



KIBERJINOYATCHILIK TUSHUNCHASI VA UNING TURLARI

Quvvatova Kumush Mo'min qizi

Tashkent international university "Yurisprudensiya"

yo'nalishi 3-kurs talabasi

kumushquvvatova19@gmail.com

<https://doi.org/10.5281/zenodo.19016601>

Annotatsiya

Mazkur maqolada kiberjinoyatchilik tushunchasi, uning asosiy turlari hamda kriminologik xususiyatlari tahlil qilinadi. Shuningdek, kiberjinoyatlarning jamiyat uchun xavflilik darajasi, ularning iqtisodiy va ijtimoiy oqibatlari yoritib berilgan. Internet firibgarligi keng tarqalgan kiberjinoyat turi sifatida ko'rib chiqilib, unga qarshi kurashishning huquqiy mexanizmlari va profilaktik choralariga alohida e'tibor qaratilgan. Tadqiqot natijasida kiberjinoyatchilikka qarshi kurashishda huquqiy tartibga solish, texnik himoya vositalari va fuqarolarning axborot xavfsizligi bo'yicha bilimlarini oshirish muhim ahamiyatga ega ekanligi ta'kidlanadi.

Kalit so'zlar: kiberjinoyatchilik, internet firibgarligi, axborot xavfsizligi, kompyuter jinoyatlari, hacking, phishing, zararli dasturlar, kiberxavfsizlik, huquqiy choralar.

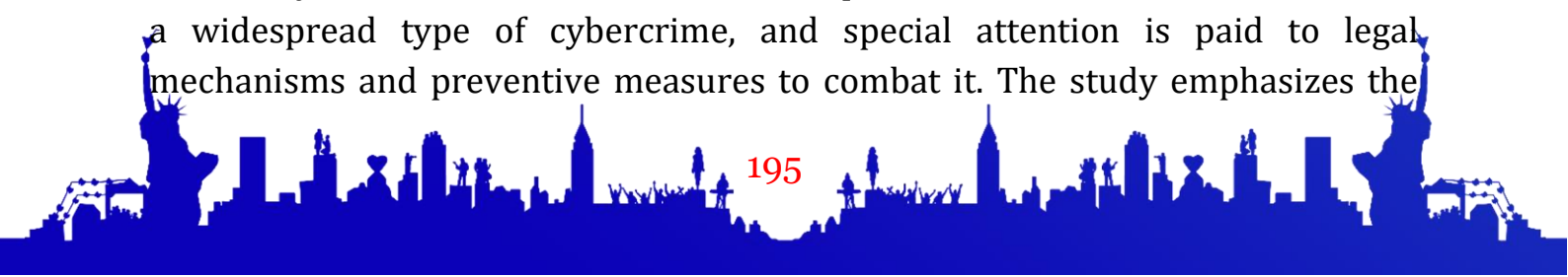
Аннотация

В данной статье анализируется концепция киберпреступности, ее основные виды и криминологические характеристики. Также освещается уровень опасности киберпреступлений для общества, их экономические и социальные последствия. Интернет-мошенничество рассматривается как широко распространенный вид киберпреступлений, и особое внимание уделяется правовым механизмам и превентивным мерам по борьбе с ним. В исследовании подчеркивается важность правового регулирования, средств технической защиты и повышения осведомленности граждан об информационной безопасности в борьбе с киберпреступностью.

Ключевые слова: киберпреступность, интернет-мошенничество, информационная безопасность, компьютерные преступления, взлом, фишинг, вредоносные программы, кибербезопасность, правовые меры.

Annotation

This article analyzes the concept of cybercrime, its main types and criminological characteristics. It also highlights the level of danger of cybercrimes for society, their economic and social consequences. Internet fraud is considered a widespread type of cybercrime, and special attention is paid to legal mechanisms and preventive measures to combat it. The study emphasizes the





importance of legal regulation, technical protection tools and increasing citizens' knowledge of information security in combating cybercrime.

Keywords: cybercrime, internet fraud, information security, computer crimes, hacking, phishing, malicious programs, cybersecurity, legal measures.

Axborot texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga katta ta'sir ko'rsatdi. Internet, elektron to'lov tizimlari, ijtimoiy tarmoqlar va turli onlayn xizmatlar insonlar uchun qulaylik yaratish bilan birga yangi turdagi jinoyatlarning paydo bo'lishiga ham sabab bo'ldi. Shunday jinoyatlardan biri – **kiberjinoyatchilik** bo'lib, u zamonaviy jamiyat uchun jiddiy xavf tug'diradi. Kiberjinoyatlar ko'pincha kompyuter tarmoqlari, internet va axborot tizimlari orqali sodir etiladi hamda davlat, tashkilot va fuqarolarga katta moddiy va ma'naviy zarar yetkazishi mumkin.

Asosiy qism:

I. Kiberjinoyatchilik tushunchasi va uning turlari

Kiberjinoyatchilik – bu kompyuter texnologiyalari, axborot tizimlari yoki internetdan foydalanib sodir etiladigan noqonuniy harakatlar majmui hisoblanadi. Bu turdagi jinoyatlarda kompyuter yoki tarmoq jinoyat quroli, nishoni yoki vositasi sifatida ishlatiladi.

Kiberjinoyatlarning asosiy turlari quyidagilardan iborat:

1. Kompyuter tizimlariga noqonuniy kirish (hacking)

Ruxsatsiz ravishda kompyuter yoki serverga kirib, ma'lumotlarni o'g'irlash yoki o'zgartirish.

2. Virus va zararli dasturlar tarqatish

Kompyuter tizimlarini ishdan chiqarish yoki ma'lumotlarni o'g'irlash maqsadida zararli dasturlar yuborish.

3. Ma'lumotlarni noqonuniy qo'lga kiritish

Bank kartalari ma'lumotlari, parollar, shaxsiy ma'lumotlarni o'g'irlash.

4. Internet firibgarligi

Soxta saytlar yoki yolg'on takliflar orqali odamlarni aldab pul olish.

5. Kiberterrorizm

Davlat yoki muhim infratuzilma tizimlariga hujum qilish orqali xavfsizlikka tahdid solish.

6. Onlayn shantaj va tahdidlar

Shaxsiy ma'lumotlarni oshkor qilish bilan qo'rqitib pul talab qilish.

II. Kiberjinoyatlarning kriminologik xususiyatlari

Kiberjinoyatlar an'anaviy jinoyatlardan bir qator kriminologik xususiyatlari bilan farqlanadi:





- Birinchidan, **anonimlik darajasi yuqori**. Internet orqali jinoyatchilar o'z shaxsini yashirishi mumkin.

- Ikkinchidan, **transmilliy xarakterga ega**. Jinoyatchi bir davlatda bo'lib, jinoyat boshqa davlatga qarshi sodir etilishi mumkin.

- Uchinchidan, **texnologik bilim talab etiladi**. Ko'p hollarda kiberjinoyatchilar yuqori darajadagi IT bilimiga ega bo'ladi.

- To'rtinchidan, **dalillarni aniqlash qiyin**. Elektron izlarni aniqlash va isbotlash murakkab bo'lishi mumkin.

- Beshinchidan, **tezkor tarqalish xususiyati mavjud**. Masalan, viruslar yoki zararli dasturlar qisqa vaqt ichida butun dunyo bo'ylab tarqalishi mumkin.

III. Kiberjinoyatlarning jamiyat uchun xavflilik darajasi

Kiberjinoyatchilik zamonaviy jamiyat uchun juda katta xavf tug'diradi. Uning xavfliligi bir necha omillar bilan belgilanadi.

- Birinchidan, **iqtisodiy zarar**. Bank tizimlari, kompaniyalar va fuqarolar katta moliyaviy yo'qotishlarga uchraydi.

- Ikkinchidan, **davlat xavfsizligiga tahdid**. Muhim davlat axborot tizimlariga hujumlar milliy xavfsizlikka zarar yetkazishi mumkin.

- Uchinchidan, **shaxsiy ma'lumotlarning oshkor bo'lishi**. Fuqarolarning shaxsiy hayoti va ma'lumotlari noqonuniy ravishda tarqalishi mumkin.

- To'rtinchidan, **jamiyatda ishonchning kamayishi**. Onlayn xizmatlarga bo'lgan ishonch pasayadi.

Bundan tashqari, kiberjinoyatlar ko'pincha boshqa jinoyatlar bilan ham bog'liq bo'ladi, masalan pul yuvish, noqonuniy savdo yoki terrorizmni moliyalashtirish.

IV. Internet firibgarligi va unga qarshi huquqiy choralar

Internet firibgarligi – bu internet orqali odamlarni aldash yo'li bilan pul yoki mulkni qo'lga kiritishdir.

Internet firibgarligining keng tarqalgan ko'rinishlari:

- Soxta internet do'konlari
- Phishing (soxta bank sahifalari orqali ma'lumot olish)
- Onlayn investitsiya firibgarligi
- Ijtimoiy tarmoqlarda pul so'rash
- Soxta lotereya yoki sovrinlar

Kiberfiribgarlikka qarshi kurashish uchun quyidagi **huquqiy choralar** qo'llaniladi:

1. Kiberjinoyatlar uchun jinoiy javobgarlikni kuchaytirish.
2. Axborot xavfsizligi bo'yicha milliy qonunchilikni takomillashtirish.





3. Maxsus kiberxavfsizlik organlarini tashkil etish.
4. Internet foydalanuvchilarini xabardor qilish va profilaktika ishlari olib borish.
5. Xalqaro hamkorlikni rivojlantirish.

Ko'pgina davlatlarda kiberjinoyatlarga qarshi kurashish uchun maxsus qonunlar qabul qilingan va maxsus kiberpolitsiya bo'linmalari faoliyat yuritmoqda.

Tahlil:

Kiberjinoyatchilik so'nggi yillarda dunyo miqyosida eng tez rivojlanayotgan jinoyat turlaridan biriga aylandi. Axborot texnologiyalarining keng qo'llanilishi bilan bir qatorda jinoyatchilar ham zamonaviy texnologiyalardan foydalanib yangi usullarni ishlab chiqmoqda. Ayniqsa, internet orqali amalga oshiriladigan firibgarlik, bank kartalari ma'lumotlarini o'g'irlash, phishing hujumlari va zararli dasturlar tarqatish holatlari keskin ortib bormoqda.

Tahlillar shuni ko'rsatadiki, kiberjinoyatlar ko'pincha aholining axborot xavfsizligi bo'yicha yetarli bilimga ega emasligi sababli sodir bo'ladi. Ko'plab foydalanuvchilar shaxsiy ma'lumotlarini himoya qilish, ishonchsiz havolalardan foydalanmaslik yoki kuchli parollardan foydalanish kabi oddiy xavfsizlik qoidalariga rioya qilmaydi.

Bundan tashqari, kiberjinoyatchilikning transmilliy xususiyatga ega bo'lishi uni aniqlash va jazolashni murakkablashtiradi. Jinoyatchi boshqa davlat hududida joylashgan bo'lishi mumkinligi sababli, tergov jarayonida xalqaro hamkorlik muhim ahamiyat kasb etadi. Shu boisdan, kiberjinoyatlarga qarshi kurashishda nafaqat milliy, balki xalqaro darajadagi hamkorlikni rivojlantirish zarur.

Takliflar:

Kiberjinoyatchilikka qarshi samarali kurashish maqsadida quyidagi takliflarni ilgari surish mumkin:

1. **Axborot xavfsizligi bo'yicha aholining bilimini oshirish** – fuqarolar o'rtasida internetdan xavfsiz foydalanish bo'yicha targ'ibot va o'quv dasturlarini kengaytirish.
2. **Qonunchilikni takomillashtirish** – kiberjinoyatlar uchun javobgarlik choralari yanada kuchaytirish va zamonaviy tahdidlarga mos ravishda qonunlarni yangilash.
3. **Maxsus kiberxavfsizlik markazlarini rivojlantirish** – davlat organlari va tashkilotlarda axborot tizimlarini himoya qiluvchi mutaxassislarni tayyorlash va maxsus markazlar faoliyatini kengaytirish.





4. **Xalqaro hamkorlikni kuchaytirish** – kiberjinoyatlar transmilliy xususiyatga ega bo'lganligi sababli davlatlar o'rtasida tezkor ma'lumot almashinuvi va qo'shma tergov mexanizmlarini rivojlantirish.

5. **Texnik himoya vositalarini keng joriy etish** – tashkilotlarda zamonaviy antivirus tizimlari, ma'lumotlarni shifrlash va xavfsizlik monitoringi tizimlarini joriy qilish.

Xulosa:

Kiberjinoyatchilik zamonaviy axborot jamiyatining eng dolzarb muammolaridan biridir. Internet va raqamli texnologiyalar rivojlanishi bilan bu turdagi jinoyatlar ham murakkablashib bormoqda. Shu sababli davlat organlari, tashkilotlar va fuqarolar axborot xavfsizligini ta'minlashga alohida e'tibor qaratishi zarur. Kiberjinoyatlarga qarshi samarali kurashish uchun huquqiy, texnik va tashkiliy choralarni kompleks ravishda qo'llash muhim hisoblanadi. Kiberjinoyatchilikka qarshi kurashda va oldini olishda bitta davlatda qabul qilingan qonun va harakatlar orqali iijobiy natijaga erishi bulmaydi balki umummiliy xalqaro miqyosda xamkorlik, davlatlar aro ushbu sohaga tegishli yagona huquqiy tizimni ishlab chiqish, xalqaro standartlardan keng foydalanish va tergov jarayonlarida tatbiq etishdan iborat bo'ladi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi Jinoyat kodeksi. – Toshkent: Adolat, 2023.
2. O'zbekiston Respublikasi "Axborotlashtirish to'g'risida"gi Qonuni. – Toshkent, 2003.
3. O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risida"gi Qonuni. – Toshkent, 2022.
4. Abdumajidov G.A. Kriminologiya. – Toshkent: TDYU nashriyoti, 2020.
5. Interpol tashkiloti rasmiy sayti: <https://www.interpol.int>
6. Birlashgan Millatlar Tashkiloti Kiberjinoyatchilik bo'yicha materiallari: <https://www.unodc.org>

