“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 1, ISSUE 6, 2023. SEPTEMBER
ResearchBib Impact Factor: 8.654/2023 ISSN 2992-8869

KIBERXAVFSIZLIKDAN HIMOYALANISHDA IT (INFORMATION TECHNOLOGY) SOHASINI AHAMIYATI VA ZARURLIGI

Xolboyev Sevdiyor Toyir o‘g‘li

Annoatatsiya: Bugungi axborortlashuv asrida har bir sohadagi turli ko‘rinishdagi xavf-xatarlarni hisobga olgan holda, ularni oldindan bartarf etishda muhim hisoblangan, “Information technology”(axborotlashgan qurilmalar) vositalarini joriy etishdan iboratdir. Bugungi jamiyatda axborotlarni izlash, ularni qayta ishlash va tarqatish muhim sanalib, ularni ishonchliligi hamda to‘liqligini ta’minlash zarur hisoblanadi. Chunki, shu orqali kiberxavfsizlikni ta’minlashimiz mumkin bo‘ladi.

Kalit so‘zlar: axborortlashuv asri, soha, xavf-xatarlar, Information technology, axborotlashgan qurilmalar, jamiyat, kiberxavfsizlik.

Kirish:

Axborot kommunikatsiya texnologiyalari sohasi qanchalik rivoj topgani sari, uning afzalligi va qulayliklaridan foydalanish bilan bir qatorda, butun mamlakatimizda axborot xavfsizligini ta’minlash eng dolzarb masalaga aylanib bormoqda, Ushbu soha albatta rivojlanishi kerak va buni qilamiz...

SH.M.Mirziyoyev

Jahonda kuzatilayotgan jadal globallashuv hamda axborotlashuv jarayoni, ularning faoliyatini yanada aniq olib borilishi zarurligini ham anglatadi.

Yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat axborotkommunikatsiya texnologiyalariga tobora ko‘proq qaram bo‘lib borayotganligi bois, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega.

Shu sababli, har bir tashkilotga, kiberxavfsizlikni ta’minlash maqsadida, mazkur soha bilan shug‘ullanuvchi xodimlar jalb qilinmoqda va xodimlarni kiberxavfsizlikka oid bilimlar bilan muntazam tanishtirib borish uchun qator seminar-treyning mashg‘ulotlari tashkil etilmoqda. Oliy ta’lim muassasalarida ham kiberxavfsizlikni fan sifatida o‘tilishi buning yaqqol misolidir.

Metodologik tahlil:

Axborot xavfsizligi – tasodifiy va atayin qilingan hujumlardan himoyalanish. Axborot xavfsizligi ko‘p qirrali faoliyat sohasi bo‘lib, unga faqat tizimli va kompleks yondashuv muvaffaqiyat keltirishi mumkin

Axborotni ishlash, uzatish va to‘plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo‘qolishi, buzilishi va oshkor etilishi bilan bog‘liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash axborot texnologiyalari rivojining yetakchi yo‘nalishlaridan biri hisoblanadi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda qaraladi.

Hujumchi kabi fikrlash - bo‘lishi mumkin bo‘lgan xavfni oldini olish maqsadida qonuniy foydalanuvchining hujumchi kabi fikrlash jarayoni.

Tizimli fikrlash - kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.

Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini o‘rganishda muhim hisoblanadi.

Axborot xavfsizligi - axborotning holati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo‘l qo‘yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.

Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo‘naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar, kerak bo‘lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

Axborot xavfsizligi sohasi, axborotning ifodalanishidan qat’iy nazar (qog‘oz ko‘rinishidagi, elektron va insonlar fikrlashida, og‘zaki va vizual) intelektual huquqlarni himoyalash bilan shug‘ullanadi. Kiberxavfsizlik esa elektron shakldagi axborotni (barcha holatdagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug‘ullanadi.

Bundan tashqari, hukumatlar tomonidan moliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced 12 persistent threats, APT) ham aynan kiberxavfsizlikka tegishli. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo‘nalishi deb tushunish uni to‘g‘ri anglashga yordam beradi.

Kiberxavfsizlikning bilim sohalari. CSEC2017 JTF manbasiga ko‘ra kiberxavfsizlik 8 ta bilim sohasiga bo‘lingan, o‘z o‘rnida ularning har biri qismsohalarga bo‘linadi

“*Ma’lumotlar xavfsizligi*” bilim sohasining maqsadi ma’lumotlarni saqlash, ishlash va uzatishda himoyani ta’minlash. Mazkur bilim sohasida himoyani to‘liq amalga oshirish uchun matematik va analitik algoritmlardan foydalaniladi.

“*Dasturiy ta’minot xavfsizligi*” bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy vositalarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.

“*Tashkil etuvchilar xavfsizligi*” bilim sohasi katta tizimlarda integrallashgan tashkil etuvchilarni loyihalashga, sotib olishga, testlashga, tahlillashga va texnik xizmat ko‘rsatishga e’tibor qaratadi. Tizim xavfsizligi gohida tashkil etuvchilar xavfsizligidan farq qiladi. Tashkil etuvchilar xavfsizligi tizimning qanday loyihalanganligiga, yaratilganligiga, sotib olinganligiga, boshqa tarkibiy qismlar bilan bog‘langanligiga, qanday ishlayotganligiga va saqlanayotganligiga bog‘liq bo‘ladi.

“*Aloqa xavfsizligi*” bilim sohasi tashkil etuvchilar o‘rtasidagi aloqani himoyalashga e’tibor qaratib, o‘zida fizik va mantiqiy ulanishni mujassamlashtiradi.

“*Tizim xavfsizligi*” bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat tizim xavfsizligining jihatlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun, nafaqat uning tarkibiy qismlari va ularning bog‘lanishlarini tushunish, balki yaxlitlikni ham hisobga olish talab etiladi. Ya’ni, tizimni to‘liqligicha ko‘rib chiqish talab etiladi. Mazkur bilim sohasi, “Tashkil etuvchilar xavfsizligi” va “Aloqa xavfsizligi” bilim sohalari bilan bir qatorda, tashkil etuvchilar bog‘lanishlarining xavfsizligi va undan yuqori tizimlarda foydalanish masalasini hal etadi.

“*Inson faoliyati xavfsizligi*” bilim sohasi kiberxavfsizlik bilan bog‘liq inson hatti-harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida ma’lumotlarni va shaxsiylikni himoya qilishga e’tibor qaratadi.

“*Tashkilot xavfsizligi*” bilim sohasi tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini madadlash uchun risklarni boshqarishga e’tibor qaratadi.

“*Ijtimoiy xavfsizlik*” bilim sohasi jamiyatda u yoki bu darajadagi ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. Kiberjinoyatchilik, qonunlar, axloqiy munosabatlar, siyosat, shaxsiy hayot va ularning bir-biri bilan munosabatlari ushbu bilim sohasidagi asosiy tushunchalar hisoblanadi.

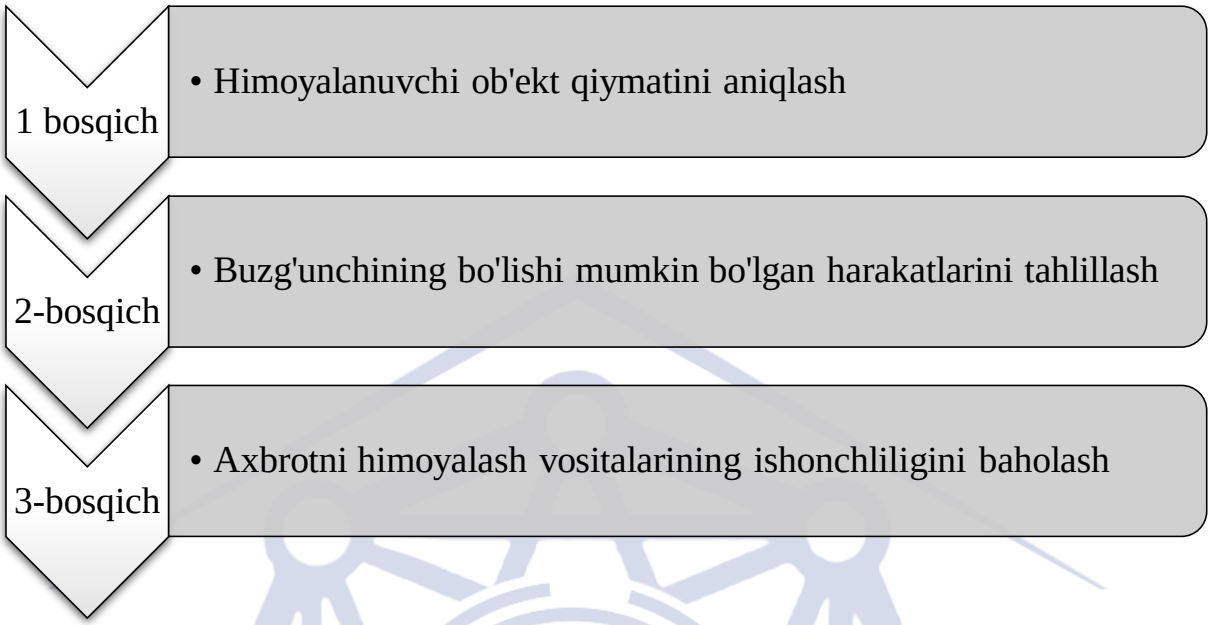
Natijalar va muhokamalar:

Axborot ximoyasi konsepsiyasini ishlab chiqish bosqichlari.

Konsepsiya – axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yullari.

Konsepsiyada ifodalangan maqsadlar, masalalar va ularni bo‘lishi mumkin bo‘lgan yechish yullari asosida axborot xavfsizligini ta’minlashning muayyan rejalari shakllantiriladi.

Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади.



Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko‘rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo‘lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:

1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat’iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma’naviy-etik. Obyektda qat’iy belgilangan o‘zini tutish qoidalarining buzilishi ko‘pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo‘llab quvvatlash.

3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to‘siqlar yaratish.

4. Ma’muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo‘llash.

Axborot xavfsizligini ta’minlashda amalga oshiriladigan dastlabki choralardan biri bu - fizik xavfsizlik hisoblanadi. Ruxsat etilmagan fizik

boshqarishni, shaxs tomonidan amalga oshiriladigan tahdidlarni va muhitga bog‘liq tahdidlarni oldini olish uchun tashkilotlar mos fizik xavfsizlik boshqaruvini sharoitida bo‘lishi shart. Tizim administratori fizik xavfsizlikga qaratilgan tahdidlardan saqlanish uchun fizik xavfsizlik choralari o‘rnatilgani va tshg‘ri ishlayotganini kafolatlashi shart.

Fizik xavfsizlik fizik qurilmalarni, shaxslarni, tarmoq va ma’lumotni hujumlardan himoyalash bilan shug‘ullanadi. Ma’lumot, tarmoqlar va qurilmalar xavfsizligi o‘zida tabiiy va sun’iy (inson tomonidan qilingan) tahdidlardan himoyalashni mujassamlashtiradi.

Tashkilotlar fizik xavfsizlikni ta’minlash uchun mos himoya vositalaridan foydalanishlari zarur. Bunda, tashkilotlar o‘z infratuzilmasi va axborot tizimlarining fizik xavfsizligiga ta’sir qiluvchi barcha yullarni inobatga olishi shart.

Xulosa:

Butun dunyodagi har bir sohada kiberxavfsizlik jarayonlarini kuzatilayotgan bir vaqtda ularga qarshi samarali faoliyat olib boradigan IT sohasini alohida ta’kidlab o‘tishimiz joizdir. Sababi, aynan kiberxavfsizlik axborotlar bilan uzviy bog‘liq hisoblanib, ularni turli xildagi ko‘rinishga keltirmaslik uchun himoya tizimini yanada mustahlashlashimiz zaruridir.

Kiberxavfsizlikni samarali bartaraf etishda “Information Technology” qurilmalarini qo‘llash orqali har bir tashkilot va korxonalarni moliyaviy hisobotlarini hamda mamlakat miqyosidagi qonun hujjatlarini ham xavfsizligini ta’minlashga erishgan bo‘lamiz. Bu esa, o‘z navbatida turli ko‘rinishdagi jinoyatlarni oldini olishimizni anglatadi.

Foydalanilgan adabiyotlar ro‘yxati.

1. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O‘quv qo‘llanma. –T.: «Aloqachi», 2019.

2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.

3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.

4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –T.: «Aloqachi», 2008, 382 bet.

5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.

6. Марков А. С., Барабанов А. В., Дорофеев А. В., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С.Маркова. –М.: ДМК Пресс, -2017. – 224с