ISSN 2181-3187

OLIY TA’LIM MUASSASASI MA’LUMOTLARINI HIMOYA QILISH HAMDA MAVJUD HIMOYALASH TIZIMLARI

Xusenov Murodjon Zoxirovich
Buxoro davlat universiteti, e-mail: m.z.xusenov@buxdu.uz,
ORCID: 0000-0002-1533-3102

Annotatsiya: Jamiyatni axborotlashtirish hozirgi zamonning davr talabiga aylanib bormoqda. Inson faoliyat olib borayotgan barcha sohalar axborotni qabul qilish, qayta ishlash va o‘zlashtirish jarayonlari bilan uzviy bog‘liq. Hozirgi kunda kompyuter va axborot texnologiyalari jadal sur’atda, yangilanib, o‘zgarib, rivojlanishi bilan birga kundalik turmushimizning asosiga aylanib bormoqda.

Kalit so‘zlar: Kompyuter, xavfsizlik, virus, antivirus, kriptografik usullar, axborot, axborotlashtirish, axborotni himoya qilish

Asosiy qism: AHQKT obyektlarda axborot xavfsizligini ko‘p sonli mumkin bo‘lgan xavflardan himoya qilish uchun yaratiladi. U yoki bu xavfni blokirovkalash uchun himoya qilishning usullarini va vositalarini ma’lum bir to‘plami ishlatiladi. Ularning ba’zi birlari axborotni bir vaqtning o‘zida bir nechta xavflardan himoya qiladi. Usullarning ichida universal usullar ham mavjuddir, ular istalgan himoya qilish tizimi uchun asosiy hisoblanadi. Bu axborotni himoya qilishning huquqiy usullaridir, bu ixtiyoriy vazifali himoya qilish tizimini rasmiy ravishda ko‘rishni va ishlatishni asosi bo‘lib xizmat qiladi; bu tashkiliy usullardir, ular odatda bir nechta xavflarni bartaraf (qaytarish) etish uchun ishlatiladi; bu texnik usullardir, ular tashkiliy va texnik tadbirlarga asoslangan holda ko‘pchilik xavflardan axborotlarni himoya qiladi.

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

- kompyuter jinoyatchiligi uchun jazolash me’yorlarini ishlab chiqish;
- dasturlovchilarni mualliflik huquqlarini himoya qilish;
- jinoiy va fuqarolik qonunchiligini, hamda kompyuter jinoyatchiligi sohasida sud ishini mukammallashtirish;
- kompyuter tizimlari ishlab chiquvchilar ustidan jamoat nazorati masalalari;
- bu masalalar bo‘yicha mos xalqaro shartnomalarni qabul qilish va h.k.

Axborotni himoya qilishni tashkiliy choralari ko‘rib chiqadi:

- kompyuter tizimlarini qo‘riqlashni;
- xodimlarni tanlab olish;
- o‘ta muhim ishlarni faqat bir kishi tomonidan olib borilishi holatlarini inkor qilish;
- tizimni, u ishdan chiqqanidan keyin, ishlash qobiliyatini tiklash rejasini borligi;

ISSN 2181-3187

- axborot xavfsizligi tizimini ta’minlaydigan shaxslarga javobgarlikni berish;
- kompyuter markazini joylashgan joyini tanlash va h.k.

Himoya qilishni texnik usullari apparatli, dasturli va apparat-dasturliga bo‘linadilar. Elektron hisoblash texnikasiga mo‘ljallangan xavfsizliklarni ta’minlashni asosiy yo‘nalishlari quyidagilardir:

- KT va T larida taqiqlangan axborotga murojaat qilishdan himoya qilish;
- virusga qarshi himoya qilish;
- istalmagan elektromagnit va akustik maydon va nurlanishlar orqali ushlab olishni bartaraf etish;
- kriptografik usullar asosida xabarlarni yuqori tuzilishli berkligini ta’minlash.

Texnik usullar (dasturli, apparatli va dastur-apparatli) kelgusida yanada batafsil ko‘rib chiqilishi uchun axborotni huquqiy va tashkiliy himoya qilishni ta’minlash masalalariga to‘xtalib utamiz. Axborot – huquq obyektidir. Kompyuter jinoyatchiligi uchun asboblar sifatida telekommunikatsiya va hisoblash texnikasi vositalari, dastur ta’minoti va intellektual bilimlar, ularni mukammallashgan sohalari nafaqat gina kompyuterlar, korporativ va global tarmoqlargina bo‘lib qolmasdan, balki zamonaviy yuqori axborot texnologiyalari vositalari ishlatiladigan, katta hajmdagi axborotlar qayta ishlanadigan, masalan, statistika va moliya institutlari, faoliyatni istalgan sohasi bo‘lishlari mumkin.

Istalgan muassasaning faoliyati aloqa kanallari bo‘yicha axborotlarni olish, qayta ishlash, qarorlar qabul qilish, uzatish jarayonlarisiz mumkin emasdir. Bu jarayonlarni ta’minlaydigan barcha vositalar kompyuter jinoyatchiligi uchun asboblar hisoblanadi yoki asboblar sifatida ishlatilishi mumkin.

O‘zbekistonda, MDH barcha davlatlaridagi kabi, yaqin vaqt-largacha kompyuter jinoyatchiliklari bilan samarali kurashishni imkoniyati yo‘q edi. Hozir esa vaziyat o‘zgara boshladi. Informatika, axborotni himoya qilish va davlat sirlari sohasida bevosita qonunchilik asoslari 10 dan ortiq asosiy qonunlarda va O‘zbekiston Respublikasi Prezidentini bir qator farmoyishlarida aks ettirilgandir. Asosiy qonunlarda axborotni va axborotli resurslarni maqsadlari, obyektlari tushunchalari va huquqiy asoslari aniqlangandir.

“Axborot, axborotlashtirish va axborotni himoya qilish to‘g‘risida” gi qonun fuqarolarni axborotga konstitutsion huquqini ta’minlash, uni ochiqligini va unga murojaat qilishlikni, fuqarolar va tashkilotlar tomonidan qonunchilik, ijroiya va sud hokimiyati organlari to‘g‘risidagi axborotni va boshqa axborotni olishni, jamoat va shaxsiy manfaatga ega bo‘lgan ta’minlashga, hamda jamiyatda axborot bilan muloqot qilishga va axborotlashtirishni rivojlantirishga ko‘maklashish uchun da’vat qiladi. Unda axborotni hujjatlashtirish va uni axborot resurslarini ochiq va cheklangan murojaat qilish toifalariga tegishligi, axborotga murojaat qilish bo‘yicha mexanizmlarni va vakolatlarni aniqlash, axborotni huquqiy himoya qilish tartibi

ISSN 2181-3187

masalalari, bu sohada buzg‘unchiliklar uchun javobgarlikni o‘rnatish mexanizmlari masalalari aks ettirilgan.

Qonun bilan aniqlangan axborotni himoya qilish maqsadlari:

- o‘g‘irlashlarni, buzishlarni, chiqib ketishlarni, qalbakilashtirishlarni bartaraf etish;

- shaxsni, jamiyatni, davlatni xavfsizligini ta’minlash;

- axborotni yo‘qotish, buzish, blokirovkalash bo‘yicha taqiqlangan harakatlarni bartaraf etish;

- shaxsiy sirni va shaxsiy ma’lumotlarni maxfiyligini saqlashga fuqarolarni konstitutsiyaviy huquqlarini himoya qilish;

- davlat sirini, hujjatlashtirilgan axborotni maxfiyligini saqlash.

Qonun bilan axborot xavfsizligi obyektlari aniqlangan, ularga quyidagilar tegishlidir:

1) axborot resurslarini barcha ko‘rinishlari;

2) axborotni olishga, tarqatishga va ishlatishga, maxfiy axborotni va intellektual mulkni himoya qilishga fuqarolarni, huquqiy shaxslarni va davlatning huquqlari;

3) turli sinfli va vazifali axborot tizimlarini o‘z ichiga oladigan axborot resurslarini shakllantirish, tarqatish va ishlatish tizimi ma’lumotlar kutubxonalari, arxivlari, tizimlari va yirik to‘plamlari axborot texnologiyalari axborotni yig‘ish, qayta ishlash, saqlash va uzatishning reglamentlari va jarayonlari ilmiy-texnikaviy va xizmat ko‘rsatadigan xodimlar;

4) axborotni qayta ishlash va tahlil qilish markazlarini, axborot almashish va telekommunikatsiya kanallarini ishlashini ta’minlash mexanizmlarini, telekommunikatsiyali tizimlarini va tarmoqlarni, shu jumladan axborotni himoya qilishni tizimlarini va vositalarini o‘z ichiga olgan axborotlashgan infratuzilma;

5) ommaviy axborot va tashviqot vositalariga asoslanadigan jamiyat ongini (dunyoqarash, axloqiy qadr-qimmatlar, odob baholari, xulqni ijtimoiy–yo‘l qo‘yiladigan stereoturlari va insonlar o‘rtasidagi o‘zaro munosabatlar).

Qonun bo‘yicha chegaralangan murojaat qilinadigan xabarlar himoya qilinadi va himoya qilish darajasini ularning egasi aniqlaydi, himoya choralarini javobgarligi esa nafaqat gina egasida emas, balki foydalanuvchida ham bo‘ladi. Faqat hujjatlashtirilgan axborotgina himoya qilinadi. Hujjatlashtirilgan axborot Davlat siriga va maxfiy axborotga bo‘linadi.

Davlat siriga davlat tomonidan himoya qilinadigan uning harbiy, tashqi siyosiy, iqtisodiy, razvyedka, kontrrazvyedka va tezkor qidiruv faoliyati sohasidagi xabarlar tegishli bo‘ladi. Bu xabarlarning egasi va foydalanuvchisi davlatning o‘zi bo‘ladi, shuning uchun uning o‘zi himoya qilish bo‘yicha talablarni ilgari suradi va ularning boshqarilishini nazorat qiladi. Bu talablarni buzilishi barcha qat’iy qonunlar bilan jazolanadi.

ISSN 2181-3187

Maxfiy axborot – hujjatlashtirilgan axborot bo‘lib, uning huquqiy rejimi davlat, tijorat, sanoat va boshqa jamiyat faoliyati sohasidagi harakat qilayotgan qonunchilikni maxsus me’yorlari bilan o‘rnatilgan. Egalari – muassasalar va tashkilotlar, ular bu axborotlarga ega bo‘ladilar va u bilan amallar bajaradilar, hamda ular himoya qilish darajasini o‘rnatadilar. Maxfiylikni buzilgan holatda ba’zi bir sanksiyalarni qo‘llash quyidagi rasmiyatchiliklar oldindan bajarilgan hollardagina mumkindir:

- axborot haqiqatdan ham qimmatbaho bo‘lishi kerak;
- muassasa axborotga erkin murojaat qilishni inkor etish va uning maxfiyligini qo‘riqlash uchun ma’lum bir choralarni ko‘rishi kerak;
- barcha xodimlar axborotning maxfiyligi to‘g‘risida ogohlantirilgan bo‘lishi kerak.

Maxfiy axborotni turi – bu shaxsiy maxfiy ma’lumotlardir. Ammo bu masalada huquqiy asoslar yetarlicha ishlab chiqilmagan bo‘lsa ham, davlat shaxsiy axborotni himoya qilishni o‘zining shaxsiy nazorati ostiga olgan. Bu toifaga shaxsiy va oilaviy sirlar, shaxsiy ma’lumotlar, yozishmalar sirlari, telefondagi, pochtadagi, telegrafdagi va boshqa xabarlar tegishlidir.

Umumiy ko‘rinishda maxfiy xarakterli ma’lumotlar tarkibi quyidagi ko‘rinishga ega:

- shaxsiy ma’lumotlar;
- tergov va sud ishi siri;
- xizmat siri;
- kasb-hunar siri;
- tijorat siri;
- kashfiyotlarni mohiyati haqida.

Asosiy qonunlarda kompyuter axboroti sohasidagi atamalar va tushunchalar aniqlangandir (kompyuter axboroti, EHM uchun dastur, EHM (kompyuter), EHM tarmog‘i, ma’lumotlar bazasi va h.k.).

Kompyuter jinoyatchilikni ko‘rib chiqiladigan asosiy moddalarni o‘z ichiga oladi:

- kompyuter axborotiga qonunsiz murojaat qilish;
- EHM uchun zarar yetkazadigan dasturlarni yaratish, ishlatish va tarqatish;
- EHM, EHM tizimlari va ularning tarmoqlarini ishlatish qoidalarini buzish.

Modda bo‘yicha kompyuter axborotiga (mashina tashuvchisidagi, EHM dagi yoki EHM tarmoqlaridagi) noqonuniy murojaat qilish uchun, agar bu axborotni yo‘qotishga, blokirovkasiga, o‘zgarishiga yoki nusxalanishiga olib kelgan bo‘lsa, hamda hisoblash tarmoqlarida ishlashni buzganligi uchun javobgarlik ko‘zda tutilgan. Taqiqlangan axborotni yo‘qolishiga, blokirovkalanishiga, o‘zgarishiga yoki nusxalanishiga, axborot tizimlarining ishlashini buzilishiga, olib keladigan dasturlarni EHM uchun tuzganlik uchun ham joriy javobgarlik ko‘zda tutilgan.

ISSN 2181-3187

EHM, EHM tizimlari yoki ularning tarmoqlarini, ularda ishlashga ruxsati bo‘lgan shaxs tomonidan, ishlatish qoidalarini buzganligi uchun ham, agar bu faoliyat natijasida qonun bilan qo‘riqlanadigan axborotni yo‘qotishga, blokirovkalashga yoki o‘zgartirishga olib kelsa va jiddiy zarar yetkazsa, javobgarlik o‘rnatilgan.

Kompyuter axborotini himoya qilishning tashkiliy usullari. Kompyuter axborotini himoya qilishning tashkiliy usullarini, himoya qilish darajasini tanlash uchun, mavjud bo‘lgan axborotni oldindan tahlil qilishni o‘tkazishdan boshlash kerak. Faqat hujjatlashtirilgan axborotgina himoya qilinganligi uchun, hujjatlashtirishni qat’iyan standart bo‘yicha o‘tkazish kerak. Oddiy axborot uchun ham, hisoblash texnikasi vositalari bilan yaratiladigan mashinogrammaga va mashina tashuvchilaridagi hujjatlarga huquqiy kuchni berish uchun ham standartlar mavjuddir.

Davlat standarti hujjatning 31 ta rekvizitlarini ko‘zda tutsa ham, ularning hammasini bo‘lishi shart emas. Asosiy rekvizit –matndir, unga ma’lum bir huquqiy kuchni berish uchun muhim rekvizitlar – sana va imzo kerakdir. Avtomatlashtirilgan axborotlashgan tizimning hujjatlari uchun elektron imzo kerakdir. Axborotni himoya qilish qimmatga tushadi, shuning uchun uning muhimligi va qimmatbaholigi bo‘yicha axborotni himoya qilish prinsiplaridan kelib chiqish kerak. Taqiqlangan murojaat qilishni aniqlash uchun kerakdir:

- fayllarning bayonnomalari, ayniqsa, tizimga kirish bayonnomalarini muntazam tekshirish;
- odatdan tashqari vaqtlarda noma’lum foydalanuvchilarni ulanishini kuzatish;
- foydalanuvchilarning biror-bir vaqt oralig‘ida ishlatilmagan va yanada harakatga kelib qolgan identifikatorlariga e’tiborni qaratish.

Tarmoqda begonalarni paydo bo‘lishini aniqlashni usullaridan bittasi, alohida faylda tarmoq bo‘yicha barcha jarayonlarni va ulanishlarni qayd etuvchi odatdagi jarayonni (Shell tilini) har 10 minutda ishga tushirish hisoblanadi. Bu dastur foydalanuvchilar ro‘yxatlarini, barcha joriy jarayonlarni va tarmoqdagi ulanishlarni shakllantiradi.

Korxonalar, tashkilotlar va h.k. tarmoqlarda samarali himoya qilish bilan axborot xavfsizligi ma’muriyati xizmati shug‘ullanishi kerak, uning vazifasiga foydalanuvchilarni kompyuter tarmog‘i resurslariga nazorat qilinadigan murojaat etishni, uning hayot siklini barcha bosqichlarida tashkil etish va qo‘llab-quvvatlash, tarmoq xavfsizligi holatini kuzatish va undagi bo‘lib o‘tayotgan foydalanuvchilarning taqiqlangan harakatlariga tezkor ravishda munosabat bildirish kerak bo‘ladi.

Himoya qilish vositalari bozorida himoya qilish tizimining ko‘pgina xilma-xili mavjuddir. Tarmoq ma’muriyati ularni qo‘llashni zarurligini va tartibini aniqlashi kerak. Barcha kompyuterlar ham qo‘shimcha himoya qilish vositalariga muhtoj bo‘lmaydi. quyidagi holatlarda himoya qilish vositalarini qo‘llash maqsadga muvofiqdir:

ISSN 2181-3187

· ma’lumotlarni kriptografik himoya qilishni kompyuter vositalariga joylashtirishda;

· foydalanuvchilar tomonidan texnologiyada ko‘zda tutilmagan harakatlarga yo‘l qo‘ymaslik uchun tarmoqda foydalanuvchilarning harakatlarini reglamentlash va bayonnomalashtirish kerak bo‘lganda;

· kompyuterning lokal resurslariga (disklar, kataloglar, fayllar, tashqi qurilmalar) foydalanuvchilarning murojaat qilishini cheklash, hamda kompyuterning dastur vositalarini tarkibini va sozlamasini mustaqil ravishda o‘zgartirish imkoniyatini inkor qilish kerak bo‘lganda. Bu masalalarni hal qilish uchun ma’muriyat yo‘riqnomalarida ko‘zda tutilgan harakatlarni bajarish kerak.

Foydalanuvchilarning vakolatlarini va tarmoqda axborotni himoya tizimini sozlashni boshqarish bo‘yicha muammolari tarmoqqa murojaat qilishni boshqarishni markazlashgan tizimini ishlatish asosida yechilishi mumkin. Murojaat qilishni boshqarishni maxsus serveri himoya qilishning markaziy ma’lumotlar bazasini himoya qilishning lokal ma’lumotlar bazasi bilan (ma’lumotlarni himoya qilishning taqsimlangan bazasi) avtomatik sinxronizasiyasini amalga oshiradi. Bu, bundan tashqari, tarmoqni yoki markaziy serverni ishdan chiqishi ishchi stansiyalarda himoya qilish vositalarini ishlashiga to‘sqinlik qilmasligini kafolatlaydi.

Xavfsizlik ma’muriyati tarmoq holatini ham tezkor (kompyuter tarmog‘ini himoya qilinganlik holatini kuzatish yo‘li bilan), ham tezkor emas (axborotni himoya qilish tizimini hodisalarni qayd qilish jurnalini mazmunini tahlil qilish yo‘li bilan) nazorat qilishi kerak.

Viruslardan himoya qilishni tashkiliy usullariga kelganda, kompyuterni yoki kompyuter tarmog‘ini zararlanish xavfini tashkiliy va profilaktik tadbirlar to‘plamini – “kompyuter gigiyenasini” qo‘llash bilan kamaytirish mumkin, bu “gigiyena” tavsiya etadi:

- faqatgina litsenziyaga ega bo‘lgan dastur ta’minotini (DT) ishlatish;
- “kompyuter gigiyenasi” talablariga rioya qilinmagan kompyuterlardan fayllarni nusxalashni bajarmaslik kerak;
- tushunib bo‘lmaydigan yoki tushunarsiz xatarli parollarni ishlatish;
- xarid qilinayotgan dasturlar tizimi dasturchilar tomonidan o‘rganib chiqilishi kerak;
- yangi dasturlar “karantin” muddatini o‘tishi kerak;
- tekshirilgan yangi DT “ top-toza” kompyuterda dubllanishi kerak, asl nusxa yozishdan himoya qilinadi;
- kompyuterlarga begona shaxslarni murojaat qilishini cheklash;
- viruslar simptomini aniqlanganda barcha foydalanuvchilarni va tizimli dasturchilarni (viruslar bo‘yicha mutaxassislarni) ogohlantirish.

Umuman, viruslardan himoya qilish asoslanadi:

ISSN 2181-3187

1) kompyuterlarning tezkor imkoniyatlariga;
2) dastur vositalariga;
3) tizimli dastur ta’minotiga;
4) himoya qilishning tizimli dasturli vositalariga.

Tashkiliy vositalar kompyuterlarni viruslar bilan zararlanish xavfini minimallashtirish, zararlanganda esa – tezda foydalanuvchiga axborot berish va virusni va uning oqibatlarini oldini olishni yengillashtirish imkonini beradi.

Tashkiliy vositalar quyidagi tadbirlarni o‘z ichiga oladi:

1) Zaxiralash:
- OT va DT ning barcha asosiy tashkil etuvchilarini arxivlarda mavjudligi;
- o‘zgaradigan fayllarni arxivlarini har kuni olib borish;

2) Profilaktika:
- vinchesterning faol qismidagi ma’lumotlarni disketalarga doimiy ravishda ko‘chirish;
- DT tashkil etuvchilarini va foydalanuvchilarning dasturlarini alohida saqlash;

3) Taftish:
- disketalarda yangi olinadigan dasturlarni viruslar borligiga tadqiqot qilish;
- vinchesterning fayllarini uzunliklarini doimiy ravishda tekshirish;
- DT ni saqlash va uzatishda nazorat yig‘indilarini doimiy ravishda tekshirish;
- vinchesterning va ishlatiladigan disketalarning tizimli fayllarini yuklanadigan sektorlarini mazmunini tekshirish;

4) Filtrlash:
- vinchesterning mantiqiy disklarga, ularga murojaat qilishni turli xil imkoniyatlari bilan, bo‘lib chiqish;
- faylli tizim ustidan kuzatishni rezidentli dastur vositalarini ishlatish;

5) Maxsus dastur vositalari bilan himoya qilish.

Axborot xavfsizligini ichki tahdiddan himoya qilish. Axborot xavfsizligiga ichki tahdidlar tarkibiga kompaniya xodimlarining qasddan (firibgarlik, o‘g‘irlik, maxfiy ma’lumotlarni buzish yoki yo‘q qilish, sanoat josusligi va boshqalar) va qasddan bo‘lmagan (xodimlarning past malakasi yoki ehtiyotsizligi tufayli ma’lumotlarni o‘zgartirish yoki yo‘q qilish) holatlari; shuningdek, ma’lumotlarni qayta ishlash va saqlash uchun dasturiy ta’minot yoki apparat vositalarining nosozliklari kiradi. Axborot xavfsizligiga ichki tahdidlarning xavfini kamaytirish uchun quyidagilar qo‘llanilishi mumkin:

- Maxfiy ma’lumotlarni tarqalishidan himoyalash (DLP)
- Zaifliklarni boshqarish tizimini joriy etish

Maxfiy ma’lumotlarning tarqalishidan himoya qilish. Mazkur xizmat ichki xavfsizlik tahdidlarining (insayderlarning ma’lumotlari yaxlitligi, mavjudligi yoki maxfiyligini buzish bo‘yicha qasddan qilgan harakatlari) monitoringi va ularga qarshi

ISSN 2181-3187

kurashishning integratsiyalashgan tizimini qurishdir. Ushbu kompleksni amalga oshirish biznes ma'lumotlarini saqlash, foydalanish va uzatish holatida ruxsatsiz kirishdan himoya qilishni ta'minlash imkonini beradi.

DLP-tizimi quyidagilarni ta'minlash imkonini beradi: ma'lumotlarni uzatish kanallarini boshqarish (HTTP, HTTPS, FTP, E-mail, IM, P2P va boshqalar), so'nggi nuqtalarni boshqarish (ish stansiyalari, noutbuklar), o'rindosh uzatmalar, USB qurilmalari, printerlar ustidan nazorat va hokazolar. Ushbu tizim markazlashtirilgan nazoratni va qarshi choralarni samarali qo'llash, shuningdek, xavfsizlik hodisalari uchun zarur dalillar bazasini yaratish imkonini beradi. Shu bilan birga, tizimning o'zi foydalanuvchilar uchun to'laqonli "shaffof" bo'lib qolaveradi.

Mazkur ilova, tarmoq va apparat darajalaridagi zaifliklarni markazlashtirilgan boshqaruvi majmuasini yaratish axborot tizimlarida paydo bo'ladigan zaifliklarga real vaqt rejimida samarali javob berish imkonini beradi, shu bilan ushbu zaifliklardan mahalliy tarmoqlar va ish stansiyalarida zararli dasturlar yoki buzg'unchilar tomonidan foydalanish xavfini kamaytiradi. Zaiflikni boshqarish tizimini joriy etish natijalari:

- ish stansiyalari va serverlarni virusga qarshi himoya qilish tizimi
- xavflarni baholash va zaifliklarni boshqarishni avtomatlashtirish va optimallashtirish
- xavflarni kamaytirish va tahdidlarni bartaraf etish
- rahbarlar, auditorlar va texnik mutaxassislarning ehtiyojlariga muvofiq markazlashtirilgan hisobot tizimi

Axborot xavfsizligini tashqi tahdiddan himoya qilish. Tashqi xavfsizlik tahdidlari deganda tashqi muhit tahdidlari tushuniladi. Axborot xavfsizligiga tashqi tahdidlardan himoya qilish yechimlari:

- tashkilotning perimetrini himoya qilish
- zararli kod va spamlardan himoyalash
- ma'lumotlarning maxfiyligini ta'minlash
- tashkilotning WEB-resurslarini (veb-saytlar, axborot tizimlari) himoya qilish.

Tashkilotning perimetri himoyasi. Ushbu chora-tadbirlar majmui tashkilotning axborot resurslarini passiv va faol himoya qilishning yaxlit tizimini yaratishga qaratilgan.

- Xavfsizlik devori. Korporativ tarmoqning alohida segmentlari va global tarmoq o'rtasida kirishni boshqarish tizimlarini loyihalash va qurish
- Tajovuzlarni aniqlash va oldini olish tizimlarini (IDS/IPS) to'liq tahlillash. Hujumlarga nisbatan avtomat ravishda javob berish va ularni qaytarish qobiliyatiga ega bo'lgan hujum imzolari mavjudligi sababli, trafikni tahlil qiluvchi dasturiy va dasturiy-apparat tizimlari

ISSN 2181-3187

- Hujumlardan himoya qiluvchi dasturiy va apparat tizimlarini joriy etish. Korporativ resurslarni zararlardan, zaifliklardan, DoS hujumlaridan himoya qilish vositalari.

Zararli kod va spamdan himoyalash. Zararli kod va spamdan himoyalovchi ko‘p darajali himoyani yaratish quyidagi korporativ tizimlarni amalga oshirishni o‘z ichiga oladi:

- ish stansiyalari va serverlarni virusga qarshi himoya qilish tizimi
- trafik tarkibini filtrlash tizimi
- spamga qarshi himoya tizimi

Ma’lumotlarning maxfiyligini ta’minlash. Bu ichki xavfsizlikni buzuvchilar va uchinchi shaxslar tomonidan maxfiy ma’lumotlarning murosaga kelishi, o‘g‘irlanishi, o‘zgartirilishi yoki yo‘q qilinishining oldini olishga qaratilgan tashkiliy va texnik chora-tadbirlari majmuidir. Ushbu xizmatlar quyidagilarni taklif qiladi:

- aloqa kanallarini shifrlash (VPN, SSL, PKI tashkil etish)
- axborot tashuvchilarni shifrlash (xavfsiz konteynerlarni yaratish, shifrlash va ma’lumotlarni saqlash uchun korporativ tizimni yaratish)

Tashkilotning WEB-resurslarini himoya qilish. Tashkilotning tashqi WEB-resurslarining xavfsizligini tahlil qilish tarmoq va ilovalar darajasida zaifliklar mavjudligini aniqlash va ularni himoya qilish bo‘yicha bir qator tavsiyalarni ishlab chiqish imkonini beradi.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi qonuni, 11.12.2003 yildagi 560-II-son
2. Завгородний В.И. Комплексная зашита информации в компютерних системах // Учебное пособие. — М.: Мир, 2001. — 264 с.
3. Виталий Задорожний. Области применения и принципи построения биометрических
4. M.Z.Xusenov, L.O.Sharipova, Oliy ta’lim muassasalarida masofaviy ta’limni joriy qilish, “Pedagogik mahorat” ilmiy-nazariy va metodik jurnal. 2022, № 2 B: 94-96
5. M.Z.Xusenov, L.O.Sharipova, Kimyo fanini o‘qitishda VR texnologiyasini qo‘llash, Pedagogik mahorat Ilmiy-nazariy va metodik jurnal maxsus son (2021-yil, dekabr) 164-166
6. M.Z.Khusenov, L.O.Sharipova, Statistical analysis of network problems and their impact on the practice of social computing in Uzbekistan, E3S Web of Conferences Volume 389, 09017 (2023) Ural Environmental Science Forum “Sustainable Development of Industrial Region-31 May 2023