# AXBOROT XAVFSIZLIGI. ASOSIY TUSHUNCHALARI VA TASHKILIY –HUQUQIY TA’MINOTI.

*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali akademik litseyi informatika va axborot texnologiyalari fani o’qituvchisi*
**Israyiljanova Gulbaxor Saminjanovna**

Axborot xavfsizligi - bu axborotni tasodifiy yoki qasddan ta'sir qilishdan himoya qilish vositalari to'plamidir. Axborot xavfsizligi - axborotlashtirish ob'ektidagi ma'lumotlarni tashqi va ichki ta'sirlardan himoya qilish usullari va amaliyotlari to'plamdir.

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

Bugungi kunda axborot tizimiga tahdidlarning 100 dan ortiq pozitsiyalari va turlari mavjud. Turli diagnostika usullaridan foydalangan holda barcha xavflarni tahlil qilish muhimdir. Tahlil qilingan ko'rsatkichlar va ularning tafsilotiga asoslanib, axborot makonidagi tahdidlardan himoya tizimini malakali qurish mumkin. Bu axborot sohasidagi nusxasini jamiyatning va davlatning qiziqishlarini muvozannatlashtirilgan yig‘indisi bilan aniqlanadigan milliy qiziqishlarining himoyalanganlik xolatlarini ifoda etadi.

Axborotlashtirish obyektida axborot xavfsizligi tizimini yaratish uchta tamoyilga asoslanadi.

Birinchi tamoyil - maxfiylik. Foydalanuvchi o'z vazifalarini bajarishi uchun zarur bo'lgan ma'lumotlarning faqat bir qismiga kirish huquqiga ega bo'lishi kerak. Ushbu tamoyilni amalga oshirish usullaridan biri ma'lumotlarni tartiblash (toifalash) hisoblanadi.

Ikkinchi tamoyil - yaxlitlik. Axborot o'zgarishlar yoki buzilishlardan himoyalangan bo'lishi kerak. U ishonchli aloqa kanallari orqali saqlanishi, qayta ishlanishi va uzatilishi kerak. Har qanday o'zgartirish bir foydalanuvchi tomonidan amalga oshiriladi, tasdiqlash yoki rad etish esa boshqasi tomonidan amalga oshiriladi. Axborot tizimidagi har qanday operatsiyalarni qayd etish majburiydir.

Uchinchi tamoyil - foydalanish imkoniyati. Bunda ma'lumotlar kerak bo'lganda foydalanuvchi uchun mavjud bo'lishi kerak. Axborot tizimi barcha sharoitlarda foydalanish imkoniyatini ta'minlashi kerak.

Axborot xavfsizligiga tahdidlar o'zini namoyon qilmaydi, balki xavfsizlik tizimining himoyalanmagan bo'g'inlari bilan mumkin bo'lgan o'zaro ta'sir orqali, ya'ni zaiflik omillari orqali namoyon bo'ladi. Asosiy tahdid quyidagi omillar tufayli yuzaga keladi:

- dasturiy ta'minot va apparat platformasining nomukammalligi;
- axborot oqimidagi avtomatlashtirilgan tizimlar strukturasining turli xarakteristikalari;

- tizimlarning ishlash jarayonlarining bir qismi nuqsonli;
- aloqa protokollari va interfeyslarining noto'g'riligi;
- qiyin ish sharoitlari va ma'lumotlarning joylashuvi.

Ko'pincha tahdid manbalari ma'lumotlarga zarar yetkazilishi sababli noqonuniy foyda olish maqsadida ishga tushiriladi. Ammo himoya darajasining etarli emasligi va tahdid qiluvchi omilning ommaviy ta'siri tufayli tahdidlar tasodifan paydo bo'lishi ham mumkin.

*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:*

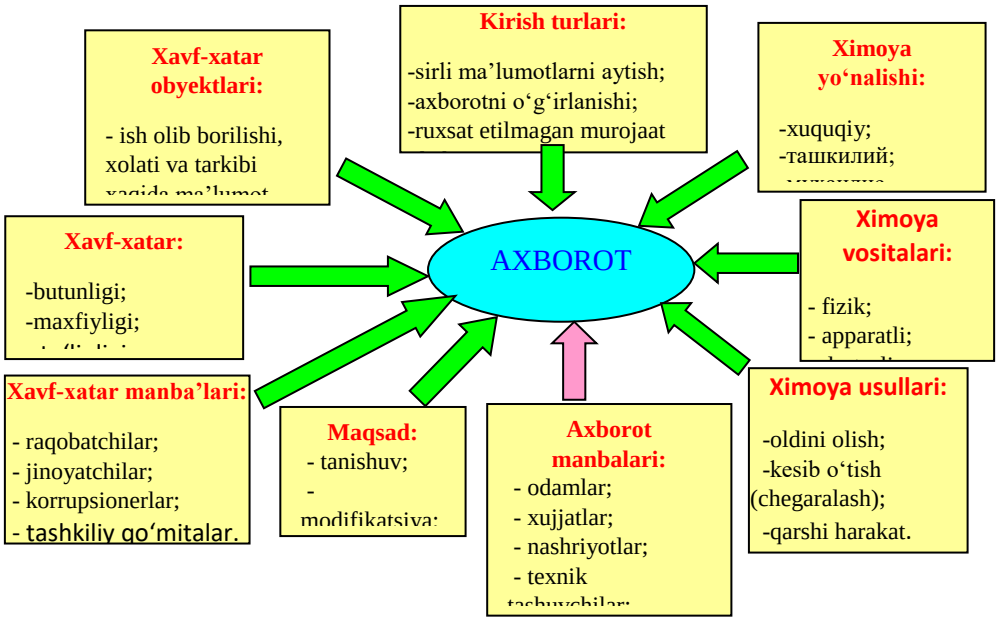
- begona shaxs tomonidan ekrandan axborotni o‘qish;
- shifrlangan axborotni dastur yordamida ochish;
- axborot tashuvchilar (disk, disketalar)ni o‘g‘irlash.

*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.




1-Rasm. 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 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. 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.

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 chiqaradi. Kompyuter tizimlari va tarmoqlarining tezkor rivojlanishi, internet tizimini hayotga 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 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 yaratishdir.

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.

Shunday qilib 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. Axborot xavfsizligi zamonaviy dunyoda har bir tashkilot va shaxs uchun ustuvor masalalardan biridir. Ma’lumotlarni himoya qilish nafaqat kiberhujumlardan, balki ichki xavflardan ham ehtiyot choralarini ko‘rishni talab etadi. Texnik, tashkiliy va huquqiy choralarni uyg‘unlashtirish orqali axborot xavfsizligini samarali ta’minlash mumkin.

**FOYDALANILGAN ADABIYOTLAR:**

1. Mirziyoev Sh.M. Erkin va farovon, demokratik O‿zbekiston davlatini birgalikda barpo etamiz. O‿zbekiston Respublikasi Prezidenti lavozimiga kirishish tantanapi marosimiga bag‿ishlangan Oliy Majlis palatalarining qo‿shma majlisidagi nutk, Toshkent, 2016.566.

2. Mirziyoev Sh.M. Tanqidiy tahlil, qatiy tartib-intizom va shaxsiy javobgarlik - har bir rahbar faoliyatining kundalik qoidasi bo‿lishi kerak. Mamlakatimizni 2016 yilda ijtimoiy-iktisodiy rivojlantirishning asosiy yakunlari va 2017 yilga muljallangan iktisodiy dasturning eng muxim ustuvor yunalishlariga bagishlangan Vazirlar Maxkamasining kengaytirilganmajlisidagi ma‘ruza, 2017 yil 14 yanvarToshkent, Uzbekiston, 2017. 104-6.

3. Mirziyoev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta‘minlash- yurt taraqqiyoti va xalk farovonligining garovi. Uzbekiston Respublikasi Konstitutsiyasi kabul kilinganining 24 yilligiga bagishlangan tantanapi marosimdagi ma‘ruza. 2016 yil 7 dekabr- Toshkent, Uzbekiston, 2017. 48-6.

4. Israyiljanova G.S, Umarov A.M. Axborotni ruxsatsiz foydalanishlardan himoyalash. Models and methods for increasing the efficiency of innovative research: a collection scientific works of the International scientific conference (11 May 2024) - Berlin:2024. Part 34 – 410 p.

5. Seymour Bosworth, Michel Ye. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

6. Shon Harris. ALL IN ONE CISSP. McGraw-Hill 2013. 7. G‿aniev S. K., Karimov M. M., Tashev K. A. —Axborot xavfsizligi‖. Aloqachi. 2008.

8. Makarenko S. I., Informatsionnaya bezopasnost. Uchebnoe posobie. Stavropol, 2009.

9. Michael Ye. Whitman. Herbert J. Mattord. Principles of Information Security, Fourth Edition. Course Technology, Cengage Learning. 2012.