O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM FAN VA INNOVATSIYALAR VAZIRLIGI

GULISTON DAVLAT UNIVERSITETI

«Axborot texnologiyalari» kafedrasi

60610200-Axborot tizimlari va texnologiyalari bakalavriat ta’lim yo‘nalish bo‘yicha ta’lim olayotgan talabalar uchun

«AXBOROT XAVFSIZLIGI »

fanidan mashg‘ulotlarini bo‘yicha

U S L U B I Y K O‘ R S A T M A

GULISTON – 2024

UO'K 004.056(075.8)

32.811.4ya73

Axborot xavfsizligi fanidan uslubiy ko‘rsatma A.A.Taniberdiyev Guliston: GulDU, 2024.-16 b.

Ushbu uslubiy ko‘rsatma Guliston davlat universiteti 60610200-Axborot tizimlari va texnologiyalari bakalavriat ta’lim yo‘nalish bakalavriat ta’lim yo‘nalishi talabalari uchun mo‘ljallangan bo‘lib, “Axborot xavfsizligi” fanidan laboratoriya ishlarining tavsiyalari keltirilgan. Har bir laboratoriya ishi bo‘yicha nazariy qism, bajariladigan ishning mohiyati, maqsadi va vazifalari, komputerning tashkil etuvchilari, tizimli va amaliy dasturli ta’minot, amaliy dasturlardan foydalanish, grafik dasturlardan foydalanish vazifalar maqsad qilib qo‘yilgan.

Uslubiy ko‘rsatma universitetning 60610200-Axborot tizimlari va texnologiyalari bakalavriat ta’lim yo‘nalishi talabalari uchun uslubiy ko‘rsatma sifatida tavsiya qilingan.

Taqrizchilar: Abdurahimov D.B. – Axborot texnologiyalari kafedrasi dotsenti

Niyozov M.B – Pedagogika fanlari nomzodi, dotsent. (Phd).

Ushbu uslubiy ko‘rsatma Guliston davlat universiteti Axborot texnologiyalari va Fizika-matematika fakulteti “Axborot texnologiyalari” kafedrasining 20___-yil __- _____dagi __-sonli yigilishida muhokama qilingan.

Ushbu uslubiy ko‘rsatma Guliston davlat universiteti Axborot texnologiyalari va Fizika-matematika fakulteti ilmiy Kengashining 20___-yil_____dagi __-sonli yig‘ilishda muhokama qilingan va universitet o‘quv-uslubiy Kengashiga tavsiya etilgan.

Ushbu uslubiy ko‘rsatma Guliston davlat universiteti o‘quv-uslubiy Kengashi 20__-yil _____dagi___-sonli qarori bilan nashrga tavsiya etilgan.

.

SO‘Z BOSHI

Axborot kommunikatsiya texnologiyalari sohasi qanchalik rivoj topgani sari, uning afzalligi va qulayliklaridan foydalanish bilan bir qatorda, butun mamlakatimizda axborot xavfsizligini ta‘minlash eng dolzarb masalaga aylanib bormoqda, Ushbu soha albatta rivojlanishi kerak va buni qilamiz...

SH.M.Mirziyoyev

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, konfedensial ma‘lumotlarga ruxsatsiz 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 zararning 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.

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-tadbirlar qanday 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 aktuallligi bo„lib, uni yo„q qilinishidan va ruxsat etilmagan o„zgartirishlardan himoyalanganliligidir. 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.

Kriptografiya
Shifirlash
Kodlash
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) shifirlash
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‘rniga 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-yilda shu 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 bu rchagidan 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. boot viruslari fayl viruslari tarmoq viruslari 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 koʻrsating.

a) WinRaR, WinZip
b) WinDos, WinZip
c) WinZip, WinXp
d) NOD 32, MSAfee

Birinchi kodlashni qoʻllagan inson qaysi qatorda toʻgʻri 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, Yaʻni kodlash uchun nimadan foydalangan.

a) Sisital tayoqchadan
b) Siyohdan
c) Gugurt tayoqchadan
d) Qush patidan

Qadimgi rim imperatori Yuliy Sezar axborotning maxfiyligini saqlash uchun qanday usulini o'ylab topgan.

a) alifboni surish
b) notekis kodlash
c) tekis kodlash
d) matnni kodlash

Axborotlarni kodlash usullaridan biri Morze kodlash usulida axborot qanday belgi yordamida kodlanadi.

a) tire, nuqta, boʻshliq
b) qoʻshtirnoq, tire, nuqta
c) undov, boʻshliq, 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 holatiga o‘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‗lgan axborot.
b) Kalit – matnlarni to‗siqlarsiz shifrlash va deshifrlash uchun kerak bo‗lgan ma‘lumot.
c) Kalit – matnlarni to‗siqlarsiz shifrlash va deshifrlash uchun kerak bo‗lgan hujjat.
d) Kalit – matnlarni to‗siqlarsiz shifrlash va deshifrlash uchun kerak bo‗lgan fayl.

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‗rnini almashtirish, gammirlash, blokli shifrlash
b) Monoalfavitli almashtirish, o‗rnini almashtirish, gammirlash
c) Ko‗palfavitli almashtirish, o‗rnini almashtirish, gammirlash

d) O‗rnini 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 Computer Security 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 himoyalanishning 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) oshkoralik

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 qobilyati

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) Hakerlar 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 birinchi turi qanday nomlanadi?

a) o‘rin almashtirish
b) Joylashtirish
c) Gammalashtirish
d) shifrlanishi kerak bo‘lgan ma`lumotlarni analitik o‘zgartirish

DES shifrlash algoritmida shifrlash bloki hajmi necha bit?

a) 64
b) 28
c) 256
d) 32

DES shifrlash algoritmida 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 algoritmida shifrlash bloki hajmi necha bit?

a) 64
b) 28
c) 256
d) 32

GOST 2847-89 shifrlash algoritmida kalit hajmi necha bit?

a) 256
b) 32
c) 64
d) 28

GOST 2847-89 shifrlash algoritmida 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 foydalanuvchinomi **/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 foydalanuvchinomi **/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‟milashning 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 butunliligini tekshirish
b) Axborot ishonchliligini tekshirish
c) Axborot konfidensialigini tekshirish

d) Axborot mavjudligi tekshirish

GLOSSARIY

Ajratilgan xonaning akustik himoyasi – ovozning to‘siq konstruktsiyaorqali to‘g‘ridan – to‘g‘ri o‘tishi yo‘li bilan nutqiy maxfiy yoki konfidentsialaxborotni ajratilgan xona tashqarisiga sirqib chiqishini oldini olish bo‘yicharejalashtirilgan 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. Himoyalanuvchi axborot yoki resurslar. 2. Tashkilot uchun qiymatli 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, zaxarlangan dasturiy modullar va tizimli makonlarni aniqlashga, hamda zaxarlangan 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 identifikasiyasini 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 choralarni 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 himoyalanish 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 jixatlarida 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 algoritm.

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 harakatiga ta‘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 diskretsion boshqarish – mavzu alomati bo‘yicha obyektdan foydalanish konsepsiyasi (modeli). Unga binoan vakolatlarning 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 foydalanuvchanlik 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, noxolislar, 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/ infrastrukturasini, 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 guruhlarning 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‘tkazisish 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 algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.

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 choralarini 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 asimetrik 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 – kriptotizmga 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 asimetrik algoritm.

Raqamli imzoni shakllantirish algoritmi – raqamli imzo sxemasining tarkibiy qismi. Kirish yo‘liga imzolanuvchi xabar, maxfiy kalit, hamda raqamli imzo sxemasining ochiq parametrlari beriluvchi algoritm (umuman randomizatsiyalangan algoritm). Algoritm 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. 1izoh. Riskni nazoratlash o‘z ichiga har qanday jarayonni, siyosatni, usulni, amaliyotni va riskni modifikasiyalovchi boshqa harakatlarni olishi mumkin. 2izoh. Riskni nazoratlash doimo istalgan va kutilgan effektni bermasligi mumkin.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik 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 (shifrmatnga 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 algoritm. 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 himoyalanishi.

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 haqiqiyligi kodi - bir-biriga ishonuvchi ishtirokchilar tomonidan xabarlarni 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 - aparat 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 himoyalanishni 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 - asboblar, texnologiyalar guruhini hamda ma‘lumotlarni o‘z ichiga olgan axborot xavfsizligi sohasi.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o‘zgartiruvchi algoritm. 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 – xarakteristikalari va alomatlari 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 tushunchalri.
2. ―Axborot xavsizligi‖ tarifi.
3. ―Axborotni himoyalash‖ tarifi.
4. O‘z.R konistitutsiyasining qaysi moddalari axborot haqida?

5. Axborotga qanday tahdidlar mavjud.
6. Axborotning konfedensiallikga tahdid nima?
7. Axborotning ishonchliligiga tahdid nima?
8. Axborotning butunlililigiga tahdid nima?
9. Axborotning ruxsat etilganliligiga tahdid nima?
10. Axborot xavsizligining buzilishga sabablarni ayting.
11. ―Axborotga xavfsizligiga tahdid‖ tarifi.
12. Axborotga xavfsizligiga tahdid turlari.
13. Axborotga tabiiy xarakterdagi tahdidlar.
14. Axborotga suniy xarakterdagi tahdidlar.
15. Kiberxavsizlik, kiberjinoyatchlik, kiberfiribgarlik tushunchalari.
16. Kiberjinoyatchlikning turli ko‘rinishlari qaysilar?
17. Kiberterorizimning ommalashishiga sabab nima?
18. ATlaring rivojlanishiga salbiy ta‘sir qilivchi 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. ISCII kodlash tizimi.
25. Binar (2 lik) kodlash.
26. Shifrlash tushunchasi.
27. Deshifrlash tushunchasi.
28. Kiriptografiya tushunchasi va tarixi.
29. Kriptologiya, kriptoanaliz tushunchalari.
30. Kiriptografiyaning rivojlanish davrlari.
31. O‗rniga 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. Vijiner 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. RSAva El-Gamal asimmetrik shifrlash tizimlari.
44. Steganografiya tushunchasi va tarixi.
45. Steganografiya turkumlanishi.
46. Xesh funksiya tarifi va qo‘lanilishi.
47. Xesh funksiya qanday xususiyatlarga ega?
48. Elektron raqamli imzo.
49. ERI to‘g‘risidagi qoninning mazmuni.
50. Identifikatsia 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.

ADABIYOTLAR

1. Mirziyoev Sh.M. Erkin va farovon, demokratik O‗zbekiston davlatini birgalikda barpo etamiz. O‗zbekiston Respublikasi Prezidenti lavozimiga kirishish tantanapi marosimiga bag‗ishlangan Oliy Majlis palatalarining qo‗shma majlisidagi nutk, Toshkent, 2016.566.
2. Mirziyoev Sh.M. Tanqidiy tahlil, qatiy tartib-intizom va shaxsiy javobgarlik - har bir rahbar faoliyatining kundalik qoidasi bo‗lishi kerak. Mamlakatimizni 2016 yilda ijtimoiy-iktisodiy rivojlantirishning asosiy yakunlari va 2017 yilga muljallangan iktisodiy dasturning eng muxim ustuvor yunalishlariga bagishlangan

Vazirlar Maxkamasining kengaytirilganmajlisidagi ma‘ruza, 2017 yil 14 yanvarToshkent, Uzbekiston, 2017. 104-6.

3. Mirziyoev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta‘minlash- yurt taraqqiyoti va xalk farovonligining garovi. Uzbekiston Respublikasi Konstitutsiyasi kabul kilinganining 24 yilligiga bagishlangan tantanapi marosimdagi ma‘ruza. 2016 yil 7 dekabr- Toshkent, Uzbekiston, 2017. 48-6.
4. Mirziyoev Sh.M. Buyuk kelajagimizni mard va olijanob xalkimiz bilan birga quramiz. Mazkur kitobdan O‗zbekiston Respublikasi Prezidenti Shavkat Mirziyoevning 2016 yil 1 noyabrdan 24 noyabrga qadar Qoraqalpog‗iston

Respublikasi, viloyatlar va Toshkent shaxri saylovchilari vakillari bilan o‗tkazilgan saylovoldi uchrashuvlarida so‗zlagan nutklari o‗rin olgan.- Toshkent, O‗zbekiston, 2017. 488-6.

5. Seymour Bosworth, Michel Ye. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.
6. Shon Harris. ALL IN ONE CISSP. McGraw-Hill 2013.
7. G‗aniev S. K., Karimov M. M., Tashev K. A. ―Axborot xavfsizligi‖. Aloqachi. 2008.
8. Makarenko S. I., Informatsionnaya bezopasnost. Uchebnoe posobie. Stavropol, 2009.
9. Michael Ye. Whitman. Herbert J. Mattord. Principles of Information Security, Fourth Edition. Course Technology, Cengage Learning. 2012.

Internet saytlari

1. www.intuit.ru
2. www.sec.ru
3. http7/opensecuritvtraining.info/

TANIBERDIYEV AKBARJON ABDUGANIYEVICH

Axborot xavfsizligi

fanidan bo‘yicha

USLUBIY KO‘RSATMA

120100, Guliston sh. 4-mavze, GulDU, Asosiy bino, 2-qavat. tel: (67) 225-41-76