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

TOSHKENT VILOYATI KASBIY TA’LIMNI RIVOJLANTIRISH VA MUVOFIQLASHTIRISH

BOSHQARMASI

Oqqo’rg’on tumani 1-son kasb hunar maktabi

“TASDIQLAYMAN”

Oqqo’rg’on tuman 1-son

kasb-hunar maktabi direktori: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ S.Vohidov

“\_\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021 yil

# **AXBORAT XAVFSIZLIGI MAXSUS FANIDAN** Tayyorlov yo’nalishi: 0.52.01.00 Informatika va axborot texnologiyalari ( tarmoqlar va sohalar bo’yicha) Kasb: 3.52.01.03. – Kompyuter grafikasi va dizayn operatori.

# Pedagogik kengashining 2021- yildagi 30 avgustdagi 1- sonli yig’ilishida o’quv jarayoniga qo’llashga tavsiya etildi. O’qitish materiallari to’plamini kafedrasining 2021- yildagi 1-sonli yig’ilishida muhokama etildi va ma’qullandi.

# Kafedra mudiri: Boymatova P O’qituvchi: Yo’ldosheva D

**TO’PLAMNING MUALLIFI TO’GRISIDA MA’LUMOT**

|  |
| --- |
|  |

O’qituvchining FISH: Dildora Yo’ldosheva Po’lat qizi Ma’lumoti: To’liqsiz tugallanmagan oliy Mutaxassisligi: Matematika va informatika

Pedagogik ish staji: 1-yil

Ish joyi: Oqqo’rg’on tuman 1-son kasb-hunar maktabi Elektron pochta manzili: [yoldosheva.dildora@mail.ru](mailto:yoldosheva.dildora@mail.ru)

Telefon raqami +99899-403-45-23

O’QITISH MATERIALLARI TO’PLAMI TARKIBI:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № |  | To’plam tarkibi |  | Shakli |
| 1 |  | Taqvim-mavzular rejasi |  | Jadval |
| 2 |  | Fanning ta’lim texnologiyasi |  | Nusxa (PDF) |
| 3 |  | Mavzular to’plami |  | Yozma+(CD Word) |
| 4 |  | Baholash vositalari |  | Matn, jadval |
| 5 |  | Vizual-didaktik resurslar |  |  |

.

|  |  |  |
| --- | --- | --- |
|  |  |  |

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

TOSHKENT VILOYATI KASBIY TA’LIMNI RIVOJLANTIRISH VA MUVOFIQLASHTIRISH

BOSHQARMASI

OQQO’RG’ON TUMAN

1-SON KASB-HUNAR MAKTABI

“TASDIQLAYMAN”

Oqqo’rg’on tuman kasb-hunar maktabi direktori: *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*S.Vohidov

“\_\_\_\_”\_\_\_\_\_\_\_\_\_\_2021 yil

AXBOROT XAVSIZLIGI MAXSUS FANIDAN

### **ISHCHI DASTURI**

Ishchi dastur Pedagogik innovatsiyalar, kasb-hunar ta’limi boshqaruv hamda pedagog kadrlarni qayta tayyorlash va ularning malakasini oshirish institute tomonidan ishlab chiqilgan O’zbekiston Respublikasi Oliy va o’rta maxsus ta’lim vazirligi huzuridagi Oliy va o’rta maxsus, kasb-hunar ta’limi yo’nalishlari boyicha o’quv-uslubiy birlashmalar faoliyatini Muofiqlashtiruvchi kengashning 2021-yil 28-avgustdagi 5-son yig’ilishida ma’qullangan va Vazirlikning 2021-yil 28-avgustdagi 375- son buyrug’I bilan tasdiqlangan va joriy etilgan “Kompyuter grafikasi va dizayn operatori” kasbining malaka talablari asosida hamda fanning namunaviy o'quv dasturi asosida ishlab chiqildi.

### 0.52.01.00-Informatika va axborot texnologiyalari( tarmoqlar va sohalar bo’yicha ) 3.52.01.03-Kompyuter grafikasi va diazayn operatori 1.Kompyuter grafikasi va diazyn operatori

#### Oqqo’rg’on tumani 1-son kasb hunar maktabi tomonidan kvalifikatsiyalar bo‘yicha ishlab chiqilgan 2021yil 30 avgustda tasdiqlangan ishchi o‘quv rejasida Kasbga kirish fani (moduli)ga jami 60 soat ajratilgan.

#### Tuzuvchi (lar): D.Yo’ldosheva Oqqo’rg’on tumani 1-son kasb

#### hunar maktabi maxsus fan o’qtuvchisi

#### 

#### Taqrizchi (lar): P.Boymatova Oqqo’rg’on tumani 1-son kasb hunar maktabi

#### kafedra mudiri

#### 

#### O.Berdiyor Oqqo’rg’on tumani 1-son kasb hunar

#### maktabi bo’lim mudiri

#### 

#### 

#### 

#### 

#### Oqqo’rg’on tumani 1-son kasb hunar maktabining 2021 yil 30 avgustdagi Pedagogik kengashida muhokama qilindi, mazkur ishchi o‘quv dasturini tasdiqlashga va o‘quv jarayoniga tadbiq etishga qaror qilindi. Bayonnoma № 1

Oqqo’rg’on tuman xokimligining kasbiy ta’limni rivojlantirish v amuvofiqlashtirish hududiy boshqarmasi direktori tamonidan 2021 yil 28 avgustdagi 5-son tasdiqlangan namunaviy o'quv rejada “Axborot xavfsizligi ” faniga ajratilgan soatlar miqdori:

O'quvchining umumiy o'quv yuklamasi soat, shu jumladan mashg'ulot turlari bo'yicha ajratilgan soatlar:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Mashg'ulot turlari | Ajratilgan  soat | Shu jumladan semestrlar bo'yicha | | | |
|  |  |  |  |
| I | II | III | IV |
| 1 | Auditoriya jami yuklamasi | 120 | 30 | 30 | 30 | 30 |
| 2 | Nazariy mashg'ulot | 30 |  |  |  |  |
| 3 | Amaliy mashg'ulot | 30 |  |  |  |  |
| 4 | Seminar |  |  |  |  |  |
| 5 | Laboratoriya  mashg'uloti |  |  |  |  |  |
| 6 | Kurs ishi (loyihasi) |  |  |  |  |  |
| 7 | Yakka tartibli mashg'ulot |  |  |  |  |  |
| 8 | O'quvchining mustaqil ishi | 42 | 7 | 7 | 14 | 14 |

Tuzuvchilar: D.Yo’ldosheva Oqqo’rg’on tuman kasb-hunar maktabi Maxsus fan o’qtuvchisi

Taqrizchi: O.Berdiyorov Oqqo’rg’on tuman kasb-hunar maktabi o’quv bo’lmi mudiri

-

“Axborot xavsizligi ” faning ishchi o'quv dasturi va ekspert guruhining xulosasi

ta'lim muassasasining 2021 yil 30 avgustdagi Pedogogik kengashida

muhokama qilindi, tasdiqlashga va o'quv jarayoniga tadbiq etishga qaror qilindi. Bayonnoma №

MUNDARIJA;

1. Tushintirish xati.
2. O‘quv fani (moduli)ning maqsad va vazifalari, o‘zlashtirish natijasi;
3. O‘quv fani (moduli)ning mashg‘ulot turlari bo‘yicha mavzular rejasi va mazmuni;
4. Laboratoriya ishlari mavzulari;
5. O‘quv fani (moduli)ning moddiy-texnik ta'minoti;
6. Fan (modul) ning o‘zlashtirish darajasini nazorati va baholash;
7. Tavsiya etilgan adabiyotlar va saytlar ro‘yxati.

TUShUNTIRISh XATI

Mazkurishchi dastur Pedagogik innovatsiyalar, kasb-hunar ta’limi boshqaruv hamda pedagog kadrlarni qayta tayyorlash va ularning malakasini oshirish institute tomonidan ishlab chiqilgan O’zbekiston Respublikasi Oliy va o’rta maxsus ta’lim vazirligi huzuridagi Oliy va o’rta maxsus, kasb-hunar ta’limi yo’nalishlari boyicha o’quv-uslubiy birlashmalar faoliyatini Muofiqlashtiruvchi kengashning 2021-yil 28-avgustdagi 5-son yig’ilishida ma’qullangan va Vazirlikning 2021-yil 30-avgustdagi 375-son buyrug’i bilan tasdiqlangan va joriy etilgan “Kompyuter grafikasi va dizayn operatori” kasbining malaka talablari asosida hamda fanning na’munaviy o'quv dasturi asosida ishlab chiqildi.

Kompyuter grafikasi dizayn operatori kasbining malaka talablarida berilgan maxsus fanlar turkumiga kiruvchi ushbu "Axborot xavsizligi" fanining "Bilimlar" va "Ko'nikmalar" bandida keltirib o'tilgan bilim va ko'nikmalarning talablarining katta qismi kompyuter grafikasining Axborot xavsizligi bo'limiga tegishli bo'lib (qariyb 80-85 %), ushbu yo'nalish uchun alohida "Axborat xavsizligi" fani ham o'qitiladi. Malaka talablarida keltirilgan asosiy bilim va ko'nikmalarga qo'yilgan talablar esa vektorli grafikaga tegishli.

Shularni hisobga olgan holda ishchi dasturni ishlab chiqishda malaka talablarida ko'rsatilgan bilim va ko'nikmalarning katta qismi Pedagogik innovatsiyalar, kasb-hunar ta'limi boshqaruv hamda pedagog kadrlarning qayta tayyorlash va

ularning malakasini oshirish instituti O'quv uslubiy

birlashmasining 2021yil 20 avgustdagi 3-sonli majlis bayoni

bilan ma'qullangan hamda institutining metodik kengashining 2021 yil 28 avgustdagi

5-sonli majlis bayoni bilan ma'qullangan hamda

O'zbekiston Respublikasi Oliy va o'rta maxsus, kasb-hunar ta'limi yo'nalishlari bo'yicha o'quv-uslubiy birlashmalar faoliyatini Muvofiqlashtiruvchi

Kengashining 2021 yil 30 avgustdagi 375-sonli majlis bayoni

bilan ma'qullangan hamda Oliy va o'rta maxsus ta'lim vazirligining 2021 yil

30 avgustdag 375-sonli buyrug'i bilan tasdiqlangan na'munaviy o'quv

dasturi asosida tayyorlandi

.

# Kirish Mazkur ishchi dastur 0.52.01.00-Informatika axborot texnologiyalari (tarmoqlar va sohalar bo’yicha) yo‘nalishida ta’lim oluvchi o‘quvchilarda mutaxassislikka oid turli xil vazifalarni bajara olish qobiliyatini o‘stirish va shakllantirishga qaratilgan.

# Kasbga kirish fani o‘quvchilarni 0.52.01.00-Informatika axborot texnologiyalari (tarmoqlar va sohalar bo’yicha) yo’nalishida keng miqiyosda bilimga ega bo‘lishda mustaqil fikrlay olishga o‘rgatadi.

# Ta’lim jarayonida o‘qitish ishlari zamon talabiga mos ravishda kompyuterlar yordamida dasturlash asoslariga oid yozilgan kompakt-disklardan, so‘nmas internet tarmog‘ining Informatika va AT faniga oid ma’lumotlaridan, yangi texnologiyalar na’munalari berilgan video filmlar, slayda va albomlar kabi ko‘rgazmali qurollarni namoyish qilish asosida olib boriladi.

# Kasbga kirish fani o‘quv rejasidagi dars soatlaridan 60 soat dars soati 25 soat nazariy va 35 soat amaliy darslarga bo‘linib, Pedagogik innovatsiyalar, kasb-hunar ta’limi boshqaruv hamda pedagog kadrlarni qayta tayyorlash va ularning malakasini oshirish institute tomonidan ishlab chiqilgan O’zbekiston Respublikasi Oliy va o’rta maxsus ta’lim vazirligi huzuridagi Oliy va o’rta maxsus, kasb-hunar ta’limi yo’nalishlari boyicha o’quv-uslubiy birlashmalar faoliyatini Muofiqlashtiruvchi kengashning 2021-yil 28 avgustdagi 5-son yig’ilishida ma’qullangan va Vazirlikning 2020-yil 14-avgustdagi 419-son buyrug’i bilan tasdiqlangan va joriy etilgan “Kompyuter grafikasi va dizayn operatori” kasbining malaka talablari asosida kasb- hunar maktablarida 0.52.01.00-Informatika axborot texnologiyalari (tarmoqlar va sohalar bo’yicha) tayyorlov yo’nalishlari uchun ishlab chiqildi.

# Malaka talablari bo‘yicha mavzular 2 soatlik dars mashg’ulotlari uchun mo’ljallab tayyorlandi.

# 

# MUNDARIJA

# O‘quv fani (moduli)ning maqsad va vazifalari, o‘zlashtirish natijasi;

# O‘quv fani (moduli)ning mashg‘ulot turlari bo‘yicha mavzular rejasi va

# mazmuni;

# O‘quv fani(moduli)ning moddiy-texnik ta’minoti;

# Fan (modul)ning o‘zlashtirish darajasini nazorati va baholash; 5.Tavsiya etilgan adabiyotlar va saytlar ro‘yxati.

### O’QUV FANNING MAQSADI VA VAZIFALARI

***Fanning maqsadi:*** 30.52.01.00-Informatika axborot texnologiyalari (tarmoqlar va sohalar bo’yicha) yo‘nalishida ta’lim oluvchi o‘quvchilarda mutaxassislikka oid turli xil kompyuter dasturlari va ular bilan ishlash, vazifalarni bajara olish qobiliyatini o‘stirish va shakllantirishga qaratilgan

***Fanning vazifasi:*** Kasbga kirish fani o‘quvchilarni Kompyuter grafikasi va dizayn operatori mutaxassisligi bo’yicha keng miqiyosda bilimga ega bo‘lishda mustaqil fikrlay olishga o‘rgatadi. Ularda kompyuter grafikasi, grafik dizayn, grafik

### axborotlarni tasvirlash va kompyuter grafikasi dasturlari bilan ishlash ko'nikmasini shakllantiriladi.

### FANNING KVALIFIKATSION XARAKTERISTIKASI

#### O‘quvchilar fanni o‘qib tugatgandan so‘ng quyidagi bilimlarga ega bo‘lishlari zarur:

#### Dasturga kirish;

#### Grafik axborotlarni tasvirlash asoslari. Kompyuter grafikasi turlari;

#### Power Point dasturi interfeysini o‘rnatish va taqdimotlarni yaratish bosqichlari;

#### Corel Draw dasturi, interfeysi va unda ishlash asoslari

#### Fanni o‘qish jarayonida quyidagi ko‘nikmalarga ega bo‘lishlari zarur:

#### Adobe Photoshop dasturi interfeysi va ishlash asoslari;

#### Macromedia Flash dastur interfeysi va uning ishchi muhitini sozlash;

#### Uch o‘lchamli grafika tushunchasi, turlari, ishlatish sohalari, Macromedia Flash, 3DS Max) dasturlari bilan ishlash.

#### FANNI O‘QITISHDA ZAMONAVIY AXBOROT VA PEDAGOGIK TEXNOLOGIYALARI BO‘YICHA TAVSIYALAR

#### Pedagogik texnologiya turlarini tanlash shakllantirilishi ko‘zda tutilgan bilim, ish harakati usullari, shaxsiy fazilatlar, mashg‘ulotlarning tashkiliy shakli, qo‘llanilayotgan metodlar, vositalar va shu kabi ko‘plab omillarga bog‘liq. Kasbga doir turli ko‘rgazma, ko‘rik – tanlovlarda o‘quvchilarning ishtirokini muntazaam ravishda tashkillashtirib borish, bu o‘quvchilarda ijodkorlik hamda badiiy saviyani o‘stirishda qo‘l keladi.

#### Zamonaviy ta’lim texnologiyalari o‘quvchilarni egallayotgan bilim, ish – harakat usullari va shaxsiy fazilatlarini izlab topishga mustaqil o‘rganishg, o‘z fikrlarini bayon etishga imkon beradi. Bu jarayonda o‘qituvchi – o‘quvchining shaxsining shakllanishi, rivojlanishiga sharoit yaratib, boshqaruvchilik, yo‘naltiruvchilik funksiyalarini bajaradi.

#### Dars davomida klaster (tarmoq), boshqaruv; talaba, o‘qituvchi shaxsi treningi; aqliy hujum, kichik guruhlarda ishlash, ko‘rgazmali davra suhbati, bahs – munozara, muamolli vaziyat va boshqa metodlaridan keng foydalaniladi.

*Ta’lim jarayonida ilg‘or pedagogik uslub va texnologiyalari, axborot telekommunikatsiya texnologiyalari, elektron ta’lim resurslari va multimedia taqdimotlaridan foydalanish tavsiya etiladi*

O‘qitish metodlari.

Ushbu fanni o‘qitish jarayonida kuyidagi metodlardan foydalanish tavsiya etiladi:

1. ogzaki so‘rov - tushuntirish, ma'ruza, o‘kuv muhokamasi, o‘kuvchilar bilan ishlash;
2. ko‘rsatish metodi - ko‘llanmalarni ko‘rsatish, plakatlar, rasmlar, modellar, maketlar, filmlarni namoyish etish;

v) amaliy usul - rejalash, loyiha va tadqiqot ishlari bo‘yicha dasturlash masalalari va boshqa metodlar; muammoli, evristik, klaster, aqliy hujum, 3x4 metodi. (o‘qituvchi tomonidan aniqlanadi).

g) ma'ruza, amaliy mashg‘ulot, va qo‘shimcha adabiyotlar, ta'limning zamonaviy metodlari, zamonaviy pedagogik va axborot - kommunikatsiya tenxnologiyalaridan qo‘llaniladi

O‘qitishning texnik vositalari.

“Axborot xavfsizligi ” fanidan amaliy mashgulotlar kuyidagi vositalar bilan jihozlangan laboratoriyalarda o‘tish tavsiya etiladi:

1. Internetga ulangan shaxsiy kompyuterlarda.
2. Proektor
3. LCD proektor
4. Proektor uchun ekran
5. Matnli vizual - vositalar
6. Maxsus adabiyotlar
7. Videofilmlar
8. Texnik vositalar
9. Doska
10. Kompyuter
11. Proektor
12. Skaner, rangli printer
13. Informatika fanidan multimedia to‘plami;

Baholash tizimi.

O‘quvchilarning bilimi, ko‘nikma va malakalarini baholash Oliy va o‘rta maxsus ta'lim vazirligi, O‘rta maxsus, kasb-hunar ta'limi markazi tomonidan tasdiqlangan “Akademik litsey va kasb-hunar kollejlari o‘quvchilarining bilimi, ko‘nikma va malakalarini nazorat qilishning reyting tizimi to‘g‘risida” gi Nizom asosida amalga oshiriladi. O‘quvchilarni olayotgan bilim, malaka va ko‘nikmalari ballar asosida doimiy baholab boriladi. Yakuniy baholashdan oldin oraliq nazoratlar o‘tkazilib, tor doiradagi ko‘rgazmalar tashkil qilinadi. Semestr oxirlarida esa ushbu fanning malakali o‘qituvchilari va maxsus fan o‘qituvchilari tomonidan tuzilgan komissiya a'zolari ko‘rgazmada qatnashayotgan o‘quvlarni bajargan ishlariga qarab baholab chiqadilar.

Joriy baholash me’zonlari A’lo bahoga:

* bajargan ishining nazariy va amaliy ahamiyatini, maqsadi va vazifasini atroflicha tushungan bo‘lsa;
* vazifani mustaqil ijodiy yondashib bajara olsa;
* chizgan xaritalarining mazmunini tushunsa, to‘g‘ri bayon qilib bersa;
* voqyea-hodisalar tafsilotlarini, chegaralarini buzmay to‘g‘ri tasvirlasa;
* geografik ob'ektlaming nomlarini kartografik qonunlarga amal qilib to‘liq yozgan bo‘lsa;
* xaritada tasvirlangan tafsilotlarni ilmiy va mantikiy ketma-ketlikda to‘liq tavsiflab bersa

rofillar, grafiklar, jadvallar va boshqa chizmalarni to‘g‘ri chizgan va voqyea- hodisalarni o‘zgarib borish, rivojlanish qonuniyatlarini ilmiy va mantiqiy to‘g‘ri talqin etsa;

* ishni belgilangan muddatda va puxta tayyorlab topshirsa.

Yaxshi bahoga:

* bajargan ishining nazariy va amaliy ahamiyatini, maqsadi va vazifasini tushungan bo‘lsa;
* vazifani mustaqil bajara olsa;
* chizgan xaritalarining mazmunini tushunsa, to‘g‘ri bayon qilib bersa;
* voqyea-hodisalar tafsilotlarini, chegaralarini buzmay to‘g‘ri tasvirlasa;
* geografik ob'ektlarning nomlarini kartografik qonunlarga amal kilib, lekin to‘liq yozmagan bo‘lsa;
* xaritada tasvirlangan tafsitotlarni ilmiy va mantiqiy ketma-ketlikda tavsiflashda biroz xatoga yo‘l qo‘ysa;
* profillar, grafiklar, jadvallar va boshqa chizmalarni to‘g‘ri chizgan va voqyea- hodisalarni o‘zgarib borish, rivojlanish qonuniyatlarini talqin etishda ayrim kamchiliklarga yo‘l qo‘ysa;
* ishni belgilangan muddatda topshirsa.

O‘rta bahoga:

* bajargan ishining nazariy va amaliy ahamiyatini, maqsadi va vazifasi haqida umumiy tasavvurga ega bo‘lsa;
* vazifani mustaqil bajara olmay, ayrim yordamga muhtoj bo‘lsa;
* xaritalarni mazmunan to‘g‘ri chizgan va tushungan, ammo bayonida qiynalsa;
* voqyea-hodisalar tafsilotlarini, chegaralarini buzib tasvirlasa;
* geografik ob'ektlarning nomlarini to‘liq yozmagan bo‘lsa;
* xaritada tasvirlangan tafsilotlarni bayon kilishda ilmiy va mantiqiy chalkashliklarga yo‘l qo‘ysa;
* profillar, grafiklar, jadvallar va boshqa chizmalarni deyarli to‘g‘ri chizgan, ammo talqin etishda chalkashliklarga yo‘l qo‘ysa;
* ishda ayrim kamchiliklar bo‘lsa va belgilangan muddatda topshirilmasa.

Qoniqarsiz bahoga:

* ishni bajarmagan yoki nazariy va amaliy ahamiyatini tushunmagan bo‘lsa;
* vazifani mustaqil bajara olmasa;
* xaritalarning mazmunini xato tasvirlagan va tavsiflab berolmasa;
* geografik ob'ektlarning nomi to‘lik emas va kartografik qonunlarga amal qilib yozilmagan bo‘lsa;
* profillar, grafiklar, jadvallar va boshqa chizmalarni chizishda qo‘pol xatolarga yo‘l qo‘ygan va tavsiflab berolmasa yoki chizmagan bo‘lsa.
* hisobotni chala va o‘z vaqtida topshirmasa yoki umuman topshirmasa.

Oraliq va yakuniy baholash mezonlari A’lo bahoga:

* savolga atroflicha aniq va to‘g‘ri javob yozilgan bo‘lsa;
* o‘quv dasturidan tashqari zamonaviy ma'lumotlardan xabardorligi bilinib tursa;
* qonuniyatlar, nazariya va gipotezalar, tushuncha va terminlar to‘g‘ri va aniq yozilgan bo‘lsa;
* ilmiy xatoliklarga yo‘l qo‘yilmay javob mazmunining ilmiy va mantiqiyligi saqlangan holda puxta yozilgan bo‘lsa;
* orfografik va grammatik xatoliklar uchramasa.

Yaxshi bahoga:

* savolga to‘g‘ri javob yozilgan bo‘lsa;
* savolga yozilgan javob o‘quv dasturi talablari bilan cheklangan, ammo juz'iy kamchiliklari bo‘lsa;
* javoblarda ilmiylik buzilmagan, mantiqiylik saqlangan bo‘lsa;
* qonuniyatlar, nazariya va gipotezalar, tushuncha va terminlar to‘g‘ri yozilgan bo‘lsa;
* orfografik va grammatik xatoliklar uchrasa;
* ba'zi fikrlarda ayrim kamchiliklar uchrasa.

O‘rta bahoga:

* savolga javobning uchdan ikki qismi to‘g‘ri yozilgan bo‘lsa;
* javoblar to‘liq emas, lekin ba'zi bir xatoliklarni inobatga olmaganda umuman to‘g‘ri;
* ilmiy va mantiqiy chalkashliklar uchrasa;
* qonuniyatlar, nazariya va gipotezalar, tushuncha va terminlarda ba'zi bir noaniqliklarga yo‘l qo‘yilgan bo‘lsa;
* orfografik va grammatik xatoliklar bo‘lsa.

Qoniqarsiz bahoga:

* savolga javobning uchdan bir qismi to‘g‘ri yoki umuman yozilmagan bo‘lsa;
* javob noto‘g‘ri bo‘lsa;
* javobda noaniqlik, mantiqiy va ilmiy xatoliklar bo‘lsa;
* orfografik va grammatik xatoliklar ko‘p bo‘lsa;

## O‘quv dasturi umumiy talablari

|  |  |
| --- | --- |
| **Dastur nomi** | Axborot xavfsizligi |
| **Ajratilgan soat** | 80 |
| **O‘qituvchining mashg‘ulotida qatnashib**  **o‘zlashtirilishi**  **lozim bo‘lgan mavzular soni** | 6 |
| **Dasturning maqsadi** | Axborot xavfsizligini ta’minlash bilan bog‘liq masalalarni yechishda axborot - kommunikatsiya tizimlarida axborotlarni himoyalash texnologiyalarining o‘rni va istiqbolli yo‘nalishlari profiliga mos bilim, ko‘nikma va malakani ta’lim standartida  talab qilingan bilimlarni shakllantirish. |
| **O‘zlashtirish natijalari** | 1. Axborot xavfsizligi tushunchasi, uni qo‘llanish sohasi hamda axborot xavfsizligini ta’minlash chora tadbirlari, usullari va vositalarini tahlil qilib ular asosida axborotni himoyalash qobiliyatlarini egallash; 2. Axborot - kommunikatsion tizimlarni samarali himoyalash usul va vositalarini qo‘llay bilish. |
| **Bilimlar** | * davlatning axborot xavfsizligini ta’minlashning maqsadlari, vazifalari, prinsiplari va asosiy yo‘nalishlari to‘g‘risida; * axborotlarni himoyalashning asosiy yo‘nalishlari; * axborotni kriptografik himoyalash usullari; * identifikatsiya va autentifikatsiya; * elektron biznes va elektron biznes muhofaza qilish masalalari; * ma’lumotlarni uzatish tarmoqlarida axborotlarni himoyalash. * mualliflik huquqi orqali axborotni himoya qilishning huquqiy asoslari; |
| **Ko‘nikmalar** | * davlatning axborot infratuzilmasini tahlil qilish qobiliyati; * kompyuter va kompyuter tarmoqlari uchun dasturiy va apparat himoyasini o‘rnatish va sozlash; * axborotni himoya qilishning kriptografik usullaridan foydalanish qobiliyati; * identifikatsiya va autentifikatsiya; * e-biznes va e-biznes muhofaza qilish masalalari; * elektron raqamli imzo va undan foydalanish huquqi; * mualliflik huquqi va tijorat sirlaridan foydalangan holda axborotni himoya qilishni farqlash qobiliyati; * ma’lumotlarni uzatish tarmoqlarida axborotlarni himoyalash; |
| **O‘quv rejasiga muvofiq bog‘liq bo‘lgan boshqa o‘quv**  **fanning nomi** | axborot texnologiyalari asoslari |
| **O‘qitishni tashkiliy shakli** | N – Nazariy ta’lim; A – Amaliy ta’lim;  NA – Nazariy va amaliy ta’lim birgalikda tashkil etiladi; MX – Maxsus xonada o‘tkaziladigan mashg‘ulot. |
| **Dasturga qo‘yilgan talab** | Majburiy |
| **O‘qitish tili** | Guruhda belgilangan o‘qitish tili asosida |
| **Baholash tartibi** | Baholash bo‘yicha amaldagi tartib asosida |
| **O‘quvchilarning bilim va**  **ko‘nikmalarini baholash** | Yozma, og‘zaki, savol-javob, test, amaliy topshiriq |

**O‘quv dasturi mazmuni**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Mavzular nomi | Mavzuning qisqacha mazmuni | Jami | O‘qitishning tashkiliy shakli | Mustaqil ta’lim |
| 1. | Axborot xavfsizligi konsepsiyasi | Axborotning qimmatliligi. Axborot xavfsizligining konseptual modeli. Kompyuter viruslari va virusdan himoyalanish. Virusdan himoyalanish  tizimini yaratish. | 12 | N | 4 |
| 2. | Axborotlarni  himoyalashning asosiy yo‘nalishlari | Axborotni huquqiy muhofaza qilish. Tashkiliy axborot himoyasi. | 12 | N, A | 4 |
| 3. | Axborotlarni kriptografik himoyalash usullari | Axborotni himoyalashning texnik tizimlari. Simmetrik va asimmetrik shifrlash tizimlari. Elektron raqamli imzo. Xodimlarning maxfiy  ma’lumotlarga kirishlarini ro‘yxatga olish | 18 | N | 6 |
| 4. | Identifikatsiya va autentifikatsiya | Foydalanuvchi identifikatsiyasi va autentifikatsiyasi. Parollar va sertifikatlar asosida autentifikatsiya  qilish. Axborotlarni himoyalash metodologiyasi | 12 | N,A | 4 |
| 5. | Elektron tijorat uni himoyalash  muammolari | E-biznes va tijorat modellari.  E-biznes tizimini himoya qilish muammolari. | 18 | N,A | 6 |
| 6. | Ma’lumotlarni uzatish tarmoqlarida ma’lumotlarni  himoyalash | Tarmoqlararo ekranlashtirilgan texnologiya. Xususiy xavfsiz virtual tarmoqlar VPN tarmog‘i. Simsiz  tarmoqlarda axborotlarni himoyalash. | 8 | N,A | 4 |
| Jami | |  | 80 | 40/40 | 28 |

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

TOSHKENT VILOYATI KASBIY TA’LIMNI RIVOJLANTIRISH VA MUVOFIQLASHTIRISH

BOSHQARMASI

OQQO’RG’ON TUMAN

1-SON KASB-HUNAR MAKTABI

“TASDIQLAYMAN”

Oqqo’rg’on tuman 1-son

kasb-hunar maktabi direktori:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_S.Vohidov

“\_\_\_\_\_”\_\_\_\_\_\_\_\_\_\_2021 yil

AXBOROT XAVSIZLIGI MAXSUS FANIDAN

TAQVIMIY-MAVZULAR REJASI

0.52.01.00-Informatika va axborot texnologiyalari( tarmoqlar va sohalar bo’yicha ) 3.52.01.03-Kompyuter grafikasi va diazayn operatori 1.Kompyuter grafikasi va diazyn operatori

Pedagogik kengashining 2021 yildagi 30 avgust 1- sonli yig’ilishida o’quv

jarayoniga qo’llashga tavsiya etildi.

O’qitish materiallari to’plamini kafedrasining 2021 - yildagi 1-sonli

yig’ilishida muhokama etildi va ma’qullandi.

Kafedra mudiri: Boymatova .P

O’qituvchi: Yo’ldosheva. D

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Mavzular nomi | Jami | O’qitishning tashkiliy shakli | Mustaqil ta’lim | O’quvchilarnig bilim va ko’nikmalarini  baholash | Guruh va sana |
| **1 bob** | **Axborot xavsizligi konsepsiyasi** | **12** |  | **6** |  |  |
| 1 | Axborotning qimmatligi | 2 | nazariy | 1 | Yozma,og’zaki, savol-javob |  |
| 2 | Axborot xavsizligining konseptual modeli | 2 | nazariy | 1 | Test ,amaliy topshiriq , savol-javob |  |
| 3 | Kompuyuter viruslari | 2 | nazariy | 1 | Amaliy topshiriq, savol-javob |  |
| 4 | Virusdan himoyalanish | 2 | Nazariy, amaliy | 1 | Yozma,og’zaki, savol-javob |  |
| 5 | Virusdan himoyalanish tizimini yaratish | 2 | Nazariy, amaliy |  | Amaliy topshiriq, savol-javob |  |
| 6 | Virusdan himoyalanish tizimini yaratish | 2 | Nazariy, amaliy | 1 | Yozma,og’zaki, savol-javob |  |
| **II-bob** | **Axboratlarni himoyalashning asosiy yo’nalishlari** | **24** |  | **6** |  |  |
| 7 | Huquqiy axborat tushunchasi | 2 | Nazariy, amaliy |  | Yozma ,Amaliy topshiriq, savol-javob |  |
| 8 | Huquq sohasidagi axborot jarayonlari | 2 | Nazariy, amaliy | 1 | Amaliy topshiriq, savol-javob |  |
| 9 | Huquq sohasidagi axborotlashtirish borasidagi davlat siyosatining vazifalari | 2 | Nazariy, amaliy |  | Yozma ,Amaliy topshiriq, savol-javob |  |
| 10 | O’zbekiston Respublikasi hamda MDH ga a’zo davlatlarning yagona huquqiy-axborot maydonini yaratish | 2 | Nazariy, amaliy | 1 | Test savollari Amaliy topshiriq, savol-javob |  |
| 11 | Axborotlashtirish sharoitlarida axborot maydononi yaratish | 2 | Nazariy, amaliy |  | Amaliy topshiriq, savol-javob |  |
| 12 | Axborat xavsizligi sohasidagi munosabatlarni huquqiy tartibga solishning tuzilmasi | 2 | Nazariy, amaliy | 1 | Yozma,og’zaki, savol-javob |  |
| 13 | Axborot texnologiyalariga oid huquqbuzarlik va unga qarshi kurash yo’nalishi | 2 | Nazariy, amaliy | 1 | Amaliy topshiriq, savol-javob |  |
| 14 | Shaxs ,jamiyat va davlat manfaatlarini sifatsiz axbootlarning ta’siridan, axborot tarqatish tartibining buzilishidan himoya qilish | 2 | Nazariy, amaliy | 1 | Amaliy topshiriq, savol-javob |  |
| 15 | Kompyuter tarmoqlarida axborotni himoyalash | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob |  |
| 16 | Axborotni himoya qilish tizimini amalga oshirilishi usullari | 2 | Nazariy, amaliy | 1 | Test,amaliy topshiriq, savol-javob |  |
| 17 | Axborot xavfsizligi siyosati | 2 | Nazariy, amaliy |  | Test,amaliy topshiriq, savol-javob |  |
| 18 | Tizimlarni tahlil qilish metodi |  |  |  |  |  |
| **III-bob** | **Axborotlarni kriptografik himoyalash usullari** | **32** |  | **10** |  |  |
| 19 | Axborotlarni kriptografik himoyalash usullari | 2 | Nazariy, amaliy | 1 | Test,amaliy topshiriq, savol-javob |  |
| 20 | Axborotni homoyalashning texnik tizimlari | 2 | Nazariy, amaliy | 1 |  |  |
| 21 | Simmetrik va asimmetrik shifirlash tizimlari | 2 | Nazariy, amaliy | 1 | Yozma , amaliy topshiriq, savol-javob |  |
| 22 | Elektron raqamli imzo | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob |  |
| 23 | Xodimlarning maxfiy ma’lumotlarga kirishlarini ro’yxatga olish | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob |  |
| 24 | Blokli shifrlash algoritmlari | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob |  |
| 25 | Blowfish kriptoalgoritmi | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob,yozma |  |
| 26 | Shifrlash va deshifrlash blok sxemasi | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob,yozma |  |
| 27 | Blowfish kriptoalgoritmining dasturiy modeli | 2 | Nazariy, amaliy | 1 | amaliy topshiriq, savol-javob,yozma |  |
| 28 | Axborotlarni kriptografiyali himoyalash tamoyillari | 2 | Nazariy, amaliy |  | amaliy topshiriq, savol-javob,yozma |  |
| 29 | Kriptografik shifrlash vositalari nima? | 2 | Nazariy, amaliy |  | Test,amaliy topshiriq, savol-javob |  |
| 30 | Kriptografik himoya YaN | 2 | Nazariy |  |  |  |

**DARS REJASI № 1**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :”**Axborot xavfsizligi ”

**Dars mavzusi:**Axborotning qimmatliligi .

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborot tug’risida ma’lumot 2. Axborotning qimmatliligi |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:   1. Mavzuga oid misollarning yechilishini ko’rsatadilar. 2. Mavzuni aytib beradilar. 3. Mavzuni izohlab beradilar. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Kompyuterda mashqlar bajarish |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:   1. Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:   1. 9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.   Maqsad va vazifalarni belgilash:   1. Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi. 2. Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi. 3. O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.   Ta’lim oluvchilar bilimini faollashtirish:   1. Savol-javob orqali bilimlarni faollashtiradi.   Yangi o’quv material bayoni:   1. Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.   Asosiy xolatlarni yozdiradi:   1. Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.   Yangi mavzu materiallarini mustahkamlash:   1. Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi. 2. Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi. 3. Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |
| 3-bosqich. Yakuniy  (10 daq) | Mashg’ulot yakuni:   1. Faol ishtirok etgan o’quvchilarni javoblarini izohlab baholaydi va rag’batlantiradi.   Uyga vazifani berilishi:   1. Kelgusi mashg’ulotga vazifa va uni bajarish yuzasidan yuriqnoma beradi. | Baholari bilan tanishadilar.  Topshiriqni yozib oladilar. |

**NAZARIY DARS REJASI № 2**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborot xavfsizligining konseptual modeli.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborot xavfsizligi 2. Axborot xavfsizligining konseptual modeli. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Axborot xavfsizligining konseptual modeli ishlash asoslari bajaradilar . |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Misol va mashqlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.   1. Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 3**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Kompyuter viruslari

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Kompyuter viruslari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Kompyuter viruslari hadida tushuncha beradi . |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashqlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №4**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Virusdan himoyalanish.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Virusdan himoyalanish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Virusdan himoyalanish usullarini urganadi |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №5**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Virusdan himoyalanish tizimini yaratish.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Virusdan himoyalanish  2. Virusdan himoyalanish tizimini yaratish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Virusdan himoyalanish tizimini yaratish |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №6**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Virusdan himoyalanish tizimini yaratish

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Virusdan himoyalanish  2.Virusdan himoyalanish tizimini yaratish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. . Virusdan himoyalanish tizimini yaratish  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №7**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Huquqiy axborot tushunchasi

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Huquqiy axborot tushunchasi  2.Axborot jarayonlari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. . Huquqiy axborot tushunchasitushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №8**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Huquq sohasidagi axborot jarayonlari

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Huquq sohasidagi axborot  2. Huquq sohasidagi axborot jarayonlari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Huquq sohasidagi axborot jarayonlari tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 9**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Huquq sohasidagi axborotlashtirish borasidagi davlat siyosatining vazifalari.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Huquq sohasidagi axborotlashtirish  2.Axborotlashtirish borasidagi davlat siyosatining vazifalari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulotga  oid amaliy mashqlar bajara oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Huquq sohasidagi axborotlashtirish borasidagi davlat siyosatining vazifalari tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 10**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**O’zbekiston Respublikasi hamda MDH ga a’zo davlatlarning yagona huquqiy –axborot maydonini yaratish.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. O’zbekiston Respublikasi hamda MDH ga a’zo davlatlarning yagona huquqiy –axborot maydonini yaratish  2.Huquqiy –axborot maydonini yaratish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Huquqiy –axborot maydonini yaratish  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №11**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborotlashtirish sharoitlarida axborot sohasidagi huquq va erkinliklarni himoya qilish.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborotlashtirish sharoitlarida axborot sohasidagi huquq  2. Axborot sohasidagi huquq va erkinliklarni himoya qilish. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Axborot sohasidagi huquq va erkinliklarni himoya qilish tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №12**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborot xavsizligi sohasidagi munosabatlarni huququiy tartibga solishning tuzilmasi.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborot xavsizligi sohasidagi munosabatlar  2.Axborot xavsizligi sohasidagi munosabatlarni huququiy tartibga solishning tuzilmasi. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3 Axborot xavfsizligi sohasidagi munosabatlartug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 13**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborot texnologiyalariga oid huquqbuzarlik va unga qarshi kurash yo’llari.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborot texnologiyalariga oid huquqbuzarlik  2.Axborot texnologiyalariga oid huquqbuzarlik va unga qarshi kurash yo’llari. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Axborot texnologiyalariga oid huquqbuzarlik va unga qarshi kurash yo’llari |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №14**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Shaxs,jamiyat va davlat manfaatlarini sifatsiz axborotlarning ta’siridan , axborot tarqatish tartibining buzilishidan himoya qilish .

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Shaxs,jamiyat va davlat manfaatlarini sifatsiz axborotlar  2.Sifatsiz axborotlarning ta’siridan , axborot tarqatish tartibining buzilishidan himoya qilish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Shaxs,jamiyat va davlat manfaatlarini sifatsiz axborotlarning ta’siri. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №15**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Kompyuter tarmoqlarida axboratni himoyalash.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Kompyuter tarmoqlarida axboratni himoyalash.  2. Tarmoqlarda axboratni himoyalash. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Oq-qora gradatsiyali tasvirlarda morfologik operatsiyalar tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №16**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborotni himoya qilish tizimini amalga oshirilishi usullari

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1.Axborotni himoya qilish  2.Axborotni himoya qilish tizimini amalga oshirilishi usullari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Axborotni himoya qilish tizimini amalga oshirilishi usullaritug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №17**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborot xavfsizligi siyosati.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborot xavfsizligi siyosati..  2.Xavfsizlik choralarini ko’rish. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot asoslari fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy mashg’ulotlarni bajara oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3 . Axborot xavfsizligi siyosati tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №18**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Tizimlarni tahlil qilish .

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Tizimlarni tahlil qilish.  2.Tahlil qilish usullari . |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Tizimlarni tahlil qilish tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI №19**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborotlarni kriptografik himoyalash usullari.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborotlarni kriptografik himoyalash.  2. Axborotlarni kriptografik himoyalash usullari. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Axborotlarni kriptografik himoyalash usullari tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 20**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborotni himoyalashning texnik tizimlari .

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborotni himoyalashning texnik tizimlari . |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Axborotni himoyalashning texnik tizimlari  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 21**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Simmetrik va asimmetrik shifrlash tizimlari.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborotni himoyalashning texnik tizimlari 2. Simmetrik va asimmetrik shifrlash tizimlari. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Simmetrik va asimmetrik shifrlash tizimlari  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 22**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Elektron raqamli imzo.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Axborotni himoyalashning texnik tizimlari .  2. Elektron raqamli imzo. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Elektron raqamli imzo tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 23**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Xodimlarning maxfiy ma’lumotlarga kirishlarini ro’yxatga olish.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Xodimlarning maxfiy ma’lumotlari. 2. Xodimlarning maxfiy ma’lumotlarga kirishlarini ro’yxatga olish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Axborotni himoyalashning texnik tizimlari  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 24**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Blokli shifrlash algoritmlari.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Blokli shifrlash algoritmlari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Blokli shifrlash algoritmlari  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 25**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Blowish kriptoalgoritmi.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Blowish kriptoalgoritmi. 2. Blowish kriptoalgoritmining vazifalari. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3.Blowish kriptoalgoritmi  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 26**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Shifrlash va deshifrlash blok sxemasi.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Shifrlash va deshifrlash blok sxemasi. 2. Deshifrlash blok sxemasi ko’rsatib berish |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Shifrlash va deshifrlash blok sxemasi  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 27**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Blowfish kriptoalgoritmining dasturiy modeli.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Blowfish kriptoalgoritmining dasturiy modeli 2. Dasturiy modellarda ishlash |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Blowfish kriptoalgoritmining dasturiy modeli tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 28**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Axborotlarni kriptografiyali himoyalash tamoyillari.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1 .Axborotlarni kriptografiyali himoyalash.  2. Axborotlarni kriptografiyali himoyalash tamoyillari. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Axborotlarni kriptografiyali himoyalash tamoyillaritug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**\**

**NAZARIY DARS REJASI № 29**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Kriptografik shifirlash vositalari nima?

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Kriptografik shifirlash vositalari nima?  2. Kriptografik shifirlash vositalari vazifalari. |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Kriptografik shifirlash vositalari  tug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**NAZARIY DARS REJASI № 30**

**Nazariy o’quv mashg’ulotining o’qitish texnologiyasi**

**O’quv fanining nomi :**Axborot xavfsizligi

**Dars mavzusi:**Kriptografik himoya.

**O’quv mashg’ulotining o’qitish texnologiyasi modeli.**

|  |  |
| --- | --- |
| Vaqt: 80 daqiqa | Ta’lim oluvchilar soni: |
| O’quv mashg’uloti shakli va turi: | A |
| O’quv mashg’uloti rejasi: | 1. Kriptografik himoya 2. Kriptografik himoya turlari |
| O’quv mashg’ulotining maqsadi: O’quvchilarda Axborot xavfsizligi fani bo’yicha bilim va ko’nikmalarni hosil qilish | |
| O’qitish natijasi: | Ushbu Mustahkamlash uchun amaliy mashg’ulot mavzusini o’zlashtirish natijasida o’quvchida shakllanadigan asosiy bilim: Mustahkamlash uchun amaliy mashg’ulot.  ko’nikma: Mustahkamlash uchun amaliy mashg’ulot bajara oladi, Kompetensiya: Mustahkamlash uchun amaliy mashg’ulot  oid amaliy masalalarni yecha oladi; |
| Pedagogik vazifalar:  1.Mavzu rejasi bilan tanisgtirish.  2. Mavzuni tushuntirish.  3. Mavzuga oid misollarning yechilishini ko’rsatib berish. | O’quv faoliyat natijalari:  1.Mavzuga oid misollarning yechilishini ko’rsatadilar.  2.Mavzuni aytib beradilar.  3. Kriptografik himoyatug’risida tushunchaga ega bo’ladi. |
| O’qitish metodlari: | Kitob bilan ishlash |
| O’qitish vositasi: | Yozuv taxtasi, slaydlar |
| O’quv mashg’ulotini tashkil etish shakli: | Yakka tartibda |
| O’qitish sharoiti: | Informatika xonasi |
| Qayta aloqaning usul va vositalari: | Amaliy mashg’ulotlar |

**O’quv mashg’ulotining texnologik xaritasi.**

|  |  |  |
| --- | --- | --- |
| **Ish bosqichlai va vaqti** | **Faoliyat mazmuni** | |
| **O’qituvchi** | **Ta’lim o’luvchi** |
| 1-bosqich. O’quv mashg’ulotiga kirish. (5daq) | Tashkiliy qism:  1.Oquvchilarni mashg’ulotga tayyorgarligi va davomatini tekshiradi. | Mashg’ulotga tayyorlanadilar. |
| 2- bosqich. Asosiy  (65 daq) | Tayanch bilimlarni faollashtirish:  2.9- sinfda o’tilgan mavzu bo’yicha o’quvchilarga savollar beriladi, ularni baholaydi.  Maqsad va vazifalarni belgilash:  3.Mashg’ulotning nomi, rejasi, maqsad va o’qitish natijalari bilan tanishtiradi.  4.Mustaqil ishlash uchun adabiyotlar bilan tanishtiradi.  5.O’quv mashg’ulotida o’quv ishlarni baholash mezoni va ko’rsatkichlari bilan tanishtiradi.  Ta’lim oluvchilar bilimini faollashtirish:  6.Savol-javob orqali bilimlarni faollashtiradi.  Yangi o’quv material bayoni:  7.Nazariy mashg’ulotning rejasi va tuzilishiga muvofiq, o’qitish jarayonini tashkil etish bo’yicha harakatlar tartibini bayon etadi.  Asosiy xolatlarni yozdiradi:  8.Slaydlarni mavzu bo’yicha asosiy nazariy holatlarni yozdiradi.  Yangi mavzu materiallarini mustahkamlash:  9.Mustahkamlash uchun savollar beriladi. Jarayon yakka tartibda davom etishini ma’lum qiladi.  10.Yakka tartibda topshiriq beriladi va baholash mezoni bilan tanishtiradi.  11.Bilimlarni mustahkamlash uchun qaytar aloqa o’tkaziladi. | Uy vazifani taqdim etadilar. Savollarga javob beradilar.  Mavzu nomi va rejasini yozib oladilar. Diqqat qiladilar. Savollarga javob beradilar. Yozib oladilar.  Diqqat qiladilar. Savollarga javob beradilar.  Yakka tartibda topshiriqlarni bajaradilar. Ma’lumotlarni daftarga qayd qiladilar. |

**1-mavzu:Axborotning qimmatliligi** .

Insoniyat o’zining rivojlanishi tarixi mobaynida modda, quvvat va axborotlarni o’zlashtirib kelgan. Bu rivojlanishning butun bir davrlari shu bosqichning ilђor texnologiyasi nomi bilan atalgan. Masalan: «Tosh asr» - mehnat suroli yasash uchun toshga ishlov berish texnologiyasini egallash bosqichi, «kitob chop etish asri» - axborotni tarsatishning yangi usulini o’zlashtirish bosqichi, «elektr asri» - quvvatning yangi turlarini o’zlashtirish bosqichi shular jumlasidandir. Bundan 20-30 yillar ilgari «atom asri» boshlandi deyilgan bo’lsa, hozirgi kunda «axborot asri», «EHM asri» deb ataladi. «Informatika va axborot texnologiyalari» fanining kelib chisishi, uning uch tarkibiy qismi algoritm, dastur va hisoblash vositalarini paydo bo’lishi va rivojlanishi bilan bog’liq. Informatika axborotlarni EHM yordamida tasvirlash, saslab turish, uzatish va ishlov berish usullarini o’rganadigan fandir. EHMlarni ishlab chisish va undan foydalanish sohaqida katta yutuslarga erishgan olim V.M.Glushkov ta'biri bilan aytsak: «Yangi asr boshida texnik jihatdan rivojlangan mamlakalarda aksariyat axborot EHM xotirasida joylashgan bo’ladi. XXI asr axborotlardan ana shu axborotlardan foydalanishni bilmagan kishi, XX asr boshida o’sish va yozishni» bilmagan odamga o’xshab soladi. Bundan kelib chissan holda, «Informatika va axborot texnologiyalari» fanini o’rganish ikkinchi savodxonlik bilan tengdir. (Savol: EHM deganda nimani tushunasizq) Informatika fani ham boshqa fanlar satorida olamni bilish uchun xizmat siladi. Axborot umumiy ta'rifga ega bo’lmagan imperik tushuncha. Axborot nima degan savolga, falsafa fani bizni o’rab turgan borlisni ifodasi deb tushuntirsa, axborotlardan amalda foydalanuvchilar axborot va saslanish, shakl o’zgartirish va uzatish mumkin bo’lgan ashyo, (obyekt) deb tushintiradi. Bizni o’rab turgan borlis haqidagi bilimlar yoki har qanday malumotlar axborot deb ataladi. Axborot deganda biror modda yoki jarayonni tushunish kerak emas, balki ana shu modda yoki jarayonni turli jihatlarini sonlar, formulalar, belgi yoki tushunchalar orqali tavsiflaydigan vaqilni tushunish kerak. Insonning ijodiy yoki mehnat faoliyati, fan va texnikaning rivoji, jonli mavjudodlarning o’zini to’tishi, har qanday avtomatik tarzda ishlaydigan qurilmalar faoliyati axborotni ayirboshlash bilan bog’liq. EHMni paydo bo’lishi jamiyat rivojlanishida insilobiy o’zgarishlarga sabab bo’ldiki, insonga axborotni yiђish, saslash va ishlov berish bilan bog’lik bo’lgan asliy mehnatni avtomatlashtirish imkonini berdi. Bu xildagi jarayonlarni avtomatlashtirish istisodiy-tashkil iy tuzumlarga, texnologik jarayonlarni boshqa rishga, loyihalar tuzish, ilmiy izlanishlar, o’sish-o’rganish va boshqa sohalarga kirib bordi. Shunday silib ilmiy-texnik rivojlanishning asosiy yo’nalishi paydo bo’ldi. Kiritish-chisarish qurilmalari bilan ta'minlangan EHMlar katta hajmdagi axborotlarni yig’ib, xotirada saslab turish va kerak bo’lganda katta tezlikda kerakli axborotni berish mumkin. Mbaytli disk o’zida katta O’zbek Qomusining 25 tomini saqlay oladi, ana shu axborotni o’qib olish uchun esa 1 minut vaqt kifoya. Axborot texnologiyasi deganda, hajmi oshib borayotgan axborot oqimini yig’ish, saqlab turish, ishlov berish va uzatishni EHMlar yordamida amalga oshiradigan usullarni majmuasi tushuniladi. Ushbu usullarni turli ko’rinishda ishlatilishi insonga zarur axborotlarni olish uchun EHM bilan muloqotda bo’lishni taqozo etadi. EHM deganda axborotlar va hisoblashlarni algoritm asosida ishlov berishni tezlashtiradigan yoki avtomatik tarzda amalga oshiradigan qurilmani tushunamiz. Shunday silib «Hisoblash mashinasi» tushunchasi «axborot» va «algoritm» tushunchalari bilan chambarchas bog’liq. Odatda «axborot» so’zi ma'lumotning mazmuni va ahamiyati bilan birlashtirib yuboriladi. Masalan: kelish kuni haqidagi xat, gar bu kun haqida allasachon bilsak hech qanday axborot bermaydi. Olimlar aytishiga qaraganda, bizni o’rab turgan olamni bilish haqidagi bilimlar hajmi 10 yilda 2 marta, sayta ishlanishi zarur axborot hajmi 1 yilda kvadrati marta oshmosda. Ma'lumki, mamlakatimizda 1 yilda 60 mlrd xat - hujjat yaratiladi. Har bir xatni sayd silish uchun 5 dasisa sarflansa har kuni, 8 soatdan ishlab 1 yil davomida 1,7 mln. odam shuђullanishi kerak. Har bir xatni tayyorlashga o’rtacha bir soat sarflansa, yil davomida (dam olishsiz) 21 mln. odam shuђulanishi kerak. Lekin mehnat unumdorligini shu darajada oshirishi nafasat hisoblash ishlarini avtomatlashtirish, balki axborotni yiђish, saslab turish va uzatish ishlarini ham avtomatlashtirish kerak. Axborotni abstrakt tushunchalar satoriga, masalan, matematik formulalar satoriga quyish mumkin, lekin u har doim moddiy quvvat shaklida fizik asosiga ega bo’lgan holda namoyon bo’ladi va shuning uchun ham uni o’lchash mumkin. Kundalik hayotimizda uzlukli axborotni bir so’zlar orqali o’zlashtirib kelamiz. So’zlar esa o’z navbatida harflar va maxsus belgilardan tashkil topadi. Bu turdagi axborotlar matnli axborot deb ataladi. Sayta ishlayotgan axborot turiga sarab, hisoblash texnikasi vositalari uch turga bo’linadi: 1) Uzluksiz (analog) elektron hisoblash mashinalari (AEHM), bu xildagi mashinalarda vaqt birligi ichida uzluksiz ustida hisoblash ishlari bajariladi. 2) Rakamli (diskret) elektron hisoblash mashinalari (REHM), bo’larda vaqt birligi ichida rasamlardan tashkil topgan diskret (uzlukli) siymatlar ustida amallar bajariladi. 3) Aralash (gibrid) elektron hisoblash mashinalari (GEHM) bu xildagi mashinalar AEHM larni axborotlarni uzluksiz kiritib-chisarish, REHMlarni esa axborotlarni katta tezlikda ishlov berish kabi xususiyatlarni o’zida mujassamlashtirgan. Axborot noaniqligini teng ikki martaga kamaytiradigan ma'lumot, axborot o’lchov birligi bit deb ataladi. Uzatish tezligi 1 sekundiga uzatiladigan bitlar soni bilan o’lchanadi (masalan 19200 bitG`sek). Bir sekundda bajara oladigan amallar soni EHMning hisoblash tezligi deb ataladi (masalan 500000 amalG`sek). Ikqilik ma'lumotlardagi axborot misdorini o’lchash uchun bit va baytlardan tashsari, quyidagi kattaroq birliklardan ham foydalaniladi. Informatsiyaning eng kichik birligi - bu bit(b). 8 bit 1 Bayt hisoblanadi va bitta simvol yoki harf bilan ustma-ust tushishi mumkin. 1 Kilobayt(KB)= 1024 B 1 Megabayt(MB)=1024 KB 1 Gigabayt(GB)=1024 MB 1 Terabayt(GB)=1024 TB Operativ xotiraning o’rtacha hajmi 4-2048 MB Qattiq disk uchun 0,6-1000 GB Egiluvchan magnitli disk uchun 1,4-4 MB Kompakt disk (yoki DVD disk) uchun 0,6-18 GB Strimmer uchun 0,6-400 GB Magnitooptik disk uchun 1-1000 GB O’xshatish uchun, agar 1 bit=1,25 mm desak, bayt=sm, kbayt=1000 sm, mbayt=10 km, gbayt=10.000 km ga teng bo’ladi.

**2.mavzu**:Axborot xavsizligining konseptual modeli.

TizimliDT axborotni qayta ishlovchi dasturlarni yaratish samaradorligini oshirish va ularni EXM da qo’llash uchun hamda EXM dan foydalanuvchilarga EXM resurslari bilan ishlash bo`yicha ma'lum xizmatlarni taklif etish uchun mo’ljallangan. Amaliy dasturli ta'minot (ADT) foydalanuvchining aniq bir muammoli masalasini yoki shunday masalalar sinfini yechish uchun mo’ljallangan (ADT ni ko’pincha dasturli ilova deb ataladi). Tizimli dasturli ta'minot tarkibi: Tizimli dasturli ta'minot o’z ichiga quyidagilarni oladi: ¬ Operatsion tizim (OT) — TDT ning har doimgi, doimiy qismi bo’lib, u ShK ning turli rejimlarda samarali ishlashini ta'minlaydi, dasturning bajarilishini va D T tizimi Servisli tizimlar Instrumental dasturli vositatalar Texnik hizmat ko’rsatish tizimi Instrumental dasturli tizimi Tehnik hizmat kursatish tizimi Yuklagichla r Diagnostikli Interfeysl tizimi OC qobiqlari Utilitlar Matn muharrirlari Testli Operatsion tizimi MS-DOS MS-DOS MSDOS MS-DOS MS-DOS OS/2 MS-DOS MS-DOS UNIX MS-DOS MS-DOS Windows …. Sozlash vositalari foydalanuvchi va EXM tashqi qurilmalarining o’zaro ishini tashkil etadi. ¬ Servisli dasturlar, ular foydalanuvchiga va uning dasturlariga qo’shimcha xizmatlar to’plamini taklif etib, OT ning imkoniyatlarini kengaytiradi. ¬ Instrumentalli (vositali) dasturli vositalar, ular DT ni samarali ishlab chiqish va sozlash uchun mo’ljallangan. ¬ Texnik xizmat ko’rsatish tizimi, u diagnostika, jixozlarni tiklash va ShK da nuqsonlarni topishni yengillashtiradi, shu bilan birga uning yanada yuqoriroq ishonchliligini va axborotlarni o’zgartirish jarayonlarining bajarilish aniqligini ta'minlaydi. . ShK lar uchun quyidagi OT turlari keng tarqalgan:

• MS DOS - IBM PC AT va XT ShK lari uchun;

• OS/2 - IBM PS/2 va 80386 va undan yuqori MP li PC AT ShK lari uchun;

• UNIX — 32 razryadli IBM PS/2 va 80386 va undan yuqori MP li IBM PC AT ShK lari uchun;

• Windows 95 — 32 razryadli, 80386 va undan yuqori MP li IBM PC AT ShK lari uchun;

• Windows NT — 32 razryadli, 80486 va undan yuqori MP li IBM PC AT ShK lari uchun. Avval ta'kidlanganidek, shaxsiy kompyuterlar - bu axborotni ishlovchi universal mashinalardir. Kompyuterlarni ishlatish uchun ularga tushunarli bo’lgan tilda bajarilishi lozim bo’lgan ishlar haqida aniq va batafsil ko’rsatmalar ketma-ketligini tuzish kerak. Bunday ko’rsatmalar ketma-ketligi dastur (programma) deyiladi. O’zicha kompyuter hech qanday ishni bajara olmaydi, u faqat berilgan dastur bo’yicha tegishli ishni bajarishi mumkin. Kompyuterda ishlaydigan dasturlarni 3 xil kategoriyaga bo’lish mumkin:

1)Amaliy dasturlar; bu dasturlar foydalanuvchiga kerak bo’lgan ishlarning bajarilishini bevosita ta'minlaydi (funksiya qiymatlarini hisoblash, har xil massivlarni qayta ishlash, rasm chizish, matnlarni muharrirlash va hokazo).

2) Sistemali yoki tizimli dasturlar; bu dasturlar har xil yordamchi vazifalarni bajaradi (kompyuter haqida ma'lumot chiqarib berish, axborotdan nusxa ko’chirish va hokazo).

3)Instrumental sistemalar yeki tizimlar (dasturlashtirish tizimlari); bu tizimlar kompyuter uchun yangi dasturlar tuzilishini ta'minlaydi. Bu dasturlar kategoriyalarining har birini alohida o’rganamiz. Sistemali dasturlar. 1) Operasion tizim yoki operasion sistema. Operasion sistema sistemali dasturlar orasida alohida o’rinni egallaydi. Bu sistema foydalanuvchi bilan kompyuter o’rtasidagi muloqotni ta'minlaydi, kompyuterni boshqarishni ta'minlaydi. Kompyuter ishga qo’shilishi bilan operasion sistema dasturlari birdan kompyuter xotirasiga yuklanadi. IBM PC kompyuterlarida ko’proq Microsoft firmasi ishlab chiqqan MS DOS operasion tizim ishlatiladi. 2) Drayverlar. Drayverlar - dasturlar kompyuterning kiritish - chiqarish qurilmalarini, tezkor xotirasini boshqarish bo’yicha operasion tizim DOSning imkoniyatlarini kengaytiradi. Drayverlar yordamida kompyuterga yangi qurilmalarni ulash mumkin yoki mavjud qurilamalardan boshqacharoq foydalanish mumkin. 3) Qobiq - dasturlar; bu dasturlar operatsion tizim DOS dasturlariga nisbatan kompyuter bilan qulayroq va ko’rgazmali muloqot o’rganish imkoniyatini beradi. Qobiq - dasturlardan ko’proq Norton Commander, XTree, Pro Gold va boshqalari ishlatiladi. 4) Utilitlar; bular yordamchi vazifalarni bajaruvchi dasturlardir. Masalan: Norton Utilities nomli sistemali dasturlar majmui mavjuddir. Amaliy dasturlar. IBM PC kompyuterlari uchun turli soxalarda qo’llaniladigan yuz minglab har xil amaliy dasturlar ishlab chiqilgan. Eng keng qo’llaniladigan dasturlar quyidagilardir:

1) Matn muharrirlari. Bular kompyuter yordamida matn va hujjat tayorlaydi.

2) Nashriyot tizimlari. Bular tipografiyadek (bosmaxonadek) xujjat tayorlaydi.

3) Jadvali prosessorlar. Bular jadval ko’rinishida berilgan sonli ma'lumotlarni qayta ishlaydi.

4) Ma'lumotlar bazalarini boshqarish tizimlari. Bular axborotlar massivlarini qayta ishlaydi. Kompyuterdan foydalanuvchilar o’z masalalarini yechish uchun tuzgan dasturlar majmui.

5) Kompyuterdan foydalanuvchilarni yechish uchun tuzgan dasturlar majmuni. Dasturlashtirish tizimlari. IBM PC kompyuter uchun un minglab dasturlar bo’lsa ham, ular foydalanuvchini qiziktirgan ayrim masalalarni yechishga mo’ljallanmagan bo’lishi mumkin. Bunday hollarda foydalanuvchi kerakli dasturni o’zi tuzadi. Yangi dasturni tuzish uchun qaysidir dasturlashtirish tizimi ishlatiladi. IBM PC kompyuterlarida ko’pincha SI, SI++, Paskal va Beysik tillari asosida yaratilgan TURBO C, TURBO C++, TURBO PASCAL, MICROSOFT C, MICROSOFT BASIC dasturlash tizimlari ishlatiladi. Foydalanuvchi kompyuter bilan paketli hamda dialogli usullarda o’zaro xamkorlik qilishlari mumkin. Paketli usul iqtisodiy vazifalarni yechishni markazlashtirilgan holda tashkil qilishda eng keng tarqalgan turi. Paketli usulda hisoblash jarayonini tashkil qilish foydalanuvchining EHMga kirishisiz qurilgan. Uning vazifasi vazifalar paketi bo’yicha dastlabki ma'lumotlarni tayyorlash va EHM uchun ishlab chiqarishga vazifalar, dasturlar va meyoriy-ma'lumotnomaviy ma'lumotlarga ega bo’lgan ishlab chiqarish markaziga uzatish bilan cheklangan. Foydalanuvchi va EHM o’zaro hamkorligining dialogli usuli insonni axborotlarni EHMda ishlab chikarish jarayoniga tezkor aralashishi uchun imkoniyat yaratadi. Dialog tizimining foydalanish tarifi quyidagi talablarni qondirishi kerak:

• Foydalanuvchining tizimga osonlik bilan moslashishi;

• Hisoblash, mantiqiy tadbirlar va atamalarning bir xilligi;

• Foydalanuvchi videoterminal ekrani yoki bosib chikaruvchi qurilmaga EHMdan yordam olish payti yoki javob harakatlarnii o’tkazishsh zarurligini ko’rsatish bilan chikariladigan ma'lumotla axborotlar yoki kerakli yuriqnomalar bilan ta'minlash;

• Dialoglarning qisqacha shakllaridan foydalanish;

• Tizimli axborotlarni operasion tizimlar va maxsus dasturlar bilan amalga oshiraladigan himoya vositalarining mavjudligi. Menyu, andoza, buyruk, tabiy til dialogning tashkil qilishning keng tarkalgan turlaridir. Menyu dialogning turi sifatida yakuniy foydalanuvchi uchun juda qulaydir. Menyu turidagi dialogni faqat videoterminal ekraniga tizimning belgilangan vazifasini chikarish orqali amalga oshirish mumkin. Andoza - bu, yakuniy foydalanuvchi va EHM o’zaro hamkorligining muloqot usuli, uning har bir qadamida tizim faqat foydalanuvchi kiruvchi axborotning formati bo’yicha sintaktik cheklanishni qabul qiladi. Buyruq - turidagi dialog foydalanuvchi tomonidan quyiladi. Tabiy til - dialogning shunday turiki, unda foydalanuvchi tomonidan so’rov va javob tabiyga yaqin tilda olib boriladi. Axborotlarni avtomatlashgan holda ishlab chikarishning tarmoqli usuli Tarmoq - bu, hisoblash resurslarining samarali taqsimlanishni ta'minlovchi dasturiy, texnik va kommunikasion vositalar majmui. Ochiqlilik. Zamonaviy ShK istalgan turdagi tarmoqlar konturiga ulanish imkoniyatini ta'minlashdan iboratdir. Resurslar. Tarmoqning ahamiyatliligi va qadrililigi unda saqlanayotgan bilimlar, ma'lumotlar majmui va texnik vositalarni tezkor taqdim etish yoki ishlab chikarish kobilyati bilan aniklanidi. Ishonchlilik. Avariyali usul haqidagi tezkor xabarlar, testdan o’tkazish va dasturli-mantiqiy nazoratning yuqori ko’rsatkichini ta'minlash sifatida talqin qilinadi. Dinamiklik. Tarmoqni foydalanuvchi suroviga javob qilish vaqtini kamaytirishdan iborat buladi. Avtonomlik. Turli darajadagi tarmoqlar mustakil ishlashining imkoniyati sifatida tushuniladi. Kommunikasiyalar.Ular oldiga tarmoqning foydalanuvchi tomonidan qabul kilingan xar kanday konfigurasiyasi bo’yicha ShKlarning anik uzaro xamkorligini ta'minlash bilan bog’liq alohida kuyiladi. ShKning tarmoq ulanish tuzilmasi bilan aniklanadigan topologiya tarmoqning muxim tarifi bulidi. Topologiya ikki tur - jismoniy va mantikiyga ajratiladi. Jismoniy topologiya deganda tarmoq tugunlari aloka kanallariga ulanishining xakikiy chizmasi, mantikiy turida esa tugunlar urtasidagi ma'lumotlar okimlari yyonalishining tuzilmasi tushuniladi. Bu ikki tur xamma vaqt xam mos kelavermaydi. Tarmoqlarning bir necha topologik tuzilmalari mavjud: shinali, yulduzsimon, daraxt kurinishidagi, doiraviy va ko’p alokali. Utkazuvchi texnologiyalarda kanallardagi jismoniy muhit sifatida kuyidagilardan foydalaniladi:

• Yassi ikki tomirli kabel;

• Simlarning urilgan jufti;

• Nur utkazgich va boshalar; Tarmoqni tanlash bo’yicha ishlar kuyidagilarni nazarda tutadi:

1. Muammo soha bilan tanishish.

2. Tarmoqli operasion tizimni tanlash.

3. Apparatli karorlar bo’yicha takliflarni, jumladan: kompyuterlar bo’yicha, kommunikasion uskunalar bo’yicha tanlash. Tarmoqni kalit ostida yaratishga kodir malakali tizimli integrasiyalarning uch asosiy alomatini farqlash mumkin: Birinchidan, firma tizimli tarmoqli integrayiyalash soxasida ixtisoslashishi kerak. Ikkinchidan, firma tavsiya etilgan uskunalar va dasturli ta'minlashning asosiy yetkazib beruvchilari bilan uzok muddatli bitimlarga ega bo’lishi lozim. Uchinchidan, firma tarmoqlarni loyixalashtirish, o’rnatish va kuzatish bo’yicha yetarli ish tajribasiga ega bo’lishi kerak. Zamonaviy axborot texnologiyalarining gurkirab rivojlanishi va uni qo’llash sohasining kengayishi dasturiy ta'minotning (DT) jadal rivojlanishiga olib keldi. Shuni takidlash kerakki, 1990 yilda jahon jamiyatida dasturiy ta'minotga 100 mlrd. AKSH dollaridan ziyod mablag sarflandi. Bunda DT rivojlanishi yyonalishi shuni ko’rsatadiki, harakatlar tendentsiyasi yiliga 20% usib bormokda. Axborot tizimlarining DTi deganda, hisoblash texnikasi vositalari bilan ma'lumotlarni qayta ishlash tizimini yaratish va ulardan foydalanish uchun dasturiy va xujjatli vositalarni jamlash tushuniladi. Dasturiy ta'minot tomonidan bajariladigan funktsiyalarga bog’liq holda, uni ikki guruhga bo’lish mumkin: tizimli dasturiy ta'minot va amaliy dasturiy ta'minot. Tizimli dasturiy ta'minot kompyuterda axborotni qayta ishlash jarayonini tashkil etadi va amaliy dasturlar uchun me'yordagi ish muhitini ta'minlaydi. Amaliy DT foydalanuvchining aniq vazifalarini xal etish va umuman axborot tizimining hisoblash jarayonini tashkil etish uchun mo’ljallangan. Tizimli DT tarkibiga quyidagilar kiradi: - operatsion tizimlar; - servis dasturlar; - dasturlash tillari translyatorlari; - texnik xizmat dasturlari.

**3-mavzu:Kompyuter viruslari.**

Hozirgi kunda kompyuter foydalanuvchilari oldida katta muammo-viruslardan himoyalanish muammosi turadi. Ayniqsa bu muammo katta korxonalarga zarar keltirmoqda. Chunki kompyuter viruslari ishi natijasida malumotlar o’chiriladi. Ma'lumotlarni, hamda kompyuterlarni himoyalash uchun maxsus mutaxasislar himoya sistemalarini yaratishga jalb qilingan. Lekin shunday bo’lsada, bu sistemalar to’lik kafolat bera olmaydi. Chunki viruslarni yangi no'malum turlarini hisobga olib bo’lmaydi. Shuning uchun davolovchi programmalarni yangilab turish maqsadga muvofiq. 1984 yili AQSH dagi Loxay universitetida o`tkazilayetgan axborotlarning xavsizligi bo`yicha o`tkazilayetgan 7-konferentsiyada F.Koyen tomonidan «Kompyuter virusi» termini ishlatildi. Qisqa vaqt ichida virus muammosi juda tez o`sdi. Virus dasturlar uncha katta sigimga ega bo’lmaydi, assembler tilida yozilgan bo’ladi. Malum shart bajarilsa,o’z -o’zidan Ko’payishi xususiyati faollashadi. 1987 -1989 yillarda IBM PC da «BRAIN», «VIENA», «CASCADE» viruslari paydo bo`ldi. Ekranda harflar to`qila boshladi, foydalanuvchilar o`z manitorlarini tamirlashga shoshilganlar olomoni paydo bo`lgan, so`ng kompyuter boshqa yerliklar gimnini chala boshladi. Hamma tushundiki,bu virus, bitta emas o’nlab viruslar. «BRAIN» virus Boot sektor ustidan golib bo’ldi. Bunday zaharlarga qarshi ANTI –kat dasturlar (Oleg Kotik ) yaratila boshlandi.ANTII –kat «TIME» virusini aniqlashga imkon berdi. Viruslar EXE yoki COM kengaytmani fayllarga tez ilashishi bilan, ularni ishdan chiqara boshlaydi. Ko`rinmas viruslar «BIAST-512» paydo bo`lishi kompyuterlarning janjalkashli kasalliklari paydo bo`ldi. Faylli viruslar faylning boshlanish qismiga yoki faylning oxiriga ilashib oladi. Viruslar faylning o`rtasiga, faylning jadval qismlaridagi bush sohaga yoki matinni fayl qismlariga ilashib oladi. Faylli viruslar hatto o`zining nusxasi operativ xotirada mavjudligini tekshiradi, agar topilmasa, xotirani ishg`ol qiladi va undagi fayllarni zaharlaydi. Yo’qlovchi viruslar sistemali diskning, vinches-terning yo’qlovchi sektorlarini zaharlaydi. Yo’qlovchi virusning ishlash printspi operattsion sistemanng yo’qlash algaritimiga asoslangan bo’lib, yo’qlovchi (Boot –program) dasturini bo’zib yubordi, yani programma tarkibiga qandaydir simvollarni joylashtiradi. Makro viruslar Microsoft offise tarkibiga kirgan ilovalarning ichki foydalanadigon tili VBA bo’zilishi bilan bog’liq bo`ladi. Tarmoq viruslari global, loqal Tarmoqlar bilan ishlaganda paydo bo’ladi, protoqollarni bo’zib yuboradi. Tarmoq viruslarining ishlash printsipi asosan tarmoq orqali mustaqil ravishda o`z kadrlarini jo`natib yuboradi.Tarmoq viruslariga Morris viruslarin kiritish mumkin.

Antivirus dasturlar.

Kompyuter viruslari bilan samarali ko’rashishda antivirus dasturlaridan foydanalinadi, mavjud antivirus dasturlar viruslardan 100 foiz tozalash imkonini bera olmaydi. Viruslardan tozalash uchun virus dasturiga kontur dastur yozilishi bilan antivirus dasturlar yaratiladi. Antivirus dasturlarining ishlash printspi fayllar sektorlar va sistema xotiralarini tekshirish va ulardagi yangi va malum viruslarni izlashdan iborat. Antivirus dasturlarning oxirgi vakillaridan foydalanish tavsiya etiladi. Kasperskiy laboratriya mahsuloti. Kasperskiy laboratriyasi antivirus programma taminotini ANTI VIRAL Tolkat PRo (AVP) nomi bilan tavsiya qiladi. Laboratriya antivirus himoyalarining barcha tillari antivirus skanerlar, monitorlar, revizor kontrolerlar taqdim etiladi. AVP operatsion sistemalarni ,pochta sistemalarni viruslardan tozalaydi. AVP kompyuterviruslarining barcha kanallar orqali mumkun bo’lgan imkoniyatlarini to’liq nazorat qilishni taminlaydi. (Munozara: Viruslardan himoyalanish uchun sizning nazaringizda qanday ishlar qilish kerak?) Doctor Web antivirus dasturi bilan ishlash. Keng tarkatilgan antivirus dasturlaridan biri Doctor Web ( Dr. Web) hisoblanadi. Qo’yida biz uni qanday ishlatish mumkinligini ko’rsatamiz. Albatta Doctor Web har doim yangilanishida bo’ladi, chunki Yangi virus dasturlar paydo bo’ladi. Doctor Web da ishni boshlash uchun u joylashgan katalogdan Dr. Web. Exe dasturi kompyuterga yo’qlanadi. Bu dastur 32 bitli Windows turkumidagi amaliyot tizimlar uchun mo’ljallangan bo’lib, qisqacha Dr Web 32W deb ataladi. DrWeb32W Funksional jihatdan DOSning DrWeb antivirusga o’xshash. Lekin DrWeb ning 4.0 laxjasidan boshlab antivirus dastur ishlashining arxitekturasi va algoritmiga sezilarli o’zgartirishlar kiritilgan. Bu esa o’z navbatida yangi antiviruslar yaratilishiga asos bo’ldi. DrWeb 4.0 antivirusning asosiy yangiligi modul printsiplarining qo’llanilganidir, ya'ni viruslar bazasi alohida faylda tashkil etilagn bo’lib, u asosiy dastur ishga tushganidan so’ng qo’shimcha fayl sifatida yo’qlanadi. Natijada operativ xotira yetishmovchiligining oldi olinadi. DrWeb32 antivirus dasturida dastur biror muhitda ( masalan, Windows 95G`98G`NT) ishlaydigan qobiq dastur va muhitga bog’liq bo’lmagan yadrodan tashkil topadi. Dasturlarni bunday tashkil etish qo’yidagi afzalliklarga ega: - bitta virus bazasining faylidan Dos ning DrWeb dasturi uchun ham, Windows 95G`98G`NT, OSG`2, Novell Netware uchun ham foydalanish mumkin; - dasturning yadrosini boshqa qobiq dasturlar va Amaliy dasturlarga ulash mumkin; - qobiq dasturlar, yadrolar va virus bazalarini Internet tarmogi orqali avtomatik kengaytirish hamda yangilash imkonini beradi. DrWeb32ning Yana boshqa yangiliklaridan biri uning test qilinadigan ob'yektlarini ixtiyoriy diskdagi kataloglar ro’yxatidan ( hatto alohida fayllarni ham ) tanlash imkoniyatining mavjudligidir. DrWeb32 antivirus dasturini ishga tushirganda ( Windows ning ish stolidan, PUSK tavsiyanomasining PROGRAMMA` bo’limidan, MS Office tavsiyanomasidan, PUSK tavsiyanomasining VO`POLNIT bo’limidan,…) monitor ekranida qo’yidagi DrWeb for Win32 dastur darchasida ochiladi .

Nazorat uchun savollar:

1. Tizimli va amaliy daraja nima? 2. Arxivlash qanday amalga oshiriladi? 3. Kompyuter virusi nima? Viruslarning qanday turlarini bilasiz? 4. Viruslardan himoyalanish vositalari nimalar? 5. Viruslarni davolash, ya'ni antivirus dasturlarining qanday guruhlari mavjud? 6. DrWeb dasturi qanday yo’qlanadi va uning asosiy tavsiyanomasi qanday bo’limlarni o’z ichiga olgan?

4-mavzu:Virusdan himoyalanish.

Virus paydo bo’lish belgilari. Zararlangan kompyuterda eng muhimi virusni aniqlash. Buning uchun virusni asosiy belgilarini bilish kerak: 1.Funktsional dasturlarni ishini to’xtatish yoki noto’g’ri ishlashi; 2.Kompyuterni sekin ishlashi; 3.OS ni yuklanmasligi; 4.Fayl va kataloglarni yo’qolishi yoki ulardagi ma`lumotlarni buzilishi; 5.Fayllar modifikatsiyasining sana va vaqtining o’zgarishi; 6.Fayl hajmining o’zgarishi; 7.Diskdagi fayllar miqdorining keskin ko’payishi; 8.Bo’sh operativ xotira hajmining keskin kamayishi; 9.Kutilmagan ma`lumotlar va tasvirlarning ekranga chiqishi; 10.Kutilmagan tovushlarning paydo bo’lishi; 11 .Kompyuterning tez-tez osilib kolishi. Yuqoridagi belgilar boshqa sabablarga ko’ra ham bo’lishi mumkinligini eslatib o’tamiz. Virusga qarshi dasturlar Kompyuter viruslarini aniqlash va ulardan himoyalanish uchun maxsus dasturlarning bir necha xillari ishlab chiqilgan bo’lib, bu dasturlar kompyuter viruslarini aniqlash va yo’qotishga imkon beradi. Bunday dasturlar virusga qarshi dasturlar deb yuritiladi. Umuman, barcha virusga qarshi dasturlar zaharlangan dasturlarning va yuklama sektorlarning avtomatik tarzda tiklanishini ta’minlaydi. Viruslarga qarshi dasturlar foydalanadigan viruslarni aniqlashning asosiy usullari quyidagilar: - etalon bilan taqqoslash usuli; - evristik taxlil; - virusga qarshi monitoring; - o’zgarishlarni aniqlovchi usul; - kompyuterning kiritish/chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o’rnatish va h. Etalon bilan taqqoslash usuli eng oddiy usul bo’lib, ma’lum viruslarni qidirishda niqoblardan foydalanadi. Virusning niqobi-mana shu muayyan virusga xos kodning qandaydir o’zgarmas ketma-ketligidir. Virusga qarshi dastur ma’lum virus niqoblarini qidirishda tekshiriluvchi fayllarni ketma-ket ko’rib chiqadi (skanerlaydi). Evristik tahlil. Kompyuter virusi ko’payishi uchun xotirada nusxalanish, sektorga yozilish kabi qandaydir muayyan xarakatlarni amalga oshirishi lozim. - 37 - Virusga qarshi monitoring. Ushbu usulning mohiyati shundan iboratki, kompyuter xotirasida boshqa dasturlar tomonidan bajariluvchi shubhali harakatlarni monitoringlovchi virusga qarshi dastur doimo bo’ladi. Virusga qarshi monitoring barcha ishga tushiriluvchi dasturlarni, yaratiluvchi, ochiluvchi va saqlanuvchi xujjatlarni, Internet orqali olingan yoki disketdan yoki har qanday kompakt-diskdan nushalangan dastur va xujjatlarning fayllarini tekshirishga imkon beradi. Agar qandaydir dastur xavfli harakatni qilishga urinmoqchi bo’lsa, virusga qarshi monitor foydalanuvchiga xabar beradi. O’zgarishlarni aniqlovchi usul. Diskni taftish qiluvchi deb ataluvchi ushbu usulni amalga oshirishda virusga qarshi dastur diskning xujumga duchor bo’lishi mumkin bo’lgan barcha sohalarini oldindan xotirlaydi, so’ngra ularni vaqti-vaqti bilan tekshiradi. Virus kompyuterlarni zaharlaganida qattiq disk tarkibini o’zgartiradi: masalan, dastur yoki xujjat fayliga o’zining kodini qo’shib qo’yadi, Autoexec.bat fayliga dastur-virusni chaqirishni qo’shadi, yuklama sektorni o’zgartiradi, faylyo’ldosh yaratadi. Disk sohalari xarakteristikalarining qiymatlari solishtirilganida virusga qarshi dastur ma’lum va no’malum viruslar tomonidan qilingan o’zgarishlarni aniqlashi mumkin. Kompyuterlarning kiritish/chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o’rnatish. Kompyuterlarning tizimli platasiga viruslardan himoyalashning oddiy vositalari o’rnatiladi. Bu vositalar qattiq disklarning bosh yuklama yozuviga hamda disklar va disketlarning yuklama sektorlariga barcha murojaatlarni nazoratlashga imkon beradi. Agar qandaydir dastur yuklama sektorlar tarkibini o’zgartirishga urinsa, himoya ishga tushadi va foydalanuvchi ogohlantiriladi. Ammo bu himoya juda ham ishonchli emas. Virusga qarshi dasturlarning xillari. Virusga qarshi dasturlarning quyidagi xillari farqlanadi: - dastur-faglar (virusga qarshi skanerlar); - dastur-taftishchilar (CRC-skanerlar); - dastur-blokirovka qiluvchilar; - dastur-immunizatorlar. Dr.Web — Rossiyaning virusga qarshi ommaviy dasturi, Windows 9x/NT/2000/XP/7/8 uchun mo’ljallangan bo’lib, faylli, yuklama, va fayl-yuklama viruslarni qidiradi va zararsizlantiradi. AVP (Antivirus Kasperskogo Personal) — Rossiyaning virusga qarshi paketi. Eset Nod32 Antivirus Symantec Antivirus — Symantec kompaniyasining korporativ foydalanuvchilarga taklif etgan virusga qarshi mahsuloti to’plamiAxborot lotincha information so`zidan olingan bo`lib, tushuntirish, biror narsani bayon qilish yoki biror narsa, yoki hodisa haqida ma'lumot ma'nosini anglatadi.Inson yashaydigan dunyo turli moddiy va nomoddiy ob'еktlar, shuningdеk, ular o`rtasidagi o`zaro aloqa va o`zaro ta'sirlardan, ya'ni jarayonlardan tashkil topgan. Sezish a'zolari, turli asboblar va hokazolar yordamida qayd etiladigan tashqi dunyo dalillari ma'lumotlar deb ataladi. Ma'lumotlar aniq vazifalarni hal etishda zarur va foydali deb topilsa - axborotga aylanadi. Demak, ma'lumotlarga u yoki bu sabablarga ko‗ra foydalanilmayotgan yoki texnik vositalarda qayta ishlanilayotgan, saqlanayotgan, uzatilayotgan belgilar yoki yozib olingan kuzatuvlar sifatida qarash mumkin. Agar bu ma'lumotlardan biror narsa to‗g‗risidagi mavhumlikni kamaytirish uchun foydalanish imkoniyati tug‗ilsa, ma'lumotlar axborotga aylanadi. Demak, amaliyotda foydali deb topilgan, ya'ni foydalanuvchining bilimlarini oshirgan ma'lumotlarnigina axborot deb atasa bo‗ladi. Masalan, qog‗ozga telefon raqamlarini ma'lum tartibda yozib, birovga ko`rsatsangiz, u buni ma'lumot sifatida qabul qiladi. Biroq ana shu har bir telefon raqami qarshisiga muayyan korxona yoki tashkilot nomi, uning faoliyat turi yozib qo`yilsa, avvalgi ma'lumot axborotga aylanadi. Ma'lum vazifalarni hal etish natijasida yangi ma'lumotlar - bilimlar, ya'ni tartibga solingan haqqoniy yoki sinovdan o`tgan xabarlar paydo bo`ladi. Ular qonunlar, nazariyalar hamda tasavvur va qarashlarning boshqacha jamlanmasi sifatida umumlashgan bo`ladi. Keyinchalik bu bilimlar o`zga vazifalarni hal etish yoki oldingisini aniqlashtirish uchun zarur bo`lgan ma'lumotlar tarkibiga kiradi.Inson o‗z hayotida doimo ma'lumotlar bilan ish ko‗radi. Ularni o‗zining sezgi a'zolari orqali qabul qiladi. Kundalik turmushimizda biz axborot deganda atrof - muhitdan (tabiatdan yoki jamiyatdan), sezgi a'zolarimiz orqali qabul qilib, anglab oladigan har qanday ma'lumotni tushunamiz. Tabiatni kuzata turib, insonlar bilan muloqotda bo‗lib, kitob va gazetalar o‗qib, televizion ko‗rsatuvlar ko‗rib, biz axborot olamiz. Matematik olim axborotni yanada kengrok tushunadi. U axborot qatoriga fikr yuritish orqali xulosa chiqarish natijasida hosil bo‗lgan bilimlarni ham kiritadi. Boshqa soxa xodimlari ham axborotni o‗zlaricha talqin etadilar. Shunday qilib, turli sohalarda axborot turlicha tushunilar ekan. Lekin axborotlarning umumiy tomonlari ham borki, u ham bo‗lsa beshta muhim xossaga ega bo‗lishligidir. Bular axborotni yaratish, qabul qilish, saqlash, ishlov berish va uzatish xossalaridir. 1. Axborotni dinamik xarakteri. Axborot static ob‘yekt hisoblanmaydi.U ma‘lumotlar va ularni o‗rganish metodlarini o‗zaro ta‘siri natijasida yuzaga keladi va doimo o‗zgarib turadi.Boshqa hamma vaqt u ma‘lumot holida bo‗ladi. Shunday qilib , axborot faqatgina axboriy jarayonning kechishi momentidagina mavjud. 2. Metodlarni adekvatligiga qo„yilgan talablar.Bitta ma‘lumotni o‗zi , uni o‗rganish metodlarini adekvatligi darajasiga qarab turli axborotni berishi mumkin.Masalan xitoy tilini bilmaydigan kishi uchun, Pekindan kelgan xat faqatgina qog‗ozning sifati,rangi, varaqlar soni haqida axborot beradi.Lekin bu xatni mazmunini beruvchi to‗liq axborot emas.Adekvat metoddan foydalanish (xitoy tilini bilish) natijasida boshqa axborot olinadi. 3.Ma‟lumotlar va ularni o„rganish metodlarining o„zaro ta‟sirini dialektik xarakteri. Ma‘lumotlar tashqi dunyo dalillarini registratsiyalash natijasida yuzaga kelgani uchun ular ob‘yektivdir. Ayni vaqtda metodlar subyektiv hisoblanadi Sun‘iy metodlarni asosida turli soha kishilari ( subyektlar ) tomonidan tayyorlangan va tuzilgan algoritmlar yotadi . Tabiiy metodlarni asosida esa subyektlarni biologic hususiyatlari yotadi.Shunday qilib axborot ob‟yektiv ma‟lumot va sub‟yektiv metodlarni o„zaro dialektik ta‟siri momentida yuzaga keladi va mavjud bo„ladi. Axborotning xususiyatlari. Axborotdan foydalanish imkoniyati va samaradorligi uning reprezentativligi, mazmundorligi, yetarliligi, aktualligi, o‗z vaqtidaligi, aniqligi, ishonarliligi, barqarorligi kabi asosiy iste'mol sifat ko‗rsatkichlari bilan bog‗liqdir: 1) axborotning reprezentativligi - ob'ekt xususiyatini adekvat ifoda etish maqsadlarida uni to‗g‗ri tanlash va shakllantirish bilan bog‗liqdir. 2) axborotning mazmundorligi - semantik (mazmuniy) hajmini ifoda etadi. 3) axborotning yetarliligi (to„laligi) - qaror qabul qilish uchun minimal, lekin yetarli tarkibga (ko‗rsatkichlar jamlamasiga) ega ekanligini bildiradi. To‗g‗ri qaror qabul qilish uchun to‗liq bo‗lmagan, ya'ni yetarli bo‗lmagan, xuddi shuningdek, ortiqcha bo‗lgan axborot ham foydalanuvchining qabul qilgan qarorlari samaradorligini kamaytiradi. 4) axborotning aktualligi (dolzarbligi) - axborotdan foydalanish vaqtida uning boshqarish uchun qimmatliligini saqlanib qolishi bilan belgilanadi va uning xususiyatlari, o‗zgarishi dinamikasi hamda ushbu axborot paydo bo‗lgan vaqtdan buyon o‗tgan vaqt oralig‗iga bog‗liq bo‗ladi. 5) axborotning o„z vaqtidaligi - uning avvaldan belgilab qo‗yilgan vazifani hal etish vaqti bilan kelishilgan vaqtdan kechikmasdan olinganligini bildiradi. 6) axborotning aniqligi - olinayotgan axborotning ob'ekt, jarayon, hodisa va hokazolarning real holatiga yaqinligi darajasi bilan belgilanadi. 7) axborotning ishonarliligi - axborotning real mavjud ob'ektlarni zarur aniqlik bilan ifoda etish xususiyati bilan belgilanadi. 8) axborotning barqarorligi - axborotning asos qilib olingan ma'lumotlar aniqligini buzmasdan o‗zgarishlarga ta'sir qilishga qodirligini bildiradi. Ma'lumotlar. Ma'lumotlar - axborotni dialektik tashkil qiluvchi qismi. Informatsion jarayonni borishi davomida ma'lumotlar bir turdan ikkinchi turga o‗tadi. Ma'lumotlarni qayta ishlash turli operatsiyalarni o‗z ichiga oladi. Ma'lumotlar ustida o‗tkaziladigan asosiy operatsiyalarni quyidagi ro‗yxatda keltiramiz: • Ma'lumotlarni yig„ish - qaror qabul qilish uchun yetarli darajada to‗liq ma'lumotga ega bo‗lish maqsadida

• Ma'lumotlarni formallashtirish - turli manba‘lardan olingan ma'lumotlarni , o‗zaro taqqoslash uchun , bir xil formaga keltirish

• Ma'lumotlarni fil‟trlash- qaror qabul qilishga zaruriyati bo‗lmagan "ortiqcha" ma'lumotlarni tushirib qoldirish

• Ma'lumotlarni tartiblash - foydalanish oson bo‗lishi maqsadida

• Ma'lumotlarni arxivlash- ma'lumotlarni saqlashda iqtisodiy tejamkorlikka erishish. • Ma'lumotlarni himoyalash- ma'lumotlarni yo‗qolishi yoki o‗zgarib ketishidan saqlash uchun qilinadigan tadbirlar

• Ma'lumotlarni yuborish- informatikada ma'lumotni qabul qilib oluvchi - klient, ma'lumot manba‘si esa -server deyiladi.

• Ma'lumotlarni shaklini almashtirish-ma'lumotni bir formadan boshqasiga yoki bir strukturadan ikkinchi strukturaga o‗tkazish Ma'lumotlar ustida bajariladigan hamma operatsiyalarni ro‗yxatini keltirib bo‗lmaydi. Va biz shunday xulosaga kelamizki, ma'lumotlar ustida ishlash katta qiyinchilik bilan kechadi, demak bu ishni avtomatlashtirish zarur. Ma'lumotlar ustida ishlashni avtomatlashtirish uchun , turli ma'lumotlarni bir xil formaga keltirish kerak , shu maqsadda ma'lumotlarni kodlash usulidan foydalanishadi. Kodlash vositalari fan va texnikaning ba'zi sohalarida muvaffaqiyat bilan qo‗llanib kelinmoqda.Masalan matematik ifodalarni yozish sistemasi, ko‗rlar uchun Brayl sistemasi, telegraf kodi va boshqalar. Hisoblash texnikasida ham o‗z kodlash sistemasi mavjud bo‗lib, u ma'lumotlarni 0 va 1 belgilar ketma- ketligi ko‗rinishida ifodalashga asoslangan. Bu belgilar ikkilik raqamlari deyilib, ingliz tilidagi ifodasi - binary digit yoki qisqacha bit. Ikki xil tushunchadan birini 0 yoki 1 ( rost yoki yolg‗on, ha yoki yo‗q, oq yoki qora va x.k.) bir bit bilan ifodalanishi mumkin. Agar bitlar miqdorini ikkitagacha oshirsak, u holda to‗rt xil tushunchani ifodalash mumkin 00 01 10 11 Uch bit bilan sakkizta turli tushunchalarni kodlash mumkin: 000 001 010 011 100 101 110 111 Ikkilik kodlash sistemasida razryadlar miqdorini bittaga oshirsak, qiymatlar miqdori ikki baravar ortadi, ya'ni bu sistemada umumiy formula quyidagi ko‗rinishda bo‗ladi: m N=2 Bu yerda N – o‗zaro bog‗liq bo‗lmagan kodlanuvchi qiymatlar miqdori, m - ikkilik kodlash sistemasida qabul qilingan razryad miqdori.

5-mavzu:Virusdan himoyalanish tizimini yaratish.

Shrift - Matnga tegishli xususiyatlarni o’zgartirish. Shu buyruk tanlangandan keyin ekranda qo’yidagi oyna xosil kilinadi. Bu oyna 3 kisimdan iborat: ShRIFT- matn shaklini(shriftini), kurinishini, kattaligini, rangini, chiziklar turini va ular rangini xamda xar xil kushimcha effektlarni (uchirgan xarflar, yukori yoki pastki belgilar, soyali, burtib chikkanva bosilgan xarflar xamda boshka effektlar) urnatish. INTERVAL - matn xarflar enining foizi, ular urtasidagi masofa va satrga karaganda joylanishi (yukoriga yoki pastda) o’zgartirish. ANIMASIYa - matn xarflarini animasion efektlar bilan jixozlash. 2. Абзац - Абзацlarga tegishli xususiyatlarni o’zgartirish. Shu buyruk tanlangandan keyin ekranda qo’yidagi oyna xosil kilinadi. Bu oynadagi : OTSTUPЫ I INTERVALЫ kismi yordamida Абзацni gorizontal joylanishi, chap va ung tomondan koldirilgan masofa, birinchi satr joylanishi, oldingi va 40 keytngi Абзацlar urtasidagi masofa, Абзацning satrlar urtasidagi masofani o’zgartirish. POLOJENIYe NA STRANISE kismi yordamida Абзацning varakadan varakaga va satrdan satrga utishni sozlash.

3. Список - Ruyxatlarni kurinishini ko’rish va o’zgartirish. Shu buyruk tanlangandan keyin ekranda qo’yidagi oyna xosil kilinadi. Bu oynadagi MARKIROVANNЫY kismi yordamida belgili ruyxat kurinishini tanlaymiz. Pastagi RISUNOK va Izmenit tugmalari yordamida belgi kurinishini o’zgartiramiz. NUMEROVANNЫY kismi yordamida rakamli ruyxat kurinishini o’zgartiramiz. MNOGOUROVNEVЫY kismi yordamida esa murakkab ruyxat kurinishini o’zgartiramiz. 4. Granisы i zalivka - Matnga ramkalar va fonlarni (orka ranglarni) urnatish. Bu buyruk bizga tanlangan Абзац yoki varak chegaralarini ramka va rang bilan bezashga imkoniyat beradi. ` Ush bu buyruk dialog oynadagi GRANISA bo’limidan tanlangan Абзацni ramkalash, STRANISA bo’limida varakani ramka bilan bezash mumkin. Bu bo’limlarda ramkalarga chiziklar turini, rangni, kalinligini va tasvirini o’zgartirishimiz mumkin. ZALIVKA bo’limi yordamida yesa Абзац orkasini rang bilan buyash mumkin. 5. Колонкы - Matnni ustunlarini kurinishini o’zgartirish. Shu buyruk tanlangandan keyin ekranda buyruk dialog oyna xosil kilinadi. Ushbu oyna yordamida biz ustunlar sonini, ular enini va urtasidagi masofani tanlashimiz mumkin. 41 Pastki КОЛОНКЫ ODINAKOVOY ShIRINЫ bayrokcha yordamida ustunlarni avtamotik teng kilishimiz mumkin. RAZDELITEL bayrokcha yordamida esa ustunlar urtasida chiziklarni qo’yishimiz mumkin. 6. Tabulyasiya - TAB tugmasi xususiyatlarini o’zgartirish 7. Bukvisa - Абзац birinchi xarfining kurinishini o’zgartirish. 8. Napravleniye teksta - Matnning yozilish yunalinishini o’zgartirish (fakat jadval va ustki yozuvlarda ishlaydi.) 9. Registr - Tanlangan xarflarni registrini (bosh yoki kichik xarflar kurinishi) o’zgartirish. 10. AvtoФормат - Документni tayyor xolatga olib kelish. 11. Biblioteka stiley - Документlarni tayyor xolatlarni ko’rish yoki o’zgartirish. 12. Stil - Dokumetdagi stillarni ko’rish, o’zgartirish va yangilarni yaratish. 13. Fon - Документ varakalarning orka rangini o’zgartirish (fakat VEB ДОКУМЕНТ kurinishida ishlaydi). 14. Obyekt - Tanlangan obyektlarni xususiyatlarini ko’rish. Сервис menyusi komandalarining mazmuni:

1. Орфография. . . - Imlo xatolarini tekshirish tizimini ishga tushiradi.

2. Yazыk - Xatolarni tekshirish tilini o’zgartirish yoki tanlangan suzga sinonim topish.

3. Statistika - Документ xakida umumiy ma’lumotlarni ko’rish.

4. Avtoreferat - Документ matnidan xar xil asosiy satrlarni tanlab olish

5. Avtozamena. . . - Komanda kursatilgan belgilar ketma-ketligini avtomatik ravishda bitta belgigi o’zgartirishni amalga oshiradi. Bu buyruk tanlangandan keyin qo’yidagi dialog oyna xosil kilinadi.

6-mavzu: Virusdan himoyalanish tizimini yaratish.

Bu nima va unga qarshi qanday kurashish kerak? Bu mavzuga o’nlab kitoblar va yuzlab maqolalar yozilgan. Kompyuter viruslariga qarshi minglab professional mutaxassislar ko’plab kompaniyalarda ish olib borishmoqda. Bu mavzu o’ta qiyin va muhimki ko’p e`tiborni talab qilmoqda. Kompyuter virusi ma`lumotni yo’qotish sabablaridan biri va asosiysi bo’lib qolmoqda. Viruslar ko’plab tashkilot va kompaniyalarni ishlarini buzishga olib kelganligi ma`lum. Shunday ma`lumotlar mavjudki, Niderlandiya gospitallaridan birida bemorga kompyuter qo’ygan tashxis bo’yicha iste`mol qilingan dori oqibatida bemor olamdan o’tgan. Bu kompyuter virusining ishi bo’lgan. E`tiborsizlik bilan qilingan ishdan kompyuter tezda virus bilan zararlanadi. Inson kasallik virusi bilan zararlansa issiqligi o’zgarishi, vazni o’zgarishi, xolsizlanish va og’riqning paydo bo’lishi ko’zda tutiladi. Kompyuter virusi bilan zararlangan kompyuterlarda quyidagilar kuzatiladi: dasturlarning ishlashining sekinlashishi, fayllarni hajmi o’zgaradi, g’ayritabiiy va ba`zi bir noma`lum xatoliklar, ma`lumotlar va sistema fayllari yo’qotilishi. Ba`zi viruslar zararsiz ko’payadi, lekin qo’rqinchli emas. Bu viruslar ekranga xato ma`lumot chiqaradi. Ammo, bir turdagi viruslar hujum qiluvchi, ya`ni, yomon asoratlar qoldiruvchi hisoblanadi. Masalan, viruslar qattik diskdagi ma`lumotlarni o’chirib tashlaydi. Virus nima? Virus(Virus) inglizcha ―yuqumli boshlanish‖, ―yomon boshlanish – buzuvchi boshlanish‖, ―yuqumli kasal‖ degan ma`nolarni anglatadi. Mashxur «doktor» lardan biri D.N.Lozinskiy virusni kotibaga o’xshatadi. Tartibli kotibani faraz qilsak, u ishga keladi va stolidagi bir kunda qilishi kerak bo’lgan ishlarni - qog’ozlar qatlamini ko’radi. U bir varog’ni ko’paytirib bir nusxasini o’ziga ikkinchisini keyingi qo’shni stolga qo’yadi. Keyingi stoldagi kotiba ham kamida ikki nusxada ko’paytirib, yana bir kotibaga o’tkazadi. Natijada kontoradagi birinchi nusxa bir necha nusxalarga aylanadi. Ba`zi nusxalar yana ko’payib boshqa stollarga ham o’tishi mumkin. Kompyuter viruslari taxminan shunday ishlaydi, Faqat qog’ozlar o’rnida endi dasturlar, kotiba bu - kompyuter. Birinchi buyruq «ko’chirish-nusxa olish» bo’lsa, kompyuter buni bajaradi va virus boshqa dasturlarga o’tib oladi. Agar kompyuter biror zararlangan dasturni ishga tushirsa virus boshqa dasturlarga tarqalib borib butun kompyuterni egallashi mumkin. Agar bir dona virusning ko’payishiga 30 sekund vaqt ketsa, bir soatdan keyin bu 1000000000 dan ortib ketishi mumkin. Aniqrog’i kompyuter xotirasidagi bo’sh joylarni band qilishi mumkin. - 33 - Xuddi shunday voqea 1988 yili Amerikada sodir bo’lgan. Global tarmoq orqali uzatilayotgan ma`lumot orqali virus bir kompyuterdan boshqasiga o’tib yurgan. Bu virus Morris virusi deb atalgan. Ma`lumotlarni virus qanday yo’q qilishi mumkin degan savolga shunday javob berish mumkin: Virus nusxalari boshqa dasturlarga tez ko’payib o’tib oladi; Kalendar bo’yicha 13-sana juma kunga to’g’ri kelsa hamma xujjatlarni yo’q qiladi. Buni hammaga ma`lum «Jerusalem» («Time» virusi ham deb ataladi) virusi juda «yaxshi» amalga oshiradi. Ko’p xollarda bilib bo’lmaydi, virus qayerdan paydo bo’ldi. Virusni aniqlanishi shundaki, u kompyuter sistemasida joylashib va ko’payib borishiga bog’lik. Misol uchun, nazariy jihatdan operatsion sistemada virus davolab bo’lmaydi. Bajaruvchi kodning sohasini tuzish va o’zgartirish ta`qiqlangan sistema misol bo’lishi mumkin. Virus hosil bo’lishi uchun bajariluvchi kodlar ketma-ketligi ma`lum bir sharoitda shakllanishi kerak. Kompyuter virusining xossalaridan biri o’z nusxalarini kompyuter tarmoqlari orqali bajariluvchi obyektlarga ko’chiradi. Bu nusxalar ham o’z-o’zidan ko’payish imkoniyatiga ega.Biologik viruslardan farqli o’laroq, kompyuter viruslarini inson tomonidan tuziladi. Viruslar kompyuter foydalanuvchilariga katta zarar yetkazadi. Ular kompyuter ishini to’xtatadi yoki qattiq diskdagi ma`lumotlarni o’chiradi. Virus sistemaga bir necha yo’llar bilan tushishi mumkin: ma’lumot tashuvchi qurilmalar, dasturiy ta`minot yuklangan CD-ROM, tarmoq interfeysi yoki modemli bog’lanish, global Internet; tarmog’idagi elektron pochta. Ma’lumot tashuvchi qurilma virusdan zararlanishi oson. Zararlangan kompyuterga ma’lumot tashuvchi qurilmani solib o’qitilganda diskning bosh sektoriga virus tushadi. Internet ma`lumotlar almashinishiga katta imkoniyat yaratadi. Lekin, kompyuter viruslari va zararli dasturlar tarqalishi uchun yaxshi muhit yaratadi. Albatta Internetdan olingan barcha ma`lumotlarda virus bor deb bo’lmaydi. Kompyuterda ishlovchi ko’pchilik mutaxassislar va operatorlar qabul qilinadigan ma`lumotlarni viruslardan tekshirishni doimo bajaradi. Internet da ishlayotgan har bir kishi uchun yaxshi antivirus himoya zarur. «Kasperskiy laboratoriyasi» texnik ta`minot xizmati statistikasiga ko’ra, viruslardan zararlangan xolatlarning 85% i elektron pochta orqali sodir bo’lgan. 1999 yilga nisbatan xozirgi kunda bu ko’rsatkich 70 % tashkil etadi. «Kasperskiy laboratoriyasi» elektron pochtalarga yaxshi antivirus himoyasi kerakligini ta`kidlaydi. Virus tuzuvchilarga elektron pochta juda qulay. Amaliyot shuni ko’rsatadiki, ommabop dasturlar, operatsion sistemalar, ma`lumotlarni uzatish texnologiyalari uchun viruslar ko’plab tuzilmoqda. Xozirda elektron pochta biznes va boshqa sohalarda muloqot uchun asosiy vosita bo’lib qolmoqda. Shuning uchun virus tuzuvchilari elektron pochtaga diqqatini qaratmoqda. - 34 - Kompyuter virusining ko’p ta’riflari mavjud. Birinchi ta’rifni 1984 yili Fred Koen bergan: "Kompyuter virusi - boshqa dasturlarni, ularga o’zini yoki o’zgartirilgan nusxasini kiritish orqali, ularni modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko’payish qobiliyatini saqlaydi". Virusning o’z-o’zidan ko’payishi va hisoblash jarayonini modifikatsiyalash qobiliyati bu ta’rifdagi tayanch tushunchalar hisoblanadi. Kompyuter virusining ushbu xususiyatlari tirik tabiat organizmlarida biologik viruslarning parazitlanishiga o’hshash. Hozirda kompyuter virusi deganda quyidagi xususiyatlarga ega bo’lgan dasturiy kod tushuniladi: - asliga mos kelishi shart bo’lmagan, ammo aslining xususiyatlariga (o’z-o’zini tiklash) ega bo’lgan nusxalarni yaratish qobiliyati; - hisoblash tizimining bajariluvchi ob’ektlariga yaratiluvchi nusxalarning kiritilishini ta’minlovchi mexanizmlarning mavjudligi. Ta’kidlash lozimki, bu xususiyatlar zaruriy, ammo yetarli emas. Ko’rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta’sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to’ldirish lozim. Viruslarni quyidagi asosiy alomatlari bo’yicha turkumlash mumkin: - yashash makoni; - operatsion tizim; - ishlash algoritmi xususiyati; - destruktiv imkoniyatlari. Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo’yicha turkumlash asosiy va keng tarqalgan turkumlash hisoblanadi.

7-mavzu: Huquqiy axborot tushunchasi.

Axborotning muximlik darajasi qadim zamonlardan ma’lum. SHuning uchun xam qadimda axborotni himoyalash uchun turli xil usullar qo’llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o’qiy olmagan. Asrlar davomida bu san’at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o’n yil oldin hamma narsa tubdan o’zgardi, ya’ni axborot o’z qiymatiga ega bo’ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o’g’irlaydilar, buzib talqin etadilar va soxtalashtiradilar. SHunday qilib, axborotni himoyalash zaruriyati tug’iladi. Axborotni qayta ishlash sanoatining paydo bo’lishi axborotni himoyalash sanoatining paydo bo’lishiga olib keladi. Xavfsizlikning asosiy yo’nalishlari Axborot xavfsizligi. Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo’llanilmoqda (iqtisod, fan, ta’lim, xarbiy ish, turli texnologiyalarni boshqarish va x.k.) Iqtisodiy xavfsizlik. Milliy iqtisodda axborotlarni yaratish, tarqatish, qayta ishlash va foydalanish jarayoni hamda vositalarini qamrab olgan Yangi tarmoq vujudga keldi. «Milliy axborot resursi» tushunchasi Yangi iqtisodiy kategoriya bo’lib xizmat qilmoqda. Davlatning axborot resurslariga keltirilayotgan zarar axborot xavfsizligiga xam ta’sir ko’rsatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakllantirish va uning asosida jahon yagona axborot maydoniga kirib borish natijasida milliy iqtisodimizga turli xildagi zararlar keltirish xavfi paydo bo’lmoqda. Mudofaa xavfsizligi. Mudofaa sohasida xavfsizlikning asosiy ob’ektlaridan bo’lib, mamlakatning mudofaa potentsialining axborot tarkibi va axborot resurslari hisoblanmoqda. Xozirgi kunda barcha zamonaviy qurollar va harbiy texnikalar juda ham kompyuterlashtirilib yuborildi. SHuning uchun xam ularga axborot qurollarini qo’llash ehtimoli katta. Ijtimoiy xavfsizlik. Zamonaviy axborot – kommunikatsiyalar texnologiyalarining milliy iqtisod barcha tarmoqlarida keng qo’llanishi inson psixologiyasi va jamoa ongiga «yashirin» ta’sir ko’rsatish vositalarining samaradorligini yuksaltirib yubordi. - 7 - Ekologik xavfsizlik. Ekologik xavfsizlik – global masshtabdagi muammodir. «Ekologik toza», energiya va resurs tejaydigan, chiqindisiz texnologiyalarga o’tish faqat milliy iqtisodni axborotlashtirish hisobiga qayta qurish asosidagina yo’lga qo’yish mumkin. Avtomatlashtiriltan axborot tizimlarida axborotlar o’zining hayotiy davriga ega bo’ladi. Bu davr uni yaratish, undan foydalanish va kerak bo’lmaganda yo’qotishdan iboratdir (2-rasm ). Axborotlar xayotiy davrining xar bir bosqichida ularning himoyalanganlik darajasi turlicha baholanadi. Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muxim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulki huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshha moddiy hamda nomoddiy zararlar keltirishi mumkin bo’lgan turli kirishlar va o’g’irlashlardan himoyalashdir. 2-rasm Axborot xavfsizligi deb, ma’lumotlarni yo’qotish va o’zgartirishga yo’naltirilgan tabiiy yoki sun’iy xossali tasodifiy va qasddan ta’sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi. Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va xujjatlarni o’g’irlash yoki nusxa olishdan iborat bo’lsa, hozirgi paytdagi xavf esa kompyuter ma’lumotlari to’plami, elektron ma’lumotlar, elektron massivlardan ularning egasidan ruxsat so’ramasdan foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi. Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, Axborotning hayotiy davri Axborotni saqlash va arxivlash So’rovlar bo’yicha axborotlarni tanlash Axborotni qayta ishlash Saqlash uchun axborotlarni tizimlashtirish, tartibga solish va o’girish Axborotdan foydalanish Olingan axborot Axborotlarni foydaliligi va aniqligi bo’yicha baholash Hisobot ma’lumotlari Birlamchi axborot Axborotlarni yangilab turish Eski axborotlarni yo’kotish .

8-mavzu: Huquq sohasidagi axborot jarayonlari.

Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar yetkazmokchi bo’lgan nohuquqiy muomaladan xar qanday xujjatlashtirilgan, ya’ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan xolda moddiy jismda qayd etilgan axborot ximoyalanishi kerak. Axborot xavfsizligi nuktai nazaridan axborotni quyidagicha turkumlash mumkin: • maxfiylik — aniq bir axborotga fakat tegishli shaxslar doirasigina kirishi mumkinligi, ya’ni foydalanilishi qonuniy xujjatlarga muvofik cheklab qo’yilib, xujjatlashtirilganligi kafolati. Bu bandning buzilishi o’g’irlik yoki axborotni oshkor qilish, deyiladi; • konfidentsiallik — inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; • yaxlitlik — axborot boshlang’ich ko’rinishda ekanligi, ya’ni uni saqlash va uzatishda ruxsat etilmagan o’zgarishlar qilinmaganligi kafolati; bu bandning buzilishi axborotni soxtalashtirish deyiladi; • autentifikatsiya — axborot zaxirasi egasi deb e’lon qilingan shaxs xaqiqatan xam axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi; • apellyatsiya qilishlik — yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo’llaniladi. Kerak bo’lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati. Yukoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin: • ishonchlilik — tizim meyoriy va g’ayri tabiiy xollarda rejalashtirilganidek o’zini tutishlik kafolati; • aniqlilik — xamma buyruqlarni aniq va to’liq bajarish kafolati; • tizimga kirishni nazorat qilish — turli shaxs guruxlari axborot manbalariga xar xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati; • nazorat qilinishi — istalgan paytda dastur majmuasining xoxlagan kismini tulik tekshirish mumkinligi kafolati; • identifikatsiyalashni nazorat qilish — xozir tizimga ulangan mijoz aniq o’zini kim deb atagan bulsa, aniq o’sha ekanligining kafolati; • qasddan buzilishlarga to’sqinlik — oldindan kelishilgan me’yorlar chegarasida qasddan xato kiritilgan ma’lumotlarga nisbatan tizimning oldindan kelishilgan xolda o’zini tutishi. Axborotni ximoyalashning maqsadlari kuyidagilardan iborat: - axborotning kelishuvsiz chikib ketishi, ugirlanishi, yo’qotilishi, o’zgartirilishi, soxtalashtirilishlarning oldini olish; - shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf – xatarning oldini olish; - axborotni yo’q qilish, o’zgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish; - xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta’minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish; - 9 - - axborot tizimida mavjud bulgan shaxsiy ma’lumotlarning shaxsiy maxfiyligini va konfidentsialligini saklovchi fukarolarning konstitutsion xukuklarini ximoyalash; - davlat sirini, konunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saklash; - axborot tizimlari, texnologiyalari va ularni ta’minlovchi vositalarni yaratish, ishlab chikish va kullashda sub’ektlarning xukuklarini ta’minlash.

9-mavzu: Huquq sohasidagi axborotlashtirish borasidagi davlat siyosatining vazifalari.

Tarmoq texnologiyalari rivojining boshlang’ich bosqichida viruslar va kompyuter xujumlarining boshqa turlari ta’siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bog’liqligi katta emas edi. Hozirda, xujumlar sonining doimo o’sishi hamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bog’liqligi sharoitida mashina vaqtining yo’qolishiga olib keluvchi hatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi. Misol tariqasida keltirish mumkinki, faqat 2003 yilning birinchi choragida dunyo miqyosidagi yo’qotishlar 2002 yildagi barcha yo’qotishlar yig’indisining 50%ini tashkil etgan, yoki bo’lmasa 2006 yilning o’zida Rossiya Federeatsiyasida 14 mingdan ortiq kompyuter jinoyatchiligi holatlari qayd etilgan. Korporativ tarmoqlarda ishlanadigan axborot, ayniqsa, zaif bo’ladi. Hozirda ruxsatsiz foydalanishga yoki axborotni modifikatsiyalashga, yolg’on axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo’ladi: - kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot hajmining oshishi; - ma’lumotlar bazasida muhimlik va mahfiylik darajasi turli bo’lgan axborotlarning to’planishi; - ma’lumotlar bazasida saqlanayotgan axborotdan va hisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi; - masofadagi ishchi joylar soninig oshishi; - foydalanuvchilarni bog’lash uchun Internet global tarmog’ini va aloqaning turli kanallarini keng ishlatish; - foydaluvchilar kompyuterlari o’rtasida axborot almashinuvining avtomatlashtirilishi. Axborot xavfsizligiga tahdid deganda axborotning buzilishi yoki yo’qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan harakatlar tushuniladi. Oldindan shuni aytish mumkinki, so’z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommertsiya qiymatiga ega bo’lgan qismi xususida ketyapti. Zamonaviy korporativ tarmoqlar va tizimlar duchor bo’ladigan keng tarqalgan tahdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlikka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi manba) bo’lishi mumkin. Bunday ajratish to’g’ri, chunki bitta tahdid uchun (masalan, o’g’irlash) tashqi va ichki manbalarga qarshi harakat usullari turlicha bo’ladi. Bo’lishi - 10 - mumkin bo’lgan tahdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta’minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi. Tez-tez bo’ladigan va xavfli (zarar o’lchami nuqtai nazaridan) tahdidlarga foydalanuvchilarning, operatorlarning, ma’murlarning va korporativ axborot tizimlariga xizmat ko’rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba’zida bunday xatoliklar (noto’g’ri kiritilgan ma’lumotlar, dasturdagi xatoliklar sabab bo’lgan tizimning to’xtashi yoki bo’zilishi) to’g’ridan to’g’ri zararga olib keladi. Ba’zida ular niyati buzuq odamlar foydalanishi mumkin bo’lgan nozik joylarni paydo bo’lishiga sabab bo’ladi. Global axborot tarmog’ida ishlash ushbu omilning yetarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo’lishi mumkin, oxirgisi ayniqsa xavfli. Zarar o’lchami bo’yicha ikkinchi o’rinni o’g’irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishlash rejimlari va himoyalash choralari bilan a’lo darajada tanish bo’lgan tashkilot shtatidagi xodimlar aybdor bo’lib chiqdilar. Global tarmoqlar bilan bog’langan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan yetarlicha nazorat yo’qligi bunday faoliyatga qo’shimcha imkon yaratadi. Xafa bo’lgan xodimlar (hatto sobiqlari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon yetkazishlari mumkin. Xodim ishdan bo’shaganida uning axborot resurslaridan foydalanish xuquqi bekor qilinishi nazoratga olinishi shart. Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo’lishi mumkin bo’lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo’lib tuyulmasa ham, Internetda ishlash tajribasi ko’rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga duchor bo’lar ekan. Xavf-xatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog’i kompyuterlarining xujumlarga qarshi turishi yoki bo’lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko’rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan sasofadan foydalanish xollari alohida ko’rilishi lozim. Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti duchor bo’ladigan xavf-xatar baholanishi va zarur choralar ko’rilishi zarur. Ravshanki, himoyaga tahdidni nazoratlash va zarur choralarni ko’rish uchun tashkilotning sarfharajati tashkilotda aktivlar va resurslarni himoyalash bo’yicha hech qanday choralar ko’rilmaganida kutiladigan yo’qotishlardan oshib ketmasligi shart. Umuman olganda, tashkilotning kompyuter muhiti ikki xil xavf-xatarga duchor bo’ladi:

1. Ma’lumotlarni yo’qotilishi yoki o’zgartirilishi.

2. Servisning to’xtatilishi. Tahdidlarning manbalarini aniqlash oson emas. Ular niyati buzuq odamlarning bostirib kirishidan to kompyuter viruslarigacha turlanishi mumkin. Bunda inson xatoliklari xavfsizlikka jiddiy tahdid hisoblanadi.

korporativ axborot tizimida xavfsizlikning buzilish manbalari bo’yicha statistik ma’lumotlarni tasvirlovchi aylanma diagramma keltirilgan.

10-mavzu:O’zbekiston Respublikasi hamda MDH ga a’zo davlatlarning yagona huquqiy –xaborot maydononi yaratish.

Kompyuter jinoyatchiligi statistikasi tahlil etilsa qayg’uli manzaraga ega bo’lamiz. Kompyuter jinoyatchiligi yetkazgan zararni narkotik moddalar va qurollarning noqonuniy aylanishidan olingan foydaga qiyoslash mumkin. Faqat AQSHda "elektron jinoyatchilar" yetkazgan har yilgi zarar qariyb 100 mld. dollarni tashkil etar ekan. Yaqin kelajakda jinoiy faoliyatning bu turi daromadliligi, pul mablag’larining aylanishi va unda ishtirok etuvchi odamlar soni bo’yicha yaqin vaqtlargacha noqonuniy faoliyat orasida daromadligi bilan birinchi o’rinni egallagan noqonuniy biznesning uch turidan uzib ketish ehtimolligi katta. Bu noqonuniy bizneslar-narkotik moddalar, qurol va kam uchraydigan yovvoyi hayvonlar bilan savdo qilish. Davlat va xususiy kompaniyalar faoliyatining sotsiologik tadqiqi ma’lumotlariga qaraganda XXI asrning birinchi yillarida iqtisodiy sohadagi jinoyatchilik bank va boshqa tizimlarning axborot- kommunikatsion komplekslariga bo’lishi mumkin bo’lgan g’arazli iqtisodiy harakatlarga qaratilgan bo’ladi. Kredit-moliya sohasidagi kompyuter jinoyatchiligining soni muttasil o’sib bormoqda. Masalan onlayn magazinlarida 25%gacha qalloblik to’lov amallari qayd etilgan. SHunga qaramasdan G’arb davlatlarida elektron tijoratning-yuqori daromadli zamonaviy biznesning faol rivojlanishi ko’zga tashlanmoqda. Ma’lumki, bu soha rivojlanishi bilan parallel ravishda "virtual" qalloblarning ham daromadi oshadi. Qalloblar endi yakka holda harakat qilmaydilar, ular puxtalik bilan tayyorlangan, yaxshi texnik va dasturiy qurollangan jinoiy guruhlar bilan, bank xizmatchilarining o’zlari ishtirokida ishlaydilar. Xavfsizlik sohasidagi mutaxassislarning ko’rsatishicha bunday jinoyatchilarning ulushi 70%ni tashkil etadi. "Virtual" o’g’ri o’zining hamkasbi-oddiy bosqinchiga nisbatan ko’p topadi. Undan tashqari "virtual" jinoyatchilar uyidan chiqmasdan harakat qiladilar. Foydalanishning elektron vositalarini ishlatib qilingan o’g’rilik zararining o’rtacha ko’rsatkichi faqat AQSHda bankni qurolli bosqinchilikdan kelgan zararning o’rtacha statistik zararidan 6-7 marta katta. Bank xizmati va moliya amallari sohasidagi turli xil qalloblik natijasida yo’qotishlar 1989 yili 800 mln. dollardan 1997 yili — 100 mlrd. dollarga yetgan. Bu ko’rsatkichlar o’sayapti, aslida yuqorida keltirilgan ma’lumotlardan bir tartibga oshishi mumkin. CHunki ko’p yo’qotishlar aniqlanmaydi yoki e’lon qilinmaydi. O’ziga xos "indamaslik siyosati"ni tizim ma’murlarining o’zining tarmog’idan ruxsatsiz foydalanganlik tafsilotini, bu noxush xodisaning takrorlanishidan qo’rqib va o’zining himoya usulini oshkor etmaslik vajida muhokama etishni xoxlamasliklari bilan tushunish mumkin. Kompyuter ishlatiladigan inson faoliyatining boshqa sohalarida ham vaziyat yaxshi emas. Yildan-yilga xuquqni muhofaza qiluvchi organlariga kompyuter jinoyatchiligi xususidagi murojaatlar oshib bormoqda. Barcha mutaxassislar viruslarning tarqalishi bilan bir qatorda tashqi xujumlarning keskin oshganligini e’tirof etmoqdalar. Ko’rinib turibdiki, kompyuter jinoyatchiligi - 16 - natijasida zarar qat’iy ortmoqda. Ammo kompyuter jinoyatchiligi ko’pincha "virtual" qalloblar tomonidan amalga oshiriladi deyish haqiqatga to’g’ri kelmaydi. Hozircha kompyuter tarmoqlariga suqilib kirish xavfi har biri o’zining usuliga ega bo’lgan xakerlar, krakerlar va kompyuter qaroqchilari tomonidan kelmoqda. Xakerlar, boshqa kompyuter qaroqchilaridan farqli holda, ba’zida, oldindan, maqtanish maqsadida kompyuter egalariga ularning tizimiga ki-rish niyatlari borligini bildirib qo’yadilar. Muvaffaqiyatlari xususida Internet saytlarida xabar beradilar. Bunda xaker musobaqalashuv niyatida kirgan kompyuterlariga zarar yetkazmaydi. Krakerlar (cracker) — elektron "o’g’rilar" manfaat maqsadida dasturlarni buzishga ixtisoslashganlar. Buning uchun ular Internet tarmog’i bo’yicha tarqatiluvchi buzishning tayyor dasturlaridan foydalanadilar. Kompyuter qaroqchilari — raqobat qiluvchi firmalar va xatto ajnabiy maxsus xizmatlari buyurtmasi bo’yicha axborotni o’g’irlovchi firma va kompaniyalarning yuqori malakali mutaxassislari. Undan tashqari ular begona bank schetidan pul mablag’larini o’g’irlash bilan ham shug’ullanadilar. Ba’zi "mutaxassislar" jiddiy guruh tashkil qiladilar, chunki bunday kriminal biznes o’ta daromadlidir. Bu esa tez orada, "virtual" jinoyatning zarari jinoyat biznesining an’anaviy xilidagi zarardan bir tartibga (agar ko’p bo’lmasa) oshishiga sabab bo’ladi. Hozircha bunday tahdidni betaraflashtirishning samarali usullari mavjud emas.

11-mavzu: Axborotlashtirish sharoitlarida axborot sohasidagi huquq va erkinliklarini himoya qilish.

Axborot xavfsizligining siyosatini ishlab chiqishda, avvalo himoya qilinuvchi ob’ekt va uning vazifalari aniqlanadi. So’ngra dushmanning bu ob’ektga qiziqishi darajasi, hujumning ehtimolli turlari va ko’riladigan zarar baholanadi. Nihoyat, mavjud qarshi ta’sir vositalari yetarli himoyani ta’minlamaydigan ob’ektning zaif joylari aniqlanadi. Samarali himoya uchun har bir ob’ekt mumkin bo’lgan tahdidlar va xujum turlari, maxsus instrumentlar, qurollar va portlovchi moddalarning ishlatilishi ehtimolligi nuqtai nazaridan baholanishi zarur. Ta’kidlash lozimki, niyati buzuq odam uchun eng qimmatli ob’ekt uning e’tiborini tortadi va ehtimolli nishon bo’lib xizmat qiladi va unga qarshi asosiy kuchlar ishlatiladi. Bunda, xavfsizlik siyosatining ishlab chiqilishida yechimi berilgan ob’ektning real himoyasini ta’minlovchi masalalar hisobga olinishi lozim. Qarshi ta’sir vositalari himoyaning to’liq va eshelonlangan kontseptsiyasiga mos kelishi shart. Bu degani, qarshi ta’sir vositalarini markazida himoyalanuvchi ob’ekt bo’lgan kontsentrik doiralarda joylashtirish lozim. Bu holda dushmanning istalgan ob’ektga yo’li himoyaning eshelonlangan tizimini kesib o’tadi. Mudofaaning har bir chegarasi shunday tashkil qilinadiki, qo’riqlash xodimining javob choralarini ko’rishiga yetarlicha vaqt mobaynida xujumchini ushlab turish imkoni bo’lsin. - 17 - So’nggi bosqichda qarshi ta’sir vositalari qabul qilingan himoya kontseptsiyasiga binoan birlashtiriladi. Butun tizim hayoti tsiklining boshlang’ich va kutiluvchi umumiy narxini dastlabki baholash amalga oshiriladi. Agar bir binoning ichida turli himoyalash talablariga ega bo’lgan ob’ektlar joylashgan bo’lsa, bino otseklarga bo’linadi. SHu tariqa umumiy nazoratlanuvchi makon ichida ichki perimetrlar ajratiladi va ruxsatsiz foydalanishdan ichki himoya vositalari yaratiladi. Perimetr, odatda, fizik to’siqlar orqali aniqlanib, bu to’siqlardan o’tish elektron usul yoki qo’riqlash xodimlari tomonidan bajariluvchi maxsus muolajalar yordamida nazoratlanadi. Umumiy chegaraga yoki perimetrga ega bo’lgan binolar guruhini himoyalashda nafaqat alohida ob’ekt yoki bino, balki uning joylanish joyi ham hisobga olinishi zarur. Ko’p sonli binolari bo’lgan yer uchastkalari xavfsizlikni ta’minlash bo’yicha umumiy yoki qisman mos keladigan talablarga ega bo’ladi, ba’zi uchastkalar esa perimetr bo’yicha to’siqqa va yagona yo’lakka ega. Umumiy perimetr tashkil etib, har bir binodagi himoya vositalarini kamaytirish va ularni faqat xujum qilinishi ehtimoli ko’proq bo’lgan muhim ob’ektlarga o’rnatish mumkin. Xuddi shu tariqa uchastkadagi har bir imorat yoki ob’ekt xujumchini ushlab qolish imkoniyati nuqtai nazaridan baholanadi. Yuqoridagi keltirilgan talablar tahlili ko’rsatadiki, ularning barchasi axborotni ishlash va uzatish qurilmalaridan xuquqsiz foydalanish, axborot eltuvchilarini o’g’irlash va sabotaj imkoniyatini yo’l qo’ymaslikka olib keladi. Binolar, imoratlar va axborot vositalarining xavfsizlik tizimini nazorat punktlarini bir zonadan ikkinchi zonaga o’tish yo’lida joylashtirgan holda kontsentrik halqa ko’rinishida tashkil etish maqsadiga muvofiq hisoblanadi. Axborot xizmati binolari va xonalariga kirishning nazorati masalasiga kelsak, asosiy chora-nafaqat bino va xonalarni, balki vositalar kompleksini, ularning funktsional vazifalari bo’yicha ajratish va izolyatsiyalash. Bino va xonalarga kirishni nazoratlovchi avtomatik va noavtomatik tizimlar ishlatiladi. Nazorat tizimi kunduzi va kechasi kuzatish vositalari bilan to’ldirilishi mumkin. Xavfsizlikning fizik vositalarini tanlash himoyalanuvchi ob’ektning muhimligini, vositalarga ketadigan harajatni va nazorat tizimi ishonchliligi darajasini, ijtimoiy jihatlarni va inson nafsi buzuqligini oldindan o’rganishga asoslanadi. Barmoq, kaftlar, ko’z to’r pardasi, qon tomirlari izlari yoki nutqni aniqlash kabi biometrik indentifikatsiyalash ishlatilishi mumkin. SHartnoma asosida texnik vositalarga xizmat - 18 - ko’rsatuvchi xodimlarni ob’ektga kiritishning maxsus rejimi ko’zda tutilgan. Bu shaxslar identifikatsiyalanganlaridan so’ng ob’ektga kuzatuvchi hamrohligida kiritiladi. Undan tashqari ularga aniq kelish rejimi, makoniy chegaralanish, kelib-ketish vaqti, bajaradigan ish xarakteri o’rnatiladi. Nihoyat, bino perimetri bo’yicha bostirib kirishni aniqlovchi turli datchiklar yordamida kompleks kuzatish o’rnatiladi. Bu datchiklar ob’ektni qo’riqlashning markaziy posti bilan bog’langan va bo’lishi mumkin bo’lgan bostirib kirish nuqtalarini, ayniqsa ishlanmaydigan vaqtlarda, nazorat qiladi. Vaqti-vaqti bilan eshiklar, romlar, tom, ventilyatsiya tuynuklari va boshqa chiqish yo’llarining fizik himoyalanish ishonchliligini tekshirib turish lozim. Har bir xonaga ichidagi narsaning muhimliligiga bog’liq foydalanish tizimiga ega bo’lgan zona sifatida qaraladi. Kirish-chiqish xuquqi tizimi shaxs yoki ob’ekt muhimligiga bog’liq holda selektsiyali va darajalari bo’yicha rutbalangan bo’lishi shart. Kirish-chiqish xuquqi tizimi markazlashgan bo’lishi mumkin (ruxsatlarni boshqarish, jadval va kalendar rejalarining rejalashtirilishi, kirish-chiqish xuquqining yozma namunalari va h.). Nazorat tizimini vaqti-vaqti bilan tekshirib turish va uni doimo ishga layoqatli holda saqlash lozim. Buni ixtisoslashgan bo’linmalar va nazorat organlari ta’minlaydi. SHaxsiy kompyuter va fizikaviy himoya vositalari kabi o’lchamlari kichik asbobuskunalarni ko’zda tutish mumkin. Yuqorida keltirilganlarga xulosa qilib, kompyuter tarmoqlarini himoyalashda axborot xavfsizligi siyosati qanday aniqlanishi xususida so’z yuritamiz. Odatda ko’p sonli foydalanuvchilarga ega bo’lgan korporativ kompyuter tarmoqlari uchun maxsus "Xavfsizlik siyosati" deb ataluvchi, tarmoqda ishlashni ma’lum tartib va qoidalarga bo’ysindiruvchi (reglamentlovchi) hujjat tuziladi. Siyosat odatda ikki qismdan iborat bo’ladi: umumiy printsiplar va ishlashning muayyan qoidalari. Umumiy printsiplar Internetda xavfsizlikka yondashishni aniqlasa, qoidalar nima ruxsat etilishini va nima ruxsat etilmasligini belgilaydi. Qoidalar muayyan muolajalar va turli qo’llanmalar bilan to’ldirilishi mumkin. Himoyaga qo’yiladigan talablarning asosini tahdidlar ro’yxati tashkil etadi. Bunday talablar o’z navbatida himoyaning zaruriy vazifalari va himoya vositalarini aniqlaydi. Demak, kompyuter tarmog’ida axborotni samarali himoyasini ta’minlash uchun himoya tizimini loyihalash va amalga oshirish uch bosqichda amalga oshirilishi kerak. - xavf-xatarni taxlillash; - xavfsizlik siyosatini amalga oshirish; - xavfsizlik siyosatini madadlash. Birinchi bosqichda kompyuter tarmog’ining zaif elementlari taxlillanadi, tahdidlar aniqlanadi va baholanadi, himoyaning optimal vositalari tanlanadi. Xavfxatarni taxlillash xavfsizlik siyosatini qabul qilish bilan tugallanadi. Ikkinchi bosqich — xavfsizlik siyosatini amalga oshirish moliyaviy xarajatlarni hisoblash va masalalarni yechish uchun mos vositalarni tanlash bilan boshlanadi. Bunda tanlangan vositalar ishlashining ixtilofli emasligi, vositalarni yetkazib beruvchilarning obro’si, himoya mexanizmlari va beriladigan kafolatlar xususidagi to’la axborot olish - 19 - imkoniyati kabi omillar hisobga olinishi zarur. Undan tashqari, axborot xavfsizligi bo’yicha asosiy qoidalar aks ettirilgan printsiplar hisobga olinishi kerak. Uchinchi bosqich — xavfsizlik siyosatini madadlash bosqichi eng muhim hisoblanadi. Bu bosqichda o’tkaziladigan tadbirlar niyati buzuq odamlarning tarmoqqa bostirib kirishini doimo nazorat qilib turishni, axborot ob’ektini himoyalash tizimidagi "rahna"larni aniqlashni, konfidentsial ma’lumotlardan ruxsatsiz foydalanish hollarini hisobga olishni talab etadi. Tarmoq xavfsizligi siyosatini madadlashda asosiy javobgarlik tizim ma’muri bo’ynida bo’ladi. U xavfsizlikning muayyan tizimi buzilishining barcha xollariga operativ munosabat bildirishi, ularni taxlillashi va moliyaviy vositalarning maksimal tejalishini hisobga olgan holda himoyaning zaruriy apparat va dasturiy vositalaridan foydalanishi shart.

12-mavzu: Axborot xavsizligi sohasidagi munosabatlarni huquqiy tartibga solishning tuzilmasi.

Kompyuter tizimida ro’yxatga olingan har bir sub’ekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma’noda indentifikatsiyalovchi axborot bog’liq. Bu ushbu sub’ektga nom beruvchi son yoki simvollar satri bo’lishi mumkin. Bu axborot sub’ekt indentifikatori deb yuritiladi. Agar foydalanuvchi tarmoqda ro’yxatga olingan indentifikatorga ega bo’lsa u legal (qonuniy), aks holda legal bo’lmagan (noqonuniy) foydalanuvchi hisoblanadi. Kompyuter resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o’tishi lozim. Identifikatsiya (Identification) - foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan funktsiyadir. Foydalanuvchi tizimga uning so’rovi bo’yicha o’zining identifikatorini bildiradi, tizim esa o’zining ma’lumotlar bazasida uning borligini tekshiradi. Autentifikatsiya (Authentication) — ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o’zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o’tqazishda tekshiruvchi taraf tekshiriluvchi tarafning xaqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi. Odatda foydalanuvchi tizimga o’z xususidagi noyob, boshqalarga ma’lum bo’lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi. Identifikatsiya va autentifikatsiya sub’ektlarning (foydalanuvchilarning) haqiqiy ekanligini aniqlash va tekshirishning o’zaro bog’langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog’liq. Sub’ektni identifikatsiyalash va autentifikatsiyalashdan so’ng uni avtorizatsiyalash boshlanadi. Avtorizatsiya (Authorization) — subektga tizimda ma’lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya sub’ekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli ajrata olmasa bu tizimda axborotning konfidentsialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma’murlash muolajasi uzviy bog’langan. Ma’murlash (Accounting) — foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik xodisalarini oshkor qilish, taxlillash va ularga mos reaktsiya ko’rsatish uchun juda muhimdir. Ma’lumotlarni uzatish kanallarini himoyalashda sub’ektlarning o’zaro autentifikatsiyasi, ya’ni aloqa kanallari orqali bog’lanadigan sub’ektlar xaqiqiyligining o’zaro tasdig’i bajarilishi shart. Xaqiqiylikning tasdig’i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. ―Ulash‖ atamasi orqali - 31 - tarmoqning ikkita sub’ekti o’rtasida mantiqiy bog’lanish tushuniladi. Ushbu muolajaning maqsadi — ulash qonuniy sub’ekt bilan amalga oshirilganligiga va barcha axborot mo’ljallangan manzilga borishligiga ishonchni ta’minlashdir. O’zining xaqiqiyligining tasdiqlash uchun sub’ekt tizimga turli asoslarni ko’rsatishi mumkin. Sub’ekt ko’rsatadigan asoslarga bog’liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo’linishi mumkin: - biror narsani bilish asosida. Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda ―so’rov javob‖ xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko’rsatish mumkin; - biror narsaga egaligi asosida. Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va touch memory qurilmalari; - qandaydir daxlsiz xarakteristikalar asosida. Ushbu kategoriya o’z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko’zining rangdor pardasi va to’r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. Bu kategoriyada kriptografik usullar va vositalar ishlatilmaydi. Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi. Parol — foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan narsa. O’zaro autentifikatsiya uchun foydalanuvchi va uning sherigi o’rtasida parol almashinishi mumkin. Plastik karta va smart-karta egasini autentifikatsiyasida shaxsiy identifikatsiya nomeri PIN sinalgan usul hisoblanadi. PIN — kodning mahfiy qiymati faqat karta egasiga ma’lum bo’lishi shart. Dinamik — (bir martalik) parol - bir marta ishlatilganidan so’ng boshqa umuman ishlatilmaydigan parol. Amalda odatda doimiy parolga yoki tayanch iboroga asoslanuvchi muntazam o’zgarib turuvchi qiymat ishlatiladi. ―So’rov-javob:tizimi - taraflarning biri noyob va oldindan bilib bo’lmaydigan ―so’roV: qiymatini ikkinchi tarafga jo’natish orqali autentifikatsiyani boshlab beradi, ikkinchi taraf esa so’rov va sir yordamida hisoblangan javobni jo’natadi. Ikkala tarafga bitta sir ma’lum bo’lgani sababli, birinchi taraf ikkinchi taraf javobini to’g’riligini tekshirishi mumkin.

13-Axborot texnologiyalariga oid huquqbuzarlik va qarshi kurash yo’llari.

Himoyalanishni taxlillash vositalari zaifliklarni topib va o’z vaqtida yo’q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishiga bo’ladigan barcha sarf-harajatlar kamayadi. Himoyalanishni taxlillash vositalari tarmoq sathida, operatsion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko’paytirish, axborot tizimiga "ichkarilab borish" va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin. Tarmoq protokollari va servislari himoyalanishini tahlillash vositalari. Har qanday tarmoqda abonentlarning o’zaro aloqasi ikkita va undan ko’p uzellar orasida axborot almashinish muolajalarini belgilovchi tarmoq protokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislarini ishlab chiqishda ularga ishlanuvchi axborot xavfsizligini ta’minlash bo’yicha talablar (odatda shubxasiz yetarli bo’lmagan) qo’yilgan. SHu sababli, tarmoq protokollarida aniqlangan zaifliklar xususida axborotlar paydo bo’lmoqda. Natijada, korporativ tarmoqda foydalanadigan barcha protokol va servislarni doimo tekshirish zaruriyati tug’iladi. Himoyalanishni taxlillash tizimi zaifliklarni aniqlash bo’yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga xujumlarida qo’llaniladiganiga o’xshash. Zaifliklarni aniqlash maqsadida skanerlash tekshiruvchi tizim xususidagi dastlabki axborotni, xususan, ruxsat etilgan protokollar va ochiq portlar, operatsion tizimnnig ishlatiluvchi versiyalari va h. xususidagi axborotni olish bilan boshlanadi. Skanerlash keng tarqalgan xujumlar, masalan, to’liq saralash usuli bo’yicha parollarni tanlashdan foydalanib, suqilib kirishni imitatsiyalashga urinish bilan tugaydi. Himoyalanishni taxlillash vositalari yordamida tarmoq sathida nafaqat Internetning korporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichki tarmog’ida tekshirishni amalga oshirish mumkin. Tarmoq sathida himoyalanishni taxlillash tizimi tashkilot xavfsizlik darajasini baholashga hamda tarmoq dasturiy va apparat ta’minotini sozlash samaradorligini nazoratlashga xizmat qiladi. Xujumlarni aniqlash Tarmoq axborotini taxlillash usullari. Mohiyati bo’yicha, xujumlarni aniqlash jarayoni korporativ tarmoqda bo’layotgan shubhali harakatlarni baholash jarayonidir. Boshqacha aytganda xujumlarni aniqlash- hisoblash yoki tarmoq resurslariga yo’naltirilgan shubhali harakatlarni identifikatsiyalash va ularga reaktsiya ko’rsatish jarayoni. Hozirda xujumlarni aniqlash tizimida quyidagi usullar ishlatiladi: - statistik usul; - ekspert tizimlari; - 39 - - neyron tarmoqlari. Statistik usul. Statistik yondashishning asosiy afzalligi allaqachon ishlab chiqilgan va o’zini tanitgan matematik statistika apparatini ishlatish va sub’ekt xarakteriga moslash. Avval tahlillanuvchi tizimning barcha sub’ektlari uchun profillar aniqlanadi. Ishlatiladigan profillarning etalondan har qanday chetlanishi ruxsat etilmagan foydalanish hisoblanadi. Statistik usullar universal hisoblanadi, chunki mumkin bo’lgan xujumlarni va ular foydalanadigan zaifliklarni bilish talab etilmaydi. Ammo bu usullardan foydalanishda bir qancha muammolar paydo bo’ladi: 1. Statistik tizimlar xodisalar kelishi tartibiga sezuvchanmaslar; ba’zi xollarda bir xodisaning o’zi, kelishi tartibiga ko’ra anomal yoki normal faoliyatni xarakterlashi mumkin. 2. Anomal faoliyatni adekvat identifikatsiyalash maqsadida xujumlarni aniqlash tizimi tomonidan kuzatiluvchi xarakteristikalar uchun chegaraviy (bo’sag’aviy) qiymatlarni berish juda qiyin. 3. Statistik usullar vaqt o’tishi bilan buzg’unchilar tomonidan shunday "o’rnatilishi" mumkinki, xujum harakatlari normal kabi qabul qilinadi. Ekspert tizimlari. Ekspert tizimi odam-ekspert bilimlarini qamrab oluvchi qoidalar to’plamidan tashkil topgan. Ekspert tizimidan foydalanish xujumlarni aniqlashning keng tarqalgan usuli bo’lib, xujumlar xususidagi axborot qoidalar ko’rinishida ifodalanadi. Bu qoidalar harakatlar ketma-ketligi yoki signaturalar ko’rinishida yozilishi mumkin. Bu qoidalarning har birining bajarilishida ruxsatsiz faoliyat mavjudligi xususida qaror qabul qilinadi. Bunday yondashishning muhim afzalligi - yolg’on trevoganing umuman bo’lmasligi. Ekspert tizimining ma’lumotlari bazasida hozirda ma’lum bo’lgan aksariyat xujumlar stsenariyasi bo’lishi lozim. Ekspert tizimlari, dol-zarblikni saqlash maqsadida, ma’lumotlar bazasini muttasil yangilashni talab etadi. Garchi ekspert tizimlari qaydlash jurnallaridagi ma’lumotlarni ko’zdan kechirishga yaxshi imkoniyatni tavsiya qilsada, so’ralgan yangilanish e’tiborsiz qoldirilishi yoki ma’mur tomonidan qo’lda amalga oshirilishi mumkin. Bu eng kamida, ekspert tizimi imkoniyatlarining bo’shashiga olib keladi. Ekspert tizimlarining kamchiliklari ichida eng asosiysi - noma’lum xujumlarni akslantira olmasligi. Bunda oldindan ma’lum xujumning xatto ozgina o’zgarishi xujumlarni aniqlash tizimining ishlashiga jiddiy to’siq bo’lishi mumkin. Neyron tarmoqlari. Xujumlarni aniqlash usullarining aksariyati qoidalar yoki statistik yondashish asosida nazoratlanuvchi muhitni tahlillash shakllaridan foydalanadi. Nazoratlanuvchi muhit sifatida qaydlash jurnallari yoki tarmoq trafigi ko’rilishi mumkin. Bunday taxlillash ma’mur yoki xujumlarni yaniqlash tizimi tomonidan yaratilgan, oldindan aniqlangan qoidalar to’plamiga tayanadi. Xujumni vaqt bo’yicha yoki bir necha niyati buzuq odamlar o’rtasida har qanday bo’linishi ekspert tizimlar yordamida aniqlashga qiyinchilik tug’diradi. Xujumlar va ular usullarining turli-tumanligi tufayli, ekspert tizimlari qoidalarining ma’lumotlar bazasining hatto doimiy yangilanishi ham xujumlar diapazonini aniq identifikatsiyalashni kafolatlamaydi.

14-mavzu: Shaxs, jamiyat va davlat manfaatlarini sifatsiz axborotlarning ta’siridan ,axborot tarqatish tartibining buzilishidan himoya qilish.

Internet ning gurillab rivojlanishi natijasida dunyoda axborotni tarqatish va foydalanishda sifatiy o’zgarish sodir bo’ldi. Internet foydalanuvchilari arzon va qulay kommunikatsiyaga ega bo’ldilar. Korxonalar Internet kanallaridan jiddiy tijorat va boshqaruv axborotlarini uzatish imkoniyatlariga qiziqib qoldilar. Ammo Internetning qurilishi printsipi niyati buzuq odamlarga axborotni o’g’irlash yoki atayin buzish imkoniyatini yaratdi. Odatda TCP/IP protokollar va standart Internet-ilovalar (e-mail, Web, FTP) asosida qurilgan korporativ va idora tarmoqlari suqilib kirishdan kafolatlanmaganlar. Internetning hamma yerda tarqalishidan manfaat ko’rish maqsadida tarmoq xujumlariga samarali qarshilik ko’rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq VPN yaratish ustida ishlar olib borildi. Natijada 1990 yilning boshida virtual xususiy tarmoq VPN kontseptsiyasi yaratildi. "Virtual" iborasi VPN atamasiga ikkita uzel o’rtasidagi ulanishni vaqtincha deb ko’rilishini ta’kidlash maqsadida kiritilgan. Haqiqatan, bu ulanish doimiy, qat’iy bo’lmay, faqat ochiq tarmoq bo’yicha trafik o’tganida mavjud bo’ladi. Virtual tarmoq VPNlarni qurish kontseptsiyasi asosida yetarlicha oddiy g’oya yotadi: agal global tarmoqda axborot almashinuvchi ikkita uzel bo’lsa, bu uzellar orasida ochiq tarmoq orqali uzatilayotgan axborotning konfidentsialligini va yaxlitligini ta’minlovchi virtual himoyalangan tunnel qurish zarur va bu virtual tunneldan barcha mumkin bo’lgan tashqi faol va passiv kuzatuvchilarning foydalanishi xaddan tashqari qiyin bo’lishi lozim. SHunday qilib, VPN tunneli ochiq tarmoq orqali o’tkazilgan ulanish bo’lib, u orqali virtual tarmoqning kriptografik himoyalangan axborot paketlari uzatiladi. Axborotni VPN tunneli bo’yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan: - o’zaro aloqadagi taraflarni autentifikatsiyalash; - uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash); - etkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish. Bu vazifalar bir biriga bog’liq bo’lib, ularni amalga oshirishda axborotni kriptografik himoyalash usullaridan foydalaniladi. Bunday himoyalashning samaradorligi simmetrik va asimmetrik kriptografik tizimlarning birgalikda ishlatilishi evaziga ta’minlanadi. VPN qurilmalari tomonidan shakllantiriluvchi VPN tunneli himoyalangan ajratilgan liniya xususiyatlariga ega bo’lib, bu himoyalangan ajratilgan liniyalar umumfoydalanuvchi tarmoq, masalan Internet doirasida, saflanadi. VPN qurilmalari virtual xususiy tarmoqlarda VPN-mijoz, VPN-server yoki VPN xavfsizligi shlyuzi vazifasini o’tashi mumkin. VPN-mijoz odatda shaxsiy kompyuter asosidagi dasturiy yoki dasturiy-apparat kompleksi bo’lib, uning tarmoq dasturiy ta’minoti u boshqa VPN-mijoz, VPN-server yoki VPN xavfsizligi shlyuzlari bilan almashinadigan trafikni shifrlash va autentifikatsiyalash uchun modifikatsiyalanadi. - 41 - VPN-server server vazifasini o’tovchi, kompyuterga o’rnatiluvchi dasturiy yoki dasturiy-apparat kompleksidan iborat. VPN-server tashqi tarmoqlarning ruxsatsiz foydalanishidan serverlarni himoyalashni hamda alohida kompyuterlar va mos VPNmahsulotlari orqali himoyalangan lokal tarmoq segmentlaridagi kompyuterlar bilan himoyalangan ulanishlarni tashkil etishni ta’minlaydi. VPN-server VPN-mijozning server platformalari uchun funktsional analog hisoblanadi. U avvalo VPN-mijozlar bilan ko’pgina ulanishlarni madadlovchi kengaytirilgan resurslari bilan ajralib turadi. VPN-server mobil foydalanuvchilar bilan ulanishlarni ham madadlashi mumkin. VPN xavfsizlik shlyuzi. (Security gateway) ikkita tarmoqqa ulanuvchi tarmoq qurilmasi bo’lib, o’zidan keyin joylashgan ko’p sonli xostlar uchun shifrlash va autentifikatsiyalash vazifalarini bajaradi. VPN xavfsizligi shlyuzi shunday joylashtiriladiki, ichki korporativ tarmoqqa atalgan barcha trafik u orqali o’tadi. VPN xavfsizligi shlyuzining adresi kiruvchi tunnellanuvchi paketning tashqi adresi sifatida ko’rsatiladi, paketning ichki adresi esa shlyuz orqasidagi muayyan xost adresi hisoblanadi. VPN xavfsizligi shlyuzi alohida dasturiy yechim, alohida apparat qurilmasi, hamda VPN vazifalari bilan to’ldirilgan marshrutizatorlar yoki tarmoqlararo ekran ko’rinishida amalga oshirilishi mumkin. Axborot uzatishning ochiq tashqi muhiti ma’lumot uzatishning tezkor kanallarini (Internet muhiti) va aloqaning sekin ishlaydigan umumfoydalanuvchi kanallarini (masalan, telefon tarmog’i kanallarini) o’z ichiga oladi. Virtual xususiy tarmoq VPNning samaradorligi aloqaning ochiq kanallari bo’yicha aylanuvchi axborotning himoyalanish darajasiga bog’liq. Ochiq tarmoq orqali ma’lumotlarni xavfsiz uzatish uchun inkapsulyatsiyalash va tunnellash keng ishlatiladi. Tunnellash usuli bo’yicha ma’lumotlar paketi umumfoydalanuvchi tarmoq orqali xuddi oddiy ikki nuqtali ulanish bo’yicha uzatilganidek uzatiladi. Har bir "jo’natuvchi-qabul qiluvchi" juftligi orasiga bir protokol ma’lumotlarini boshqasining paketiga inkapsulyatsiyalashga imkon beruvchi o’ziga xos tunnel-mantiqiy ulanish o’rnatiladi. Tunnellashga binoan, uzatiluvchi ma’lumotlar portsiyasi xizmatchi hoshiyalar bilan birga yangi "konvert"ga "joylash" amalga oshiriladi. Bunda pastroq sath protokoli paketi yuqoriroq yoki xudi shunday sath protokoli paketi ma’lumotlari maydoniga joylashtiriladi. Ta’kidlash lozimki, tunnelashning o’zi ma’lumotlarni ruxsatsiz foydalanishdan yoki buzishdan himoyalamaydi, ammo tunnellash tufayli inkapsulyatsiyalanuvchi dastlabki paketlarni to’la kriptografik himoyalash imkoniyati paydo bo’ladi. Uzatiluvchi ma’lumotlar konfidentsialligini ta’minlash maqsadida jo’natuvchi dastlabki paketlarni shifrlaydi, ularni, yangi IP- sarlavha bilan tashqi paketga joylaydi va tranzit tarmoq bo’yicha jo’natadi.

15-mavzu: Kompyuter tarmoqlarida axborotni himoyalash .

Simsiz tarmoqlar odamlarga simli ulanishsiz o’zaro bog’lanishlariga imkon beradi. Bu siljish erkinligini va uy, shahar qismlaridagi yoki dunyoning olis burchaklaridagi ilovalardan foydalanish imkonini ta’minlaydi. Simsiz tarmoqlar odamlarga o’zlariga qulay va xoxlagan joylarida elektron pochtani olishlariga yoki Web-sahifalarni ko’zdan kechirishlariga imkon beradi. Simsiz tarmoqlarning turli xillari mavjud, ammo ularning eng muhim xususiyati bog’lanishning kompyuter qurilmalari orasida amalga oshirilishidir. Kompyuter qurilmalariga shaxsiy raqamli yordamchilar (Personal digital assistance, PDA), noutbuklar, shaxsiy kompyuterlar, serverlar va printerlar taalluqli. Odatda uyali telefonlarni kompyuter qurilmalari qatoriga kiritishmaydi, ammo eng yangi telefonlar va hatto naushniklar ma’lum hisoblash imkoniyatlariga va tarmoq adapterlariga ega. Yaqin orada elektron qurilmalarning aksariyati simsiz tarmoqlarga ulanish imkoniyatini ta’minlaydi. Bog’lanish ta’minlanadigan fizik xudud o’lchamlariga bog’liq holda simsiz tarmoqlarning quyidagi kategoriyalari farqlanadi: - simsiz shaxsiy tarmoq (Wireless personal-area network, PAN); - simsiz lokal tarmoq (Wireless local-area network, LAN); - simsiz regional tarmoq (Wireless metropolitan-area network, MAN): - simsiz global tarmoq (Wireless Wide-area network, WAN). Simsiz shaxsiy tarmoqlari uzatishning katta bo’lmagan masofasi bilan (17 metrgacha) ajralib turadi va katta bo’lmagan binoda ishlatiladi. Bunday tarmoqlarning xarakteristikalari o’rtacha bo’lib, uzatish tezligi odatda 2Mb/s dan oshmaydi. Bunday tarmoq, masalan, foydalanuvchi PDA sida va uning shaxsiy kompyuterida yoki noutbukida ma’lumotlarni simsiz sinxronlashni ta’minlashi mumkin. Xuddi shu tariqa printer bilan simsiz ulanish ta’minlanadi. Kompyuterni tashqi qurilmalar bilan ulovchi simlar chigalliklarining yo’qolishi yetarlicha jiddiy afzallik bo’lib, buning evaziga tashqi qurilmalarning boshlang’ich o’rnatilishi va keyingi, zaruriyat tug’ilganda, joyining o’zgartirilishi anchagina osonlashadi. - 43 - Simsiz lokal tarmoqlar ofislarning ichida va tashqarisida, ishlab chiqarish binolarida uzatishlarning yuqori xarakteristikalarini ta’minlaydi. Bunday tarmoqlardan foydalanuvchilar odatda noutbuklarni, shaxsiy kompyuterlarni va katta resurslarni talab etuvchi ilovalarni bajarishga qodir protsessorli va katta ekranli PDA larni ishlatishadi. Xizmatchi tarmoq xizmatlaridan majlislar zalida yoki binoning boshqa xonalarida bo’la turib foydalanashi mumkin. Bu xizmatchiga o’z vazifalarini samarali bajarishga imkon beradi. Simsiz lokal tarmoqlar uzatishning 54Mbit/sgacha tezligida barcha ofis yoki maishiy ilovalar talablarini qondirish imkoniga ega. Xarakteristikalari, komponentlari, narxi va bajaradigan amallari bo’yicha bunday tarmoqlar Ethernet xilidagi an’anaviy simli lokal tarmoqlariga o’xshash. Simsiz regional tarmoqlar yuzasi bo’yicha shaxarga teng bo’lgan xududga xizmat qiladi. Aksariyat xollarda ilovalarni bajarishda belgilangan ulanish talab etiladi, ba’zida esa mobillik zarur bo’ladi. Masalan, kasalxonada bunday tarmoq asosiy bino va masofadagi klinikalar orasida ma’lumotlarni uzatishni ta’minlaydi. Yoki energetik kompaniya bunday tarmoqdan shaxar masshtabida foydalanib, turli tumanlardan beriladigan ish naryadlaridan foydalanishini ta’minlaydi. Natijada, simsiz regional tarmoqlar mavjud tarmoq infratuzilmalarini bir yerga to’playdi yoki mobil foydalanuvchilarga mavjud tarmoq infratuzilmalari bilan ulanishni o’rnatishga imkon beradi. Simsiz regional tarmoqlarning xarakteristikalari turlicha. Ulanishlarda infraqizil texnologiyaning ishlatilishi ma’lumotlarni uzatish tezligining 100 Gbit/s va undan katta bo’lishini ta’minlaydi. Simsiz global tarmoqlar mobil ilovalarning, ulardan mamlakat yoki xatto kontinent masshtabida foydalanishni ta’minlash bilan ishlanishini ta’minlaydi. Iqtisodiy mulohazalarga tayangan holda, telekommunikatsiya kompaniyalari ko’pgina foydalanuvchilar uchun uzoq masofadan ulanishni ta’minlovchi simsiz global tarmoqning nisbatan qimmat infratuzilmasini yaratadilar. Bunday yechimning xarajati barcha foydalanuvchilar o’rtasida taqsimlanadi, natijada abonent to’lovi unchalik yuqori bo’lmaydi. Simsiz global tarmoq xarakteristikalari nisbatan yuqori emas, ma’lumotlarni uzatishning tezligi 56 Kbit/s ni, ba’zida 170 Kbit/s ni tashkil etadi. Simsiz global tarmoqlarga xos ilovalar Internetdan foydalanishni, elektron pochta xabarlarini uzatish va qabul qilishni, foydalanuvchi uydan yoki ofisdan tashqarida bo’lganida korporativ ilovalardan foydalanishni ta’minlovchi ilovalardir. Abonentlar, masalan, taksida ketayotganlarida yoki shahar bo’yicha sayr qilinayotganlarida ulanishni o’rnatishlari mumkin. Umuman, simsiz global tarmoqdan foydalanuvchilar xududiy chegaralanmaganlar. Simsiz tarmoq tuzilmasi. Simsiz tarmoqlarda simli tarmoqda ishlatiladigan komponentlar ishlatiladi. Ammo, simsiz tarmoqlarda axborot xavo muhiti (medium) orqali uzatishga yaroqli ko’rinishga o’zgartirilishi lozim.

16-mavzu: Axborot himoya qilish tizimini amalga oshirilish usullari.

Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiyalash bo’lib, u an’anaviy ko’p martali parollarni ishlatishi-ga asoslangan. Tarmoqdagi foydalanuvchini oddiy autentifikatsiyalash muolajasini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan foydalanuvchi kompyuter klaviaturasida o’zining identifikatori va parolini teradi. Bu ma’lumotlar autentifikatsiya serveriga ishlanish uchun tushadi. Autentifikatsiya serverida saqlanayotgan foydalanuvchi identifikatori bo’yicha ma’lumotlar bazasidan mos yozuv topiladi, undan parolni topib foydalanuvchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikatsiya muvaffaqiyatli o’tgan hisoblanadi va foydalanuvchi legal (qonuniy) maqomini va avtorizatsiya tizimi orqali uning maqomi uchun aniqlangan xuquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi. Eng keng tarqalgan usul — foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o’qish va yozishdan himoyalash atributlari o’rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ruyxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funktsiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir. Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul — foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o’qish va yozishdan himoyalash atributlari o’rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ruyxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funktsiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur - 47 - imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir. Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funktsiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli urniga uning bir tomonlama funktsiya h(.) dan foydalanib olingan tasvirini yuborishi shart. Bu o’zgartirish g’anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki g’anim yechilmaydigan sonli masalaga duch keladi. Ko’p martali parollarga asoslangan oddiy autentifikatsiyalash tizi-mining bardoshligi past, chunki ularda autentifikatsiyalovchi axborot ma’noli so’zlarning nisbatan katta bo’lmagan to’plamidan jamlanadi. Ko’p martali parollarning ta’sir muddati tashkilotning xavfsizligi siyosatida belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular lug’atda bo’lmasin va ularni topish qiyin bo’lsin. Bir martali parollarga asoslangan autentifikatsiyalashda foydalanishga har bir so’rov uchun turli parollar ishlatiladi. Bir martali dinamik parol faqat tizimdan bir marta foydalanishga yaroqli. Agar, hatto kimdir uni ushlab qolsa ham parol foyda bermaydi. Odatda bir martali parollarga asoslangan autentfikatsiyalash tizimi masofadagi foydalanuvchilarni tekshirishda qo’llaniladi. Bir martali parollarni generatsiyalash apparat yoki dasturiy usul oqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to’lov plastik kartochkalariga o’xshash mikroprotsessor o’rnatilgan miniatyur qurilmalar ko’rinishda amalga oshiradi. Odatda kalitlar deb ataluvchi bunday kartalar klaviaturaga va katta bo’lmagan displey darchasiga ega. Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni qo’llashning quyidagi usullari ma’lum: 1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish. 2. Legal foydalanuvchi va tekshiruvchi uchun umumiy bo’lgan tasodifiy parollar ruyxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish. 3. Foydalanuvchi va tekshiruvchi uchun umumiy bo’lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish. Birinchi usulni amalga oshirish misoli sifatida SecurID autentikatsiyalash texnologiyasini ko’rsatish mumkin. Bu texnologiya Security Dynamics kompaniyasi tomonidan ishlab chiqilgan bo’lib, qator kompaniyalarning, xususan Cisco Systems kompaniyasining serverlarida amalga oshirilgan. Vaqt sinxronizatsiyasidan foydalanib autentifikatsiyalash sxemasi tasodifiy sonlarni vaqtning ma’lum oralig’idan so’ng generatsiyalash algoritmiga asoslangan. Autentifikatsiya sxemasi quyidagi ikkita parametrdan foydalanadi: • har bir foydalanuvchiga atalgan va autentifikatsiya serverida hamda foydalanuvchining apparat kalitida saqlanuvchi noyob 64-bitli sondan iborat maxfiy kalit; • joriy vaqt qiymati. Autentifikatsiyaning bu sxemasi bilan yana bir muammo bog’liq. Apparat kalit generatsiyalagan tasodifiy son katta bo’lmagan vaqt oralig’i mobaynida haqiqiy parol hisoblanadi. SHu sababli, umuman, qisqa muddatli vaziyat sodir bo’lishi mumkinki, - 48 - xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi. Bir martali paroldan foydalanuvchi autentifikatsiyalashni amalga oshiruvchi yana bir variant - «so’rov-javob» sxemasi bo’yicha autentifikatsiyalash. Foydalanuvchi tarmoqdan foydalanishga uringanida server unga tasodifiy son ko’rinishidagi so’rovni uzatadi. Foydalanuvchining apparat kaliti bu tasodifiy sonni, masalan DES algoritmi va foydalanuvchining apparat kaliti xotirasida va serverning ma’lumotlar bazasida saqlanuvchi maxfiy kaliti yordamida rasshifrovka qiladi. Tasodifiy son - so’rov shifrlangan ko’rinishda serverga qaytariladi. Server ham o’z navbatida o’sha DES algoritmi va serverning ma’lumotlar bazasidan olingan foydalanuvchining maxfiy kaliti yordamida o’zi generatsiyalagan tasodifiy sonni shifrlaydi. So’ngra server shifrlash natijasini apparat kalitidan kelgan son bilan taqqoslaydi. Bu sonlar mos kelganida foydalanuvchi tarmoqdan foydalanishga ruxsat oladi. Ta’kidlash lozimki, «so’rovjavob» autentifikatsiyalash sxemasi ishlatishda vaqt sinxronizatsiyasidan foydalanuvchi autentifikatsiya sxemasiga qaraganda murakkabroq. Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo’lgan tasodifiy parollar ruyxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo’linuvchi ro’yxati maxfiy parollar ketma-ketligi yoki to’plami bo’lib, har bir parol faqat bir marta ishlatiladi. Ushbu ro’yxat autentifikatsion almashinuv taraflar o’rtasida oldindan taqsimlanishi shart. Ushbu usulning bir variantiga binoan so’rov-javob jadvali ishlatiladi. Bu jadvalda autentifikatsilash uchun taraflar tomonidan ishlatiluvchi so’rovlar va javoblar mavjud bo’lib, har bir juft faqat bir marta ishlatilishi shart. Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo’lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

• o’zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;

• bir tomonlama funktsiyaga asoslangan parollar ketma-ketligi. Ushbu usulning mohiyatini bir tomonlama funktsiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o’zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

17-mavzu: Axborot xavsizligi siyosati.

Axborotning muximlik darajasi qadim zamonlardan ma’lum. SHuning uchun xam qadimda axborotni himoyalash uchun turli xil usullar qo’llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o’qiy olmagan. Asrlar davomida bu san’at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o’n yil oldin hamma narsa tubdan o’zgardi, ya’ni axborot o’z qiymatiga ega bo’ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o’g’irlaydilar, buzib talqin etadilar va soxtalashtiradilar. SHunday qilib, axborotni himoyalash zaruriyati tug’iladi. Axborotni qayta ishlash sanoatining paydo bo’lishi axborotni himoyalash sanoatining paydo bo’lishiga olib keladi. Xavfsizlikning asosiy yo’nalishlari Axborot xavfsizligi. Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo’llanilmoqda (iqtisod, fan, ta’lim, xarbiy ish, turli texnologiyalarni boshqarish va x.k.) Iqtisodiy xavfsizlik. Milliy iqtisodda axborotlarni yaratish, tarqatish, qayta ishlash va foydalanish jarayoni hamda vositalarini qamrab olgan Yangi tarmoq vujudga keldi. «Milliy axborot resursi» tushunchasi Yangi iqtisodiy kategoriya bo’lib xizmat qilmoqda. Davlatning axborot resurslariga keltirilayotgan zarar axborot xavfsizligiga xam ta’sir ko’rsatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakllantirish va uning asosida jahon yagona axborot maydoniga kirib borish natijasida milliy iqtisodimizga turli xildagi zararlar keltirish xavfi paydo bo’lmoqda. Mudofaa xavfsizligi. Mudofaa sohasida xavfsizlikning asosiy ob’ektlaridan bo’lib, mamlakatning mudofaa potentsialining axborot tarkibi va axborot resurslari hisoblanmoqda. Xozirgi kunda barcha zamonaviy qurollar va harbiy texnikalar juda ham kompyuterlashtirilib yuborildi. SHuning uchun xam ularga axborot qurollarini qo’llash ehtimoli katta. Ijtimoiy xavfsizlik. Zamonaviy axborot – kommunikatsiyalar texnologiyalarining milliy iqtisod barcha tarmoqlarida keng qo’llanishi inson psixologiyasi va jamoa ongiga «yashirin» ta’sir ko’rsatish vositalarining samaradorligini yuksaltirib yubordi. - 7 - Ekologik xavfsizlik. Ekologik xavfsizlik – global masshtabdagi muammodir. «Ekologik toza», energiya va resurs tejaydigan, chiqindisiz texnologiyalarga o’tish faqat milliy iqtisodni axborotlashtirish hisobiga qayta qurish asosidagina yo’lga qo’yish mumkin. Avtomatlashtiriltan axborot tizimlarida axborotlar o’zining hayotiy davriga ega bo’ladi. Bu davr uni yaratish, undan foydalanish va kerak bo’lmaganda yo’qotishdan iboratdir (2-rasm ). Axborotlar xayotiy davrining xar bir bosqichida ularning himoyalanganlik darajasi turlicha baholanadi. Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muxim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulki huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshha moddiy hamda nomoddiy zararlar keltirishi mumkin bo’lgan turli kirishlar va o’g’irlashlardan himoyalashdir. 2-rasm Axborot xavfsizligi deb, ma’lumotlarni yo’qotish va o’zgartirishga yo’naltirilgan tabiiy yoki sun’iy xossali tasodifiy va qasddan ta’sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi. Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va xujjatlarni o’g’irlash yoki nusxa olishdan iborat bo’lsa, hozirgi paytdagi xavf esa kompyuter ma’lumotlari to’plami, elektron ma’lumotlar, elektron massivlardan ularning egasidan ruxsat so’ramasdan foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi. Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, Axborotni

foydalanish osonligi va maxfiyligini ta’minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi. Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar yetkazmokchi bo’lgan nohuquqiy muomaladan xar qanday xujjatlashtirilgan, ya’ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan xolda moddiy jismda qayd etilgan axborot ximoyalanishi kerak. Axborot xavfsizligi nuktai nazaridan axborotni quyidagicha turkumlash mumkin: • maxfiylik — aniq bir axborotga fakat tegishli shaxslar doirasigina kirishi mumkinligi, ya’ni foydalanilishi qonuniy xujjatlarga muvofik cheklab qo’yilib, xujjatlashtirilganligi kafolati. Bu bandning buzilishi o’g’irlik yoki axborotni oshkor qilish, deyiladi; • konfidentsiallik — inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; • yaxlitlik — axborot boshlang’ich ko’rinishda ekanligi, ya’ni uni saqlash va uzatishda ruxsat etilmagan o’zgarishlar qilinmaganligi kafolati; bu bandning buzilishi axborotni soxtalashtirish deyiladi; • autentifikatsiya — axborot zaxirasi egasi deb e’lon qilingan shaxs xaqiqatan xam axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi; • apellyatsiya qilishlik — yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo’llaniladi. Kerak bo’lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati. Yukoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin: • ishonchlilik — tizim meyoriy va g’ayri tabiiy xollarda rejalashtirilganidek o’zini tutishlik kafolati; • aniqlilik — xamma buyruqlarni aniq va to’liq bajarish kafolati; • tizimga kirishni nazorat qilish — turli shaxs guruxlari axborot manbalariga xar xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati; • nazorat qilinishi — istalgan paytda dastur majmuasining xoxlagan kismini tulik tekshirish mumkinligi kafolati; • identifikatsiyalashni nazorat qilish — xozir tizimga ulangan mijoz aniq o’zini kim deb atagan bulsa, aniq o’sha ekanligining kafolati; • qasddan buzilishlarga to’sqinlik — oldindan kelishilgan me’yorlar chegarasida qasddan xato kiritilgan ma’lumotlarga nisbatan tizimning oldindan kelishilgan xolda o’zini tutishi. Axborotni ximoyalashning maqsadlari kuyidagilardan iborat: - axborotning kelishuvsiz chikib ketishi, ugirlanishi, yo’qotilishi, o’zgartirilishi, soxtalashtirilishlarning oldini olish; - shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf – xatarning oldini olish; - axborotni yo’q qilish, o’zgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish; - xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta’minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish;

18-mavzu: Tizimlarni tahlil qilish metodi.

Tarmoq texnologiyalari rivojining boshlang’ich bosqichida viruslar va kompyuter xujumlarining boshqa turlari ta’siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bog’liqligi katta emas edi. Hozirda, xujumlar sonining doimo o’sishi hamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bog’liqligi sharoitida mashina vaqtining yo’qolishiga olib keluvchi hatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi. Misol tariqasida keltirish mumkinki, faqat 2003 yilning birinchi choragida dunyo miqyosidagi yo’qotishlar 2002 yildagi barcha yo’qotishlar yig’indisining 50%ini tashkil etgan, yoki bo’lmasa 2006 yilning o’zida Rossiya Federeatsiyasida 14 mingdan ortiq kompyuter jinoyatchiligi holatlari qayd etilgan. Korporativ tarmoqlarda ishlanadigan axborot, ayniqsa, zaif bo’ladi. Hozirda ruxsatsiz foydalanishga yoki axborotni modifikatsiyalashga, yolg’on axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo’ladi: - kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot hajmining oshishi; - ma’lumotlar bazasida muhimlik va mahfiylik darajasi turli bo’lgan axborotlarning to’planishi; - ma’lumotlar bazasida saqlanayotgan axborotdan va hisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi; - masofadagi ishchi joylar soninig oshishi; - foydalanuvchilarni bog’lash uchun Internet global tarmog’ini va aloqaning turli kanallarini keng ishlatish; - foydaluvchilar kompyuterlari o’rtasida axborot almashinuvining avtomatlashtirilishi. Axborot xavfsizligiga tahdid deganda axborotning buzilishi yoki yo’qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan harakatlar tushuniladi. Oldindan shuni aytish mumkinki, so’z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommertsiya qiymatiga ega bo’lgan qismi xususida ketyapti. Zamonaviy korporativ tarmoqlar va tizimlar duchor bo’ladigan keng tarqalgan tahdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlikka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi manba) bo’lishi mumkin. Bunday ajratish to’g’ri, chunki bitta tahdid uchun (masalan, o’g’irlash) tashqi va ichki manbalarga qarshi harakat usullari turlicha bo’ladi. Bo’lishi - 10 - mumkin bo’lgan tahdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta’minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi. Tez-tez bo’ladigan va xavfli (zarar o’lchami nuqtai nazaridan) tahdidlarga foydalanuvchilarning, operatorlarning, ma’murlarning va korporativ axborot tizimlariga xizmat ko’rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba’zida bunday xatoliklar (noto’g’ri kiritilgan ma’lumotlar, dasturdagi xatoliklar sabab bo’lgan tizimning to’xtashi yoki bo’zilishi) to’g’ridan to’g’ri zararga olib keladi. Ba’zida ular niyati buzuq odamlar foydalanishi mumkin bo’lgan nozik joylarni paydo bo’lishiga sabab bo’ladi. Global axborot tarmog’ida ishlash ushbu omilning yetarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo’lishi mumkin, oxirgisi ayniqsa xavfli. Zarar o’lchami bo’yicha ikkinchi o’rinni o’g’irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishlash rejimlari va himoyalash choralari bilan a’lo darajada tanish bo’lgan tashkilot shtatidagi xodimlar aybdor bo’lib chiqdilar. Global tarmoqlar bilan bog’langan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan yetarlicha nazorat yo’qligi bunday faoliyatga qo’shimcha imkon yaratadi. Xafa bo’lgan xodimlar (hatto sobiqlari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon yetkazishlari mumkin. Xodim ishdan bo’shaganida uning axborot resurslaridan foydalanish xuquqi bekor qilinishi nazoratga olinishi shart. Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo’lishi mumkin bo’lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo’lib tuyulmasa ham, Internetda ishlash tajribasi ko’rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga duchor bo’lar ekan. Xavf-xatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog’i kompyuterlarining xujumlarga qarshi turishi yoki bo’lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko’rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan sasofadan foydalanish xollari alohida ko’rilishi lozim. Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti duchor bo’ladigan xavf-xatar baholanishi va zarur choralar ko’rilishi zarur. Ravshanki, himoyaga tahdidni nazoratlash va zarur choralarni ko’rish uchun tashkilotning sarfharajati tashkilotda aktivlar va resurslarni himoyalash bo’yicha hech qanday choralar ko’rilmaganida kutiladigan yo’qotishlardan oshib ketmasligi shart. Umuman olganda, tashkilotning kompyuter muhiti ikki xil xavf-xatarga duchor bo’ladi: 1. Ma’lumotlarni yo’qotilishi yoki o’zgartirilishi. 2. Servisning to’xtatilishi. Tahdidlarning manbalarini aniqlash oson emas. Ular niyati buzuq odamlarning bostirib kirishidan to kompyuter viruslarigacha turlanishi mumkin. Bunda inson xatoliklari xavfsizlikka jiddiy tahdid hisoblanadi. 1.1-rasmda korporativ axborot tizimida xavfsizlikning buzilish manbalari bo’yicha statistik ma’lumotlarni tasvirlovchi aylanma diagramma keltirilgan.

19-Axborotlarni kriptografik himoyalash usullari.

Masala sharti Blowish simmetrik blokli shirlash algoritmi tadqiqiga bag`ishlangan. Bu ishni bajarish uchun, yani tahlillash ishini ikki bosqichda amalga oshirishga harakat qildim. Bunda biz dastlab blokli algoritmlarni tahlil qilamiz va tuzulishini o`rganib chiqamiz. So`ngra esa Blowfish algoritmini boshqa algaritmlar bilan solishtirgandagi natijalari bilan taqqoslaymiz. Oxirida blowfish shifrlash dasturi ishlash jarayoni bilan tanishib, olingan natijalar orqali xulosalar chiqaramiz.

«Kriptografiya» atamasi dastlab «yashirish, yozuvni bеrkitib qo‘ymoq» ma’nosini bildirgan. Birinchi marta u yozuv paydo bo‘lgan davrlardayoq aytib o‘tilgan. Hozirgi vaqtda kriptografiya dеganda har qanday shakldagi, ya’ni diskda saqlanadigan sonlar ko‘rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko‘rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo‘lgan har qanday axborotga nisbatan qo‘llash mumkin. Maxfiylikni ta’minlashga qaratilgan kriptografiya kеngroq qo‘llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo‘llaniladigan usullarning o‘zi axborotni himoyalash bilan bog‘liq bo‘lgan ko‘p jarayonlarda ishlatilishi mumkin.

Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta’minlaydi. Masalan, to‘lov varaqlarini elеktron pochta orqali uzatishda uning o‘zgartirilishi yoki soxta yozuvlarning qushilishi mumkin. Bunday hollarda axborotning yaxlitligini ta’minlash zaruriyati paydo bo‘ladi. Umuman olganda kompyutеr tarmog‘iga ruxsatsiz kirishning mutlaqo oldini olish mumkin emas, lеkin ularni aniqlash mumkin. Axborotning yaxlitligini tеkshirishning bunday jarayoni, ko‘p hollarda, axborotning haqiqiyligini ta’minlash dеyiladi. Kriptografiyada qo‘llaniladigan usullar ko‘p bo‘lmagan o‘zgartirishlar bilan axborotlarning haqiqiyligini ta’minlashi mumkin.

Sirli (maxfiy) aloqalar sohasi kriptologiya dеb aytiladi. Ushbu so‘z yunoncha **«**kripto**»** — sirli va **«**logus**»** — xabar ma’nosini bildiruvchi so‘zlardan iborat. Kriptologiya ikki yo‘nalish, ya’ni kriptografiya va kriptotahlildan iborat.

Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta’minlashdan iborat.

Kriptotahlilning vazifasi esa kriptograflar tomonidan ishlab chiqilgan himoya tizimini ochishdan iborat.

Hozirgi kunda kriptotizimni ikki sinfga ajratish mumkin:

• simmеtriyali bir kalitlilik (maxfiy kalitli);

• asimmеtriyali ikki kalitlilik (ochiq kalitli).

Simmеtriyali tizimlarda quyidagi ikkita muammo mavjud:

1) Axborot almashuvida ishtirok etuvchilar qanday yo‘l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?

2) Jo‘natilgan xabarning haqiqiyligini qanday aniqlasa bo‘ladi?

Ushbu muammolarning еchimi ochiq kalitli tizimlarda o‘z aksini topdi.

Ochiq kalitli asimmеtriyali tizimda ikkita kalit qo‘llaniladi. Biridan ikkinchisini hisoblash usullari bilan aniqlab bo‘lmaydi.

Birinchi kalit axborot jo‘natuvchi tomonidan shifrlashda ishlatilsa, ikkinchisi axborotni qabul qiluvchi tomonidan axborotni tiklashda qo‘llaniladi va u sir saqlanishi lozim.

**Оchiq matn**

Shifrlash algoritmi

Shifrlanmagan matn

UzBoy

Zorro

Dеshifrlash algoritmi

**Оchiq matn**

*1-rasm.Shifrlash va deshifrlash blok sxemasi*

Ushbu usul bilan axborotning maxfiyligini ta’minlash mumkin. Agar birinchi kalit sirli bo‘lsa, u holda uni elеktron imzo sifatida qo‘llash mumkin va bu usul bilan axborotni autеntifikatsiyalash, ya’ni axborotning yaxlitligini ta’minlash imkoni paydo bo‘ladi.

Axborotni autеntifikatsiyalashdan tashqari quyidagi masalalarni yеchish mumkin:

• foydalanuvchini autеntifikatsiyalash, ya’ni kompyutеr tizimi zahiralariga kirmoqchi bo‘lgan foydalanuvchini aniqlash:

• tarmoq abonеntlari aloqasini o‘rnatish jarayonida ularni o‘zaro autеntnfikatsiyalash.

Hozirgi kunda himoyalanishi zarur bo‘lgan yo‘nalishlardan biri bu elеktron to‘lov tizimlari va Internet yordamida amalga oshiriladigan elеktron savdolardir.

**20-mavzu: Axborot himoyalashning texnik tizimlari.**

**Kriptografi**ya — ma’lumotlarni o‘zgartirish usullarining to‘plami bo‘lib, ma’lumotlarni himoyalash bo‘yicha quyidagi ikkita asosiy muammolarni hal qilishga yo‘naltirilgan: **maxfiylik; yaxlitlilik.**

Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o‘zgartira olmaslik haqida dalolat bеradi.

Kriptografiya tizimini sxеmatik ravishda quyidagicha tasvirlash mumkin:

Kalit

Jo‘natuvchi

Shifrlash

Тiklash

Qabul qiluvchi

Yovuz niyatli shaxs

*2-rasm.Kalit yordamida shifrlash blok sxemasi*

Bu еrda kalit qandaydir himoyalangan kanal orqali junatiladi (chizmada punktir chiziklar bilan tasvirlangan). Umuman olganda, ushbu mеxanizm simmеtriyali bir kalitlik tizimiga taalluklidir.

Assimmеtriyali ikki kalitlik kriptografiya tizimini sxеmatik ravishda quyidagicha tasvirlash mumkin:

Bu holda himoyalangan kanal bo‘yicha ochiq kalit jo‘natilib, maxfiy kalit jo‘natilmaydi.

Yоvuz niyatli shaxslar uz maqsadlariga erisha olmasa va kriptotaxlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u holda kriptotizim **kriptomustahkam tizim dе**b aytiladi.

Kriptotizimning mustaxkamligi uning kaliti bilan aniklanadi va bu kriptotahlilning asosiy qoidalaridan biri bo‘lib hisoblanadi.

Ushbu ta’rifning asosiy ma’nosi shundan iboratki, kriptotizim barchalarga ma’lum tizim hisoblanib, uning o‘zgartirilishi ko‘p vakt va mablag‘ talab qiladi, shu bois ham faqatgina kalitni o‘zgartirib turish bilan axborotni himoyalash talab qilinadi.

**Kalit 1**

**Kalit 2**

Junatuvchi

### Shifrlash

Tiklash

### Qabul qiluvchi

Yovuz niyatli shaxs

*3-rasm.Assimmetrik shifrlash algoritmi blok sxemasi*

***Kompyutеr ma’lumotlarini himoyalashning tеxnik-dasturiy vositalari***

Ushbu vositalarni quyidagicha tasniflash mumkin:

Vositalar

I. Fоydalanuvchilarni identifikatsiyalash va autentifikatsiyalash tizimi

### II. Disk ma’lumotlarini shifrlash tizimi

III. Тarmoq bo‘yicha uzatiladigan ma’lumotlarni shifrlash tizimi

IV. Elektron ma’lumotlarni autentifikatsiyalash tizimi

V. Тayanch axbоrotlarni boshqarish vositalari

*4-rasm.Ma’lumotlarni himoyalash texnik-dasturiy vositalar*

1. ***Foydalanuvchchilarni idеntifikatsiyalash va autеntifikatsiyalash tizimi.***Ushbu tizim foydalanuvchidan olingan ma’lumot buyicha uning shaxsini tеkshirish, xakikiyligini aniklash va shundan cyng unga tizim bilan ishlashga ruxsat bеrish lozimligini bеlgilab bеradi.

Bu holda asosan foydalanuvchidan olinadigan ma’lumotni tanlash muammosi mavjud bulib, uning quyidagi turlari mavjud:

• foydalanuvchiga ma’lum bo‘lgan maxfiy axborot, masalan, parol’, maxfiy kalit va boshqalar;

• shaxsning fiziologik paramеtrlari, masalan, barmok izlari, kuzning tasviri va boshqalar.

Birinchisi an’anaviy, ikkinchisi esa biomеtrik idеntifikatsiyalash tizimi, dеyiladi.

II. ***Disk ma’lumotlarini shifrlash tizimi.***Ushbu tizimning asosiy maksadi diskdagi ma’lumotlarni himoyalashdir. Bu holda mantikiy va jismoniy boskichlar ajratiladi. Mantikiy boskichda fayl asosiy ob’еkt sifatida bulib, faqatgina ba’zi bir fayllar himoyalanadi. Bunga misol kilib, arxivator dasturlarini kеltirish mumkin. Jismoniy boskichda disk tulaligicha himoyalanadi. Bunga misol sifatida Norton Utilities tarkibidagi Diskreet shifrlovchi dasturni kеl­tirish mumkin.

III. ***Tarmoq buyicha uzatiladigan ma’lumotlarni shifrlash tizimi.***Ushbu tizimda ikki yunalishni ajratish mumkin:

• kanal buyicha, ya’ni aloka kanallari buyicha junatiladigan barcha ma’lumotlarni shifrlash;

• abonеntlar buyicha, ya’ni aloka kanallari buyicha junatiladigan ma’lumotlarning faqatgina mazmuniy kismi shifrlanib, kolgan xizmatchi ma’lumotlarni ochik koldirish.

IV. ***Elеktron ma’lumotlarni autеntifikatsiyalash ti­zimi.***Ushbu tizimda tarmoq buyicha bajariladigan elеk­tron ma’lumotlar almashuvida hujjatni va uning muallifini autеntifikatsiyalash muammosi paydo buladi.

1. ***Tayanch axborotlarni boshqarish vositalari.***Ushbu tizimda tayanch axborotlar sifatida kompyutеr tizimi va tarmogida kullaniladigan barcha kriptografik kalitlar tushuniladi. Bu holda kalitlarni gеnеratsiyalash, saqlash va taksimlash kabi boshqaruv funktsiyalarini ajratishadi.

***21-*mavzu Simmetrik va asimmetrik shifirlash tizimlari.**

Kriptografiya nuktai – nazaridan shifr — bu kalit dеmakdir va ochik ma’lumotlar tuplamini yopik (shifrlangan) ma’lumotlarga uzgartirish kriptografiya uzgartirishlar algoritmlari majmuasi hisoblanadi.

**Kalit** — kriptografiya uzgartirishlar algoritmining ba’zi-bir paramеtrlarining maxfiy holati bulib, barcha algoritmlardan yagona variantini tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy kursatkich bulib **kriptomustaxkamlik** hisoblanadi.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar kuyiladi:

• еtarli darajada kriptomustaxkamlik;

• shifrlash va qaytarish jarayonining oddiyligi;

• axborotlarni shifrlash oqibatida ular hajmining ortib kеtmasligi;

• shifrlashdagi kichik xatolarga ta’sirchan bo‘lmasligi.

Ushbu talablarga quyidagi tizimlar javob bеradi:

• o‘rinlarini almashtirish;

• almashtirish;

• gammalashtirish;

• analitik uzgartirish.

Birinchi bo'limda biz simmetrik kriptotizimlarni ikki turga, ya'ni blokli va oqimli shifrlashga ajratgan edik. Kriptografiyada blokli shifrlash algoritmlari keng qo'llanilib, mohiyat jixatdan quyidagicha. Masalan, ochiq matn 128-bit uzunlikka ega bo'lgan qismlarga ajratiladi va har bir qismlar ustida alohida-alohida amallar bajariladi. Kiruvchi ushbu qism ustida maxfiy kalit asosida amallar bajariladi va natijada 128-bitli shifr matn olinadi.

Blokli shifrlash algoritmlari yaratilish asosiga ko'ra quyidagi turlarga bo'linadi:

Takrorlanuvchi blokli shifrlash(Iterated block ciphers);

O'zratirish-almashtirish tarmoqlari (Substitution-permutation networks);

Feystel tarmog'iga asoslangan (Feistel ciphers);

Lai-Massey shifrlari (Lai-Massey ciphers);

Amallarga asoslangan(Operations);

Takrorlanuvchi blokli shifrlash(Iterated block ciphers). Ko'plab blokli shifrlash algoritmlari takrorlanuvchi shifrlash algoritmlariga asoslanadi, ya'ni ochiq matnning aniq bir bo'lagi qaytariluvchi almashtirish amali orqali shifr matnning aniq bir qismiga almashtiriladi. Ushbu qaytariluvchi almashtirish amali odatda raund amali deb atalib, har bir almashtirish jarayoni raund deb ataladi.

Odatda raund fuknsiyasi R har bir raunda alohida qiymatlar oladi, Ki. Ular esa o'z o'rnida haqiqiy kalitdan hosil qilinadi.

M\_i=R\_(K\_i ) (M\_(i-1))

Bu erda, M\_0- ochiq matn, M\_r - shifr matn raundga mos holda.

Odatda kalit bilan ochiq matn XOR amali orqali qo'shiladi.

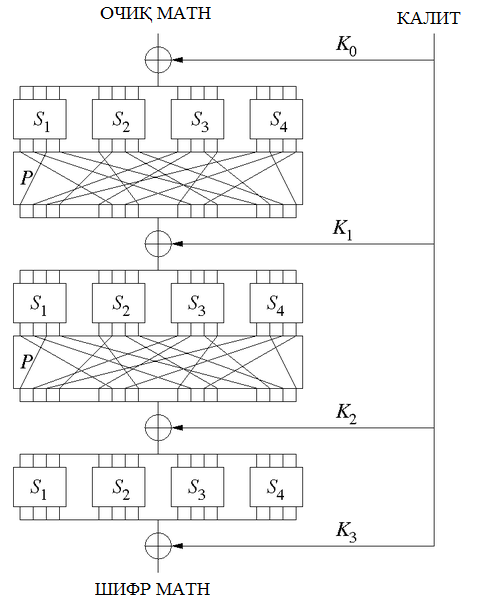
M\_i=M⨁K\_0

M\_i=R\_(K\_i ) (M\_(i-1) );i=0..r

C=M\_r⊕K\_(r+1)

O'zgaratirish-almashtirish tarmoqlari (Substitution-permutation networks). Blokli shifrlash algoritmlari orasida eng muhim bo'lgan yaratish turlaridan biri o'zratirish-almashtirish tarmoqlari (Substitution-permutation networks, SPN) sanalib, har bir raundda aynan bir bir xil belgilangan amallar bosqichi bajariladi.

Ushbu usulda shifrlash algoritmi quyidagicha :



*5-rasm. SPN tarmoq tuzilishi*

Ushbu shifrlash usuli asosida almashtirish bloki (S-box) lardan foydalanib, ushbu bloklarda kirish baytlariga teng chiqish baytlari olinadi.

Ushbu usulda kalit bilan ochiq matn qismlari XOR amalida qo'shilib, keyingi modul kirish qiymati hisoblanadi.

Ushbu usulda yaratilgan shifrlash algoritmlaridan eng mashhuri AES standarti sanalib, har uzunlikdagi kalit va blok uzunliklaridan foydalanadi.

Feystel tarmog'iga asoslangan (Feistel ciphers). Dastlabki blokli shifrlash usullari aynan Feystel tarmog'iga asoslangan bo'lib, bu tarmoqning asosi 5-rasmda keltirilgan.



*6-rasm. Feystel tarmog'i*

Ushbu tarmoq mohiyati quyidagicha, ya'ni kirish blogi (bu tarmoqda 64 bit kirish blogi tavsiya etiladi) ikki qismga(chap va o'ng qismlarga) ajratilib, kalit asosida qism ustida amallar bajariladi.

Ushbu tarmoqda ko'plab simmetrik blokli shifrlash algoritmlari yaratilgan bo'lib, ular orasida eng mashhurlari, GOST 28147-89, DES, Blowfish, CAST, Twofish va boshqalar.

Bugungi kunda ko'plab amalda qo'llanilib kelinayotgan kompьyuterlardagi arifmetik amallarni bajaruvchi qurilma ikkilik sanok sistemasida 32 razryad bilan ifodalanuvchi sonlar uchun mo'ljallangan. Kelajakda kompьyuter foydalanuvchilari uchun bundan ham katta 64, 128 va xokazo razryadli sonlar ustida arifmetik amallar bajarish imkoniyatini beruvchi tezkor qurilmalar yaratilishi tabiiy hol. Shularni hisobga olib, Feystel tarmog'iga asoslangan shifrlash algoritmlarini akslantirish asoslarini saqlab qolgan holda, K-kalit uzunliklarini oshirish masalasi yechiladi. Mana shunday masalani yechish uchun Feystel tarmog'i quyidagicha takomillashtiriladi:



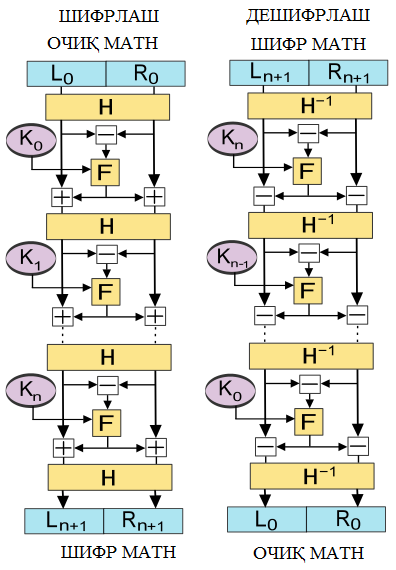
*7-rasm. Takomillashgan Feystel tarmog'i i- raundi*

**22-mavzu: Elektron raqamli imzo.**

Takomillashtirish parametri ga bog'liq holda shifrlash algoritmi xossalari va bardoshliligini saqlab qolgan holda algoritm kaliti uzunligini oshirib borish imkoniyati mavjud. Bu esa, o'z navbatida, hisoblash texnikasi qurilmalarining takomillashuvi natijasida algoritm kaliti uzunligi to'liq tanlash usuliga bardoshsiz bo'lib qolishining oldini oladi.

2. Algorim tezligi takomillashtirish parametri ga bog'liq emas, ya'ni Feystel tarmog'iga asoslangan takomillashgan va asosiy algoritm tezliklari teng. Bu xossa o'z navbatida algoritm tezligini saqlab qolgan holda takomillashtirish imkoniyatini beradi.

Lai-Massey shifrlari (Lai-Massey ciphers). Ushbu usulda asoslangan kriptografiy tizimlar Feystel tarmog'iga o'xshash bo'lib, farqli tomoni raund funksiyasi qaytmasdir. Bu usulda ham kirish bloki ikki qismga ajratiladi[12].



*8-rasm. Lai-Massey shifrlari tuzilishi*

Bunda, F raund funksiyasi, H esa yarim-raund funksiyasi. K\_0,K\_1,..K\_n lar esa 0,1,…,n ga mos raund kalitlari. Bu erda asosiy amallar quyidagilar:

Kiruvchi blok ikki teng (R0, L0) qismga bo'linadi;

Raund soniga mos quyidagi amallar ketma-ketligi bajariladi:

L\_(i+1)^',R\_(i+1)^'=H(L\_i^'+T\_i,R\_i^'+T\_i)

Shifrlangan matn esa quyidagiga teng:

(L\_(n+1),R\_(n+1) )=(L\_(n+1)^',R\_(n+1)^' ).

Shifr matnni (L\_(n+1),R\_(n+1) ) deshifrlashda raund soniga mos holda i=n,n-1,…,0 quyidagilar hisoblanadi:

(L\_i^',R\_i^')=H^(-1) (L\_(i+1)^'-T\_i,R\_(i+1)^'-T\_i)

Bu erda, T\_i=F(L\_(i+1)^'-R\_(i+1)^',K\_i ) va (L\_(n+1)^',R\_(n+1)^')=H^(-1) (L\_(n+1),R\_(n+1))

U holda ochiq matn quyidagiga teng bo'ladi: (L\_0,R\_0 )=(L\_0^',R\_0^')

Amallarga asoslangan (Operations). Hozirgi zamonaviy ko'plab simmetrik shifrlash algoritmlari va xesh qiymatlari ARX (add-rotate-XOR) algoritmiga asoslanadi. Bunday nomlanishiga sabab, ushbu algoritmga modul bo'yicha qo'shish, berilgan qiymat bo'yicha surish, XOR amalida qo'shish amallaridan tashkil topgan.

Hozirga kunda ushbu algoritm tarkibidagi amallarni apparat va dasturiy tarzda amalga oshirish sodda bo'lganligi va amallarni bajarishda yuqori tezlikga egaligi sababli juda ham mashhur. Bu turdagi algoritmlar vaqt bo'yicha bo'ladigan hujumlarga bardoshli sanalsada, surish kriptotahliliga bardoshsizdir.

Blokli shifrlash algoritmlari modellari(Block cipher mode of operation). Simmetrik shifrlash algoritmlarida xavfsizlik nuqtai-nazaridan kriptografik tizimlardan ma'lum ketma-ketliklarga asoslanib foydalinish mavjud. Bu toifadagi algoritmlar blokli shifrlash algoritimlari modellari sanaladi.

Ushbu algoritmlarda amalga oshiruvchi vektor (initialization vector, IV) dan foydalaniladi. Amalga oshiruvchi vektor ma'lum bitlar ketma-ketligidan iborat bo'lib, ochiq matnga yoki kalitga ma'lum algoritm bo'yicha qo'shiladi. Bu kattalik kalitdan farqli sanalib, odatda zarur bo'lsa ham sir saqlanmaydi.

Hozirda quyidagi modellar keng qo'llaniladi:

- Electronic codebook (ECB);

- Cipher-block chaining (CBC);

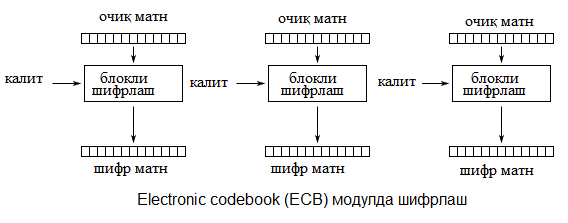
- Propagating cipher-block chaining (PCBC);

- Cipher feedback (CFB);

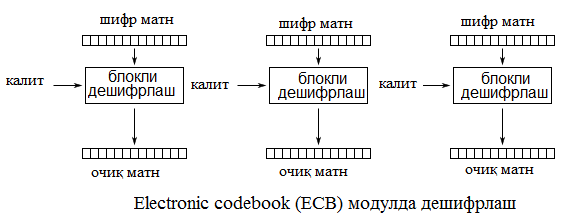
- Output feedback (OFB);

- Counter (CTR).

Electronic codebook (ECB). Dastlabki sodda modellardan biri bo'lib, ochiq mant bloklarga bo'linadi va har bir blok ustida kalit bilan amallar bajariladi.



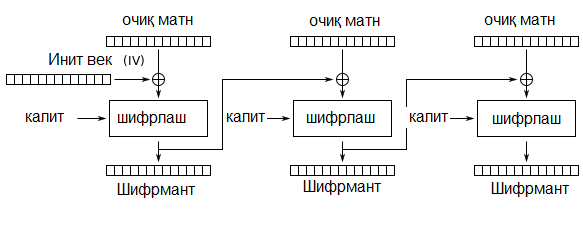
*9-rasm. ECB modulda shifrlash*



*10-rasm. ECB modulda deshifrlash*

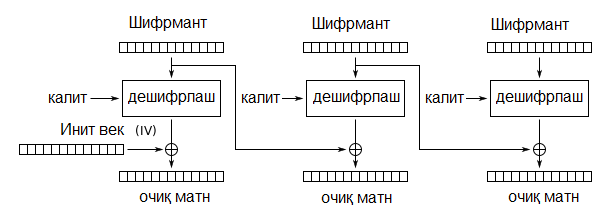
Ushbu modelning asosiy kamchiligi bir xil ochiq matn bir xil shifr matnga almashadi. Bulardan tashqari bu model matnni yashirish kabi vazifalarni bajarmaydi. Shularni hisobga olgan holda o'ta maxfiy axborotlar bilan ishlashda ushbu modeldan foydalanish tavfiya etilmaydi.

Cipher-block chaining (CBC). Ushbu model 1976 yil IBM tomonidan ishlab chiqilgan bo'lib, dastlab ochiq matnga boshlang'ich vektor qo'shilib, natija kalit yordamida shifrlanadi.



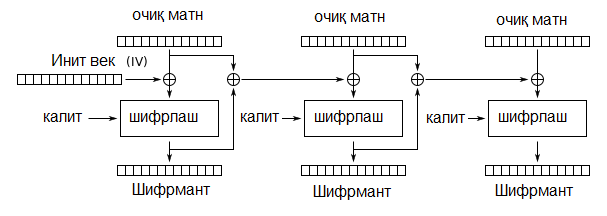
*11-rasm. SVS modelda shifrlash*

Deshifrlashda shifrmatn kalit yordamida deshifrlanib, boshlang'ich vektorga qo'shiladi va natijada ochiq matn olinadi.

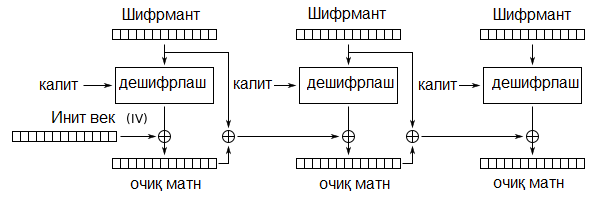


*12-rasm. SVS modelda deshifrlash*

Propagating cipher-block chaining (PCBC). Ushbu model Kerberos v4 va WASTE pratakollarida foydalanilgan bo'lsada, bardoshlsizligi sababli amalda keng qo'llanilmaydi.

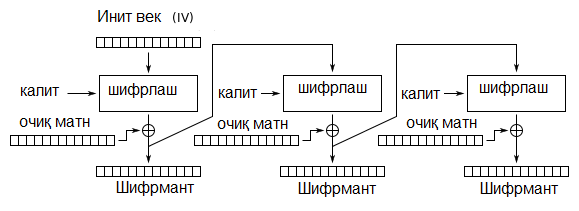


*13-rasm. RSVS modelda shifrlash*

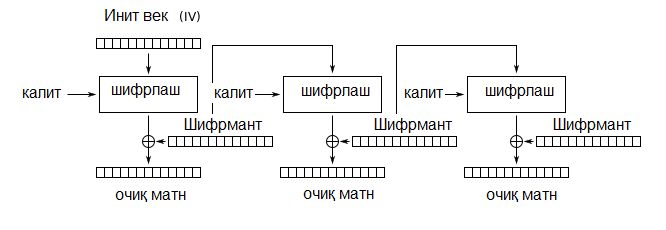


*14-rasm. RSVS modelda deshifrlash*

Cipher feedback (CFB). Ushbu model SVS modeliga yaqin bo'lib, ushbu modelda deshifrlash SVS modelida shifrlash amaliga o'xshaydi.

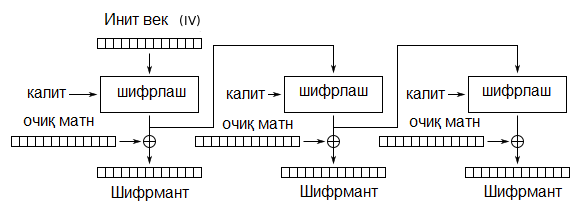


*15-rasm. CFB modelda shifrlash*

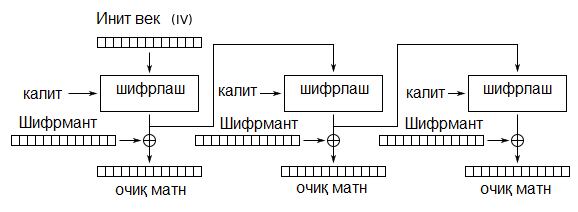


*16-rasm. CFB modelda deshifrlash*

Output feedback (OFB). Ushbu modelda shifrlash amali sinxron oqimli shifrlash algoritmlarida blokli shifrlashni amalga oshirish uchun amalda foydalaniladi. Ushbu modelda shifrlashda keyingi blok oldingi blokga bog'liq bo'lganligi sababli, parallel ravishda amalga oshirish imkoniyati mavjud emas.



*17-rasm. OFB modelda shifrlash*



*18-rasm. OFB modelda shifrlash*

**23-mavzu: Xodimlarning maxfiy ma’lumotlarga kirishlarini ro’yxatga olish.**

Elektron biznes xaridor va sotuvchi orasidagi aloqani tashkil etish, buyurtmani ifodalash, muxokama qilish, o’zgartirish, tovarlarni va xizmatlarni sotish usullarini hamda to’lovni amalga oshirish jarayonlarini o’zgartirish uchun yangi texnologiyalardan foydalanadi. Hozirda elektron tijorat va biznesning aksariyat - 49 - muammolari axborot xavfsizligi bilan bog’liq, ya’ni xavfsizlik muammolari elektron tijorat va biznes rivojidagi jiddiy to’siq xisoblanadi. Har qanday tijorat kompaniyasining boshqa kompaniyalar bilan yoki ushbu kompaniyaning bo’limlari orasida aloqa o’rnatilishi zarur. Hozirda global Internet tarmog’i o’zining uzellari o’rtasida ishonchli va arzon axborot almashinuvini ta’minlaydi. Ochiq global Internet tarmog’i kanallaridan faol foydalanuvchi elektron biznesning ishlashi jarayonida ko’pgina xavf-xatarlar paydo bo’ladi. Internetdan foydalanish kanallari kompaniyaning axborot resurslaridan chetdan foydalanishga imkon berishi mumkin. Kommunikatsion, xususan HTTP — protokol asosidagi dasturlardan extiyotsizlik bilan foydalanish axborot tizimining ishga layoqatligini buzuvchi va/yoki axborot tizimima’lumotlarini buzuvchi maxsus dastur — "Troyan otlarining" kirishiga olib kelishi mumkin. Bu xil dasturlarning ichida viruslar eng tarqalgan. O’ziga xos malakali mutaxassislar korporativ axborot tarmoqlariga bilinmasdan kirish uchun ko’pincha umummaqsad tarmoqlardan foydalanadilar. Elektron qutisining tez-tez ishlatilishi niyati buzuq odamlarga elektron biznes bilan shug’ullanuvchi tashkilot foydalananuvchilari nomlarini obro’sizlantirishga yordam berishi mumkin. Foydalanuvchilar ma’lumotlarini (ismlar, parollar, PIN — kodlar va h.) saqlovchi tizimining zaif joylarini qidirishdan tarmoqda keng ishlatiluvchi maxsus dasturlardan foydalanish mumkin. Internet konfidentsial axborotni dunyoning istalgan nuqtasiga yuborishi mumkin, ammo agar u yetarlicha ximoyalanmagan bo’lsa, ushlab qolinishi, nusxalashtirilishi, o’zgartirilishi hamda har qanday chetdagi foydalanuvchilar -niyati buzuq odamlar, raqiblar va oddiy qiziquvchilar tomonidan o’qilishi mumkin. Masalan, yetarlicha himoyalanmagan to’lov topshirig’i yoki kredit kartochka nomerini jo’natayotganda esda tutish lozimki, jo’natish xususiy/shaxsiy tarmoq orqali amalga oshirilmayapti va chetdagi foydalanuvchilar xabaringizni manipulyatsiya qilish imkoniyatiga ega. Undan tashqari xabaringiz almashtirilib qo’yilishi mumkin: xabarlarni xuddi V foydalanuvchidan yuborilganidek A foydalanuvchidan yuborish usullari mavjud. Internet tarmog’i mahsus paket, tamomila qonuniy paketlar, sonining xaddan tashqari ko’pilgi uzatishdagi buzilishlar, tarmoq komponentlarining nosozligi tufayli ishga layoqat bo’lmasligi mumkin. Bunday xollar ―xizmat qilishdan voz kechish‖ deb ataladi va elek-tron tijorat uchun eng jiddiy tahdid hisoblanadi. Axborot xavfsizligi elektron biznes tizimining eng muxim elementlaridan biri xisoblanadi va usullar va vositalarning butun bir to’plami yordamida ta’minlanishi shart. Elektron tijorat sohasidagi savdo ko’lami Internet xavfsizligi masalalaridan tashvishlangan xaridorlar, sotuvchilar va moliya insitutlarining boshidan kechiruvchi qo’rquvlari bilan chegaralanadi. Bu qo’rquvlar, hususan, quyidagilarga asoslanadi: - konfidentsiallikka kafolatning yo’qligi-kimdir ma’lumotlaringizni uzatilayotganida ushlab qolishi va qiymatli axborotni (masalan, kredit kartochkangizning nomerini, tovar yetqazib berish sanasi va adres) topishga urinishi mumkin; - amalda ishtirok etuvchilarni tekshirish darajasining yetarli emasligi - tranzaktsiya qatnashchilari tekshirilmaganida tomonlarning biri ―maskarad‖ uyushtirishi mumkinki, uning oqibati ikkinchi tomonga ancha qimmatga tushadi. Masalan, xaridor saytga kirib undagi kompaniyaning haqiqiyligiga shubha qiladi, shunday hol ham ro’y berishi - 50 - mumkinki, xaridor kredit kartochkasining nomerini yetarlicha vakolatga ega bo’lmagan shaxsga beradi; - sotuvchida buyurtma bergan xaridor kredit kartochkasining qonuniy egasi ekanliginining tekshirish imkoni yo’q; - kredit kartochkasining bank - emitenti to’lovni bajarishga talab qo’ygan sotuvchini tekshirishni istab qolishi mumkin; - ma’lumotlar yaxlitligiga kafolat yo’q - xatto ma’lumotlarni jo’natuvchi indentifikatsiyalangan bo’lsada, uchinchi tomon ma’lumotlarni, ular uzatilishi vaqtida, o’zgartirish imkoniyatiga ega. Axborot xavfsizligini ta’minlash nuqtai nazaridan elektron tijoratning namunaviy qo’llanilishini — Internet orqali maxsulotga va xizmatlarga ega bo’lishni ko’raylik. Ushbu jarayon quyidagi bosqichlar orqali ifodalanishi mumkin. 1. Buyurtmachi Web-server orqali maxsulot yoki xizmatni tanlaydi va mos buyurtmani rasmiylashtiradi. 2. Buyurtma magazinning buyurtmalar ma’lumotlari bankiga kiritiladi. 3. Buyurtma berilgan maxsulot yoki xizmatni olish mumkinligini ma’lumotlarning markaziy bazasi orqali tekshiriladi. 4. Agar mahsulotning olinishi mumkin bo’lmasa, buyurmachi u to’g’rida ogohlantiriladi va mahsulot yoki xizmatga ega bo’lish jarayoni to’xtatiladi. Mahsulotga so’rov boshqa skladga (buyurtmachi roziligida) yo’naltirilishi mumkin. 5. Agar maxsulot yoki xizmat mavjud bo’lsa buyurtmachi to’lovni tasdiqlaydi va buyurtma mos ma’lumotlar bazasiga kiritiladi. Elektron magazin mijozga buyurtma tasdig’ini yuboradi. Ko’pgina xollarda (ayniqsa endigina ish boshlagan kompaniyalarda) buyurtmalar, tavarlarning borligini tekshirish va h. uchun yagona ma’lumotlar bazasi mavjud. 6. Mijoz onlayn rejimida buyurtma xaqini to’laydi. 7. Tovar buyurtmachiga yetqaziladi. Elektron tijorat bilan shug’ullanadigan kompaniyalar yuqorida keltirilgan bosqichlarda duch keladigan tahdidlar quyidagilar: - elektron magazin Web-saytining sahifasini almashtirib quyish. Bu tahdidni amalga oshirishning asosiy usuli — foydalanuvchi so’rovini boshqa serverga yo’llash. Bu tahdid oltincha bosqichda buyurtmachi kredit kartochkasining nomerini kiritganda kuchayadi; - yolg’on buyurtmalar berish va elektron magazin xodimlari tomonidan firibgarlik qilish. Hozirda ichki/tashqi tahdidlar munosabati 60/40ni tashkil etadi; - elektron tijorat tizimida uzatiladigan ma’lumotlarni ushlab qolish. Buyurtmachining kredit kartasi xususidagi axborotni ushlab qolish o’zgacha xavf-xatarni tug’diradi; - kompaniyaning ichki tarmog’iga kirish va elektron magazin komponentlarini obro’sizlantirish; - ―xizmat qilishdan voz kechish‖ (denial of service) xujumini amalga oshirish va elektron tijorat ishlashini yoki uning uzelini buzish. - 51 - Ushbu tahdidlar natijasida kompaniya - elektron bitim provayderi - mijozlar ishonchini yo’qotadi, moddiy zarar ko’radi. Ba’zi xollarda bu kompaniyalarga kredit kartochka nomeri fosh qilingani uchun da’vo qo’zg’atilishi mumkin. ―Xizmat qilishdan voz kechish‖ xujumsi natijasida elektron magazinning ishlashi buzilishi mumkin, uning ishga layoqatligini tiklashga inson, vaqt va material resurslari talab etiladi.

**24-mavzu: Blokli shifrlsh algoritmi.**

Birinchi bo'limda biz simmetrik kriptotizimlarni ikki turga, ya'ni blokli va oqimli shifrlashga ajratgan edik. Kriptografiyada blokli shifrlash algoritmlari keng qo'llanilib, mohiyat jixatdan quyidagicha. Masalan, ochiq matn 128-bit uzunlikka ega bo'lgan qismlarga ajratiladi va har bir qismlar ustida alohida-alohida amallar bajariladi. Kiruvchi ushbu qism ustida maxfiy kalit asosida amallar bajariladi va natijada 128-bitli shifr matn olinadi.

Blokli shifrlash algoritmlari yaratilish asosiga ko'ra quyidagi turlarga bo'linadi:

Takrorlanuvchi blokli shifrlash(Iterated block ciphers);

O'zratirish-almashtirish tarmoqlari (Substitution-permutation networks);

Feystel tarmog'iga asoslangan (Feistel ciphers);

Lai-Massey shifrlari (Lai-Massey ciphers);

Amallarga asoslangan(Operations);

Takrorlanuvchi blokli shifrlash(Iterated block ciphers). Ko'plab blokli shifrlash algoritmlari takrorlanuvchi shifrlash algoritmlariga asoslanadi, ya'ni ochiq matnning aniq bir bo'lagi qaytariluvchi almashtirish amali orqali shifr matnning aniq bir qismiga almashtiriladi. Ushbu qaytariluvchi almashtirish amali odatda raund amali deb atalib, har bir almashtirish jarayoni raund deb ataladi.

Odatda raund fuknsiyasi R har bir raunda alohida qiymatlar oladi, Ki. Ular esa o'z o'rnida haqiqiy kalitdan hosil qilinadi.

M\_i=R\_(K\_i ) (M\_(i-1))

Bu erda, M\_0- ochiq matn, M\_r - shifr matn raundga mos holda.

Odatda kalit bilan ochiq matn XOR amali orqali qo'shiladi.

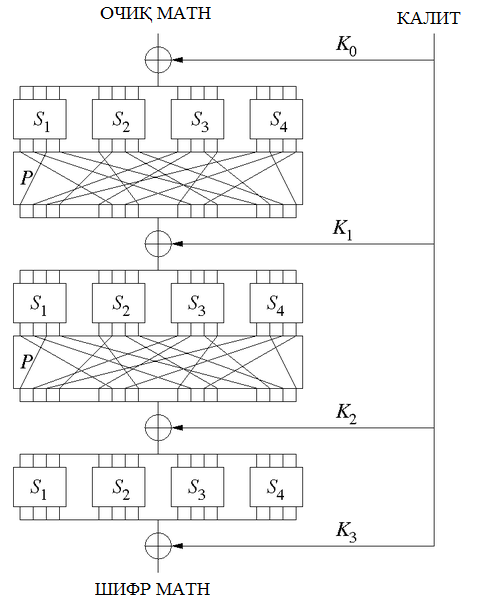
M\_i=M⨁K\_0

M\_i=R\_(K\_i ) (M\_(i-1) );i=0..r

C=M\_r⊕K\_(r+1)

O'zgaratirish-almashtirish tarmoqlari (Substitution-permutation networks). Blokli shifrlash algoritmlari orasida eng muhim bo'lgan yaratish turlaridan biri o'zratirish-almashtirish tarmoqlari (Substitution-permutation networks, SPN) sanalib, har bir raundda aynan bir bir xil belgilangan amallar bosqichi bajariladi.

Ushbu usulda shifrlash algoritmi quyidagicha :



*5-rasm. SPN tarmoq tuzilishi*

Ushbu shifrlash usuli asosida almashtirish bloki (S-box) lardan foydalanib, ushbu bloklarda kirish baytlariga teng chiqish baytlari olinadi.

Ushbu usulda kalit bilan ochiq matn qismlari XOR amalida qo'shilib, keyingi modul kirish qiymati hisoblanadi.

Ushbu usulda yaratilgan shifrlash algoritmlaridan eng mashhuri AES standarti sanalib, har uzunlikdagi kalit va blok uzunliklaridan foydalanadi.

Feystel tarmog'iga asoslangan (Feistel ciphers). Dastlabki blokli shifrlash usullari aynan Feystel tarmog'iga asoslangan bo'lib, bu tarmoqning asosi 5-rasmda keltirilgan.



*6-rasm. Feystel tarmog'i*

Ushbu tarmoq mohiyati quyidagicha, ya'ni kirish blogi (bu tarmoqda 64 bit kirish blogi tavsiya etiladi) ikki qismga(chap va o'ng qismlarga) ajratilib, kalit asosida qism ustida amallar bajariladi.

Ushbu tarmoqda ko'plab simmetrik blokli shifrlash algoritmlari yaratilgan bo'lib, ular orasida eng mashhurlari, GOST 28147-89, DES, Blowfish, CAST, Twofish va boshqalar.

Bugungi kunda ko'plab amalda qo'llanilib kelinayotgan kompьyuterlardagi arifmetik amallarni bajaruvchi qurilma ikkilik sanok sistemasida 32 razryad bilan ifodalanuvchi sonlar uchun mo'ljallangan. Kelajakda kompьyuter foydalanuvchilari uchun bundan ham katta 64, 128 va xokazo razryadli sonlar ustida arifmetik amallar bajarish imkoniyatini beruvchi tezkor qurilmalar yaratilishi tabiiy hol. Shularni hisobga olib, Feystel tarmog'iga asoslangan shifrlash algoritmlarini akslantirish asoslarini saqlab qolgan holda, K-kalit uzunliklarini oshirish masalasi yechiladi. Mana shunday masalani yechish uchun Feystel tarmog'i quyidagicha takomillashtiriladi:



25-mavzu: Blowish kripto algoritmi.

Blowfish algoritmi B. Shnayer tomonidan ishlab chiqilgan bo'lib, 1993 yilda e'lon qilingan. B. Shnayer algoritmga quyidagilarni asos qilib olingan.

* Tezlik. 32 razryadli mikroprotsessorlarda Blowfish algoritmi 26 taktda shifrlaydi.
* Kompaktlilik. Blowfish kompьyuter xotirasida eng kamida 5 kilobayt joy egallaydi.
* Oddiylik. Blowfish algoritmida qo'shish, XOR, va tablitsadan o'rin almashtirish qo'llaniladi. Bu esa tahlilni osonlashtiradi.
* O'zgaruvchan bardoshlilik. Blowfish algoritmi kaliti uzunligi o'zgaruvchan va 448 bitgacha yetish mumkin.

Bu algoritm Feystel tarmog'iga asoslangan bo'lib, bloki uzunligi 64 bitga, raundlar soni 16 ga va raund kalitlari uzunligi esa 32 bitga teng. Blowfish shifrlash algoritmi i-raundi quyidagi funksional sxemada keltirilgan:



*23-rasm. Blowfish kriptoalgoritmining i-raundi*

Blowfish kriptoalgoritmi raundilari F funksiyasi quyidagicha:

1) 32 bitli chap qism 8 bitli  qismlarga bo'linadi.

2)  8 bitli qismlar  bloklar yordamida o'rin almashtiriladi. O'rin almashtirish formulasi quyidagicha:

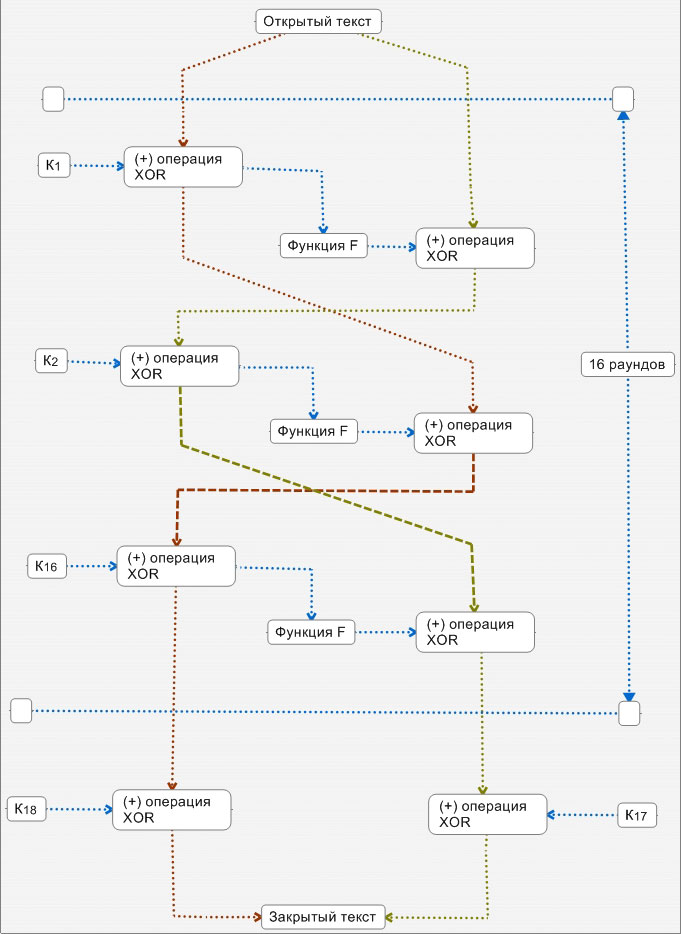


Bu yerda har bir -blok 256 ta 32 bitli elementga ega, ya'ni 8 bitli sonni 32 bitli songa akslantirib beradi. Masalan, birinchi -blok quyidagicha:

*2-jadval*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0xd1310ba6 | 0x98dfb5ac | 0x2ffd72db | 0xd01adfb7 | 0xb8e1afed | 0x6a267e96 | 0xba7c9045 | 0xf12c7f99 |
| 0x24a19947 | 0xb3916cf7 | 0x0801f2e2 | 0x858efc16 | 0x636920d8 | 0x71574e69 | 0xa458fea3 | 0xf4933d7e |
| 0x0d95748f | 0x728eb658 | 0x718bcd58 | 0x82154aee | 0x7b54a41d | 0xc25a59b5 | 0x9c30d539 | 0x2af26013 |
| 0xc5d1b023 | 0x286085f0 | 0xca417918 | 0xb8db38ef | 0x8e79dcb0 | 0x603a180e | 0x6c9e0e8b | 0xb01e8a3e |
| 0xd71577c1 | 0xbd314b27 | 0x78af2fda | 0x55605c60 | 0xe65525f3 | 0xaa55ab94 | 0x57489862 | 0x63e81440 |
| 0x55ca396a | 0x2aab10b6 | 0xb4cc5c34 | 0x1141e8ce | 0xa15486af | 0x7c72e993 | 0xb3ee1411 | 0x636fbc2a |
| 0x2ba9c55d | 0x741831f6 | 0xce5c3e16 | 0x9b87931e | 0xafd6ba33 | 0x6c24cf5c | 0x7a325381 | 0x28958677 |
| 0x3b8f4898 | 0x6b4bb9af | 0xc4bfe81b | 0x66282193 | 0x61d809cc | 0xfb21a991 | 0x487cac60 | 0x5dec8032 |
| 0xef845d5d | 0xe98575b1 | 0xdc262302 | 0xeb651b88 | 0x23893e81 | 0xd396acc5 | 0x0f6d6ff3 | 0x83f44239 |
| 0x2e0b4482 | 0xa4842004 | 0x69c8f04a | 0x9e1f9b5e | 0x21c66842 | 0xf6e96c9a | 0x670c9c61 | 0xabd388f0 |
| 0x6a51a0d2 | 0xd8542f68 | 0x960fa728 | 0xab5133a3 | 0x6eef0b6c | 0x137a3be4 | 0xba3bf050 | 0x7efb2a98 |
| 0xa1f1651d | 0x39af0176 | 0x66ca593e | 0x82430e88 | 0x8cee8619 | 0x456f9fb4 | 0x7d84a5c3 | 0x3b8b5ebe |
| 0xe06f75d8 | 0x85c12073 | 0x401a449f | 0x56c16aa6 | 0x4ed3aa62 | 0x363f7706 | 0x1bfedf72 | 0x429b023d |
| 0x37d0d724 | 0xd00a1248 | 0xdb0fead3 | 0x49f1c09b | 0x075372c9 | 0x80991b7b | 0x25d479d8 | 0xf6e8def7 |
| 0xe3fe501a | 0xb6794c3b | 0x976ce0bd | 0x04c006ba | 0xc1a94fb6 | 0x409f60c4 | 0x5e5c9ec2 | 0x196a2463 |
| 0x68fb6faf | 0x3e6c53b5 | 0x1339b2eb | 0x3b52ec6f | 0x6dfc511f | 0x9b30952c | 0xcc814544 | 0xaf5ebd09 |
| 0xbee3d004 | 0xde334afd | 0x660f2807 | 0x192e4bb3 | 0xc0cba857 | 0x45c8740f | 0xd20b5f39 | 0xb9d3fbdb |
| 0x5579c0bd | 0x1a60320a | 0xd6a100c6 | 0x402c7279 | 0x679f25fe | 0xfb1fa3cc | 0x8ea5e9f8 | 0xdb3222f8 |
| 0x3c7516df | 0xfd616b15 | 0x2f501ec8 | 0xad0552ab | 0x323db5fa | 0xfd238760 | 0x53317b48 | 0x3e00df82 |
| 0x9e5c57bb | 0xca6f8ca0 | 0x1a87562e | 0xdf1769db | 0xd542a8f6 | 0x287effc3 | 0xac6732c6 | 0x8c4f5573 |
| 0x695b27b0 | 0xbbca58c8 | 0xe1ffa35d | 0xb8f011a0 | 0x10fa3d98 | 0xfd2183b8 | 0x4afcb56c | 0x2dd1d35b |
| 0x9a53e479 | 0xb6f84565 | 0xd28e49bc | 0x4bfb9790 | 0xe1ddf2da | 0xa4cb7e33 | 0x62fb1341 | 0xcee4c6e8 |
| 0xef20cada | 0x36774c01 | 0xd07e9efe | 0x2bf11fb4 | 0x95dbda4d | 0xae909198 | 0xeaad8e71 | 0x6b93d5a0 |
| 0xd08ed1d0 | 0xafc725e0 | 0x8e3c5b2f | 0x8e7594b7 | 0x8ff6e2fb | 0xf2122b64 | 0x8888b812 | 0x900df01c |
| 0x4fad5ea0 | 0x688fc31c | 0xd1cff191 | 0xb3a8c1ad | 0x2f2f2218 | 0xbe0e1777 | 0xea752dfe | 0x8b021fa1 |
| 0xe5a0cc0f | 0xb56f74e8 | 0x18acf3d6 | 0xce89e299 | 0xb4a84fe0 | 0xfd13e0b7 | 0x7cc43b81 | 0xd2ada8d9 |
| 0x165fa266 | 0x80957705 | 0x93cc7314 | 0x211a1477 | 0xe6ad2065 | 0x77b5fa86 | 0xc75442f5 | 0xfb9d35cf |
| 0xebcdaf0c | 0x7b3e89a0 | 0xd6411bd3 | 0xae1e7e49 | 0x00250e2d | 0x2071b35e | 0x226800bb | 0x57b8e0af |
| 0x2464369b | 0xf009b91e | 0x5563911d | 0x59dfa6aa | 0x78c14389 | 0xd95a537f | 0x207d5ba2 | 0x02e5b9c5 |
| 0x83260376 | 0x6295cfa9 | 0x11c81968 | 0x4e734a41 | 0xb3472dca | 0x7b14a94a | 0x1b510052 | 0x9a532915 |
| 0xd60f573f | 0xbc9bc6e4 | 0x2b60a476 | 0x81e67400 | 0x08ba6fb5 | 0x571be91f | 0xf296ec6b | 0x2a0dd915 |
| 0xb6636521 | 0xe7b9f9b6 | 0xff34052e | 0xc5855664 | 0x53b02d5d | 0xa99f8fa1 | 0x08ba4799 | 0x6e85076a |

**26-mavzu: Shifrlash va deshifrlash blok sxemasi**



*24-rasm.Blowfish algoritmining shifrlash blok sxemasi*

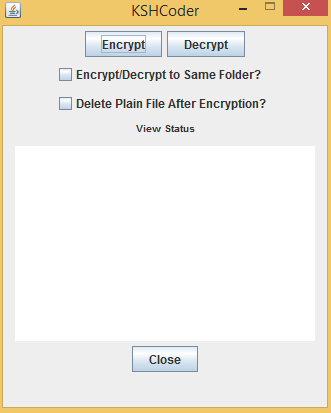
Deshifrlash jarayoni:

### 

*25-rasm.Blowfish algoritmining deshifrlash blok sxemasi*

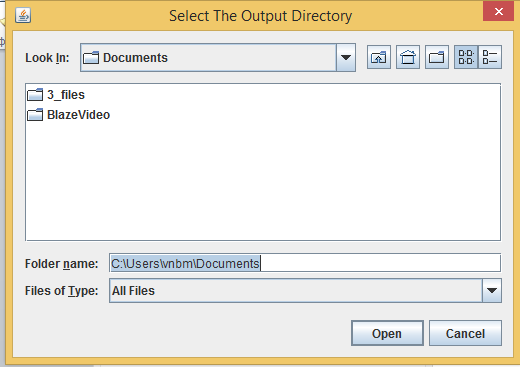
27-mavzu:Blowish kriptoalgaritmining dasturiy modeli.

Blowfish shifrlash algoritmini ishga tushirganimizda bizga quyidagi oyna hosil bo’ladi:



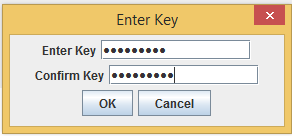
*26-rasm.Asosiy oyna*

Bu oynada biz shifrlash yoki deshifrlash turini tanlaymiz va shifrlanadigan fayl tanlanadi.



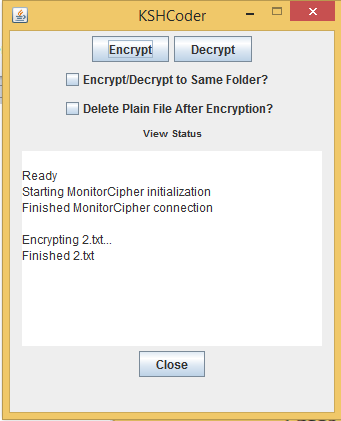
*27-rasm.Fayl tanlash oynasi*

Fayl tanlab bolinganidan keyin shifrlash kaliti tanlanadi:



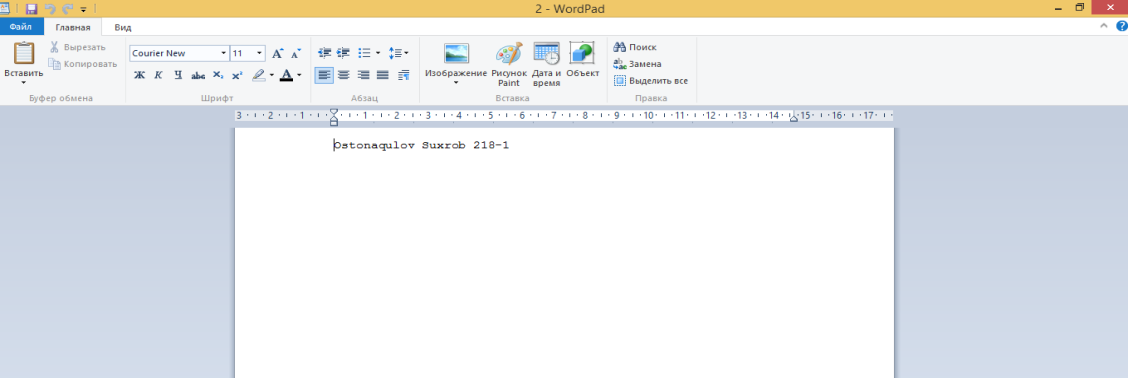
*27-rasm.Kalit kiritish oynasi.*

Kodni kiritib bo’lganimizdan keyin dastur o’z ishini yakunlanadi va bizga natijaviy fayl qaysi faylda joylashganini ko’rsatadi:



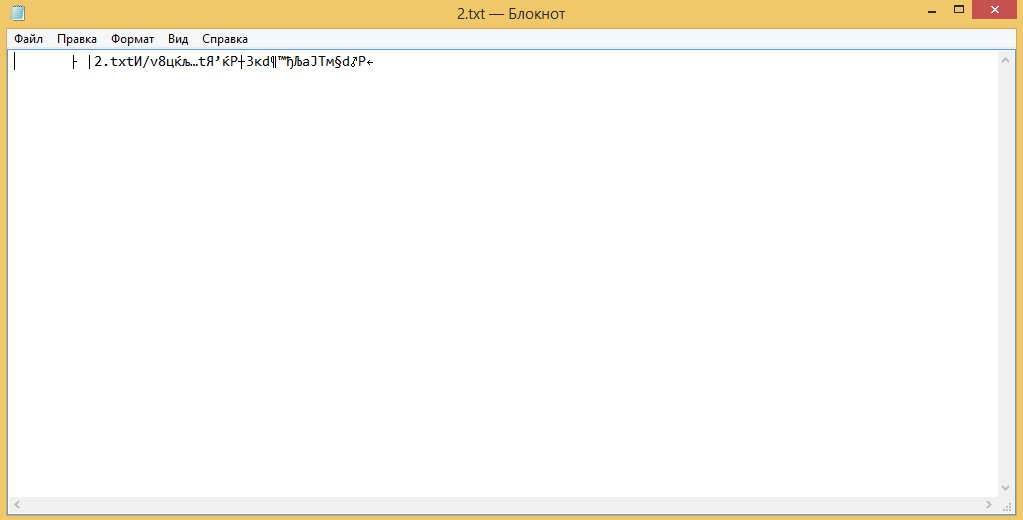
*28-rasm.Dastur yakuni*

Dastur quyidagi ochiq matnni shifrlaydi:



*29-rasm.Ochiq matn*

Dastur natijasi quyidagicha:



*30-rasm.shifrmatn*

28-mavzu: Axborotlarni kriptografiyali himoyalash tamoyillari.

Axborotning himoyalashning aksariyat mexanizmlari asosini shifrlash tashkil etadi. Axborotni shifrlash deganda ochiq axborotni (dastlabki matnni) shifrlangan axborotga o’zgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi. Axborotni qayta akslantirish yordamida himoyalash muammosi inson ongini uzoq vaqtlardan buyon bezovta qilib kelgan. Kriptografiya tarixi – inson tili tarixi bilan tengdosh. Hatto dastlabki xat yozish ham o’z-o’zicha kriptografik tizim hisoblangan, chunki qadimgi jamiyatda faqat alohida shaxslargina xat yozishni bilganlar. Qadimgi Yegipet va Qadimgi Hindistonning ilohiy kitoblari bunga misol bo’la oladi. Xat yozishning keng tarqalishi natijasida kriptografiya alohida fan sifatida vujudda keldi. Dastlabki kriptotizimlardan eramizning boshlaridayoq foydalanilgan. TSezar o’z xatlarida tizimli shifrlardan foydalangan. Kriptografik tizimlar birinchi va ikkinchi jahon urushlarida jadal rivojlandi. Urush yillaridan so’ng va hozirga qadar hisoblash vositalarining jadal rivojlanishi kriptografik usullar yaratishni tezlashtirdi va ularning mukammalligini oshirdi. Bir tomondan, kompyuter tarmoqlaridan foydalanish kengaydi, jumladan, Internet global tarmog’i. Bu tarmoqda begona shaxslardan himoyalanishi zarur bo’lgan hukumat, harbiy, tijorat va shaxsiy xarakterga ega bo’lgan axborotning katta hajmi harakatlanadi. Boshqa tomondan, qudratli kompyuterlar, tarmoqli va neyronli hisoblash texnologiyalarining paydo bo’lishi ochish mumkin emas deb hisoblangan kriptografik tizimlarning obro’siga putur yetkazdi. Kriptologiya – axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi (kryptos – maxfiy, sirli, logos - fan). Kriptologiya ikki yo’nalishga bo’linadi – kriptografiya va kriptoanaliz. Bu ikki yo’nalishning maqsadlari qaramaqarshi. Kriptografiya – axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi. Kriptoanaliz – kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi. Bu kitobda asosiy e’tibor kriptografik usullarga qaratilgan. Zamonaviy kriptografiya quyidagi to’rtta bo’limlarni o’z ichiga oladi: 1. Simmetrik kriptotizimlar. 2. Ochiq kalitli kriptotizimlar. 3. Elektron imzo tizimlari. 4. Kalitlarni boshqarish. Kriptografik usullardan foydalanishning asosiy yo’nalishi – maxfiy axborotning aloqa kanalidan uzatish (masalan, elektron pochta), uzatiladigan xabarning uzunligini o’rnatish, axborotni (hujjatlarni, ma’lumotlar bazasini) shifrlangan holda raqamli vositalarda saqlash. SHunday qilib, kriptografiya axborotni shunday qayta ishlash imkonini beradiki, bunda uni qayta tiklash faqat kalitni bilgandagina mumkin. - 21 - Shifrlash va deshifrlashda qatnashadigan axborot sifatida biror alifbo asosida yozilgan matnlar qaraladi. Bu terminlar ostida quyidagilar tushuniladi. Alifbo – axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam. Matn – alifbo elementlarining tartiblangan to’plami. Zamonaviy ATlarida qo’llaniladigan alifbolarga misol sifatida quyidagilarni keltirish mumkin: \* Z33 alifbosi – rus alifbosining 32 harflari va bo’sh joy belgisi; \* Z256 alifbosi – ASCII va KOI-8 standart kodlariga kiruvchi belgilar; \* Binar alifbo - Z2={0, 1} \* Sakkizlik yoki o’n oltilik alifbolar. SHifrlash – akslantirish jarayoni: ochiq matn deb ham nomlanadigan matn shifrmatnga almashtiriladi. Deshifrlash – shifrlashga teskari jarayon. Kalit asosida shifrmatn ochiq matnga akslantiriladi. Kalit – matnni shifrlash va shifrini ochish uchun kerakli axborot. Kriptografik tizim – ochiq matnni akslantirishning T oilasini o’zida mujassamlashtiradi. Bu oila a’zolari k bilan indekslanadi yoki belgilanadi. k parametr kalit hisoblanadi. K kalitlar fazosi – bu kalitning mumkin bo’lgan qiymatlari to’plami. Odatda kalit alifbo harflari ketma-ketligidan iborat bo’ladi. Kriptotizimlar simmetrik va ochiq kalitli tizimlarga bo’linadi. Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi. Ochiq kalitli kriptotizimlarda bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan bo’ladi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi, yopiq kalit faqat qabul qiluvchigagina ma’lum. Kalitlarni tarqatish va kalitlarni boshqarish terminlari axborotni akslantirish tizimlari jarayoniga tegishli. Bu iboralarning mohiyati foydalanuvchilar o’rasida kalit yaratish va tarqatishdir. Elektron raqamli imzo deb – xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimchaga aytiladi (elektron xujjatdagi mazkur elektron xujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan xolda maxsus o’zgartirish natijasida xosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron xujjatdagi axborotda xatolik yo’qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo). Kriptobardoshlilik deb kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifiga aytiladi. Kriptobardoshlilikning bir necha ko’rsatkichlari bo’lib, ular:

• barcha mumkin bo’lgan kalitlar soni;

• kriptoanaliz uchun zarur bo’lgan o’rtacha vaqt. Kriptografik tizim - 22 - Tk akslantirish unga mos keluvchi algoritm va k kalit qiymati bilan aniqlanadi. Axborotni himoyalash maqsadida samarali shifrlash kalitni yashirin saqlashga va shifrning kriptobardoshliligiga bog’liq. Deyarli tub son – tub bo’lish ehtimoli 1 ga yaqin. Belgi – axborotni fiksirlangan uzunlikdagi ko’rinishi SHA – Secure Hash Algorithm ma’lumotni xeshlash algoritmi vaqtinchalik shtempel - vaqtni belgilab qo’yish mexanizmi Diffi - Xellman algoritmi – ikki abonent o’rtasida o’zaro kalit almashinish algoritmi Autentifikatsiya – shaxsini haqqoniyligini tasdiqlash.

29-mavzu: Kriptografik shifrlash vositalari nima?

Ma’lumotlarni kriptografik akslantirish jarayoni dasturiy va apparatli amalga oshirilishi mumkin. Apparatli ta’minot qimmat, ammo u sermahsullik, oddiylik, himoyalanganlik kabi afzalliklarga ega. Dasturiy ta’minot foydalanishga qulayligi uchun ko’proq amaliy hisoblanadi. Amalga oshirish usullariga bog’liq bo’lmagan holda axborotni himoyalashning zamonaviy kriptografik tizimlariga quyidagi umumiy talablar qo’yiladi:

• shifrlash algoritmini bilish shifrmatn kriptobardoshliligini tushirib yubormasligi lozim. Barcha kriptotizimlar bu talabga javob berishi kerak;

• shifrlangan xabarning biror qismi va unga mos ochiq matn asosida kalitni aniqlash uchun zarur bo’lgan amallar soni mumkin bo’lgan umumiy kalitlarga sarflanadigan amallar sonidan kam bo’lmasligi kerak;

• shifrlangan matndan ochiq matnni hosil qilish uchun mumkin bo’lgan kalitlar to’plamini to’la ko’rib chiqish amallari soni qat’iy past ko’rsatkichga ega bo’lishi va zamonaviy kompyuterlar imkoniyatlari chegarasidan chiqib ketishi kerak;

• shifrlash algoritmini bilish himoyaga ta’sir qilmasligi kerak;

• kalitdagi yoki boshlang’ich ochiq matndagi kichik o’zgarishlar shifrlangan matnni tubdan o’zgartirib yuborishi kerak;

• shifrlash algoritmining tarkibiy elementlari o’zgarmas bo’lishi lozim;

• shifrlash jarayonida qo’shilgan qo’shimcha bitlar shifrmatnda bir butunligini saqlashi va yetarlicha yashirilgan bo’lishi talab etiladi

; • shifrmatn uzunligi ochiq matn uzunligiga teng bo’lishi kerak;

• shifrlash jarayonida ketma-ket qo’llaniladigan kalitlar o’rtasida o’zaro oddiy va oson bog’liqlik bo’lmasligi kerak;

• mumkin bo’lgan kalitlar to’plamidagi ixtiyoriy kalit, shifrmatnning kriptobardoshliligini ta’minlashi kerak;

• algoritm ham dasturiy, ham apparatli realizatsiyaga qulay, va kalit uzunligining o’zgarishi, shifrlash algoritmining sifatini pasaytirmasligi kerak. - 23 - Axborotni simmetrik algoritmlar asosida kriptografik ximoyalash tamoyillari Shifrlash kriptotizimining umumlashtirilgan sxemasi Uzatiluvchi axborot matni M kriptografik o’zgartirish Yek1 yordamida shifrlanadi, natijada shifrmatn C olinadi: Kriptotizimlarning ikkita sinfi farqlanadi:

1. simmetrik kriptotizim (bir kalitli);

2. asimmetrik kriptotizim (ikkita kalitli). SHifrlashning simmetrik kriptotizimida shifrlash va rasshifrovka qilish uchun bitta kalitning o’zi ishlatiladi. Demak, shifrlash kalitidan foydalanish xuquqiga ega bo’lgan har qanday odam axborotni rasshifrovka qilishi mumkin. SHu sababli, simmetrik kriptotizimlar mahfiy kalitli kriptotizimlar deb yuritiladi. Ya’ni shifrlash kalitidan faqat axborot atalgan odamgina foydalana olishi mumkin. Elektron xujjatlarni uzatishning konfidentsialligini simmetrik kriptotizim yordamida ta’minlash masalasi shifrlash kaliti konfidentsialligini ta’minlashga keltiriladi. Odatda, shifrlash kaliti ma’lumotlar fayli va massividan iborat bo’ladi va shaxsiy kalit eltuvchisidan masalan, disketda yoki smart-kartada saqlanadi. SHaxsiy kalit eltuvchisi egasidan boshqa odamlarning foydalanishiga qarshi choralar ko’rilishi shart. Simmetrik shifrlash axborotni "o’zi uchun", masalan, egasi yo’qligida undan ruxsatsiz foydalanishni oldini olish maqsadida, shifrlashda juda qulay xisoblanadi. Bu tanlangan fayllarni arxivli shifrlash va butun bir mantiqiy yoki fizik disklarni shaffof(avtomatik) shifrlash bo’lishi mumkin. Simmetrik shifrlashning noqulayligi - axborot almashinuvi boshlanmasdan oldin barcha adresatlar bilan maxfiy kalitlar bilan ayirboshlash zaruriyatidir. Simmetrik kriptotizimda maxfiy kalitni aloqaning umumfoydalanuvchi kanallari orqali uzatish mumkin emas. Maxfiy kalit jo’natuvchiga va qabul qiluvchiga kalitlar tarqatiluvchi himoyalangan kanallar orqali uzatilishi kerak. Mavjud barcha kriptografik usullar quyidagi sinflarga ajratiladi: - 24 - Mono- va ko’p alifboli o’rniga qo’yishlar (podstanovkalar). Bir xil alifbodan foydalangan holda ochiq matnni boshqa matnga murakkab yoki qiyin qoida bo’yicha almashtirish o’rniga qo’yish hisoblanadi. Yuqori kriptobardoshlilikni ta’minlash uchun katta kalitlardan foydalanishga to’g’ri keladi. O’rin almashtirishlar (perestanovkalar) Bu ham uncha murakkab bo’lmagan kriptografik akslantirish hisoblanadi, odatda boshqa usullar bilan birgalikda foydalaniladi. Gamma qo’shish (Gammalash) Bu usulda kalit asosida generatsiya qilinadigan psevdotasodifiy sonlar ketmaketligi ochiq matn ustiga qo’yiladi. Blokli shifrlar shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish usullarini (mumkin bo’lgan takrorlashlar va navbatlar bilan) tasvirlaydi. Blokli shifrlar yuqori kriptobardoshlilikka ega ekanligidan amalda u yoki bu sinf akslantirishidan ko’proq uchraydi. Amerika va Rossiyaning shifrlash standartlari aynan shu sinf shifrlariga asoslangan.

30-mavzu: Kriptografik himoya.

Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilishda turli kalitlardan foydalaniladi: - ochiq kalit K axborotni shifrlashda ishlatiladi, maxfiy kalit k dan hisoblab chiqariladi; - maxfiy kalit k , uning jufti bo’lgan ochiq kalit yordamida shifrlangan axborotni rasshifrovka qilishda ishlatiladi. Maxfiy va ochiq kalitlar juft-juft generatsiyalanadi. Maxfiy kalit egasida qolishi va uni ruxsatsiz foydalanishdan ishonchli ximoyalash zarur (simmetrik algoritmdagi shifrlash kalitiga o’xshab). Ochiq kalitning nusxalari maxfiy kalit egasi axborot almashinadigan kriptografik tarmoq abonentlarining har birida bo’lishi shart. Simmetrik kriptotizimlar Podstanovkalar Gammalash Perestanovkalar Blokli shifrlar - 25 - Asimmetrik kriptotizimda shifrlangan axborotni uzatish quyidagicha amalga oshiriladi: 1. Tayyorgarlik bosqichi: - abonent V juft kalitni generatsiyalaydi: maxfiy kalit kV va ochiq kalit KV; - ochiq kalit KV abonent A ga va qolgan abonentlarga jo’natiladi. 2. A va V abonentlar o’rtasida axborot almashish: - abonent A abonent Vning ochiq kaliti KV yordamida axborotni shifrlaydi va shifrmatnni abonent Vga jo’natadi; - abonent V o’zining maxfiy kaliti kV yordamida axborotni rasshifrovka qiladi. Hech kim (shu jumladan abonent A ham) ushbu axborotni rasshifrovka qilaolmaydi, chunki abonent Vning mahfiy kaliti unda yo’q. Asimmetrik kriptotizimda axborotni ximoyalash axborot qabul qiluvchi kaliti kV ning mahfiyligiga asoslangan. Asimmetrik kriptotizimlarning asosiy hususiyatlari quyidagilar: 1. Ochiq kalitni va shifr matnni himoyalangan kanal orqali jo’natish mumkin, ya’ni niyati buzuq odamga ular ma’lum bo’lishi mumkin.

2. SHifrlash YeV : M ► C va rasshifrovka qilish DB: S ► M algoritmlari ochiq. Shifrlash standartlari. Kriptografik kalitlarni boshqarish. Xeshlash funktsiyasi O’zbekistonning axborotni shifrlash standarti. Ushbu "Ma’lumotlarni shifrlash algoritmi" standarti O’zbekiston aloqa va axborotlashtirish agentligining ilmiy-texnik va marketing tadqiqotlari markazi tomonidan ishlab chiqilgan va unda O’zbekiston Respublikasining "Elektron raqamli imzo xususida"gi va "Elektron xujjat almashinuvi xususida"gi qonunlarining me’yorlari amalga oshirilgan. Ushbu standart — kriptografik algoritm, elektron ma’lumotlarni himoyalashga mo’ljallangan. Ma’lumotlarni shifrlash algoritmi simmetrik blokli shifr bo’lib, axborotni shifrlash va rasshifrovka qilish uchun ishlatiladi. Algoritm 128 yoki 256 bit uzunligidagi ma’lumotlarni shifrlashda va rasshifrovka qilishda 128, 256, 512 bitli kalitlardan foydalanishi mumkin. Rossiyaning axborotni shifrlash standarti. Rosssiya Federatsiyasida hisoblash mashinalari, komplekslari va tarmoqlarida axborotni kriptografik o’zgartirish algoritmlariga davlat standarti (GOST 2814-89) joriy etilgan. Bu algoritmlar maxfiylik - 26 - darajasi ixtiyoriy bo’lgan axborotni hech qanday cheklovsiz shifrlash imkonini beradi. Algoritmlar apparat va dasturiy usullarida amalga oshirilishi mumkin. Standartda axborotni kriptografik o’zgartirishning quyidagi algoritmlari mavjud: - oddiy almashtirish; - gammalash; - teskari bog’lanishli gammalash; - imitovstavka. AQSHning axborotni shifrlash standarti. AQSHda davlat standarti sifatida DES(Data Encryption Standart) standarti ishlatilgan. Bu standart asosini tashkil etuvchi shifrlash algoritmi IBM firmasi tomonidan ishlab chiqilgan bo’lib, AQSH Milliy Xavfsizlik Agentligining mutaxasislari tomonidan tekshirilgandan so’ng davlat standarti maqomini olgan. DES standartidan nafaqat federal departamentlar, balki nodavlat tashkilotlar, nafaqat AQSHda, balki butun dunyoda foydalanib kelingan. Kriptografik kalitlarni boshqarish Har qanday kriptografik tizim krpitografik kalitlardan foydalanishga asoslangan. Kalit axboroti deganda axborot tarmoqlari va tizimlarida ishlatiluvchi barcha kalitlar majmui tushuniladi. Agar kalit axborotlarining yetarlicha ishonchli boshqarilishi ta’minlanmasa, niyati buzuq odam unga ega bo’lib olib tarmoq va tizimdagi barcha axborotdan hohlaganicha foydalanishi mumkin. Kalitlarni boshqarish kalitlarni generatsiyalash, saqlash va taqsimlash kabi vazifalarni bajaradi. Kalitlarni taqsimlash kalitlarni boshqarish jarayonidagi eng ma’suliyatli jarayon hisoblanadi. Simmetrik kriptotizimdan foydalanilganda axborot almashinuvida ishtirok etuvchi ikkala tomon avval maxfiy sessiya kaliti, ya’ni almashinuv jarayonida uzatiladigan barcha xabarlarni shifrlash kaliti bo’yicha kelishishlari lozim. Bu kalitni boshqa barcha bilmasligi va uni vaqti-vaqti bilan jo’natuvchi va qabul qiluvchida bir vaqtda almashtirib turish lozim. Sessiya kaliti bo’yicha kelishish jarayonini kalitlarni almashtirish yoki taqsimlash deb ham yuritiladi. Asimmetrik kriptotizimda ikkita kalit-ochiq va yopiq (maxfiy) kalit ishlatiladi. Ochiq kalitni oshkor etish mumkin, yopiq kalitni yashi-rish lozim. Xabar almashinuvida faqat ochiq kalitni uning haqiqiyligini ta’minlagan holda jo’natish lozim. Kalitlarni taqsimlashga quyidagi talablar qo’yiladi: • taqsimlashning operativligi va aniqligi; • taqsimlanuvchi kalitlarning konfidentsialligi va yaxlitligi. Kompyuter tarmoqlaridan foydalanuvchilar o’rtasida kalitlarni taqsimlashning quyidagi asosiy usullaridan foydalaniladi. 1. Kalitlarni taqsimlovchi bitta yoki bir nechta markazlardan foydalanish. 2. Tarmoq foydalanuvchilari o’rtasida kalitlarni to’g’ridan-to’g’ri almashish. Birinchi usulning muammosi shundaki, kalitlarni taqsimlash markaziga kimga, qaysi kalitlar taqsimlanganligi ma’lum. Bu esa tarmoq bo’yicha uzatilayotgan barcha xabarlarni o’qishga imkon beradi. Bo’lishi mumkin bo’lgan suiiste’mollar tarmoq xavfsizligining jiddiy buzilishiga olib kelishi mumkin. - 27 - Xeshlash funktsiyasi Xeshlash funktsiyasi (xesh-funktsiyasi) shunday o’zgartirishki, kirish yo’liga uzunligi o’zgaruvchan xabar M berilganida chišish yo’lida belgilangan uzunlikdagi šator h(M) ќosil bo’ladi. Boshšacha aytganda, xesh-funktsiya h(.) argument sifatida uzunligi ixtiyoriy xabar (xujjat) M ni šabul šiladi va belgilangan uzunlikdagi xeshšiymat (xesh) H=h(M)ni šaytaradi. Xeshlash funktsiyasi šuyidagi xususiyatlarga ega bo’lishi lozim: 1. Xesh-funktsiya ixtiyoriy o’lchamli argumentga šo’llanishi mumkin. 2. Xesh-funktsiya chišish yo’lining šiymati belgilangan o’lchamga ega. 3. Xesh-funktsiya h(x) ni ixtiyoriy "x" uchun yetarlicha oson ќisoblanadi. Xeshfunktsiyani ќisoblash tezligi shunday bo’lishi kerakki, xesh-funktsiya ishlatilganida elektron rašamli imzoni tuzish va tekshirish tezligi xabarning o’zidan foydalanilganiga šaraganda anchagina katta bo’lsin. 4. Xesh-funktsiya matn M dagi orasiga šo’yishlar (vstavki), chišarib tashlashlar (vыbrosы), joyini o’zgartirishlar va ќ. kabi o’zgarishlarga sezgir bo’lishi lozim. 5. Xesh-funktsiya šaytarilmaslik xususiyatiga ega bo’lishi lozim. 6. Ikkita turli xujjatlar (ularning uzunligiga boђliš bo’lmagan ќolda) xeshfunktsiyalari šiymatlarining mos kelishi eќtimolligi juda kichkina bo’lishi shart, ya’ni ќisoblash nuštai nazaridan h(x')=h(x) bo’ladigan x'≠ xni topish mumkin emas.