

KIBER XAVFSIZLIK MUAMMOLARI VA YECHIMLARI

Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti, Milliy tadqiqot universiteti, "Texnologik jarayonlarni avtomatlashtirish va boshqaruv" kafedrası Axborot tizimlari va texnologiyalari bakalavr ta'lim yo'nalishi talabasi

Mamatqulov Mirvoxid Mirzoxid o'g'li

Anotatsiya: Maqolada yurtimizda hamda jahondagi kiberxavfsizlik va axborot xavfsizligi borasidagi yangilanishlar, unda kuzatilayotgan muammolar va ularni aniqlash hamda ularni bartaraf etish yo'llari, axborot xavfsizligi hamda kiberxavfsizlik to'g'risidagi qonunlar, meyoriy hujjatlar hamda Prezidentimiz tomonidan joriy etilgan qarorlari, axborot xavfsizligini ta'minlash yechimlari va ularning turli yo'llari, kiberxavfsizlikni ta'minlashning zamonaviy yo'llari hamda shu boradagi fikr mulohazalar yoritilgan .

Kalit so'zlar: Global, axborot xavfsizligi, kiberxavfsizlik, axborot kriptografiya, telekamunikatsiya, raqamli imzo, algoritim.

Annotation: In the article, there are updates on cyber security and information security in our country and in the world, the problems observed in it and ways to identify and eliminate them, information security and cyber security laws, regulatory documents and decisions introduced by the President, ensuring information security solutions and their different ways, modern ways of ensuring cyber security and opinions in this regard are highlighted.

Key words: Global, information security, cyber security, information cryptography, telecommunications, digital signature, algorithm.

Аннотация: В статье представлены последние новости о кибербезопасности и информационной безопасности в нашей стране и в мире, наблюдаемые в ней проблемы и способы их выявления и устранения, законы об информационной безопасности и кибербезопасности, нормативные документы и постановления, внесенные Президентом.

решения по обеспечению информационной безопасности и их разные способы, освещены современные способы обеспечения кибербезопасности и мнения по этому поводу.

***Ключевые слова:** Глобальный, информационная безопасность, кибербезопасность, информационная криптография, телекоммуникации, цифровая подпись, алгоритм.*

Xozirgi kunda har qanday davlatning axborot resurslari uning iqtisodiy va harbiy salohiyatini belgilovchi omillardan biri hisoblanadi. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni movaffiqiyatli shakllantirilishini ta'minlaydi. Bunday jamiyatda axborot almashinuv tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot-kommunikatsiyalar texnologiyalarini qo'llash keng ko'lamda amalga oshiriladi[1]. Mamlakatimizda hozirgi kunda axborot xavfsizligiga, shaxsiy ma'lumotlarning oshkor bo'lmasligiga ham alohida e'tibor berilmoqda. O'zbekiston Respublikasi Prezidentining "Axborot-kommunikatsiya texnologiyalari sohasidagi loyihalarni boshqarish tizimini yanada takomillashtirish chora tadbirlari to'g'risida" 2017-yil 29-avgustdagi PQ- 3245-son qaroriga muvofiq zamonaviy texnologiyalardan foydalangan holda axborot va jamiyat xavfsizligini ta'minlash axborot xavfsizligiga hozirgi vaqtdagi tahdidlar to'g'risidagi ma'lumotlarni yig'ish, tahlil qilish hamda ularni bartaraf etish ko'zda tutilgan. Axborot xavfsizligini ta'minlash muntazam va kompleks xarakterga ega ko'p qirrali faoliyatini amalga oshirishni ko'zda tutadi. Uni amalga oshirishda axborot xavfsizligidan manfaatdor taraflar oldiga qo'yiladigan vazifalarga alohida e'tibor berish zarur. Shuningdek O'zbekiston Respublikasi Prezidentining 2018-yil 21- noyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish ularni himoya qilish tizimini takomillashtirish chora- tadbirlari to'g'risida" gi PQ-4024-son qaroriga asosan axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha davlat inspeksiyasi va uning huzurida "Texnik ko'maklashish markazi"

DUK tashkil etilgan bu boradagi amaliy holatlardan muhim bosqichi deb hisoblash mumkin.

Kiberxavfsizlik.

Kompyuter xavfsizligi, kiberxavfsizlik yoki axborot texnologiyalari xavfsizligi (IT xavfsizligi) — bu kompyuter tizimlari va tarmoqlarini ma'lumotlarni oshkor qilish, o'g'irlash yoki ularning apparat, dasturiy ta'minot yoki elektron ma'lumotlariga zarar etkazish, shuningdek, buzilishdan himoya qilish. Ular taqdim etadigan xizmatlarni noto'g'ri yo'naltirish[1][2].

Axborot texnologiyalari xavfsizligi sohasi kompyuter tizimlari, Internet, Bluetooth, Wi-Fi kabi simsiz tarmoq standartlariga bo'lgan ishonchning kengayishi. Aqlli qurilmalar, jumladan, smartfonlar, televizorlar va turli xil qurilmalarning o'sishi tufayli muhim ahamiyatga ega bo'ldi. Buyumlarning internetini(IoT) tashkil etuvchi qurilmalar. Kiberxavfsizlik ham siyosiy foydalanish, ham texnologiya nuqtai nazaridan axborot tizimlarining murakkabligi tufayli bugungi kunda muhim muammolardan biri hisoblanadi. Uning asosiy maqsadi: tizimning ishonchliligi, yaxlitligi hamda ma'lumotlar maxfiyligini ta'minlashdan iborat.

Axborot xavfsizligi (inglizcha: Information Security, shuningdek, inglizcha: InfoSec) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish, tadqiq qilish, yozib olish yoki yo'q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma'lumotlar qanday shaklda bo'lishidan qat'iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta'minlashning asosiy maqsadi ma'lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo'llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta'sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Ushbu faoliyatni standartlashtirish maqsadida ilmiy va kasbiy hamjamiyatlar texnik axborot xavfsizligi choralari, yuridik javobgarlik, shuningdek, foydalanuvchi va ma'murlarni tayyorlash standartlari sohasida asosiy metodologiya, siyosat va tarmoq standartlarini ishlab chiqishga qaratilgan doimiy hamkorlik asosida ish olib boradi. Ushbu standartlashtirishga asosan ma'lumotlarga kirish, qayta ishlash, saqlash va uzatishni tartibga soluvchi keng ko'lamli qonunlar va qoidalar ta'sir ko'rsatadi. Biroq, tashkilotda agar doimiy takomillashtirish madaniyati to'g'ri shakllantirilmagan bo'lsa, har qanday standartlar va metodologiyalarni joriy etish yuzaki ta'sir ko'rsatishi mumkin .

Mavzuning dolzarbligi.

Hozirgi kunda axborot xavfsizligini ta'minlash eng dolzarb muammolardan biri bo'lib hisoblanadi. Axborot xavfsizligi sohasida amal qilinadigan hujjatlar va standartlarni hamda axborot xavfsizligi siyosatining asosiy nizomlarini aniqlash, kompyuter texnikasi vositalaridan, dasturlardan va ma'lumotlardan foydalanishni boshqarish, virusga qarshi himoya, rezervli nusxalash masalalari ta'mirlash va tiklash ishlarini o'tkazish. axborot xavfsizligi sohasidagi mojarolar xususida xabardor qilish axborot xavfsizligi siyosatini aniqlashda amalga oshirilishi lozim. Axborot xavfsizligiga bo'lishi mumkin bo'lgan tahdidlarni tahlillash yaratilayotgan himoyalash tizimiga qo'yiladigan talablarning to'liq to'plamini aniqlash maqsadida amalga oshiriladi. Zamonaviy axborot tizimida saqlanuvchi va ishlanuvchi axborot juda ko'p omillarning ta'siriga duchor bo'lishi sababli tahdidlarning to'liq to'plamini tavsiflash masalasini formallashtirish mumkin emas. Shuning uchun tahdidlarni to'liq ro'yxatini emas balki tahdidlar sinfini ro'yxatini aniqlash maqsadga muvofiq hisoblanadi. Axborot xavfsizligi sohasiga oid xalqaro standartlarning asosiy maqsadi axborot texnologiyalari mahsulotlarini ishlab chiqaruvchilar iste'molchilar va kvalifikatsiyalash bo'yicha ekspertlar orasida o'zaro aloqani yaratish hisoblandi.

Kiberxavfsizlik sohasida xalqaro hamkorlikni amalga oshirish va kibertahdidlarga qarshi kurashish bo'yicha umumiy yondashuvlarni ishlab

chiqish, kiberjinoyatchilik bo'yicha tergov harakatlarini olib borish hamda kiberjinoyatchilikning oldini olish borasidagi sa'y-harakatlarni birlashtirish, shuningdek O'zbekiston Respublikasining kibermakonidan terrorchilik, ekstremistik va boshqa qonunga xilof faoliyatda foydalanilishiga yo'l qo'ymaslik choralarini ko'rish. kiberxavfsizlik holati ta'minlanganligi yuzasidan davlat nazorati va tekshiruv vazifasini amalga oshirish maqsadida davlat organlari hamda tashkilotlarining, muhim axborot infratuzilmasi obyektlarining axborot tizimlariga va resurslariga belgilangan tartibda to'sqinlik kirish hamda ularga ulanish, shuningdek ushbu obyektlardagi axborot tizimlarining va resurslarning kiberxavfsizligini ta'minlash vositalarining joriy etilishiga hamda ulardan foydalanilishiga doir ma'lumotlarni o'rganish, davlat organlari va tashkilotlarining, shuningdek muhim axborot infratuzilmasi obyektlarining axborot tizimlari hamda resurslari ma'lumotlarining saqlanishini ta'minlash ichki axborot xavfsizligi siyosatiga muvofiq ma'lumotlarning zaxira nusxalarini yaratish yo'li bilan amalga oshiriladi, ularning saqlanish muddati oxirgi uch oydan kam bo'lmasligi kerak. kiberxavfsizlik hodisalariga nisbatan choralar ko'rish mexanizmlarining ishlab turishini va kiberxavfsizlikni ta'minlash bo'linmalarining ishlashini ta'minlashi, ular mavjud bo'lmagan taqdirda esa vakolatli davlat organining ruxsati bilan outsorsing xizmatlaridan belgilangan tartibda foydalaniladi.

Axborot tizimlari va resurslarida aniqlangan zaifliklar, kibertahdidlar. kiberhujumlar hamda boshqa buzg'unchilik harakatlari to'g'risidagi. shuningdek axborotlashtirish obyektlari haqidagi axborot ulani himoya qilish bo'yicha tegishli choralar ko'rilganidan keyin kiberxavfsizlik subyekting ruxsati bilan oshkor qilinishi mumkin. Xalqaro kiberjinoyatlarga garshi kurashish masalalariga doir axborot, agar bunday ma'lumotlar dastlabki tergov harakatlariga yoki sud jarayonlariga to'sqinlik qilmasa hamda kiberhujumlarni to'xtatishga, kibermakandan foydalanilgan holda sodir etiladigan jinoiy xatti-harakatlarni o'z vaqtida aniqlashga va ularga barham berishga xizmat qilsa, chet davlatlarga va xalqaro tashkilotlarga oldindan so'rovsiz berilishi mumkin

Foydalanilgan adabiyotlar ro'yxati:

1. <https://zenodo.org/records/6549174>
2. https://uz.m.wikipedia.org/wiki/Kompyuter_xavfsizligi
3. <https://texnokun.uz/?p=7558>
4. <https://tryengineering.org/uz/news/the-value-of-cyber-security/>
5. <https://texnokun.uz/?p=7123>