INTERNET FIRIBGARLARI VA UNGA QARSHI HUQUQIY CHORALAR

Ilmirova Ruxshona Baxtiyar qizi
Tashkent International University
"Yurisprudensiya" yo'nalishi, 3-kurs talabasi
E-mail: *ilmirovar@gmail.com*

Annotatsiya: *Ushbu ishda zamonaviy texnologiyalar rivojlanishi natijasida yuzaga kelgan internet firibgarligi (kiberfiribgarlik) muammosi tahlil qilinadi. Maqolada kiberjinoyatchilikning o'ziga xos xususiyatlari, xususan, ijtimoiy muhandislik va axborot texnologiyalari orqali amalga oshiriladigan o'g'rilik turlari ko'rib chiqiladi. Tadqiqot davomida O'zbekiston Respublikasining milliy qonunchiligidagi (Jinoyat kodeksining tegishli moddalari) va xalqaro miqyosdagi huquqiy javobgarlik choralari o'rganiladi. Yakunda aholining kiber-savodxonligini oshirish va huquqiy mexanizmlarni takomillashtirish bo'yicha amaliy tavsiyalar beriladi.*

Kalit so'zlar: *Internet firibgarligi, kiberjinoyatchilik, kiberxavfsizlik, axborot texnologiyalari, raqamli iqtisodiyot, fishing, ijtimoiy muhandislik, shaxsiy ma'lumotlar, Jinoyat kodeksi, huquqiy javobgarlik.*

Аннотация: *В данной работе анализируется проблема интернет мошенничества (кибермошенничества), возникшая в результате развития современных технологий. В статье рассматриваются специфические особенности киберпреступлений, в частности, виды краж, совершаемые с использованием методов социальной инженерии и информационных технологий. В ходе исследования изучаются меры правовой ответственности в национальном законодательстве Республики Узбекистан (соответствующие статьи Уголовного кодекса) и на международном уровне. В заключение даются практические рекомендации по повышению киберграмотности населения и совершенствованию правовых механизмов.*

Ключевые слова: *Интернет-мошенничество, киберпреступность, кибербезопасность, информационные технологии, цифровая экономика, фишинг, социальная инженерия, персональные данные, Уголовный кодекс, юридическая ответственность.*

Abstract: *This work analyzes the problem of Internet fraud (cyber fraud) that has arisen as a result of the development of modern technologies. The article examines the specific features of cybercrime, in particular, types of theft committed through social engineering and information technologies. During the study, legal liability measures in the national legislation of the Republic of Uzbekistan (relevant articles of the Criminal Code) and at the international level are studied. Finally, practical recommendations are given to increase the cyber literacy of the population and improve legal mechanisms.*

Keywords: *Internet fraud, cybercrime, cybersecurity, information technology, digital economy, phishing, social engineering, personal data, Criminal Code, legal liability.*

Kirish

Internetdagi firibgarlik — Internet orqali insonlarga tegishli pul, qimmatbaho narsalar va meros kabi shaxsiy mulklarini o‘g‘irlash, o‘marish, talom-toroj qilish maqsadida tashkillashtiriluvchi kiberjinoy firibgarlik, aldov turlaridan biri. Internet firibgarligi yagona, o‘ziga xos jinoyat hisoblanmaydi, biroq kibermakonda sodir etiladigan bir qator noqonuniy harakatlarni o‘z ichiga oladi. Firibgarlikning ushbu turi o'g'irlik jinoyatidan farq qiladi. Chunki bu holatda jabrlanuvchi ongli ravishda firibgarga shaxsiy ma’lumoti, pul yoki mol-mulkidan foydalanish ixtiyorini topshiradi Zamonaviy globallashuv jarayonlari va raqamli iqtisodiyotning jadal rivojlanishi internetning jamiyat hayotidagi ahamiyatini yanada kuchaytirmoqda. Axborot texnologiyalaridagi innovatsion yechimlar, onlayn to‘lov tizimlari, elektron hukumat platformalari, masofaviy ta’lim va elektron tijoratning kengayishi insonlarning kundalik faoliyatini sezilarli darajada yengillashtirdi.

Xalqaro Kiberxavfsizlik Forumi ma’lumotlariga ko‘ra, 2023–2024 yillarda internet firibgarliklari tufayli yetkazilgan global zarar 8 trln. AQSh dollaridan oshgan bo‘lib, 2025 yilga kelib bu ko‘rsatkich 10 trln. dollarga yetishi prognoz qilinmoqda. Bu raqamlar ushbu muammoning dolzarbligini yanada chuqurlashtiradi.

Rivojlanayotgan mamlakatlar, xususan O‘zbekiston uchun ham internet firibgarligi jiddiy xavf tug‘diruvchi omillar qatoridan joy olmoqda. So‘nggi yillarda elektron tijorat hajmining keskin ortishi, aholining onlayn to‘lovlarga o‘tishi, bank kartalari sonining ko‘payishi va mobil ilovalarning keng qo‘llanilishi firibgarlar tomonidan turli manipulyatsion sxemalar ishlab chiqilishiga imkon bermoqda. Soxta internet-do‘konlar, o‘zini bank xodimi sifatida tanishtiruvchi shaxslar, investitsiya nomi ostida tuzilgan moliyaviy piramidalar, ijtimoiy tarmoqlarda soxta akkountlar orqali amalga oshiriladigan aldovlar, shuningdek, fishing, vishing va smishing texnikalari O‘zbekiston bozorida eng ko‘p uchrayotgan firibgarlik shakllaridir. Raqamli savodxonlik darajasining pastligi, axborot madaniyatining yetarlicha shakllanmaganligi hamda shaxsiy ma’lumotlarni himoya qilish borasidagi beparvolik firibgarlar faoliyatini yanada osonlashtirmoqda.

I. Huquqiy muammolar va qonunchilik tahlili

O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi (Firibgarlik) 3-qismi "b" bandida axborot tizimlaridan foydalanib sodir etilgan firibgarlik uchun javobgarlik belgilangan. Biroq, amaliyotda quyidagi muammolar mavjud:

- Transchegaraviylik: Jinoyatchi bir davlatda, jabrlanuvchi ikkinchi davlatda bo'lishi tergov jarayonini murakkablashtiradi.
- Anonimlik: VPN, proxy-serverlar va anonim brauzerlar jinoyatchilarning shaxsini aniqlashni qiyinlashtiradi.
- Raqamli dalillar: Elektron ma'lumotlarni protsessual tartibda mustahkamlash va sudga taqdim etishda yagona standartlarning yetishmasligi.

II. Kiberfiribgarlikning turlari va xususiyatlari

Kiberfiribgarlik bir necha asosiy turga bo‘linadi:

1. Bank kartalari va elektron hamyonlarni o‘g‘irlash–firibgarlar foydalanuvchilarning karta ma’lumotlarini noqonuniy ravishda egallab, pul

mablag‘larini o‘zlashtiradi.

2. Elektron tijorat orqali firibgarlik–onlayn do‘konlarda soxta mahsulotlar sotish yoki to‘lovni amalga oshirmasdan mol-mulkni egallash.

3. Shaxsiy ma’lumotlarni noqonuniy egallash–foydalanuvchilarning pasport, telefon, elektron pochta va boshqa ma’lumotlari firibgarlar qo‘liga tushadi.

4. Zararli dasturlar va xakerlik hujumlari–kompyuter yoki mobil qurilmalarga zararli dasturlar o‘rnatish, tizimga kirib, ma’lumotlarni o‘g‘irlash yoki bloklash.

Har bir tur o‘ziga xos xususiyatlarga ega bo‘lib, unga qarshi kurashish usullari ham farqlanadi. Kiberfiribgarlikning tezkorligi, anonimligi va hududsizligi uni an’anaviy jinoyatlardan murakkab qiladi.

Metodologiya

Ushbu maqolada sifatli va miqdoriy tadqiqot metodlari qo‘llanildi. Birinchidan, so‘nggi yillarda internet firibgarliklarining statistik ma’lumotlari tahlil qilindi (ENISA, 2022; CERT.uz, 2023). Ikkinchidan, o‘zbek foydalanuvchilarining onlayn xavfsizlik bo‘yicha xatti-harakatlari va tajribasi so‘rovnomalar orqali o‘rganildi. Uchinchidan, ilg‘or tadqiqotlar va xalqaro maqolalar asosida firibgarlikni aniqlash va oldini olish bo‘yicha amaliy tavsiyalar ishlab chiqildi.[1]

Tahlil va natijalar

Internet firibgarliklari zamonaviy raqamli makonda eng tez o‘sayotgan jinoyat turlaridan biri bo‘lib, uning ko‘lami yildan yilga kengayib bormoqda. So‘nggi yillarda olib borilgan xalqaro va mintaqaviy tadqiqot natijalari firibgarlikning faqat texnik omillar emas, balki ijtimoiy-psixologik omillar bilan ham chuqur bog‘liqligini namoyon etadi. 2024–2025 yillarga doir statistik ma’lumotlar internet firibgarliklarining global miqyosda keskin oshganini va uning iqtisodiyot, jamiyat hamda shaxsiy xavfsizlikka jiddiy zarar keltirayotganini ko‘rsatadi.

Jadval: Kiberjinoyatlarning huquqiy tahlili va himoya vositalari

Kiberjinoyat shakli va usuli	**Huquqiy kvalifikatsiya (O‘zR Jinoyat kodeksi)**	**Jabrlanuvchining himoyalanish algoritmi**	**Tahliliy manba va asoslar**
Fishing va Skimming **(Plastik kartadagi mablag‘larni masofadan o‘g‘irlash)**	**169-modda** (O‘g‘rilik) va **278-4-modda** (Kompyuter ma’lumotlarini modifikatsiya qilish)	Bank ilovasi orqali kartani bloklash, tranzaksiya chiqarilmasini olish va IIV Kiberxavfsizlik markaziga murojaat qilish.	O‘zR Markaziy banki hisobotlari va IIV Kiberjinoyatlarga qarshi kurashish bo‘linmasi ma’lumotlari.

Kiberfiribgarlik **(Onlayn savdo yoki soxta yutuqlar orqali aldash)**	**168-modda** (Firibgarlik, axborot texnologiyalaridan foydalangan holda)	Pul o‘tkazmasi chekini saqlash, yozishmalarni skrinshot qilish va firibgarning telefon raqamini IIVga taqdim etish.	O‘zR Oliy sudi Plenumi qarorlari va huquqni muhofaza qiluvchi organlarning statistik to‘plamlari.
Raqamli tovlamachilik **(Shaxsiy ma’lumotlarni tarqatish bilan qo‘rqitish)**	**165-modda** (Tovlamachilik) va **141-1-modda** (Shaxsiy hayot daxlsizligini buzish)	Jinoyatchi bilan muloqotni to‘xtatish, dalillarni elektron shaklda muhrlash va kiber-patrul xizmatiga xabar berish.	Xalqaro "INTERPOL" kiberjinoyatchilikka qarshi kurash metodikasi va milliy qonunchilik bazasi.
Xakerlik hujumlari **(Profillarni buzib kirish va ma’lumotlarni o‘chirish)**	**278-1-modda** (Kompyuter axborotidan qonunga xilof ravishda foydalanish)	Ikki bosqichli autentifikatsiyani yoqish, texnik ko‘rikdan o‘tkazish va axborot tizimiga noqonuniy kirish fakti bo‘yicha da’vo qo‘zg‘atish.	"Kiberxavfsizlik markazi" DUK yillik monitoring natijalari va tizimli tahlillar.

Yuqorida keltirilgan tizimli ma’lumotlar kiberjinoyatchilikning nafaqat texnik nosozlik, balki murakkab ijtimoiy-huquqiy fenomen ekanligini yaqqol namoyon etadi. Tahlillar shuni ko‘rsatadiki, zamonaviy kiberhujumlarning muvaffaqiyati ko‘p hollarda texnologiyalarning zaifligidan emas, balki inson psixologiyasi va huquqiy hushyorlikning sustligidan oziqlanadi.[2]

Tahliliy kuzatuvlar shuni tasdiqlaydiki, kibermakondagi xavfsizlik strategiyasi faqatgina texnik cheklovlardan iborat bo‘lmay, unda huquqiy ong va raqamli madaniyat uyg‘unligi talab etiladi. [2]

Xulosa

Internet firibgarligiga qarshi kurashish nafaqat huquqiy normalarni kuchaytirishni, balki aholining raqamli immunitetini oshirishni ham talab etadi, bu esa "ko‘rinmas urush"da eng samarali mudofaa hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. “Internet firibgarliklari va ularga qarshi kurash usullari” Ashurov Kamron Samarqand Iqtisodiyot va Servis Instituti [319 – bet]

2. “Strategic Directions of Science Development and International Best Practices” International scientific online conference (Kiberjinoyat qurboni bo‘lmang: internetdagi

haq-huquqlaringizni qanday himoya qilish kerak) Abdualimov Olimjon Xolmamatovich [297-bet]

3. O‘zbekistonda kiberfiribgarlikning zamonaviy shakllari va ularga qarshi kurashish usullari: huquqiy munosabat va yechimlar tahlili https://worldlyjournals.com/index.php/Yangiizlanuvchi/article/view/11839

4. Fanlararo tafakkur respublika ilmiy-amaliy konferensiyasi1-Jild. 1-Son.Avgust.2025-yil/[8-bet] https://www.globalscholars.uz/index.php/ft/article/view/75/62

5. O‘zbekiston Respublikasi Jinoyat kodeksi, Toshkent, 2021