

KIBERJINOYATCHILIK VA UNGA QARSHI KURASH TIZIMI

To‘lanboyev Islombek Ilhomjon o‘g‘li

Farg‘ona yuridik texnikumi

“Sud-huquqiy faoliyat” yo‘nalishi 2-bosqich 43-24-guruh o‘quvchisi.

Odilova Bahora Muzaffarjon qizi

Farg‘ona yuridik texnikumi

“Sud-huquqiy faoliyat” yo‘nalishi 2-bosqich 43-24-guruh o‘quvchisi.

<https://doi.org/10.5281/zenodo.17592387>

Annotatsiya. Ushbu maqola O‘zbekistonda hackerlik, onlayn firibgarlik, kartalarni “urish”, Telegram orqali aldash va shaxsni o‘g‘irlash kabi jinoyatlarning qonuniy javobgarligi va tergov amaliyotini yoritadi. Muqaddimada kiberjinoyatlarning keng tarqalishi va jamiyatga ta’siri haqida so‘z yuritiladi.

Maqola, shuningdek, O‘zbekiston Respublikasining Jinoyat Kodeksida belgilangan jazolarni, tergov jarayonlarini va ushbu jinoyatlarga qarshi kurashish usullarini ko‘rib chiqadi. Kiberxavfsizlikning ahamiyati va shaxsiy ma’lumotlarni himoya qilish masalalari ham muhokama qilinadi. Umuman olganda, insho kiberjinoyatlarga qarshi kompleks yondoshuv zarurligini ta’kidlaydi va qonuniy chora-tadbirlarni kuchaytirish zaruriyatini ko‘rsatadi.

Kalit so‘zlar: Hackerlik, onlayn firibgarlik, kartalarni “urish”, telegram orqali aldash, shaxsni o‘g‘irlash, qonuniy javobgarlik.

Аннотация. В данной статье рассматриваются вопросы уголовной ответственности и следственной практики в Узбекистане за такие преступления, как хакерство, онлайн-мошенничество, взлом банковских карт, обман через Telegram и кража личности. Во введении описывается широкое распространение киберпреступлений и их влияние на общество.

Статья также анализирует наказания, предусмотренные Уголовным кодексом Республики Узбекистан, особенности расследования и методы борьбы с указанными преступлениями. Обсуждаются вопросы кибербезопасности и защиты личных данных. В целом, работа подчёркивает необходимость комплексного подхода к борьбе с киберпреступностью и усиления правовых мер.

Ключевые слова: хакерство, онлайн-мошенничество, взлом карт, обман через Telegram, кража личности, уголовная ответственность.

Annotation. This article examines the legal liability and investigative practices in Uzbekistan regarding crimes such as hacking, online fraud, card skimming, deception via Telegram, and identity theft. The introduction discusses the widespread nature of cybercrimes and their impact on society.

The article also analyzes the penalties stipulated in the Criminal Code of the Republic of Uzbekistan, the investigation procedures, and the methods of combating these offenses. Issues of cybersecurity and personal data protection are also discussed. Overall, the paper emphasizes the need for a comprehensive approach to combating cybercrime and strengthening legal measures.

Keywords: hacking, online fraud, card skimming, Telegram deception, identity theft, legal liability.

KIRISH

Hozirgi kunda internet va raqamli texnologiyalarning rivojlanishi bilan birga, onlayn firibgarlik, hakkerlik va shaxsiy ma'lumotlarni o'g'irlash kabi jinoyatlarning ko'payishi kuzatilmoqda. Ushbu maqolada, hakkerlik va onlayn firibgarlikning turli turlari, ularning qonuniy jihatlari, tergov amaliyoti va bunday jinoyatlarga qarshi kurashish usullari haqida so'z yuritamiz.

Asosiy qism: Hakkerlik, asosan, kompyuter tizimlariga ruxsatsiz kirish va ma'lumotlarni o'g'irlash, o'zgartirish yoki yo'q qilish bilan bog'liq faoliyatdir. Hackerlar ikki turga bo'linadi: "oq" (yaxshi) va "qora" (yomon) hackerlar. Oq hackerlar tizimlarni himoya qilish, zaif joylarini aniqlash va ularni tuzatish uchun ishlaydi. Qora hackerlar esa, shaxsiy ma'lumotlarni o'g'irlash, firibgarlik qilish va boshqa jinoyatlarni amalga oshirish maqsadida tizimlarga kiradilar.

Onlayn firibgarlik, internet orqali amalga oshiriladigan har qanday firibgarlikdir. Bu firibgarlik turlari ko'p, jumladan:

1. Phishing: Foydalanuvchilarni soxta saytga olib borish orqali shaxsiy ma'lumotlarni o'g'irlash.
2. Kartalarni "urish": Kredit yoki debit kartalaridan noqonuniy foyda olish.
3. Telegram orqali aldash: Ijtimoiy tarmoqlarda yoki messengerlarda odamlarni aldab, pul yoki ma'lumotlarni o'g'irlash.

Hakkerlik va onlayn firibgarlik ko'plab mamlakatlarda jinoiy javobgarlikni keltirib chiqaradi. Qonunlar, odatda, bu turdagi jinoyatlarni qamrab oluvchi maxsus qoidalar va kodekslar orqali belgilangan.

O'zbekiston Respublikasining Jinoyat Kodeksida kompyuter jinoyatlari va onlayn firibgarliklarni jazolashga oid qoidalar mavjud. Masalan, 2021 yil 1 yanvardan kuchga kirgan yangi qonun bilan, internet orqali firibgarlik qilishga oid jinoyatlar uchun jazolar kuchaytirilgan.

1. Hakkerlik: Ruxsatsiz kirish va tizimlarni buzish uchun javobgarlik.
2. Onlayn Firibgarlik: Internet orqali pul yoki boshqa qiymatli narsalarni aldash.

Hakkerlik va firibgarlikning xalqaro jihatlari ham muhimdir. BMT va boshqa xalqaro tashkilotlar, elektron jinoyatlarga qarshi kurashish uchun turli konventsiyalar va protokollarni ishlab chiqqan. Masalan, 2001 yilda qabul qilingan "Zamonaviy Texnologiyalar orqali Jinoyatga Qarshi Konventsiya" (Budapest Convention) ko'plab mamlakatlar o'rtasida hamkorlikni kuchaytiradi.

Hakkerlik va onlayn firibgarliklarni tergov qilish murakkab jarayon. Tergovchilar ko'plab usullarni qo'llaydilar:

1. Raqqaslik: Jinoyat joyidagi dalillarni to'plash.
2. Kompyuter Tizimlarini Tahlil Qilish: Buzilgan yoki firibgarlik qilingan tizimlarni tahlil qilish.
3. Ma'lumotlarni olish: Shaxsiy ma'lumotlar va moliyaviy operatsiyalarni to'plash.

Tergovchilarga duch keladigan qiyinchiliklar orasida:

- Anonimlik: Hackerlar ko'pincha o'zlarini yashirish uchun turli usullarni qo'llaydilar.
- Yurisdiksiya: Turli mamlakatlar o'rtasidagi qonunlar farq qiladi, bu esa tergov jarayonini murakkablashtiradi.
- Texnologik Rivojlanish: Texnologiyaning tez o'zgarishi, yangi usullar va vositalarni talab qiladi.

Bunday jinoyatlarga qarshi kurashish uchun bir qator usullar mavjud:

1. Ta'lim va o'qitish: Foydalanuvchilarni onlayn xavfsizlik bo'yicha o'qitish.
2. Texnologik himoya: Antivirus dasturlari, firewalls va boshqa himoya vositalarini qo'llash.
3. Qonuniy chora-tadbirlar: Qonunlarni kuchaytirish va jinoyatchilarni jazolash.

Bugungi kunda, internet va raqamli texnologiyalarning rivojlanishi bilan birga, hackerlik kabi jinoyatlarning ko'payishi kuzatilmoqda. O'zbekiston ham bu tendentsiyadan chetda qolmayapti. Hackerlik nafaqat shaxsiy ma'lumotlarni o'g'irlash, balki moliyaviy firibgarliklar, tizimlarni buzish kabi turli jinoyatlarni o'z ichiga oladi. Ushbu insho orqali O'zbekistonda hackerlikning muammolari, uning oqibatlari va qonuniy jazolari haqida so'z yuritamiz.

Hackerlik — bu kompyuter tizimlariga ruxsatsiz kirish va ma'lumotlarni o'g'irlash yoki o'zgartirish bilan bog'liq faoliyatdir. O'zbekistonda hackerlik faoliyati, asosan, quyidagi turlarga bo'linadi:

1. Ruxsatsiz Kirish: Bu turdagi hackerlar ma'lumotlarni o'g'irlash yoki tizimlarga zarar yetkazish maqsadida ruxsatsiz kirishga urinishadi.

2. Onlayn Firibgarlik: Internet orqali odamlarni aldab, pul yoki shaxsiy ma'lumotlarni o'g'irlash.

Kompyuter yoki tarmoq tizimlarida buzilishlar yaratish.

O'zbekiston Respublikasining Jinoyat Kodeksida hackerlik va kompyuter jinoyatlari uchun jazolar aniq belgilangan. Ushbu qonunlar quyidagi jihatlarni o'z ichiga oladi:

- Ruxsatsiz Kirish: Boshqa shaxsning kompyuter tizimlariga ruxsatsiz kirganlik uchun jinoiy javobgarlik mavjud. Bu holatda, qamoq jazosiga olib kelishi mumkin.

- Ma'lumotlarni o'g'irlash: Shaxsiy yoki moliyaviy ma'lumotlarni o'g'irlash ham jinoiy javobgarlikni keltirib chiqaradi. Bunday jinoyatlar uchun qamoq jazosi belgilangan.

- Tizimlarni Buzish: Agar hackerlar tizimlarga zarar yetkazsa, bu ham jinoiy javobgarlikka olib keladi. Jazolar, odatda, qamoq muddati bilan ifodalanadi.

Hackerlik va kompyuter jinoyatlarini tergov qilish murakkab jarayon. Tergovchilar ko'plab usullarni qo'llashadi, jumladan, raqamli dalillarni to'plash, kompyuter tizimlarini tahlil qilish va jinoyatchilarni aniqlash. Biroq, hackerlar ko'pincha anonim bo'lishadi, bu esa ularni topishni qiyinlashtiradi.

Jazolarni amaliyotda qo'llashda esa, jinoyatning og'irligi, jinoyatchining avvalgi faoliyati va boshqa omillar hisobga olinadi. O'zbekistonda hackerlik uchun jazolarni kuchaytirish va qonunlarni yangilash zarurati har doim mavjud.

Xulosa

Hackerlik O'zbekistonda jiddiy muammo hisoblanadi. Shaxsiy ma'lumotlar, moliyaviy xavfsizlik va jamiyat barqarorligiga tahdid soladi. Bunday jinoyatlarga qarshi kurashish uchun qattiq qonunlar, samarali tergov usullari va jamiyatda onlayn xavfsizlik haqida ta'lim berish zarur.

Faqat kompleks yondoshuv orqali biz hackerlik kabi jinoyatlarga qarshi kurashishimiz mumkin. Hackerlik va onlayn firibgarlik zamonaviy jamiyatda jiddiy muammo hisoblanadi. Ular nafaqat shaxsiy ma'lumotlarga, balki moliyaviy xavfsizlikka ham tahdidlarga sabab bo'ladi.

Ushbu jinoyatlarga qarshi kurashish uchun qonuniy, texnologik va ta'limiy choralar zarur.

Faqat bunday kompleks yondoshuv orqali biz ushbu muammolarga qarshi samarali kurashishimiz mumkin.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasi Jinoyat Kodeksi. (2021). O'zbekiston Respublikasi Qonun hujjatlari.
2. Kiberxavfsizlik to'g'risida qonun. (2019). O'zbekiston Respublikasi Prezidentining qarori.
3. I.Karimov. Kiberjinoyatlar: Muammo va qarshi chora-tadbirlar. (2020). -T.: O'zbekiston Milliy Universiteti nashri.
4. A.Murodov. Onlayn firibgarlik va uning oqibatlari. "Xalqaro jurnal" (2022). 34(2), 45-56.
5. D.Rahmonov. Tizimlarni himoya qilish va kiberxavfsizlik. -T.: (2021). Informatika va axborot texnologiyalari instituti.
6. O'zbekiston Respublikasi Ichki ishlar vazirligi. (2023). Kiberjinoyatlarga qarshi kurashish bo'yicha hisobot.
7. O'zbekiston Respublikasining davlat statistikasi. (2022). Internet va kiberjinoyat statistikasi.