KIBERMAKONDA SODIR ETILADIGAN JINOYATLAR VA ULARGA QARSHI KURASHISH MEXANIZMLARI

Mirolimova Marjona Sherali qizi
O'zbekiston Respublikasi IIV Akademiyasi 2-bosqich kursanti

Annotatsiya: *Mazkur maqolada, ayni vaqtda O'zbekistonda kiberjinoyatlar, hozirgi muammolar va kiberjinoyatlarga qarshi kurashish, kiber jinoyatchilikning turlari, ularning alomatlari, ulardan qanday himoyalanish zarurligi, kiber jinoyatchilikka qarshi aholining barcha qatlami orasida huquqiy ong va madaniyatni rivojlantirish, ya'ni fuqarolarga kiber jinoyatchilikning tashqi belgilari va ulardan qanday birlamchi himoyalanish mumkinligi haqida ma'lumotlarni yetkazish orqali imunitet hosil qilish masalalari tahlil qilingan.*

Kalit so'zlar: *kiber jinoyat, raqamli texnalogiya, kiberbulling, kiberterrorizm, ransomware, DDos hujumlari, Phishing, antimalware, autentifikatsiya.*

XXI asr – raqamli texnologiyalar asri hisoblanadi.Hozirda hayotimizni uyali telefon, internet, kompyuterlarsiz tasavvur etish qiyin. Bugun har bir inson axborot taxnologiyalari bilan chambarchas bog'liq, internetdan foydalanuvchilar soni esa kundan-kunga ortib bormoqda. Chunki yer yuzining deyarli istalgan nuqtasidan internetga ulanish imkoni mavjud.

Biz muloqot qilish va biznes yuritish uslubimizdan tortib, o'zimizni ko'ngil ochish va ma'lumot izlash tarzimizgacha, raqamli texnologiyalar bizning mavjudligimizning barcha jabhalariga kirib bordi.Turli xil internet do'konlari, turli xildagi yetkazib berish xizmatlari, onlayn kurslar, onlayn to'lovlar va shunga o'xshash yangidan-yangi bizneslar ko'payibgina qolmay, bulardan noto'g'ri foydalanayotganlar soni ham oshyapti.

Raqamli texnologiya misli ko'rilmagan qulaylik va ulanishlarni keltirib chiqargan bo'lsada, u jinoiy xatti-harakatlarning yangi shakllarini keltirib chiqardi va an'anaviy qonunchilik asoslari hal qilish uchun yetarli darajada muammolarni ko'paytirdi.

Kiberjinoyatchilar bir paytda faqat jismoniy dunyoda amalga oshirilgan harakatlarni amalga oshirish uchun onlayn tizimlardagi zaifliklardan foydalanadilar. Raqamli texnologiyalar asrida o'g'irlik, firibgarlik, bezorilik kabi jinoyatlarining yangi shakl va o'lchamlarga ega turlari shakllarda paydo bo'lmoqda. Bu xavf- kiber hujumlar (raqamli hujumlar) bo'lib, buning natijasida, internet orqali pul o'tkazmalari, davlat va tijorat sirlari, fuqarolarning daxlsizligi xavf ostida qolishi mumkin. Masalan, moliyaviy firibgarlik nafaqat an'anaviy usullarni, balki ishlab chiqilgan onlayn firibgarlik va fishing hujumlarini ham o'z ichiga oladi.

Quyida kiberjinoyatlarning keng tarqalgan turlari keltirib o'tilgan: [1]

[1] https://www.uzmarkaz.uz/en/news/kibermakondagi-jinoyatlar-va-ularning-oldini-olish-choralari

Kiberbulling – virtual olamda axborot texnologiyalari va raqamli texnologiyalardan foydalangan holda biror bir shaxs yoki guruh haqida haqoratli xabarlarni internet tarmog‘ida tarqatish yoxud joylashtirishni anglatadi.

Kiberterrorizm – har qanday davlat yoki jamiyat o‘rtasida turli xil qo‘rquv va vahima o‘rnatish maqsadida noqonuniy va buzg’unchi haraklarni bitta shaxs yoki guruh tomonidan amalga oshirilishi.

Kompyuter firibgarligi — bu axborot texnologiyalari va internetdan foydalanib, odamlar yoki tashkilotlardan noqonuniy yo‘l bilan pul, ma’lumot yoki mol-mulkni qo‘lga kiritish jinoyatidir.

Ransomware — bu zararli dastur fayllarga kirishni cheklash uchun foydalaniladigan, ba’zida to‘lov to‘lanmasa, ma’lumotlarni doimiy ravishda o‘chirib tashlash bilan tahdid qiladigan kiber to‘plashning bir turi. Kapersky Lab 2016 Security Bulletin hisobotiga ko‘ra, biznes har 40 daqiqada Ransomware qurboni bo‘ladi.

2021-yilda har 11 daqiqada biznesga hujum qilishni bashorat qilgan. Ransomware dunyodagi eng tez o‘sib borayotgan kiberjinoyatlardan biri bo‘lib qolmoqda, 2021-yilda ransomware zararlarining taxminan 20 milliard dollarga yetgani aytilgan bo‘lsa, 2025-yilda bu raqam taxminan 57 milliard dollar atrofida baholanmoqda — ya’ni so‘nggi yillarda ransomware global iqtisodiyotga sezilarli va tez o‘sayotgan zarar yetkazmoqda. Ransomware zararlarining 2031 yilda 275 milliard dollar dan oshishi kutilgan.

DDos hujumlari -Tizimga bir vaqtning o’zida ko‘plab so‘rovlar yuborish orqali serverlarni ishdan chiqarishga qaratilgan hujumlar. Bu orqali veb-saytlar va onlayn xizmatlar vaqtincha to‘xtab qolishi mumkin. DDoS hujumlari – ma’lum bir veb-sayt yoki serverga ortiqcha yuk tushirib, uni ishlamay qolishiga sabab bo‘luvchi jinoyatlardan biridir.

Phishing — bu kiberfiribgarlik usuli bo‘lib, unda jinoyatchilar o‘zini ishonchli tashkilot (bank, davlat idorasi, mashhur kompaniya,) sifatida ko‘rsatib, foydalanuvchilarning maxfiy ma’lumotlarini qo‘lga kiritishga harakat qiladi. Maqsadi login va parollarni olish, bank karta ma’lumotlarini o‘g‘irlash ,shaxsiy identifikatsiya ma’lumotlarini qo‘lga kiritish

Zamonaviy jamiyatda sodir etilayotgan kiber taxdidlarning tobora soni va salohiyatini ko‘payishi axborot texnologiyalari davridagi har bir davlat uchun o‘ta dolzarb bo’lgan asosiy vazifa - axborot xavfsizligini ta'minlash zarurligini keltirib chiqarmoqda.

Bundan tashqari yaqin yillar davomida mamlakatimiz hududida keng tarqalayotgan kiberjinoyatlarni xisobga oladigan bo’lsak, ushbu turdagi jinoyatlarga qarshi kurashish va oldini olishda birinchi navbatda jinoyat turlarini, kelib chiqish sabablari xamda xorijiy tajriba va xalqaro tasis etilgan standartlarni chuqurroq o‘rganish hamda huquqni muhofaza etuvchi organlar faoliyatida hamda hayotimizda foydalanish bugungi kundagi asosiy vazifalarimizdan biridir.

Shuningdek, Tojikiston poytaxti Dushanbe shahrida 2021-yil 17-sentabr kuni bo‘lib o‘tgan Shanxay hamkorlik tashkiloti Davlat rahbarlari Kengashining yubiley majlisida, Shavkat Mirziyoev kibermakondagi zamonaviy tahdid va xatarlarga munosib javob qaytarish uchun SHHTning axborot xavfsizligi sohasidagi ekspertlar forumini ta’sis etish to‘g‘risida tashabbus bilan chiqqanligi bu sohaga oid yanada ko‘plab izlanishlar olib borishimiz kerakligini ko‘rsatib turmoqda.[2]

Hozirgi paytda kiberjinoyatlarga qarshi kurashishning zamonaviy mexanizmlari joriy etilgan bo’lib ularga quyidagilar kiradi ;

1. Tashkiliy mexanizmlar
2. Texnik himoya mexanizmlari
3. Tashkiliy choralar
4. Xalqaro hamkorlik
5. Profilaktika va xabardorlik

1. Huquqiy mexanizmlar

Kiber jinoyatlarga qarshi kurashishda eng muhim omillardan biri — mustahkam huquqiy baza yaratishdir.

Xalqaro miqyosda bu borada United Nations tomonidan kiberxavfsizlik va axborot xavfsizligiga oid tashabbuslar ilgari surilgan. Shuningdek, Council of Europe tomonidan qabul qilingan Kiberjinoyatlar to‘g‘risidagi Budapesht konvensiyasi davlatlar o‘rtasida hamkorlikni kuchaytirishga xizmat qiladi.

Milliy darajada esa har bir davlat o‘z Jinoyat kodeksi va axborot xavfsizligiga oid qonunlari orqali quyidagilarni belgilaydi:

Kompyuter ma’lumotlariga noqonuniy kirish uchun javobgarlik;

Ma’lumotlarni yo‘q qilish yoki o‘zgartirish uchun jazo;

Elektron firibgarlik va identifikatsiya o‘g‘irligiga qarshi choralar.

Huquqiy mexanizmlar jinoyatchilarni aniqlash, jazolash va profilaktika choralarini ko‘rishga asos bo‘ladi.

2. Texnik himoya mexanizmlari

Texnik vositalar kiber hujumlarning oldini olishda muhim rol o‘ynaydi. Ular quyidagilarni o‘z ichiga oladi:

Kriptografiya va ma’lumotlarni shifrlash;

Antivirus va antimalware dasturlari;

Ikki bosqichli autentifikatsiya ;

Zaxira nusxa (backup) tizimlari;

Texnik choralar yordamida axborot tizimlari himoyalanadi, hujumlar erta aniqlanadi va zarar miqdori kamaytiriladi.

3. Tashkiliy mexanizmlar

Kiber jinoyatlarga qarshi kurashishda maxsus institut va tuzilmalar tashkil etiladi. Ko‘plab davlatlarda:

[2] https://daryo.uz/2021/09/17/shavkat-mirziyoyev-shht-majlisida-kibermakondagi-tahdidlarga-qarshi-axborot-xavfsizligi-sohasidagi-ekspertlar-forumini-tasis-etishni-ilgari-surdi/

Kiberxavfsizlik markazlari (CERT/CSIRT) faoliyat yuritadi;

Ichki ishlar va maxsus xizmatlar tarkibida kiberjinoyatlar bo‘limlari mavjud;

Korxonalarda axborot xavfsizligi siyosati (ISMS) joriy etiladi.

Xalqaro miqyosda esa Interpol orqali transchegaraviy kiberjinoyatlar bo‘yicha hamkorlik amalga oshiriladi.

4. Profilaktika va ta’lim

Kiber jinoyatlarning oldini olishda aholining kiber savodxonligini oshirish muhim ahamiyatga ega. Buning uchun:

Aholi o‘rtasida tushuntirish ishlari olib boriladi;

Ta’lim muassasalarida kiberxavfsizlik fanlari o‘qitiladi;

Phishing va internet firibgarligi haqida ogohlantirish kampaniyalari o‘tkaziladi.

5. Xalqaro hamkorlik

Kiber jinoyatlar ko‘pincha bir nechta davlat hududida amalga oshiriladi. Shu bois xalqaro hamkorlik muhimdir. Davlatlar o‘rtasida:

Ma’lumot almashish;

Qo‘shma tergovlar o‘tkazish;

Global tahdidlar bo‘yicha tezkor ogohlantirish tizimlari joriy etiladi.

Xalqaro hamkorlik kiber jinoyatchilar uchun xavfsiz hudud qolmasligini ta’minlashga yordam beradi.

O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi “Raqamli mahsulotlar (xizmatlar) iste’molchilari huquqlarini himoya qilish va raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashishni kuchaytirish choralari to‘g‘risida” PQ-381-son qaroriga asosan, soha mutaxassislari kiberjinoyatchilikka qarshi kurashishda o‘z malakalarini oshirib borishi yo‘lga qo‘yildi. O‘zbekiston Respublikasi Ichki ishlar vazirligida kiberxavfsizlikni ta’minlash[3]

Xulosa qilib aytganda Kiberjinoyatlar zamonaviy dunyoning eng muhim muammolaridan biri bo‘lib, ulardan himoyalanish har bir inson va tashkilot uchun dolzarb vazifadir. Kuchli parollar ishlatish, ikki bosqichli autentifikatsiya, antivirus dasturlaridan foydalanish,shaxsiy ma’lumotlarni va sms tasdiqlash kodlarni hech kimga bermaslik, past foizli kredit yoki tez boyib ketish reklamalariga ishonmaslik kabi choralarga rioya qilish orqali xavfsizlikni ta’minlash lozim . Kiberjinoyatlarga qarshi kurash faqat texnologik himoya bilan cheklanmay, balki foydalanuvchilarning ongli va ehtiyotkor bo‘lishini ham talab etadi.

Texnologik rivojlanish bilan birga, kiberjinoyatlar ham takomillashmoqda, shuning uchun himoya choralari doimiy ravishda yangilanib borishi lozim.

Bundan tashqari, kiberxavfsizlik sohasi bo‘yicha bilimlarni oshirish, foydalanuvchilarning xabardorligini kuchaytirish va maxsus treninglar o‘tkazish kiberjinoyatlarga qarshi samarali kurashishning muhim omillaridan biridir.

[3] https://ipkmvd.uz/media/pdf/kitoblar/IIV_MOI_2024_yil_5_dekabr_konferensiya_materiallari_toplami_y2qYbSe.pdf

Har bir inson internetdan foydalanganda ehtiyotkorlik bilan harakat qilishi, shubhali havolalardan saqlanishi va shaxsiy ma’lumotlarini himoya qilishi zarur.

Kelajakda texnologik taraqqiyot bilan birga kiberjinoyatlar ham yanada rivojlanishi mumkin, shuning uchun har bir inson va tashkilot o‘z xavfsizligini ta’minlashga doimiy ravishda e’tibor qaratishi lozim.

Kiberjinoyatlar bilan samarali kurashish uchun ham texnologik, ham huquqiy jihatdan harakat qilish zarur bo‘lib, har bir foydalanuvchi o‘zining axborot xavfsizligiga mas’uliyat bilan yondashishi lozim.