishi yoki o'g'irlanishi, tasodiy tufayli zararlanishi va yo'q qilinishi, yong'indan himoyalash yoki tabiiy ofatlardan himoyalash bilan shug'ullanadi.

Texnik nazorat. Texnik nazorat mantiqiy nazorat kabi qaraladi. Texnik nazorat tashkilotdagi fizik avtivlarga yoki binolarga ruxsatlarni nazoratlash uchun texnologiyalardan foydalanadi. U odatda taqiqlangan hududda ruxsatlarni nazoratlash uchun kompyuter qurilmalari, dasturlar, amallar va ilovalardan foydalanadi.

Fizik xavfsizlikni nazoratlash: joylashuv va arxitektura

Tashkilotlar o'zlari uchun bino sotib olishdan yoki ijaraga olishdan oldin fizik xavfsizligiga ta'sir qilishi mumkin bo'lgan ko'plab omillarni e'tiborga olishi shart. Bu omillar o'z ichiga binoning joylashuvi, qo'shni binolar, elektr va suv manbalari, kanalizatsiya tizimi, kichik va katta yo'llarga yaqinligi, transport masalasi, tez yordam ko'rsatish holati, shifoxona, ayeroportga yaqinligi,

mazkur hududda mahalliy holatda jinoyatchilar ko'rsatkichi yoki turli xavfsizlik insidentlarini mavjudligi va h.k.larni oladi. Tanangan hudud tabiiy ofatlardan, masalan, toshqinlar, tarmadolar, yer silkinishi, dovul, yong'inlar va hak.lardan xoli bo'lishi kerak. Binoning joylashuvi haqida yetarlicha axborotga ega bo'lingandan so'ng, ichki tuzilma va arxitekturani loyihalash va rejalashtirish amalga oshiriladi. Joylashuv arxitekturasini loyihalash va rejalashtirish vaqtida, tashkilot tomondan binodagi barcha

aktivlarning ro'yxati tayyor bo'lishi lozim.

Tashkilot infratuzilma va arxitekturani loyihalash vaqtida quyidagi joxatlarga yetibor berishi lozim:

binoga kirish eshiklarining sonini, asosiy kirish, zinalar, lift, mashina stoyankasi, o'tish yo'laklari va qabul qilish hududini o'z ichiga olgan holda, aniqlashtirish;

joylashgan hududingizga yaqin qo'shni binolarni topish va ular uchun ichki va tashqi arxitekturani tekshirish. Atrofdagi narsalar haqida qo'shimcha ma'lumot

olish uchun binolarning egasi va menedjerlari bilan suhbatlashish.

katastropik buzilishlar va tashqi tomondan aktivlarni ko'rinishi orqali zarar etuvchi aktivlarni tahlil qilish;

agar bino boshqa tashkilotlar bilan sheriklikda foydalanilsa, ularni sizning shaxsiy ma'lumotlaringizga va muhim aktivlaringizga ta'siri haqida o'ylang;

fizik xavfsizlikni, maxfiy ma'lumotni saqlash va tashkilot ishlarini samarali amalga oshirish yo'lga qo'yishni boshqarish uchun talab etilgan muhim infratuzilmani aniqlashtirish.

Fizik xavfsizlikni nazoratlash: yong'inga qarshi tizimlar

Yong'inga qarshi tizimlar fizik xavfsizlikni ta'minlashda muhim omil hisoblanadi. Yong'in yuzaga kelganini avtomatlashgan yoki avtomatlashmagan shakllarda aniqlash mumkin.



2.1-rasm. Yong'inga qarshi himoya vositalari.

– Turli yong'inga qarshi tizimlar o'zida aktiv yong'inga qarshi himoyani va passiv yong'inga qarshi himoyani mujassamlashtirgan.

– Aktiv yong'inga qarshi himoya. Aktiv yong'inga qarshi himoya tashkilotda yong'in yuzaga kelgani haqida ogohlantirishni ta'minlaydi. Mazkur turdagi himoya tizimi odatda tijoriy joylarda, ishlab chiqarish joylarida va savdo uylarida o'rnatiladi. Ushbu himoya usulining asosiy maqsadi yong'inni binoning boshqa qismlarini tarqalmasligini oldini olish hisoblanadi. Ushbu himoya tizimi yong'inga qarshi chora ko'rishda ma'lum ishlarni amalga oshirishi talab etiladi. Mazkur harakatlar avtomatik yoki avtomatik bo'lgan tarzda amalga oshiriladi.

– Aktiv yong'inga qarshi himoya tizimi suv sepish, tutun/ yong'indan ogohlantirish tizimlari, o't o'chirgich va turli sprej sepish tizimlarini o'zi ichiga oladi.

– Aktiv yong'inga qarshi tizimlar quyidagilarni o'z ichiga oladi:

– Yong'inni aniqlash tizimi: ushbu tizim yong'in tarqalishidan oldin uni aniqlashga yordam beradi. Ushbu tizim tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilarni o'z ichiga oladi.

– Yong'inni bartaraf etish tizimlari: ushbu tizimlar inson aralashuvisiz yong'inni dastlabki bosqichlarida uni bartaraf etish bilan shug'ullanadi. Ushbu tizimlar zararni kamaytirishga va qurilmalarni yo'q bo'lishidan himoyalaydi.

– Yong'inni bartaraf etish tizimlari avtomatik va avtomatik bo'lgan turlarga ajratiladi. Ushbu tizimlarga: o'to'chirgich (ognetushiyet), suv purkash tizimlarini misol keltirsa bo'ladi.

– Yong'inga qarshi passiv himoya. Yong'inga qarshi passiv himoya tizimlari bino bo'ylab yong'inni tarqalishini oldini olishga foydalaniladi. Yong'inga qarshi eshiklar, oynalar va devorlar passiv yong'inga qarshi himoya usuli sifatida foydalanilishi mumkin. Ushbu himoya tizimi boshqa biror tizim tomonidan ishga tushurilishni talab etmaydi.

– Passiv yong'inga qarshi himoya usuli amaliyotda quyidagi usullar asosida oshiriladi:

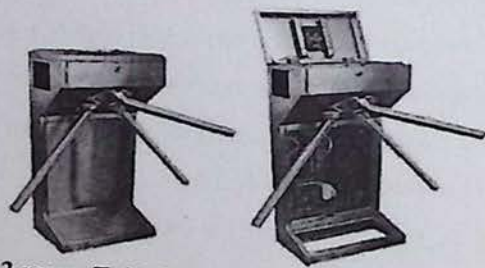
- minimal darajada yonuvchan materiallardan foydalanish;
- binoga yong'inni tarqalishini oldini olish uchun qo'shimcha yetaj yoki xonalarni qurish;
- binoga istiqomat qiluvchilarni yong'in sodir bo'lganda qilinishi zarur bo'lgan ishlar bilan tanishtirish;
- yong'inga aloqador tizimlarni to'g'ri madadlar;
- yetarli sondagi qo'shimcha chiqish yo'llarining mavjudligi.
- Fizik xavfsizlikni nazoratlash: fizik to'siqlar
- Fizik xavfsizlikni ta'minlashda tashkilotda ruxsatsiz kirishlarni oldini olish

muhim hisoblanadi. Bu vazifani bajarishda odatda turli fizik to'siqlardan foydalaniladi. Fizik to'siqlar fizik chegarani umumiy hududdan taqiqlangan hududga ajratadi. Ushbu to'siqlarni joylashuv o'rniga ko'ra: tashqi, o'rta va ichki to'siqlarga ajratish mumkin. Tashqi to'siqlar odatda zabor, devor va boshqalarni o'z ichiga oladi. O'rta to'siqlar odatda olamon va insonlarni taqiqlash uchun foydalaniladi. Ichki to'siqlarni esa eshiklar, derazalar, reshlyotkalar, oynalar, pardalar va hak.lar tashkil etadi.

– Bino ichida foydalaniluvchi fizik to'siqlarni quyidagi turlari mavjud:

– Zaborlar elektr zaborlar metal to'siqlar. Ushbu to'siqlar odatda taqiqlangan hududlarni, nazoratlangan hududlarni va ruxsat etilmagan kirishdan himoyalani belgilashda foydalaniladi. Fizik to'siqlarni amalga oshirishdan asosiy maqsad:

- hujumchini bloklash va ushlab qolish;
- tashkilot chegarasini belgilash;
- xavfsiz hududni tashqi hujumlardan himoyalash;
- transportlarni kirishidan himoyalash;
- portlovchi hujumlardan himoyalash.
- Tumba. Ushbu to'siq kichik vertikal shakldagi tumba shaklida bo'lib, avtomabillarni kirishidan himoyalashda foydalaniladi.
- Turniketlar. Turniketlar bir vaqtda bir shaxsni ichkariga kirishini yoki chiqishini ta'minlaydi. Bunda tizim shaxs tomonidan mos tanga, билет, barmoq izi yoki token ko'rsatilganda kirishga ruxsat beradi.
- Boshqa to'siqlar. Fizik himoyani tashkil qilishda bundan tashqari turli eshiklar, oynalar, reshlyotkalar, oynalar, deraza pardalaridan foydalaniladi.



2.2-rasm. To'siqlarga misollar

Fizik xavfsizlikni nazoratlash: xavfsizlik xodimi

Xavfsizlik xodimi (qo'riqchi) tashkilot fizik xavfsizligini amalga oshirish, monitor qilib borish va madadlashni amalga oshiradi. Ular maxfiy axborotni yo'qolishidan, o'g'irlanishidan, noto'g'ri foydalanishidan himoyalash uchun xavfsizlik tizimini o'rnatish, baholash va ishlab chiqishga javobgardirlar. Yuqori malakali va tajribaga ega xodim ixtiyoriy tashkilotning xavfsizligiga muhim ro'y

o'ynaydi. Tashkilotda xodimlar tomonidan amalga oshirilgan himoya 24x7x365 tartibida amalga oshirilishi zarur. Fizik xavfsizlikka jalb etilgan shaxslar quyidagilar:

Qo'riqchilar. Qo'riqchilar odatda asosiy kirish eshigidan va darvozadan kiruvchilarni va xoimlarni nazoratlashga javobgardir. Ular xususan, begona shaxslarning tashkilot hududida kirmasligini, turli taqiqlangan paketlar va jixozlarni olib kirmaslikni ta'minlashi talab etiladi. Tashkilotdagi barcha kirish eshiklaridagi holatlar qo'riqchilar tomonidan CCTV kameralar yordamida yozib va saqlanib boriladi.

Tashkilotdagi qo'riqchilar boshlig'i. Tashkilotdagi qo'riqchilar boshlig'i qo'riqchilar harakatini kuzatish, talab etilgan vaqtda qo'riqchilarga ko'mak berish, olamonni bartaraf etish, binodagi qulflarni, zamoklarni, yoritish tizimlarini boshqarishga javobgar.

Xavfsizlik xodimi. Ushbu shaxsning vazifasi tashkilot atrofida o'rnatilgan xavfsizlikka aloqador jixozlarni amalga oshirish

va boshqarishdan iborat bo'lib, ularni to'g'ri ishlayotganini kafolatlashi shart. Axborot xavfsizligining bosh xodimi (Chief Information Security Officer). O'tgan davrlarda, axborotxavfsizligining bosh xodimi tashkilotdagi barcha

xavfsizlikka aloqador jarayonlarni nazoratlashi, hattoki tarmoq va tizim xavfsizligiga ham javobgar bo'lgan. Hozirda esa, ushbu shaxslarga asosan texnik tomondan bilim va ko'nikmalar talab etiladi.

Ruxsatlarni nazoratlash: autentifikatsiya usullari Tashkilotdagi o'rta to'siqlar vazifasini o'tovchi turniketlar odatda shaxslarni autentifikatsiyalash vazifasini ham o'taydi yoki bu vazifa qo'riqchilar tomonidan ham amalga oshirilishi mumkin. Shaxslarni autentifikatsiyadan o'tganda turli axborotdan foydalaniladi va ular quyidagilar:

biror narsani bilishga asoslangan;

biror narsaga egalik qilishga asoslangan; biometrik parametrlarga asoslangan.

Fizik xavfsizlikni nazoratlash: fizik qulflar

Ruxsatsiz fizik kirishlarni cheklashda turli qulflar mavjud. Har bir tashkilot o'zining xavfsizlik talabidan kelib chiqqan holda ulardan mosini tanlashi shart. Quyidagi turdagi fizik qulflar mavjud:

Mexanik qulflar: tashkilotda fizik ruxsatlarni cheklashning eng oson usuli hisoblanadi. Ushbu qulflar kalitli yoki kalitsiz bo'lishi mumkin. Mexanik qulflarning ikki turi mavjud:

Raqamli qulflar: raqamli qulflarda yeshikni ochish uchun barmoq izi, smart karta yoki PIN kodni kiritishi talab etiladi. Ular ochish uchun biror narsani (kalitni) olib yurishni talab etmaydi va oson foydalaniladi.

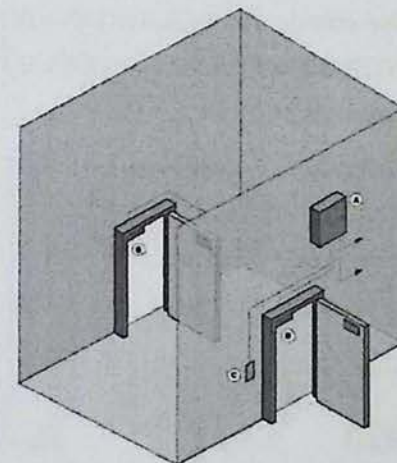
Elektr/ elektromagnetik qulflar: elektr qulflar yoki elektron qulflash tizimi elektr quvvatni kamaytiradi va natijada eshik ochiladi. U odatda magnit va motor asosida qulfni aktivlashtiradi va deaktivlashtiradi. Ushbu qulflar ochish uchun kalitni talab etmaydi.

Kombinatsion qulflar: ushbu qulflar raqam va belgilar kombinatsiyasidan iborat bo'ladi. Foydalanuvchi uni ochishi uchun ularning kombinatsiyasidan iborat bo'lgan maxfiy sirni kiritishi talab etiladi.

Fizik xavfsizlikni nazoratlash: Yashirin qurol/ kontrabanda qurilmalarini aniqlash moslamasi

Fizik xavfsizlikni nazoratlash: qopqon

Qopqon chegarani buzib o'tuvchini tutuvchi va fizik xavfsizlikni nazoratlash vositasi hisoblanadi. Ushbu vosita odatda xavfsiz hududni xavfsiz bo'lmagan hududdan ajratadi. Qopqon mexanik qulflashga asoslangan kichik soha bo'lib, ikkita kirish eshigi mavjud. Ikkinchi eshik ochilishidan oldin birinchi eshik yopilgan holatda bo'ladi. Shaxsni autentifikatsiyalash smart karta, PIN kod yoki biometrik usullar asosida amalga oshirilishi mumkin.



2.3-rasm. Qopqon

Fizik xavfsizlikni nazoratlash: xavfsizlik yorliqlari va ogohlantiruvchi signallar

Xavfsizlik yorliqlari yuqori va past xavfsizlik sohasida axborotga bo'lgan murajaatni cheklash uchun foydalaniladi. Ushbu yorliqlar foydalanuvchilar tomonidan oson tushuniladi va ular ma'lumotdan foydalana olishlari mumkin yoki mumkin emasligini bilishadi. Buning uchun tashkilotdagi ma'lumotlar dastlab xavfsizlik yorliqlari bilan ta'minlanadi.

- Odatda quyidagi turdagi xavfsizlik yorliqlari mavjud:
- ochiq ma'lumotlar (unclassified);
- cheklangan ma'lumotlar (restricted);
- konfidensial ma'lumotlar (confidential);
- maxfiy ma'lumotlar (secret);
- o'ta maxfiy ma'lumotlar (top secret).

Axborotga murojaat qilishdan oldin uning yorlig'iga qarab, ruxsat bor yoki yo'qligini aniqlash va ruxsat bo'lsa undan foydalanish amalga oshiriladi.

Ogohlantiruvchi signallar odatda tashkilotda ruxsat etilmagan harakatlarni amalga oshirni kamaytirish uchun foydalaniladi. Ushbu signallar tashkilotda katta hajmli hodimlarni cheklash uchun katta amaliy yordam beradi. Odatda

ogohlantiruvchi signallar sifatida –TAQIQLANGAN HUDUD” (RESTRICTED AREA), —OGOHLANTIRISH” (WARNING),—XAVFLI” (DANGER)

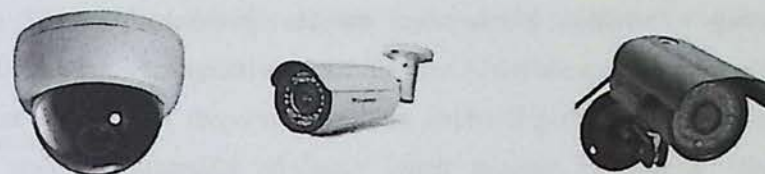
iboralardan foydalaniladi.



2.4-rasm. Ogohlantiruvchi belgilar

Fizik xavfsizlikni nazoratlash: video kuzatuv vositalari

Video kuzatuv tashkilotning fizik xavfsizligini ta'minlashda muhim komponent hisoblanadi. Ushbu tizimlar tashkilot aktivlarini bosqinchilardan, o'g'rilardan himoyalashda muhim ahamiyatga ega. Video kuzatuv moslamalari odatda tashkilotning kirish eshiklarida, zallarda va ishchi sohalarida o'rnatiladi. Ushbu vositalar tashkilotga kirishdagi va chiqishdagi harakatlarni kuzatishda yordam beradi. Hozirgi kundagi video kuzatuv vositalari nafaqat harakatlarni qayd etishda balki, bo'layotgan harakatlarni aniqlash imkonini beradi. Masalan, taqiqlangan jixoz olib kirayotgan yoki chiqayotgan holatni aniqlaydi va ogohlantirish signalini yuboradi yoki janjal bo'layotgan holatni aniqlab, zarur signalni yuboradi. Video kuzatuv vositalari sifatida odatda, quyidagi kameralar amalda foydalanib kelinmoqda:



2.5-rasm. Kuzatuv kameralari

- Fizik xavfsizlikni nazoratlash: fizik xavfsizlik siyosati va muolajalari
- Har bir tashkilot samarali fizik xavfsizlikni amalga oshirish uchun talab qilingan fizik xavfsizlik siyosatini va muolajalarini amalga oshirishi shart. Fizik xavfsizlik siyosati turli tashkilotlar uchun turlicha bo'ladi.
- Xususan, tashkilot fizik xavfsizligining siyosati o'zida quyidagilarni mujassamlashtiradi:
 - tashkilotni fizik xavfsizligi nuqtai-nazaridan;
 - xodimlarning vazifalari va majburiyatlari;
 - foydalanishlarni boshqarishni nazoratlash;
 - qaydlash va auditlash.
- Fizik xavfsizlik muolajasi o'qida quyidagilarni oladi:
 - qulflash tizimini boshqarish;
 - suqilib kirish insidentlarini qaydlash;
 - tashrif buyuruvchilarni boshqarish;
 - konfidensial materiallarni yo'q qilish;
 - qog'oz ko'rinishidagi axborot uchun toza stol siyosatini va axborotni ishlashda toza ekran siyosatini amalga oshirish.
- Toza stol siyosatiga ko'ra tashkilot uchun muhim bo'lgan axborotni xodimlar tomonidan qarovsiz qoldirilmaligi yoki ovqatlanganda oshxonalarga olib kirilmaligi zarur. Toza ekran siyosatiga ko'ra esa xodim o'z kompyuteridan foydalanish davomida uni qarovsiz qoldirmaslikka e'tibor qaratadi.
 - Boshqa fizik xavfsizlik choralari: yoritish tizimlari
 - Yoritish tizimlari tashkilot binosi xavfsizligini ta'minlashda muhim ahamiyat

kasb etadi. Tashkilot binolarining atrofida yetarlicha yoritish amalga oshirilmaganligi boshqa xavfsizlik vositalarining vazifasiga salbiy ta'sir o'tkazadi. Masalan, agar tashkilotning kirishida, mashina turar joyida yoki kuzatuv kamerasi o'rnatilgan hududlarda yoritish tizimi yetarlicha ishlamasa, u holda ushbu hududlardagi obyektlar vainsonlarni aniqlash imkoniyati kamayadi. Muhitning yoritish tizimi holat va sezuvchanlikga aloqador holda quyidagilarga bo'linadi:

– doimiy yoritish tizimlari – tashkilot binosi atrofida har doim o'rnatiluvchi yoritish vositalari.

– kutish rejimidagi yoritish tizimlari – biror ogohlantiruvchi signal asosida avtomatik yoki avtomatik bo'lmagan shaklda ishlaydi.

– harakatlanuvchi yoritish tizimlari – qo'lda boshqariluvchi yoritish tizimlari bo'lib, kechasi va zarur bo'lganda yoritish uchun foydalaniladi.

– favqulotda yoritish tizimlari – elektr quvvati manbalari ishdan chiqqanda yoki elektr energiyasi uzilganda vaqtinchalik tashkilot binolarini yoritish bilan shug'ullanadi.

Fizik xavfsizlikni amalga oshirilganini quyidagilar orqali baholanadi:

1. Ruqsatsiz kirishlarni oldini olish uchun mos ruqsatlarni nazoratlashusullarini o'rnatilgani.

2. Muhim hududlar to'g'ri yoritish tizimi asosida kuzatilayotgani.

3. Turli tahdidlar, yong'in, tutun, elektr, suv va hak.lar uchun aniqlovchi ogohlantiruvchi tizimlar o'rnatilgani va ularni to'g'ri ishlayotgani.

4. To'g'ri eshiklarni qulflash tizimi o'rnatilgani va ularni to'g'ri ishlayotgani.

5. Tashkilot binosi va hududini yetarli sondani qo'riqchilar tomonidan qo'riqlanayotgani.

6. Xavfsizlik xodimlarini to'g'ri o'quv mashg'ulotlariga yuborilgani.

7. Xavfsizlik xodimlarini ishonarli agentliklardan olingan.

8. Tashkilotdagi kuzatuv kameralari to'g'ri o'rnatilgani va uzluksiz ishlayotgani.

9. Fizik xavfsizlik insidentlarini aniqlash va qayd qilish uchun to'g'rimuolajalar amalga oshirilgani.

10. Favqulotda vaziyatlar uchun xodimlar bilan aloqa o'rnatuvchi axborotni mavjudligi.

Nazorat savollari

1. Fizik xavfsizlik nima?
2. OSI modelining qaysi sathi fizik pog'ona hisoblanadi?
3. Fizik xavfsizlikni amalga oshirish nimani ta'minlaydi?
4. Axborotlarni himoyalashning qanday chora tadbirlari mavjud?

5-Mavzu: Sodda shifrlash algoritmlari. O‘rinlarini almashtirishshifrlari.

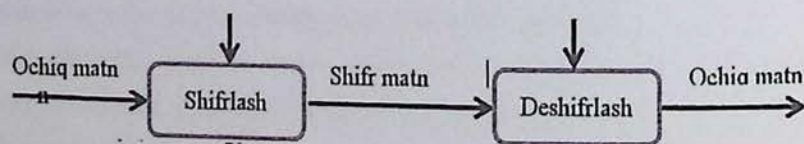
Sehrli kvadrat.

Tayanch iboralar: Ochiq matn, shifr matn, kalit, kriptografiya, kriptozim, kriptologiya, shifrlar, deshifrlash, jadval usuli, sezar shifrlash.

Insoniyat axborotni himoya qilish muammosi bilan yozuv paydo bo‘lgandan beri shug‘ullanadi. Bu muammo harbiy va diplomatik ma’lumotlarni yashirincha uzatish zaruratidan kelib chiqqan. Masalan, antik spartalilar harbiy ma’lumotlarni shifrlashgan. Xitoyliklar tomonidan oddiy yozuvni iyerogriflar ko‘rinishida tasvirlashlari uni xorijiyatlardan yashirish imkonini bergan.

«Kriptografiya» atamasi grek tilidan tarjima qilinganda «yashirish, yozuvni berkitib qo‘ymoq» ma’nosini bildiradi. Atamaning ma’nosi kriptografiya kerakli ma’lumotni yashirin saqlash va himoyalash maqsadida ko‘llanishini anglatadi.

Shifr yoki kriptotizim ma’lumotni shifrlash uchun foydalaniladi. Haqiqiy shifrlanmagan ma’lumot ochiq matn deb atalib, shifrlashning natijasi shifmatn deb ataladi. Haqiqiy ma’lumotni qayta tiklash uchun shifmatnni deshifrlash zarur bo‘ladi. Kalit kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi. Kriptotizimning “qora quti” sifatidagi ko‘rinishi rasmda keltirilgan.



2.6-rasm. Kriptotizimning “qora quti” sifatidagi ko‘rinishi.

Axborotni himoyalash uchun kodlashtirish va kriptografiya usullari qo‘llaniladi.

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

Kriptografiya deb maxfiy xabar mazmunini shifrlash, Ya’ni ma’lumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan

axborotga ruxsat etilmagan kirishga to‘siq qo‘yish usuliga aytiladi.

Kalit- matnni shifrlash va shifrini ochish uchun kerakli axborot.

Kriptozim - kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo‘yiladi:

- yetarli darajada kriptobardoshlilik;
- shifrlash va qaytarish jarayonining oddiyligi;
- axborotni shifrlash oqibatida ular hajmining ortib ketmasligi;
- shifrlashdagi kichik xatolarga tasirchan bo‘lmasligi.

Shifrlash va deshifrlash masalalariga tegishli bo‘lgan, ma’lumotlarni tashkil etadi. Alfavit - axborotlarni ifodalash uchun foydalaniladigan chekli sondagi belgilar to‘plami. Misollar sifatida:

- o‘ttiz oltita belgidan (harfdan) iborat o‘zbek tili alfaviti;
- o‘ttiz ikkita belgidan (harfdan) iborat rus tili alfaviti;
- yigirma sakkizta belgidan (harfdan) iborat lotin alfaviti;
- ikki yuzi ellik oltita belgidan iborat ASSII kompyuter belgilarining alfaviti;
- binar alfavit, Ya’ni 0 va 1 belgilardan iborat bo‘lgan alfavit;
- sakkizlik va o‘n oltilik sanoq sistemalari belgilaridan iborat bo‘lgan alfavitlarni keltirish mumkin.

Simmetrik shifrlarda ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi.

Sodda shifrlar va ularning xossalari

An’anaviy (klassik) shifrlash usullariga o‘rinlarini almashtirish shifrlari, oddiy va murakkab almashtirish shifrlari va ularning kombinatsiyalari va modifikatsiyalari kiradi. Ta’kidlash joizki, o‘rinlarini almashtirish shifrlari va almashtirish shifrlarining kombinatsiyalari amaliyotda qo‘llanilayotgan har xil turdagi simmetrik shifrlarni tashkil etadi.

O'rinlarini almashtirish shifrlarida shifrlanadigan matnning harflari shu matn bloki ichida ma'lum qoidalar bo'yicha o'rin almashtiriladi. O'rinlarini almashtirish shifrlari eng sodda va eng qadimiy hisoblanadi.

Shifrovchi jadvallar. Tiklanish (XIV asr oxirlari) davrining boshlarida o'rinlarini almashtirish shifrlarida shifrovchi jadvallardan foydalanilgan. Shifrovchi jadvalning kaliti sifatida: jadvalning o'lchami; o'rin almashtirishni belgilovchi so'z yoki jumla; jadval tuzilishining xususiyati bo'lgan.

Kalit sifatida jadvalning o'lchami berilishi eng sodda jadvali shifrlash hisoblanadi. Quyidagi matn berilgan bo'lsin:

AXBOROT XAVFSIZLIGI ASOSLARIDA

Ushbu axborot ustun bo'yicha ketma – ket jadvalga kiritiladi:

2.1-jadval.

A	R	A	I	G	O	R
X	O	V	Z	I	S	I
B	T	F	L	A	L	D
O	X	S	I	S	A	A

Natijada, 4x7 o'lchovli jadval tashkil qilinadi.

Энди шифрланган матн қаторлар бўйича аниқланади, яъни ўзимиз учун 4 тадан белгиларни ажратиб ёзамиз.

ARAIGOR XOVSISI BTFLALD OXZISAA

Bu yerda kalit sifatida jadval o'lchovlari xizmat qiladi.

Tabiiyki, uzatuvchi va qabul qiluvchi kalit jadval o'lchami bo'lishligini o'zaro kelishib olishlari kerak. Deshifrlashda teskari amal bajariladi.

Sehrli kvadrat deb, katakchalariga 1 dan boshlab natural sonlar yozilgan, undagi har bir ustun, satr va diagonal bo'yicha sonlar yig'indisi bitta songa teng bo'lgan kvadrat shaklidagi jadvalga aytiladi.

Sehrli kvadratga sonlar tartibi bo'yicha belgilar kiritiladi va bu belgilar satrlar

bo'yicha o'qilganda matn hosil bo'ladi.

Misol tariqasida 4x4 o'lchovli sehrli kvadratni olamiz, bunda sonlarning 880 ta har xil kombinatsiyasi mavjud. Kvadratni quyidagicha to'ldiramiz:

2.2-jadval.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Boshlang'ich matn sifatida quyidagi TOVAR OLTIDA KELDI matnini olamiz va jadvalga joylashtiramiz:

2.3-jadval.

I	V	O	E
R	D	A	T
I	O	L	K
A	D	L	T

Shifrlangan matn jadval elementlarini satrlar bo'yicha o'qish natijasida tashkil topadi:

IVOE RDAT IOLK ADLT

O'rta va katta o'lchamdagi sehrli kvadratlar yordamida, u davrlarda mustahkam shifrlashni amalga oshirish mumkin bo'lgan. Chunki deshifrovka qilishda barcha variantlarni qo'lda amalga oshirib bo'lmas edi.

Insoniyat axborotni himoya qilish muammosi bilan yozuv paydo bo'lgandan beri shug'ullanadi. Bu muammo harbiy va diplomatik ma'lumotlarni yashirincha uzatish zaruratidan kelib chiqqan. Masalan, antik spartalilar harbiy ma'lumotlarni

shifrlashgan. Xitoyliklar tomonidan oddiy yozuvni iyerogriklar ko'rinishida tasvirlashlari uni xorijiydardan yashirish imkonini bergan.

«**Kriptografiya**» atamasi grek tilidan tarjima qilinganda «yashirish,yozuvni berkitib qo'ymoq» ma'nosi bildiradi. Atamaning ma'nosi kriptografiya kerakli ma'lumotni yashirin saqlash va himoyalash maqsadida qo'llanishini anglatadi.

Eramizdan oldingi XX asr. Mesopatamiyada o'tkazilgan qazilmalar vaqtida engqadimiy shifrlangan matnlar topilgan. Loydan yasalgan taxtachaga qoziqchalar bilan yozilgan matn hunarmandlarning sopol buyumlarini qoplash uchun tayyorlanadigan bo'yoqning retsepti bo'lib, u tijorat siri hisoblangan. Qadimgi misrliklarning diniy yozuvlari va tibbiyot retseptlari ham ma'lum.

Eramizdan oldingi IX asrning o'rtalari. Plutarx bergan ma'lumotlariga ko'ra, ana shu davrda shifrovchi qurilma – skital, qo'llanilgan bo'lib, u o'rin almashtirishlar orqali matnni shifrlash imkonini bergan. Matnni shifrlashda so'zlar biror diametrlil silindrga (skitalga) o'ralgan ensiz lentaga yozilgan. Lentayoyilganda unda ochiq matn harflarining o'rinlari almashtirilgan holati hosil bo'lgan. Bunda kalit sifatida silindrning diametri xizmat qilgan. Bunday matnni shifrdan yechish usulini Aristotel taklif etgan. U lentani konusga o'raganva o'qilishi mumkin bo'lgan so'z yoki so'zning bir qismini ko'rsatuvchi joy silindrning diametri deb hisoblagan.

Eramizning 56-yili. Y.Sezar gallar bilan urush vaqtida shifrlashning almashtirish turini qo'llagan. Ochiq matn alfaviti ostiga sikl bo'yicha (Sezarda uchta pozitsiyaga) siljitish orqali shu alfavit yozilgan. Shifrlashda ochiq matndagi alfavitlar, ya'ni yuqori qismda joylashgan harflar quyi qismdagi mos harflar bilan almashtirilgan. Bu turdagi shifrlash Y.Sezargacha ma'lum bo'lgan bo'lsa-da, lekin bunday shifrlash usuli uning nomi bilan yuritiladi.

An'anaviy (klassik) shifrlash usullariga o'rinlarini almashtirish shifrlari, oddiy va murakkab almashtirish shifrlari va ularning kombinatsiyalari va modifikatsiyalari kiradi. Ta'kidlash joizki, o'rinlarini almashtirish shifrlari va almashtirish shifrlarining kombinatsiyalari amaliyotda qo'lla nilayotgan har xil turdagi simmetrik shifrlarni tashkil etadi.

O'rinlarini almashtirish shifrlarida shifrlanadigan matnning harflari shumatn bloki ichida ma'lum qoidalar bo'yicha o'rin almashtiriladi. O'rinlarini almashtirish shifrlari eng sodda va eng qadimiy hisoblanadi.

Shifrovchi jadvallar. Tiklanish (XIV asr oxirlari) davrining boshlarida o'rinlarini almashtirish shifrlarida shifrovchi jadvallardan foydalanilgan. Shifrovchi jadvallarning kaliti sifatida: jadvalning o'lchami; o'rin almashtirishni belgilovchi so'z yoki jumla; jadval tuzilishining xususiyati bo'lgan.

Kalit sifatida jadvalning o'lchami berilishi eng sodda jadvalli shifrlash hisoblanadi. Quyidagi matn berilgan bo'lsin:

OBJEKT BELGILANGAN JOYGA BORADI

Ushbu axborot ustun bo'yicha ketma – ket jadvalga kiritiladi:

O	K	L	A	N	G	R
B	T	G	N	J	A	A
Y	B	I	G	O	B	D
E	E	L	A	Y	O	I

Natijada, 4x7 o'lchovli jadval tashkil qilinadi.

Endi shifrlangan matn qatorlar bo'yicha aniqlanadi, ya'ni o'zimiz uchun 4 tadan belgilarni ajratib yozamiz.

OKLA NGRB TGNJ AAYB IGOB DEEL AYOI

Bu yerda kalit sifatida jadval o'lchovlari xizmat qiladi.

Tabiiyki, uzatuvchi va qabul qiluvchi kalit jadval o'lchami bo'lishligini o'zaro kelishib olishlari kerak. Deshifrlashda teskari amal bajariladi.

Oddiy almashtirish orqali shifrlash

Shifrlanadigan matnning harflari berilgan qoida bo'yicha shu yokiboshqa alfavitdagi harflarga almashtiriladi. Oddiy almashtirish shifrida berilgan matnning har bir harfi shu alfavitdagi unga mos qo'yilgan boshqa harfga almashtiriladi.

Odatda, bu shifrlash usuli bir alfavitli almashtirish shifri deb ataladi.

Sezarning shifrlash tizimi. Sezarning shifrlash usuli oddiy almashtirish shifrining xususiy holdir. Bu usulda alfavitning har bir harfi K songa surilgan harfga almashtirilgan. Surilish alfavit oxiriga yetganda, uning boshidan boshlangan. Sezar K=3 bo'lgan siljitishni qo'llagan. Quyidagi jadvalda bu siljitishdagi lotin grafikasidagi harflarining mosligi keltirilgan:

A	D	J	M	S	V
B	E	K	N	T	W
C	F	L	O	U	X
D	G	M	P	V	Y
E	H	N	Q	W	Z
F	I	O	R	X	A
G	J	P	S	Y	B
H	K	Q	T	Z	C
I	L	R	U		

Sezarning «keldim, ko'rdim, yutdim» mazmundagi xabari VENI VIDI VICI, u taklif etgan usulda shifrlanganda YHQL YLGL YLFL ko'rinishni oladi.

Sezar usulining kamchiligi bu bir xil harflarning o'z navbatida, bir xil harflarga almashishidir. Kriptotahlilda harflarning takrorlanish chastotasi yordamida bu usulda shifrlangan matn tezgina rasshifrovka qilinishi mumkin.

Kalit so'zli Sezar tizimi. Sezarning kalit so'zli shifrlash tizimi bitta alfavitli almashtirish tizimi hisoblanadi. Bu usulda kalit so'zi orqali harflarning surishda va tartibini o'zgartirishda foydalanadi.

Misol tariqasida kalit so'zi sifatida DIPLOMAT so'zi va surish 5 ga teng qilib olingan bo'lsin. Kalit so'zi alfavit ostiga 5 ta harfga surilgan holda yoziladi:

0	1	2	3	4	5					10					15					20					25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
						D	I	P	L	O	M	A	T												

Alfavitning qolgan alfavit ketma-ketligida kalit so'zdan keyin yoziladi.

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	D	I	P	L	O	M	A	T	B	C	E	F	G	H	J	K	N	Q	R	S	U

Natijada, berilgan matnning harflariga mos almashtiruvchi harflar aniqlanadi. Agar ochiq matn TOVAR KELDI bo'lsa, shifrlashdan so'ng JCNVG MZAYL matniga aylanadi.

Kriptografik akslantirishlar

Odatda kriptografiya ma'lumotlarni shifrlashda (deshifrlashda) quyidagi ikki turdagi akslantirishlardan foydalaniladi. Ulardan biri o'rni qo'yish (substitution) akslantirish bo'lsa, ikkinchisi o'rin almashish (permutation) akslantirishidir.

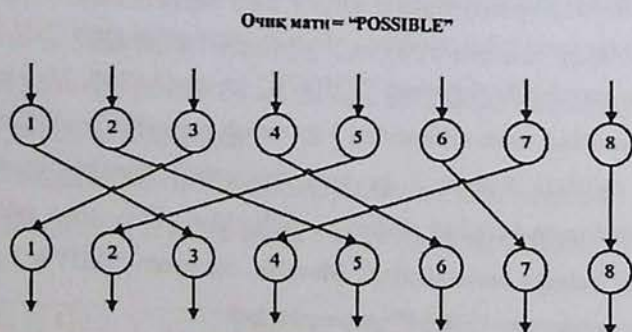
O'rni qo'yish akslantirishi. Ushbu akslantirish sodda va zamonaviy simmetrik kriptografik algoritmlarning asosi hisoblanadi. O'rni qo'yish akslantirishida, ochiq matn belgilari bir alfavitdan olinib, unga mos shifmatn boshqa bir alfavitdan olinadi. Sodda ko'rinishda olingan o'rni qo'yish akslantirishi asosida shifrlash uchun olingan matn quyida keltirilgan. Ushbu sodda shifrlash usuli Sezar nomi bilan mashhur. Masalan, agar ochiq matn "HELLO" ga teng bo'lsa, unga mos holda shifmatn "KHOOR" ga teng bo'ladi. Mazkur holda shifmatn alifbosi ochiq matn alifbosidan 3 ga surish natijasida hosil qilingan va shuning uchun shifrlash kalitini 3 ga teng deb qarash mumkin. Deshifrlash jarayonida esa shifmatn belgilari shifmatn alifbosidan olinib, unga mos ochiq matn alifbosidagi belgiga almashtiriladi. Masalan, shifmatn "ILUVW" ga teng bo'lsa, unga mos ochiq matn "FIRST" ga teng bo'ladi.

1.1-jadval.

[illegible]

Oʻrniga qoʻyish akslantirishida ochiq matndagi belgilar shifratmda boʻlmasligi mumkin. Biroq, ochiq matndagi belgilarning takrorlanish chastotasi shifratmdagi belgilarda ham bir xil boʻladi (koʻp alifboli oʻrniga qoʻyish usullari bundan mustasno). Masalan, yuqoridagi misolda ochiqmatndagi “L” harfining takrorlanish chastotasi 2 ga teng. Uning oʻrniga qoʻyilgan shifratmdagi “O” harfining ham takrorlanish chastotasi 2 ga teng. Bu holat ochiqmatndagi qolgan belgilar uchun ham oʻrinli.

O'rin almashtirish akslantirishi. Ushbu akslantirishga ko'ra, ochiq matn belgilarining o'zni biror qoidaga ko'ra o'zaro almashtiriladi. Bunda ochiq matnga ishtirok etgan belgilar shifratga ham ishtirok etib, faqat ularning o'zni almashgan holda bo'ladi (1.5-rasm).



1.5-rasm. Sodda o'rin almashtirish usuliga misol

1.1. Kriptografiyaning tarixi

Ma'lumotlarni shifrlashning dastlabki ko'rinishlaridan ming yillar avval foydanib kelingan. Yaqin o'n yilliklarga qadar foydalanilgan shifrlarni - klassik shifrlar deb atalgan. Kriptografiyaning fan sifatida taraqqiy etishini ko'plab adabiyotlarda turlicha davrlarga bo'lingan bo'lib, turlicha yondashuvlarga asoslaniladi. Masalan, ba'zi manbalarda hisoblash qurilmalari yaratilgunga qadar foydalanilgan shifrlar – klassik shifrlar davriga tegishli deb olingan. Undan keyingi davr esa zamonaviy shifrlar davri deb yuritiladi. Biroq, hisoblash qurilmalari yaratilgunga qadar bo'lgan davr juda uzoq bo'lgani bois, ularni ham qismdavrlarga ajratish muhim ahamiyat kasb etadi.

Kriptologiyani fan sifatida shakllanishini quyidagi davrlarga ajratish mumkin:

1. Qadimiy davr (qadimiy davr klassik shifrlari). Ushbu davr klassikshifrlari asosan bir alfavitli oʻrniga qoʻyish va oʻrin almashtirish akslantirishlariga asoslangan. Ularga misol tariqasida Sezar, Polibiya kvadrati usullarini keltirish mumkin.

2. O'rta davr (o'rta davr klassik shifrlari). Ushbu davr shifrlari asosan ko'p alifboli o'rni qo'yishga asoslangan bo'lib, ularga Vijiner, Atbash usullarini misol keltirish mumkin. Ushbu davr shifrlari birinchi davr shifrlariga qaraganda yuqori bardoshlikka ega bo'lgan.

3. 1 va 2 – jaxon urishi davri (1 va 2- jaxon urishi davri klassik shifrlari).
Ushbu davr kriptotizimlari asosan elektromexanikaga asoslangan bo'lib, radioto'lqin orqali shifratni uzatishni (morze alifbosi) amalga oshirgan. Mazkur davrga oid shifrlash usullariga Zimmermann telegrafi, Enigma shifri, SIGABA mashinalarini misol keltirish mumkin.

4. Kompyuter davri (zamonaviy shifrlar). Ushbu davr shifrlari hisoblash qurilmalariga mo'ljallangan bo'lib, yuqori xavfsizlik darajasiga ega hisoblanadi. Zamonaviy shifrlarga misol sifatida DES, AES, GOST 28147-89, IDEA, A5/1, RC4 (barchasi simmetrik) va RSA, El-Gamal (ochiq kalitli) larni keltirish mumkin.

Bir martali bloknot

Bir martali bloknot (one time pad) yoki Vernam shifri nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanib, tarixda turli vaqtlarda va joylarda foydalanilgan bo'lsada, ko'p hollarda amalga oshirishning imkoniyati mavjud emas. Bir martali deb atalishiga asosiy sabab, undagi kalitning (bloknotning) bir marta foydalanilishi bo'lib, shunning uchun uni aksariyat hollarda amalga oshirishning imkoni mavjud bo'lmaydi.

Ushbu shifrlash algoritmini tushuntirish uchun keling 8 ta belgidan iborat bo'lgan alfavit olingan bo'lsin. Olingan alfavit va unga mos bo'lgan binar qiymatlar quyidagi jadvalda keltirilgan. Shuni esda saqlash kerakki, alifbo va unga mos bo'lgan bit qiymatlari barcha uchun ochiq va sir saqlanmaydi (ASCII jadvali kabi).

1.2-jadval

Белгилар	E	H	I	K	L	R	S	T
Бинар қиймат	000	001	010	011	100	101	110	111

Faraz qilinsin, biror qonuniy foydalanuvchi A bir martali bloknotdan foydalangan holda "HEILHITLER" matnini shifrlab, o'z sherigi B tomonga yuborishi talab etilsin. Ushbu ochiq matnni binar qiymatdagi ko'rinishi esa quyidagicha bo'ladi:

1.3-jadval

H	E	I	L	H	I	T	L	E	R
001	000	010	100	001	010	111	100	000	101

Bir martali bloknot usulida shifrlash uchun ochiq matn uzunligiga teng bo'lgan tasodifiy tanlangan kalit zarur bo'ladi. Ochiq matnga kalitni XOR amalida qo'shish orqali shifmatn hosil qilinadi (R – ochiq matn, K – kalit va S – shifmatn

deb belgilansa): $C = P \oplus K$. XOR amali ($\oplus$) binar amal hisoblanib, quyida keltirilgan:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Yuqoridagi jadvaldan, $x \oplus y \oplus y = x$ tenglik o'rinligi bilish qiyin emas va shuning uchun bir martali parolda deshifrlash uchun shifmatnga kalitni XOR amalida qo'shishning o'zi yetarli hisoblanadi: $P = C \oplus K$.

Faraz qilinsin A tomon yuqorida keltirilgan ochiq matn uzunligiga teng bo'lgan quyidagi kalitga ega bo'lsin:

111 101 110 101 111 100 000 101 110 000

Ushbu kalit asosida A tomon quyidagi shifmatnni hisoblaydi:

1.4-jadval

	H	E	I	L	H	I	T	L	E	R
Ochiq matn:	001	000	010	100	001	010	111	100	000	101
Kalit: 111 101 110 101 111 100 000 101 110 000										
shifmatn:	1	1	1	0	1	1	1	0	1	10
	1	0	0	0	1	1	1	0	1	1
	0	1	0	1	0	0	1	1	0	
	S	R	L	H	H	H	T	H	S	R

A tomonidan yuborilgan shifratn B tomonda bir xil kalit mavjudligi sababli osongina deShifrlanadi:

1.4-jadval

	S	R	L	H	H	H	T	H	S	R
Shifratn:	110	101	100	001	110	110	111	001	110	101

Kalit: 111 101 110 101 111 100 000 101 110 000

Ochiq matn:	001	000	010	100	001	010	111	100	000	101
	H	E	I	L	H	I	T	L	E	R

Ushbu shifrlash algoritmi uchun quyidagi ikki holatni qarab chiqish muhim. Birinchi holatda, faraz qilinsin A tomoning dushmani M bor va u A tomon quyidagi kalitdan foydalanilgan deb biladi:

101 111 000 101 111 100 000 101 110 000

Agar M dushman ushbu kalitni B tomonga uzatishni imkonidan chiqsa, u holda B tomon shifratnni deshifrlash orqali quyidagiga ega bo'ladi:

1.4-jadval

	S	R	L	H	H	H	T	H	S	R
Shifratn:	110	101	100	001	110	110	111	001	110	101

"Kalit": 101 111 000 101 111 100 000 101 110 000

"Ochiq matn":	011	010	100	100	001	010	111	100	000	101
	K	I	L	L	H	I	T	L	E	R

Agar B tomon kriptografiyadan umuman xabari bo'lmasa, u holda A tomonning qarori muhokamaga sabab bo'ladi.

Faraz qilinsin boshqacha senariy mavjud. A foydalanuvchi o'z dushmani M tomonidan qo'lga olindi va dushman shifratnga ham ega. Dushman shifratnini

o'qiy olmaydi va shuning uchun A tomondan uning kalitini aytishini talab etadi. A tomon o'zini har ikkala tomonga "o'ynashini" aytib, shifratnini deshifrlash kaliti deb quyidagini aytadi:

111 101 000 011 101 110 001 011 101 101

Ushbu kalit orqali dushman M shifratnini deShifrlaganda quyidagi ochiq matnga ega bo'ladi:

1.6-jadval

	S	R	L	H	H	H	T	H	S	R
Шифратн:	110	101	100	001	110	110	111	001	110	101
"Калит":	111	101	000	011	101	110	001	011	101	101
"Очиқ матн":	001	000	100	010	011	000	110	010	011	000
	H	E	L	I	K	E	S	I	K	E

Agar dushman kriptogarfiya haqida ma'lumotga ega bo'lmasa, ushbu ochiq matnga ishonadi va A tomonni qo'yib yuboradi.

Kafolatga ega emasligi sababli, ushbu keltirilgan misollar bir martali bloknot shifrlari bardoshli ekanini ko'rsatadi. Bir martali bloknotda agar kalit tasodifiy tanlansa va bir marta foydalanilgan taqdirda hujumchi shifratndan ochiq matn haqida biror axborotga ega bo'la olmaydi (albatta ma'lumotni uzunligidan tashqari). Ya'ni, berilgan shifratn uchun mos "kalit" yordamida shifratn uzunligidagi ixtiyoriy "ochiq matnlar"ni generatsiya qilish mumkin va bunda barcha ochiq matnlar bir xil o'xshashlikka ega. Shuning uchun shifratndan ochiq matn haqida biror foydali axborotni olishning imkoni yo'q. Kriptografik nutqai nazardan shifratnlar o'zidan ortiq ma'lumotni bera olmaydi.

Buning uchun albatta, bir martali bloknot to'g'ri foydalanilgan, undagi kalit tasodifiy tanlangan, bir marta foydalaniladi va faqat A va B tomonlarga ma'lum bo'lishi talab etiladi.

Bir martali bloknot bardoshlikni ta'minlar ekan, nima uchun har doim undan foydalanilmaydi? Buning asosiy sababi, har bir ochiq matn uchun uning uzunligiga teng bo'lgan tasodifiy kalitni (bloknoti) generatsiya qilish va qabul qiluvchi deshifrlashdan oldin xavfsiz uzatishning imkoniyati yo'qligidir. Agar ochiq matn uzunligidagi kalitni (bloknotni) xavfsiz uzatishning imkoniyati mavjud bo'lsa, u holda kalitning o'rimga ochiq matnni uzatish foydali emasmi? Uni shifrlashdan nima ma'no?

Bir martali bloknot usulidan tarixda cheklangan uzunlikdagi ma'lumotlarni shifrlash qisman foydalanilgan bo'lsada, hozirgi kundagi katta hajmli ma'lumotlarni uzatish uchun bir martali bloknotni to'liq amaliy tomondan qo'llab bo'lmaydi.

Bir martali bloknotda kalitlardan faqat bir marta foydalanishdan maqsad nima? Faraz qilaylik, quyidagi ikki ochiq matn P_1 va P_2 bitta kalit

K dan foydalanib shifrlangan: $C_1 = P_1 \oplus K$ va $C_2 = P_2 \oplus K$. Kriptografiyada ushbu holatni "xavflilik" deb ataladi va bir martali bloknot xavfli holatda deb tushiniladi, ya'ni foydalanilgan kalit ortiq muammo tug'dirmaydi:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Mazkur holda shifmatn haqiqiy ochiq matn haqida ba'zi axborotni oshkor qiladi. Agar bir kalitdan foydalanib ko'p marta shifrlash amalga oshirilsa bu katta xavfga olib kelishi mumkin. Mazkur holatni quyidagi misolda ko'rib chiqaylik. Faraz qilaylik, quyidagi ikkita ochiq matn berilgan bo'lsin (belgilarning binar kodi yuqoridagi jadvaldagi kabi):

$$P_1 = \text{LIKE} = 100\ 010\ 011\ 000 \text{ va } P_2 = \text{KITE} = 011\ 010\ 111\ 000.$$

Har ikkala ochiq matn yagona kalit $K = 110\ 011\ 101\ 111$ shifrlangan va shifmatnlar quyidagiga teng bo'lgan:

	L	I	K	E	
P_1 :	100	010	011		000
K :	110	011	101		111
C_1 :	010	001	110		111
	I	H	S	T	

	K	I	T	E	
P_2 :	011	010	111		000
K :	110	011	101		111
C_2 :	101	001	010		111
	R	H	I	T	

Agar hujumchi kriptotahlil bilan yaqindan tanish bo'lsa va har ikkala ochiq matn bir xil kalit yordamida shifrlanganini bilsa, ochiq matnlardagi 2 va 4 harflarni bir xilligini osongina aniqlaydi. Sababi, mos o'rindagi shifmatn belgilaribir xil. Bundan tashqari, hujumchi taxminiy P_1 ochiq matn oladi va uni to'g'riligini P_2 ochiq matn bilan tekshirib ko'radi. Faraz qilaylik, hujumchi birinchi ochiq matn sifatida $P_1 = \text{KILL} = 011\ 010\ 100\ 100$ ni olgan bo'lsin. Bu holda u unga mos bo'lgan taxminiy kalitni quyidagicha hisoblaydi:

$$\text{Taxminiy } P_1: \begin{array}{cccc} & K & I & L & L \\ 011 & 010 & 100 & 100 \end{array}$$

$$C_1: \underline{010\ 001\ 110\ 111}$$

$$\text{Taxminiy } K: \underline{001\ 011\ 010\ 011}$$

Olingan kalit K yordamida esa ikkinchi shifmatndan ochiq matnni hisoblaydi:

C_2 :	101	001	010	111
Тахминий K :	001	011	010	111
Тахминий P_2 :	100	010	000	100
	L	I	E	L

Hisoblangan kalit K ikkinchi ochiq matn P_2 uchun mos bo'lmagani sababli, hujumchi taxmin qilgan birinchi ochiq matni P_1 ni noto'g'riligini

biladi. Shu tarzda hujumchi qachonki birinchi ochiq matnni $P1 = LIKE$ tarzida taxmin qilsa, ikkinchi ochiq matnni to'g'ri $P2 = KITE$ topa oladi.

Kodlar kitobi. Kodlar kitobi ko'rinishidagi klassik shifrlash birinchi jaxon urushi davrida ommalashgan. Kodlar kitobi lug'atga o'xshash kitob bo'lib, so'zlardan (ochiq matn so'zlari) va unga mos bo'lgan kod so'zlardan (Shifrmatn) tashkil topgan. shifrlash uchun ushbu kodlar kitobidan zarur bo'lgan so'z aniqlanadi va unga mos bo'lgan kod so'z shifrmatn sifatida olinadi. Deshifrlashdaesa ushbu jarayonning teskarisi amalga oshiriladi. YA'ni, kodlar kitobidan shifrmatndagi kod so'z topiladi va ochiq matn sifatida unga mos bo'lgan so'z tanlanadi. Birinchi jaxon urushi davrida Nemislar tomonidan foydalanilgan kodlarkitobi na'munasi quyidagi jadvalda keltirilgan:

1.7-jadval

ОЧИК МАТН	Шифрматн
Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedensschluss	17149

Masalan, —Februar” so'zini shifrlash uchun butun so'z 5-belgili kod so'z 13605 bilan almashtirilgan. Yuqorida keltirilgan kodlar kitobi, shifrlash uchun foydalanilgan bo'lib, deshifrlash uchun kod so'zlar ustuni bo'yicha tartiblangan ko'rinishdagi kod so'zlar kitobidan foydalanilgan. Kod so'zlar kitobi o'rniga qo'yish akslantirishiga asoslangan bo'lib, bunda bir belgi emas balki butun so'z, ba'zida esa butun boshli ibora o'rniga kod so'z qo'yilgan.

Yuqoridagi jadvalda keltirilgan kod so'zlar mashhur Zimmermann telegramini shifrlash uchun foydalanilgan. 1917 yilda birinchi jaxon urishi davrida, Germaniya tashqi ishlar vaziri Artur Zimmermann Germaniyaning Meksikadagi elchisiga shifrlangan ko'rinishdagi telegram yuboradi. 1.6-rasmda keltirilgan

shifrlangan xabar Britaniyaliklar tomonidan tutib olinadi. Bu vaqtda Britaniya va Fransiya Germaniya bilan urushayotgan va AQSH esa betaraf holatda edi.



1.6-rasm. Zimmerman telegrami

Ruslar tomonidan Nemislar kodlar kitobini zarar etgan versiyasi tiklanadi va Britaniyaga yuboriladi. Murakkab tahlildan so'ng, Britaniyaliklar Zimmerman telegrami yozilgan vaqtidagi kodlar kitobidagi bo'shliqlarni to'ldirishadi va uni deshifrlashadi. Telegramda aytilishicha, Germaniya hukumati cheklanmagan suvosti urushi boshlanishini rejalashtirmoqda va bu AQSH bilan urushga olib kelishi mumkin degan xulosaga kelinadi. Natijada, Zimmerman o'z elchisiga Meksikani AQShga nisbatan urushda Germaniya ittifoqchisi bo'lishga undashi kerakligini aytadi. Xususan, Meksika Texas, Yagni Meksika va Arizona shtatlaridagi hududlarini qaytarib olishga undagan. AQShda ushbu telegramma oshkor bo'lgandan so'ng, jamoatchilik Germaniyaga qarshi turdi va shundanso'ng AQSH urushga kiradi.

Nazorat savollari

1. Kriptografiya manosi nima?
2. Kalit nima?
3. Kriptoanaliz nima?
4. Shifrlash va deshifrlash farqi.

6-MAVZU: Sezarning shifrlash tizimi, Vijnerning shifrlash tizimi.

Tayanch iboralar: O‘rin almashtirish orqali shifrlash, Sezarning shifrlash, Vijnerning shifrlash

O‘rin almashtirish orqali shifrlash

Shifrlanadigan matnning harflari berilgan qoida bo‘yicha shu yoki boshqa alfavitdagi harflarga almashtiriladi. Oddiy almashtirish shifrida berilgan matnning har bir harfi shu alfavitdagi unga mos qo‘yilgan boshqa harfga almashtiriladi. Odatda, bu shifrlash usuli bir alfavitli almashtirish shifri deb ataladi.

Sezarning shifrlash tizimi. Sezarning shifrlash usuli oddiy almashtirish shifrlanish xususiy holidir. Bu usulda alfavitning har bir harfi K songa surilgan harfga almashtirilgan. Surilish alfavit oxiriga yetganda, uning boshidan boshlangan. Sezar $K=3$ bo‘lgan siljitishni qo‘llagan. Quyidagi jadvalda bu siljitishdagi lotin grafikasidagi harflarining mosligi keltirilgan:

2.4-jadval.

A	D	J	M	S	V
B	E	K	N	T	W
C	F	L	O	U	X
D	G	M	P	V	Y
E	H	N	Q	W	Z
F	I	O	R	X	A
G	J	P	S	Y	B
H	K	Q	T	Z	C
I	L	R	U		

Sezarning «keldim, ko‘rdim, yutdim» mazmundagi xabari VENI VIDI VICI, u taklif etgan usulda shifrlanganda YHQL YLGL YLFL ko‘rinishni oladi.

Sezar usulining kamchiligi bu bir xil harflarning o‘z navbatida, bir xil harflarga almashishidir. Kriptotahlilda harflarning takrorlanish chastotasi yordamida bu usulda shifrlangan matn tezgina rasshifrovka qilinishi mumkin.

Vijnerning shifrlash tizimi. XVI asrda fransuz diplomati Vijnern tomonidan yaratilgan shifrlash tizimi 1586 yilda chop etilgan. U mashhur ko‘palfavitli tizim

hisoblanadi. Vijnern tizimi Sezar shifrlash tizimiga qaraganda mukammalroq hisoblanib, unda kalit harfdan harfga almashtiriladi. Bunday ko‘p alfavitli almashtirish shifrlash jadvali orqali ifodalash mumkin. Quyidagi jadvallarda rus va lotin alfavitlari uchun mos keluvchi jadvallarko‘rsatilgan. Bu jadvallardan matnni shifrlash va uni ochish uchun foydalaniladi. Jadvalning ikkita kirishi bo‘lib:

yuqori qatordagi harflardan kiruvchi ochiq yozuv uchun foydalaniladi.

chap ustunda esa kalit so‘zi joylashadi.

Ochiq matnni shifrlashda bu matn bir satrga yoziladi. Uning ostidagi satrga kalit so‘z joylashtiriladi. Agar kalit so‘zning uzunligi qisqa bo‘lsa, bu so‘z ochiq matnning oxirgi harfigacha takrorlab yoziladi. Shifrlash jarayonida jadvalning yuqori qismida joylashgan ochiq matnning harfi topiladi va chap qismdan kalit so‘zning harfi tanlanadi. Satr va ustun kesishgan katakdagi harf berilgan harfni almashtiradi.

2.5-jadval.

Xabar	B	A	Y	R	A	M	K	U	N	I
Kalit	V	A	Z	A	V	A	Z	A	V	A
Shifrmtn	G	A	R	R	V	M	S	U	P	I

Vijnerning shifrlash tizimi. XVI asrda fransuz diplomati Vijnern tomonidan yaratilgan shifrlash tizimi 1586-yilda chop etilgan. U mashhur ko‘palfavitli tizim hisoblanadi. Vijnern tizimi Sezar shifrlash tizimiga qaraganda mukammalroq hisoblanib, unda kalit harfdan harfga almashtiriladi. Bunday ko‘p alfavitli almashtirish shifrlash jadvali orqali ifodalash mumkin. Quyidagi jadvallarda rus va lotin alfavitlari uchun mos keluvchi jadvallar ko‘rsatilgan. Bu jadvallardan matnni shifrlash va uni ochish uchun foydalaniladi.

Jadvalning ikkita kirishi bo‘lib:

- yuqori qatordagi harflardan kiruvchi ochiq yozuv uchun foydalaniladi.
- chap ustunda esa kalit so‘zi joylashadi.

Ochiq matnni shifrlashda bu matn bir satrga yoziladi. Uning ostidagisatrga

		PLAINTEXT LETTERS																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
KEYWORD LETTERS	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	G	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	H	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	J	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	K	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	L	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	M	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	N	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	O	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Q	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	R	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	U	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	V	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1. O'rin almashtirish orqali shifrlash.
2. Sezarning shifrlash tizimi.
3. Vijnerning shifrlash tizimi.

Tayanch iboralar: Ma'lumotlarni shifrlash, arxivlash, WinRar arxivlash dasturi, WinZip arxivlash dasturi.

Fayllarni arxivlash - fayllarni arxivlash jarayoni orqali siqilgan, ixchamlangan holatda diskda saqlash demakdir. Arxivlash qattiq disk ishdan chiqishi yoki faylning tasodifan o'chirilishi sodir bo'lgan hollarda joriy faylni qayta tiklash uchun yordam beruvchi vosita sifatida ham qo'llaniladi.

Bunda har bir qism fayl ham arxiv fayli deb ataladi.

Arxivlash jarayonida ayrim fayllar juda yaxshi ixchamlanishi, bahzi hollarda arxivlash natijasida boshlang'ich fayl 10-20 baravar siqilishi ham mumkin.

Masalan, dastur fayllariga nisbatan tekst va rasm fayllari ancha yaxshi ixchamlanadi.

Hozirgi kunda har xil arxivatorlar bir-biridan siqish darajasi, tezligi, foydalanishda qulayliklari, imkoniyat darajasi bo'yicha farq qiladi. Foydalanuvchi har xil turdagi arxiv fayllarini kengaytmasi bo'yicha farqlaydi. Siqish turi shu arxivning formati deyiladi.

Arxivlangan fayl arxivda qaysi fayllar borligini bildiruvchi sarlavhaga ega bo'ladi. Arxiv sarlavhasida unda saqlanuvchi har bir fayl uchun quyidagi ma'lumotlar saqlanadi:

- fayl nomi;
- fayl saqlanuvchi katalog haqida ma'lumot;
- faylning oxirgi marta qayta ishlangan sanasi va vaqti;
- faylning diskdagi va arxivdagi o'lchami;
- arxivning to'liqligini tekshirishda ishlatiladigan har bir faylning tsiklik tekshirish kodi.

Arxiv fayllari oddiy fayllar kabi nomlanadi. quyida biz Windowsmuhitida fayllarni arxivlash uchun yaratgan WinRar dasturi bilan tanishib chiqamiz.

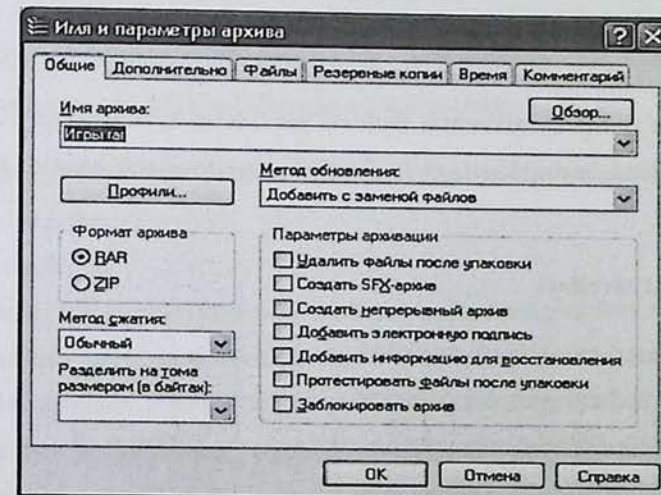
WinRar arxivlash dasturi

WinRar arxivlovchi dasturi RAR formatidagi arxiv fayllari hosil qiladi.

RAR formatidagi arxivning ustunlik tomonlari bir nechta bo'lib, ular birinchidan zichlash samaradorligi ancha yuqori, ikkinchidan ko'p tomli va uzuluksiz arxivlar hosil qila oladi, uchinchidan 8 Eksobaytgacha hajmli fayllarni xam arxivlash imkonini beradi.

Tom deb arxivning bir necha qismdan iborat bo'laklarga bo'linishiga aytiladi.

Odatda tomlar katta xajmdagi arxivni bir necha disklarda saqlash uchun qo'llaniladi. Bu xolda birinchi tom odatdagidek .rar kengaytmali bo'ladi, qolganlari esa mos ravishda .r00, .r01, .r02 va xokazo. Tomlar xam uzuluksiz vaxam o'zini-o'zi ochadigan ko'rinishlarda bo'lishi mumkin. Yaratilgan tomlarni o'zgartirish, Ya'ni unga biror faylni qo'shish, yangilash yoki undan biror faylni o'chirish mumkin emas.



2.7-rasm. WinRar arxivlash dasturi oynasi.

Fayl va papkalarni uzuluksiz arxivlash deganda, ularni faqat RAR formatida, maxsus usulda bitta ma'lumotlar ketma-ketligi sifatida qaralib zichlashtirishga aytiladi. Bu bilan zichlash samaradorligi ancha yuqori bo'lishiga erishiladi. Ammo bunday arxivlashning kamchiliklari xam bor, masalan:

ularni yangilash, yahni orasidagi biror faylni yangisi bilan almashtirish, oddiy arxivlashdan ko'ra sekinroq amalga oshiriladi;

biror faylni arxivdan chiqarish uchun barcha oldinroqda turganlari tekshirib chiqiladi, agar ulardan birortasi buzilgan bo'lsa, u xolda arxivdan umuman chiqarib bo'lmaydi;

Bunday arxivlash usulidan quyidagi xollarda foydalangan maqsadga muvofiq: arxivni kamdan-kam yangilansa;

- arxivdagi fayllardan bir yoki bir nechtasini tez-tez chiqarib turish zarurati bo'lmasa;

zichlash samaradorligi zichlash tezligidan muhimroq bo'lsa.

Bu arxivlovchi dastur xar ikkala formatda xam, kompyuterda WinRar arxivatori bo'lmasa xam o'zini-o'zi ocha oladigan SFX ko'rinishidagi .exe kengaytmali arxiv fayllari yaratish imkonini beradi. Shuning uchun uni to'g'ridan-

to'g'ri ishga tushirish orqali ochish mumkin. Bu xolda barcha fayllar arxivdan chiqadi.

Bundan tashqari arxivlangan fayllarni parol bilan himoyalab qo'yish, fizik buzilgan fayllarni qayta tiklash va boshqa ko'pgina amallarni bajarish imkonini yaratib beradi.

Nazorat savollari

1. Ma'lumotlarni shifrlash dasturlari.
2. Ma'lumotlarni arxivlash dasturlari.
3. Arxivlash dasturlarining imkoniyatlari.

8-Mavzu: Steganografiya.

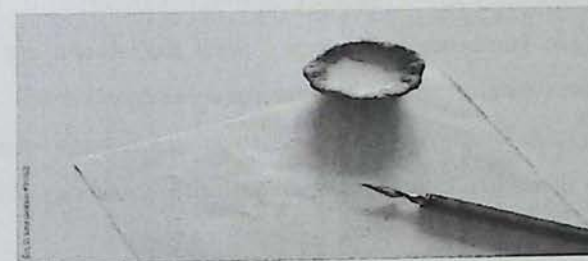
Tayanch iboralar: Steganografiya tushunchasi, Steganografiyadan foydalanishning tarixiy faktlari, "Micropoint" tushunchasi.

Steganografiya - bu uzatish faktini sir tutgan holda ma'lumotni yashirin uzatish haqidagi fan.

Tarixiy faktlar

Qadimgi Rimda mum taxtasidan qirib tashlanib, keyin ular daraxtga yashirin xabarni tirnashdi, keyin mum bilan qoplangan va mum ustida ochiq xat yozgan.

Lenin qamoqqa olinib, o'z asarlarini sut bilan yozgan, xavf tug'ilganda yoyayotgan non bo'laklarining "siyoh"iga quygan. Shu tarzda yozilgan varaqlar vasiyatnomaga topshirilib, u yerda choyshablar chiroq yoki sham ustida qizdirilib, partiya a'zolari tomonidan ko'chirilgan.



2.8-rasm. Qog'ozga sut bilab yozish jihozlari.

«Mikro nuqta» Kattalashtirilganda "mikrodot" bosilgan sahifaning tasvirini, chizmalarini, chizmalarini beradi.

Steganografiya turkumlari

1. 90-yillarning oxirida steganografiyaning bir necha yo'nalishlari paydo bo'ldi:
2. Klassik steganografiya - "kompyuter bo'lmagan usullar" ni o'z ichiga oladi.
3. Kompyuter steganografiyasi - kompyuter platformasining xususiyatlariga va kompyuter ma'lumotlar formatlarining maxsus xususiyatlaridan foydalanishga

asoslangan klassik steganografiyaning yo'nalishi.

4. Raqamli steganografiya - klassik steganografiyaning raqamli ob'ektlarga qo'shimcha ma'lumotlarni yashirish yoki kiritishga asoslangan yo'nalish bo'lib, bu ob'ektlarning ma'lum bir buzilishlarini keltirib chiqaradi.

Steganografiyaning asosiy vazifalari

- Maxfiy ma'lumotlarni ruxsatsiz kirishdan himoya qilish;
- Tarmoq resurslarini monitoring qilish va boshqarish tizimlarini yengish;
- Kamuflyaj dasturi;
- Intellektual mulkning ayrim turlari uchun mualliflik huquqini himoya qilish.

Steganografik tizim yoki stegotizim - maxfiy axborot uzatish kanalini shakllantirish uchun foydalaniladigan vositalar va usullar to'plami.

Konteyner - maxfiy xabarlarni yashirish uchun mo'ljallangan har qanday ma'lumot. Bo'sh konteyner - o'rnatilgan xabarsiz konteyner;

To'ldirilgan konteyner yoki stego - ichki ma'lumotni o'z ichiga olgan konteyner. Inline (yashirin) xabar - konteynerga o'rnatilgan xabar.

Steganografik kanal yoki oddiygina stego kanali stego uzatish kanalidir. Stegokey yoki shunchaki kalit ma'lumotni yashirish uchun zarur bo'lgan maxfiy kalitdir.

Stegotizimdagi himoya darajalari soniga (masalan, oldindan shifrlangan xabarni joylashtirish) qarab, bir yoki bir nechta stegokey bo'lishi mumkin.

Stegotizimga hujimlar

- Ma'lum to'ldirilgan konteynerga asoslangan hujum.
- Ma'lum o'rnatilgan xabarga asoslangan hujum.
- Tanlangan yashirin xabarga asoslangan hujum.
- Tanlangan yashirin xabarga asoslangan moslashuvchan hujum.
- Tanlangan to'ldirilgan konteynerga asoslangan hujum.

- Ma'lum bo'sh konteynerga asoslangan hujum.
- Tanlangan bo'sh konteynerga asoslangan hujum.
- Konteyner yoki uning bir qismining ma'lum matematik modeliga asoslangan hujum.

Nazorat savollari.

1. Qadimda steganografiyaning qo'llanilishi.
2. Kompyuter steganografiyasi.
3. Raqamli steganografiya.

9-MAVZU: Ochiq kalitli shifrlash algoritmlari.

Tayanch iboralar: Ochiq kalitli shifrlash, Raqamli sertifikatlar, Skriptografikmustaxkamlik, ERI.

Zamonaviy kriptografiya quyidagi bo'limlarni o'z ichiga oladi.

1. Simmetrik kriptotizimlar
2. Assimetrik kriptotizimlar.

Simmetrik kriptotizimlar. Simmetrik kriptotizimlarda shifrlash va deshifrlash uchun bitta kalitdan foydalaniladi. (Shifrlash – ochiq matn deb ataluvchi dastlabki matnni shifrlangan matn holatiga o'tkazish. Deshifrlash – shifrlashga teskari bo'lgan jarayon yani kalit yordamida shifrlangan matnni dastlabki matn holatiga yetkazish). Demak, shifrlash kalitidan foydalanish huqukiga ega bo'lgan odamgina axborotni deshifrlashi mumkin. Shu sababli, simmetrik kriptotizimlar mahfiy kalitli kriptotizimlar deb yuritiladi. Ya'ni shifrlashkalitidan faqat axborot atalgan odamgina foydalana olishi mumkin.

Asimetrik kriptotizimlar. Assimetrik kriptotizimlarda bir-biriga matematik usullar bilan bog'langan ochiq va maxfiy kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan bo'ladi, shifrni ochish esa faqat maxfiy kalit yordamida amalga oshiriladi, maxfiy kalit faqat qabul qiluvchigagina ma'lum va uni ruhsatsiz foydalanishdan ishonchli himoyalashi zarur. Asimetrik kriptotizimda axborotni himoyalash axborot qabul qiluvchi kalitining mahfiyligiga asoslangan.

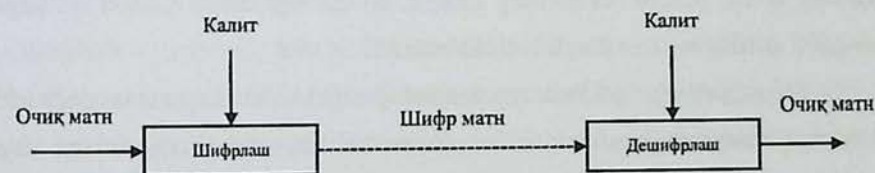
Kriptografik metodlardan foydalanishning asosiy yo'nalishlari – aloqa kanallari orqali maxfiy axborotni uzatish (masalan, elektron pochta), uzatiladigan xabarlarni aslligini o'rnatish, ma'lumotlarni (hujjatlar, ma'lumotlar bazalari) ko'chma tashuvchi xotiralarda shifrlangan shaklda saqlash.

Bugungi kunda deyarli barcha ma'lumotlar almashinish axborot texnologiya vositalari orqali amalga oshirilmoqda. Bu esa o'z navbatida, ushbu ma'lumotlarni

boshqa begona shaxslar tomonidan noqonuniy tarzda ko'rish, o'zgartirish va qayta yuborishga bo'lgan xatti-harakatlarni oldini olish va axborot xavfsizligini ta'minlashga bo'lgan ehtiyojni yanada ortishiga olib keldi.

- *Kriptologiya* – maxfiy kodlar"ni yaratish va buzish fani va sanati;
- *Kriptografiya* – maxfiy kodlar"ni yaratish bilan shug'ullanadi;
- *Kriptologiya* – maxfiy kodlar"ni buzish bilan shug'ullanadi;
- *Kripto* – yuqoridagi tushunchalarga (hattoki bundanda ortig'iga) sinonim bo'lib, kontekst ma'nosiga ko'ra farqlanadi.

Shifr yoki kriptotizim ma'lumotni shifrlash uchun foydalaniladi. Haqiqiy shifrlanmagan ma'lumot ochiq matn deb atalib, shifrlashning natijasi shifrmtn deb ataladi. Haqiqiy ma'lumotni qayti tiklash uchun shifrmtnni deshifrlash zarur bo'ladi. Kalit kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi. Kriptotizimning "qora quti" sifatidagi ko'rinishi 2.9 – rasmda keltirilgan.



2.9-rasm. Kriptotizimning "qora quti" sifatidagi ko'rinishi

Shifrlash va deshifrlash masalalariga tegishli bo'lgan, ma'lum bir alfavitda tuzilgan ma'lumotlar matnlarni tashkil etadi.

Alfavit - axborotlarni ifodalash uchun foydalaniladigan chekli sondagi belgilar to'plami. Misollar sifatida:

- o'ttiz oltita belgidan (harfdan) iborat o'zbek tili alfaviti;
- o'ttiz ikkita belgidan (harfdan) iborat rus tili alfaviti;
- yigirma sakkizta belgidan (harfdan) iborat lotin alfaviti;
- ikki yuzi ellik oltita belgidan iborat ASSII kompyuter belgilarining alfaviti;
- binar alfavit, Ya'ni 0 va 1 belgilardan iborat bo'lgan alfavit;
- sakkizlik va o'n oltilik sanoq sistemalari belgilaridan iborat bo'lgan

alfavitlarni keltirish mumkin.

Simmetrik shifr: Simmetrik shifrlarda ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi. Bundan tashqari ochiq kalitli (assimetrik) kriptotizimlar mavjud bo'lib, unda shifrlash va deshifrlash uchun turlicha kalitlardan foydalaniladi. Turli kalitlardan foydalanilgani bois, shifrlash kalitini oshkor qilsa bo'ladi va shuni uchun ochiq kalitni kriptotizim deb ataladi. Ochik kalitni kriptotizimlarda shifrlash kalitini ochiq kaliti deb atalsa, deshifrlash kalitini shaxsiy kalit deb ataladi. Simmetrik kalitli kriptotizimlarda esa kalit - simmetrik kalit deb ataladi.

Kerkxofs prinsipi

Ideal shifrlar uchun kalitsiz shifmatndan ochiq matnni tiklashning imkoni bo'lmasligi zarur. Bu shart, hattoki hujumchilar uchun ham o'rinli. Hujumchi algoritmi (Shifrlash algoritmi) haqida barcha ma'lumotlarni bilgan taqdirda ham kalitsiz ochiq matnni tiklashning imkoni bo'lmasligi zarur. Ushbu qo'yilgan maqsad, amalda bundan farqdi bo'lishi mumkin.

Kriptografiyaning fundamental nazariyasiga ko'ra kriptotizimning ichki ishlash prinsipi hujumchiga to'liq oshkor bo'lishi zarur. Hujumchiga faqat kriptotizimda foydalanilgan kalit noma'lum bo'lishi zarur. Bu ta'limot Kerkxofs prinsipi deb ataladi.

Kerkxofs prinsipining asosiy mohiyati. Agar hujumchi kriptotizimni qanday ishlashini bilmasa, u holda uni kriptotizimga hujum qilishi yanada qiyinlashadi. U holda, nima uchun biz xujumchini ishini osonlashtirmoqdamiz? Kriptotizim xavfsizligi uchun sir tutilgan loyihalashga ishonishning bir nechta muammolari mavjud. Birinchidan, —sir tutilgan” kriptotizimlarning tavsilotlari kamdan-kam hollarda uzoq vaqt sir saqlanib qoladi. Dasturiy ta'minotdan algoritmi tiklash uchun teskari muhandislik usullaridan foydalanish mumkin va ular orqali hattoki qurilmalarda yozilgan algoritmlarni qayta tiklash (aniqlash) mumkin. Bundan tashqari yana bir muhim jixat shundaki, uzoq vaqt sir tutilgan kriptotizim ommaga oshkor bo'lganda, xavfsiz emasligi isbotlangan. Sir tutilgan kriptotizimlar kichik

doiradagi foydalanuvchilar (mutaxassislar) tomonidan ishlab chiqilgani va testlangani bois, ko'p sonli foydalanuvchilar (ommaga oshkor etilganda) tomonidan testlanish natijasida uni xavfsiz emasligi ko'p hollarda aniqlangan. Bunga misol sifatida, Microsoft tomonidan kriptotizimlar ishlab chiqishda

Kodlash va shifrlash orasidagi farq.

Aksariyat hollarda foydalanuvchilar ma'lumotni shifrlash va kodlash tushunchalarini bir xil deb tushuniladi. Aslida esa ular ikki turlicha tushunchalardir. Kodlash – ma'lumotni osongina qaytarish uchun hammaga (hattoki hujumchiga ham) ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir. Kodlash ma'lumotlardan foydalanish qulayligini ta'minlash uchun amalga oshiriladi va hamma uchun ochiq bo'lgan sxemalardan foydalaniladi. Masalan, ASCII, UNICODE, URL Encoding, base64.

ASCII kodlash standarti

Shifrlash – jarayonida ham ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar (deshifrlash kalitiga ega bo'lgan) qayta o'zgartirishi mumkin bo'ladi. shifrlashdan asosiy maqsad ma'lumotni maxfiylikini ta'minlash bo'lib, uni qayta o'zgartirish ba'zi shaxslar (deshifrlash kalitiga ega bo'lmagan) uchun cheklangan bo'ladi.

Dekodlash jarayoni ham deshifrlash jarayoni kabi kodlash uchun teskari jarayon hisoblanib, biror ochiq sxema yordamida o'zgartirilgan ma'lumotlar xuddi shu sxema asosida teskari o'zgartiriladi. Masalan, ASCII asosida —Z” ni 16sanoq tizimiga o'zgartirilganda (kodlaganda) u —5A” ga teng bo'lgan bo'lsa, —5A” ni dekodlash jarayonida u —Z” ga qayta o'zgartiriladi.

Kriptografiyada esa jo'natuvchi faqat ochiq matn ko'rinishidagi xabar yuborishi mumkin, bunda u xabarni ochiq tarmoq (masalan, Internet) orqali uzatishdan oldin shifrlangan matnga o'zgartiradi. Ushbu shifrlangan xabar qabul qiluvchiga kelganida esa yana oddiy matn ko'rinishiga qaytariladi. Umumiy holda ma'lumotni shifrlashdan asosiy maqsad (simmetrik yoki ochiq kalitli kriptografik

tizimlar asosida farqi yo'q) – ma'lumotni maxfiyligini qolganlardan sir tutishdir.

Ochiq kalitli shifrlash algoritmlari.

Ochiq kalitli tizimlarini qo'llash asosida qaytarilmas yoki bir tomonli funktsiyalardan foydalanish yotadi. Bunday funktsiyalar quyidagi xususiyatlarga ega. Ma'lumki ma'lum bo'lsa $y=f(x)$ funktsiyani aniqlash oson. Ammo uning ma'lum qiymati bo'yicha x ni aniqlash amaliy jihatdan mumkin emas. Kriptografiyada yashirin deb ataluvchi yo'lga ega bo'lgan bir tomonli funktsiyalar ishlatiladi. parametrli bunday funktsiyalar quyidagi xususiyatlarga ega. Ma'lum uchun Ez va Dz algoritmlarini aniqlash mumkin. Ez algoritmi yordamida aniqlik sohasidagi barcha x uchun $fz(x)$ funktsiyani osongina olish mumkin. Xuddi shu tariqa Dz algoritmi yordamida joiz qiymatlar sohasidagi barcha x uchun teskari funktsiya $x=f^{-1}(y)$ ham osongina aniqlanadi. Ayni vaqtda joiz qiymatlar sohasidagi barcha y va deyarli barcha, uchun xatto Ez ma'lum bo'lganida ham $f^{-1}(y)$ ni hisoblashlar yordamida topib bo'lmaydi. Ochiq kalit sifatida ishlatilsa, maxfiy kalit sifatida x ishlatiladi.

Ochiq kalitni ishlatib shifrlash amalga oshirilganda o'zaro muloqatda bo'lgan sub'ektlar o'rtasida maxfiy kalitni almashish zaruriyati yo'qoladi. Bu esa o'z navbatida uzatiluvchi axborotning kriptohimoyasini soddalashtiradi.

Ochiq kalitli kriptotizimlari bir tomonli funktsiyalar ko'rinishi bo'yicha farqlashmumkin. Bularning ichida RSA, El'-Gamal va Mak-Elis tizimlarini aloxida tilga olish o'rinli. Hozirda eng samarali va keng tarqalgan ochiq kalitli shifrlash algoritmi sifatida RSA algoritmini ko'rsatish mumkin. RSA nomi algoritmni yaratuvchilari familiyalarining birinchi xarfidan olingan (Rivest, Shamir va Adleman).

RSA algoritmi. Ko'p sonli turli ochiq kalitli kriptotizimlar ichida keng tarqalgani 1977-yilda ixtiro qilingan va uning mualliflari Ron Rivest, Ada Shamir va Leonard Eydelman nomiga qo'yilgan RSA kriptotizimidir. Ular, katta tub sonlarni aniqlash, hisoblash jihatdan oddiy ekanligidan hamda shunday ikkita katta

sonlarning ko'paytmasi bo'lgan sonni ko'paytuvchilarga ajratish judayam qiyin, amalda mumkin emasligidan foydalanishgan. RSA shifrini ochish shunday ko'paytuvchilarga ajratishga tengligi isbotlangan (Rabin teoremasi). Shuning uchun kalit uzunligi qanday bo'lishidan qat'iy nazar shifrnı ochish uchun talab qilinadigan amallarning quyi chegarasini baholash, zamonaviy kompyuterlarning tezligini bilgan holda shifrnı ochish uchun kerak bo'ladigan vaqtnı ham aniqlash mumkin.

RSA algoritmining himoyalanganlik kafolatini aniqlash imkoniyati, uning boshqa ochiq kalitli algoritmlar orasida mashhur bo'lishining sababi hisoblanadi. Shuning uchun RSA algoritmidan bank kompyuter tizimlarida foydalanilmoqda, ayniqsa uzoq masofadagi mijozlar bilan ishlashda (kredit kartochkalarga xizmat ko'rsatishda) qo'llanilmoqda.

Algoritm modul' arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan. Algoritmni quyidagi qadamlar ketma-ketligi ko'rinishida ifodalash mumkin.

1-qadam. Ikkita 200 dan katta bo'lgan tub son p va q tanlanadi.

2-qadam. Kalitning ochiq tashkil etuvchisi n hosil qilinadi $n=p \cdot q$.

3-qadam. Quyidagi formula bo'yicha Eyler funktsiyasi hisoblanadi:

$$\phi(p, q) = (p-1) \cdot (q-1).$$

Eyler funktsiyasi n bilan o'zaro tub, 1 dan n gacha bo'lgan butun musbat sonlar sonini ko'rsatadi. O'zaro tub sonlar deganda 1 dan boshqa birorta umumiy bo'luvchisiga ega bo'lmagan sonlar tushuniladi.

4-qadam. $f(p, q)$ qiymati bilan o'zaro tub bo'lgan katta tub son d tanlabolinadi.

5-qadam. Quyidagi shartni qanoatlantiruvchi e soni aniqlanadi

$$e \cdot d \bmod \phi(p, q) = 1$$

Bu shartga binoan ko'paytmaning $f(p, q)$ funktsiyaga bo'lishdan qolganqoldiq 1ga teng. e soni ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabulqilinadi. Maxfiy kalit sifatida d va n sonlari ishlatiladi.

6-qadam. Dastlabki axborot uning fizik tabiatidan qat'iy nazar raqamli ikkili ko'rinishda ifodalanadi. Bitlar ketma-ketligi L bit uzunlikdagi bloklarga ajratiladi,

bu erda $L \geq \log_2 l$ shartini qanoatlantiruvchi eng kichik butun son. Har bir blok $[0, n-1]$ oraliqqa taalluqli butun musbat son kabi ko'riladi. Shunday qilib, dastlabki axborot $X(i)$, $i =$ sonlarning ketma-ketligi orqali ifodalanadi. I ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

7-qadam. shifrlangan axborot quyidagi formula bo'yicha aniqlanuvchi $Y(i)$ sonlarning ketma-ketligi ko'rinishida olinadi:

Axborotni Deshifrlash qilishda quyidagi munosabatdan foydalaniladi:
 $X(i) = (Y(i))^d \pmod{n}$.

Misol. "GAZ" so'zini shifrlash va deshifrlash qilish talab etilsin. Dastlabki so'zni shifrlash uchun quyidagi qadamlarni bajarish lozim.

1-qadam. $p=3$ va $q=11$ tanlab olinadi.

2-qadam. $n=p \cdot q=33$ hisoblanadi.

3-qadam. $f(p,q)=(p-1) \cdot (q-1)=20$ Eyler funktsiyasi aniqlanadi.

4-qadam. O'zaro tub son sifatida $d=3$ soni tanlab olinadi.

5-qadam. $e \cdot d \pmod{f(p,q)}=1$ shartini qanoatlantiruvchi e soni tanlanadi.

Aytaylik, $e=7$.

6-qadam. Dastlabki so'zning alfavitdagi xarflar tartib raqami ketma-ketligiga mos son ekvivalenti aniqlanadi. A xarfiga -1, G xarfiga -4, Z xarfiga -9. O'zbek alfavitida 36ta xarf ishlatilishi sababli ikkili kodda ifodalash uchun $6 \geq \log_2 36$ ta ikkilixona kerak bo'ladi. Dastlabki axborot ikkili kodda quyidagi ko'rinishga ega bo'ladi:

2.7-jadval

G	A	Z
000100	000001	001001

000100 000001 001001.

Blok uzunligi butun sonlar ichidan shartini qanoatlantiruvchi minimal' sonsifatida aniqlanadi. $L \geq \log_2 33$ bo'lganligi sababli $L=6$.

Demak, dastlabki matn ketma-ketlik ko'rinishida ifodalanadi.

7-qadam. Ketma-ketligi ochiq kalit $\{7,33\}$ yordamida shifrlanadi:

$$Y(1) = (4^7 \pmod{33}) = 16384 \pmod{33} = 16$$

$$Y(2) = (1^7 \pmod{33}) = 1 \pmod{33} = 1$$

$$Y(3) = (9^7 \pmod{33}) = 4782969 \pmod{33} = 15$$

Shifrlangan so'z $Y(i) = \langle 16, 1, 15 \rangle$

Shifrlangan so'zni Deshifrlash qilish maxfiy kalit $\{3,33\}$ yordamida bajariladi:

$$Y(1) = (16^3 \pmod{33}) = 4096 \pmod{33} = 4$$

$$Y(2) = (1^3 \pmod{33}) = 1 \pmod{33} = 1$$

$$Y(3) = (15^3 \pmod{33}) = 3375 \pmod{33} = 9$$

Dastlabki son ketma-ketligi Deshifrlash qilingan $X(i) = \langle 4, 1, 9 \rangle$ ko'rinishida dastlabki matn bilan almashtiriladi. Natijada "GAZ" dastlabki matn hosil bo'ladi.

Keltirilgan misolda hisoblashlarning soddaligini ta'minlash maqsadida mumkinbo'lgan kichik sonlardan foydalanildi.

El'-Gamal tizimi. El'-Gamal tizimi chekli maydonlarda diskret logarifmlarning hisoblanish murakkabligiga asoslangan. RSA va El'-Gamal tizimlarining asosiy kamchiligi sifatida modul' arifmetikasidagi murakkab amallarning bajarilishi zaruriyatini ko'rsatish mumkin. Bu o'z navbatida aytarlicha hisoblash resurslarini talab qiladi.

Mak-Elis kriptotizimida xatoliklarni tuzatuvchi kodlar ishlatiladi. Bu tizim RSA tizimiga nisbatan tezroq amalga oshirilsada, jiddiy kamchilikka ega. Mak-Elis kriptotizimida katta uzunlikdagi kalit ishlatiladi va olingan shifmatn uzunligi dastlabki matn uzunligidan ikki marta katta bo'ladi.

Barcha ochiq kalitli shifrlash metodlari uchun NP-to'liq masalani (to'liq saralash masalasi) echishga asoslangan kriptotaxlil metodidan boshqa

metodlarining yo'qligi qat'iy isbotlanmagan. Agar bunday masalalarni echuvchi samarali metodlar paydo bo'lsa, bunday xildagi kriptotizim obro'sizlantiriladi.

Yuqorida ko'rilgan shifrlash metodlarining kriptoturg'unligi kalit uzunligiga bog'liq bo'lib, bu uzunlik zamonaviy tizimlar uchun, loaqal, 90 bitdan katta bo'lishi shart. Ayrim muhim qullanishlarda nafaqat kalit, balki shifrlash algoritmi ham mahfiy bo'ladi. shifrlarning kriptoturg'unligini oshirish uchun bir necha kalit (odatda uchta) ishlatilishi mumkin. Birinchi kalit yordamida shifrlangan axborot ikkinchi kalit yordamida shifrlanadi va h.

Shifrlashning o'zgaruvchan algoritmlarini qo'llash tavsiya qilinadi. Bunda shifrlash kaliti shifrlashning muayyan algoritmini tanlash uchun ham ishlatiladi.

Ochiq kalitlardan foydalanuvchi shifrlash metodlarining afzalligi, avvalo, maxfiy kalitlarni tarqatish zaruriyatining yo'qligidir. Katta masofalarda tarqalgan komp'yuter tizimlari uchun maxfiy kalitlarni tarqatish aytarlicha murakkab masala hisoblanadi. Ochiq kalitli tizimlarning ommalashuviga maxfiy kalitlarning faqat ularni to'liq saralash orqali olinishidan boshqa yo'l bilan olib bo'lmasligi isbotining yo'qligi to'sqinlik qiladi.

RSA tizimi bo'yicha loyiha keyslarini yaratish va talabalar bilimini tekshirish usullari.

Ishdan maqsad: RSA shifrlash algoritmi ishlash prinsipini o'rganish vauning dasturlash tillarida loyihalash.

RSA kriptografik algoritimning python dasturlash tilida yozilgan dasturi:

#1-Qadam. RSA shifrlash algoritmi uchun 200 dan kam bo'lmaga p vaq sonlarini kiriting!

```
print('p tub son kiriting! p:=')
```

```
p=int(input())
```

```
print('q tub son kiriting! q:=')
```

```
q=int(input())
```

```
# n ni aniqlaymiz
```

```
n=p*q print('n=',n)
```

```
#3-Qadam
```

```
#Eyler funksiyasi m ni aniqlaymiz.
```

```
m=(p-1)*(q-1)
```

```
print('m=',m)
```

```
#4-Qadam
```

```
# m bilan o'zoro tub bo'lgan {t} sonlar to'plami aniqlanadi
```

```
t=[]
```

```
for i in range (1,m+1):
```

```
    k=0
```

```
    for j in range (1,i+1):
```

```
        if i%j==0:
```

```
            k=k+1
```

```
    if k==2:
```

```
        if m%i!=0:
```

```
            t.append(i)
```

```
print("d=",t)
```

```
# {t} sonlar to'plamidan tasodifiy d-DESHIFRLASH kaliti tanlanadi
```

```
import random d=random.choice(t)
```

```
print("Deiflash kaliti tanlanadi(d;n):=",d,";",n)
```

```
#5-Qadam
```

```
# (e*d mod m=1) tenglamadan e-SHIFRLASH kaliti topiladi
```

```
e=1
```

```
while (e*d%m!=1)or(e==d):
```

```
    e=e+1
```

```
print("Sifrlash kaliti (e;n):=",e,";",n)
```

```
#Ochiq matn shifrlash JARAYONI
```

```
shifmatn=[]
```

```
s=input("Ochiq matn kiriting:")
```

```
s1="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
l=len(s)
```

```
for t in range (0,l):
```

```
    x = s1.index(s[t])+1
```

```
    y=x**e%n
```

```
    shifmatn.append(y)print(x," ",end="")
```

```
print("shifmatn:",shifmatn)
```

```
#DESHIFRLASH JARAYONI
```

```
deshifmatn=[]
```

```
s=shifmatn
```

```
l=len(s)
```

```
for t in range (0,l):
```

```
    y=int(s[t])**d%n
```

```
    deshifmatn.append(y)
```

```
print("deshifmatn:",deshifmatn)
```

```
#DESHIFRLASH KODINI HARFLARGA O'GIRISH
```

```
s0=""
```

```
s1="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
for t in range (0,l):
```

```
    z=deshifmatn[t]-1
```

```
    s0=s0+s1[z]
```

```
print(s0)
```

```
RSA FAYL BILAN ISHLASHGA MO'JALLANGAN DASTURI:
```

```
fin = open("input.txt")
```

```
fout = open("output.txt","w")
```

```
s = fin.readline()
```

```
l=len(s)
```

```
print("Matn uzunligi:",l)
```

```
#1-Qadam
```

```
print('p tub son kiriting! p:=')p=int(input())
```

```
print('q tub son kiriting! q:=')q=int(input())
```

```
#2-Qadam
```

```
# n ni aniqlaymizn=p*q print('n=',n)
```

```
#3-Qadam
```

```
#Euler formulasidan m ni aniqlaymiz
```

```
m=(p-1)*(q-1)
```

```
print('m=',m)
```

#4-Qadam

m bilan o'zaro tub bo'lgan {t} sonlar to'plami aniqlanadi

```
t=[]
for i in range (1,m+1):
    k=0
    for j in range (1,i+1):
        if i%j==0:
            k=k+1
    if k==2:
        if m%i!=0:
            t.append(i)
```

```
print("d=",t)
```

{t} sonlar to'plamidan tasodifiy d-DESHIFRLASH kaliti tanlanadi

```
import random
d=random.choice(t)
print("Deifrlash kaliti tanlanadi(d;n):=",d,";",n)
```

#5-Qadam

($e \cdot d \bmod m = 1$) tenglamadan e-SHIFRLASH kaliti topiladi

```
e=1
while (e*d%m!=1)or(e==d):
    e=e+1
print("Sifrlash kaliti (e;n):=",e,";",n)
```

#Ochiq matn shifrlash JARAYONI

```
index=[]
shifrmtn=[]
shifrmtn2=""
```

```
for t in range (0,l):
    x = ord(s[t])
    index.append(x)
    y=x**e%n
    shifrmtn.append(y)
    shifrmtn2+=bin(y)

print("index:",index)
print("shifrmtn:",shifrmtn)
print("shifrmtn2:",shifrmtn2)
print("Shifrlash muvofiqiyatli bajarildi!!!")
```

#DESHIFRLASH JARAYONI

```
deshifrmtn=[]
s=shifrmtn
for t in range (0,l):
    y=int(s[t])**d%n
    deshifrmtn.append(y)
print("deshifrmtn:",deshifrmtn)
```

#DESHIFRLASH KODINI HARFLARGA O'GIRISH

```
ss=""
for t in range (0,l):
    son=deshifrmtn[t]
    ss+=chr(son)
print(ss)
```

```
fout.write(str(s))
fout.write("\n")
fout.write(str(index))
```

```

fout.write("\n")
fout.write(str(shifmatn))
fout.write("\n")
fout.write(shifmatn2)
fout.write("\n")
fout.write(str(ss))
fin.close()
fout.close()
i=input("Deshifrlash muvofiqiyatli bajarildi!!!")

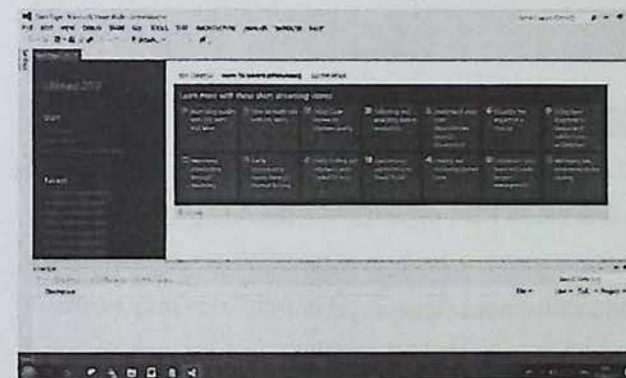
```

Keys topshiriq: Microsoft Visual Studio muhitining WindowsFormsApplication

C# dasturlash tilida RSA algoritmi loyihasini bajarish tartibi.

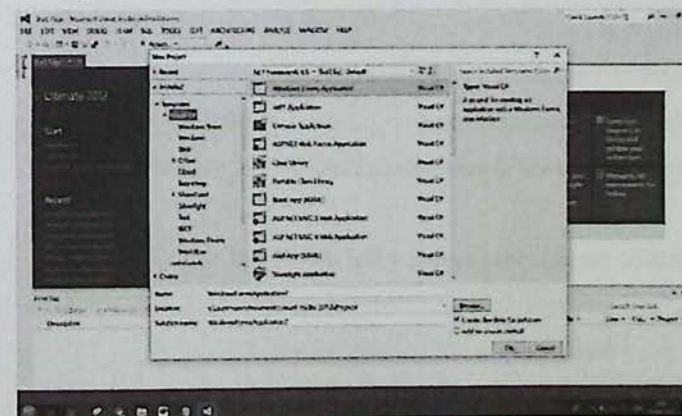
Microsoft Visual Studio muhitida loyiha yaratish uchun:

1. Microsoft Visual Studio ilovasini <https://visualstudio.microsoft.com> rasmiysaytida yuklaymiz va komputerrimizga o'rnatamiz.
2. Microsoft Visual Studio ilovasini ishga tushiramiz.



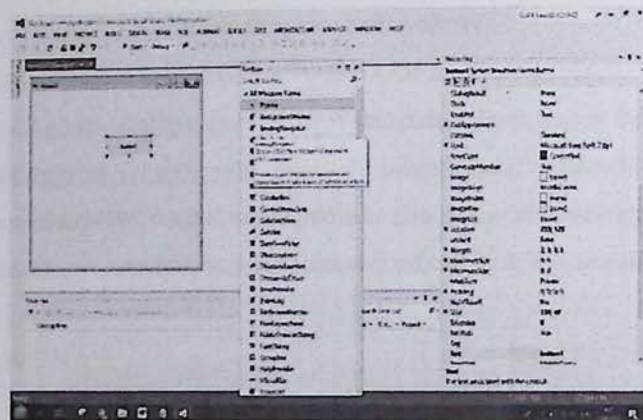
2.1- rasm. Microsoft Visual Studio ilovasi bosh oynasi.

3. Unda New Project->Visual C#-> WindowsFormsApplication ni tanlaymiz.



2.2-rasm. WindowsFormsApplicationni tanlash.

4. WindowsFormsApplicationning oynasi obyektlar joylashtirish.



2.3-rasm. WindowsFormsApplicationning asosiy oynasi.

C# dasturlash tilida RSA algoritmi loyihasining kodi:

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
namespace WindowsFormsApplication6
{
    public partial class Form1 : Form
    {
        int m;
        public Form1()
        {
            InitializeComponent();
        }
    }
}
```

```
}
```

```
private void label5_Click(object sender, EventArgs e)
{
}
```

```
private void button1_Click(object sender, EventArgs e)
{
    int p = int.Parse(textBox1.Text);
    int q = int.Parse(textBox2.Text);
    int n = p * q;
    m = (p-1) * (q-1);
    textBox3.Text = n.ToString();
    textBox4.Text = m.ToString();
}
```

```
private void button2_Click(object sender, EventArgs e)
{
    for (int i = 2; i <= m; i++)
    {
        bool tub = true;
        for (int j = 2; j < i; j++)
        {
            if (i % j == 0)
            {
                tub = false;
                break;
            }
        }
    }
}
```

```

        if (tub == true)
            richTextBox1.Text += i + ",";
        }
    }

private void textBox1_TextChanged(object sender, EventArgs e)
{
}

private void button5_Click(object sender, EventArgs e)
{
    int e1=1;
    int d = int.Parse(textBox5.Text);
    while ((e1*d%m!=1)|| (e1==d))
    { e1 = e1 + 1; }
    textBox6.Text = e1.ToString();
}

private void button3_Click(object sender, EventArgs e)
{
    string s=richTextBox2.Text;
    int l = s.Length;
    for (int i = 1; i < l; i++)
    {
        int a = s[i];
        int b=int.Parse(textBox6.Text);
        int n=int.Parse(textBox3.Text);

```

```

        int c=1;
        for (int j = 0; j < b; j++)
        { c = c * a; }
        c = c % n;
        richTextBox3.Text+=n.ToString()+",";
    }
}
}

```

Dastur narijasi:

2.4-rasm. RSA algoritmi dastur narijasi ko'rinish.

1-Keys topshiq: Guruh talabalari uchun individual keys topshirig'i asosida bilimini tekshirish.

Amaliy ishni bajarishdan maqsad: Talalar axborotlarning kompyuter xotirasida qanday ko'rinishda kodlanishni o'rganish.

Ishni bajarish uchun dastur namunasi:

```

s="Assalom"
n=int(len(s))

```

```
ss=""
```

```
for i in range (n):
```

```
    b=bin(ord(s[i]))
```

```
    b=b[2:]
```

```
    l=len(b)
```

```
    while (l!=8):
```

```
        b='0'+b
```

```
        l=l+1
```

```
    ss+=b
```

```
print(ss)
```

2.1-jadval

№	Axborot	ASCII o'nlikdagi kodi	ASCII ikkilikdagi kodi
Misol uchun	Assalom	[65, 115, 115, 97, 108, 111, 109]	[01000001011100110111001 0110000101101100 01101111 01101101]
1.	Do'stlar		
2.	Olam		
3.	Dunyo		
4.	Axborot		
5.	Texnologiyar		
6.	Ma'lumot		
7.	Xabar		
8.	Xavfsiz		
9.	Omad		
10	Yutuq		

2 - Keys topshiq: Guruh talabalari uchun individual keys topshirig'i asosida bilimini tekshirish.

Amaliy ishini bajarishdan maqsad: Talalar axborotlarni RSA algoritimida deshifrlashni o'rganish.

2.1-jadval

№	Shifrlangan xabar	Deshifrlash kaliti (d ; n)
Misol uchun	[65, 115, 115, 97, 108, 111, 109]	203 ; 323
1.	[68, 111, 351, 115, 116, 108, 97, 114]	293 ; 437
2.	[79, 108, 97, 109]	137 ; 299
3.	[68, 117, 110, 121, 111]	31 ; 253
4.	103, 9, 420, 36, 171, 36, 261]	157 ; 551
5.	[240, 3, 245, 123, 228, 188, 228, 198, 259, 265, 337, 681]	277 ; 667
6.	[65, 115, 115, 97, 108, 111, 109]	203 ; 323
7.	[68, 111, 351, 115, 116, 108, 97, 114]	293 ; 437
8.	[79, 108, 97, 109]	137 ; 299
9.	[68, 117, 110, 121, 111]	31 ; 253
10.	103, 9, 420, 36, 171, 36, 261]	157 ; 551

Nazorat savollari:

1. Simmetrik shifrlash
2. Asimmetrik shifrlash
3. RSA nima?
4. Eyler funksiyasi manosi nima?

III-Bob. AXBOROT XAVFSIZLIGINI TA'MINLASHNING USUL VAVOSITALARI.

10-Mavzu: Identifikatsiya, autentifikatsiya va avtorizatsiya.

Tayanch iboralar: Identifikatsiya, autentifikatsiya, avtorizatsiya

Tizim resurslarini boshkarish bilan bog'lik bo'lgan xavfsizlik muammosi uchun ruxsatlarni nazoratlash terminini —soyabon" sifatida foydalanish bo'ladi. Mazkur soxaga oid tushuntirishlarni olib borganda 3 ta asosiy muxim bo'lgan soxa mavjud: identifikatsiya, autentifikatsiya va avtorizatsiya.

Identifikatsiya - shaxsni kimdir deb davo qilish jarayoni. Masalan, siz telefonda uzingizni tanitishingizni identifikatsiyadan o'tish deb aytish mumkin. Bunda siz uzingizni, masalan, —Men Sherzodman" deb tanitasiz. Bu urinda

"Boxodir" sizning identifikatoringiz bo'lib xizmat qiladi. Shunday qilib, identifikatsiya - subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni hisoblanadi. Bundan tashkari, elektron pochta tizimida ham pochta manzilni - identifikator sifatida karash mumkin. Pochta manzilini taqdim etish jarayonini esa identifikatsiyalash jarayoni sifatida karash mumkin. Elektron pochta tizimida pochta manzili takrorlanmas yoki unikal bo'ladi. Shundan kelib chikib aytish mumkinki, foydalanuvchining identifikatori tizim ichida unikal va takrorlanmasdir.

Autentifikatsiya - foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini anikdash jarayoni. Masalan, foydalanuvchini shaxsiy kompyuterdan foydalanish jarayonini olsak. Dastlab kirishda foydalanuvchi o'z identifikatorini (Ya'ni, foydalanuvchi nomini) kiritadi va u orqali tizimga o'zini tanitadi (identifikatsiya jarayonidan o'tadi). Shundan so'ng, tizim foydalanuvchidan taqdim etilgan identifikatori xaqiqiyiligini tekshirish uchun parolni suraydi. Agar identifikatorga mos parol kiritilsa (Ya'ni, autentifikatsiyadan o'tsa), foydalanuvchi kompyuterdan foydalanish imkoniyatiga ega bo'ladi. Boshqa so'z bilan aytganda, autentifikatsiyani foydalanuvchi yoki

subyekttni xaqiqiyiligini tekshirish jarayoni deb aytish mumkin.

Autentifikatsiyadan o'ttandan so'ng foydalanuvchi tizim resursidan foydalanish imkoniyatiga ega bo'ladi. Birok, autentifikatsiyadan o'tgan foydalanuvchiga tizimda ixtiyoriy amallarda bajarishga ruxsat berilmaydi. Masalan, autentifikatsiyadan o'tgan imtiyozga ega foydalanuvchi uchun dasturlarni o'rnatish imkoniyatini berilishi talab etilsin. Xo'sh, autentifikatsiyadan o'tgan foydalanuvchiga kanday qilib ruxsatlarni cheklash mumkin? Mazkur masalalar bilan aynan, avtorizatsiya soxasi shugullanadi.

Avtorizatsiya - identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayonidir.

Xavfsizlik soxasida terminlar standartlashtirilgan ma'nolaridan ayri qo'llaniladi. Xususan, ruxsatlarni nazoratlash ko'p xollarda avtorizatsiyagasinonim sifatida ishlatiladi. Birok, mazkur kursda ruxsatlarni nazoratlash kengroq qaraladi. Ya'ni, avtorizatsiya va autentifikatsiya jarayonlari ruxsatlarni nazoratlashning qismlari sifatida qaraladi.

Yuqorida keltirilgan atamalarga berilgan ta'riflarni umumlashtirgan xolda quyidagicha xulosa qilish mumkin:

Identifikatsiya - siz kimsiz?

Autentifikatsiya - siz xakikatdan ham sizmisiz?

Avtorizatsiya - sizga buni bajarishga ruxsat bormi?

Autentifikatsiya

Autentifikatsiyada yoki identifikatsiya jarayonlarida subyektlar inson ko'rinishida yoki qurilma (kompyuter) ko'rinishida bo'lishi mumkin. Ya'ni, inson insonni autentifikatsiyadan o'tkazishi mumkin, mashina insonni autentifikatsiyadan o'tkazishi mumkin yoki mashina mashinani autentifikatsiyadan o'tkazishi mumkin. Mazkur ma'ruzada mashina insonni yoki mashina mashinani autentifikatsiyadan o'tkazish ssenariylariga asosiy e'tibor qaraladi.

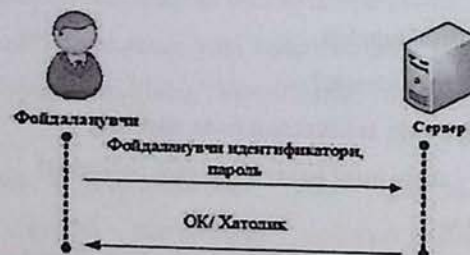
Mashina insonni quyidagi "narsalar" asosida autentifikatsiyadan o'tkazishi

mumkin:

- siz bilgan biror narsa (something you know);
- sizda mavjud biror narsa (something you have);
- sizning biror narsangiz (something you are).

“Siz bilgan biror narsa” xolatiga parol misol bo‘la oladi. “Sizda mavjud biror narsa” xolatiga esa smartkartalar, token, mashinaning pulti yoki kaliti misol bo‘la oladi. “Sizning biror narsangiz” xolati odatda biometrik parametrlarga sinonim sifatida qaraladi. Masalan, xozirda siz noutbuk sotib olib, undagi barmoq izi skaneri orqali autentifikatsiyadan o‘tishingiz mumkin.

Parol - faqat foydalanuvchiga ma‘lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta‘minlovchi biror axborot. Parol amalda autentifikatsiya jarayonida keng qo‘llaniluvchi parametr hisoblanadi. Masalan, biz o‘z shaxsiy kompyuterlarimizdan foydalanish xukukini olish uchun talab etilgan parolni kiritishimiz talab etiladi. Mazkur xolatni mobil telefonlar uchun ham ishlatish mumkin. Parolga asoslangan xolatdagi autentifikatsiyalash jarayonining umumiy ko‘rinishi 3.1-rasmda keltirilgan.



3.1-rasm. Parolga asoslangan mashina-insonni autentifikatsiyalash jarayoni

Parolga asoslangan autentifikatsiyalash quyidagi xususiyatlarga ega:

- parolga asoslangan autentifikatsiyani amalga oshirish qo‘lay (sarf xarajati kam, almashtirish oson);
- foydalanuvchi paroli odatda unga alokador ma‘lumot bo‘ladi (masalan,

uning yaxshi ko‘rgan futbol komandasi, telefon rakami va xak.) (123456, 12345, dm>yeg(u) va shuning uchun "hujumchilar" tomonidan aniklanishi oson;

- murakkab parollarni esda saklash murakkab(masalan, }De}{43}Yettb+u);
- parolga asoslangan autentifikatsiya usuli amalda keng qo‘llaniluvchi usul.

Smartkarta yoki token

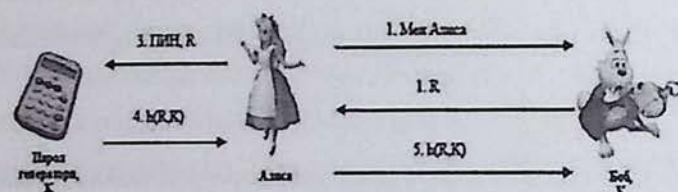
Smartkartalar yoki qurilma ko‘rinishidagi tokenlar autentifikatsiyalash uchun qo‘llaniladi. Smartkarta - kredit karta o‘lchamidagi qurilmabo‘lib, kichik xajmdagi xotira va hisoblash imkoniyatiga ega. Smartkarta odatda o‘zida biror maxfiy kattalikni, kalit yoki parolni, sakdaydi va xattoki biror hisoblashni amalga oshiradi. 3.2-rasmda maxsus maqsadli smartkarta va uni o‘quvchi qurilma (smartkarta o‘quvchi kurilma) aks ettirilgan.



3.2-rasm. Smartkarta va smartkarta o‘quvchi

Biror narsa asosida autentifikatsiyalash usullarini turli ko‘rinishlarda amalga oshirish mumkin. Masalan, parollar generatorini misol qilib olaylik. Parollar generatori kichik qurilma bo‘lib, tizimda kirishda qo‘llaniladi. Faraz qilaylik Alisada parol generatori mavjud va undan foydalanib Bobdan autentifikatsiyadan o‘tmokchi. Buning uchun Bob biror tasodifiy son K ni ("savolni") Alisaga yuboradi. Alisa qabul qilingan K sonini va parol generatoridan foydalanish uchun talab qilingan PIN ni parol generatoriga kiritadi. Parol generatori esa Alisagajavobni taqdim etadi va u Bobga uzatiladi. Agar javob to‘g‘ri bo‘lsa, Alisa

autentifikatsiyadan o'tadi, aks xolda o'ta olmaydi. Mazkur senariyning umumiy ko'rinishi 3.3-rasmda keltirilgan.



3.3-rasm. Tokenga asoslangan autentifikatsiya jarayoni

Keltirilgan sxemaga ko'ra, Bob va parol generatorida taqsimlangan kalit K bo'lishi shart. Ushbu sxemada "savol-javob" mexanizmi ishlatilgan. Ya'ni, savol sifatida Bob Alisaga R sonini uzatadi va unga mos bo'lgan javob - $h(R, K)$ ni qabul qiladi. Qabulqilgan ma'lumotni tekshirish orqali Bob Alisani xaqiqiyligini tekshiradi.

Smartkarta yoki "sizda mavjud biror narsa" asosida autentifikatsiya usullari quyidagi xususiyatlarga ega:

- smartkartaga asoslangan autentifikatsiyada biror narasani esda sakdashni talab etilmaydi;
- amalga oshirish va qurilma narxi yuqori (xususan, token yo'qolgan takdirida uni almashtirish qimmatga tushadi);
- token yoki smartkartani yo'qotib ko'yish muammosi mavjud;
- token xavfsiz olib yurilsa yuqori xavfsizlik darajasini ta'minlaydi.

Biometrik parametrlarga asoslangan autentifikatsiya

Biometrik parametrga asoslangan autentifikatsiya usulida biometrik parametr insonning uzi uchun kalit sifatida xizmat qiladi. Juda ham ko'plab biometrik parametrlar mavjud, masalan, barmoq izi, yuz tasviri, ko'z qorachigi, ovoz, xarakter tarzi, qulok shakli, qo'l shakli va xak. Biometrik parametrlarga asoslangan autentifikatsiya usuli amalda keng qo'llaniladi. Masalan, ko'p qavatli uylarni kirish eshiklarida yoki tashkilotlarga kirishda barmoq iziga asoslangan autentifikatsiya

usuli, noutbuklarda va mobil telefonlarda yuz tasviriga asoslangan yoki barmoq iziga asoslangan autentifikatsiyadan keng qo'llaniladi (3.4-rasm).



3.4-rasm. Biometrik na'munalarga misollar

Axborot xavfsizligi sohasida biometrik parametrlar parollarga karaganda yuqori xavfsizlikni ta'minlovchi alternativ sifatida qaraladi. Biometrik parametrlarga asoslangan autentifikatsiya usuli quyidagi xususiyatlarga ega:

- biometrik parametrga asoslangan usul o'zida esda sakdash va birga olib yurish zaruriyatini talab etmaydi;
- biometrik parametrga asoslangan autentifikatsiyani amalga oshirish parolga asoslangan usuldan qimmat va tokenga asoslangan usuldan arzon hisoblanadi (ba'zi, istisno xolatlar mavjud);
- biometrik parametrni almashtirish imkoniyati mavjud emas, Ya'ni, agar biometrik parametr qalbakilashtirilsa, U xolda autentifikatsiya tizimi shu foydalanuvchi uchun to'liq buzilgan hisoblanadi;
- turli biometrik parametrlarga asoslangan autentifikatsiya usullari insonlar tomonidan turli darajada qabul qilinadi.

Autentifikatsiya sohasida foydalanish uchun ideal biometrik parametr quyidagilarni qanoatlantirishi shart:

- universal bo'lishi - biometrik parametr barcha foydalanuvchilarda bo'lishi shart;
- farqli bo'lish - tanlangan biometrik parametr barcha insonlar uchun farq qilishi shart;
- o'zglik - tanlangan biometrik parametr vaqt o'tishi bilan o'zgarmaymas

qolishi shart;

– to‘planuvchanlik - fizik xususiyat osonlik bilan to‘planuvchi bo‘lishi shart. Amalda fizik xususiyatni to‘planuvchanligi, insonning jarayonga e‘tibor berishiga ham bog‘lik bo‘ladi.

Biometrik parametr nafaqat autentifikatsiya masalasini yechishda balki, identifikatsiyalashda ham keng qo‘llaniladi. Ya‘ni, “Siz kimsiz?” degan savolga javob bera oladi. Masalan, BI da jinoyatchilarga tegishli barmoq izlari bazalari mavjud. Ushbu bazada barmoq izlari (barmoq izi tasviri, foydalanuvchi nomi) shaklida sakdanadi va bu orqali biror insonni jinoyatchilar ro‘yxatida bor yo‘qligini tekshira oladi. Buning uchun, tekshiriluvchi insondan barmoq izi tasviri olinadi va u RV1 bazasida mavjud bo‘lsa, u xolda tekshiriluvchi insonning nomi barmoq izi tasviriga mos foydalanuvchi nomi bilan bir xil bo‘ladi.

Bir tomonlama va ikki tomonlama autentifikatsiya

Agar tomonlardan biri ikkinchisini autentifikatsiyadan o‘tkazsa, bir tomonlama autentifikatsiya deb ataladi. Agar xar ikkala tomon bir-birini autentifikatsiyadan o‘tkazsa, u xolda ikki tomonlama autentifikatsiya deb ataladi. Masalan, elektron pochtdan foydalanish davomida faqat server foydalanuvchini xaqiqiyiligini tekshiradi (parol orqali) va shu sababli uni bir tomonlama autentifikatsiyalash deb atash mumkin. Elektron to‘lovlarni amalga oshirishda esa ham server foydalanuvchini autentifikatsiyadan o‘tkazadi ham foydalanuvchi serverni autentifikatsiyadan o‘tkazadi. Shuning uchun mazkur xolatni ikki tomonlama autentifikatsiyalash deb aytish mumkin.

Ko‘p faktorli autentifikatsiya

Yuqorida keltirilgan barcha autentifikatsiya ssenariylarida faqat bitta omil uchun xaqiqiylikni tekshirish amalga oshirildi. Masalan, pochtda kirishda faqat parolni bilsangiz siz autentifikatsiyadan o‘ta olasiz yoki kirishda barmoq izini to‘g‘ri kiritsangiz, eshik ochiladi. Ya‘ni, server faqat foydalanuvchidan parolni yoki barmoq izini to‘g‘ri bo‘lishini istayapti. Mazkur ko‘rinishdagi autentifikatsiya - bir faktorli autentifikatsiya deb ataladi. Bir faktorli autentifikatsiyada tekshirish faqat bitta faktor bo‘yicha (masalan, parol) amalga

oshiriladi.

Birok, bir faktorli autentifikatsiyalashni amalda joriy qilish natijasida yuqori xavfsizlikni ta‘minlash mumkin emas. Masalan, ovozga asoslangan autentifikatsiya tizimini olaylik. Agar hujumchi foydalanuvchini ovozi diktafonga yozib olib, uni autentifikatsiyadash o‘tish jarayonida taqdim etsa, osonlik bilan autentifikatsiya tizimini aldash o‘tishi mumkin. Sababi, faqat bitta faktor (ovoz) bo‘yicha tekshirish amalga oshirilmokda. Shunga o‘xshash xolatni parolga asoslangan yoki tokenga asoslangan autentifikatsiya jarayonida xam kuzatish mumkin.

Mazkur muammoni bartaraf etish uchun, birinchi faktorga ko‘shimcha qilib, yana boshka faktorlardan foydalanish mumkin. Masalan, ovozga asoslangan autentifikatsiyalashda ko‘shimcha qilib paroldan foydalanish mumkin. Ya‘ni, foydalanuvchi dastlab tizimga o‘z ovozi orqali autentifikatsiyadan o‘tadi va udan so‘ng parol bo‘yicha autentifikatsiyadan o‘tkaziladi. Xar ikkala bosqichda ham autentifikatsiyadan muvaffaqiyatli o‘tilganda, foydalanuvchi tizimdan foydalanish imkoniyatiga ega bo‘ladi. Ko‘p faktorli autentifikatsiyalashdan foydalanishda xayotimizda xam ko‘plab misollar keltirish mumkin. Masalan, plastik kartadan to‘lovni amalga oshirishda. Plastik kartadan to‘lovni amalga oshirishdagi autentifikatsiya jarayoni o‘zida “sizda mavjud biror narsa” va “siz bilgan biror narsa” usullarini birlashtirgan. Ya‘ni, dastlab foydalanuvchida plastik kartani o‘zini bor bo‘lishini talab etadi va ikkinchidan uni PIN kodini bilishni talab etadi. Shu sababli, ushbu usulni ko‘p faktorli autentifikatsiyalash deb aytish mumkin.

Ko‘p faktorli autentifikatsiya usuli faktorlardan bittasi qalbakilashtirilgan takdirda xam autentifikatsiya jarayonini buzilmasligiga olib keladi.

Autentifikatsiya usullariga qaratilgan hujumlar

Mavjud autentifikatsiya usullarini buzishda ko‘plab hujum usullaridan foydalaniladi. Ushbu hujum usullarini autentifikatsiya usullariga mos ravishda quyidagicha tavsiflash mumkin:

1. Siz bilgan biror narsa. Autentifikatsiyalashning mazkur usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

- a. Parollar lug'atidan foydalanishga asoslangan hujum. Bunga ko'ra statistika bo'yicha eng ko'p qo'llaniluvchi parollar yordamida autentifikatsiyadan o'tishga xarakat qilinadi.
- b. Parollarni barcha variantlarini ko'rib chikish. Ushbu usulda parolning bo'lishi mumkin bo'lgan barcha variantlari generatsiya qilinadi va ular tekshirib ko'riladi.
- c. "Elka orqali karash" hujumi. Ushbu hujum foydalanuvchi parolni kiritish jarayonida yonida turib qarab turish orqali bilib olishni maqsad qiladi.
- d. Zararli dasturlar asosida hujum. Shunday maxsus dasturiy vositalar mavjudki ular foydalanuvchi kompyuterida o'matilib, klaviatura orqali kiritilgan barcha ma'lumotlarni serveriga uzatadi.

2. Sizda mavjud biror narsa. Autentifikatsiyaning mazkur usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

- a. Fizik o'g'irlash. Hujumning mazkur turi tokenni yoki smart kartani o'g'irlashni maqsad qiladi. Mazkur hujum bu toifdagi autentifikatsiya uchun eng xavfli hujum hisoblanadi.
- b. Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi. Ba'zi tokenlar dasturiy ko'rinishda bo'lib, mobil qurilmalarda ishlaydi va shu sababli zararli dastur tomonidan boshqarilishi mumkin.

3. Sizning biror narsangiz. Autentifikatsiyaning mazkur usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

- a. Qalbakilashtirish. Hujumning mazkur turi biometrik parametрни qalbakilashtirishni maqsad qiladi. Masalan, yuzlari o'xshash bo'lgan Xasan o'miga Xusan autentifikatsiyadan o'tishi yoki sifati yuqori bo'lgan foydalanuvchi yuz tasviri mavjud rasm bilan tizimni aldashni misol qilish mumkin.
- b. Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish. Ushbu hujumbevosita foydalanuvchilarni biometrik parametrlari (masalan, barmoq izi tasviri, yuz tasviri va xak) sakdangan bazaga qarshi amalga oshiriladi. Ya'ni, tanlangan foydalanuvchini biometrik parametrlari hujumchini biometrik parametrlari bilan almashtiriladi.

Autentifikatsiya usullariga qaratilgan hujumlarni oldini olish uchun xar bitta usulda o'ziga xos qarshi choralari mavjud. Umumiy xolda mazkur hujumlarni oldini olish uchun quyidagi ximoya usullari va xavfsizlik choralari tavsiya etiladi:

1. Murakkab parollardan foydalanish. Aynan ushbu usul parolni barcha variantlarini tekshirib ko'rish va lug'atga asoslangan hujumlarni oldini olishga katta yordam beradi.
2. Ko'p faktorli autentifikatsiyadan foydalanish. Mazkur usul yukorida keltirilgan barcha muammolarni bartaraf etishda katta amaliy yordam beradi.
3. Tokenlarni xavfsiz saqlash. Ushbu tavsiya biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olish uchun samarali hisoblanadi.
4. Tiriklikka tekshirishdan foydalanish. Ushbu usul biometrik parametrlarga asoslangan autentifikatsiyalash usullarida tasvir orqali aldab o'tish hujumini oldini olish uchun samarali hisoblanadi.

11-Mavzu: Elektron tijorat xavfsizligi.

Tayanch iboralar: elektron tijorat, elektron pul, elektron hamyon, internet-banking, mobil-banking.

Elektron tijorat tushunchasi. Elektron tijorat faoliyati O'zbekiston Respublikasining —Elektron tijorat to'g'risida"gi 2004 yil 29 apreldagi 613-II son Qonuni bilan belgilanadi va amalga oshiriladi.

Elektron tijorat Internet tarmog'idagi tijorat sohasiga oid faollikni, unda oldi-sotdini amalga oshirishini ifodalash uchun qo'llaniladi. U kompyuter tarmog'idan foydalangan holda xarid qilish, sotish, servis xizmatini ko'rsatishni amalga oshirish, marketing tadbirlarini o'tkazish imkoniyatini ta'minlaydi.

Elektron tijoratning an'anaviy savdo turlaridan farqi. Elektron tijoratning an'anaviy savdo turidan quyidagi xarakterli xususiyatlari bilan farqlanadi:

- xaridor o'ziga qulay vaqt, joy va tezlikda mahsulotni tanlash va sotib olish imkoniyatiga ega;
- savdo-sotiq faoliyatini ish faoliyati bilan birga parallel ravishda, Ya'ni ishlab chiqarishdan ajralmagan holda olib borish imkoniyati mavjud;
- ko'p sonli xaridorlarning bir vaqtning o'zida bir nechta firmalarga murojaat qila olishi. Bu ko'p sonli xaridorlarning aloqa vositalari yordamida sotuvchilar bilan muloqotda bo'lish imkoniyati;
- kerakli mahsulotlarni tezlikda izlab topish va shu mahsulotlari bor firmalarga murojaat qilishda texnika va transport vositalaridan samarali foydalanish, mahsulotlarni bir joyga yig'ish va ularni sotib olishda aniq manzillarga murojaat qilish. Ortiqcha vaqt va xarajatlarni kamaytiradi;
- xaridorning yashash joyi, sog'lig'i va moddiy ta'minlanish darajasidan qat'iy nazar hamma qatori teng huquqli mahsulot sotib olish imkoniyati;
- hozirgi kunda chiqqan jahon standartlariga javob beradigan mahsulotlarni tanlash va sotish imkoniyati;
- elektron tijorat sotuvchining mahsulotlarini (ish, xizmatlarini) sotish

jarayonidagi imkoniyatini yanada kengaytiradi va yangilaydi. Endi sotuvchi mahsulotlarini sotish jarayonini tezlashtirishi, yangi va sifatli mahsulotlarni muntazam almashtirishi, mahsulotlarning aylanma xarakatini tezlashtirishi kerak bo'ladi.

Elektron tijoratda savdoni tashkil qilish firmalarning raqobatini kuchaytiradi, monopoliyadan chiqaradi va mahsulotlarning sifatini oshirish imkoniyatini beradi. Xaridorlar kundalik xayotida kerakli mahsulotlar ichida sifatlarini tanlashi mumkin. Chet el firmalariga murojaat qiladi.

Elektron pullar tushunchasi. Elektron pul – bu pul birligiga tenglashtirilgan belgilar hamda kupyura va tanga rolini bajaruvchi juda katta son yoki fayllardir.

Bunday tizimning faoliyat ko'rsatish harajatlari boshqalaridan ancha kam. Bundan tashqari, elektron pullar to'liq anonimlikni ta'minlashi mumkin, chunki uni ishlatgan mijoz haqida hech qanday ma'lumot berilmaydi.

Elektron pul birliklari.

WMY – O'zbekiston zonasida operatsiyalarni amalga oshirish uchun UZSning Y-hamyondagi ekvivalenti.

WMR – rubl zonasida operatsiyalarni amalga oshirish uchun RURning R-hamyondagi ekvivalenti, WMR operatsiyalarining kafili bo'lib WebMoney Transfer ning Rossiya hududidagi vakili "BMP" MChJ xizmat qiladi.

WMZ – AQSh dollarida operatsiyalarni amalga oshirish uchun USD ning Z-hamyondagi ekvivalenti.

WME – EVRO da operatsiyalarni amalga oshirish uchun EURning E-hamyondagi ekvivalenti, WMZ va WME operatsiyalarining kafili bo'lib Amstar Holdings Limited, S.A. xizmat qiladi.

WMU – Ukraina zonasida operatsiyalarni amalga oshirish uchun UAHning U-hamyondagi ekvivalenti, WMU operatsiyalarining kafili bo'lib "Ukrainskoe Garantiynoe Agentstvo" MChJ xizmat qiladi.

WMB – Bellorusiya zonasida operatsiyalarni amalga oshirish uchun BYRning V-hamyondagi ekvivalenti.

WMG – 1 gramm oltinning G-hamyondagi ekvivalenti.

WBC va WMD – WMZning S va D hamyonlardagi kredit operatsiyalari uchun ekvivalenti.

Internet to'lov tizimlari, ular orqali to'lovlar va xaridlarni amalga oshirish.

Texnika vositalaridan, axborot texnologiyalaridan va axborot tizimlari xizmatlaridan foydalangan holda elektron to'lov hujjatlari vositasida naqd pulsiz hisob-kitoblarni amalga oshirish elektron to'lovdir.

Elektron to'lov tizimida tovarG'xizmatlar to'lovi xaridorning elektron hisobidan shaxsiy bank raqami hisobiga pul mablag'larini chiqarish imkoniga ega bo'lgan sotuvchining elektron hisobiga pul mablag'larini o'tkazish yo'li bilan amalga oshiriladi.

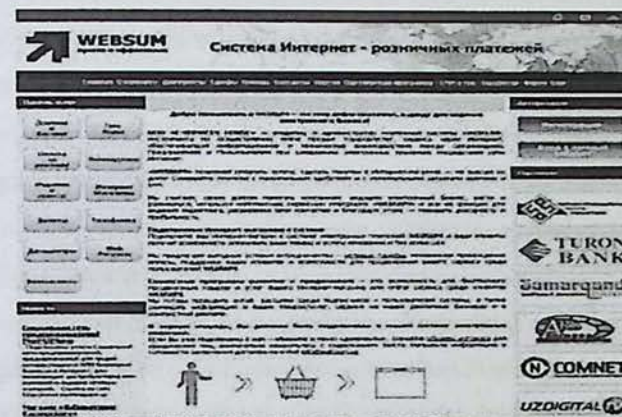
Quyidagi elektron to'lov tizimlari mavjud:

WEBSUM; iPAY; PAYNET; WEBMONEY; IntellectMoney; Perfect Money; RBK Money; V-money.

Elektron to'lov tizimlari yordamida Internet va IP-telefoniyaga ulanish uchun

«PIN» kodlar va internet do'konlardan tovarlarni harid qilish, uyali aloqa xizmati, shaxar telefoniyasi, kommunal xizmatlar, domen va xosting, reklama, televidenie, chiptalar, datatsentrlar, veb resurslar uchun haq to'lash mumkin.

iPAY – bu UzExdagi birja savdolarida, www.uzbex.com global savdo maydonchasida, hamda iPAY tizimiga qo'shilgan internet do'konlarda onlayn to'lovlarni amalga oshirish imkonini beruvchi, O'zbekiston Respublikasi tovarhom-ashyo birjasining to'lov tizimidir.



3.5-rasm. WEBSUM elektron to'lov tizimi.



3.6-rasm. iPAY elektron to'lov tizimi.

Internet-banking. To'lov tizimlari orasida alohida guruh, bu Internet banking funksiyasini bajaruvchi tizim, Ya'ni Internet orqali bank operatsiyani amalga oshirish hisoblanadi.

Internet-banking – bankdagi hisob raqamni Internet orqali boshqarish imkoniyatini beradigan xizmat. Internet banking tizimida samarali ishlash uchun Internetga ulangan va Internet brouzerga ega kompyuter bo'lishi etarli hisoblanadi.

Internet-banking imkoniyatlari quyidagilarni bajarishga imkon beradi:

- bankka barcha turdagi moliyaviy hujjatlarni yuborish;
- istalgan davr uchun bankdagi hisob raqamlardan ko'chirmalar va ularga tegishli boshqa hujjatlarni olish;
- haqiqiy vaqt tartibida to'lov hujjatlari bank ishlovidan o'tishining barcha bosqichlarini kuzatish;
- xatolar to'g'risida xabarlarni tezkor olish;
- kirim va chiqim to'lov hujjatlarini ko'rish va chop etish.

Internet-banking va bankdan tashqari elektron to'lovlar tizimlarining yanada rivojlanish jarayonida on-layn sotuvlar sektorida jadal o'sishni kutish lozim, bunda ulgurji va chakana savdo bilan shug'ullanuvchi barcha kompaniyalar Internet tarmog'i orqali tovarlarini bemaol sotishlari mumkin bo'ladi. To'lovlarning bankdan tashqari sektorini rivojlantirishning keyingi bosqichi bumobil to'lovlar tizimlari bo'ldi.

Elektron karmon, ularni to'ldirish va pul olish.4

Elektron karmon - bu elektron pullarni saqlash uchun mo'ljallangan vosita. Tovarlarini sotish va xarid qilishga mo'ljallangan veb texnologiyalar asosida yaratilgan axborot tizimi tomonidan amalga oshiriladigan vazifalar quyidagilardan tashkil topadi:

- mijozga tovar (xizmat) haqida ma'lumot berish;
- mijozdan tovar (xizmat)ga buyurtma qabul qilish.

Ba'zan onlaynli to'lov tizimlaridan foydalanilganda uchinchi vazifa-to'lov haqini olish, tovarni sotishda esa yana to'rtinchi vazifa - haqi to'langan tovarni jo'natish qo'shiladi.

Elektron karmonni to'ldirish va ulardan pul echishni quyidagi usullar bilan amalgaoshirish mumkin:

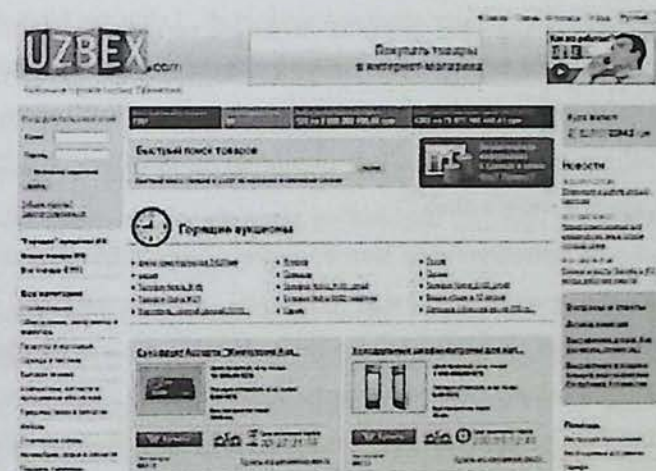
- Tijorat banklarida naqd pul bilan;
- Bank kartalari (VISA, MasterCard, UzKart) yordamida;
- Pochta orqali;

- Internet-banking yordamida;
- Pul o'tqazmalar tizimlari yordamida;
- Mobil aloqa yordamida.

Internet do'konlar va internet birja.

Bugungi kunda "Internet do'kon" nomi ostida turli ko'lam va maqsaddagi echimlarning keng spektri taklif qilinmoqda. WEBSUM elektron to'lov tizimidan foydalanadigan internet do'konlar quyida keltirilgan:

UzEx internet birja - bu shaxsiy kompyuter orqali UzEx savdo maydonchalarida savdo qilish imkoniyatini beruvchi global milliy savdo maydonchasi. Ushbu savdo tizimi, iPAY tizimi foydalanuvchilariga, maksimal qulayliklar bilan osongina o'z tovarlarini sotish va kerakli tovarlarni harid qilish imkonini beradi.



3.7-rasm. Uzbex.com O'zbekiston global savdo tizimi.

Elektron tijorat - O'zbekiston iqtisodiyotida: mavjud holat, muammolar va istiqbollar

Jahon hamjamiyatining ko'zlangan rivojlanish va farovonlikka erishish uchun, axborot texnologiyalariga (AT) bo'lgan ehtiyoji katta sur'atlar bilan oshib borayapti. Iqtisodiy o'sishning faollashuvi, dunyo aholisi yashash darajasining

yaxshilanishi axborot texnologiyalarining kundalik hayotimizga singib ketгани natijasidir. Dunyo tajribasi shuni ko'rsatadiki erkin axborot oqiminingta'minlanishi bozor iqtisodiyotiga o'tishni tezlashtiradi va sotsial farovonlikni oshiradi.

Axborot texnologiyalarining tez rivojlanishi iqtisodda ham o'z aksini topmasdan qolmaydi. Hozirgi kunda iqtisodda, ayniqsa tadbirkorlik sohasida erishilayotgan yutuqlar negizida aynan axborot texnologiyalari turli segmentlarining yuqori darajada rivojlanganligi va samarali qo'llanishi yotadi.

O'zbekiston iqtisodiyoti ham bundan mustasno emas albatta. Yaqqol misol sifatida axborot texnologiyalarining bir qator segmentlari masalan, ma'lumotlar yetkazish tarmoqlari, axborot internet-resurslari va ular orasidagi elektron hujjat almashuv, biznes va tijoratning barqaror rivojlanayotganini keltirish mumkin. O'zbekiston uchun axborot texnologiyalarini rivojlantirish yangi iqtisodiy aloqalarni ta'minlashda muhim ahamiyat kasb etadi. Lekin bu jarayon, axborot texnologiyalari sohasida ta'lim standartlarining oshishi, milliy telekommunikatsiya tarmoqlarining modernizatsiyalashuvi, huquqiy bazaning shakllanishi oqibatida vujudga keladigan jamiyatning ma'lum darajadagi informatsion tayorligi mavjud bo'lgan holatdagina sodir bo'ladi.

O'zbekiston iqtisodiyotining ham bosqichma-bosqich rivojlanishi oqibatida biznes faoliyatini yuritishning yangi prinsiplari, ayniqsa elektron tijoratning ahamiyati juda oshdi. Bugungi kunga kelib, har bir internet foydalanuvchisi elektron tijorat so'zining ma'nosini tushunishga harakat qilib ko'rgan. Hali o'zining uzoq tarixini qurishga ham ulgurmagan bunday faoliyat bilan bog'liq AQSh bozorlarida yiliga o'rtacha 1,5-2 trln. AQSh dollari miqdorida mablag'lar aylanadi.

"Elektron tijorat" termini EDI (Elektronic Data Interchange – ma'lumotlarni elektron almashish), elektron pochta, internet, intranet (kompaniya ichida axborot almashish) va ekstranet (tashqi dunyo bilan axborot almashish) kabi texnologiyalarni o'z ichiga oladi. O'z navbatida **Elektron kommersiya tizimi** uch sinfga bo'linadi:

- Chakana savdoni tashkil qilishbo'yicha (biznes-iste'molchi, B2C);
- Biznes hamkor bilan aloqlar o'rnatish (biznes-biznes, B2B);
- Iste'molchilar o'rtasidagi savdo (iste'molchi-iste'molchi, C2C);

Misol sifatida: – virtual auksion www.Ebay.com ni keltirish mumkin

Elektron tijoratning o'ziga xos qulayliklari va ustunliklari mavjud:

- Xalqaro operatsiyalarda axborot olish tezligi oshadi;
- Ishlab chiqarish va sotish davri qisqaradi;
- Arzon kommunikatsion vositalardan foydalanish evaziga axborot almashish xarajatlari kamayadi.

Kompaniya axborot texnologiyalarini samarali qo'llash orqali iste'molchibilan ochiq munosabat o'rnatish, mahsulot va xizmatlar to'g'risida hamkor va mijozlarni tezkor axborot bilan ta'minlash, sotuvning alternativ yo'llarini, misol uchun tijorat saytlarida elektron do'konlar ochish va yaratish imkoni beradi.

O'zbekistonda elektron tijoratni rivojlantirish jarayonlari amalda Bugungi kunga kelib, O'zbekistonda davlat organlari elektron tijoratni rivojlantirishda, dunyo tajribasida keng qo'llanilgan quyidagi prinsiplarga amal qilishmoqda.

- Elektron tijoratni rivojlantirishda korporativ sektor faol rol o'ynashilozim;
- Elektron tijoratga nisbatan, davlat organlari tomonidan asoslanmagan turli cheklovlar qo'yilishiga yo'l qo'yilmaslik lozim;
- Davlat hokimiyati elektron tijorat jarayoniga, ushbu soha subyektlarini qo'llab-quvvatlash va huquq bazasini takomillashtirish maqsadida aralishishi mumkin;
- Elektron tijoratni boshqarish chora-tadbirlarini ishlab chiqishda davlat hokimiyati Internetning o'ziga xosliklarini inobatga olishi lozim;
- Elektron tijorat jarayoni ma'muriy-hududiy bo'linish va davlat chegaralariga bog'liq bo'lmagan ravishda, global masshtabda sodir bo'lishilozim.

Iqtisodiy rivojlanish oqibatida O'zbekiston xalqaro iqtisodiyot tizimida

toborao'z mavqe'ini mustahkamlab bormoqda. Bu esa o'z navbatida elektron tijorat infratuzilmasini takomillashtirish, uning jahon bozorida kuchli raqobatchi sifatida paydo bo'lishini ta'minlash zaruriyatini keltirib chiqaradi. Yuqoridagi holatlar inobatga olingan holda elektron tijoratning asosini, Ya'ni huquqiy bazasini takomillashtirish bo'yicha bir qancha sezilarli ishlar amalga oshirildi. 2004 yil 29 aprelda N613-II "Elektron tijorat" to'g'risida O'zbekiston Respublikasi qonuni, 2007 yil 30 noyabrda Vazirlar Mahkamasining №21 "Elektron tijoratni rivojlantirish" to'g'risidagi va 2007 yil 12 iyunda "Elektron tijorat tizimini amalda qo'llashda to'lov tizimini takomillashtirish" to'g'risidagi qarorlar qabul qilindi. Bundan tashqari Respublikada elektron tijoratni rivojlantirish maqsadida

"Ekarmon" loyihasi ishlab chiqildi va u samarali tarzda amaliyotga joriy qilinmoqda. Olib borilgan va bajarilgan ishlar asosida bir qancha ijobiy natijalarga erishildi. Masalan, axborot almahinuvi tezligini oshirish va unga sarflanadigan vaqtni kamaytirish maqsadida olib borilgan ishlarning natijasi Respublikada xalqaro axborot tarmoqlari tezligini oshishida ko'rinadi.

Elektron tijoratni rivojlantirish jamiyatimiz uchun qanday natijalar beradi?

- Elektron tijoratning rivojlanishi O'zbekiston mehnat bozori strukturasiga ijobiy ta'sir ko'rsatadi. Yuqori axborot texnologiyalarini sanoatlashtirishminglab yangi ish o'rinlarini yaratadi.
- O'zbekiston iqtisodiyotining barqarorlashishi, tovar va xizmatlarning raqobatbardoshligi kuchayishi va elektron tijorat rivojlanishining bir paytda sodir bo'lishi eksport imkoniyatlarimizning oshishiga olib keladi.
- Elektron tijorat aholi turmush darajasining yaxshilanishini, marketing, menejment kabi sohalarning rivojlanishini ta'minlaydi.

Shunday qilib, O'zbekistonda elektron tijoratni rivojlantirish imkoniyatlari yildan yilga o'sib borayotganligini alohida ta'kidlab o'tish lozim. Uning rivojlanishi milliy ishlab chiqaruvchilarimizga yangi bozorlar ochish, yangi mijozlar topish imkoniyatlarini yaratadi. Elektron tijoratni rivojlantirish bo'yicha tanlangan va

amaldagi yo'ldan to'g'ri borish, kelajakda O'zbekiston iqtisodiyotini jahon bozorining yetakchi vakillaridan biriga aylantiradi. O'zbekistonda elektron tijorat bo'yicha mavjud muammolarni hal qilishning to'g'ri yo'li tanlanganligi xalq farovonligida, jamiyatimizning taraqqiy topishida, iqtisodiy rivojlanishimizda o'z aksini topadi.

Nazorat savollari

1. Elektron tijorat, elektron pul vaelektron hamyon tushunchalari.
2. Internet-banking, mobil-banking tushunchalari.
3. Elektron tijorat xavsizligini ta'minlash choralari.

12-MAVZU: Kompyuter viruslari va antiviruslar.

Tayanch iborolar: Kompyuter viruslari, kompyuter antiviruslari, detektorlar faglar, vaksinalar, privivka, filtrlar, rivizorlar.

«Kompyuter viruslari» - kompyuter tizimlarida tarqalish va o'z-o'zidan qaytadan tiklanish (replikatsiya) xususiyatlariga ega bo'lgan bajariluvchi yoki sharxlanuvchi kichik dasturlardir. Viruslar kompyuter tizimlarida saqlanuvchi dasturiy ta'minotni o'zgartirishi yoki yo'qotishi mumkin.

Virus tarixi

Ilk bora 1983-yil 11-noyabr kuni Janubiy Kaliforniya universiteti talabasi, amerikalik Fred Koyen 5 daqiqadan 1 soatgacha bo'lgan tezlikda ko'paya oladigan kompyuter virusi taqdimotini o'tkazgan.

Shundan so'ng, oradan bir yil o'tib, Koyen kompyuter tarmoqlari bo'ylab viruslarning tarqalish xavfi va antivirus dasturlarini yaratish imkoniyatlari haqida kitob yozadi.

Birinchi yaratilgan virus (1986 yilda yaratilgan) —Brain" deb nomlangan bo'lib, u faqat kompyuter disketlari orqali tarqalgan. Birinchi antivirus dasturi esa 1988-yilda ishlab chiqilgan.

Ichida virus joylashgan dastur zararlangan deb ataladi. Bunday dastur o'z ishini boshlaganda, oldin boshqarishni virus o'z qo'liga oladi. Virus boshqa dasturlarni topadi va «zararlantiradi» hamda biror-bir zararli ishlarni (masalan, fayllarni yoki diskda fayllarni joylashish jadvalini buzadi, tezkor xotirani ishlash jarayonini pasaytiradi va h.k.) bajaradi. Virusni niqoblash uchun boshqa dasturlarni zararlantirish va zarar yetkazish bo'yicha ishlar har doim ham emas, aytaulik ma'lum bir shartlar bajarilganda bajarilishi mumkin. Virus unga kerakli ishlarni bajargandan keyin u boshqarishni o'zi joylashgan dasturga uzatadi va u dastur odatdagiday ishlay boshlaydi. Shu bilan birga tashqi ko'rinishdan zararlangan dasturning ishlashi zararlanmagandek kabi ko'rinadi.

Viruslarning ko'pgina ko'rinishlari shunday tuzilganki, zararlangan dastur

ishga tushirilganda virus kompyuter xotirasida har doim qoladi va vaqti-vaqti bilan dasturlarni zararlantiradi va kompyuterda zararli ishlarni bajaradi.

Virusning barcha harakatlari yetarlicha tez bajarilishi mumkin va biror-bir xabarni bermaydi, shuning uchun foydalanuvchi kompyuterda birorta odatdan tashqari ishlar bo'layotganini payqashi juda mushkuldir.

Kompyuterda nisbatan kam dasturlar zararlangan bo'lsa, virusning borligi deyarli sezilarsiz bo'ladi. Lekin vaqt o'tishi bilan kompyuterda qandaydir g'alati hodisalar ro'y bera boshlaydi, masalan:

- ba'zi dasturlar ishlashdan to'xtaydilar yoki noto'g'ri ishlaydi;
- ekranga begona xabar yoki belgilar chiqadi;
- kompyuterning ishlash tezligi sekinlashadi;
- ba'zi bir fayllar buzilib qoladi va h.k.

Bu vaqtga kelib, qoidaga ko'ra, foydalanuvchi ishlayotganda yetarlicha ko'p (yoki hatto ko'pchilik) dasturlar viruslar bilan zararlangan, ba'zi bir fayl yoki disklar esa ishdan chiqqan hisoblanadi. Bundan tashqari, foydalanuvchi kompyuteridagi zararlangan dasturlar disketalar yordamida yoki lokal tarmoq bo'yicha foydalanuvchi hamkasblari va o'rtoqlarining kompyuteriga o'tib ketgan bo'lishi mumkin.

Viruslarning ba'zi bir ko'rinishlari o'zlarini yanada xavfliroq kirib tushadilar. Ular boshlanishda katta miqdordagi dasturlarni yoki diskarni bildirmasdan zararlantiradilar, keyin esa jiddiy shikastlanishlarini keltirib chiqaradi, masalan, kompyuterdagi butun qattiq diskni formatlaydi. Dastur – virus sezilarsiz bo'lishi uchun u katta bo'lmasligi kerak. Shuning uchun, qoidaga ko'ra, viruslar yetarlicha yuqori malakali dasturlovchilar tomonidan Assembler tilida yoziladi.

Kompyuter viruslarini paydo bo'lishi va tarqatilishi sabablari, bir tomondan, inson shahsiyatining ruhiyatida va uning yomon xislatlarida yashirinadi (havaslar, qasos olishlar, tan olinmagan ijodkorlarning mansabparastligi, o'z qobiliyatlarini konstruktiv qo'llash imkoniyati yo'qligi), ikkinchi tomondan esa, himoya qilishning apparat vositalarini va shaxsiy kompyuterning operatsion tizimi tomonidan qarshi

harakatlarning yo'qligi bilan bog'liqdir.

Viruslarni kompyuterga kirib olishining asosiy yo'llari olinadigan disklar (egiluvchan va lazerli) ham kompyuter tarmoqlari hisoblanadi. Qattiq diskni viruslar bilan zararlaniishi kompyuterni virusni o'zida saqlagan disketadan yuklaganda amalga oshishi mumkin. Bunday zararlaniish tasodifiy bo'lishim mumkin, masalan, disketani A diskovoddan chiqarib olmasdan va kompyuterni qayta yuklanganda, bunda disketa tizimli bo'lmasligi ham mumkindir. Disketani zararlantirish juda oddiyroqdir. Unga virus hattoki, agar disketani zararlangan kompyuter diskovodiga qo'yilganda va uning mundarijasini o'qilganda, tushish mumkin.

Zararlangan disk bu yuklanish sektorida dastur – virus joylashgan diskdir.

Virusni o'z ichiga olgan dastur ishga tushirilgandan keyin boshqa fayllarni zararlantirish mumkin bo'lib qoladi. Eng ko'proq viruslar bilan diskning yuklanadigan sektori va .EXE, .COM, .SYS yoki BAT kengaytmasiga ega bo'lgan fayllar zararlaniadi. Kam matnli va grafikli fayllar kam zararlaniadi.

Zararlangan dastur, bu unga tadbiiq qilingan dastur – virusni o'z ichiga olgan dasturdir. Kompyuter virusi bilan zararlaniishda o'z vaqtida uni payqash juda muhimdir. Buning uchun viruslarni paydo bo'lishining asosiy belgilari to'g'risida bilimlarga ega bo'lish kerak. Ularga quyidagilar tegishli bo'lishi mumkin:

- oldin muvaffaqiyatli ishlagan dasturlarning ishlashdan to'xtashi yoki noto'g'ri ishlashi;
- kompyuterning sekin ishlashi;
- operatsion tizimni yuklash imkoni yo'qligi;
- fayl va kataloglarni yo'qolib qolishi yoki ularning mazmunini buzilishi;
- fayllarni o'zgartirilganlik sanasi va vaqtining o'zgarishi;
- diskda fayllar soni bexosdan juda oshib ketishi;
- bo'sh tezkor xotira o'lchamining jiddiy kamayishi;
- ekranga ko'zda tutilmagan xabarlarni yoki tasvirlarni chiqarish;
- ko'zda tutilmagan tovushli xabarlarni berish;

- kompyuter ishlashda tez-tez bo'ladigan osilib qolishlar va buzilishlar.

Ta'kidlash kerakki, yuqorida sanab o'tilgan hodisalar viruslarni kelib chiqishi bilan bo'lishi majburiy emas, boshqa sabablarning oqibatlari ham bo'lishi mumkin. Shuning uchun kompyuter holatini to'g'ri diagnostikalash har doim mushkuldir.

Kompyuter virusi kompyuterda mavjud bo'lgan disklardagi istalgan faylni yetarlicha o'zgartirish va buzishi mumkin. Lekin fayllarning ba'zi bir turlarini virus «zararlantirishi» mumkin. Bu shuni bildiradiki, virus bu fayllarga «tadbiiq» qilinishi mumkin, Ya'ni ularni shunday o'zgartiradiki, ular virusni o'z ichidasaqlaydi va bu virus ba'zi bir holatlarda o'zining ishini boshlashi mumkin.

Ta'kidlash lozimki, dastur va hujjatlarning matnlari, ma'lumotlar bazasining axborotli fayllari, jadvalli protsessor jadvallari va boshqa shunga o'xshash fayllar virus bilan zararlaniishi mumkin emas, bu fayllarni viruslar buzishi mumkin.

Kompyuter viruslari va ularning klassifikatsiyalari

Barcha kompyuter viruslari quyidagi alomatlari bo'yicha klassifikatsiyalanishim mumkin:

- yashash muhiti bo'yicha;
- yashash muhitining zaxarlanishi bo'yicha;
- zararkunandalik ta'sirning xavfi darajasi bo'yicha;
- ishlash algoritmi bo'yicha.

Yashash muhiti bo'yicha kompyuter viruslari quyidagilarga bo'linadi:

- tarmoq viruslari;
- fayl viruslari;
- yuklama viruslar;
- kombinatsiyalangan viruslar.

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiriti ladi (eng ko'p tarqalgan viruslar xili), yoki fayl yo'ldoshlarni (kompan'on viruslar) yaratadi yoki faylli tizimlarni (linkviruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o'zini diskning yuklama sektoriga (boot sektoriga) yoki

vinchesterning tizimli yuklovchisi (Master Boot Record) bo'lgan sek torga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makro dasturlarini va fayllarini, xususan MicroSoft Word, MicroSoft Excel va h. kabi ommaviy muharrirlarning fayl xujjatlarini va elektron jadvalarini zaharlaydi.

Tarmoq viruslari o'zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba'zida tarmoq viruslarini "qurt" xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet

qurtlarga (Internet bo'yicha tarqaladi), IRC qurtlarga (chatlar, Internet Relay Chat) bo'linadi.

Yashash muhitining zaxarlanishi usuli bo'yicha kompyuter viruslari quyidagilarga bo'linadi:

- rezident;
- rezident bo'lmagan;

Rezident viruslar faollashganlaridan so'ng to'laligicha yoki qisman yashash muhitidan (tarmoq, yuklama sektori, fayl) hisoblash mashinasining asosiy xotirasiga ko'chadi. Bu viruslar, odatda, faqat operatsion tizimga ruxsat etilgan imtiyozli rejimlardan foydalanib yashash muhitini zaxarlaydi va ma'lum sharoitlarda zararkunandalik vazifasini bajaradi.

Rezident bo'lmagan viruslar faqat faollashgan vaqtlarida hisoblash mashinasining asosiy xotirasiga tushib, zaxarlash va zararkunandalik vazifalarini bajaradi. Keyin bu viruslar asosiy xotirani butunlay tark etib yashash muhitida qoladi. Agar virus yashash muhitini zaxarlamaydigan programmani asosiy xotiraga joylashtirsa bunday virus rezident bo'lmagan virus deb hisoblanadi.

Foydalanuvchining informatsion resurslari uchun xavf darajasi bo'yicha kompyuter viruslarini quyidagilarga ajratish mumkin:

- beziyon viruslar;
- xavfli viruslar;

- juda xavfli viruslar;

Yashash makonini o'zgartirmaydigan viruslar o'z navbatida ikkita guruhga ajratilishi mumkin.

- viruslar-«yo'ldoshlar» (companion). Viruslar-«yo'ldoshlar» fayllarni o'zgartirmaydi. Uning ta'sir mexanizmi bajariluvchi fayllarning nusxalarini yaratishdan iboratdir.

- Viruslar-«qurtlar» tarmoq orqali ishchi stansiya tushadi, tarmoqning boshqa abonentlari bo'yicha virusni jo'natish adreslarini hisoblaydi va virusni uzatishni bajaradi.

Algoritmning murakkabligi, mukammalik darajasi va yashirinish xususiyatlari bo'yicha yashash makonini o'zgartiradigan viruslar quyidagilarga bo'linadi:

- talaba viruslar;
- «stels» viruslar (ko'rinmaydigan viruslar);
- polimorf viruslar.

Talaba-viruslar malakasi past yaratuvchilar tomonidan yaratiladi. Bunday viruslar, odatda, rezident bo'lmagan viruslar qatoriga kiradi, ularda ko'pincha xatoliklar mavjud bo'ladi, osongina taniladi va yo'qotiladi.

«Stels» viruslar malakali mo'taxasislar tomonidan yaryatiladi. «Stels»-viruslar operatsion tizimning shikastlangan fayllarga murojaatlarini ushlab qolish yo'li bilan o'zini yashash makonidagiligini yashiradi va operatsion tizimni axborotning shikastlanmagan qismiga yo'naltiradi. Virus rezident hisoblanadi, operatsion tizim programmalari ostida yashirinadi, xotirada joyini o'zgartirishi mumkin. «Stels» - viruslar rezident antivirus vositalariga qarshi ta'sir ko'rsata olish qobiliyatiga ega.

Polimorf viruslar ham malakali mo'taxasislar tomonidan yaratiladi, va doimiy tanituvchi guruxlar-signaturalarga ega bo'lmaydi. Oddiy viruslar yashash makonining zaxarlanganligini aniqlash uchun zaxarlangan obyektga maxsus tanituvchi ikkili ketma-ketlikni yoki simvollar ketma-ketligini (signaturani)

joylashtiradi. Bu ketma-ketlik fayl yoki sektorning zaxarlanganligini aniqlaydi.

Viruslar bilan kurashish usullari va vositalari

Viruslar tarqalishining ommalashuvi, ular ta'siri oqibatlarining jiddiyligi virusga qarshi maxsus vositalarni va ularni qo'llash metodlarini yaratish zaruriyatini tug'dirdi. Virusga qarshi vositalar yordamida quyidagi masalalar yechiladi:

- kompyuter tizimlarida viruslarni aniqlash;
- viruslar ta'siri oqibatlarini yo'qotish.
- Kompyuter tizimlarida viruslarni aniqlashning quyidagi metodlari mavjud:
- skanerlash;
- o'zgarishlarni bilib qolish;
- evristik taxlil;
- rezident qorovullardan foydalanish;
- programmani vaksinatsiyalash;
- viruslardan apparat-programm himoyalanih.

Viruslarga qarshi programmlar yordamida viruslar ta'siri oqibatlarini yo'qotishning ikki usuli mavjud.

Birinchi usulga binoan tizim ma'lum viruslar ta'siridan so'ng tiklanadi. Virusni yo'qotuvchi programmani yaratuvchi virusning stukturasini va uning yashash makonida joylashish xarakteristikalarini bilishi shart.

Ikkinchi usul noma'lum viruslar bilan zaxarlangan fayllarni va yuklama sektorini tiklashga imkon beradi. Fayllarni tiklash uchun tiklovchi programma fayllar xususidagi viruslar yo'qligidagi axborotni oldindan saqlashi lozim. Zaxarlanmagan fayl xususidagi axborot va viruslar ishlashining umumiy prinsiplari xususidagi axborotlar fayllarni tiklashga imkon beradi.

Hozirgi vaqtda viruslarni yo'qotish uchun ko'pgina usullar ishlab chiqilgan va bu usullar bilan ishlaydigan dasturlarni antiviruslar deb atashadi. Antiviruslarni, qo'llanish usuliga ko'ra, quyidagilarga ajratishimiz mumkin: detektorlar, faglar, vaksinalar, privivkalar, revizorlar, monitorlar.

Detektorlar – virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topadi va xabar beradi. Yangi viruslarni aniqlay olmasligi detektorlarning kamchiligi hisoblanadi.

Faglar – yoki doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oldingi holatiga qaytaradi.

Vaksinalar - yuqoridagilardan farqli bo'lib, u himoyalananayotgan dasturga o'rnatiladi. Natijada dastur zararlangan deb hisoblanib, virus tomonidan o'zgartirilmaydi. Faqatgina ma'lum viruslarga nisbatan vaksina qilinishi uning kamchiligi hisoblanadi. Shu bois, ushbu antivirus dasturlar keng tarqalmagan.

Privivka - fayllarda xuddi virus zararlagandek iz qoldiradi. Buning natijasida viruslar privivka qilingan faylga yopishmaydi.

Filtrlar – qo'riqllovchi dasturlar ko'rinishida bo'lib, rezident holatda ishlab turadi va viruslarga xos jarayonlar bajarilganda, bu haqida foydalanuvchiga xabar beradi.

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

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

Doktor dasturlari nafaqat virus bilan kasallangan fayllarni topadi, balki ularni davolab, dastlabki holatiga qaytaradi. Bunday dasturlarga Aidstest, DoctorWebdasturlarini misol qilib keltirish mumkin. Yangi viruslarning to'xtovsiz paydobo'lib turishini hisobga olib, doktor dasturlarni ham yangi versiyalari bilan almashtirib turish lozim.

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

Bu harakatlar quyidagicha bo'lishi mumkin :

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

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

Hozirgi kunda kompyuter viruslariga qarshi kurashga ixtisoslashgan kompaniyalar vujudga kelgan. Ular har kun, har soat mijozlarning kompyuteridagi mavjud viruslarni topib, ularni yo'q qiladigan antivirus dasturlarini yaratadilar. Hozirgi kunda kompyuter viruslariga qarshi kurashuvchi antivirus dasturlaridan eng asosiylari Kaspersky Anti-Virus (AVP) ScriptChecker, NortonAntivirus, DrWeb, Adinf, AVPlar hisoblanadi. KasperskyAnti-Virus dasturi bugungi kunda kompyuter viruslarining 100000 dan ortiq turini aniqlaydi va davolaydi.

Kompyuter viruslaridan himoya qilish usullari

Kompyuter viruslaridan himoya qilishning uchta chegarasi mavjuddir:

- viruslarning kirib kelishini bartaraf etish;
- agar virus baribir kompyuterga kirgan bo'lsa, virus hujumini bartaraf etish;
- agar hujum baribir amalga oshgan bo'lsa, buzuvchi oqibatlarni bartaraf etish.

Himoya qilishni amalga oshirishning uchta usuli mavjuddir:

- himoya qilishning dasturli usullari;
- himoya qilishning apparatli usullari;
- himoya qilishning tashkiliy usullari.

Muhim ma'lumotlarni himoya qilish masalasida ko'pincha maishiy yondashish ishlatiladi: «kasallikni davolagandan ko'ra uning oldini olgan yaxshiroq». Afsuski, aynan u eng buzuvchi oqibatlarni keltirib chiqaradi.

Kompyuterga viruslarni kirib olish yo'lida barrikadalarni yaratib olib, ularning mustahkamligiga ishonib va buzuvchi hujumdan keyingi harakatlarga tayyor bo'lmasdan qolmaslik kerak. Shu bilan birga, virusli hujum, bu muhim ma'lumotlarni yo'qotishni yagona bo'lmagan hattoki keng tarqalmagan sababidir. Shunday dasturli uzilishlar mavjudki, ular operatsion tizimni ishdan chiqarishi mumkin hamda shunday apparatli uzilishlar borki, ular qattiq diskni ishlashga layoqatsiz qilib qo'yish qobiliyatiga egadirlar. O'g'irlash, yong'in yoki boshqa favqulodda holatlar natijasida muhim ma'lumotlar bilan birgalikda kompyuterni yo'qotish ehtimoli har doim ham mavjuddir. Shuning uchun xavfsizlik tizimini yaratishni birinchi navbatda «oxiridan» boshlash kerak – istalgan ta'sirni, U virus hujumi, xonada o'g'irlik yoki qattiq diskni fizik ishdan chiqishidan qat'iy nazar, buzuvchi oqibatlarini bartaraf etishdan boshlash kerak.

Ma'lumotlar bilan ishonchli va xavfsiz ishlashga faqat shundagina erishiladiki, agar istalgan kutilmagan hodisa, shu jumladan kompyuterni to'liq fizik ishdan chiqarish ham, salbiy oqibatlarga olib kelmasligi kerak.

Zararkunanda dasturiy ta'minotlar

Zararli dastur - bu kompyuterga, serverga, mijozga yoki kompyuter tarmog'iga zarar yetkazish uchun ataylab yaratilgan har qanday dastur.

Zararli dasturiy vositalar foydalanuvchini ruxsatisiz hujumchi kabi g'arazli amallarni bajarishni maqsad qilgan vosita hisoblanib, ular yuklanuvchi kod (.exe), aktiv kontent, skript yoki boshqa ko'rinishda bo'lishi mumkin. Hujumchi zararli dasturiy vositalardan foydalangan holda tizim xafsizligini obro'sizlantirishi, kompyuter amallarini buzishi, maxfiy axborotni to'plashi, veb saytdagi kontentlarni modifikatsiyalashi, o'chirishi yoki qo'shishi, foydalanuvchi kompyuterini boshqaruvini qo'lga kiritishi mumkin. Bundan tashqari zararli dasturlar, hukumat tashkilotlardan va korporativ tashkilotlardan katta hajmdagimaxfiy axborotni olish uchun ham foydalanilishi mumkin.

Zararli dasturlar turlari:

– viruslar: o'zini o'zi ko'paytiradigan programma bo'lib, o'zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi.

– troyan otlari: bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi.

– Adware: marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi dasturiy ta'minot.

– Spyware: foydalanuvchi ma'lumotlarini qo'lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

– Rootkits: ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi.

– Backdoors: zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish.

– mantiqiy bombalar: zararli dasturiy vosita bo'lib, biror mantiqiy shart qanoatlantirilgan vaqtda o'z harakatini amalga oshiradi.

– Botnet: Internet tarmog'idagi obro'sizlantirilgan kompyuterlar bo'lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi.

– Ransomware: mazkur zararli dasturiy ta'minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo'yib, to'lov amalga oshirilishini talab qiladi.

Mantiqiy bomba

O'zidan ko'payish yo'q

Sonini oshib borishi: nol

Yuqumliligi: mumkin

Mantiqiy bomba ikki qismdan iborat kod hisoblanadi:

1. Foydali yuklama qismi bajarilish uchun harakat qismi hisoblanadi. Foydali yuklama qismi hohlagan ko'rinishda bo'lishi mumkin, lekin zarar keltiruvchi effekt

ma'nosiga ega bo'ladi.

2. Trigger, mantiqiy shart bo'lib foydali yuklama qismini bajarilishini nazoratga oladi va baholanadi. Triggerning aniq sharti tasavvur bilan chegaralangan bo'ladi va sana, foydalanuvchining tizimga kirishi yoki operatsion tizim versiyasi kabi mahalliy shartlarga asoslanadi. Shu tarzda triggerlar masofadan to'rib o'rnatiluvchi ko'rinishda loyihalanishi mumkin yoki bo'lmasa qandaydir holatni mavjud emasligiga ko'ra.

Mantiqiy bombalar mavjud kodning ichiga kiritilishi yoki bo'lmasa avtonom tarzda bo'lishi mumkin. Oddiy parazitik (yuqumli) namuna quyida ko'rsatilgan bo'lib, trigger sifatida aniq sana ishlatilganda kompyuterni buzilishiga olib kelishi mumkin:

legitimate code

if date is Friday the 13th:

crash_computer()legitimate code

Troyan otlari

O'zidan ko'payish : yo'q

Sonini oshib borishi: nol

Yuqumliligi: Ha

Ushbu turdagi zarar keltiruvchi dasturlar Greklar va Troyaliklar o'rnatilgan urush dasrida ishlatilgan nayrangga asoslanadi va shu uchun shunaqa nom olgan.

Axborot kommunikatsiya texnologiyalarida troyan oti bu dastur bo'lib, qandaydirdasozda vazifani bajarishga mo'ljallangan bo'ladi. Biroq qo'shimcha tarzda zarar keltiruvchi vazifani xufiyona bajaradi. Klassik namunasi sifatida tizimga kirishdaparni ushlab olish dasturini keltirish

mumkin, u «username» i «password» kabi autentifikatsiya so'rovlarini qayd etadi va foydalanuvchi tomonidan axborot kiritilishini kutib turadi. Ushbu holat yuz berganda o'zining yaratuvchisi uchun parollarni ushlab oluvchi dastur o'ziga yozib quyadi, so'ngra esa — noto'g'ri parol” degan xabarni tizimga real kirish oldidan chiqaradi. Hech nimadan shubhalanmagan foydalanuvchi xato qilgandek bo'ladi.

Backdoors (orqa eshik)

O'zidan ko'payish: yo'q

Sonini oshib borishi: nol

Yuqumliligi: mavjud

Backdoor (tuynuk) bu oddiy xavfsizlik tekshiruvidan o'ta oladigan har qanday mexanizmdir. Dasturchilar ba'zida orqa eshikni (tuynuk) qonuniy asoslarga ko'ra hosil qilishadi.

Mantiqiy bombalar kabi orqa eshik (tuynuk) dasturlari ham dastur kodida yoki avtonom dasturlarda bo'lishi mumkin. Orqa eshik (tuynuk) namunasi quyidagi kodda ko'rsatilgan bo'lib, u tizimga kirishda autentifikatsiya jarayonini aylanib o'tadi.

```
username = read_username ( )
password = read_password ( )if username is —133t h4ck0r":
return ALLOW_LOGIN
if username and password are valid:
return ALLOW_LOGINelse:
return DENY_LOGIN
```

Virus

O'zidan ko'payish: ha

Sonini oshib borishi: ijobiy

Yuqumliligi: ha

Barcha vaqtlarning eng kuchli 4 virusi

1. I LOVE YOU

I LOVEYOU hozirgi kunga qadar yaratilgan eng kuchli zararli viruslardan biri hisoblanadi. U butun dunyo bo'ylab kompyuter tizimlariga vayronagarchiliklarni keltirib chiqardi va taxminan 10 milliard dollar zarar keltirdi. Dunyo kompyuterlarining 10 foizi zararlangan deb hisoblangan. Hukumatlar va yirik korporatsiyalar infeksiyani oldini olish uchun pochta

tizimlarini oflayn rejimga o'tkazganlar.

Virus ikki filipinlik dasturchi Reonel Ramones va Onel de Guzman tomonidan yaratilgan. Bu virus sotsial injineriyadan foydalanib, odamlarni

—qo'shimcha havolani" bosishga majbur qildi. Bu holda sevgini tan olish so'rovi bo'lgan. Ilova aslida TXT fayl sifatida shakllanadigan skript bo'lgan. Chunki o'shapaytda Windows ushbu faylning haqiqiy kengaytmasini yashirgan yedi.

Bosish tugmachasini bosgandan so'ng, u foydalanuvchini yuborish ro'yxatidagi har bir kishiga o'zini yuboradi va fayllarni qayta yozishni davom ettiradi. Bu esa kompyuterni o'chirib bo'lmaydigan holatga tushiradi.

2. Code Red

Code Red birinchi marta 2001 yilda paydo bo'lgan va eEye Digital Security tashkilotining ikki xodimi tomonidan topilgan. Bu kashfiyot paytida juftliklar Code Red Mountain Dew nomli ichimlikni ichganligi sababli Code Red deb nomlangan.

Tizimda bufer toshib ketish muammosidan foydalanib, Microsoft IIS veb-serveri o'rnatilgan kompyuterlarni nishon qilib olgan. U qattiq xotirada juda oz iz qoldiradi. Chunki u to'liq xotirada ishlay oladi, hajmi 3569 baytga teng.

Infeksiyani yuqtirganida, u yuz nusxani yaratishga kirishadi, lekin dasturlashdagi xato tufayli u yana ko'payadi va ko'plab tizim resurslarini iste'mol qilib tugatadi.

Eng esda qolarli alomat bu ta'sirlangan veb-sahifalarda —Xitoyliklar tomonidan hujum qilindi" deb qoldirgan xabar bo'lib, u o'zi ham memga aylangan. Keyinchalik vaksina chiqarildi va keyinchalik 2 milliard dollargacha zarar keltirgani hisoblangan. Jami 1-2 million serverlar ta'sir ko'rsatdi. Shu davrda 6 million IIS serverlar mavjud bo'lgan.

3. Melissa

Florida shtatidagi yekzotik raqqos nomi bilan 1999 yilda Devid L. Smit tomonidan yaratilgan. Bu virus bilan zararlangan Word hujjati, alt.sex nomi bilan markazlashmagan tarmoq guruhiga joylashtirilgan va pornografik saytlar uchun parollar ro'yxati deb da'vo qilingan. Bu narsa odamlarni qiziqitirdi va yuklab olib

ochganda ishga tushadi.

Virus o'zini elektron pochta manzillar kitobidagi 50 ta odamga yuboradi va bu elektron pochta trafikining ko'payishiga olib keladi. Bu hukumat va korporatsiyalarning elektron pochta xizmatlarini buzgan. Bundan tashqari, ba'zan ularga Simpsons (Amerika animatsiya janri) ma'lumotnomasini qo'shish orqali hujjatlarni buzadi.

Oxir oqibat Smit Word hujjatini unga topshirishganida qo'lga olindi. Fayl o'g'irlangan AOL akkauntidan foydalanib yuklangan va ularning yordami bilan huquqni muhofaza qilish idoralari uni avj olganidan bir haftadan kamroq vaqt ichida hibsga olishga muvaffaq bo'lishgan.

U FQB bilan Anna Kournikova virusini yaratuvchisi sifatida tanilgan boshqa virus yaratuvchilarini ushlashda hamkorlik qildi. Hamkorligi uchun u bor-yo'g'i 20 oy xizmat qildi va belgilangan 10 yillik qamoq jazosi uchun 5000 dollar miqdorida jarima to'ladi. Ma'lum qilinishicha, virus 80 million dollar zarar yetkazgan.

4. Sasser

Windows OT qurti birinchi marta 2004 yilda kashf yetilgan bo'lib, uni Netsky qurti yaratgan talaba Sven Jaschan yaratgan. Ushbu chuvalchang Local Security Authority Subsystem Service (LSASS) tizimida bufer to'lib toshishi mumkin bo'lgan zaiflikdan foydalandi. Bu esa kompyuterning buzilishiga sabab bo'luvchi lokal qayd yozuvi xavfsizlik siyosatini nazoratlash imkonini bergan. Bundan tashqari, u tizim manbalarini Internet orqali boshqa mashinalarga tarqatish va boshqalarga avtomatik ravishda yuqtirish uchun foydalanadi.

Bu virus aviakompaniyalar, axborot agentliklari, jamoat transporti, kasalxonalar va boshqa ko'plab muhim infratuzilmalarga ta'sir qilib, milliondan ortiq infeksiyalanish holatini qayd qildi. Umuman, zarar 18 milliard dollarga tushdi. Jaschen balog'at yoshiga yetmaganlikda ayblanib, 21 oy shartli qamoq jazosiga hukm qilindi.

Viruslarga oid statistikalar.

1. Amerikaliklar kiberjinoatlardan juda ham qo'rqadi 70% Amerikaliklar kompyuter va onlayn tarmoq orqali shaxsiy ma'lumotlarini o'g'irlanishidan xavotirda. Boshqa holat, terrorizmdan esa 24% aholi va 17% i o'ldirilishlaridan qo'rqadi.

2. MS Office – birlamchi nishon

Eng keng tarqalgan viruslar asosan .exe kengaytmali fayllar ko'rinishida bo'lsa, ularni bosmaslik va pochta orqali qabul qilinganlarini yuklamaslikni hamma yaxshi biladi. Biroq, foydalanuvchilar oddiy .doc faylni yuklashdan shubhalanmaydilar. Hozirda zararli dasturlarning 38% Word hujjatlari sifatida yashiringan.

3. Ransomware hanuzgacha mavjud

Ransomware turidagi zararli dasturlarni hozirgi kunda tarqalishi kamaygan degan gaplar noto'g'ri. 2019 yilda tashkilotlar va foydalanuvchilar tomonidan 11.5 milliard dollar turli holatlar uchun to'lanishi kutilmoqda. Ushbu hujumlarning asosiy qurbonlari mahalliy tashkilotlar bo'lib, ularga Jackson County, GA, Orange County, NC, va Baltimore, MD larni keltirish mumkin.

4. Zararli dasturlarning zarar hajmi ortmoqda

2015 yilda zararli dasturlarning qiymati allaqachon ajablantirgan 500 milliard dollarni tashkil qilgan. Qisqa vaqt ichida kiberjinoatlarning iqtisodiy zarari 4 baravarga oshib, 2 trilion dollarga yetdi. Ushbu tendensiya bo'yicha 2021 yilda kelib ularning qiymati 6 triloyni dollarga etadi.

5. Xakerlarning qiziqishi mobil telefonlarga nisbatan ortdi

Mobil telefonlarning keng tarqalishi natijasida, ular hozirgi kunga kelib xakerlarning asosiy nishoniga aylandi. Mobil qurilmalar uchun zararli dasturlar asosan Android ilovalarining eski versiyalariga qaratilgan va ular hozirgi kunda Android va Appstoreda keng tarqalgan.

Har kuni 24000 yaqin zararli dasturlar bloklanadi.

6. Aksariyat zararli dasturiy vositalar pochta orqali kirib kelmoqda

Elektron pochta hozirgi kunda zararli dasturlarning keng tarqalishiga xizmat qilayotgan vosita bo'lib, 50000 xavfsizlik insidentlarining 92% pochta orqali kirib keladi. Undan keyingi o'rinda brauzerga asoslangan tarqalish usuli (masalan, ko'chirish) o'rin olgan.

7. Kiberjinoyatchilikning asosiy motivatsiyasi – pul

Hujumchilarning 76% amalga oshirilayotgan kompyuter hujumidan moddiy foyda olishni maqsad qiladi.

Nazorat savollari:

1. Kompyuter virusi nima?
2. Fayl va disklarda kompyuter viruslari mavjudligini tekshirish.
3. Elementlarni, uzil(tugun)va qurilmalarda kompyuter viruslari mavjudligini tekshirish.
4. Virus nima va uning bajaradigan vazifasi?
5. Viruslar kompyuterda qanday paydo bo'ladi?
6. Viruslarning qanday turlarini bilasiz?
7. Kompyuterda viruslar mavjudligi qanday aniqlanadi?
8. Antivirus dasturlarining qanday turlarini bilasiz?

13-Mavzu: Axborot xavfsizligi siyosati.

Tayanch iboralar: IT security, kiberxavfsizlik, konfidensiallik, yaxlitlik, foydalanuvchanlik

Axborotni muhofaza qilish davlat tizimi axborotni himoyalovchi texnikani qo'llaydigan idoralar va ijro etuvchilar hamda himoya obyektlari majmuini ifodalaydi. Bu tizim axborotni muhofaza qilish sohasidagi huquqiy,tashkiliy-boshqaruv va me'yoriy hujjatlarga muvofiq tashkil etiladi va faoliyat yuritadi. Shu bilan birga mamlakat milliy xavfsizligini ta'minlash tizimining tarkibiy qismi hisoblanadi va davlat xavfsizligini axborot sohasidagi ishki va tashqi tahdidlardan himoyalashga yo'naltirilgan.

Axborot xavfsizligi tushunchasi.

Axborot xavfsizligi deganda tabiiy yoki su'niy xarakterdagi tasodifiy yoki qasddan qilingan ta'sirlangan axborot va uni qo'llab-quvvatlab turuvchi infrastrukturaning himoya-langanligi tushuniladi. Bunday ta'sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalari, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo'llab quvvatlovchi infrastukturaga jiddiy zarar yetkazishi mumkin.

Axborot xavfsizligi siyosati

O'zbekiston Respublikasi Vazirlar Mahkamasining 2013 yil 16 sentabridagi

“O'zbekiston Respublikasi aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo'mitasi huzuridagi “Elektron hukumat” tizimini rivojlantirish markazi va Axborot xavfsizligini ta'minlash markazlarini tashkilotish chora-tadbirlari to'g'risida” gi qarori bilan markazlar tashkil etildi va faoliyati yo'lga qo'yildi.

Axborotni muhofaza qilish axborotni ixtiyoriy ko'rinishda yo'qotishda (o'g'irlash, buzish, qalbakilash- tirish) ko'riladigan zararining oldini olishni ta'minlashi lozim. Axborotni muhofaza qilish choralari axborot xavfsizligiga oid amaldagi qonun va me'yoriy hujjatlar asosida va axborotdan foydalanuvchilarning

manfaatlariga ko'ra tashkil etilishi zarur. Yuqori darajada axborotni muhofaza qilishni kafolatlash uchun muntazam ravishda murakkab ilmiy – texnik vazifalarni hal etish va himoya vositalarini takomillashtirish talab etiladi.

Bugungi kunda axborot xavfsizligini ta'minlaydigan uchta asosiy tamoil Ya'ni ma'lumot butunligi, axborotning konfidensialligi va foydalanish huquqlariga ega barch foydalanuvchilar axborotdan foydalana olishlari; bilan bir qatorda ayrim faoliyat sohalari (huquqni muhofaza qilish organlari, mudofaa va maxsus tuzilmalar, bank va moliya institutlari, axborot tarmoqlari, davlat boshqaruv tizimlari) ularda ko'riladigan masalalarning muhimligi va xarakteriga ko'ra, ularning axborot tizimlari faoliyati ishonchililigiga nisbatan yuqori talablar va xavfsizlik bo'yicha maxsus choralar ko'rilishini talab etadi.

Axborotni muhofaza qilishning samaradorligi uning o'z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirini kompleks tarzda o'tkazish axborot tarqab ketishi mumkin bo'lgan xavfli kanallarni yo'q qilishni ta'minlaydi. Vaholanki, birgina ochiq qolgan axborotning tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborot hisoblash tizimlarida axborot xavfsizligini ta'minlash nuqtai nazaridan o'zaro bog'liq bo'lgan uchta tashkil etuvchi Ya'ni axborot; texnik va dasturiy vositalar; xizmat ko'rsatuvchi personal va foydalanuvchilarga e'tibor qaratiladi.

Axborotni muhofaza qilish tamoillarini uch guruhga bo'lish mumkin: Huquqiy, tashkiliy hamda texnik razvedkadan himoyanishda va hisoblash texnikasi 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.

Axborotni muhofaza qilishda foydalanuvchi asosiy usullar bilan bir qatorda axborotlarni ma'naviy – ma'rifiy himoyalash usuli juda muhim rol o'ynaydi. Aynan inson, u korxona yoki tashkilot hodimi, maxfiy ma'lumotlardan voqif bo'lib, o'z

xotirasida ko'plab ma'lumotlarni jamlaydi va ba'zi hollarda axborot chiqib ketishi manbaiga aylanishi mumkin hamda uning aybi bilan o'zgaralar ushbu axborotga noqonuniy ega bo'ladilar. Axborotlarni ma'naviy-ma'rifiy himoyalash usulida xodimni tarbiyalash, u bilan ma'lumotlarning sifatlarini, qarashlarini shakllantirishga yo'naltirilgan maxsus ishlarni olib borish (vatanparvarlik, axborotni muhofaza qilish uning shahsan o'zi uchun ham qanday ahamiyat aks etishini tushintirish) hamda xodimni axborotni muhofaza qilish qoidalarini va usullariga o'rgatish, konfidensial axborot tashuvchilar bilan amliy ishlash ko'nikmalarini shakllantirish lozim.

Jinoyatchilikni oldini olishda huquqni muhofaza qiluvchi organlarning xodimlari turli ko'rinish va mazmundagi axborotlarni yaratish, tahrir qilish, yig'ish, tarmoqda ma'lumotlarni uzatish, qabul qilish va ishonchli muhofaza qilish kabi vazifalarni bajarish uchun talab darajasidagi nazariy bilim va amaliy ko'nikmalarga ega bo'lishi lozim.

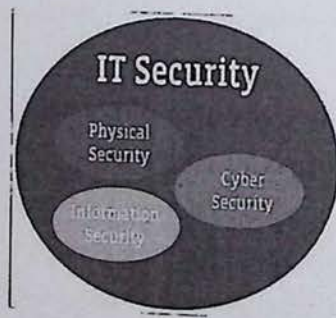
Axborotni muhofaza qilishning davlat tizimi

Axborotni muhofaza qilishning davlat tizimi axborotni muhofaza qilish sohasida tashkilotlar faoliyatini litsenziyalash nimitzimini axborotni muhofaza qilish vositalarini sertifikatlashtirish va axborot xavfsizligi talablari bo'yicha axborotlashtirish obyektlarini attestatsiyasini, kadrlarni tayyorlash, maxsus aloqa tizimlari, ilmiy tadqiqot va tajriba konstruktorlik ishlarini tashkillashtirish tizimlarini o'z ichiga oluvchi murakkab tizimdir. Axborotni muhofaza qilishning davlat tizimi ish yuritishi quyidagi qonun, me'yoriy hujjatlar asosida amalga oshiradi:

- O'zbekiston Respublikasining Konstitutsiyasi;
- "Davlat sirlarini saqlash to'g'risida" gi qonun;
- "Axborotlashtirish to'g'risida" gi qonun;
- "Maxsulotlar va xizmatlarni sertifikatlashtirish to'g'risida" gi qonun
- "Faoliyat ayrim turlarini litsenziyalash to'g'risida" gi qonun
- "Standartlashtirish to'g'risida" gi qonun

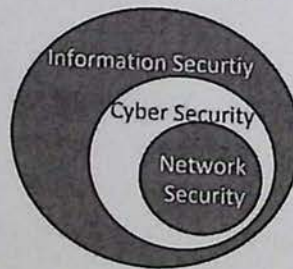
- “Aloqa to‘g‘risida”gi qonun
- “Telekommunikatsiyalar to‘g‘risida”gi qonun
- “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi qonun
- “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun
- “Elektron hujjat aylanishi to‘g‘risida”gi qonun;
- “Elektron raqamli imzo to‘g‘risida”gi qonun;
- “Elektron tijorat to‘g‘risida”gi qonun
- O‘zbekiston Respublikasi Prezidentining farmonlari va qarorlari;
- O‘zbekiston Respublikasi Vazirlar Mahkamasining qarorlari;
- Axborotni muxofaza qilish sohasidagi vazirlik, muassasa, agentlik va xo‘jaliklarning boshqa huquqiy aktlari.

Axborot tizimlari xavfsizligi.



3.8-rasm. Axborot tizimlari xavfsizligi.

Kiberxavfsizlik.



3.9-rasm. Kiberxavfsizlik.

Nima uchun kiberxavfsizlik kerak?



3.10-rasm

Kiberxavfsizlikni fundamental terminlari:

1. Konfidensiallik

- Tizim ma'lumoti va axborotiga faqat vakolatga ega subyektlar foydalanishi mumkinligini ta'minlovchi qoidalar.
- Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan "o'qilishini" ta'minlaydi.

2. Yaxlitlik (butunlik)

- Ma'lumotni aniq va ishonchli ekanligiga ishonch hosil qilish.
- Ya'ni, axborotni ruxsat etilmagan o'zgartirishdan yoki "yozish" dan himoyalash.

3. Foydalanuvchanlik

- Ma'lumot, axborot va tizimdan foydalanishning mumkinligi.

Ya'ni, ruxsat etilmagan "bajarish" dan himoyalash.

Kiberxavfsizlikni fundamental terminlari

Risk

-Potensial foyda yoki zarar.

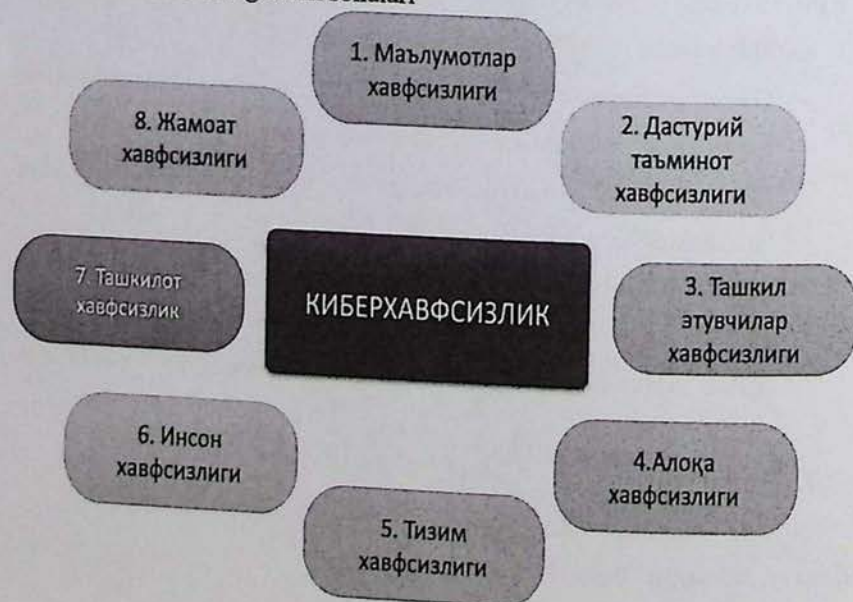
Hujumchi kabi fikrlash

- Bo'lishi mumkin bo'lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni.
- Yaxshi insonlar "yomon inson" kabi o'ylashi kerak !
- Militsiya xodimi kriminal haqida bilishi va tushinishi kerak
- Ushbu mavzuda
- Biz hujumchi foydalangan usullarini bilishni istaymiz
- Buzg'unchi motivlari haqida o'ylash kerak
- Tez – tez buzg'unchi kabi bo'lish

Tizimli fikrlash

Kafolatlangan amallarni ta'minlash uchun ijtimoiy va texnik cheklavlarni o'zaro ta'sirini hisobga oladigan fikrlash jarayoni.

Kiberxavfsizlikning bilim sohalari



Axborotni himoyalash konsepsiyasi

Axborotni himoyalash konsepsiyasi – axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yo'llari.

Konsepsiyani ishlab chiqishni uch bosqichda amalga oshirish tavsiya etiladi.

I bosqich

Himoyalanuvchi obyekt qiymatini aniqlash

II bosqich

Buzg'unchining bo'lishi mumkin bo'lgan harakatlarini tahlillash

III bosqich

Axborotni himoyalash vositalarining ishonchligini baholash

Axborot xavfsizligi siyosati bu – tashkilotning maqsadi va vazifasi hamda xavfsizlikni ta'minlash sohasidagi chora-tadbirlar tavsiflanadigan yuqori sathli reja hisoblanadi.

U xavfsizlikni ta'minlashning barcha dasturlarini rejalashtiradi. Axborot xavfsizligi siyosati tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta'minlashi shart.

Apparat vositalar va dasturiy ta'minot ish jarayonini ta'minlovchi vositalar hisoblanadi va ular xavfsizlik siyosati tomonidan qamrab olinishi shart
Tashkilotning amaliy xavfsizlik siyosati qo'yidagi bo'limlarni o'z ichiga olishi mumkin:

- umumiy nizom;
- parollarni boshqarish siyosati;
- foydalanuvchilarni identifikatsiyalash;
- foydalanuvchilarning vakolatlari;
- tashkilot axborot kommunikatsion tizimini kompyuter viruslardan himoyalash;
- tarmoq ulanishlarini o'rnatish va nazoratlash qoidolari;

- elektron pochta tizimi bilan ishlash bo'yicha xavfsizlik siyosati qoidalar;
- axborot kommunikatsion tizimlar xavfsizligini ta'minlash qoidalar;
- foydalanuvchilarning xavfsizlik siyosatini qoidalarini bajarish bo'yicha majburiyatlari va h.k.lar

Kiber xavfsizlik siyosati shablonlari

- ruxsat etiladigan shifrlash siyosati
- virusga qarshi himoya
- ruxsat etiladigan foydalanish siyosati
- xarid qilinganlarni baholash siyosati
- zaifliklarni skanerlash auditi siyosati
- avtomatik tarzda uzatiladigan pochta siyosati
- jiddiy axborotlar siyosati
- parollarni himoyalash siyosati
- xavf-xatarlarni baholash siyosati
- marshrutizator xavfsizligi siyosati
- server xavfsizligi siyosati
- VPN xavfsizligi siyosati

Xavfsizlik muammolariga zaiflik, tahdid, hujumlar kiradi.

Nazorat savollari.

1. IT security, kiberxavfsizlik tushunchalari.
2. Axborotni himoyalash konsepsiyasi.
3. konfidensiallik, yaxlitlik, foydalanuvchanlik tushunchalari.

14-Mavzu. Windows OT Foydalanuvchi qayd yozuvlarini boshqarish.

ASOSIY NAZARIY MA'LUMOT

Foydalanuvchi qayd yozuvi - bu tizimga ulanganida foydalanuvchini aniqlash uchun zarur bo'lgan ma'lumotlarni, shuningdek avtorizatsiya va audit uchun ma'lumotlarini o'z ichiga olgan yozuv.

Qayd yozuv quyidagi ma'lumotlarni o'z ichiga oladi: foydalanuvchi nomi (login), parol, to'liq ism va hokazo. Foydalanuvchi qayd yozuvi tizimdagi foydalanuvchi xatti-harakatlarining turli xil statistik xususiyatlarini ham hisobga olishi mumkin: oxirgi kirish vaqti, tizimda oxirgi seans davomiyligi, kompyuterni ulash uchun ishlatilgan manzil va hokazo.

Windows 7 OT da kompyuterlar uchun foydalanuvchi qayd yozuvlarini va domenning tarkibiga kiritilgan kompyuterlar uchun foydalanuvchi qaydyozuvlarini yaratishingiz mumkin. Ushbu laboratoriya faqat mahalliy qayd yozuvlar va guruhlarini boshqarishga qaratilgan.

Foydalanuvchilar guruhi - bu ularning barchasini bir xil nom bilan bog'lash imkonini beradigan foydalanuvchi qayd yozuvlarining to'plami. Guruhlar ma'lumotlarga kirish ruxsatini sozlash uchun qulay hisoblanadi.

Kompyuterga o'rnatilgan yangi Windows 10 operatsion tizimida ikkita qayd yozuvi mavjud – Administrator va Guest. Boshqasi OS ni o'rnatish jarayonida administrator tomonidan yaratilgan va odatiy holda Administratorlar guruhiga qo'shiladi.

O'rnatilgan guruhlarining ro'yxati quyidagi guruhlarini o'z ichiga oladi: Administratorlar (Администраторы), tajribali foydalanuvchilar (Опытные пользователи), foydalanuvchilar (Пользователи), mehmonlar (Гости), kriptografik operatorlar (Криптографические операторы), arxiv operatorlari (Операторы архива), tarmoqni sozlash operatorlari (Операторы настройки сети), masofaviy ish stoli foydalanuvchilari (Пользователи удаленного рабочего стола) va boshqalar.

Barcha o'rnatilgan guruhlarining maqsadlari va farqlari tavsifini Microsoft veb-saytida topish mumkin.

Tizimda ishlaydigan barcha ob'ektlar (foydalanuvchilar, guruhlar, mahalliy kompyuterlar, domenlar) Windows-da nafaqat nomlar bilan belgilanadi, ularning yagonaligini xavfsizlik identifikatorlari (*Security Identifiers, SID*) yordamida belgilash mumkin. Ularni har doim ham qo'lga kiritib bo'lmaydi.

Foydalanuvchi qayd yozuvi o'chirilganda xavfsizlik identifikatori ham yo'q qilinadi. Xuddi shu foydalanuvchi nomi va parol bilan, shuningdek boshqa xususiyatlar ham bir xil bo'lgan holatda yangi hisob yaratishda SID baribir boshqacha bo'ladi.

Tizimdagi ma'lum bir foydalanuvchi SID ni va u tarkibidagi guruhlarining SID ni konsolda **whoami** buyrug'idan foydalangan holda bilib olishingiz mumkin:

Windows 10 foydalanuvchi qayd yozuvlari va guruhlarini boshqarish uchun quyidagi usullarni taqdim etadi:

boshqaruv panelidagi «Foydalanuvchilar qayd yozuvi» (**Учетные записи пользователей, User Accounts**) dasturi;

boshqaruv panelidagi «Foydalanuvchilar qayd yozuvi 2» (**Учетные записи пользователей 2, User Accounts 2**) dasturi;

«Mahalliy foydalanuvchilar va guruhlar» (**Локальные пользователи и группы**) boshqaruv vositasi (**Local Users and Groups, LUG**);

net user va **localgroup** konsol buyruqlari.

Ushbu usullarning har biri o'ziga xos xususiyatlarga ega, ba'zi hollarda bitta dasturning imkoniyatlari boshqasida yo'q. Shuning uchun, eng maqbul vositaniani tanlash qiyin, barchasi sizning oldingizga qo'yilgan vazifalarga bog'liq. To'rtta usulning barchasini qamrab olgan jadval ilovada keltirilgan 1 [1].

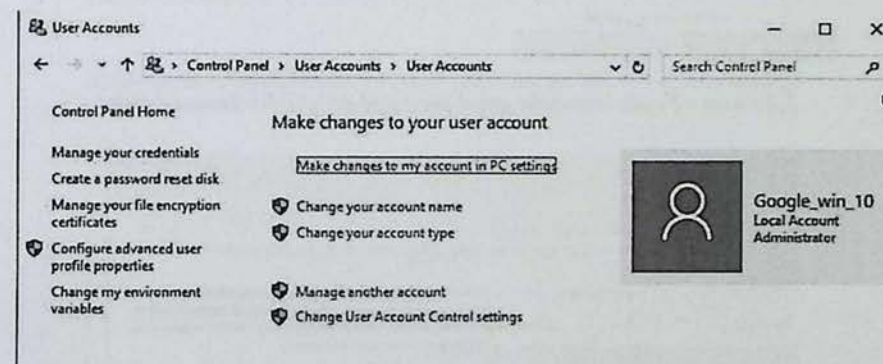
Quyida biz yuqorida sanab o'tilgan usullardan foydalangan holda foydalanuvchi qayd yozuvlari va guruhlarini boshqarish imkoniyatlarini ko'rib chiqamiz. Dastur interfeysi juda sodda ekanligi sababli, qayd yozuvlar va guruhlarini boshqarish usullarining tavsifi qisqacha taqdim etilgan.

Yangi foydalanuvchi qayd yozuvlarini yaratish yoki mavjudlarini o'zgartirish uchun, siz administrator huquqlariga ega qayd yozuv qaydnomasi sifatida tizimga kirishingiz kerak.

1. Foydalanuvchilar qayd yozuvi (User Accounts)

«Foydalanuvchilar qayd yozuvi» (**Учетные записи пользователей**) oynasini ishga tushirish uchun «Pusk» (**Пуск**) tugmasini bosish, «Boshqaruv paneli» (**Панель управления**) ni ochish va komponentalar ro'yxatidan

«Foydalanuvchilar qayd yozuvi» (**Учетные записи пользователей**) ni tanlash zarur (2.1-rasm).

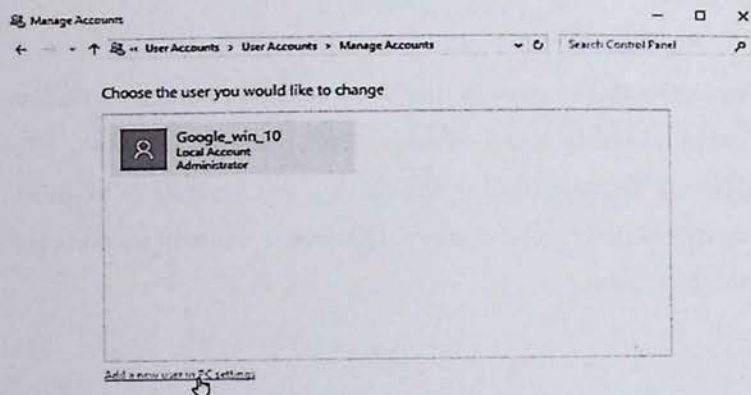


3.11-rasm «Foydalanuvchilar qayd yozuvi» oynasi

Ko'rsatilgan oynada, foydalanuvchi haqidagi ma'lumotlarni o'zgartirishingiz mumkin, xususan, siz parol, rasm, ism va foydalanuvchi qayd yozuvi turini, shuningdek parolni o'chirib tashlashingiz mumkin. Bundan tashqari, oynaning chap tomonida foydalanuvchi qayd yozuvlarini boshqarish (UAC) parametrlari va boshqa sozlamalarni boshqarish funksiyalari mavjud.

Boshqa foydalanuvchilar qayd yozuvini boshqarish, shu jumladan yangi qayd yozuvini yaratish uchun «Boshqa qayd yozuvini boshqarish» (**Управление другой учётной записью**) ni tanlang. Ko'rsatilgan oynada (2.2-rasm), siz o'zgartirmoqchi bo'lgan qayd yozuvini tanlashingiz yoki «Yangi qayd yozuvini

yaratish» (Создание учётной записи) menyusini tanlash orqali tizimda yangi foydalanuvchi yaratishni amalga oshirishingiz mumkin.



2.2-rasm «Foydalanuvchi qayd yozuvini qo'shish» ketma-ketligi



3.12-rasm «Foydalanuvchi qayd yozuvini qo'shish» ketma-ketligi

How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

Email or phone

I don't have this person's sign-in information
Privacy statement

Cancel

Next

3.13-rasm «Foydalanuvchi qayd yozuvini qo'shish» ketma-ketligi

Let's create your account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when you sign in with your Microsoft account.* Learn more

someone@example.com

Get a new email address

Password

Uzbekistan

Birth month Day Year

*If you already use a Microsoft service, go Back to sign in with that account.

Add a user without a Microsoft account

Back

Next

3.14-rasm «Foydalanuvchi qayd yozuvini qo'shish» ketma-ketligi

Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

Testing1

Make it secure.

Enter password

Re-enter password

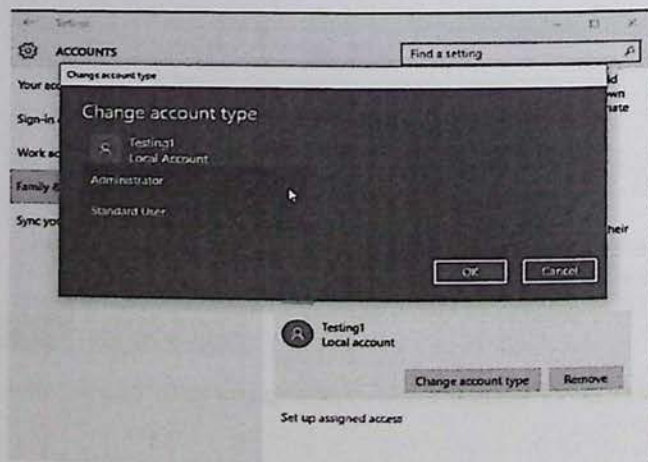
Password hint

Back

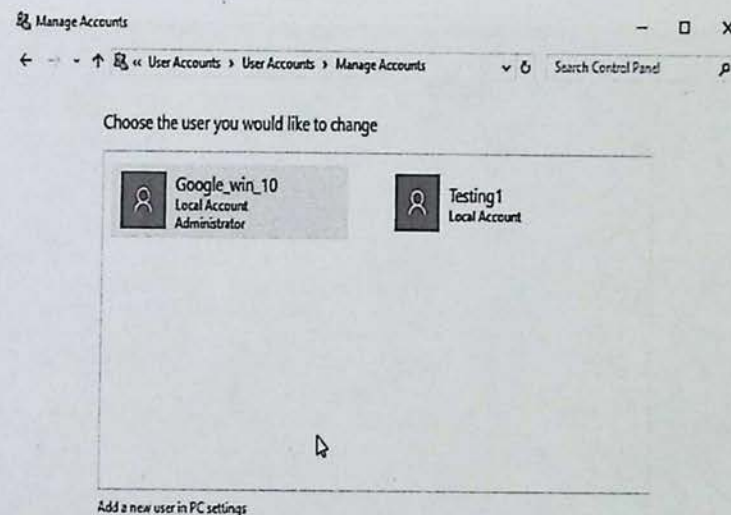
Next

3.15-rasm «Foydalanuvchi qayd yozuvini qo'shish» ketma-ketligi

«Yangi qayd yozuvini yaratish» (Создание учётной записи) oynasida (2.3-rasm) foydalanuvchi nomini kiritish va qayd yozuv turini tanlash so'raladi: Oddiy kirish ("Foydalanuvchilar" guruhi) yoki Administrator ("Administratorlar" guruhi).



3.16-rasm. «Yangi qayd yozuviga role berish» oynasi



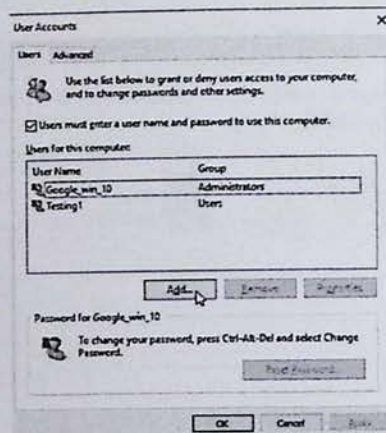
3.17-rasm. «Yangi qayd yozuvlar» oynasi

2. Foydalanuvchilar qayd yozuvi 2 (User Accounts 2)

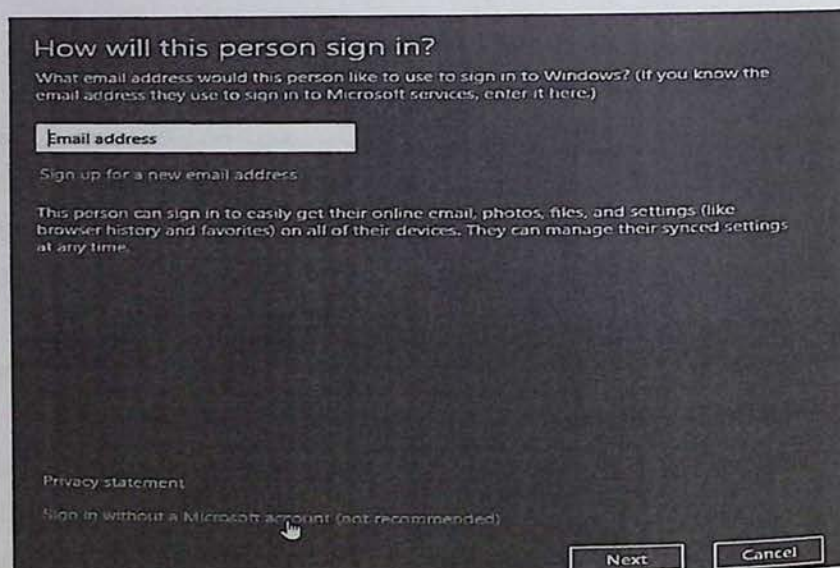
Ikkinchi usul «Foydalanuvchilar qayd yozuvi» (Учетные записи пользователей) dasturining alternativ va eski analogidir. Boshqaruv panelida «Foydalanuvchilar qayd yozuvi 2» (Учетные записи пользователей2) dasturi mavjud emas. Uni ishga tushirish uchun «Выполнить» (Win + R) dialog oynasining

«Kiritish» (Открыть) maydoniga netplwiz yoki control userpasswords2 ni kiritishingiz va «OK» tugmasini bosishingiz kerak.

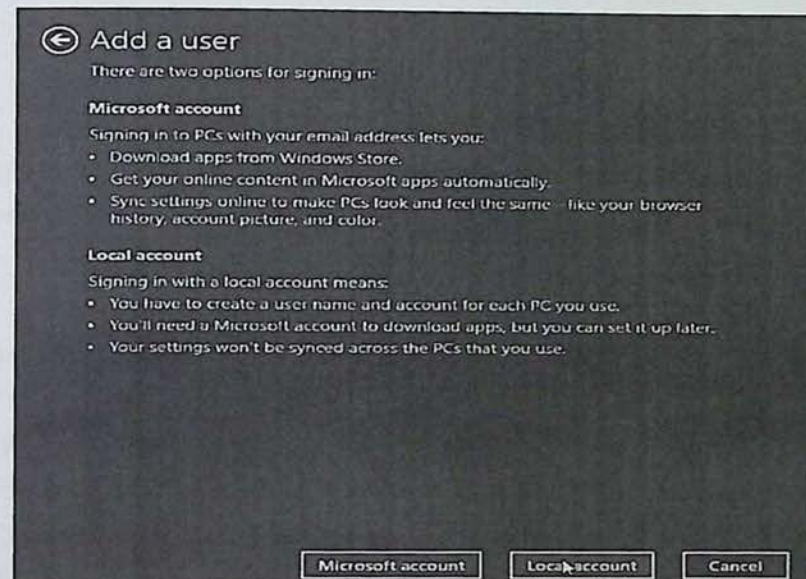
Ko'rsatilgan oynada (2.4-rasm) foydalanuvchilarni qo'shish va o'chirish mumkin, shuningdek «Xususiyatlar» (Свойства) tugmasini bosganingizda (2.5-rasm) foydalanuvchi nomini, to'liq nomini, tavsifini o'zgartirishingiz va istalgan guruhga qo'shishingiz mumkin.



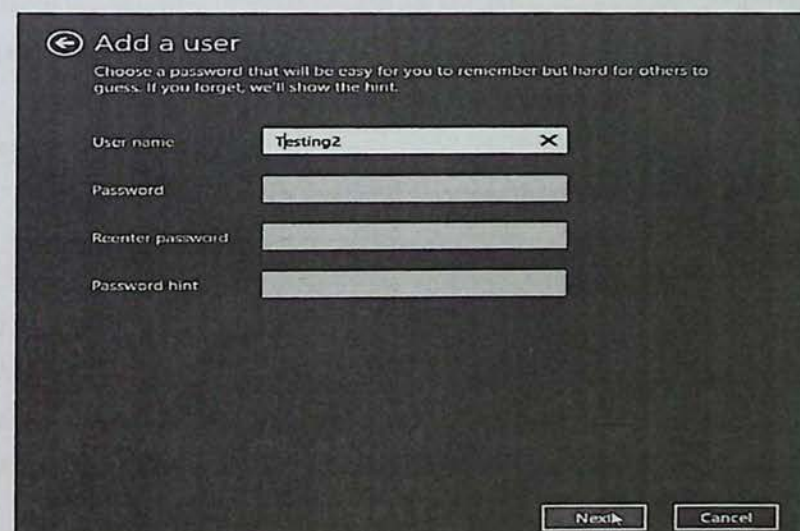
3.18-rasm. «Foydalanuvchilar qayd yozuvi 2» oynasi



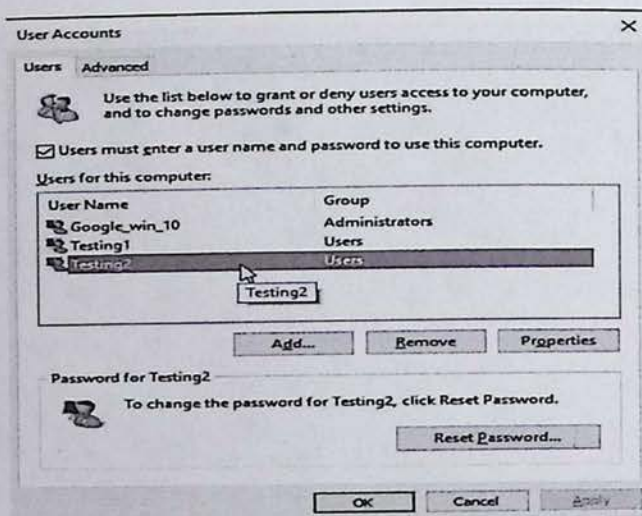
3.19-rasm. «Foydalanuvchilar qayd yozuvi 2» oynasi yaratish.



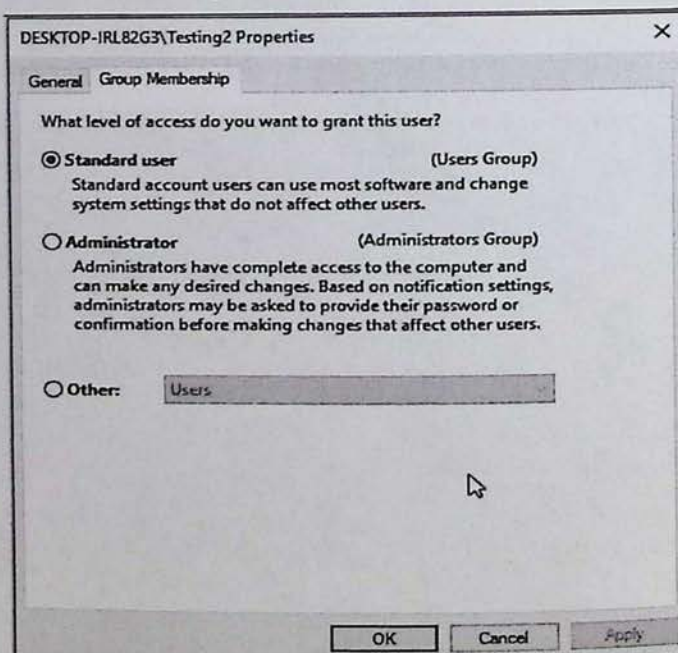
3.20-rasm. «Foydalanuvchilar qayd yozuvi 2» oynasi yaratish.



3.21-rasm. «Foydalanuvchilar qayd yozuvi 2» Testing2foydalanuvchini yaratish.



3.22-rasm. «Foydalanuvchilar qayd yozuvi 2» oynasi



3.23-rasm okna «Foydalanuvchilar qayd yozuvi 2» oynasining «Xususiyatlar»(Properties) bo'limi

3. Mahalliy foydalanuvchilar va guruhlar (Локальные пользователи и группы, Local Users and Groups)

Qayd yozuvlar va guruhlar bilan ishlashning eng ko'p funktsiyali vositasi bu «Mahalliy foydalanuvchilar va guruhlar» (Локальные пользователи и группы) ma'lumotlar to'plami, u «Kompyuterni boshqarish» (Управление компьютером) komponentida joylashgan.

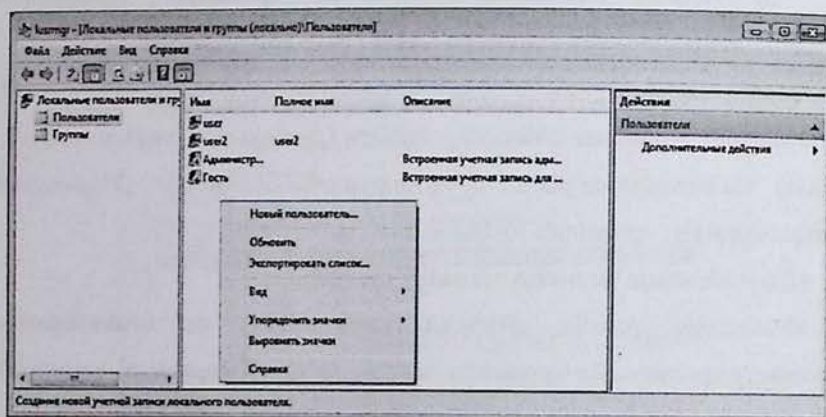
Chaqirish uchun bir nechta variantlar mavjud:

1. «Boshqaruv paneli» (Панели управления) da «Administrator» (Администрирование) komponentini tanlang, so'ng «Kompyuterni boshqarish» (Управление компьютером) ni oching. Konsol daraxtida «Mahalliy foydalanuvchilar va guruhlar» (Локальные пользователи и группы) tugunini oching;

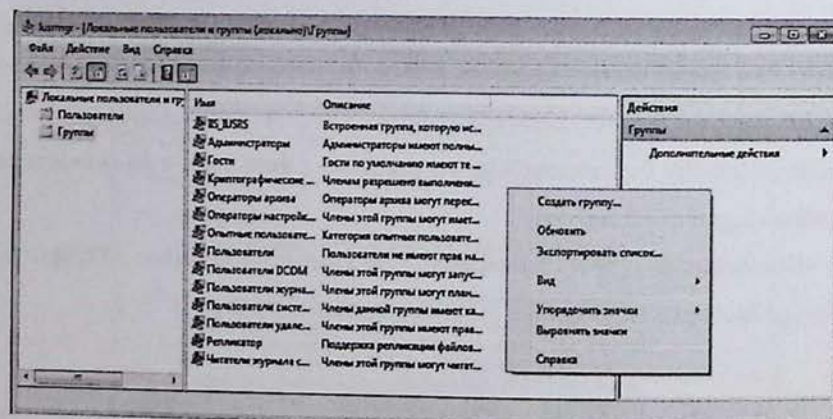
2. sichqoncha ko'rsatkichini ishchi stoli yoki «Pusk» (Пуск) menyusidagi «Kompyuter» (Компьютер) belgisiga olib borib, sichqonchaning o'ng tugmasini bosing va paydo bo'lgan ro'yxatda «Boshqaruv» (Управление) ni tanlang. Konsol daraxtida «Mahalliy foydalanuvchilar va guruhlar» (Локальные пользователи и группы) tugunini oching;

3. «Выполнить» (Win + R) dialog oynasining «Kiritish» (Открыть) maydoniga lusrmgr.msc ni kiriting va «OK» tugmasini bosing.

Ko'rsatilgan oynaning chap qismida ikkita katalog mavjud - «Foydalanuvchilar» (Пользователи) (2.6-rasm) va «Guruhlar» (Группы) (2.7- rasm). Yangi foydalanuvchi yoki guruh yaratish uchun siz oynaning o'rtasidagi bo'sh joyda sichqonchaning o'ng tugmachasini bosishingiz va kontekst menyusida mos ravishda «Yangi foydalanuvchi» (Новый пользователь) yoki «Guruh yaratish» (Создать группу) ni tanlashingiz kerak.

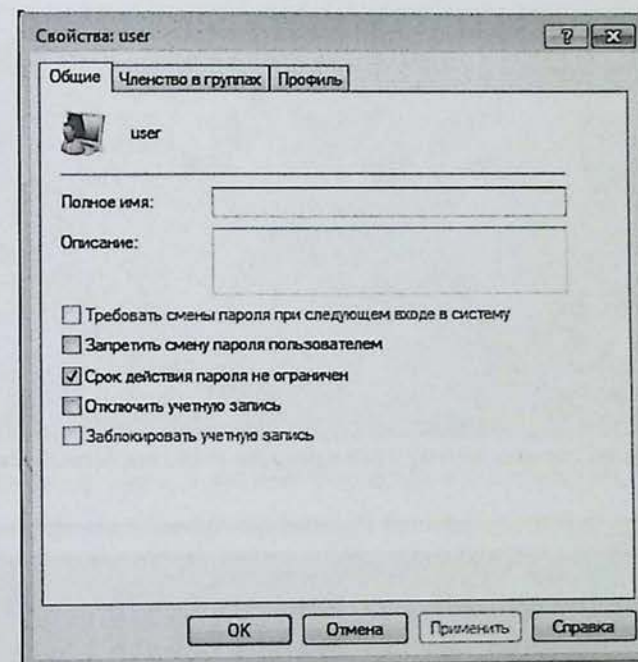


3.24-rasm. «Mahalliy foydalanuvchilar va guruhlar» (Локальные пользователи и группы) oynasi «Foydalanuvchilar» (Пользователи) bo'limi



3.25-rasm. «Mahalliy foydalanuvchilar va guruhlar» (Локальные пользователи и группы) oynasi «Guruhlar» (Группы) bo'limi

Foydalanuvchilar ro'yxatidagi yozuvlardan birini ikki marta bosganingizda hqayd yozuv sozlamalarini o'zgartirish oynasi paydo bo'ladi (2.8-rasm). Xususan, foydalanuvchining to'liq nomi va tavsifini o'zgartirish, qayd yozuvni o'chirib qo'yish va qayd yozuvni yopish, foydalanuvchining guruhlariga a'zoligini o'zgartirish va hokozo.



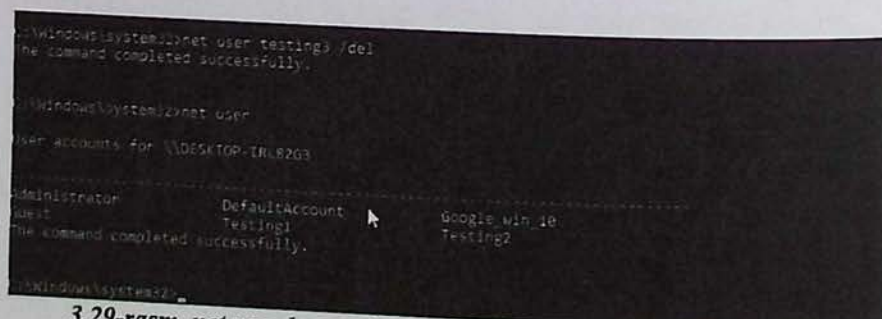
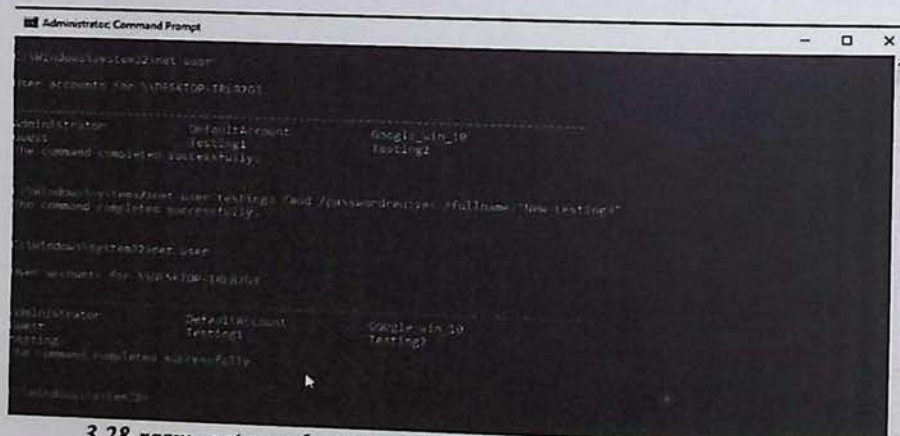
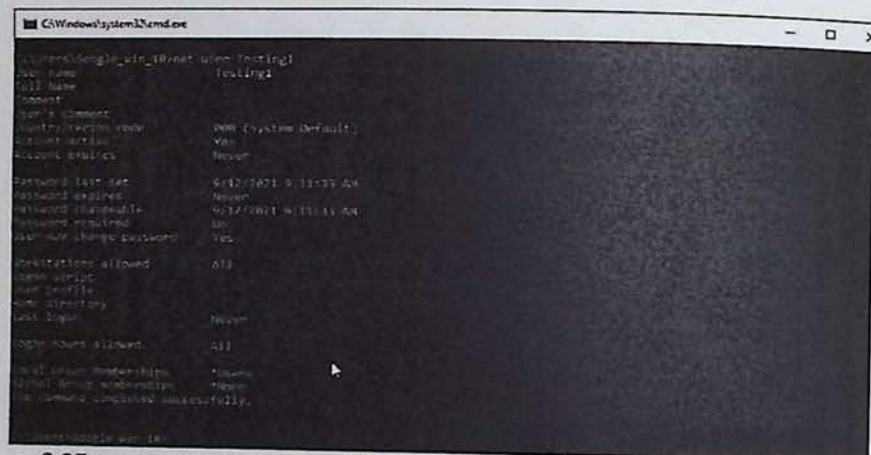
3.26-rasm. Tanlangan foydalanuvchi uchun «Xususiyatlar» (Свойства) oynasi

4. net user va net localgroup konsol komandolari

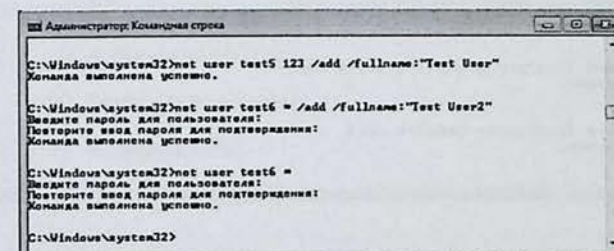
Windows OTda foydalanuvchi qayd yozuvlari va guruhlar bilan ishlash uchun ikkita konsol komandasidan foydalaniladi – ular mos ravishda **net user** va **net localgroup** komandolari.

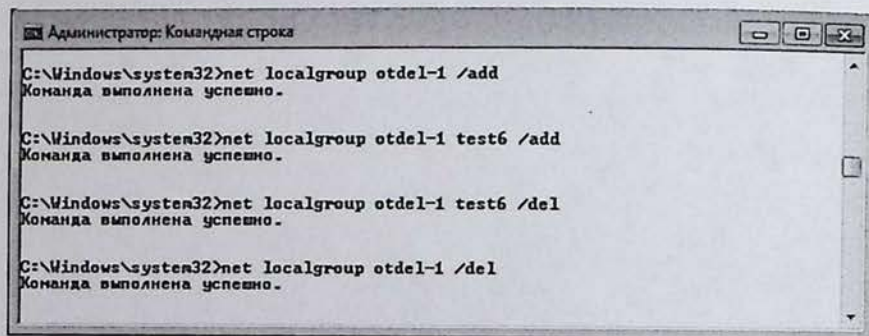
net user komandasi buyruqlar satrida tizimdagi foydalanuvchilar ro'yxatini ko'rastirish vazifasini bajaradi. Qayd yozuv nomi bilan bir xil bo'lgan buyruqni kiritish orqali foydalanuvchi to'g'risidagi batafsil ma'lumotlarni ko'rish mumkin (2.9-rasm).

Yangi foydalanuvchini yaratish uchun **/add** parametridan foydalangan holda **net user** buyrug'i ishlatiladi (2.10-rasm), o'chirishda - **/del** (2.11-rasm).



Mavjud foydalanuvchi uchun ham foydalanuvchi parolini o'rnatish mumkin. Parol foydalanuvchi nomidan keyin kiritiladi. Terilgan parolning ekranda ko'rinishligi uchun parol o'rniga * belgisini kiritish kerak (2.12-rasm).





3.32-rasm. Yangi guruh yaratish (o'chirish), net localgroup buyrug'i yordamida foydalanuvchini guruhga qo'shish (o'chirish)

Ushbu amaliy ishda yuqorida aytib o'tilgan barcha usullar bilan foydalanuvchi qayd yozuvini yaratishni o'rgandim, shuningdek foydalanuvchilar guruxi, har bir qayd yozuvga parol qo'yish, o'zgartirish, foydalanuvchilarni guruxga qo'shish va o'chirishni ko'rib chiqdim. Umuman olganda shaxsan menga foydalanuvchi qayd yozuvini yaratish buyruqlar satri bilan amalga oshirilishi maqul bo'ldi.

TESTLAR

Tasodifiy yoki oldindan ko'zlangan tabiiy yoki sun'iy xarakterga ega bo'lgan ta'sirlardan, infrastrukturani qo'llab quvvatlovchi axborot foydalanuvchilaridan va egalaridan axborotni himoyalash qaysi atama ta'rifi?

- a) Axborot xavfsizligi
- b) Kompyuter viruslari
- c) Kriptotizimlar
- d) Identifikatsiya

Axborotni xavfsizligini ta'minlashga qaratilgan kompleks chora-tadbirlarqanday ataladi?

- a) Axborotni himoyalash
- b) Kompyuter viruslari
- c) kriptotizimlar
- d) Identifikatsiya

Axborotni himoyalashning maqsadlari qaysilar.

- a) Foydalanuvchanlik, Butunlik, Maxfiylik
- b) Omaviylik, tushunarlilik
- c) Aniqlilik, tushunarlilik
- d) Diskretlik, tushunarlilik

Ma'lum vaqt oralig'ida kerakli axborot xizmatini olish imkoniyatidir. Bu axborotni himoyalashning qaysi maqsadi?

- a) Foydalanuvchanlik
- b) Butunlik
- c) Maxfiylik
- d) Aniqlilik

Axborotni aktualliligi bo'lib, uni yo'q qilinishidan va ruxsat etilmagan o'zgartirishlardan himoyalanganligidir. Bu axborotni himoyalashning qaysi maqsadi?

- a) Butunlik
- b) Maxfiylik
- c) Aniqlilik
- d) Foydalanuvchanlik

Axborotni ruxsat etilmagan murojaatlardan himoyalash. Bu axborotni himoyalashning qaysi maqsadi?

- a) Maxfiylik
- b) Aniqlilik
- c) Foydalanuvchanlik
- d) Butunlik

U (grekcha so'zi, maxfiy belgilar bilan yozilgan hat) - bu axborotni ko'zda tutilmagan foydalanuvchilardan himoyalash yo'lida, axborotni o'zgartirish bilan bog'liq bo'lgan g'oya va usullar yig'indisidir.

- a) Kriptografiya
- b) Shifrlash
- c) Kodlash
- d) Deshifrlash

Axborotlar ustida amallar bajarish qulay bo'lishi uchun aniq bir qoidalar asosida boshqa ko'rinishga o'tkazish jarayoni axborotni nima deyiladi.

- a) kodlash
- b) shifrlash
- c) deshifrlash
- d) kriptografiya

Axborotlarni kodlash insoniyat tomonidan faqat amallar bajarish qulay bo'lishi uchun emas, balki axborotni maxfiy saqlash uchun ham qo'llanilgan. Kodlashning bu ko'rinishi nima deb ataladi.

- a) shifrlash
- b) kodlash
- c) deshifrlash
- d) kriptografiya

Birinchi kodlashni qo'llagan inson qadimgi Gretsiya sarkardasi hisoblanadi.

- a) Lisandro
- b) Lionardo
- c) Sezar
- d) Vijiner

U axborotni maxfiy saqlash, Ya'ni kodlash uchun ma'lum bir qalinlikdagi "Ssital" tayoqchasini o'ylab topgan. U kim?

- a) Lisandro
- b) Lionardo
- c) Sezar
- d) Vijiner

"Ssital" tayoqchasida kodlash kodlashning qanday usuli deb ataladi.

- a) o'rin almashtirish.
- b) O'rni qoyish
- c) Aralash
- d) alifboni surish

"Sezar shifri" da matndagi harf alifboda o'zidan keyin kelgan nechanchi harfga aimashtiriladi.

- a) uchinchi
- b) ikkinchi
- c) To'rtinchi
- d) Olinchi

"Sezar shifri" kodlash usul qanday usuli deyiladi.

- a) alifboni surish
- b) o'rin almashtirish
- c) O'rniga qoyish
- d) Aralash

U 1837-yilda elektromagnit telegraf qurilmasini ixtiro qilgan va 1838-yildashu qurilma uchun telegraf kodini ishlab chiqqan. U kim?

- a) Semyuel Morze
- b) Lisandro
- c) Lionardo
- d) Sezar

Morze kodlash usulini qanday kodlash deb yuritiladi.

- a) notekis
- b) tekis
- c) murakkab
- d) oddiy

Kodlash usulida ishtirok etgan belgilar soni (hajmi) bir xil bo'lsa qanday kodlash usuli deb ataladi.

- a) tekis
- b) notekis
- c) murakkab
- d) oddiy

Kodlash usulida ishtirok etgan belgilar soni (hajmi) bir xil bo'lmasa qanday kodlash usuli deb ataladi.

- a) notekis
- b) tekis
- c) murakkab
- d) oddiy

Morze kodlash usulida nechta belgi ishlatiladi?

- a) 3
- b) 2
- c) 1
- d) 4

Friday 13" nomli virusining ish prinsipini toping.

- a) 13 sana juma kunlari ishlanayotgan fayllarni o'chiradi
- b) 13 ta faylni o'chiradi
- c) 13 sana payshanba kunlari ishlanayotgan fayllarni o'chiradi
- d) Juma kunlari 13 ta fayl o'chiradi

"Black Friday" nomli virusining ish prinsipini toping.

- a) juma kunlari ishlanayotgan fayllarni o'chiradi
- b) juma kunlari ishlanayotgan fayllarni davolaydi
- c) juma kunlari ishlanayotgan —qora" nomli fayllarni o'chiradi
- d) payshanba kunlari ishlanayotgan fayllarni o'chiradi

“Black Hole” nomli virusining ish prinsipini toping.

- a) ekranning pastki burchagidan qora tuynuk ochadi
- b) ekranning o‘ng burchagidan qora tuynuk ochadi
- c) ekranning chap burchagidan qora tuynuk ochadi
- d) ekranning yuqori burchagidan qora tuynuk ochadi

Virus guruhlari to‘g‘ri ko‘rsatilgan faylni toping.

- a) fayl, boot, makroviruslar, tarmoq viruslari
- b) rezident, norezident, mikroviruslar, tarmoq viruslari
- c) fayl, boot, mikroviruslar, tarmoq viruslari
- d) xavfsiz, xavfli, juda xavfli

Fayl viruslari qanday kengaytmadagi viruslarni zararlaydi.

- a) COM, EXE, DLL
- b) DOC, EXE, Boot
- c) Boot, EXE, DLL
- d) COM, XLS, DLL

Boot viruslar kompyuterni qaysi sohasini zararlaydi.

- a) qattiq disk (vinchester) ning yuklovchi sohasini
- b) tezkor xotira sohasini
- c) video xotira sohasini
- d) protsessorni

Operatsion sistemani yuklovchi 0 - trakiga yozib olinuvchi virusni aniqlang.

- a) boot viruslari
- b) fayl viruslari
- c) tarmoq viruslari
- d) makro viruslari

O‘zbekistonda mavjud bo‘lmagan viruslar guruhini toping.

- a) Quddus va TR
- b) TR va Avenger
- c) Datacrime va Island
- d) Avenger va Vena

Microsoft Word va Excel dasturlarida keng tarqalgan virus nomini toping.

- a) fayl
- b) boot
- c) tarmoq
- d) makrovirus

Tarmoqqa zarar keltiruvchi viruslar qanday nomlanadi.

- a) tarmoq viruslari
- b) cherv
- c) replikatorlar
- d) troyan

Morris virusi qachon internet tarmog‘iga tarqatildi.

- a) 1988-yil
- b) 1985-yil
- c) 1987-yil
- d) 1986-yil

Arxivator dasturlari ko‘rsating.

- a) WinRaR, WinZip
- b) WinDos, WinZip
- c) WinZip, WinXp
- d) NOD 32, MSafee

Birinchi kodlashni qo'llagan inson qaysi qatorda to'g'ri keltirilgan.

- a) Gretsiya sarkardasi Lisandro
- b) Rim imperatori Yuliy Sezar
- c) Nemis matematigi Vilgelm Shikkard
- d) Samuel Morze

Qadimgi Gretsiya sarkardasi Lisandro axborotni maxfiy saqlash, Ya'ni kodlash uchun nimadan foydalangan.

- a) Sisital tayoqchadan
- b) Siyohdan
- c) Gugurt tayoqchadan
- d) Qush patidan

Qadimgi rim imperatori Yuliy Sezar axborotning maxfiyligini saqlash uchunqanday usulini o'ylab topgan.

- a) alifboni surish
- b) notekis kodlash
- c) tekis kodlash
- d) matnni kodlash

Axborotlarni kodlash usullaridan biri Morze kodlash usulida axborot qandaybelgi yordamida kodlanadi.

- a) tire, nuqta, bo'shliq
- b) qo'shtirnoq, tire, nuqta
- c) undov, bo'shliq, vergul
- d) vergul, nuqta, tire

Axborotlarni maxfiy saqlash uchun kodlash ... deb ataladi.

- a) shifrlash
- b) tekis kodlash
- c) notekis kodlash
- d) kodlash

Qadimgi Gretsiya sarkardasi Lisandro axborotni maxfiy saqlash qaysi usuldan foydalangan.

- a) o'rin almashtirish
- b) tekis kodlash
- c) notekis kodlash
- d) alifboni surish

Deshifrlashtirish so'zining ma'nosi nima?

- a) shifrlashtirishga teskari jarayon. Kalit asosida shifrlangan matn o'z holatigao'zgartiriladi.
- b) matn ma'lumotlarini o'zgartirish uchun ikkilik kodi.
- c) bu grafik ma'lumotlarni o'zgartirish uchun sakkizlik kodi.
- d) bu grafik va matnli ma'lumotlarni o'zgartirish uchun sakkizlik kodi

Kalit – bu?

- a) Kalit – matnlarni to'siqlarsiz shifrlash va deshifrlash uchun kerak bo'lganaxborot.
- b) Kalit – matnlarni to'siqlarsiz shifrlash va deshifrlash uchun kerak bo'lganma'lumot.
- c) Kalit – matnlarni to'siqlarsiz shifrlash va deshifrlash uchun kerak bo'lganhujjat.
- d) Kalit – matnlarni to'siqlarsiz shifrlash va deshifrlash uchun kerak bo'lganfayl.

Ochiq kalitli tizimda shifrlash va deshifrlash uchun qanday kalit ishlatiladi?

- a) Ochiq va yopiq
- b) Ochiq
- c) Yopiq
- d) Aralash

Simmetrik kriptotizim uchun qanday usullar qo'llaniladi?

- a) O'rini almashtirish, gammirlash, blokli shifrlash
- b) Monoalfavitli almashtirish, o'rini almashtirish, gammirlash
- c) Ko'palfavitli almashtirish, o'rini almashtirish, gammirlash
- d) O'rini almashtirish, gammirlash, blokli identifikatorlar

Almashtirishlar quyidagilarga ajraladi?

- a) Mono va ko'palfavitli
- b) Monoalfavitli
- c) Ko'palfavitli
- d) To'g'ri javob yo'q

Ma'lumotlarni himoya qilish tushunchasiga?

- a) Ma'lumotlarning to'liqligini saqlash va ma'lumotga kirishini boshqarish kiradi
- b) Faylning to'liqligini saqlash kiradi
- c) Shifrning to'liqligini saqlash kiradi
- d) Kodning to'liqligini saqlash kiradi

Antivirus dasturlarini sinovdan o'tkazish bilan qanday tashkilot shug'ullanadi?

- a) Kompyuter xavfsizligi milliy assotsiatsiyasi NCSA (National ComputerSecurity Association)
- b) Intel, Seleron
- c) Seleron, IBM
- d) IBM, INTEL

Ma'lumotlarni fizik himoyalash ko'proq?

- a) Tashkiliy choralarga qarashlidir
- b) Tashkiliy va notashkiliy choralarga qarashlidir
- c) Notashkiliy choralarga qarashlidir
- d) Huquqiy choralarga qarashlidir

Himoya qilishning asosiy muammolari quyidagilardan iborat?

- a) Axborotga kirishga yo'l qo'ymaslik
- b) Faylga kirishga yo'l qo'ymaslik
- c) Shifrga kirishga yo'l qo'ymaslik
- d) Kodga kirishga yo'l qo'ymaslik

Parollar usuli?

- a) Eng oddiy va arzon, lekin ishonchli himoyani ta'minlaydi
- b) Eng ommaviy va qimmat, lekin ishonchli himoyani ta'minlaydi
- c) Eng ommaviy lekin operatsiyali tizimga kirishni ishonchli himoyani ta'minlaydi
- d) Eng murakkab lekin ishonchli himoyani ta'minlaydi

Uzoq (olis)lashtirilgan masofadan buzish nima?

- a) Xakerlik faoliyati
- b) Xavaskorlik faoliyati
- c) Abonentlik faoliyati
- d) Foydalanuvchi faoliyati

Qaysi tizimlar maqsad yomon niyatli kishilarni aldash uchun psevdoservislar bilan ishlaydi?

- a) Almashtirish tizimi
- b) Registratsion tizim
- c) Xujumlarni ushlash tizimi
- d) Butunligini nazorat qilish tizimlari

Tarmoq darajasida himoyalashning texnik usullari quyidagilarga bo'linadilar?

- a) Apparatli, dasturli, apparatdasturli
- b) Tashkillashtirilgan, tizimli, apparatli
- c) Apparatdasturli, tizimli, dasturli
- d) To'g'ri javob yo'q

Axborotdan manfaatdor bo'lish turlari ko'rsatilsin?

- a) qonuniy, noqonuniy;
- b) rasmiy, noqonuniy;
- c) qonuniy, majburiy;
- d) majburiy, ixtiyoriy;

Ochiq kalit axborot uzatuvchi uchun shaxsiy kalit uni ochish uchun kerak bo'ladigan kriptosistema bu...

- a) assimmetrik;
- b) simmetrik;
- c) odatiy;
- d) nosimmetrik;

Axborotni ochish va undan foydalanishni ta'minlaydigan vosita bu...

- a) kalit;
- b) satr;
- c) raqam;
- d) kriptotizm;

Ikkinchi jahon urushi davrida keng foydalanilgan kriptosistema bu...

- a) Simmetrik kriptosistema;
- b) assimmetrik kriptosistema;
- c) raqamlil kriptosistema;
- d) matnli kriptosistema;

Simmetrik kriptosistemalarning kamchiligi nimadan iborat?

- a) kalit yagonaligi;
- b) kalit ko'pligi;
- c) kalit soddaligi;
- d) kalit murakkabligi;

"Har kim o'zi istagan axborotni izlash, olish va uni tarqatish huquqiga ega..." O'zbekiston Respublikasi Konstitutsiyasi nechanchi moddasida yozilgan.

- a) 29-modda.
- b) 30-modda.
- c) 35-modda.
- d) 1-modda

Axborot xavfsizligi nimaga bog'liq?

- a) qo'llab-quvvatlovchi infratuzilmaga
- b) kompyuterlarga
- c) qo'llab-quvvatlovchi insonlarga
- d) ma'lumotlarga

Axborot xavfsizligining asosiy tarkibiy qismlari:

- a) yaxlitlik, ishonchlilik, maxfiylik
- b) yaxlitlik
- c) ishonchlilik,
- d) maxfiylik

Maxfiylik bu ..

- a) ma'lumotlarga ruxsatsiz kirishdan himoya
- b) yaratilgan dasturiy mahsulotlarni ishlab chiqish
- c) protseduralarning tavsifi
- d) oshkorlik

Tahdid ...

- a) ma'lum bir tarzda axborot xavfsizligini buzish ehtimoli
- b) ma'lumotlarni to'plash va jamoaviy foydalanishga mo'ljallangan dasturiy ta'minot tili tashkiliy-texnik vositalar tizimi
- c) aniqlash jarayoni ushbu bosqich talablariga javob beradigan rivojlanishning hozirgi holatiga javob beradi
- d) qo'rqitish qobiliyati

Hujum bu ...

- a) tahdidni amalga oshirishga urinish
- b) ma'lum bir tarzda axborot xavfsizligini buzish ehtimoli
- c) kerakli dasturlarni topishga mo'ljallangan dasturlar.
- d) qo'rqitish qobilyati

Virus bu ...

- a) boshqa dasturlarga joylashtirish orqali tarqatish qobiliyatiga ega kod
- b) ob'ektning so'rovga uning turiga qarab javob berish qobiliyati.
- c) ma'lum bir vazifani bajarish uchun kichik dastur
- d) Mikroorganizmlar

Axborot xavfsizligi fani qaysi fanlar bilan bog'liq?

- a) Operatsion tizimlar, dasturlash, kompyuter tarmoqlari.
- b) Fizika, Ximya
- c) Biologiya, tarix
- d) Kompyuter grafikasi va dizayn

Axborot xavfsizligi buzilishiga ko'p foiz holatda nima sabab bo'ladi?

- a) Foydalanuvchilarning ehtiyotsizligi yoki xafa bo'lgan xodimlar tomonidan.
- b) Kompyuter viruslari
- c) Hackerlar hujumi
- d) Tarmoq nosozliklari

Eng katta tezlikka ega axborot uzatish tezligiga ega bo'lgan kabel turi qaysi?

- a) Optik kabel
- b) Koaksial kabel
- c) O'ralgan juft simli kabel
- d) RJ-45 tarmoq kabeli

Viruslar asosan qaysi formatlarda bo'ladi

- a) Com, exe, bat
- b) txt, doc, ppt
- c) Psd, scf, js
- d) Dwg, psd

Axborotga murojaat etishning qanday turlari mavjud?

- a) Ruxsat etilgan va ruxsat etimlagan
- b) O'zgartiriladigan va o'zgartirilmaydigan
- c) O'chiriladigan va o'chirilmaydigan?
- d) O'qiladigan va o'qilmaydigan

Steganografiya so'zining lug'aviy ma'nosi nima?

- a) Yashirilgan yozuv
- b) Sirsiz yozuv
- c) So'z
- d) Parol

Steganografiyaning asosiy maqsadi?

- a) Maxfiy xabar mavjudligini yashirish
- b) Shifrlash
- c) Konfedentsiallik
- d) Butunlilik

Kriptoanalizning fundamental qoidasini birinchi qaysi olim keltirgan?

- a) Kerxoffom
- b) Xoffman
- c) Tsezar
- d) Rayndal

Shifrlash talablariga javob beruchi shifrlash algoritmlari guruhining birinchituri qanday nomlanadi?

- a) o‘rin almashtirish
- b) Joylashtirish
- c) Gammalashtirish
- d) shifrlanishi kerak bo‘lgan ma’lumotlarni analitik o‘zgartirish

DES shifrlash algoritmda shifrlash bloki hajmi necha bit?

- a) 64 b) 28 c) 256 d) 32

DES shifrlash algoritmda real ishlatiladigan kalit hajmi necha bit?

- a) 56 b) 28 c) 256 d) 32

DES shifrlash algoritmi asosida nima yotadi?

- a) Feystel to‘ri
- b) Joylashtirish-o‘rin almashtirish
- c) Elliptik egri chiziqlar
- d) Tub sonlar

GOST 2847-89 shifrlash algoritmda shifrlash bloki hajmi necha bit?

- a) 64 b) 28 c) 256 d) 32

GOST 2847-89 shifrlash algoritmda kalit hajmi necha bit?

- a) 256
- b) 32
- c) 64
- d) 28

GOST 2847-89 shifrlash algoritmda raundlar soni nechta?

- a) 32
- b) 48
- c) 8
- d) 6

GOST 2847-89 shifrlash algoritmi asosida nima yotadi?

- a) Feystel to‘ri
- b) Joylashtirish-o‘rin almashtirish
- c) Elliptic egri chiziqlar
- d) Tub sonlar

Identifikatsiya ...

- a) sub‘ektlarga o‘zini kimligini ma’lum qilish imkonini beradi.
- b) ob‘ektlarga o‘zini kimligini ma’lum qilish imkonini beradi.
- c) sub‘ektlarga o‘zini kimligini yashirish imkonini beradi.
- d) ob‘ektlarga o‘zini kimligini yashirish imkonini beradi.

Autentifikatsiya

- a) ikkinchi tomonni aslida kim ekanligini bilish imkonini beradi.
- b) ikkinchi tomonni aslida kim ekanligini yashirish imkonini beradi.
- c) kompyuterga tarmoq orqali kirish imkonini beradi.
- d) kompyuterga aslida kim ishlayotganligini bilish imkonini beradi.

Modem – bu ... uchun mo‘ljallangan qurilma.

- a) axborotni telefon kanallari orqali uzatish
- b) axborotni chop etish
- c) axborotni saqlash
- d) axborotni shu vaqtda qayta ishlash

Qaysi komanda buyruqlar satrida tizimdagi foydalanuvchilar ro'yxatini ko'rastish vazifasini bajaradi.

- a) net user
- b) cmd
- c) open
- d) secpol

CMD buyruqlarida net user foydalanuvchi nomi **/add buyrug'ning vazifasi.**

- a) yangi foydalanuvchi yaratadi
- b) foydalanuvchini o'chiradi
- c) mavjud foydalanuvchiga parol beradi
- d) mavjud foydalanuvchiga nomini o'zgartiradi

CMD buyruqlarida net user foydalanuvchi nomi **/del buyrug'ning vazifasi**

- a) foydalanuvchini o'chiradi
- b) yangi foydalanuvchi yaratadi
- c) mavjud foydalanuvchiga parol beradi
- d) mavjud foydalanuvchiga nomini o'zgartiradi

CMD buyruqlarida Secpol.msc buyrug'ning vazifasi

- a) Parollar siyosati oynasini ochadi
- b) yangi foydalanuvchi yaratadi
- c) mavjud foydalanuvchiga parol beradi
- d) Parollar siyosati oynasini yopadi

Maxfiy xabar mavjudligini yashirish nima deb ataladi?

- a) Steganografiya
- b) Stenografiya
- c) Kriptografiya
- d) Shifrlash

Axborot xavfsizligini ta'minlashning qanday chora-tadbirlari mavjud?

- a) Tashkiliy, huquqiy, texnik
- b) Tashkiliy, huquqiy, iqtisodiy
- c) Tashkiliy, ishtimoiy, iqtisodiy
- d) huquqiy, ommaviy, shaxsiy

Qaysi usulda axborotni saqlash va uzatishning o'zini dalili yashiringan?

- a) Steganografiya
- b) Shifrlash
- c) Kodlash
- d) Dekodlash

Qaysi usulda axborot hajmi kamayadi?

- a) Zichlashtirish
- b) Steganografiya
- c) Shifrlash
- d) Kodlash

XESH funksiyaning asosiy maqsadi nima?

- a) Axborot butunligini tekshirish
- b) Axborot ishonchliligini tekshirish
- c) Axborot konfidensialligini tekshirish
- d) Axborot mavjudligi tekshirish

GLOSSARIY

Ajratilgan xonaning akustik himoyasi – ovozning to'siq konstruksiyasiga to'g'ridan – to'g'ri o'tishi yo'li bilan nutqiy maxfiy yoki konfidensial xabarni ajratilgan xona tashqarisiga sirqib chiqishini oldini olish bo'yicha rejalashtirilgan tashkiliy-texnik tadbirlarni amalga oshirish jarayoni.

Akkreditatsiya (sertifikatsiya organining akkreditatsiyasi) – tashkilotning ma'lum (so'ralgan) sohada sertifikatsiya buyicha muayyan ishlarni bajarishga kompetentligini (qodirligini) vakolatli (nufuzli) organ tomonidan rasman tan olinishi.

Aktiv – 1. Himoyalovchi axborot yoki resurslar. 2. Tashkilot uchun qimmatli barcha narsalar. 3. Bosh ilova, umumiy madadlovchi tizim, yuqori nufuzli dastur, moddiy qism, kritik tizim missiyasi, xodimlar, jihozlar yoki mantiqiy bog'langan tizimlari guruhi.

Akustik axborot – eltuvchisi akustik signallar bo'lgan axborot.

Anonimlik – ishtirokchiga (protokol ishtirokchisiga) qandaydir harakatni anonim tarzda, ya'ni o'zini identifikatsiyalamasdan, bajarilishini ifodalaydi. Bunda, lekin, ishtirokchi ushbu harakatni bajarishga haqli ekanligini isbotlashi lozim. Anonimlik absolyut va chaqiriluvchi bo'lishi mumkin.

Antibot – robot-dasturlarni, ayg'oqchi dasturlarni (Spyware), ruxsatsiz o'rnatilgan reklama dasturiy ta'minotni (Adware) va boshqa zarar keltiruvchi dasturiy ta'minot turlarini avtomatik tarzda aniqlovchi va yo'q qiluvchi dasturiy ta'minot.

Antispufing – qonuniy identifikatsiya va autentifikatsiya ma'lumotlaridan ruxsat etilmagan foydalanishga qarshi qabul qilinuvchi choralar.

Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo'q qiluvchi dastur. Agar virus yo'q qilinmasa, zaharlangan dastur yo'q qilinadi. Yana – viruslardan himoyalashga, zararlangan dasturiy modullar va tizimli makonlarni aniqlashga, hamda zararlangan obyektlarning dastlabki holatini tiklashga mo'ljallangan dastur.

AT xavfsizlik arxitekturasi – xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.

Audit jurnali – tizim harakatlarining xronologik yozuvi. Berilgan muddatda bajariluvchi tizimli foydalanishlar va amallar yozuvlarini o'z ichiga oladi.

Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.

Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikatsiyasini tekshirish; saqlanuvchi va uzatuvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Avariya vaziyati – masalalar yechilishining to'xtalishiga sabab bo'luvchi hisoblash tizimining buzilishi.

Avtomatlashtirilgan axborot tizimi – ma'lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo'ljallangan dasturiy va apparat vositalar majmui.

Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma'lum foydalanish huquqlarini taqdim etish.

Axborot egasi – axborot resurslariga, axborot mulkdori bilan shartnoma asosida egalik qilish, ulardan foydalanish va ularni idora qilish huquqiga ega axborot munosabatlarining subyekti.

Axborot kafolati – axborot va axborot tizimlarining foydalanuvchanligini, yaxlitligini, autentifikatsiyalanishini, konfidensialligini va rad etmasligini ta'minlash orqali himoyalash va qo'riqlash choralari.

Axborot urushi – dushmanning axborotiga, axborotga asoslangan jarayonlariga va axborot tizimlariga zarar yetkazish, bir vaqtning o'zida tegishli axborotni, axborotga va axborot tizimlariga asoslangan jarayonlarni himoyalash

yo'li bilan axborot ustunligiga erishish uchun zarur choralarini ko'rish harakatlari.

Axborot xavfsizligi – axborot egasiga yoki foydalanuvchiga va madadlovchi infrastrukturaga ziyon keltiruvchi tabiiy yoki sun'iy xarakterli, tasodifiy yoki atayin qilingan ta'sirlardan axborotning va madadlovchi infrastrukturaning himoyalanganligi.

Axborot xavfsizligi - axborot holati bo'lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz uning olinishiga yo'l qo'yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalaniş darajasi holati.

Axborot xavfsizligi arxitektori - tashkilotning asosiy missiyasini himoyalash uchun kerakli axborot xavfsizligi talablari va etalon modelni, segment va yechimlar arxitekturasini o'z ichiga olgan barcha tashkilot arxitektura jihatlarida adekvat adreslangan biznes - jarayonlar va bu missiya va biznes jarayonlarni madadlovchi axborot tizimlarini ta'minlashga javobgar bo'lgan jismoniy shaxs, guruh yoki tashkilot.

Axborot xavfsizligi doktrinasi - axborot xavfsizligini ta'minlash maqsadlariga, masalalariga, prinsiplariga va asosiy yo'nalishlariga rasmiy qarashlar majmui.

Axborotdan foydalanish – shtatga oid texnik vositalardan foydalanib axborot bilan tanishish, uni xujjatlash, nusxalash, modifikatsiyalash yoki axborotni yo'q qilish jarayoni.

Axborotni texnik himoyalash - himoyalashga loyiq axborotning (ma'lumotlarning) xavfsizligini xarakatdagi qonunlarga muvofiq, texnik, dasturiy va dasturiy - texnik vositalarni ishlatib, nokriptografik usullar yordamida ta'minlashdan iborat axborot himoyasi.

Axborotni fizik (bevosita) himoyalash - himoya obyektiga vakolatsiz shaxslarning suqilib kirishlariga yoki undan foydalanishlariga to'siqlar yaratuvchi

tashkiliy tadbirlar yoki vositalar majmuini ishlatish yo'li bilan axborotni himoyalash.

Axborotni himoyalash konsepsiyasi – axborotni himoyalash bo'yicha qarashlar va umumiy texnik talablar tizimi. Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.

Axborotni huquqiy himoyalash – axborotni himoyalash bo'yicha subyektlar munosabatini rostlovchi qonuniy va me'yoriy xujjatlarni (aktlarni) ishlab chiqishni, hamda ularning bajarilishini nazorat qilishni o'z ichiga oluvchi axborotni xuquqiy usullar yordamida himoyalash.

Axborotni ishlovchi himoyalangan texnik vosita – himoyalash vositalari va usullari ishlab chiqish va tayyorlash bosqichida amalga oshirilgan axborotni ishlovchi texnik vosita.

Axborotning buzilishi – tashqi ta'sirlar (halallar), apparatura ishlashidagi buzilishlar, yoki xizmatchi xodimning bilimsizligi natijasida texnik vositalarida ishlanuvchi axborotning tasodifiy ruxsatsiz modifikatsiyalanishi.

Bot - oddiy foydalanuvchi interfeysi orqali avtomatik tarzda va/yoki berilgan jadval bo'yicha qandaydir harakatlarni bajaruvchi maxsus dastur. Kompyuter dasturlari muhokama qilinganida bot atamasi asosan Internetga qo'llash bilan ishlatiladi.

Botnet - ishga tushirilgan botlarga ega bir qancha sonli xostlardan tashkil topgan kompyuter tarmog'i. Odatda kompyuterlarga bo'ladigan tarmoq xujumlarini (spamni tarqatish, foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash, masofadagi tizimda parollarni saralash, xizmat qilishdan voz kechishga undash hujumlari va x.) koordinatsiyalash uchun ishlatiladi (inglizcha robot va network so'zlaridan olingan.).

Buferning to'lib-toshishi hujumi – buferdagi oldindan aniqlangan hajmdagi makonni qaytadan yuklash usuli bo'lib, xotiradagi ma'lumotlarni qayta yozishi va shikastlashi mumkin.

Buzilmaslik – tizimning unga yuklatilgan vazifalarni berilgan sharoitda, istalgan vaqt onida bajarish qobiliyati.

Davlat sirlaridan foydalanish - fuqarolarning davlat siridan iborat ma'lumotlardan foydalanish huquqini, korxonalar, idoralar va tashkilotlarni esa bunday ma'lumotlardan foydalanib ish yuritish huquqini rasmiylashtirish muolajasi.

Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritmi.

Dezinformatsiya – foydalanuvchi shaxslarga yolg'on tasavvurni shakllantirish maqsadida ularga uzatiluvchi xabarni atayin buzib ko'rsatish; yolg'on axborotni uzatish.

Faol hujum - dushman va/yoki buzg'unchi qonuniy foydalanuvchi harakatigata'sir etishi, masalan, qonuniy foydalanuvchi xabarini almashtirishi yoki yo'q qilishi va xabarni yaratib uning nomidan uzatishi va h. mumkin bo'lgan kriptotizimga yoki kriptografik protokolga hujum.

Faol tahdid – tizim holatini atayin ruxsatsiz o'zgartirish tahdidi. Firibgarlik hujumi - foydalanuvchilarning yoki dasturlarning ma'lumotlarni soxtalashtirish va noqonuniy afzallikka ega bo'lish yo'li bilan boshqa subyektlar sifatida muvaffaqiyatli niqoblanish vaziyati.

Foydalanish nazorati – foydalanuvchilarning, dasturlarning yoki jarayonlarning hisoblash tizimlari qurilmalaridan, dasturlaridan va ma'lumotlaridan foydalanishlarini aniqlash va cheklash.

Foydalanishni diskretion boshqarish – mavzu alomati bo'yicha obyektдан foydalanish konsepsiyasi (modeli). Unga binoan vakolatlarining ma'lum darajasiga ega foydalanish subyekti o'z xuquqini ixtiyoriy boshqa subyektga berishi mumkin.

Foydaluvchanlik - avtorizatsiyalangan mantiqiy obyekt so'rovi bo'yicha mantiqiy obyektning tayyorlik va foydaluvchanlik holatida bo'lishi xususiyati.

Himoya ma'muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz

foydalanishdan himoyalashga javobgar foydalanish subyekti.

Himoyaning faol texnik vositasi – texnik razvedka vositalariga yoki ushbu vositalarning me'yorida ishlashini, buzuvchi, niqoblovchi yoki imitatsiyalovchi faol halallar yaratilishini ta'minlovchi himoyaning texnik vositasi.

Hujum – bosqinchining operatsion muhitini boshqarishiga imkon beruvchi axborot tizimi xavfsizligining buzilishi.

Hujumni aniqlash va ogohlantirish – qaror qabul qiluvchiga maqbul javobni amalga oshirish uchun bildirish orqali ataylab qilingan ruxsat etilmagan harakatlarning aniqlanishi, korrelyatsiyasi, identifikatsiyalanishi va tavsiflanishi.

Identifikator – subyekt yoki obyektning farqlanuvchi alomatidan iborat foydalanishning identifikatsiya vositasi. Foydalanuvchilar uchun asosiy identifikatsiya vositasi parol hisoblanadi.

Identifikatsiya ma'lumotlari - tizimda muayyan qatnashchini bir ma'noli identifikatsiyalashga imkon beruvchi, unga tegishli noyob identifikatsiya ma'lumotlari majmui.

Ijtimoiy injeneriya – xizmatchi xodimlar va foydalanuvchilar bilan, turli nayrang, aldash va h. orqali chalg'itish asosidagi muloqotdan olinadigan axborot yordamida axborot tizimining xavfsizlik tizimini chetlab o'tish.

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Imzo verifikatsiyasi - ma'lumotlardagi raqamli imzoni tekshirish uchun raqamli imzo algoritmi va ochiq kalitdan foydalanish.

Insayder – guruxga tegishli yashirin axborotdan foydalanish xuquqiga ega guruh a'zosi. Odatda, axborot sirqib chiqishi bilan bog'liq insidentda muhim shaxs hisoblanadi. Shu nuqtai nazaridan, insayderlarning quyidagi xillari farqlanadi: beparvolar, manipulyatsiyalanuvchilar, ranjiganlar, noxolislari, qo'shimcha pul ishlovchilar va h.

Insident – ruxsatsiz foydalanish xuquqiga ega bo'lishga yoki kompyuter

tizimiga hujum o'tkazishga urinishning qayd etilgan holi.

Internet-firibgarlik – kredit-moliya sohasidagi —yuqori-texnologiyali“ jinoyatchilik xili bo'lib, uyushgan va, odatda, xalqaro xarakterga ega. Jinoiy strukturalar tomonidan noqonuniy daromadlar olish maqsadida foydalanishni blokirovka qilish hujumi yoki bot-tarmoqlarni yaratish kabi zamonaviy texnologiyalar ishlatiladi.

Jamiyat axborot xavfsizligi —shaxs axborot xavfsizligi” kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo'llaniladi.

Kalit – fayldagi yozuvlarni identifikatsiyalash va undan tezda foydalanish uchun ishlatiladigan belgilar majmui; yana - qandaydir axborotdan foydalanish vakolatini tasdiqlash uchun ishlatiladigan kod; yana - asosida shifrlash amalga oshiriluvchi qiymat; yana - ma'lumotlar elementlari naboridagi identifikator.

Kalit uzunligi (o'lchovi) - kalitni ifodalovchi ma'lum alfavitdagi so'z uzunligi. Ikkili kalit uzunligi bitlarda o'lchanadi.

Keylogger - klaviaturali kiritishni ushlab qolishga mo'ljallangan dastur yoki apparat vosita. Bosilgan klavishlar skan-kodlarini aniqlashni va ularni yashirincha saqlashni va/yoki yashirincha qandaydir kanal orqali uzatishni amalga oshiradi.

Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o'z ichiga oladi.

Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo'luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.

Kiberfazo – Internet, telekommunikatsiya tarmoqlari, kompyuter tizimlari va o'rnatilgan prosessorlar va kontrollerlarni o'z ichiga olgan, o'zaro bog'langan axborot tizimlari infrastrukturalar tarmog'idan tashkil topgan axborot muhitidagi global domen.

Kiber-hujum – hisoblash muhiti/ infrastrukturasi, o'chirish, buzish yoki g'arazli nazoratlash yoki ma'lumot yaxlitligini buzish yoki nazoratlanuvchi axborotni o'g'irlash maqsadida kiberfazodan foydalanuvchi tashkilotga atalgan

kiberfazo orqali amalga oshiriluvchi hujum.

Kiberjinoyatchilik - g'arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o'g'irlashga yoki buzishga yo'naltirilgan alohida shaxslarning yoki guruhlarining harakatlari.

Kiberterrorizm - insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug'diruvchi kompyuter tizimlarini izdan chiqarish bo'yicha harakatlar.

Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo'riqlash yoki himoyalash imkoniyati.

Koder (dasturchi) - internet-firibgarlik texnologiyalari bilan shug'ullanuvchi uyushgan jinoiy guruh ichidagi ixtisosliklardan biri; troyan va boshqa zarar yetkazuvchi dasturlarni yozuvchi va ularni yopiq anjumanlarda —o'ziga o'xshashlarga” sotuvchi ishtirokchini belgilaydi.

Kodlash- axborotga ishlov berish uchun qulay ko'rinish(shalilga) o'tkazish tushuniladi.

Kodlar kitobi – tarkibida tartibga solingan ochiq matn va kodlar ekvivalenti yoki so'zlarni almashtirish texnologiyasidan foydalanuvchi mashina shifrlash usuli bo'lgan hujjat.

Kodlar lug'ati – kod tizimida kod ekvivalenti berilgan ochiq matn so'zlari, raqamlari, iboralari yoki gaplar nabori.

Kompyuter xavfsizligi – axborot tizimlari aktivlarining, jumladan apparat vositalarining, dasturiy ta'minotning, o'rnatilgan mikrodasturiy vositaning va ishlanuvchi, saqlanuvchi va uzatiluvchi axborotning konfidensialligini, yaxlitligini va foydalanuvchanligini kafolatlovchi choralar va nazoratlash vositalari.

Konfidensial axborot – egasi tomonidan himoyalashni talab etuvchi tijoriy yoki shaxsiy sirdan iborat axborot.

Kriptografik algoritim – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritim.

Lug'atga asoslangan hujum – ochiq matn elementlari lug'atidan

foydalanishga asoslangan kriptotizimga hujum.

Ma'lumotlar – odam ishtiroki bilan yoki avtomatik tarzda uzatishga, izohlashga yoki ishlashga yaroqli, formallashgan ko'rinishda ifodalangan axborot.

Ma'lumotlarni tiklash – eltuvchining asl nusxasida ma'lumotlar yaxlitligi buzilganida unga ma'lumotlarning himoya nusxasi bo'lgan eltuvchidan nusxalash jarayoni.

Ma'muriy xavfsizlik choralari – tanlashni, ishlab chiqishni, tatbiq etishni, sog'liqni saqlashga oid elektron axborotni himoyalash bo'yicha xavfsizlik choralari madadlash va ushbu axborotni himoyalashga nisbatan tashkilot xodimlarini boshqarish bo'yicha ma'muriy harakatlar, siyosatlar va muolajalar.

Mantiqiy bomba – “qurbon” kompyuterida rezident joylashgan va ma'lum mantiqiy shart bo'yicha, masalan, ma'lum sanada yoki tizimning ma'lum xolatlari naborida, faollashuvchi destruktiv dasturiy komplekslarni umumlashtiruvchi atama.

Mualliflik huquqi – fan, adabiyot va san'at asarlarini yaratish va foydalanish bilan bog'liq vujudga keladigan munosabatlarni tartibga soluvchi huquqiy normalar majmui.

Nuqson - axborot tizimidagi topshiriq, adashish yoki etiborsizlik asosidagi xato bo'lib, himoya mexanizmlarini aylanib o'tishga imkon beradi.

Ochiq axborot – barcha manfaatdor shaxslarning foydalanishlari bo'yicha cheklash bo'lmagan axborot: umumfoydalanuvchi axborot.

Ochiq kalit - odatda imzoni tekshirish yoki ma'lumotni shifrlashda foydalaniluvchi asimmetrik kalit juftining ochiq qismi.

Parol yordamida himoyalash – foydalanish uchun parol kiritilishi zarur bo'lgan ma'lumotlarni himoyalash usuli.

Parollarni fosh qiluvchi - parollarni saralash yoki o'g'rilashni amalga oshiruvchi kompyuter dasturi.

Parolni buzib ochish - axborot tizimidan (tarmog'idan) yashirincha foydalanish texnikasi (usuli) bo'lib, unda hujum qiluvchi taraf parollarni fosh

qiluvchi yordamida parollarni aniqlashga (tanlashga) yoki o'g'irlashga urinib ko'radi.

Passiv hujum – kriptotizimga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta'sir etmaydi.

Raqamli axborot – kompyuter tizimlarida ishlashga, saqlashga va almashishga mo'ljallangan ma'lumotlar ko'rinishida ifodalangan axborot.

Raqamli imzo algoritmi - ma'lumotlarni raqamli imzolash uchun foydalaniluvchi asimmetrik algoritmi.

Raqamli imzoni shakllantirish algoritmi – raqamli imzo sxemasining tarkibiy qismi. Kirish yo'liga imzolovchi xabar, maxfiy kalit, hamda raqamli imzo sxemasining ochiq parametrlari beriluvchi algoritmi (umuman randomizatsiyalangan algoritmi). Algoritmi ishining natijasi raqamli imzo hisoblanadi. Raqamli imzo sxemasining ba'zi turlarida imzoni shakllantirishda protokol ishlatiladi.

Risk matritsasi - rutbalash va oqibatlariga va imkoniyatlariga rutbalar berish yo'li bilan riskni ifodalash instrumenti.

Risk menejmenti — axborot-telekommunikatsiya texnologiya resurslariga ta'sir etishi mumkin bo'lgan xavfli xodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to'liq jarayoni.

Riskni nazoratlash - riskni modifikatsiyalovchi (o'zgartiruvchi) chora. 1-izoh. Riskni nazoratlash o'z ichiga har qanday jarayonni, siyosatni, usulni, amaliyotni va riskni modifikatsiyalovchi boshqa harakatlarni olishi mumkin. 2-izoh. Riskni nazoratlash doimo istalgan va kutilgan effektini bermasligi mumkin.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A. Shamir va L. Adleman tomonidan taklif etilgan va asimmetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

Shaxsiy axborot – tarqalishi faqat mos shaxslar yoki tashkilotlar ruxsati bilan mumkin bo'lgan mamlakat fuqarolari yoki tashkilotlari manfaatlariga daxldor

axborot.

Shifrlash-Kriptografik uslublardan (shifratma va dastlabki matnga o'girish, elektron raqamli imzoni shakllantirish va tekshirish, xesh-funksiya shakllantirish va tekshirish) foydalanishga asoslangan axborotni o'zgartirish jarayoni. Axborotni shifrlash uni begonalar tomonidan o'rganish yoki o'zgartirish imkoniyatini yo'qqa chiqaradi. Shuningdek, ma'lumotlarga va dasturlarga, ulardan noqonuniy foydalanish maqsadida, ruxsatsiz raqamli imzo tizimiga kirishning oldini olishni ta'minlaydi.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritmi. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

Tahdid turlari - tahdidlarni tasodifiy va atayinlariga, aktiv va passivlariga tasniflash mumkin.

Tarmoq xavfsizligi - axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy ishlashiga tasodifiy yoki atayin aralashishdan yoki tarmoq komponentlarini buzishga urinishdan ehtiyot qiluvchi choralar. Asbob-uskunalarni, dasturiy ta'minotni, ma'lumotlarni himoyalashni o'z ichiga oladi.

Tarmoqlararo ekran - apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to'sig'i hisoblanadi.

Tizim ma'muri - tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta'minlashga javobgar shaxs.

Tizim xavfsizligi - tizim resurslaridan va funksional imkoniyatlaridan ruxsatsiz foydalanishdan hamda ishlashida turli bashorat qilinadigan yoki qilinmaydigan holatlar sabab bo'luvchi, bo'lishi mumkin bo'lgan buzilishlardan tizimning himoyalaniishi.

Virus - boshqa dasturlar bajarilayotganida o'zini ularga kirituvchi unchalik katta bo'lmagan dastur; yana - nusxalarini beixtiyor yaratish va keyinchalik yangi nusxasini nazoratlash va qayta yaratishga erishish maqsadida fayllardagi va tizimli sohalardagi boshqa dasturlarni modifikatsiyalash imkoniyatiga ega dastur.

Virusga qarshi himoya - hisoblash texnikasi va avtomatlashtirilgan tizim vositalarini dasturiy virus ta'siridan himoyalashni ta'minlashda ishlatiluvchi tashkiliy, xuquqiy, texnik va texnologik choralar kompleksi.

Xabar haqiqiyliги kodi - bir-biriga ishonuvchi ishtirokchilar tomonidan xabarlarini autentifikatsiyalash protokollarida xabarga qo'shiladigan va uning yaxlitligini va ma'lumotlar manbaining autentifikatsiyasini ta'minlashga mo'ljallangan simvollarning maxsus nabori.

Xatoliklar jurnali - tizim tomonidan adashishlar xususidagi axborot yoziladigan fayl.

Xavfsiz o'chirish - qattiq diskni qayta yozish uchun dasturiy - apparat vositalari asosidagi jarayonlardan foydalanib qayta yozish texnologiyasi.

Xavfsiz operatsion tizim - ma'lumotlar va resurslar mazmuniga mos himoyalash darajasini ta'minlash maqsadida apparat va dasturiy vositalarni samarali boshqaruvchi operatsion tizim.

Xavfsizlik - ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma'lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan

300 shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko'rib chiqilishi va modifikatsiyalanishi mumkin bo'lmagan holat.

Xavfsizlik atributi - baholanish obyektining xavfsizlik siyosatini amalga oshirishda ishlatiluvchi subyektlar, foydalanuvchilar va/yoki obyektlar bilan bog'lik axborot.

Xavfsizlik auditi - kompyuter tizimi xavfsizligiga ta'sir etuvchi bo'lishi mumkin bo'lgan xavfli harakatlarni xarakterlovchi, oldindan aniqlangan hodisalar

to'plamini ro'yxatga olish (audit faylida qaydlash) yo'li bilan himoyalaniшни nazoratlash.

Xavfsizlik xizmati ma'muri – xavfsizlikni ta'minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs (yoki shaxslar guruhi).

Xavfsizlikni aktiv testlash – nishon bilan to'g'ridan – to'g'ri o'zaro aloqaga mo'ljallangan xavfsizlikni testlash, masalan, talab qilingan nishongacha paketni yuborish.

Xavfsizlikning avtomatlashtirilgan domeni - asboblari, texnologiyalar guruhini hamda ma'lumotlarni o'z ichiga olgan axborot xavfsizligi sohasi.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritmi. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritmi. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

Xodim xavfsizligi – qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta'minlovchi usul.

Yolg'on axborot – xarakteristikalar va alomatlarini noto'g'ri akslantiriluvchi hamda real mavjud bo'lmagan obyekt xususidagi axborot.

Zombi - tizimda o'rnatilgan, boshqa tizimlarga hujum qilishga majbur qiluvchi dastur.

Axborot xavfsizligi asoslari fanidan nazorat savollari:

1. Axborot va ma'lumot tushunchalari.
2. "Axborot xavfsizligi" tarifi.
3. "Axborotni himoyalash" tarifi.
4. O'z.R konstitutsiyasining qaysi moddalari axborot haqida?
5. Axborotga qanday tahdidlar mavjud.
6. Axborotning konfidentsiallikga tahdid nima?
7. Axborotning ishonchliligiga tahdid nima?
8. Axborotning butunlililigiga tahdid nima?
9. Axborotning ruxsat etilganliligiga tahdid nima?
10. Axborot xavfsizligining buzilishga sabablarni ayting.
11. "Axborotga xavfsizligiga tahdid" tarifi.
12. Axborotga xavfsizligiga tahdid turlari.
13. Axborotga tabiiy xarakterdagi tahdidlar.
14. Axborotga suniy xarakterdagi tahdidlar.
15. Kiberxavfsizlik, kiberjinoyatchilik, kiberfiribgarlik tushunchalari.
16. Kiberjinoyatchilikning turli ko'rinishlari qaysilar?
17. Kiberterrorizmning ommalashishiga sabab nima?
18. ATlarning rivojlanishiga salbiy ta'sir qiluvchi omillar.
19. AKTga oid O'z.Rsining qonunlari.
20. Axborot xavfsizligini siyosatida axborotni himoyalashda qanday choralar ko'riladi?
21. Axborotni kodlash nima?
22. Ochiq kodlash va yopiq kodlash tushunchalari.
23. Tekis va noteks kodlash tushunchalari.
24. ISCI kodlash tizimi.
25. Binar (2 lik) kodlash.
26. Shifrlash tushunchasi.
27. Deshifrlash tushunchasi.

28. Kriptografiya tushunchasi va tarixi.
29. Kriptologiya, kriptanaliz tushunchalari.
30. Kriptografiyaning rivojlanish davrlari.
31. O'miga qo'yish shifrlash usuli.
32. O'rin almashtirish shifrlash usuli.
33. Kalit tushunchasi.
34. Kriptografiya himoyasida shifrlarga nisbatan qanday talablar qo'yiladi:
35. Sezar shifrlash algoritmi.
36. Jadval usulida shifrlash algoritmi.
37. Vijnier shifrlash algoritmi.
38. Simmetrik shifrlash algoritmlari.
39. XOR amali(modul 2 orqali qo'shish).
40. Bir martalik blaknot shifrlash algoritmi.
41. DES, AES va ГОСТ simmetrik s shifrlash tizimlari.
42. Asimmetrik yoki ochiq kalitli shifrlash algoritmlari.
43. RSA va El-Gamal asimmetrik shifrlash tizimlari.
44. Steganografiya tushunchasi va tarixi.
45. Steganografiya turkumlanishi.
46. Xesh funksiya tarifi va qo'llanilishi.
47. Xesh funksiya qanday xususiyatlarga ega?
48. Elektron raqamli imzo.
49. ERI to'g'risidagi qoninning mazmuni.
50. Identifikatsiya tushunchasi va qo'llanilishi
51. Autentifikatsiya tushunchasi va qo'llanilishi
52. Avtorizatsiya tushunchasi va qo'llanilishi
53. Parollarga asoslangan autentifikatsiya avzalliklari va kamchiliklari.
54. Biometrik xususiyatlarga asoslangan autentifikatsiya avzalliklari va kamchiliklari.
55. Elektron tijorat tushunchasi.

56. Elektron tijorat xavfsizligi.
57. Xavfli saytlarni aniqlash dasturlari.
58. Axborotni himoyalashning huquqiy, tashkiliy va texnik choralari.
59. Kompyuter tarmog'i
60. Tarmoq xavfsizligi tushunchasi
61. Lokal, mintaqaviy va global tarmoq tushunchalari.
62. Tarmoq topologiyalari.
63. Tarmoq qurilmalari.
64. Tarmoq kabellari
65. Tarmoq manzillari.
66. OSI modeli.
67. Tarmoq protakollari.
68. Tarmoq xavfsizligining asosiy maqsadlari
69. Domen tushunchasi.
70. Hosting tushunchasi.

AXBOROT XAVFSIZLIGI

O'quv qo'llanma

Muharrir:
Tehnik muharrir:
Musahhih:
Sahifalovchi:

X. Taxiroy
S. Melikuziva
M. Yunusova
G. Samigova

Nashriyot litsenziya № 2044, 25.08.2020 й

Bichimi 60x84¹/₁₆ "Cambria" garniturası, kegli 16.

Offset bosma usulida bosildi. Shartli bosma tabog'i 10,5. Adadi 100 dona.

Buyurtma № 3224526

City of book MCHJda chop etildi.

Tel.raqam: +998 94 673 66 56
+998 97 017 01 01

ISBN 978-9910-780-02-8

