

KIBERFIRIBGARLIK: ZAMONAVIY JAMIYAT MUAMMOSI

Daminov Muxtor

<https://doi.org/10.5281/zenodo.21017361>

Annotatsiya. Ushbu maqolada kiberfiribgarlikning mohiyati, uning paydo bo'lish sabablari, asosiy ko'rinishlari, jamiyat va iqtisodiyotga salbiy ta'siri, shuningdek, unga qarshi kurashishning huquqiy mexanizmlari tahlil qilinadi. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberjinoyatlar soni ortib borayotganligi, ayniqsa, internet tarmog'i, ijtimoiy tarmoqlar va elektron to'lov tizimlari orqali sodir etilayotgan firibgarliklar zamonaviy jamiyat uchun jiddiy xavf tug'dirayotgani yoritiladi. Shuningdek, O'zbekiston Respublikasida kiberxavfsizlikni ta'minlash va fuqarolarni kiberfiribgarlikdan himoya qilishga qaratilgan normativ-huquqiy hujjatlar hamda xalqaro tajribalar o'rganiladi.

Kalit so'zlar: kiberfiribgarlik, kiberjinoyat, axborot xavfsizligi, internet, elektron to'lovlar, kiberxavfsizlik, huquqiy javobgarlik, raqamli texnologiyalar.

XXI asr axborot texnologiyalari asri sifatida e'tirof etilmoqda. Bugungi kunda davlat boshqaruvi, iqtisodiyot, ta'lim, sog'liqni saqlash va kundalik hayotning deyarli barcha sohalari raqamlashtirilmoqda. Internet tarmog'ining kengayishi va elektron xizmatlarning ommalashuvi insonlar hayotini yengillashtirgan bo'lsa-da, yangi turdagi xavf va tahdidlarni ham yuzaga keltirdi.

Ana shunday tahdidlardan biri kiberfiribgarlikdir. Kiberfiribgarlik zamonaviy axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyat bo'lib, uning oldini olish va unga qarshi kurashishda jinoyat-huquqiy mexanizmlar muhim ahamiyatga ega. O'zbekiston Respublikasi Jinoyat kodeksida axborot texnologiyalari va kompyuter tizimlari bilan bog'liq huquqbuzarliklar uchun javobgarlik nazarda tutilgan. Avvalo, Jinoyat kodeksining 168-moddasi (Firibgarlik) kiberfiribgarlik bilan bog'liq holatlarga ham tatbiq etilishi mumkin.

Ushbu modda bo'yicha aldash yoki ishonchni suiiste'mol qilish yo'li bilan o'zganing mulkini yoki mulkiy huquqini qo'lga kiritish jinoyat hisoblanadi. Internet, ijtimoiy tarmoqlar yoki elektron to'lov tizimlari orqali fuqarolarni aldab pul mablag'larini qo'lga kiritish mazkur modda doirasida kvalifikatsiya qilinadi. Shuningdek, Jinoyat kodeksining 278¹-moddasi kompyuter axborotidan qonunga xilof ravishda foydalanish bilan bog'liq javobgarlikni belgilaydi. Ushbu norma kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni o'zgartirish yoki ulardan noqonuniy foydalanish holatlariga nisbatan qo'llaniladi.

Shu bilan bir qatorda, 278²-modda kompyuter axborotini modifikatsiyalashtirish, ya'ni axborotni noqonuniy ravishda o'zgartirish, yo'q qilish yoki bloklash bilan bog'liq qilmishlar uchun javobgarlikni nazarda tutadi. 278³-modda esa axborot tizimlarining ishlashiga qasddan zarar yetkazish bilan bog'liq harakatlarni jinoyat deb e'tirof etadi. Mazkur norma serverlar, axborot bazalari va elektron tizimlarga hujum qilish holatlariga nisbatan qo'llanilishi mumkin. 278⁴-modda maxsus dasturiy vositalarni tayyorlash, tarqatish yoki ulardan foydalanish orqali kompyuter tizimlariga noqonuniy ta'sir ko'rsatish bilan bog'liq harakatlar uchun javobgarlikni belgilaydi.

Bundan tashqari, kiberfiribgarlik natijasida shaxsga doir ma'lumotlarning noqonuniy tarqatilishi yoki foydalanilishi holatlarida boshqa tegishli moddalar ham qo'llanishi mumkin.

Masalan, shaxsiy hayot daxlsizligini buzish, tijorat siri yoki bank sirini oshkor qilish bilan bog'liq qilmishlar ham alohida javobgarlikka sabab bo'ladi.

Kiberjinoyatlarning transmilliy xarakterga ega ekanligi ularni tergov qilish va jinoyatchilarni javobgarlikka tortishda xalqaro hamkorlikni talab qiladi. Shu sababli O'zbekiston xalqaro kiberxavfsizlik standartlari va xorijiy davlatlar tajribasidan foydalanib, milliy qonunchilikni takomillashtirib bormoqda.

Shunday qilib, O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi hamda axborot texnologiyalari sohasidagi jinoyatlar uchun javobgarlikni nazarda tutuvchi 278¹–278⁴-moddalari kiberfiribgarlikka qarshi kurashishning muhim huquqiy asoslarini tashkil etadi. b Kiberfiribgarlik axborot texnologiyalaridan foydalanish orqali fuqarolar, tashkilotlar yoki davlatlarga moddiy yoki ma'naviy zarar yetkazishga qaratilgan noqonuniy harakatlar majmuasidir. Ushbu turdagi jinoyatlar nafaqat iqtisodiy zarar keltiradi, balki fuqarolarning axborot xavfsizligiga bo'lgan ishonchini ham susaytiradi.

So'nggi yillarda dunyo bo'yicha kiberjinoyatlar sonining keskin ortishi hukumatlar va xalqaro tashkilotlarni ushbu muammoga jiddiy e'tibor qaratishga majbur qilmoqda. Ayniqsa, bank kartalari, elektron hamyonlar, mobil ilovalar va ijtimoiy tarmoqlar orqali amalga oshirilayotgan firibgarlik holatlari keng tarqalmoqda.

Kiberfiribgarlik tushunchasi va uning mohiyati

Kiberfiribgarlik — kompyuter texnologiyalari, internet tarmoqlari va elektron aloqa vositalaridan foydalangan holda mulkiy manfaat orttirish maqsadida sodir etiladigan noqonuniy harakatdir.

An'anaviy firibgarlikdan farqli ravishda kiberfiribgarlikda jinoyatchi va jabrlanuvchi biri-biri bilan bevosita uchrashmaydi. Jinoyat masofadan turib internet orqali amalga oshiriladi. Shu sababli jinoyatchini aniqlash va javobgarlikka tortish ancha murakkab hisoblanadi.

Kiberfiribgarlikning asosiy xususiyatlari:

anonimlik; transmilliy xarakter; yuqori darajadagi yashirinlik; katta miqdordagi zarar yetkazish imkoniyati; jinoyatni sodir etish xarajatlarining nisbatan kamligi; jinoyatchini aniqlashdagi murakkablik.

Kiberfiribgarlikning asosiy turlari

1. Fishing (Phishing)

Fishing eng keng tarqalgan kiberfiribgarlik usullaridan biri hisoblanadi. Bunda firibgarlar bank, davlat organi yoki mashhur kompaniya nomidan soxta xabarlar yuborib, foydalanuvchilarning shaxsiy ma'lumotlarini qo'lga kiritadi. Masalan: bank karta raqami; PIN-kod;

SMS tasdiqlash kodi;

login va parollar.

2. Vishing

Vishing telefon qo'ng'iroqlari orqali amalga oshiriladigan firibgarlikdir. Firibgar o'zini bank xodimi yoki huquqni muhofaza qiluvchi organ vakili sifatida tanishtirib, fuqarodan maxfiy ma'lumotlarni olishga harakat qiladi.

3. Smishing

SMS xabarlarini orqali amalga oshiriladigan firibgarlik usuli bo'lib, foydalanuvchini zararli havolalarga kirishga undaydi.

4. Internet-do'kon firibgarligi

Soxta internet-do'konlar tashkil etilib, xaridorlardan oldindan to'lov olinadi, biroq mahsulot yetkazib berilmaydi.

5. Ijtimoiy tarmoqlardagi firibgarlik
[6/20/2026 2:05 PM] Mashhura: Telegram, Instagram, Facebook va boshqa platformalarda: soxta lotereyalar; investitsiya takliflari; kredit va grant va'dalari; xayriya yig'img'larini ko'rishidagi firibgarliklar keng uchraydi.

6. Karta ma'lumotlarini o'g'irlash

Firibgarlar maxsus dasturlar yoki soxta saytlar orqali bank kartalariga oid ma'lumotlarni qo'lga kiritib, mablag'larni noqonuniy ravishda yechib oladi.

7. Kriptovalyuta bilan bog'liq firibgarlik

Raqamli aktivlar bozorining rivojlanishi bilan soxta investitsiya loyihalari va piramida sxemalari ham ko'paymoqda.

Kiberfiribgarlikning yuzaga kelish sabablari: kiberfiribgarlikning keng tarqalishiga quyidagi omillar sabab bo'lmoqda:

Texnologik omillar: internet foydalanuvchilari sonining ortishi; mobil ilovalarning ko'payishi; elektron to'lov tizimlarining rivojlanishi. Ijtimoiy omillar: aholining huquqiy savodxonligi yetarli emasligi; axborot xavfsizligi madaniyatining pastligi; tez boyib ketishga intilish. Huquqiy omillar: ayrim davlatlarda qonunchilikning yetarli darajada rivojlanmaganligi; transchegaraviy jinoyatlarni tergov qilishdagi qiyinchiliklar.

Kiberfiribgarlikning jamiyatga ta'siri

Kiberfiribgarlikning salbiy oqibatlari quyidagilarda namoyon bo'ladi:

Iqtisodiy zarar: Har yili dunyo bo'yicha milliardlab dollar mablag' kiberjinoyatlar oqibatida yo'qotiladi. Fuqarolarning ishonchi pasayishi; Elektron tijorat va raqamli xizmatlarga bo'lgan ishonch kamayadi.

Davlat xavfsizligiga tahdid: Kiberjinoyatchilar davlat axborot tizimlariga ham zarar yetkazishi mumkin.

Shaxsiy ma'lumotlarning tarqalishi: Fuqarolarning shaxsiy ma'lumotlari noqonuniy ravishda uchinchi shaxslarga sotilishi mumkin.

O'zbekiston Respublikasida kiberfiribgarlikka qarshi kurashishning huquqiy asoslari: O'zbekistonda kiberxavfsizlik va kiberjinoyatlarga qarshi kurashish bo'yicha qator normativ-huquqiy hujjatlar qabul qilingan.

Jumladan: O'zbekiston Respublikasi Konstitutsiyasi; Jinoyat kodeksi; "Kiberxavfsizlik to'g'risida"gi Qonun; "Axborotlashtirish to'g'risida"gi Qonun;

"Shaxsga doir ma'lumotlar to'g'risida"gi Qonun; "Elektron hukumat to'g'risida"gi Qonun.

Mazkur hujjatlar axborot xavfsizligini ta'minlash, shaxsiy ma'lumotlarni himoya qilish hamda kiberjinoyatlar uchun javobgarlik choralari belgilaydi. O'zbekiston Respublikasi Jinoyat kodeksida kompyuter axborotiga noqonuniy kirish, axborotni o'zgartirish, yo'q qilish, bloklash va undan noqonuniy foydalanish uchun javobgarlik nazarda tutilgan.

Xalqaro tajriba:

Kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlik muhim ahamiyatga ega.

Quyidagi xalqaro hujjatlar alohida o'rin tutadi: Budapesht Konvensiyasi;, BMTning kiberjinoyatlarga qarshi tashabbuslari;, INTERPOL faoliyati;, Yevropa Ittifoqining kiberxavfsizlik strategiyalari.

Rivojlangan davlatlar sun'iy intellekt va zamonaviy monitoring tizimlari orqali kiberjinoyatlarni aniqlash samaradorligini oshirmoqda. Bundan tashqari, O'zbekiston kiberfiribgarlikning oldini olish choralari ham ko'rishmoqda.

Kiberfiribgarlikni kamaytirish uchun quyidagi choralar muhim hisoblanadi: Aholining raqamli savodxonligini oshirish, kuchli parollardan foydalanish, ikki bosqichli autentifikatsiyani joriy etish, shubhali havolalarga kirmaslik, bank ma'lumotlarini begona shaxslarga bermaslik, antivirus dasturlaridan foydalanish, davlat va xususiy sektor hamkorligini kuchaytirish va kiberxavfsizlik bo'yicha muntazam targ'ibot olib borish.

Xulosa

Kiberfiribgarlik zamonaviy jamiyatning eng dolzarb muammolaridan biri hisoblanadi.

Raqamli texnologiyalar rivojlanishi bilan ushbu jinoyat turi ham takomillashib bormoqda.

Kiberfiribgarlik fuqarolar, biznes subyektlari va davlat organlariga katta iqtisodiy hamda ma'naviy zarar yetkazadi. Shu sababli unga qarshi kurashishda huquqiy mexanizmlarni takomillashtirish, xalqaro hamkorlikni kengaytirish, zamonaviy texnologiyalarni joriy etish va aholining axborot xavfsizligi madaniyatini oshirish zarur. Faqat kompleks yondashuv orqaligina kiberfiribgarlikning salbiy oqibatlarini kamaytirish va xavfsiz raqamli muhitni yaratish mumkin.

Foydalanilgan adabiyotlar.

1. O'zbekiston Respublikasi Konstitutsiyasi.
2. O'zbekiston Respublikasi Jinoyat kodeksi.
3. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni.
4. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni.
5. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni.
6. United Nations Office on Drugs and Crime (UNODC) materiallari.
7. INTERPOL Cybercrime Reports.
8. Cybersecurity and Cybercrime Research Journal.
9. Information Security and Digital Technologies ilmiy nashrlari.