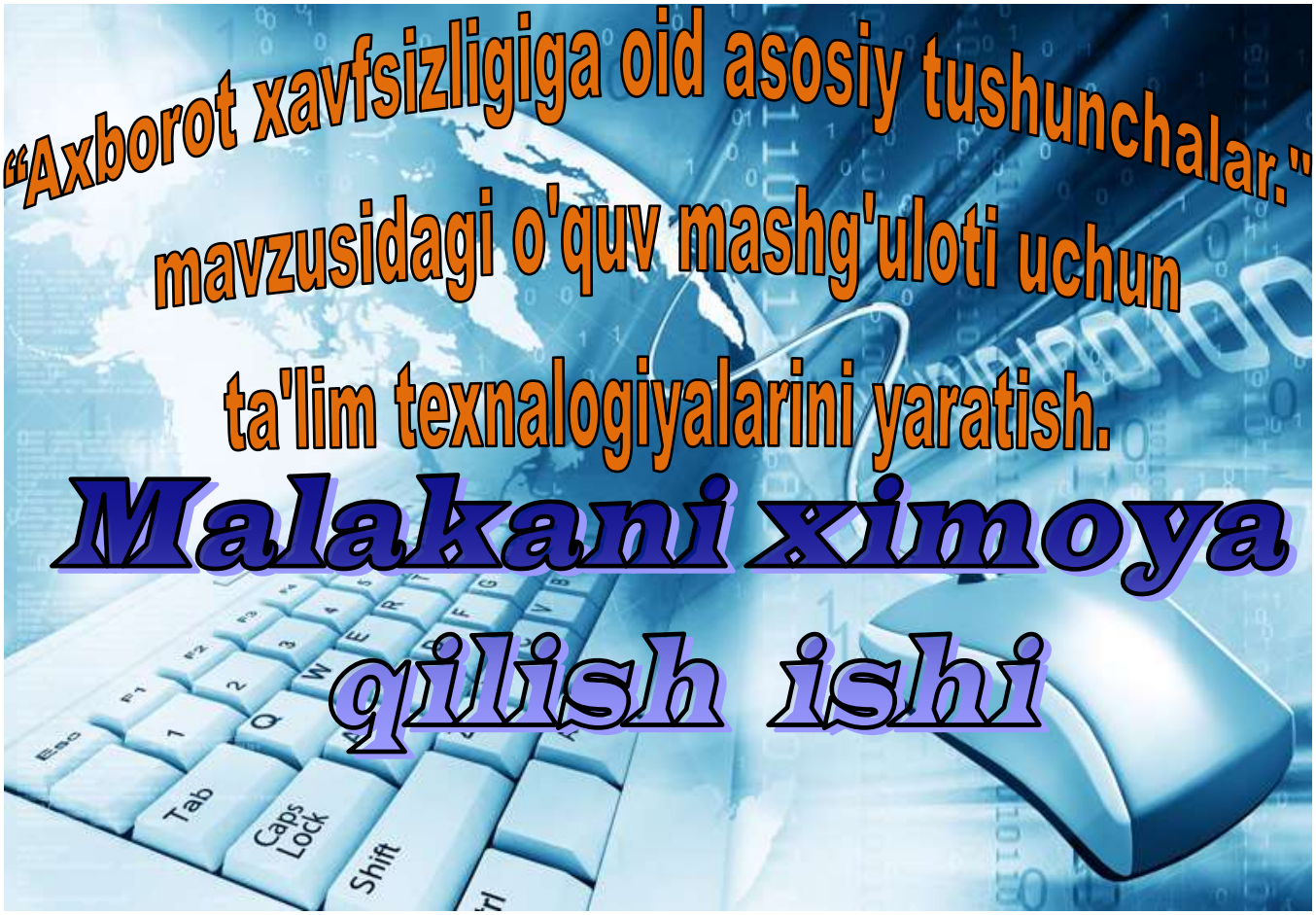
O’ZBEKISTON RESPUBLIKASI OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI
GULISTON DAVLAT UNIVERSITETI
“Malaka oshirish va qayta tayyorlash” fakulteti

Yangiyer tibbiyot kolleji “Informatika va axborot texnalogiyasi” fani o’qituvchisi
Shukurov Fazliddin Baydullayevich



Anotatsiya:

Bu bitiruv malaka ishida men tanlagan mavzu “Axborot xavfsizligiga oid asosiy tushunchalar." mavzusidagi o'quv mashg'uloti uchun ta'lim texnalogiyalarini yaratish, yani o’quvchilarga zamon talablaridan kelib chiqqan holda mavzuni o’rgatishda zamonaviy pedagogik texnalogiyalar, interfaol ta’lim metodlari, axborot komunnikatsion texnalogiyalardan samarali foydalanib qo’yilgan maqsadga erishish yo’llari ko’rsatib o’tilgan. Bu ishni bajarishda men, bitiruv malakviy ishim ilmiy rahbari U.Jo’rayev, texnika fanlari nomzodi, dotsent S.P.Allayorov bergan ko’rsatma va amaliy yordami, hamda malaka oshirishda olgan nazariy va amaliy bilimlarni qo’llagan holda amalga oshirdim.

Bitiruv maka ishi: kirish, asosiy qism, nazariy qism, o’quv metodik qism, xulosa, foydalanilgan adabiyotlar va ilovalardan iborat.

Bugungi kunda o’quvchilarga informatika va xborot texnalogiyasi fanini o’qitishda ularda axborot xavfsizligi muammolari bilim va ko’nikmasini shakillantirishni pedagogic texnalogiyalari ko’rsatib o’tilgan.

Mundarija:

I. Kirish.

Mavzuning dolzarbligi: Tez rivojlanib borayotgan kompyuter axborot texnologiyalari bizning kundalik xayotimizning barcha jabxalarida sezilarli o'zgarishlarni olib kirmoqda. Xozirda "axborot tushunchasi" sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo'lgan maxsus tovar belgisi sifatida tez-tez ishlatilmoqda. Shu bilan birga axborotning bahosi ko'p hollarda uning o'zi joylashgan kompyuter tizimining bahosida bir necha yuz va ming barobarga oshib ketmoqda. Shuning uchun tamomila tabiiy holda axborotni unga ruxsat etilmagan holda kirishdan, qasddan o'zgartirishdan, uni o'g'irlashdan, yo'qotishdan va boshqa jinoiy xarakterlardan himoya qilishga kuchli zarurat tug'iladi.

Kompyuter tizimlari va tarmoqlarida axborotni ximoya ostiga olish deganda, berilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta'minlash maqsadida turli vosita va usullarni qo'llash, choralarni ko'rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Mamlakatimiz milliy iqtisodining hech bir tarmog'i samarali va mo'tadil tashkil qilingan axborot infratuzilmasisiz faoliyat ko'rsatishi mumkin emas. Hozirgi kunda milliy axborot resurslari xar bir davlatning iqtisodiy va xarbiy salohiyatini tashkil qiluvchi omillaridan biri bo'lib xizmat kilmokda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot – kommunikatsiyalar texnologiyalarini qo'llash kengayadi. Turli xildagi axborotlar xududiy joylashishidan qat'iy nazar bizning kundalik hayotimizga Internet halqaro kompyuter tarmog'i orqali kirib keldi. Axborotlashgan jamiyat shu kompyuter tarmog'i orqali tezlik bilan shakllanib bormokda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo'qolib bormokda. Jahon kompyuter tarmog'i davlat boshqaruvini tubdan o'zgartirmoqda, ya'ni davlat axborotlarning tarqalishi mexanizmini boshqara olmay qolmoqda. SHuning uchun xam mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va yo'qotish kabi muammolar dolzarb bo'lib qoldi. Bularning bari shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib kelmoqda. Davlatning axborot xavfsizligini ta'minlash muammosi milliy xavfsizlikni ta'minlashning asosiy va ajralmas qismi bo'lib, axborot himoyasi esa davlatning birlamchi masalalariga aylanmoqda.

Malaka ishining maqsadi: o'quvchilarni axborot xavfsizligi tushunchalarini o'rgatishning samarali yo'llarini shakillantirishning nazariy va amaliy yo'nalishlari hamda pedagogik asoslarini ishlab chiqish.

***Malaka ishining predmeti*:** o'quvchilarni axborot xavfsizligi tushunchalarini o'rgatishni shakillantirishning mazmuni, shakl, uslub va vositalari.

II. Asosiy qism:

NAZARIY DARS REJASI №___ _____

Guruhlar	201 h	202 h	203 h	204 h	205 h	206 h	207 h	201 d	202 d
Dars o'tiladi-gan sana									

O'quv fanining nomi: Informatika va axborot texnalogiyasi.

Mavzu nomi: Axborot xavfsizligiga oid asosiy tushunchalar.

Darsning maqsadlari:

a) ta'limiy: O'quvchilarga Axborot xavfsizligiga oid asosiy tushunchalar. Axborot xavfsizligi muammosi. Asosiy xavf-xatarlar. Axborotlarni himoya qilishning tashkiliy, huquqiy va texnik usullari haqida tushuncha berish.
b)tarbiyaviy: Zamonaviy AKT ni biluvchi ulardan to'g'ri foydalanuvchi yoshlarni tarbiyalash.
c) rivojlantiruvchi: O'quvchilarda axborot xavfsizligiga oid asosiy tushunchalar haqida tasavurlarini rivojlantirish.

Darsdan kutilayotgan natijalar-mavzuni o'zlashtirgandan so'ng o'quvchilar quyidagi bilim va ko'nikmalarga ega bo'ladilar:
1. Axborot xavfsizligiga oid asosiy tuhunchalarni biladilar.
2. Xavfsizlikning asosiy yo'nalishlarini aytadilar.
3. Tarmoqlarda tahdidlar, zaifliklarni biladilar.
4. Korporativ xavfsizlikka tahdidlarni aytadilar.

Ta'lim metodlari: Insert, beshinchi ortiqcha, hayoliy xarita, bahs-munozara, muammoli vaziyat metodlari.

Baholash metodlari: Joriy nazorat, savol-javob, qisqa test

Axborot manbalari va texnik vositalari: Kompyuter, proeksion metodik qo'llanma, kadaskop, doska, bo'r, uslubiy qo'llanma, dasturiy vositalar, elektron taqdimot, videoproektor, mavzu bo'yicha taqdimot, test.

Darsga ajratilgan vaqt miqdori: 80 minut

Uyga vazifa: Mavzu bo'yicha savollar tuzib kelish.

O'qituvchi: Shukurov F.B _____
(imzo)

NAZARIY DARSNING TEXNOLOGIK XARITASI

T/r	**Mashg'ulot bosqichlari**	**Ajrat-ilgan vaqt**	**Mashg'ulot mazmuni**	**Ta'lim metod-lari**	**Ta'lim vosita-lari**
1.	**Tashkiliy qism**	5	Salomlashish, o'quvchilar davomatini olish, darsga tayyorgarlikni tekshirish, darsning borishini tushintirish. Guruhni 5 kishilik jamoalarga bo'lish.	Og'zaki usul	O'quv mashg'uloti jurnali, bor, doska, videoproyektor.
2	**Kirish qismi (Motivatsiya)**	15	Oldingi mavzuni savollar orqali jamoalardan so'rab ularga ballar berish, javob bergan o'quvchilarni baholash .	Savol-javob, aqliy hujum, klaster,	O'quv mashg'uloti jurnali, bor, doska, kompyuter, test dasturi
3	**Yangi mavzuning bayoni**	35	Yangi mavzu bo'yicha o'quvchilarning fikrini so'rash. Tanish so'zlarni so'rash, belgilangan reja va usul asosida mavzuni tushuntirish, bayon etish.	aqliy hujum, klaster, FSMU, bahs-munozara	Bor, doska, kompyuter, test dasturi, taqdimot, maruza matn, internet ma'lumotlari, videoproyek-tor.
4	**Mustaxkam-lash (qo'llash)**	20	Yangi mavzuni jamoalarga savollar, test bergan holda so'rab ballar berish va mavzuni mustahkamlash. O'quvchilarning mavzu bo'yicha bergan saollariga javob berish.	Beshin-chisi ortiqcha, FSMU, test, bahs-munozara	Bor, doska, kompyuter, test dasturi, taqdimot, maruza matn, internet ma'lumotlari, videoproyek-tor.
5.	**Yakuniy qism**	5	G'olib jamoalarni aniqlash, e'lon qilish, natijalarini sharhlash. ularga ballar berish. Uyga vazifa berish.	Muloqat qilish	O'quv mashg'uloti jurnali, doska, bor.

O'qituvchi: Shukurov F.B _____

(imzo)

Mavzu: Axborot xavfsizligiga oid asosiy tushunchalar.

Reja:

I. Nazariy qism.

1. *Axborot urushlari va kiberxujumlar.*
2. *Axborot-kommunikatsion tizimlar va tarmoqlarda tahdidlar, zaifliklar.*

II. Metodik qism.

Mavzuni o'qitishda interfaol usullardan foydalanish.

III. Xulosa.

IV. Adabiyotlar ro'yxati.

V. Ilovalar.

III. Nazariy qism.

1. Axborot urushlari va kiberxujumlar.

Xavfsizlik — har kuni biz to’qnashadigan hayotimizning jihati: eshikni qulflaymiz, qimmatbaho narsalarni begona ko’zlardan berkitamiz va hamyonni duch kelgan joyda qoldirmaymiz. Bu "raqamli dunyoga" ham rasm bo’lishi shart, chunki har bir foydalanuvchining kompyuteri qaroqchi hujumi ob'ekti bo’lishi mumkin. Kommertsiya tashkilotlari xavfsizlikni ta'minlash o’zining birinchi galdagi vazifasi emas, balki uni ta'minlashga sarf etiladigan harajatlarni muqarrar balo deb hisoblab kelganlar. Qandaydir darajada bu "oqilona ish": nihoyat, usiz ham ish bajarishda to’siqlar to’lib-toshib yotibdiku?! Ammo firmaning barcha korporativ binolariga kecha-kunduz kirishga ruxsat berishga jur'at etuvchi aqli joyida "sanoat kapitanlari"ni ko’rganmisiz? Albatta, yo’q! Hatto kichkina kompaniya binosining kirish yo’lida sizni qorovul, yoki kirishni chegaralovchi va nazoratlovchi tizimi qarshi oladi. Axborotni himoyalash esa hali ko’ngildagidek emas. Axborotni qanday yo’qotish mumkinligini va bu qanday oqibatlarga olib kelishini barcha ham tushunavermaydi. Yirik o’yinchilar yaxshigina saboq oldilar: xakerlar Yahoo.com, Amazon.com kabi kompaniyalarga va hatto kosmik tadqiqot agentiligi NASAga katta zarar etkazdilar. Xavfsizlik xizmati bozorining eng yirik nomoyondalaridan biri RSA Security, harqanday tahdidga qarshi chora borligi xususidagi o’ylamasdan qilgan bayonotidan bir necha kundan keyin, xujumga duchor bo’ldi.

Xavfsizlikning asosiy yo’nalishlari

Axborot xavfsizligi. Axborot xavfsizligining dolzarblashib borishi, axborotning strategic resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekomminikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnalogiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo’llanilmoqda (iqtisod, fan, ta’lim, xarbiy ish, turli texnalogiyalarni boshqarish va h.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 hizmat qilmoqda. Davlatning axborot resurslariga keltirilayotgan zarar axborot xavfsizligiga ham ta’sir ko’rsatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakillantirish va uning asosida jahon yagona axborot maydoniga kirib boorish 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’llanilishi inson psihalogiyasi va jamoa ongiga «yashirin» ta’sir ko’rsatish vositalarining samaradorligini yuksaltirib yubordi.

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.

1-rasm.

Odatda odamlardan yoki predmetlardan chiqadigan va zarar etkazadigan tahdidlar quyidagi sinflarga bo’linadi: ichki yoki tashqi va tuzilmalangan (ma'lum ob'ektga qarshi) yoki tuzilmalanmagan ("kimga Xudo beradi" qabilida adreslanuvchi). Masalan, kompyuter viruslari "tashqi tuzilmalanmagan tahdidlar" sifatida turkumlanadi va tamomila oddiy hisoblanadi. Qizig’i shundaki, foydalanuvchilar o’zining kompyuterini muayyan nishon deb hisoblamaydilar, ular

o’zlarini yaxshigina himoyalangandek sezadilar. Kerakli himoya darajasi aksariyat hollarda ishingizning holatiga bog’liq. Agar tashkilotingiz yoki kompaniyangiz qandaydir tazyiq nishoni bo’lsa, agar siz milliy energetik resurslarni taqsimlovchi yoki milliy aloqa tarmoqlariga xizmat qiluvchi davlat infratuzilmasi tarkibida bo’lsangiz, oddiy terroristlar bombalarini va pistoletlarini chetga qo’yib, turli-tuman dasturiy vositalar yordamida tashkilotingizga elektron xujumni amalga oshirish masalasini ko’radilar.

2-rasm.

Ikkinchi tomondan, savdo-sotiq va marketing bo’yicha oddiy tashkilot xususida so’z borsa, faqat mijozlar ruyxatini o’g’rilovchi xizmatchilaringiz to’g’risida, qalbaki kredit kartochkalari bo’yicha tovar oluvchi firibgarlar, tarmog’ingizga preyskurantlardan foydalanish maqsadida kiruvchi raqiblar, Web-saytingizni ta'magirlik maqsadida buzuvchilar va shunga o’xshashlar to’g’risida qayg’urishingizga to’gri keladi. Ammo, vahimaga o’rin yo’q. Birinchi navbatda kundalik ehtiyoj choralari ko’rilishi lozim. Axborotga ega bo’lishning eng ommabop usuli oddiy o’g’rilik. Siz ish stolingizda kechaga mumaygina pulni qoldirib ketmaysizu. Nima uchun boquvchingiz-shaxsiy kompyuter xavfsizligini ta'minlashga ozgina vaqt sarf qilmaysiz? Bu nafaqat apparat vositalariga, balki ma'lumotlarga ham taalluqli. Ma'lumotlarni o’g’irlatish yoki yo’qotish katta, ba'zida, tuzatib bo’lmaydigan zarar keltiradi. Ma'lumki, tizim ma'murlari barcha mahfiy materiallardan foydalanish imkoniga ega va, odatda, kompaniya foydasidan o’z ulushlariga ega emaslar. Shu sababli xuddi ular tashkilot xavfsizligiga tahdid sola oluvchilar ichida eng kattasi hisoblanadilar. Ta'kidlash lozimki, kompaniya ishga kiruvchilarni sinchiklab tekshiradi. Xuddi shunday, xavfsizlik xizmatini ta'minlovchilarga, ayniqsa maslaxat berish, rejalashtirish va mu'murlashni tavsiya etuvchilarga diqqat bilan qarash lozim. Sivilizatsiya rivojining zamonaviy bosqichida axborot nafaqat jamoat va davlat institutlari faoliyatida, balki har bir inson hayotida hal qiluvchi rolni uynaydi. Ko’z oldimizda jamiyatning

axborotlashishi shiddat bilan va ko’pincha oldindan bilib bo’lmaydigan tarzda rivojlanmoqda. Biz esa uning ijtimoiy, siyosiy, iqtisodiy va boshqa oqibatlarini tushunib etishga boshlaymiz, xolos. Jamiyatimizning axborotlashishi yagona dunyo axborot makonining yaratilishiga olib keladiki, bu makon doirasida axborotni yig’ish, ishlash, saqlash va sub'ektlar — insonlar, tashkilotlar, davlatlar o’rtasida almashish amalga oshiriladi. Ravshanki, siyosiy, iqtisodiy, ilmiy-texnikaviy va boshqa axborotlarni tezlikda almashish imkoniyati jamiyat hayotining barcha sohalarida va ayniqsa ishlab chiqarishda va boshqarishda yangi texnologiyalarning qo’llanilishi so’zsiz foydalidir. Ammo, sanoatning tezlikda rifojlanishi Er ekologiyasiga tahdid sola boshladi, yadro fizikasi sohasidagi yutuqlar yadro urushi xavfini to’g’dirdi. Axborotlashtirish ham jiddiy muammolar manbaiga aylanishi mumkin.

Urushlar doimo bo’lgan. Vaqt o’tishi bilan urushni olib borish butun bir fanga aylandi. Harqanday fandagidek urushda o’zining tarixi, o’zining qoidasi, mashhur namoyondalari, o’zining metodologiyasi paydo bo’ldi.

Zamonaviy urush g’oyasi juda ildamlab ketdi. Endi uning makoni butun er shari. Urush lokal qaroqchi xujumidan bir necha davlatlarni vayron qiluvchi global muammoga aylandi. Turli mamlakatlarning harbiy doktrinalarida elektron qurol rivoji rejalari va maxsus vazifalarga mo’ljallangan dasturiy ta'minot to’g’risida eslatishlar ko’zga tashlanmoqda. Turli razvedka manbalaridan kelayotgan axborotning tahlili natijasida xulosa qilish mumkinki, ba'zi bir davlatlarning rahbarlari xujumkor kiber-dasturlarni yaratishni moliyalamoqdalar.

Axborot urushiga oddiy vositalar yordamida harbiy harakatlar samara bermaydigan hollarga nisbatan strategik alternativa sifatida qaralmoqda.

Harbiylar tomonidan kiritilgan axborot urushi atamasi real, qirg’inli va emiruvchi harbiy harakatlar bilan bog’liq shafqatsiz va xavfli faoliyatni anglatadi. Bu urushning alohida qirralari-shtab urushi, elektron urushi, psixologik amallar va h.

Harqanday urush, axborot urushi shu jumladan, zamonaviy qurol yordamida olib boriladi. Axborot quroli yordamida, urush olib boriluvchi barcha qurollardan farqli o’laroq, e'lon qilinmagan va ko’pincha dunyoga ko’rinmaydigan urushlarni olib borish mumkin (olib borilmoqda ham). Bu qurolning ta'sir ob'ektlari — iqtisodiy, siyosiy, ijtimoiy va h. kabi jamiyat va davlat institutlari. Ma'lumotlarni uzatish tarmoqlarining kelajak janglar maydoniga aylanishi allaqachon e'tirof etilgan. Axborot quroli xujumda va mudofaada "elektron tezlik" bilan ishlatilishi mumkin. U eng ilg’or texnologiyalarga asoslangan bo’lib, harbiy nizolarni dastlabki bosqichida hal etilishini ta'minlaydi hamda umummaqsad kuchlarning qo’llanilishini istisno qiladi. Axborot quroli qo’llanishining strategiyasi xujumkor xarakterga ega. Ammo xususiy zaiflik nuqtai nazari mavjud, ayniqsa fuqorolik sektorida. Shu sababli bunday quroldan va axborot terrorizmidan himoyalanish muammosi hozirda birinchi o’ringa chiqqan. Foydalanuvchilariga dunyo tarmoqlarida ishlashni ta'minlovchi mamlakatlarning milliy axborot resurslarining zaifligihar ikki tomonga xavfli narsa.

Axborot quroli deganda axborot massivlarini yo’qotish, buzish yoki o’g’irlash vositalari, himoyalash tizimini yo’qotish, qonuniy foydalanuvchilar faoliyatini

chegaralash asbob-uskunalar va butun kompyuter tizimi ishlashi tartibini buzish vositalari tushuniladi. Hozirda xujumkor axborot quroli sifatida quyidagilarni ko’rsatish mumkin:

- kompyuter viruslari — ko’payish, dasturlarda o’rnashish, aloqa liniyalari, ma'lumotlarni uzatish tarmoqlari bo’yicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga o’xshash qobiliyatlarga ega;
- mantiqiy bombalar — signal bo’yicha yoki o’rnatilgan vaqtda harakatga keltirish maqsadida harbiy yoki fuqaro infratuzilmalariga o’rnatiluvchi dasturlangan qurilmalar;
- telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish;
- testli dasturlarni betaraflashtirish vositalari;
- ob'ekt dasturiy ta'minotiga ayg’oqchilar tomonidan atayin kiritiluvchi turli xil xatoliklar.

Universallik, maxfiylik, dasturiy-apparat amalga oshirilishining har xilligi, ta'sirining keskinligi, qo’llanilishining vaqti va joyini tanlash imkoniyati, nihoyat, foydaliligi axborot qurolini haddan tashqari xavfli qiladi. Bu qurolni, masalan, intellektual mulkni himoyalash vositasiga o’xshatib niqoblash mumkin. Undan tashqari, u hatto urush e'lon qilmasdan xujum harakatlarini avtonom tarzda olib borish imkonini beradi. Zamonaviy jamiyatda axborot qurolini ishlatish harbiy strategiyasi fuqaro sektori bilan uzviy bog’langan. Axborot qurolining, uning ta'siri shakli va usullarining paydo bo’lishi va qo’llanishi xususiyatlarining turli-tumanliligi undan himoyalanishning murakkab masalalarini vujudga keltirdi.

3-rasm.

Axborot quroli qo’llanilishini oldini olish yoki qo’llanishi oqibatlarini bartaraf qilish uchun quyidagi choralarni ko’rish lozim:

- axborot resurslarining fizik asosini tashkil etuvchi moddiytexnik ob'ektlarni himoyalash;

- ma'lumotlar bazalari va banklarining meyoriy va muttasil ishlashini ta'minlash;

- axborotdan ruxsatsiz foydalanishdan, uni buzilishidan yoki yo’q qilinishidan himoyalash;

- axborot sifatini saqlash (o’z vaqtidaligi, aniqligi, to’laligi va foydalanuvchanligi).

2. Axborot-kommunikatsion tizimlar va tarmoqlarda tahdidlar, zaifliklar.

Davlatning dunyo ochiq tarmog’iga ulanishining iqtisodiy va ilmiytexnik siyosatini axborot xavfsizligi orqali ko’rish lozim. Bu ochiq, fuqarolarning axborotga va intellektual mulkga ega bo’lish qonuniy huqukini saqlashga mo’ljallangan siyosat mamlakat xududida tarmoq asbobuskunalarini unga axborot quroli elementlarining kirishidan saqlashni ko’zda tutish lozim. Bu muammo hozirda, chet el axborot texnologiyalarini ommaviy sotib olinayotgan paytda o’ta muhimdir. Ma'lumki, dunyo axborot makoniga ulanmasdan mamlakat iqtisodini rivojlantirib bo’lmaydi. Internet tarmog’i tomonidan ta'minlangan axborot va hisoblash resurslaridan operativ foydalanishni davlatchilikni, fuqarolik jamiyati institutlarini mustahkamlash, ijtimoiy infratuzilmalarining rivojlanish shartlari sifatida talqin etish mumkin.

Ammo mamlakatning halqaro telekommunikatsiya tizimida va axborot almashinuvida ishtirokining axborot xavfsizligi muammosini kompleks hal qilmasdan mumkin emasligini aniq tasavvur etish lozim. Ayniqsa xususiy axborot resurslarini himoyalash muammosi axborot va telekommunikatsiya texnologiyalar sohasida rivojlangan mamlakatlardan texnologik orqada qolayotgan mamlakatlar uchun jiddiy hisoblanadi.

Axborot qurolini ishlab chiqishni va uni ishlatishni ximiyaviy va bakteriologik qurol kabi taqiqlash ehtimoldan uzoq. Xuddi shu kabi ko’pgina mamlakatlarning yagona global axborot makonini shakllantirish bo’yicha urinishlarini chegaralab bo’lmaydi.

Tizim ma'muri uchun himoyaning maqbul darajasini ta'minlashning yagona usuli-axborotga ega bo’lishi, chunki hozircha axborot xujumiga eng tez reaktsiya beradigan inson hisoblanadi. Demak, axborotni himoyalash ma'murlarining o’qitishga va professional o’sishiga sarf-harajat axborot xujumlariga qarshi turuvchi eng samarali vosita hisoblanadi.

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 biznes ning 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[29, 30, 32]. 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.

4-rasm.

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 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 etarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo’lishi mumkin, oxirgisi ayniqsa xavfli.

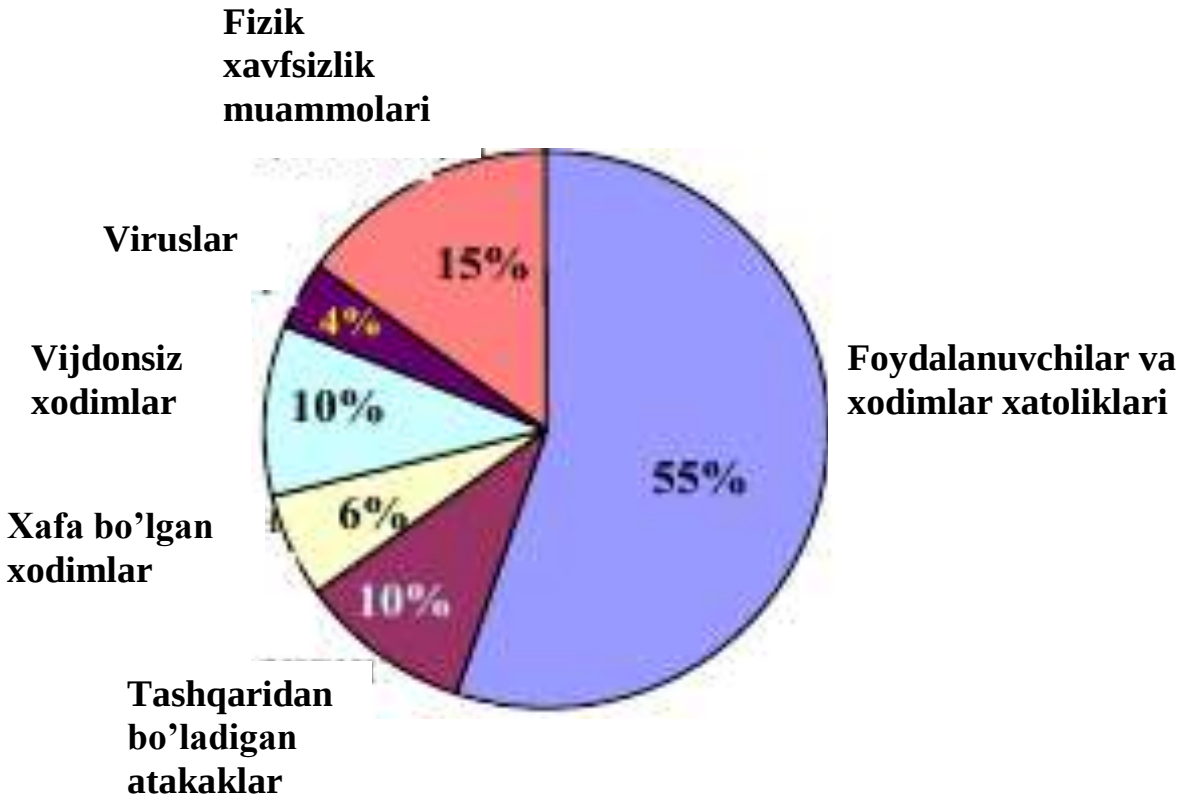
Zarar o’lchami bo’yicha ikkinchi o’rinni o’g’irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishlash rejimlari va himoyalash choralari bilan a'lo darajada tanish bo’lgan tashkilot shtatidagi xodimlar aybdor bo’lib chiqdilar. Global tarmoqlar bilan bog’langan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan etarlicha nazorat yo’qligi bunday faoliyatga qo’shimcha imkon yaratadi. Xafa bo’lgan xodimlar (hatto sobiqlari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon etkazishlari 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 etarlicha 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 masofadan 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 sarf-harajati 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.

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



5-rasm. Xavfsizlikning buzilish manbalari.

1-rasmda keltirilgan statistik ma'lumotlar tashkilot ma'muriyatiga va xodimlariga korporativ tarmoq va tizimi xavfsizligiga tahdidlarni samarali kamaytirish uchun xarakatlarni qaerga yo’naltirishlari zarurligini aytib berishi mumkin. Albatta, fizik xavfsizlik muammolari bilan shug’ullanish va inson xatoliklarining xavfsizlikka salbiy ta'sirini kamaytirish bo’yicha choralar ko’rilishi zarur. Shu bilan bir qatorda korporativ tarmoq va tizimga ham tashqaridan, ham ichkaridan bo’ladigan xujumlarni oldini olish bo’yicha tarmoq xavfsizligi masalasini echishga jiddiy e'tiborni qaratish zarur.

Mavzuga oid savollar:

1. Xavsizlik deganda nimani tushunasiz?
2. Axborot urushini aytib bering.
3. Mantiqiy bombani tushuntirib bering
4. Xavsizlikning buzilish manbalari?
5. Axborot xavsizligiga tahdidni so’zlab bering?
6. Axborot xujumi nima?
7. Kiber xujum nima?
8. Korporativ axborot tizimida xavfsizlikning buzilish manbalari?
9. Tashkilotning kompyuter muhiti qanday xavf-xatarga duchor bo’ladi?
10. Axborotlarni o’g’irlashlar va soxtalashtirishlar haqida so’zlab bering.
11. Axborotlashgan jamiyat deganda nimani tushunasiz?
12. Xavfsizliknung asosiy yo’nalishlari aytib bering?

TESTLAR

1. Globallashuv nima?
A) Axborotning tez tarqalishi
B) Xizmatlarning tez tarqalishi
V) Texnologiyalarning tez tarqalishi
G) Hamma javoblar to’g’ri
2. Psixologik axborot urushi nima?
A) Urush e`lon qilmay harbiy xarakatlar boshlash
B) Josuslar yordamida urush harakatlari olib borish
V) Diplomatiya yordamida harbiy maqsadlarga erishish
G) Odamlar ongiga maxsus va professional asosda ta`sir o’tkazish
3. Axborot qidirish, yig’ish, qayta ishlash, saqlash va tarqatish kabi jarayonlar nimani ifodalaydi?
A) Axborot tizimini
B) Informasion jarayonlarni
V) Axborot resurslarini
G) Axborot madaniyatini
4. Axborotlashgan jamiyatda nima muhim o’rinni egallaydi?
A) Texnika va texnologiya
B) Axborot va bilim
V) Bilim va texnologiya
G) Kapital va mehnat
5. Axborot bu - …
A) Hozirgi zamon sivilizasiyasining o’ziga xos yutug’i
B) Xalqlar, davlatlar, mamlakatlarni yaqinlashtiradigan hodisa
V) Jahon siyosiy ijtimoiy jarayonlarini boshqarishga xizmat qilingan hodisa
G) Hamma javoblar to’g’ri
6. Jamoatchilik fikrining harakatlantiruvchi kuchi nimada?
A) G’oya
B) Manfaatlar birligi
V) Uyushqoqlik
G) Siyosat
7. OAV vazifasi bo’lib hisoblanadi
A) jamiyatning axborotga bo’lgan ehtiyojini qondirish
B) jamoatchilik bo’sh vaqtini o’tkazishga bo’lgan ehtiyojini qondirish
V) jamiyatga ilmiy bilimlarni tarqatish
G) jamiyatning siyosiy hayotini boshqarish
8. Axborot monopoliyasini oldini olishning eng to’g’ri yo’li qanday?
A) axborot monopolyaisini xalqaro shartnomalar bilan chegaralash;
B) axborot monopoliyasini milliy qonunchilik bilan chegaralash
V) muqobil axborot manbalarni rivojlantirish
G) axborot monopoliyasi foydali jarayon, bunga zarurat yo’q

IV. O’quv metodik qism.

FSMU texnologiyasi

Ushbu texnologiya munozarali masalalarni hal etishda hamda o‘quv jarayonini bahs-munozarali o‘tkazishda qo‘llaniladi, chunki bu texnologiya talabalarni o‘z fikrini himoya qilishga, erkin fikrlash va o‘z fikrini boshqalarga o‘tkazishga, ochiq holda bahslashishga hamda shu bilan birga bahslashish madaniyatini o‘ratadi.Tinglovchilarga tarqatilgan oddiy qog‘ozga o‘z fikrlarini aniq va qisqa holatda ifoda etib, tasdiqlovchi dalillar yoki inkor etuvchi fikrlarni bayon etishga yordam beradi.
F – fikringizni bayon eting
S – fikringiz bayoniga sabab ko‘rsating
M – ko‘rsatgan sababingizni isbotlovchi dalil keltiring
U – fikringizni umumlashtiring

Jadvalni to‘ldiring

1-guruh

Savol	Idorada axborot xafvsizligini ta’minlash uchu nima qilish kerak?
(**F**) Fikringizni bayon eting	
(**S**)Fikringiz bayoniga sabab ko‘rsating	
(**M**)Ko‘rsatgan sababingizni isbotlovchi dalil keltiring	
(**U**) Fikringizni umumlashtiring	

2-guruh

Savol	Idoralarda axborot xavfsizligini 100 % ta’minlash mumkinmi?
(**F**) Fikringizni bayon eting	
(**S**) Fikringiz bayoniga sabab ko‘rsating	
(**M**) Ko‘rsatgan sababingizni isbotlovchi dalil keltiring	
(**U**) Fikringizni umumlashtiring	

Insert usuli

Insert-samarali o‘qish va fikrlash uchun belgilashning interfaol tizimi hisoblanib, mustaqil o‘qib-o‘rganishda yordam beradi. Bunda mavzular, kitob va boshqa materiallar oldindan talabaga vazifa qilib beriladi. Uni o‘qib chiqib,”v; +; -; ?;” belgilar orqali o‘z fikrini ifodalaydi.

Matnni belgilash tizimi.

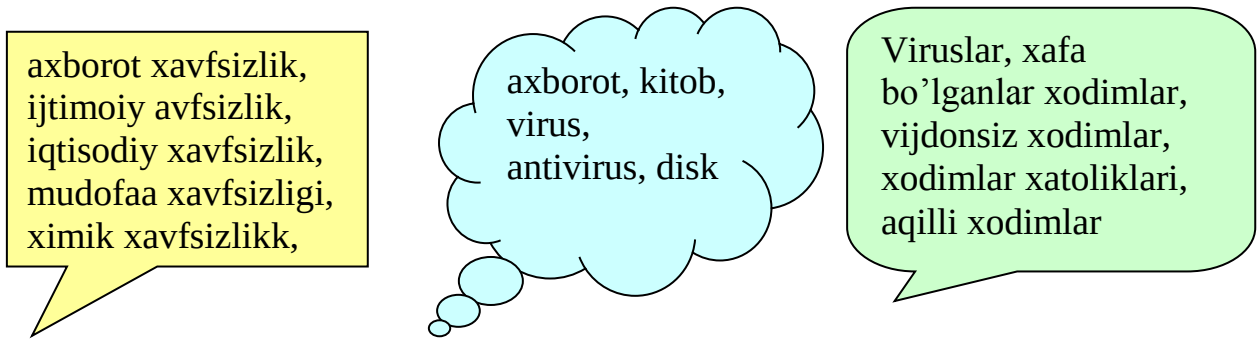
(v)-men bilgan narsani tasdiqlaydi.
(+)-yangi ma’lumot.
(-) men bilgan narsaga zid.
(?)-meni o‘ylantiradi. Bu borada menga qo‘shimcha ma’lumot zarur.

Insert jadvali

Tushunchalar	v	+	-	?
xavfsizlik				
Axborot xavfsizligi				
Kiber xujum				
Man tiqiy bomba				
Axborot xujumi				
Xavfsizlikning buzilishi				

“Beshinchisi ortiqcha” usuli

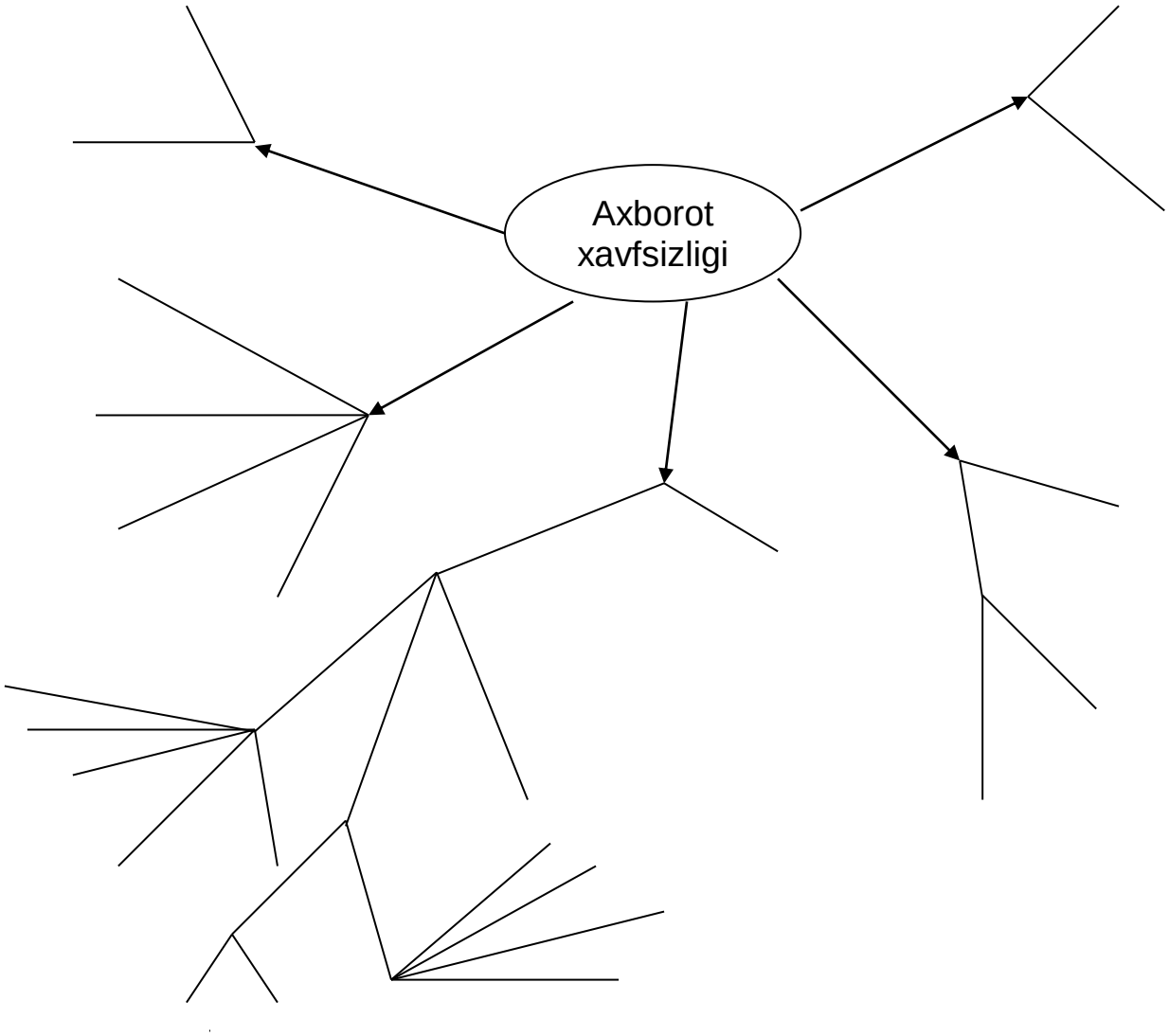
1-topshiriq. Quyida berilgan har bir shakl ichidagi so‘zlardan bittasi ortiqcha. Shu ortiqcha so‘zlarni toping, nima uchun oriqchaligini tushuntiring.



“Xayoliy xarita” texnalogiyasi

Amaliy mashg’ulotlar uchun mo’ljallangan. Ma’lum bir yirikroq mashg’ulotlar o’tib bo’lingach o’tkaziladi. Shakli: guruhlarda ishlash.

Xaritaning markaziga sxemalshtirilishi lozim bo’lgan masala, atrofiga esa tasnifiy yo’nalishlar sxemasi beriladi. Har bir guruh eng mukammal va to’liq xaritani chizishi lozim. Guruhlar haritani himoya qiladi!



«Bahs-munozara» usul

Bahs-munozara - o`quvchilarni ikki guruhga bo`lgan holda, biror mavzu bo`yicha o`zaro bahs, fikr almashinuv tarzida o`tkaziladigan o`qitish usuldir.

Har handay mavzu va muammolar mavjud bilimlar va tajribalar asosida muhokama hilinishi nazarda tutilgan holda, ushbu usul qo`llaniladi. Bahs-munozarani boshqarib borish vazifasini o`quvchilarning biriga topshirish mumkin. Bahs-munozarani erkin holatda olib borish va har bir o`quvchini munozaraga jalb etishga harakat qilish lozim.

Bahs-munozara usul o`quvchidan berilgan savolga tezroq va avvalroq ma`lumot topishga undaydi.Bu esa savollarga javob topish vaqtini tezlashtiradi va tejaydi.

«Davra suhbati» usul

Davra suhbati - o`quvchilar o`rtasida va kichik guruhlarda aylana stol atrofida o`z fikr-mulohazalarini bildirish orqali olib boriladigan o`qitash usuldir.

«Davra suhbati» usul qo`llanilganda stol-stullarni doira shaklida joylashtirish kerak. Bu har bir o`quvchining bir-biri bilan «ko`z aloqasi»!» o`rnatib turishiga yordam beradi.

Davra suhbatining og`zaki va yozma shakllari mavjuddir. Og'zaki davra suhbatida o`qituvchi mavzuni boshlab beradi va o`quvchilardan ushbu mavzu bo`yicha o`z fikr-mulohazalarini bildirishlarini so`raydi va aylana bo`ylab har bir o`quvchi o`z fikr-mulohalarini og`zaki bayon etadi. So`zlayotgan o`quvchini barcha diqqat bilan tinglaydi, agar muhokama qilish lozim bo`lsa, barcha fikr-mulohazalar tinglanib bo`lingandan so`ng muhokama hilinadi. Bu esa o`quvchilarning mustaqil fikrlashiga va nutq madaniyatining rivojlanishiga yordam beradi.

Yozma davra suhbatida ham stol-stullar aylana shaklida joylashtirilib,har bir o`quvchiga konvert qog`ozi beriladi. Har bir o`quvchi konvert usgiga ma`lum bir mavzu bo`yicha o`z savolini beradi va yonidagi o`quvchiga uzatadi. Konvertni olgan o`quvchi o`z javobini qogozga yozib, konvert ichiga solib qo`yadi va yonidagi o`quvchiga uzatadi. Barcha konvertlar aylana bo`ylab harakatlanadi. YAkuniy qismda barcha konvertlar yig'ib olinib, tahlil qilinadi.

«Muammoli vaziyat» usul

Muammoli vaziyat – o`quvchilarga muammoli vaziyatlarni tahlil qilish va ularning yechimini topishga asoslangan usuldir.

«Muammoli vaziyat» usul uchun tanlagan topshiriqning murakkabligi o`quvchilarning bilim darajalariga mos kelishi kerak. Ular qo`yilgan muammoning yechimini topishga qodir bo`lishlari kerak, aks holda yechimni topa olmagach, o`quvchilarning qiziqishlari so`nishiga, o`zlariga bo`lgan ishonchlarining yo`qolishiga olib keladi.

Muammoli vaziyatlarni o`quvchilar tomonidan yechishda qiyinchiliklarga duch kelinsa,o`qituvchi tomonidan ularga yo`nalish berib boriladi. Yoki mummoli vaziyat mavzusini shu mavzuga yaqin holda o`zgartirilishi mumkin.

«Yo`naltiruvchi matn» usul

Yo`naltiruvchi matn - o`quvchilar mustaqil ravishda yo`naltiruvchi savollar yordamida ma`lumot yig'ish, rejalashtirish, amalga oshirish vazifalarini bajaradigan usuldir.

«Yo`naltiruvchi matn» usul «loyihalash» usul bilan chambarchas bog'liqdir. Ushbu ikki usulni bir-biridan quyidagi nuqtai-nazar bo`yicha farqlash mumkin:

- «yo`naltiruvchi matn» usul o`quvchilarning mustaqil o`rganishiga qaratilgan;
- «loyihalash» usul esa o`quvchilarning mustaqil o`rganishidan tashqari, e`tiborni kasb o`rganishda kerak bo`ladigan shaxsiy qobiliyatlar va ko`nikmalarni takomillashtirishga qaratilgan.

V. Xulosa.

Hozirgi davrga kelib hayotimizni axborot texnalogiyasi, kompyutersiz tasavvur qilish mumkin emas bo'lib qoldi, men shunday xulosaga keldimki o'z malakamni oshirish kursida ta'lim jarayonida yangi pedagogik texnalogiyalarni qo'llashni, zamonaviy dasturlar bilan ishlashni mukammalliroq o'rgandim. Bundan tashqari elektron darslik yaratish, excel dasturida test yaratish, veb sahifa yaratish ko'nikmalarini mukammallashtirdim.

Xozirda "axborot tushunchasi" sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo'lgan maxsus tovar belgisi sifatida tez-tez ishlatilmoqda. Shu bilan birga axborotning bahosi ko'p hollarda uning o'zi joylashgan kompyuter tizimining bahosida bir necha yuz va ming barobarga oshib ketmoqda. Shuning uchun tamomila tabiiy holda axborotni unga ruxsat etilmagan holda kirishdan, qasddan o'zgartirishdan, uni o'g'irlashdan, yo'qotishdan va boshqa jinoiy xarakterlardan himoya qilishga kuchli zarurat tug'iladi.

Kompyuter tizimlari va tarmoqlarida axborotni ximoya ostiga olish deganda, berilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta'minlash maqsadida turli vosita va usullarni qo'llash, choralarni ko'rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Mamlakatimiz milliy iqtisodining hech bir tarmog'i samarali va mo``tadil tashkil qilingan axborot infratuzilmasisiz faoliyat ko'rsatishi mumkin emas. Hozirgi kunda milliy axborot resurslari xar bir davlatning iqtisodiy va xarbiy salohiyatini tashkil qiluvchi omillaridan biri bo'lib xizmat kilmokda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot – kommunikatsiyalar texnologiyalarini qo'llash kengayadi. Turli xildagi axborotlar xududiy joylashishidan qat'iy nazar bizning kundalik hayotimizga Internet halqaro kompyuter tarmog'i orqali kirib keldi. Axborotlashgan jamiyat shu kompyuter tarmog'i orqali tezlik bilan shakllanib bormokda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo'qolib bormokda. Jahon kompyuter tarmog'i davlat boshqaruvini tubdan o'zgartirmoqda, ya'ni davlat axborotlarning tarqalishi mexanizmini boshqara olmay qolmoqda. Shuning uchun xam mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va yo'qotish kabi muammolar dolzarb bo'lib qoldi. Bularning bari shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib kelmoqda. Davlatning axborot xavfsizligini ta'minlash muammosi milliy xavfsizlikni ta'minlashning asosiy va ajralmas qismi bo'lib, axborot himoyasi esa davlatning birlamchi masalalaridan biri bo'lib bormoqda.

VI. Foydalanilgan adabiyotlar:

1. Karimov I.A. O’zbekiston buyuk kelajak sari -T.: “O’zbekiston”, 1998.-528 b.
2. O’zbekiston Respublikasi Prezidentining 2012 yil 28 maydagi “Malakali pedagog kadrlar tayyorlash hamda o’rta maxsus, kasb-hunar ta’limi muassasalarini shunday kadrlar bilan ta’minlash tizimini yanada takomillashtirishga oid chora tadbirlar to’g’risida’gi PQ-1761 sonli qarori. – “Halq so’zi” ro’znomasi, 2012 yil 29 may.
3. Karimov I.A.“Yuksak ma`naviyat – engilmas kuch”, T.: “Ma`naviyat”, 2008. – 176 s.
4. Karimov I.A. O’zbekiston XXI asr busag’asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqqiyot kafolatlari // Xavfsizlik va barqaror taraqqiyot yo’lida. 6-jild. T.: “O’zbekiston”, 1998. 31–261 b.
5. Karimov I. “Eng asosiy mezon –hayot haqiqatini asks ettirish”, T.: “O’zbekiston”, 2009.-24 b.
6. Karimov I.A. “Mamlakatimizni modernizasiya qilish va kuchli fuqarolik jamiyatini barpo etish – ustuvor maqsadimizdir” (O’zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi va Senatining qo’shma majlisidagi ma`ruza). –T.: “O’zbekiston” 2010 yil 27 fevral`.
7. Informatika: Kasb-xunar kollejlari uchun o’quv dasturi. Mualliflar jamoasi: R.R.Boqiyev, S.S.Jumanazarov—T.:2012
8. Sattorov A. Informatika va axborot texnalogiyalari. Akademik litsey va kasb hunar kollejlari uchun darslik-T.: “O’qituvchi”, 2002 y.
9. Raxmonkulova S. I. IBM RS shaxsiy kompyuterida ishlash.—Toshkent, 1998. —224 b.
10. U. Yuldashev, Sh. K. Raxmatullaeva. Microsoft WINDOWS-98: O’quv qo’llanma.—T., 2001.—29 b.
11. U. Yuldashev, Sh. K. Raxmatullaeva. Microsoft WORD 97: O’quv qo’llanma.—T., 2001.—47 b.
12. Uzbekiston Davlat ta'lim standarti: Urta maxsus, kasb-hunar ta'limi umumta'lim fanlari. — «Ma'rifat», №86, 2000 y. 4 noyabr.
13. G’ulomov S. S., Shermuxamedov A. T., Begalov B. A. Iktisodiy informatika: Darslik G`Akademik S. S. G’ulomovning umumiy taxriri ostida.—T.: «Uzbekiston», 1999.—528 b.
14. G’ulomov S. S. va boshkalar. Axborot tizimlari va texnologiyalari: Oliy o’quv yurti talabalari uchun darslik . Akademik S. S. G’ulomovning umumiy taxriri ostida.—T.: «Shark», 2000.—592 b.

WEB resurslar

1. http://www.ziyonet.uz/ – O’zbekiston axborot ta`lim portali.
2. http://www.lex.uz/ – normativ-huquqiy axborotlar qidiruv tizimi.
3. http://www.my.gov.uz- ma’lumotlarni elektron almashish, murojaat tizimi.
4. http://www.dl.uz/ – Masofaviy ta`lim bo’yicha sayt.
5. http://www.natlib.uz – O’zbekiston milliy kutubxonasi sayti
6. http://www.ziyouz.uz – turli adabiyotlar, qiziqarli ma’lumotlar sayti.
7. http://www.ulugov.uz- qidiruv tizimi.
8. http://www.megasoft.uz- kompyuter dasturlarini yuklash sayti.
9. http://megaforum.uz- muloqat va muhokama qilish markazi.
10. http://www.uroki.uz- turli o’quv ma’lumotlar sayti.
11. http://www.wikipedia.uz- o’zbek tilidagi elektron ensiklopediya.
12. http://www.ensiklopediya.uz-O'zbekiston milliy ensiklopediyasi
13. www.edu.uz - O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi
14. www.minjust.uz - O‘zbekiston Respublikasi Adliya vazirligi
15. http://darslar.uz/ -Axborot texnalogiyalari bo’yicha o’quv qo’llanmalar va maqolalar.
16. http://ita.uz - ilmiy-texnikaviy ma’lumotlar portali.
17. http://book.uz -elektron adabiyotlar kukubxonasi.

Normativ-huquqiy aktlar

1. O’zbekiston Respublikasi Konstitusiyasi. - T.: O’zbekiston, 2010 y. / "NORMA" huquqiy axborot qidiruv tizimi.
2. «Axborotlashtirish to’g’risida» O’zbekiston Respublikasi Qonuni, 2003 y. / "NORMA" huquqiy axborot qidiruv tizimi.
3. «Elektron raqamli imzo to’g’risida» O’zbekiston Respublikasi Qonuni, 2003 y. / "NORMA" huquqiy axborot qidiruv tizimi.
4. «Elektron hujjat aylanishi to’g’risida» O’zbekiston Respublikasi Qonuni, 2004 y. / "NORMA" huquqiy axborot qidiruv tizimi.
5. O’zbekiston Respublikasi ning “Axborot olish kafolatlari va erkinligi to’g’risida”gi qonuni (24.04.1997 y.). – T.: - 12 b.
6. O’zbekiston Respublikasining „Mualliflik huquqi va turdosh huquqlar to’g’risida”gi qonuni (30.08.1996 y. N 272-I (Mazkur Qonunga O’zR 15.12.2000 y. 175-II-son Qonuniga muvofiq o’zgartirishlar kiritilgan)). – T.: - 24 b.

VII. Ilovalar.

Golasariy:

Active attack - Tajovuz. Xavfsizlikka tah didning yuzaga chiqishi.

Active threat - Xavfsizlikka taxdid. Qasddan tizimning xolatini yomonlashtirishga qaratilgan muayyan turdagi xavf-xatarning ma'lum extimolligi.

Authentication information - Autentifikatsiya axboroti. Muayyan axborot manbaining yo uni egasining aslini bilib olish uchun ishlatiladigan axborot. Buknday axborot sifatida raqamli imzo, xujjat izi, manba' izi va sh.o'. bo'lishi mumkin.

Authentication- Autentifikatsiya. Muayyan axborot manbaining yo uni egasining aslini bilib olish. Bu maqsadda nosimmetrik kriptotizimdan foydalanilganda hujjatning aslini (kelib chiqishini) xujjat tuzuvchining raqamli imzosi vositasida aniqlab olinadi. Autentifikatsiya keng ma'noda qaralganda axborotning manba'idan qat'iy nazar uning faqat ichki tuzilmasi asosida butunligini aniqlashdir.

Authorized access - Ruxsatli munosabat(kirish). Axborotga va axborot texnologiyasi elementlariga nisbatan belgilab qo'yilgan cheklov qoidalariga rioya qilingan holda faol munosabatda bo'lish.

Certify - Kalitni sertifikatsiyalash. Biror kimsaning oshkora kalitini raqamli imzo bilan tasdiqlash.

Certifying Authority - Vakolatli sertifikator. Kalitni sertifikatsiyalash va buni umumiy ma'lumotlar bazasiga kiritish huquqiga ega bo'lgan ishonchga sazovor shaxs (yo shaxslar).

Confidentiality information - Axborot pinhonaligi. Axborotning u bilan bajarladigan axborot jarayonlari davomida u bilan beruhsat tanishish yo uni ko'chirib olishga yo'l qo'ymaslik xossasi.

Confidentiality mark - Maxfiylik grifi. Xujjatlashtirilgan axborotning maxfiylik darajasini ko'rsatuvchi rekvizit (masalan, o'ta maxfiy, maxfiy, pinxona, xizmatda foydalanish uchun, oshkora).

Cryptographic method - Kriptografik metod. Axborotni shifrlashga asoslangan ximoyalash usuli.

Data destruction - Axborotni yo'q qilish. Axborotni tasodifiy xato tufayli yo qasddan moddiy tashuvchidan o'chirib yuborish yokm tashuvchisi bilan birga o'g'irlab ketish.

Data falsification - Axborotni soxtalashtirish. Axborot jarayonlari davomida axborot mazmunini qastdan buzib o'zgartirish.

Data protection - Axborot ximoyasi. Axborotning pinxonaligi, butunligi va qobilligini ta'minlashga qaratilgan huquqiy, siyosiy, tashkiliy, texnikaviy va dasturiy tadbirlar majmui.

Data transmission blocking - Axborot uzatishni to'sish. Axborot uzatishni qastdan yo tasodifiy xato tufayli to'xtatib, yo'lini o'zgartirib yo kechiktirib qo'yishdan iborat bo'lgan axborot xavfsizligining buzish turi.

Decryption - Shifrni ochish. Shifrlangan axborotni tushunarli shaklga aylantirish. Buning uchun maxfiy kalitdan foydalaniladi.

Digest - raqamli iz(daydjest). Axborotning ixcham bir tomonlama xisoblanadigan funktsiyasi yoki faylning nazorat jamlamasi. Axborot o'zgarsa daydjest ham o'zgaradi.

Digital Signature - Raqamli imzo. Axborotning raqamli izi(daydjesti)ning shu axborotning xaqiqiyligini tasdiqlovchi sub'ektning maxfiy kaliti bilan shifrlangan shakli. Raqamli imzo shu sub'ektga tegishli ekaniga ishonch xosil qilish uchun axborotning raqamli izini hammaga ma'lum bo'lgan funktsiya asosida hisoblab topib, natijani raqamli imzo egasining oshkora kaliti bilan ochilgan imzosi bilan taqqoslash (verifikatsiyalash) yetarli.

Documented information - Xujjatlashtirilgan axborot. Moddiy tashuvchida aks etgan va uni belgilovchi rekvizitlarga ega bo'lgan muayyan axborot.

Encryption - Shifrlash. Axborotni undan xabardor bo'lishi lozim bo'lmagan shaxslar uchun mutlaqo tushunarsiz shaklga keltirish amali, ximoya usuli .

Enforcement - Majburlash. Foydalanuvchi yoki ijrochiga nisbatan moddiy yoki jinoiy javobgarlik taxdidi ostida axborot jarayonlari koidalarining bajarilishiga erishishga asoslangan ximoya usuli.

Identification - Identifikatsiya. Ko'rsatilgan identifikatorni uning egasiga takdim etilgan identifikator bilan takkoslash.

Identifier - Identifikator. Axborot jarayoni subekti , vositasi va obekti(axborot)ga takdim etiladigan, fakat unga biriktirilgan noyob belgi, simvollar qatori.

Information procedure - Axborot jarayoni. Axborotni yaratish, olib-yig'ish, saqlash, himoyalash, izlash, uzatish, taqsimlash, undan foydalanish yoki unga ishlov berish jarayonlaridan biri.

Information (data) integrity - Axborotning butunligi. Axborotning axborot jarayonlari davomida uni beruxsat o'zgartirish yoki yo'qotishga yo'l qo'ymaslik xossasi.

Information availability - Axborot qobilligi. Axborotning unga nisbatan ruxsat berilgan axborot jarayonlarini bajarilishiga yaroqlik va tayyorlik xossasi.

Information distortion - Axborot buzilishi. Axborotning axborot jarayonlari davomida xalal beruvchi tashqi ta'sirlar yo jarayon vositalari va ishtirokchilarining tasodifiy xatolari yo qasddan qilingan ishlar tufayli o'zgarib qolishi.

Information modification - Axborot modifikatsiyasi. Axborot mazmuni yo xmiqdorining axborot jarayonlari davomida o'zgarishi.

Information security - Axborot xavfsizligi. Axborotninig va axborot jarayonlarini amalga oshirish vositalarining ma'lum turdagi tasodifiy va qasddan qilinadigan tahdidlardan himoyalanganlik holati

Information security service - Axborot xavfsizligini ta'minlash tizimi. Axborot xavfsizligini ta'minlovchi siyosiy, huquqiy, tashkiliy, texnikaviy va dasturiy tadbirlar, vositalar va meyorlar tizimi.

Information user - Axborot foydalanuvchisi. Axborot bilan biror axborot jarayonini amalga oshiruvchi sub'ekt (shaxs, tashkilot).

Information's security - Axborotning xavfsizligi. Axborotning tasodifiy yo qasddan qilinadigan tahdidlarga qarshi pinxonalikni, butunlikni va qobillikni saqlab qolish xossasi.

Introducer - Vositachi. Ochiq kalitlarning o'z egasiga taalluqligiga kafillik berishga vakolatli shaxs yo tashkilot. PGP dasturida vositachilar ularning ochiq kalitiga ma'lum ishonch darajasi taqdim etish orqali tayinlanadilar.

Intruders (hacker) - Axborot jinoyatchisi. Axborot xavfsizligini buzgan sub'ekt (shaxs, tashkilot).

Key - Kalit. Shifrlash, shifrni ochish, raqamli imzo qo'yish va verifikatsiya(ishonib olish)da ishlatiladigan raqamli kod. Kalitlar nosimmetrik kriptotizimlarda juft(oshkora va mahfiy) xolda hosil qilinadi va bog'lamlarda saqlanadi. Simmetrik kriptotizimlarda faqat bitta(mahfiy) kalit ishlatiladi. Aralash kriptotizimlarda kalitlar juftiga qo'shimcha tarzda mahfiy seans aliti ishlatiladi.

Key Escrow - Kalitni deponirlash. Uchinchi tomonga o'z maxfiy kalitining nusxasini berish amaliyoti. Bunda uchinchi tomon shifrlangan axborotni bilib olish imkoniga ega.

Key Fingerprint - Bosma iz. Oshkora kalitni noyob tarzda ifodalovchi(belgilovchi) raqam va harflar qatori. Kalit egasidan telefon orqali Bosma izini so'rab olib o'zingizdagi uning oshkora kaliti Bosma izi nushasi bilan taqqoslab, kalit nusxasining haqiqiy yo qalbaki ekanini bilish mumkin.

Key ID - Kalit identifikatori. Kishi o'qisa bo'ladigan kalitlar juftini noyob usulda belgilovchi qator. Kalitlarning ikki jufti bir xil foydalanuvchi identifikatoriga ega bo'lishi mumkin. Lekin kalit identifikatorlari har xil bo'ladi.

Key Pair - Kalitlar jufti. Oshkora va unga mos maxfiy kalit. Oshkor kalitli tizimda har bir foydalanuvchi kamida bitta kalitlar juftiga ega.

Keyring - Bog'lam. Kalitlar to'plami. Har bir foydalanuvchi oshkora kalitlar boylamiga va maxfiy kalitlar boylamiga ega.

Masking - Niqoblash. Axborotni axborot jarayenlari davomida kriptografik usul bilan berkitish.

Obstacle - To'siq. Ximoyalanadigan axborotga axborot jinoyatchisining yo'lini fizikaviy to'sib qo'yish asosida axborotni ximoyalash usuli.

Passiv attack - Nofaol tajovuz. Xavfsizlikka nofaol taxdidning yuzaga chiqishi.

Passiv threat - Xavfsizlikka nofaol taxdid. Tizim xolatini buzmasdan turib undan axborotning begonalarga beruxsat chiqib ketish xavfi.

Password - Parol. Amaliy munosabat boshlash uchun ishlatiladigan, subektning siri xisoblanadigan identifikator. Tizimga kirish uchun klaviatura tugmalarini bosish ketma-ketligi.

Physical threat - Fizikaviy xavf. Oqibati tizimga fizikaviy xavf keltiradigan taxdid.

Plaintext - Ochiq matn. SHifrlanmagan va imzolanmagan odatdagicha o'qib- tushuniladigan matn.

Potection strategy - Himoya strategiyasi. Malum tahdidlardan ximoyalanishni taminlashga qaratilgan mezonlarning formal tarifi.

Private Key - Maxfiy kalit. Bilishi shart bo'lgan sub'ektlardan boshqa xechkimga oshkora qilinmaydigan kalit. Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun, nosimmetrik kriptotizimlarda raqamli imzo qo'yish va axborot shifrini ochish uchun ishlatiladi.

Private Keyring - Maxfiy kalitlar boylami. Boylam egasiga tegishli bir yo undan ortiq maxfiy kalitlar to'plami.

Protection model - Ximoya modeli. Axborot ximoyasi tizimini aks ettirib, uni xavfsizlik darajasini tadqiq etishga imkon beruvchi tizim.

Public Key - Oshkora kalit. Axborotni shifrlash va raqamli imzoning to'g'riligini tekshirish uchun ishlatiladigan kalit. Oshkora kalit boshqalarga erkin tarqatiladi va birov uni bilgan bilan unga mos maxfiy kalitni hisoblab topaolmaydi.

Public Keyring - Oshkora kalitlar bog'lami. Oshkora kalitlar to'plami. Uning tarkibida boylam egasining ham o'z oshkora kaliti bor.

Public-Key Cryptography - Oshkora kalitli(nosimmetrik) kriptografiya. Oshkora va maxfiy kalitlar juftidan foydalanishga asoslangan va ishlatiladigan aloqa kanalining himoyalangan bo'lishini talab qilmaydigan kriptotizimlar texnologiyasi.

Regulation - Tartibga solish. Axborotga beruxsat munosabatda bulishni minimumga keltirishga qaratilgan texnologiyaga asoslangan ximoya usuli.

Screening - Ekranlash. Tarmoklararo ekran(branmauer)ning ruxsat etilmagan tashki axborot okimlarini utkazmay ichki tarmok xavfsizligini saklash vazifasi.

Security audit - Xavfsizlikni tekshirish. Axborot tizimi va tarmog'ining hamda axborotlarning xavfsizlik xolatini tekshirib baholash.

Security model - Xavfsizlik modeli. Axborot xavfsizligi siyosatining formal ifodasi.

Security policy - Xavfsizlik siyosati. Axborot xavfsizligini taminlashga va tajovuz oqibatlarini tugatishga qaratilgan meyorlar majmui.

Signature - Imzo. Maxfiy kalit vositasida hosil qilinadigan raqamli kod. Imzo uni verifikatsiyalash jarayonida axborot aslini(manba'ini,egasini,tasdiqlovchisini) aniqlash imkonini beradi. Raqamli imzo maxfiy kalit va imzolanayotgan xujjat mazmunining funktsiyasidir.

Subject privilege - Mualliflashtirilgan kirish sub'ekti. Axborot tizimi obektlariga va axborotga amaliy munosabatda bo'lish uchun belgilab qo'yilgan xuquqlarga ega bulgan subekt.

Trojan horse - Troyan oti. Sub'ektning qonuniy vakolatlaridan foydalanib axborotga beruxsat munosabatda bo'lishga imkon beruvchi qo'shimcha pinxona vazifalarni amalga oshiruvchi dastur.

Trusted - Ishonchli. Ochiq kalit ishonchli, agar uni siz yo biror siz vakil etgan kimsa sertifikatsiyalagan bo'lsa.

Trusted computer system - Ximoyalangan kompyuter tizimi. Ximoya vositalari majmui o'rnatilgan kompyuter tizimi.

Unauthorized access - Beruxsat munosabat. Sub'ekt tomonidan axborotga va axborot vositalariga nisbatan cheklab kuyilgan qoidalarning buzilishi.

Tahliliy qism:

Tez rivojlanib borayotgan kompyuter axborot texnologiyalari bizning kundalik xayotimizning barcha jabxalarida sezilarli o'zgarishlarni olib kirmoqda. Hozirda "axborot tushunchasi" sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo'lgan mahsus tovar belgisi sifatida tez-tez ishlatilmoqda. Shu bilan birga axborotning bahosi ko'p hollarda uning o'zi joylashgan kompyuter tizimining bahosida bir necha yuz va ming barobarga oshib ketmoqda. Shuning uchun tamomila tabiiy holda axborotni unga ruxsat etilmagan holda kirishdan, qasddan o'zgartirishdan, uni o'g'irlashdan, yo'qotishdan va boshqa jinoiy xarakterlardan ximoya qilishga kuchli zarurat tugiladi.

Kompyuter tizimlari va tarmoqlarida axborotni himoya ostiga olish deganda, berilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta'minlash maqsadida turli vosita va usullarni qo'llash, choralarni ko'rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Axborotni himoya qilish deganda:

- Axborotning jismoniy butunligini ta'minlash, shu bilan birga axborot elementlarining buzilishi, yoki yo'q qilinishiga yo'l qo'ymaslik;
- Axborotning butunligini saqlab qolgan holda, uni elementlarini qalbakilashtirishga (o'zgartirishga) yo'l qo'ymaslik;
- Axborotni tegishli huquqularga ega bo'lmagan shahslar yoki jarayonlar orqali tarmoqdan ruxsat etilmagan holda olishga yo'l qo'ymaslik;
- Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar faqat tomonlar o'rtasida kelishilgan shartnomalar asosida qo'llanilishiga ishonish kabilar tushuniladi.

Yuqorida ta'kidlab o'tilganlarning barchasi asosida kompyuter tarmoqlari va tizimlarida axborot xavfsizligi muammosining dolzarbligi va muhimligi kelib chiqadi. Shuning uchun hozirgi mavzu Respublikamizning oliy va o'rta maxsus o'quv muassasalari o'quv rejalarida munosib o'rin egallaydi.

Ushbu mavzuning vazifalari:

- O'quvchilarda kompyuter tarmoqlari va tizimlarida axborot xavfsizligi to'g'risidagi bilimlarni shakllantirish;
- Axborotni ximoya qilishning nazariy, amaliy va uslubiy asoslarini berish;
- O'quvchilarga kompyuter tarmoqlari va tizimlarida axborot xavfsizligini ta'minlashning zamonaviy usullari va vositalarini qo'llashni nazariy jixatdan o'rgatish;
- O'quvchilarni axborotni ximoya qilish bo'yicha ishlab chiqarilgan turli hil dasturiy maxsulotlardan erkin foydalana olish imkonini beradigan bilimlar bilan ta'minlash;