

KIBERJINOYATCHILIKKA QARSHI KURASHISH**Mamasiddiqova Bibioysha Komiljon qizi***Farg'ona viloyati Yuridik texnikum**1-kurs "22-22" "Yuridik xizmat" yo'nalishi*

Annotatsiya: *Ushbu maqolada Kiberjinoyatchilikka va kiberterrorizmga qarshi kiberhujumni yanada takomillashtirish chora tadbirlari to'g'risida.*

Kiberjinoyatchilik to'g'risida, axborot-kommunikatsiya texnologiyalaridan foydalanish, virtual tarmoqda daxshat solish, virus va zararli dasturlar, qonunga zid axborotlar va xakerlik hujumi haqida so'z boradi.

Kalit so'zlar: *Kiberjinoyat, kiberterrorizm, qonunbuzarlik, xavf, zarar, ma'lumotlar, axborot texnologiyalari, dasturlar, firibgarlik va mualliflik huquqini buzilishi.*

Kiberjinoyat – axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlarni tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, ma'lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o'g'irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi.

Shu o'rinda kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko'lami ham oshib borayotganini ta'kidlash joiz. Kiberterroristik harakat (kiberhujum) - kompyuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti sog'lig'iga bevosita xavf tug'diradigan yoki potensial xavf tug'dirish mumkin bo'lgan, ijtimoiy xavfli oqibatlarining boshlanishi yoki maqsadi bo'lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog'liq.

Ekspertlarning xulosasiga ko'ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko'maklashish, ummuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta'sir o'tkazish, ularni turli yo'llar bilan o'z maqsadlari sari bo'ysundirish orqali amalga oshirilmoqda.

O'zbekiston Respublikasining 2022-yil 25-fevralda qabul qilingan Kiberxavfsizlik to'g'risidagi qonunga muvofiq;

Telekommunikatsiya tarmoqlari va aloqa kanallaridagi tezkor-qidiruv tadbirlari tizimining kiberxavfsizligini ta'minlash alohida qonunchilik hujjatlarida belgilangan tartibda amalga oshiriladi.

Agar O'zbekiston Respublikasining xalqaro shartnomasida O'zbekiston Respublikasining kiberxavfsizligi to'g'risidagi qonunchiligida nazarda tutilganidan boshqacha qoidalar belgilangan bo'lsa, xalqaro shartnoma qoidalari qo'llaniladi.

Bugungi kunda jahon hamjamiyatiga integratsiyalashayotgan mamlakatlarimizda axborot kommunikatsiya texnologiyalari, axborot tizimlari va zamonaviy kompyuter texnologiyalaridan samarali foydalanish bo'yicha izchil davlat siyosati olib borilmoqda.

Undan tashqari mamlakatimizda joriy etilayotgan zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar eshigini ochib bormoqda. Mazkur jarayonda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta'minlash muammosi ham mavjud, albatta.

Bu esa eng dolzarb masalalardan biri hisoblanadi, ya'ni kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo'lgan kiberjinoyat va kiberterrorizmlarni oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Kundan-kunga takomillashib borayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta'minlashda, quyidagi talablarni bajarish orqali ulardan himoyalani, ya'ni kiberxavfsizlikni ta'minlashimiz mumkin;

- ishonchli antivirus dasturidan foydalanish,
- foydalanilayotgan dasturiy mahsulotlarning zaifliklarini doimiy nazoratdan o'tkazib turish,
- xodimlarga axborot xavfsizligi asoslarini o'rgatish,
- parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish,
- litsenziyalangan rasmiy dasturlardan foydalanish,
- axborot tizimlarini himoyalashda ko'p faktorli autentifikatsiyadan foydalanish,
- muntazam ravishda kompyuter qattiq disklaridagi ma'lumotlarni shirflash,

Shu o'rinda mamlakatimizda kiberjinoyatchilikka qarshi kurashish va uni oldini olib boruvchi vakolatli davlat idoralariga ham muayyan vazifalar yuklanishi alohida takidlash lozim.

Xususan, kiberjinoyatchilikka qarshi kurashish faoliyatida O'zbekiston Respublikasi va uning xalqini axborot texnologiyalari va kommunikatsiyalari orqali amalga oshirayotgan va bunga imkon yaratib berayotgan shaxs, jamiyat va davlat xavfsizligini va ularning manfaatlarini tashqi va ichki tartibda kibertahdidlardan himoya qilishni ta'minlash, mazkur sohada qonuniylik va qonun ustuvorligini mustahkamlash, kiberjinoyatlar va kiberhuquqbuzarliklarni oldini olish va ularni aniqlash hamda barham berish kabivazifalarni amalga oshirishi darkor.

Undan tashqari, sertifikatlangan firibgarlik ekspertlari assotsiatsiyasi tomonidan olib borilgan yaqindagina o'tkazilgan tadqiqotlar shuni ko'rsatadiki, raqamli axborot xavfsizligi tashkilotlar uchun dolzarb muammo bo'lib, direktorlar va rahbarlar kelajakda muammo yanada yomonlashishini kutishmoqda:



“Kiberfiribgarlik - bu ishbilarmonlik, elektron pochta xabarlarini buzish, xakerlik, to'lov dasturi va zararli dasturlarning eng yuqori xavf sohasi bo'lib bormoqda, ya'ni respondentlarning 85% allaqachon bu sxemalarning o'sishini ko'rishgan va 88% keying davrda yanada oshishini kutishmoqda”.

Darhaqiqat, ijtimoiy tarmoq egalari ushbu tarmoqlar sahifalarida davlat tuzumini ag'darishga da'vat qilingani uchun javobgarlikka tortilishining xalqaro miqyosdagi huquqiy asoslari yaratilmagan. Vaholanki, har bir qilingan jinoiy xatti-harakat yoki harakatsizlik mazmun-mohiyatiga ko'ra, javobsiz va jazosiz qolmasligi kerak, albatta.

FOYDALANILGAN ADABIYOTLAR RO'YHATI:

1. O'zbekiston Respublikasining Qonuni Kiberxavfsizlik to'g'risida. – T.: 2022.
2. O'zbekiston Respublikasi Konstitutsiyasi. – T.: O'zbekiston . 2019.
3. Kiberjinoiyatchilikka qarshi kiberxavfsizlik. – T.: O'zbekiston. 2022.