ZAMONAVIY DUNYODA KIBERXAVFSIZLIK

G‘aniyev Temur Komiljon o‘g‘li
Guliston davlat pedagogika instituti 2- kurs magistranti
Xakimova Farangis Abdualimovna
Guliston davlat pedagogika instituti “Aniq va tabiiy fanlar” kafedrasi o‘qituvchisi

Annotatsiya: *Zamonaviy axborot texnologiyalari rivojlangan hozirgi zamonda, dunyoning tobora raqamlashib borishi bilan birgalikda, raqamlashgan dunyoda yangi muammolar va yechimlar ham paydo bo‘lyapti. Kiberxavfsizlikni ta’minlash har bir inson va tashkilot uchun juda muhim ahamiyat kasb etayapti. Ushbu maqolada kiberxavfsizlikni ta’minlashning yo‘llari va usullari namoyon etiladi.*

Kalit so‘zlar*: kiberxavfsizlik, mediasavodxonlik, kiber-hujum, internet, shifrlash, xavfsizlik.*

Kiberxavfsizlik - bugungi dunyoda juda muhim bo‘lgan mavzu. Kiberxavfsizlik, internetda ma’lumotlarni himoya qilish, tarmoq bo‘ylab o‘tkazilayotgan faoliyatni himoya qilish, shaxsiy ma’lumotlarni himoya qilish va kiber-hujumlar va xavfli dasturlarga qarshi himoya qilishni o‘z ichiga oladi. Kiberxavfsizlikning muhim qismlaridan biri shifrlash va deshifrlashdir. Shifrlash, ma’lumotlarni shifrlash protokollari orqali himoya qilishni tushunib olgan har bir shaxsga katta yordam beradi. Buning o‘zida, shaxsiy ma’lumotlar, bank ma’lumotlari, kompaniyaning maxfiy ma’lumotlari va boshqalar kabi muhim ma’lumotlarni himoyalashda yordam beradi. Biroq, shifrlash barcha xavflarga qarshi to‘liq himoya bermaydi, shuning uchun yangi xavfsizlik texnologiyalari va uskunalari hamda xavfsizlik protokollari va standartlari dastlabki kiber-hujumlar bilan kurashishda juda muhimdir.

Kiber-hujumlar, internetdagi xavfsizlikni buzishning bir qismini tashkil etadi. Bu xavfsizlik tizimlariga, tarmoq qurilmalariga, shaxsiy ma’lumotlarga va dasturlarga zarar berish uchun tuzilgan zararli faoliyatlar jamlanmasidir. Kiber-hujumlar boshqa odamlar yoki tashqi tashkilotlar tomonidan qilinishi mumkin va xavf darajasi va shakli farqli bo‘ladi.

Kiberxavfsizlikka oid bo‘lgan dastlabki bilimlarni egallash va u haqida ma’lumotlarga ega bo‘lish har bir soha uchun juda muhimdir. O‘rganilishi kerak bo‘lgan bilimlarga, shaxsiy ma’lumotlarni himoya qilish, ma’lumotlar bazasini himoya qilish, tarmoq qurilmalarini himoya qilish, kiberxavfsizlikning huquqiy va siyosiy jihatlarini o‘rganish, xavfsizlikni ta’minlash va kiberxavfsizlik sohasidagi rivojlanishlar va yangiliklarga qarshi amalga oshirishni o‘z ichiga oladi.

Bu mavzu haqida yozilgan maqola kiberxavfsizlikning ko‘p aspektlarini qamrab oladi va internet foydalanuvchilarini kiberxavfsizlik xavflari va ularga qarshi qo‘llanma berish konseptlarini tushunishga yordam berishi lozim.

Kiberxavfsizlikning o‘zgaruvchiligi. Kiberxavfsizlik, internetdagi ma’lumotlar va tarmoq tizimlarining himoyalanganligi va xavfli dasturlar va kiber-hujumlar qarshi himoya qilinishi bilan bog‘liqdir. Internet dunyoda ko‘p kishi tomonidan ishlatilishi bilan, kiberxavfsizlik katta ahamiyatga ega bo‘lgan mavzu bo‘lib, xususan shaxsiy ma’lumotlarni himoya qilish, shaxsiy identifikatsiyani himoya qilish va internetdagi ma’lumotlar va tarmoq tizimlarining himoyalanganligini ta’minlash uchun strategiyalar va texnologiyalar rivojlanishi bilan bog‘liqdir.

Kiberxavfsizlik rishtalari va turlari. Kiber-hujumlar, internet xavfsizligiga tegishli muammolar va xavfsizlikni buzish uchun tuzilgan zararli faoliyatlar jamlanmasidir. Ular viruslar, zararli dasturlari, foydalanuvchi ma'lumotlarini olish, tarmoqni to'xtatish, xavfsizlik protokollari va tarmoq ustidagi majburiy ko'rish va boshqa ko'rishlar kabi turli xil usullar orqali amalga oshirilishi mumkin.

Kiberxavfsizlikni ta'minlash usullari. Kiberxavfsizlikni ta'minlash uchun bir nechta usullar mavjud. Ulardan biri shifrlashdir, bu xavfsizlik standartlari va protokollari orqali ma'lumotlarni shifrlash va himoya qilishni tashkil etadi. Boshqa usullar orasida, faol monitor qilish va identifikatsiya, kiberxavfsizlikni ta'minlashning amaliy asoslarini o'rganish va amalga oshirish, kiberxavfsizlikning to'g'ri aniqlanishi va taqib qilinishi, tarmoqni ta'minlash va qo'lda tutish, foydalanuvchilar uchun xavfsizlik bilan ta'minlashni taqozo qilish va boshqalar kabi usullar kiritiladi.

Kiberxavfsizlikning mustahkamligi va kelajagi Kiberxavfsizlik so'rovnoma, internet tarmoqlarini himoya qilish va kiberxavfsizlikni ta'minlashda mustahkamligini ta'minlashga va kiberxavfsizlikning kelajagiga oid strategiyalarni qamrab oladi. Bu strategiyalar, kiberxavfsizlikning yuqori darajadagi ta'minoti va xavfsizlik standartlarini o'rganish, amalga oshirish, va o'zgarishi uchun kiberxavfsizlik sohasida ko'p miqdorda resurslarni o'z ichiga oladi. Bu internet dunyosining mustahkam va xavfsiz bo'lishini ta'minlashda katta ahamiyatga ega bo'lgan bir jarayon.

Bugungi kunda kiberxavfsizlik, global tarmoqni o'z ichiga olgan hamma narsani, shu jumladan shaxsiy ma'lumotlarni, korporativ ma'lumotlarni, iqtisodiy tarmoqni, davlat tizimlarini, so'nggi qo'shimcha texnologiyalar va IoT qurilmalarini himoya qilish uchun juda katta ahamiyatga ega. Kiberxavfsizlikni ta'minlashning bir nechta yo'llari mavjud. Bu yo'llar boshqa yo'llar bilan birgalikda ishlash uchun, kiberxavfsizlikni mustahkamlashtirish va ma'lumotlarni himoya qilishda keng qamrovli strategiyalarga asoslangan.

Shifrlash: Ma'lumotlarni shifrlash, xususan ko'rsatkichlar, dastlabki kiber-hujumlarni qarshi olish uchun juda muhimdir. Asosiy ma'lumotlar, shaxsiy ma'lumotlar, va korporativ ma'lumotlar shifrlanishi lozim.

Kiberxavfsizlik ta'limga ega bo'lish: Foydalanuvchilar, tizim administratorlari va korporativ hodimlar kiberxavfsizlik ta'limidan o'tishlari kerak. Bu ta'limlar, xavfsizlik prinsiplarini, xavfsizlik texnologiyalarini va xavfsizlik qo'llanmalarini o'rganishga yordam beradi.

Dasturiy ta'minot: Dasturiy ta'minot kiberxavfsizlikni ta'minlashning juda muhim qismidir. Dasturlar, o'rnatilgan xavfsizlik tuzilmalarini ishga tushirish, xavfsizlikni tekshirish, kiber-hujumlarni aniqlash va qo'llash, va shifrlash kabi vazifalarni bajarish uchun ishlab chiqilgan.

Foydalanuvchi identifikatsiyasi va menejmenti: To'g'ri foydalanuvchi identifikatsiyasi va menejmenti kiberxavfsizlikni ta'minlash uchun katta ahamiyatga ega. Kiritishlar, parollar, biometrik identifikatsiya, va ikki bosqichli autentifikatsiya kabi vositalar ishlatilishi mumkin.

Kiberxavfsizlikni monitoring va taqib qilish: Tarmoq xodimlari kiber-hujumlarni kuzatish va uchun ariza berish va taqib qilishni amalga oshirish uchun monitorlash va monitoring vositalaridan foydalanishlari kerak. So'nggi dastur parvarishi va yangilanishi: Kiberxavfsizlik texnologiyalari va protokollari kuzatilishi va yangilanganini ta'minlash muhimdir. So'nggi kiber-xavfsizlik yangilanishlarini va dasturlarni ishlatish, kiber-hujumlar va xavfli dasturlarga qarshi ta'minotni ta'minlashda juda muhimdir.

Korporativ kiberxavfsizlik qo'llanmalari: Korporativ ma'lumotlar uchun maxsus kiberxavfsizlik qo'llanmalari va veb-xavfsizlik texnologiyalari juda muhimdir. Ular xavfsizlik ta'limga ega bo'lish, dasturiy ta'minot, foydalanuvchi identifikatsiyasi va menejmenti va ma'lumotlarni shifrlashni o'z ichiga oladi. Bu yo'llar kiberxavfsizlikni ta'minlashda muhim bo'lib, kiberxavfsizlik so'rovnoma va strategiyalarining asosini tashkil etadi.