KIBERJINOYATLARGA QARSHI KURASHDA YANGI ÓZBEKISTONDA OLIB BORILYOTGAN XAVFSIZLIK VA HUQUQIY MUAMMOLAR VA ULARNING YESHIMLARI.

Azirbaev Salamat Kuanishbaevich

Qoraqalpoq davlat universiteti yurisprudensiya tálim yónalishi yuridika fakulteti 3-kurs talabasi.Tel raqami: +998 90 700-68-62 Email: azerbaevsalamat947@gmail.com.

Annotaciya: *Ushbu maqola jahon báylab jiddiy xavf tuǵdiryapkan kiberjinoyatlar haqida bóladi.Bu maqolada kiberjinoyat tushunchasi mazmun mohiyati ularning turlari haqida va unga qanday kurashish.Davlatimizda xavsizlik va huquqiy muommolar haqida bóladi.*

Kalit sózlar: *qonun va nizomlar ,himoya ,kiberjinoyat ,kiberhujum ,kibertahdid , kiberhimoya ,DdoS ,internet erkinligi,masalar,ilimiy-tadqiqotlar.*

KIRISH

Hozirgi kunda kiberjinoyatlar jahon bo'ylab jiddiy xavf tug'dirmoqda. Raqamli texnologiyalar va internetning tez rivojlanishi bilan birga, kiberjinoyatlar ham yangi shakllarga kirib, butun dunyo bo'ylab iqtisodiy, ijtimoiy va siyosiy muammolarni keltirib chiqarmoqda. O'zbekistonda ham kiberjinoyatlarning miqdori ortib bormoqda, bu esa mamlakatda kiberxavfsizlikni ta'minlashda yangi chora-tadbirlarni ishlab chiqishni zarur qiladi. Ushbu tezisda kiberjinoyatlar, ularning turlari, O'zbekistondagi holati va kiberxavfsizlikni kuchaytirish bo'yicha tavsiyalar ko'rib chiqiladi.

Kiberjinoyatlar va ularning turlari:

Kiberjinoyat tushunchasi: Kiberjinoyatlar - bu internet va raqamli texnologiyalar yordamida amalga oshiriladigan jinoyatlardir. Ular, odatda, ma'lumotlarni o'g'irlash, firibgarlik, tizimlarni buzish, xavfsizlikni buzish kabi harakatlarni o'z ichiga oladi.

ONESEC kiberxavfsizlik kompaniyasi direktori Dmitriy Paleyev.

2023-yilda O‘zbekiston jiddiy kiberxavfsizlik muammosi bilan qarama-qarshi vaziyatda, ayni vaqtda, veb-resurslarimizga 11,2 milliondan ortiq kiberhujumlar amalga oshirildi. Ushbu kiberhujumlarning geografik kelib chiqish tahlili ba’zi tendensiyalarga yo’l ochdi. IP manzillardan olingan ma’lumotlarga ko’ra, 759 500 kiberhujum “vatani” Niderlandiya bo‘ldi. Bunday mamlakatlar qatorini shunday davom ettirish mumkin: AQSH, Rossiya, Germaniya, Hindiston va Xitoy. Ushbu tahdidlar O‘zbekistonga qaratilgan hakerlik hujumlarining qariyb 90 foizini tashkil etadi. Natijada kiberxavfsizlikni ta’minlashda transmintaqaviy hamkorlik zarur elementga aylanadi.

Ushbu Qonunda quyidagi asosiy tushunchalar qo‘llaniladi:

axborotlashtirish obyekti — turli darajadagi va maqsaddagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotga ishlov berishning texnik vositalari, ushbu vositalar o‘rnatilgan va foydalaniladigan xonalar;

kiberjinoyatchilik — axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi;

kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit;

kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

kiberxavfsizlik hodisasi — kibermakonda axborot tizimlarining ishlashida uzilishlarga va (yoki) ulardagi axborotning ochiqligi, yaxlitligi va undan erkin foydalanilishining buzilishiga olib kelgan hodisa;

kiberxavfsizlik obyekti — axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ta'minlashga doir faoliyatda foydalaniladigan axborot tizimlari majmui, shu jumladan muhim axborot infratuzilmasi obyektlari;

kiberxavfsizlik subyekti — milliy axborot resurslariga ega bo'lish, ulardan foydalanish va ularni tasarruf etish hamda ulardan foydalanish bo'yicha elektron axborot xizmatlari ko'rsatish, axborotni himoya qilish hamda kiberxavfsizlik bilan bog'liq muayyan huquqlar va majburiyatlarga ega bo'lgan yuridik shaxs va (yoki) yakka tartibdagi tadbirkor, shu jumladan muhim axborot infratuzilmasi subyektlari;

kiberhimoya — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma'lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui;

kiberhujum — kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat;

muhim axborot infratuzilmasi — muhim strategik va ijtimoiy-iqtisodiy ahamiyatga ega bo'lgan avtomatlashtirilgan boshqaruv tizimlarining, axborot tizimlari hamda tarmoqlar va texnologik jarayonlar resurslarining majmui;

muhim axborot infratuzilmasi obyektlari — davlat boshqaruvi va davlat xizmatlari ko'rsatish, mudofaa, davlat xavfsizligini, huquq-tartibotni ta'minlash, yoqilg'i-energetika majmui (atom energetikasi), kimyo, neft-kimyo tarmoqlari, metallurgiya, suvdan foydalanish va suv ta'minoti, qishloq xo'jaligi, sog'liqni saqlash, uy-joy kommunal xizmatlar ko'rsatish, bank-moliya tizimi, transport, axborot-kommunikatsiya texnologiyalari, ekologiya va atrof-muhitni muhofaza qilish, strategik ahamiyatiga ega bo'lgan foydali qazilmalarni qazib olish va qayta ishlash sohasida, ishlab chiqarish sohasida, shuningdek iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada qo'llaniladigan axborotlashtirish tizimlari;

Internet erkinligi - inson erkinligi

Har bir shaxs undan axborot olish huquqiga ega. Oqni qoradan ajratish xalqning o'ziga havola, ammo hamma uchun internetga kirish imkoniyati yaratib berilishi kerak, degan siyosat olg'a surilmoqda.

Axborot chegara tanlamaydi, virtual to'siqlarni tan olmaydi. O'tgan yili Eronda hukumatga qarshi namoyishlarda yosh ayolning otib o'ldirilishi butun dunyoni larzaga soldi. Qo'l telefoniga yozilgan fojia bir zumda internetga yo'l topgan.

Birmada 2007 yilgi ommaviy qo'zg'olon ... uni bostirishga safarbar etilgan harbiylar namoyishchilarga qarata o't ochgani hech kimga sir emas. Tasvirlar internetda fosh etildi.

Bugungi kun axborot tizimlari, deydi Amerika Davlat kotibasi Xillari Klinton, kurrai zaminni bamisoli nerv sistemasi harakatlantirib turadi.

"Hatto avtoritar jamiyatlarda ma'lumotni xalqdan yashirishga qanchalik harakat qilishmasin, kerakli axborotni baribir topib olishyapti", - deydi Xillari Klinton.

Kiberjinoyatlarning turlari:

Hakerlik: Kompyuter tizimlariga noqonuniy kirish va ma'lumotlarni o'g'irlash.

Ma'lumot o'g'irlik: Bank hisob raqamlarini, shaxsiy ma'lumotlarni va boshqa moliyaviy ma'lumotlarni o'g'irlash.

Ransomware (Shantaj dasturlari): Foydalanuvchining tizimini bloklash va uni ochish uchun pul talab qilish.

Internet orqali kiberhujumlar: Tashqi tizimlarga qarshi amalga oshiriladigan hujumlar, masalan, DDoS hujumlari (Distributed Denial of Service).

Kiberjinoyatlarning global miqyosdagi ta'siri:Kiberjinoyatlar butun dunyo bo'ylab iqtisodiy zararlarga olib kelmoqda. 2020-yilda kiberjinoyatlarning global iqtisodiy zarari 1 trillion dollarga yetgan.

O'zbekistonda kiberjinoyatlar va ularni oldini olish:

Kiberxavfsizlikka oid qonunlar va tizimlar: O'zbekistonda kiberjinoyatlar bilan kurashish uchun 2019-yilda "Kiberxavfsizlik to'g'risida"gi qonun qabul qilingan. Bu qonun mamlakatda kiberjinoyatlarga qarshi kurashish va internet xavfsizligini ta'minlashda muhim rol o'ynaydi.

Kiberxavfsizlikka oid chora-tadbirlar:

O'zbekistonda kiberxavfsizlikni ta'minlash uchun davlat va xususiy sektorlar o'rtasida hamkorlik rivojlanmoqda. Misol uchun, Yagona interaktiv davlat xizmatlari portalida shaxsiy ma'lumotlarni himoya qilish va xavfsizligini ta'minlash uchun maxsus texnologiyalar joriy etilgan.

O'zbekistonda kiberjinoyatlar ko'payishi bilan iqtisodiy va ijtimoiy zararlar ham ortib bormoqda. Elektron tijorat va moliyaviy xizmatlar sohasida firibgarliklar, bank hisob raqamlariga noqonuniy kirish, shaxsiy ma'lumotlarni o'g'irlash holatlari ko'paymoqda.

3. Huquqiy va axloqiy masalalar:

Kiberjinoyatlar bilan kurashishdagi huquqiy chora-tadbirlar:

O'zbekiston Respublikasida kiberjinoyatlar bilan kurashish uchun turli huquqiy tartiblar joriy etilgan. Shu bilan birga, jinoyat protsessual qonunlar, shuningdek, xalqaro huquq standartlariga asoslanib, kiberjinoyatlar bilan kurashishda samarali tizim yaratish zarur.

Axloqiy masalalar va jamoatchilikni ogohlantirish:

Kiberjinoyatlar faqat qonunbuzarlik emas, balki axloqiy muammo hamdir. Foydalanuvchilarni internetda xavfsiz faoliyat yuritishga o'rgatish, ularni kiberhujumlardan saqlanishga rag'batlantirish zarur.

4. Kelajakdagi chora-tadbirlar va istiqbollar:

Texnologik yechimlar va ilmiy tadqiqotlar:

Kiberjinoyatlarga qarshi kurashishda yangi texnologiyalarni, masalan, sun'iy intellekt va blokcheynni qo'llash mumkin. Bu texnologiyalar yordamida ma'lumotlarni himoya qilish va xavfsizlikni kuchaytirish mumkin.

Kiberxavfsizlik sohasidagi ilmiy-tadqiqotlar:

O'zbekistonda kiberxavfsizlikni ta'minlash uchun ilmiy tadqiqotlar olib borish zarur. Bu sohada ilmiy salohiyatni rivojlantirish, kiberjinoyatlarga qarshi yangi qonunlar va texnologiyalarni ishlab chiqish mumkin.

Xulosa:

Kiberjinoyatlar O'zbekistonda, shuningdek, butun dunyoda jiddiy xavf tug'diradi. Bu jinoyatlar nafaqat iqtisodiy, balki huquqiy va axloqiy muammolarni ham keltirib chiqaradi. Kiberjinoyatlar bilan kurashishda samarali qonunlar, texnologiyalar va xalqaro hamkorlikni kuchaytirish zarur. O'zbekistonda kiberxavfsizlikni ta'minlash uchun davlat va xususiy sektorlarning hamkorligi, shuningdek, jamoatchilikni kiberhujumlardan saqlanishga o'rgatish lozim.

MANBALAR:

1) Ózbekston Respublikasi Jinoyat kodeksi 2022-yil
2) Ózbekston Respublikasi Kiberxavfsizlik to'g'risida qonun 2019-yil
3) https://lex.uz/uz/docs/-5960604
4) https://www.amerikaovozi.com/a/a-36-2010-03-26-voa1-93371769/807021.html
5) https://daryo.uz/2024/08/27/ozbekistonda-kiberxavfsizlik