10-AMALIY MASHG’ULOT. AXBOROT XAVFSIZLIGI: ASOSIY TUSHUNCHALARI, TASHKILIY –HUQUQIY TA’MINOTI.

Axborot xavfsizligi – axborot texnologiyalarining nisbatan juda yosh va tez taraqqiy etayotgan sohalaridan biridir. Uni o‘rganish uchun axborot texnologiyasining boshqa tarmoqlari bilan kelishilgan zamonaviy asosini o‘rganish kerak. Buni hal etishda obektli – yo‘naltirilgan usul jalb qilinishi mumkin.

Axborot xavfsizligi sohasida faqat majmuaviy yondashuv asosidagina muvaffaqiyatga erishish mumkin. Bu vazifani hal etish uchun qonuniy, administrativ, protsedurali va programmali-texnik darajadagi choralar ko‘riladi.

Administrativ darajadagi xavfsizligi siyosati va dasturi, ularning tipik tuzilishi, ishlab chiqish va kuzatib borish choralari bilan tanishadilar.

Axborot xafsizligi turli matnlarda har xil ma’noga ega bo‘lishi mumkin.

Bu axborot sohasidagi nusxasini jamiyatning va davlatning qiziqishlarini muvozannatlashtirilgan yig‘indisi bilan aniqlanadigan milliy qiziqishlarining himoyalanganlik xolatlarini ifoda etish mumkin.

Shu kungacha «Axborot xavfsizligi» atamasini torroq ma’noda foydalangan. *“Axborot xavfsizligi”* deganda biz axborotni himoyalanganligi va axborotni munosobatda bo‘lgan subektlarga, shu jumladan axborot egasi foydalanuvchi hamda infratizimni qo‘llab-quvvatlab turuvchilariga ham noqulay zarar keltirishi mumkin bo‘lgan tasodifiy yoki oldindan mo‘ljallangan tabiiy va sun’iy turdagi ta’sirlardan qo‘riqlab turuvchi infratizimni tushunamiz.

*Axborot himoyasi* – axborot xavfsizligini ta’minlashga qaratilgan tadbirlar, uslublar va vositalari majmuasida iborat bo‘lib, axborotni to‘laligi; kompyuter ashyolari va unda saqlanayotgan dasturlar hamda ma’lumotlarga ruxsatsiz kirishni oldini olish; kompyuterlardagi dasturlarni ruxsatsiz foydalanishini oldini olish kabi asosiy vazifalarni ta’minlaydi:

Axborot odam, apparat va dastur orqali yo‘nalishlarida tarqalishi mumkin.

*Odamlar orqali:*

- begona shaxs tomonidan ekrandan axborotni o‘qish;

- shifrlangan axborotni dastur yordamida ochish;

- axborot tashuvchilar (disk, disketalar)ni o‘g‘irlash.

*Apparat orqali:*

- axborotlarga kirishni ta’minlaydigan maxsus apparat vositalarini kompyuterga ulash;

- elektromagnit signallarni ushlab qolish uchun maxsus texnika vositalarini qo‘llash.

*Dastur orqali:*

- axborotga dastur orqali ruxsatsiz kirishi;

- shifrlangan axborotni dastur orqali ochish;

- axborotni tashuvchilardan dastur orqali nusxalash mobaynida axborot chiqib ketishi mumkin.

Shunday qilib, axborot xavfsizligiga yondashuv, axborot tizimlari (AT)ni foydalanish bilan bog‘liq bo‘lgan axborot munosabat subektlari va bu subektlarni qiziqishlarini aniqlashdan boshlab uslubiy nuqtai nazardan to‘g‘ri bo‘ladi. Axborot xavfi – axborot texnologiyasini foydalanishning teskari tomonidir.

**Axborot xavfsizligining asosiy tashkil etuvchilari**

Axborot xavfsizligi faqat muvaffaqiyatli tizimi va kompleks yondoshuv olib keladigan ko‘p qirrali, xatto ko‘p o‘lchovli faoliyat soxasidir.

Axborot texnologiyasini foydalanish bilan aloqador, subektlarning qiziqish tamoyillarini ta’minlashni quyidagi turlariga ajratish mumkin: axborot ashyolari va qo‘llanib turadigan infrastrukturasining ochiqligi, butunligi va maxfiyligi.

Ba’zi axborot xavfsizligi asosiy tashkil etuvchilari qatoriga axborotni maxsus ruxsat (sanksiyalanmagan) nusxalashdan himoya qilishni ham qo‘shadilar.

Axborot xavfsizligi ochiqlik, butunlik va maxfiylik xususiyatlariga ega.

Ochiqlik – yetarli vaqt mobaynida talab qilingan axborot xizmatini olish imkoniyati, butunlik – axborotni dolzarbligi va qarama - qarshilik bo‘lmasligi, uning buzilishi va ruxsat berilmagan o‘zgartirishlardan himoyalash va maxfiylik – axborotga ruxsatsiz kirishdan himoyalashdan iborat. Zamonaviy kompyuter tizimlari va tarmoqlarida axborotni himoya qilish usullari. XXI – asrga kelib axborot – texnologiyalarining jadal sur’atlar bilan rivojlanishi, ijtimoiy jarayonning globallashuvi, axborot – telekommunikatsiya sohalarida jiddiy o‘zgarishlarni amalga oshishi, insoniyat jamiyatida bir qator muammolarni keltirib chiqardi.

Zamonaviy kompyuter tizimlarining yaratilishi va global axborot tarmoqlarining paydo bo‘lishi, kompyuter tizimlari va tarmoqlarining xavfsizligi muammosini yuzaga keltirdi.

Kompyuter tizimlari va tarmoqlarining xavfsizligi deganda, ularni meyoriy ishlash jarayoniga tasodifiy yoki oldindan mo‘ljallangan aralashishdan hamda ularni tashkil etuvchilarini o‘g‘irlashga, o‘zgartirishga yoki buzishga bo‘lgan intilishlardan himoya qilish tushuniladi.

Axborot texnologiyalari, zamonaviy kompyuter tizimlari va tarmoqlari hamda Internet tizimini rivojlanishining zamonaviy bosqichi axborot xavfsizligini ta’minlash muammosini tizimli o‘rganish zarurligini aniqlab berdi.

Kompyuter tizimlarida axborotni himoya qilish muammosi, ularni yaratilishi bilan deyarli bir vaqtning o‘zida axborot ustida yovuz niyatli harakatlarning aniq dalillari asosida kelib chiqdi. Kompyuter tizimlari va tarmoqlarining tezkor rivojlanishi, Internet tizimini haëtga keng tadbiq qilinishi bunday jinoyatlarni ko‘payishiga olib kelmoqda.

Shu munosabat bilan, zamonaviy axborotlashgan jamiyatda global va boshqa tarmoqlarning ulkan afzalliklari mavjudligi bilan bir qatorda, ularda axborotni himoya qilish bo‘yicha o‘ziga xos muammolarni ham yechishga to‘g‘ri keladi. Shuning uchun axborot maxfiyligi va butunligini ta’minlash bilan bog‘liq bo‘lgan ishlarni amalga oshirish uchun samarali vositalarni yaratish va qo‘llash hozirgi kunning muhim masalalaridan biriga aylanmoqda.

Zamonaviy kompyuter tizimlari va tarmoqlarida axborotni himoya qilish deganda uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborot ishonchliligi va butunligini tizimli ta’minlash maqsadida turli xil vosita va usullarni ishlatish choralarini ko‘rish va tadbirlarni o‘tkazish, ya’ni axborot xavfsizligining ko‘p pog‘onali, uzluksiz, majmuaviy va boshqariladigan tizimini yaratish tushuniladi.

Kompyuter tizimlari va tarmoqlarida axborot himoya qilishning tashkiliy, huquqiy va texnik usullari mavjud.

Axborotni himoya qilishning huquqiy usullari, ixtiyoriy vazifali himoya qilish tizimini rasmiy ravishda qurishni va ishlatishni asosi bo‘lib xizmat qiladi.

Tashkiliy usullar bir nechta xavflarni bartaraf etish uchun ishlatilsa, texnik usullar tashkiliy va texnik tadbirlarga asoslangan holda ko‘pchilik axborotlarni himoya qiladi.

Axborotni himoya qilishning huquqiy usullarida huquqiy xarakterli masalalar ko‘rib chiqiladi:

• kompyuter jinoyatchiligi uchun jazolash meyorlarini ishlab chiqish;

• dastur tuzuvchilarning mualliflik huquqlarini himoya qilish;

• jinoiy va fuqarolik qonunchiligi sohasida sud ishini mukammallashtirish;

• kompyuter tizimlarini ishlab chiquvchilar ustidan jamoat nazoratini o‘rnatish va mos xalqaro shartnomalarni qabul qilish va h.k.

Axborotni himoya qilishning tashkiliy usullarida quyidagi masalalar ko‘rib chiqiladi:

• kompyuter tizimlarini qo‘riqlash;

• xodimlarni tanlab olish;

• o‘ta muhim ishlarni faqat bitta odam tomonidan olib borilishi holatlarini inkor qilish;

• ishdan chiqqan tizimni keyinchalik tiklash rejasini borligi;

• axborot xavfsizligi tizimini ta’minlaydigan shaxslarga javobgarlikni berish;

• kompyuter markazini joylashgan joyini tanlash va h.k. Axborotni himoya qilishning texnik usullari apparatli, dasturli va apparat-dasturliga bo‘linadi. Texnik usullarda quyidagi xarakterdagi masalalar ko‘rib chiqiladi:

• kompyuter tizimlari va tarmoqlarida axborotga ruxsatsiz murojaat qilishdan himoya qilish;

• virusga qarshi himoya qilish;

• elektromagnit, akustik maydon va nurlanishlar orqali «ushlab» olishni bartaraf etish;

• kriptografik usul asosida xabarlarni yuqori tuzilishli berkligini ta’minlash.

Axborotni himoya qilishning yana quyidagi usullari ham mavjud:

• axborotni zahiralash yoki nusxalash usullari;

• axborotni himoya qilishning kriptografik usullari;

• simmetrik va nosimmetrik shifrlash usullari.

Axborotni zahiralash yoki nusxalash usullari axborotni tasodifiy xavflardan himoya qilishning eng samarali usullaridan biri hisoblanadi. Nusxalash bilan axborotni butunligi ta’minlanadi. Axborotni zahiralash usuli axborotni tiklash vaqti bo‘yicha tezkor va tezkor bo‘lmagan usullarga kiritiladi. Nusxalanadigan axborotni haqiqiy vaqt oralig‘ida ishlatishni ta’minlaydigan usullar tezkor usullarga tegishli bo‘ladi. Nusxalanadigan axborotni ishlatishga o‘tish, ushbu kompyuter tizimlari uchun haqiqiy vaqt oralig‘i tartibida axborotni ishlatishga so‘rovlarini bajarish imkonini beradigan vaqt ichida amalga oshiriladi. Ushbu shartni ta’minlamaydigan barcha usullar nusxalashning tezkor bo‘lmagan usuliga tegishli bo‘ladi.

Axborotni himoya qilishni kriptografik usullarida boshlang‘ich axborot shunday o‘zgartiriladiki, buning natijasida axborot kerakli vakolatlarga ega bo‘lmagan shaxslarga tanishish va ishlatish uchun mumkin bo‘lmay qoladi.

Boshlang‘ich axborotga ta’sir ko‘rinishi bo‘yicha kriptografik o‘zgartirishni shifrlash, stenografiya, kodlash va zichlash usullari mavjud.

Simmetrik va nosimmetrik shifrlash usullari kalitlar belgilari, turlari va o‘zgartirish uslubi bo‘yicha quyidagilardan iborat bo‘ladi:

• almashtirish usullari;

• qayta joylashtirish usullari;

• taxliliy usullar;

• additiv usullar;

• aralash usullar.

Bir alifboda yozilgan boshlang‘ich axborot belgilarini ma’lum bir qoida bo‘yicha boshqa alifbo belgilari bilan o‘zgartirish, almashtirish usullaridan iboratdir.

Ikkala alifbo belgilari o‘rtasidagi muvofiqlikni berilishi ma’lum bir algoritm bo‘yicha uzunligi K ta belgilardan tashkil topgan boshlangich T0 matn belgilarining sonli teng kuchlilarini o‘zgartirish yordamida amalga oshiriladi.

Qayta joylashtirish usuli boshlang‘ich matnni ma’lum bir uzunlikdagi bloklarga bo‘lib chiqish va keyinchalik aniq algoritm bo‘yicha har blok ichida belgilarni qayta joylashtirishdan iborat.

Taxliliy usullar esa matritsali algebrani ishlatishga asoslangan.

Additivli usullar (gammalash) kodlari boshlang‘ich axborotning raqamli kodlari bilan qo‘shiladigan raqamli kortejning tasodifiy ketma - ketligini ishlatadi. Gamma kalit hisoblanadi. Kalit qancha uzun bo‘lsa, kriptochidamlilik shuncha yuqori bo‘ladi.

**Kirish turlari:**

-sirli ma’lumotlarni aytish;

-axborotni о‘g‘irlanishi;

- ruxsat etilmagan murojaat qilish

**Ximoya yо‘nalishi:**

 -xuquqiy;

 -ташкилий;

 - мухандис-техник.

**Ximoya vositalari:**

 -fizik;

 -apparatli;

 - dasturli;

 -kriptografik.

**Ximoya usullari:**

 -oldini olish;

 -kesib о‘tish (chegaralash);

 - qarshi harakat.

**Axborot manbalari:**

 -odamlar;

 -xujjatlar;

 - nashriyotlar;

 -texnik tashuvchilar;

 -texnik vositalar;

 -chiqindi (musor)

**Maqsad:**

 -tanishuv;

 -modifikatsiya;

 - yо‘qotish.

**Xavf-xatar manba’lari:**

 -raqobatchilar;

 -jinoyatchilar;

 - korrupsionerlar;

 -tashkiliy qо‘mitalar.

**Xavf-xatar:**

-butunligi;

-maxfiyligi;

- tо‘liqligi;

- murojaat qilish.

**Xavf-xatar obyektlari:**

- ish olib borilishi, xolati va tarkibi xaqida ma’lumot

Diskda saqlangan fayllarning tasodifan oʽchirilgan holatlari uchrab turadi. Bu holat apparatlarning ishdan chiqishi yoki kompyuterga virus tushganda yuz berishi mumkin. Shu sababli hosil qilingan fayllarning nushalarini diskda saqlab qoʽyish mumkin. Bu axborottashuvchi DVD-RW deb nomlanib, diskdagi kerakli fayllar nushalarini saqlash uchun qulaydir. [[1]](#footnote-1)

***Axborot xavfsizligini ta’minlash***– bu foydalanuvchining axborotlarini himoyalashga quyilgan meyor va talablarni bajarishidir.

***Axborot xavfsizligi* –**bu axborot foydalanuvchilariga va ko‘plab axborot tizimlariga zarar keltiruvchi tabiiy yoki sun’iy xarakterga ega tasodifiy va uyushtirilgan ta’sirlardan axborotlarni va axborot kommunikatsiya tizim obektlarining himoyalanganligidir.

**Login** – shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi hisoblanadi.

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

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



***Ro‘yxatdan o‘tish*** – foydalanuvchi-larni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatish-ga huquq berish jarayoni.

Ayrim veb-saytlar foydalanuvchilarga qo‘shimcha xizmatlarni olish va pullik xizmatlarga obuna bo‘lish uchun ro‘yxatdan o‘tishni hamda login va parol olishni taklif qiladilar.

Foydalanuvchi ro‘yxatdan o‘tgandan so‘ng tizimda unga qayd yozuvi (account) yaratiladi va unda foydalanuvchiga tegishli axborotlar saqlanadi.

**Login va parolga ega bo‘lish shartlari.** Biror shaxs o‘zining login va paroliga ega bo‘lishi uchun u birinchidan axborot kommunikatsiya tizimida ruyxatdan o‘tgan bo‘lishi kerak va shundan so‘ng u o‘z logini va parolini o‘zi hosil qilishi yoki tizim tomonidan berilgan login parolga ega bo‘lishi mumkin.

**Login va parolni buzish.**Login va parolni buzish – bu buzg‘unchining biror bir maqsad yo‘lida axborot kommunikatsiya tizimi obektlaridan foydalanish uchun qonuniy tarzda foydalanuvchilarga tegishli login va parollarini buzishdir.

**Login va parolni o‘g‘irlash.** Login va parolni o‘g‘irlash – bu foydalanuvchilarning mahfiy ma’lumotlari bo‘lgan login va parollarga ega bo‘lish maqsadida amalga oshiriladigan internet firibgarligining bir turidir.

Axborot-kommunikatsiya tizimining ixtiyoriy tarkibiy qismlaridan biri bo‘lgan, hamda axborot tizimi taqdim etadigan imkoniyat mavjud bo‘lgan resurslardan belgilangan qoidalarga muvofiq bo‘lmagan holda, foydalanishni cheklash qoidalariga rioya qilmasdan foydalanish – bu resurslardan ruxsatsiz foydalanish toifasiga kiradi.

Bunday foydalanish natijasida quyidagi oqibatlar yuzaga kelishi mumkin:

axborotning o‘g‘irlanishi;

axborotni o‘zgartirish;

axborotning yo‘qotilishi;

yolg‘on axborotni kiritish;

axborotni qalbakilashtirish va h.k.

**Kompyuter virusi** – bu o‘z-o‘zidan ko‘payuvchi, kompyuter tarmoqlari va axborot tashuvchilari orqali erkin tarqaluvchi, hamda kompyuter va unda saqlanayotgan axborot va dasturlarga zarar yetkazuvchi dastur kodi yoki komandalar ketma-ketligi hisoblanadi.

Kompyuter viruslari quyidagi xossalarga ega: o‘zidan nusxa ko‘chirish, axborotdan ruxsatsiz foydalanishni amalga oshirish.

Virus, aksariyat hollarda nosozlik va buzilishlarga sabab bo‘ladi va biror hodisa yuz berishi bilan, masalan, aniq kunning kelishi bilan ishga tushirilishi mumkin.

Hozirgi kunda 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 yoki ***antiviruslar*** deb yuritiladi. Antivirus dasturlariga **AVP, Dr.Web, Nod32, Kasperskiy, Avira** dasturlarini kiritish mumkin.

Viruslarga qarshi kurashishning asosan quyidagi usullari mavjud:

Muntazam profilaktika ishlarini, ya’ni virusga tekshiruv ishlarini olib borish.

Taniqli virusni zararsizlantirish.

Taniqli bo‘lmagan virusni zarasizlantirish.



**Hujum tushunchasi va axborot xujumlari**

***Hujum tushunchasi*** – buzg‘unchining biror bir maqsad yo‘lida axborot kommunikatsiya tizimlarining mavjud himoyalash tizimlarini buzishga qaratilgan harakati.

*Axborot hujumlari odatda 3 ga bo‘linadi:*

Obekt haqida ma’lumotlar yig‘ish (razvedkalash) hujumi.

Obektdan foydalanishga ruxsat olish hujumi.

Xizmat ko‘rsatishdan voz kechish hujumi.

**MUSTAQIL BAJARISH UCHUN TOPSHIRIQLAR:**

**1-topshiriq.** Ish stolida **“Fayllar”** den nomlangan papka yarating va unga 5 ta turli tipdagi fayllarning nushasini yarating. **“Fayllar*”*** papkasini \*.rar turida arxivlang.

**2-topshiriq.** Ish stolida joylashga ***“Fayllar.rar”*** arxiv faylini NOD32 antivirus dasturi yordamida virusga tekshiring va flash diskka o’tkazing.

**3-topshiriq.** Oqituvchi fleshkasini NOD32 antivirus dasturi yordamida flesh qurilmani virusga tekshiring va ***“Axbotor havfsizligi”*** nomli fayllar jamlangan papkani kompyuterga ko’chirib o’tkazing.

**4-topshiriq.** **“Nima uchun” grafik organayzeri-** kompyuter viruslaridan saqlanish muammoning dastlabki sabablarini aniqlash boyicha fikrlar zanjiri.

**“Nima uchun” grafik organayzeri**

**Nima uchun?**

**Nima uchun?**

**Nima uchun?**

**Nima uchun?**

**TEST**

**1. Kompyuter tizimlari va tarmoqlarining havfsizligi deganda nimaga aytiladi?**

1. \*ularni meyoriy ishlash jarayoniga tasodifiy yoki oldindan mo‘ljallangan aralashishdan hamda ularni tashkil etuvchilarini o‘g‘irlashga, o‘zgartirishga yoki buzishga bo‘lgan intilishlardan himoya qilish tushuniladi
2. kompyuter tizimlarining meyoriy ishlash jarayoniga aniq mo‘ljallangan aralashishdan himoya qilish tushuniladi
3. to‘g‘ri javob yo‘q
4. meyoriy ishlash jarayonini buzishga bo‘lgan intilishlardan ogoh qilish tushuniladi

**2. Qayta joylashtirish usuli nimadan iborat?**

1. boshlang‘ich matnni ma’lum bir uzunlikdagi bloklarga bo‘lib chiqish va keyinchalik algoritm bo‘yicha belgilarni kiritish
2. \*boshlang‘ich matnni ma’lum bir uzunlikdagi bloklarga bo‘lib chiqish va keyinchalik aniq algoritm bo‘yicha har blok ichida belgilarni qayta joylashtirishdan iborat
3. to‘g‘ri javob yo‘q
4. boshlang‘ich matnni qayta joylashtirishdan iborat

**3. Kompyuter tizimlari va tarmoqlarida axborot himoya qilishning necha usuli mavjud:**

1. 2
2. 12
3. 5
4. \*3

**4. Axborot qanday yo‘nalishlarda tarqalishi mumkin?**

1. kompyuter orqali, transport orqali, havo orqali
2. \*odamlar orqali, apparat orqali, dastur orqali
3. modem orqali, telefon orqali
4. odamlar orqali, telefon orqali, havo orqali

**5. Axborot xavfsizligi hususiyatlarini ko‘rsating**

1. \*ochiqlik, butunlik va maxfiylik
2. ochiqlik, maxfiylik
3. maxfiylik
4. butunlik va maxfiylik

**6. Axborot xavfsizligi bu:**

1. Axborotni nusxasini ko‘paytirmaslik
2. Axborotdan foydalanuvchilarni sonini cheklash
3. \*Axborot xavfsizligini ta’minlash uchun ko‘riladigan barcha chora-tadbirlar
4. Axborotni maxsus jihozlarda saqlash
1. Проф. Н.В.Макаровой, В.Б.Волков. Информатика. - М.: 2011 г.(150-с) [↑](#footnote-ref-1)