

O'ZBEKISTONDA KIBERJINOYATLARNING JINOYAT-HUQUQIY TAVSIFI

Abbosov Shaxboz Ziyodbek o'g'li
Toshkent davlat yuridik universiteti
Ommaviy huquq fakulteti 2-kurs talabasi

Annotatsiya

Mazkur maqolada O'zbekiston Respublikasida kiberjinoyslarning jinoysl-huquqiy tavsifi ilmiy-nazariy va amaliy jihatdan tahlil qilingan. Tadqiqot davomida kiberjinoysl tushunchasi, uning asosiy xususiyatlari, tarkibiy elementlari (obyekt, obyektiv tomon, subyekt va subyektiv tomon) kompleks ravishda o'rganildi. Shuningdek, amaldagi jinoysl qonunchiligi hamda axborot xavfsizligi sohasidagi normativ-huquqiy hujjatlar tahlil qilinib, mavjud muammolar va ularni hal etish yo'llari yoritildi. Tadqiqot natijalari kiberjinoyslarning zamonaviy jamiyat uchun jiddiy tahdid ekanligini ko'rsatadi hamda ularni oldini olish va ularga qarshi kurashishning kompleks mexanizmlarini takomillashtirish zarurligini asoslaydi.

Kalit so'zlar: kiberjinoysl, axborot xavfsizligi, jinoysl-huquqiy tavsif, kompyuter jinoyslari, kiberxavfsizlik, phishing, axborot tizimlari, raqamli jinoysl.

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ В УЗБЕКИСТАНЕ

Аббосов Шахбоз Зиёдбек углы
Ташкентский государственный юридический
университет, факультет публичного права, студент 2 курса

Аннотация

В данной статье проведён научно-теоретический и практический анализ уголовно-правовой характеристики киберпреступлений в Республике Узбекистан. В ходе исследования рассмотрены понятие киберпреступлений, их основные признаки и элементы состава преступления (объект, объективная сторона, субъект и субъективная сторона). Также проанализированы действующее уголовное законодательство и нормативно-правовые акты в сфере информационной безопасности, выявлены существующие проблемы и предложены пути их решения. Результаты исследования свидетельствуют о том, что киберпреступления представляют серьёзную угрозу для современного общества и требуют совершенствования комплексных механизмов противодействия.

Ключевые слова: киберпреступность, информационная безопасность, уголовно-правовая характеристика, компьютерные преступления, кибербезопасность, фишинг, информационные системы, цифровые преступления.

CRIMINAL LAW CHARACTERISTICS OF CYBERCRIME IN UZBEKISTAN

*Abbosov Shakhboz Ziyodbek ogli,
Tashkent State University of Law, Faculty
of Public Law, 2nd-year student*

Abstract

This article provides a scientific and practical analysis of the criminal law characteristics of cybercrime in the Republic of Uzbekistan. The study examines the concept of cybercrime, its key features, and the elements of the corpus delicti (object, objective side, subject, and subjective side). It also analyzes the current criminal legislation and regulatory framework in the field of information security, identifying existing challenges and proposing possible solutions. The findings demonstrate that cybercrime poses a significant threat to modern society and highlight the necessity of improving comprehensive mechanisms for its prevention and counteraction.

Keywords: cybercrime, information security, criminal law characteristics, computer crimes, cybersecurity, phishing, information systems, digital crimes.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi zamonaviy jamiyatda ijtimoiy, iqtisodiy va huquqiy munosabatlarning tubdan o'zgarishiga olib kelmoqda. Raqamlashtirish jarayonlari davlat boshqaruvi, bank-moliya tizimi, ta'lim va boshqa ko'plab sohalarda samaradorlikni oshirgan bo'lsa-da, ular bilan bog'liq yangi xavf-xatarlar, xususan, kiberjinoyatlarning kengayishiga ham sabab bo'lmoqda. Ilmiy manbalarda qayd etilishicha, kiberjinoyatlar "axborot makonida sodir etiladigan va kompyuter tizimlari orqali amalga oshiriladigan ijtimoiy xavfli qilmishlar majmui" sifatida talqin etiladi¹.

Kiberjinoyatlar o'zining transchegaraviyligi, anonimligi va yuqori texnologik murakkabligi bilan an'anaviy jinoyatlardan farq qiladi. Ularning sodir etilishi uchun jismoniy mavjudlik talab etilmasligi, balki virtual muhit yetarli bo'lishi jinoyatni aniqlash va isbotlash jarayonini sezilarli darajada qiyinlashtiradi. Shu bois, mazkur jinoyatlarning jinoyat-huquqiy tavsifini aniqlash, ularni kvalifikatsiya qilish va ularga

qarshi samarali kurashish mexanizmlarini ishlab chiqish dolzarb ilmiy muammo hisoblanadi.

O'zbekiston Respublikasida ham kiberxavfsizlikni ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biri sifatida shakllanmoqda. So'nggi yillarda axborot xavfsizligini mustahkamlash, kiberjinoyatlarga qarshi kurashish va raqamli infratuzilmani himoya qilish bo'yicha qator normativ-huquqiy hujjatlar qabul qilindi. Shunga qaramay, mazkur sohada hali ham nazariy va amaliy muammolar mavjud.

Mazkur tadqiqotning maqsadi O'zbekistonda kiberjinoyatlarning jinoyat-huquqiy tavsifini kompleks tahlil qilish, ularning tarkibiy elementlarini aniqlash hamda amaldagi qonunchilik va amaliyotdagi muammolarni ochib berishdan iborat.

Kiberjinoyat O'zbekistonda eng jiddiy tahdidlardan biri bolib qolmogda — ro'yxatga olingan jinoyatlarning 42 foizi unga to'g'ri keladi. Prezidentimiz ushbu turdagi jinoyatlarga qarshi kurashishni va infratuzilmant rivolantirishni chora-tadbirlarini ishlab chiqishni topshird.

2025-y. 9-iyul. O'zbekiston Respublikasi prizidenti Sh.M.Mirziyoyev Bugungi kunda raqamli texnologiyalar jadal sur'atlarda rivojlanib, hayotimizning deyarli barcha jabhalariga kirib kelmogda. Yangi turdagi innovatsion texnologiyalar yaratilishi natijasida inson aralashuvisiz bajariladigan ishlar soni ortib, mehnat jarayonlari avtomatlashtirilmoqda. Shu bois, raqamli transformatsiya nafagat ishlab chigarish, balki ta'lim, tibbiyot, moliya va kundalik turmush tarzimizni ham tubdan o'zgartirmogda. Barcha sohalarda buni samarali va foydali taraflar juda ko'p bolishiga qaramasdan salbiy oqibatlar ham yo'q emas. Bu masalani ham imkon qaqdar bartaraf etilishga qadam va qadam erishilmogda. Ushbu muammolardan biriga to'xtaladigan bolsak, texnologiyalar orgali jinoat olamida fribgarlik shaklida sodir etilayotgan jinoyatlar soni oshib bormogda. Ushbu jinoyatlarni oldini olish va bartaraf etish harakatlari olib borilishiga garamasdan, jinoyatchilar ya'ni kiberjinoyatchilar, kiberfribgarlar ham boshqa usullarni, yangi usullarni o'ylab topishdan hech charchashmayotgani hammaizga ma'lum. So'ngi yillarda butun dunyoda raqamli texnologiyalar bilan, kompuyter texnologiyalari bilan sodir etilgan fribgarlik soni otib bormogda. Bu jarayonlar salkam 50 yil oldin boshlangan. Bu jarayon ragamli texnologiyalar rivolangani sari kiberfribgarlik ham baravar rivolanib bormogda. Ushbu jinoyatlar bugungi kunda O'zbekistonni ham chelab o'tmadi. Bizni yurtimizda ham raqamlashtirish siyosati ketayotgan bir paytda kiber tahdidlardan himoyalanishni ham zamon talab qilmoqda. Shuningdek, aynan kiberxvrsizlik statistikasiga garaydigan bolsak, ragamli texnologiyalar orgali 2025-yil oxirigacha dunyo 10.29trln dollar zarar ko'rishi pragnoz qilinmogda. O'zbekistonda esa o'tgan yilgi statistikaga qaraydigan bolsak, 2024-yil 58 800ta kiberjinoyat, bundan 97,7% bank tarmoglariga to'g'ri keladi. Ushbu masalani organishning ahamiyati shundaki zamonaviy raqamli muhitda yuzaga kelayotgan yangi turdagi jinoyatlarni chuqur tahlil gilish, ularning sabablari, usullari

va ogibatlarini aniglash hamda ularni oldini olish bo'yicha samarali chora-tadbirlar ishlab chigishdir. Bunda Iqtisodiy, huquqiy, itimoly va taxnologik ahamiyat mavjud.

Metodlar

Mazkur tadqiqotda kompleks metodologik yondashuv qo'llanildi. Avvalo, umumilmiy usullar — tahlil, sintez, induksiya va deduksiya yordamida kiberjinoyatlar tushunchasi va ularning asosiy xususiyatlari o'rganildi. Ushbu usullar orqali nazariy manbalar tizimli ravishda tahlil qilinib, umumlashtirildi.

Formal-yuridik usul asosida O'zbekiston Respublikasining Jinoyat kodeksi hamda axborot xavfsizligiga oid qonunchilik hujjatlari, jumladan, "Axborotlashtirish to'g'risida" va "Elektron hukumat to'g'risida"gi qonunlar o'rganildi. Ushbu usul jinoyat-huquqiy normalarning mazmunini aniqlash va ularni amaliyot bilan solishtirish imkonini berdi.

Qiyosiy-huquqiy usul yordamida xorijiy davlatlar tajribasi va xalqaro hujjatlar, xususan, kiberjinoyatlarga qarshi kurash bo'yicha xalqaro yondashuvlar tahlil qilindi. Bu esa milliy qonunchilikni takomillashtirish yo'nalishlarini aniqlashga xizmat qildi.

Shuningdek, empirik tahlil elementlari qo'llanilib, kiberjinoyatlarning amaliy ko'rinishlari, ularning keng tarqalgan turlari va rivojlanish tendensiyalari umumlashtirildi. Ilmiy adabiyotlar va xorijiy tadqiqotchilar fikrlari ham tahlil qilinib, tadqiqotning nazariy asoslari mustahkamlandi.

Kiberfiribgarlikka qarshi samarali kurash - bu faqat texnik vositalarga emas, balki keng qamrovli huquqiy, ijtimoiy va tashkiliy choralarni talab etadigan kompleks jarayondir. Avvalo, davlat darajasida kiberxavfsizlik siyosatini yangilash va unga qat'iy operatsion mexanizmlar

joriy etish zarur. Shu ma'noda, jinoyat kodeksi va tegishli normativ hujjatlarni zamonaviy kiberjinoyat shakillarini qamrab oladigan tarzda yangilash, mazkur hodisalar bo'yicha majburiy xabar berish mexanizmini qonuniylashtirish hamda kritik infratuzilmalar uchun muntazam kiberavfsizlik auditi va sertifikatlashtirishni joriy elsh ustuvor vazifalardir. Ushbu huquqiy tartib-intizom jinoyatlarni aniqlash, tergov va sud bosqichida samaradorlikni oshirishga xizmat qiladi.

Natijalar

Tadqiqot natijalari shuni ko'rsatdiki, kiberjinoyatlar o'ziga xos jinoyat-huquqiy xususiyatlarga ega bo'lib, ularning asosiy obyekti axborot xavfsizligi bilan bog'liq ijtimoiy munosabatlar hisoblanadi. Axborot xavfsizligi tushunchasi axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlash bilan bog'liq bo'lib, bu tamoyillar zamonaviy raqamli tizimlarning barqaror faoliyatini ta'minlaydi².

Kiberjinoyatlarning obyektiv tomoni ko'pincha kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni o'zgartirish yoki yo'q qilish, axborot tizimlarini bloklash hamda zararli dasturlarni yaratish va tarqatish kabi harakatlarda ifodalanadi.

Ushbu harakatlarning o'ziga xos jihati shundaki, ular ko'pincha yashirin va masofadan turib amalga oshiriladi. Natijada, kiberjinoyatlar yuqori darajada latent jinoyatlar sifatida namoyon bo'ladi³.

Subyekt masalasida aniqlanishicha, kiberjinoyatlar umumiy subyekt tomonidan sodir etilishi mumkin bo'lsa-da, amaliyotda ular ko'pincha axborot texnologiyalari sohasida bilim va ko'nikmaga ega shaxslar tomonidan sodir etiladi. Bu esa ularni aniqlash va tergov qilishda maxsus bilimlarning zarurligini ko'rsatadi. Ayrim ilmiy qarashlarga ko'ra, bunday jinoyatlar "intellektual jinoyatlar" sifatida baholanadi⁴.

Subyektiv tomondan kiberjinoyatlar asosan to'g'ridan-to'g'ri qasd bilan sodir etiladi. Jinoyatchi o'z harakatining ijtimoiy xavfliligini anglaydi va uning oqibatlarini oldindan ko'ra biladi. Ko'pincha jinoyatning motivi moddiy manfaat orttirish, noqonuniy daromad olish yoki ma'lumotlarni qo'lga kiritishdan iborat bo'ladi.

O'zbekiston Respublikasining Jinoyat kodeksida axborot texnologiyalari sohasidagi jinoyatlar uchun javobgarlik belgilangan bo'lib, bu normalar axborot xavfsizligini himoya qilishga qaratilgan⁵. Shu bilan birga, "Axborotlashtirish to'g'risida"gi Qonun axborot resurslari va tizimlarini himoya qilishning huquqiy asoslarini belgilaydi⁶, "Elektron hukumat to'g'risida"gi Qonun esa davlat boshqaruvida axborot xavfsizligini ta'minlashga xizmat qiladi⁷.

Shuningdek, Interpol va BMT Giyohvandlik va jinoyatchilik boshgarmasi (UNODC) tomonidan ham kiberjinoyatlarga qarshi xalqaro tavsiyalar ishlab chiqilgan. Kiberfribgarlik — bu ragamli muhitda foydalanuvchilarni aldash, ularning shasiy yoki moliyaviy ma'lumotlarini nogonuniy yo'l bilan golga kiritish, shuningdek, moddiy zarar yetkazish maqsadida amalga oshiriladigan nogonuniy harakatlardir. Amaliyotda uchraydigan kiberfribgarlik turlarining eng keng targalgan shakllariga quyidagilar kiradi: fishing (soxta elektron xabarlar orgali foydalanuvchini aldash), social engineering (inson psixologiyasidan foydalanib malumot olish), onlayn to'lov fribgarligi (soxta saytlar orqali to'lovlarni o'g'irlash), bank kartasi ma'lumotlarini o'g'irlash, soxta investitsiya va kriptovalyuta loyihalari, shuningdek, mobil ilovalar orgali amalga oshiriladigan aldov sxemalari. Bunday usullar yordamida jinoyatchilar foydalanuvchilarning e'tiborini chalgitish yoki ishonchini gozonish orgali ularning moliyaviy resurslarini egallab olishadi.

Tahlillar shuni ko'rsatdiki, O'zbekistonda eng keng tarqalgan kiberjinoyatlar qatoriga internet orqali fribgarlik, bank kartalari ma'lumotlarini o'g'irlash, phishing hujumlari va zararli dasturlar orqali ma'lumotlarni qo'lga kiritish kiradi. Ushbu jinoyatlar fuqarolarning mol-mulkiga sezilarli zarar yetkazmoqda va jamiyatda ishonch muhitiga salbiy ta'sir ko'rsatmoqda.

Muhokama

Olingan natijalar shuni ko'rsatadiki, kiberjinoyatlar zamonaviy jamiyatda tobora kengayib borayotgan murakkab ijtimoiy-huquqiy hodisa hisoblanadi. Ularning transchegaraviy xususiyati jinoyatlarni tergov qilishda jiddiy muammolarni keltirib chiqaradi. Shu sababli, xalqaro hamkorlikni rivojlantirish kiberjinoyatlarga qarshi kurashishda muhim omil hisoblanadi. Xususan, BMT tomonidan o'tkazilgan tadqiqotlarda ham global yondashuv zarurligi ta'kidlangan⁸.

Shu bilan birga, milliy qonunchilikni takomillashtirish zarurati mavjud. Amaldagi huquqiy normalar barcha zamonaviy kiberxavflarni to'liq qamrab olmaydi. Xususan, kriptovalyutalar bilan bog'liq firibgarliklar, sun'iy intellekt asosidagi hujumlar va boshqa yangi tahdidlar hali yetarli darajada huquqiy tartibga solinmagan.

Kiberjinoyatlarga qarshi kurashishda texnik infratuzilmaning rivojlanganligi ham muhim ahamiyatga ega. Raqamli dalillarni to'plash, saqlash va tahlil qilish bo'yicha zamonaviy usullarni joriy etish tergov samaradorligini oshiradi. Shu bilan birga, kadrlar tayyorlash masalasi ham dolzarb bo'lib qolmoqda.

Aholining raqamli savodxonligini oshirish ham muhim profilaktik chora hisoblanadi. Ko'plab kiberjinoyatlar aynan foydalanuvchilarning ehtiyotsizligi yoki bilim yetishmasligi sababli sodir etilmoqda. Shu bois, aholiga kiberxavfsizlik qoidalarini tushuntirish va ularni amaliy jihatdan o'rgatish zarur.

Xulosa

Yuqoridagilardan kelib chiqib, shuni xulosa qilish mumkin-ki, kiberjinoyatlar zamonaviy axborotlashgan jamiyatning eng dolzarb muammolaridan biri hisoblanadi. Ularning jinoyat-huquqiy tavsifi murakkab bo'lib, an'anaviy jinoyatlardan tubdan farq qiladi. O'zbekiston Respublikasida ushbu sohada muayyan huquqiy asoslar yaratilgan bo'lsa-da, ularni yanada takomillashtirish zarurati mavjud.

Ushbu o'rganilgan masalalar asosida shuni xulosa qilish mumkinki, kiberfiribgarlik zamonaviy jamiyat xavfsizligiga jiddiy tahdid solayotgan global muammo hisoblanadi. Kiberfiribgarlikka qarshi samarali kurash olib borish uchun davlat, fugarolar va tashkilotlar o'rtasida mustahkam hamkorlik zarur. Davlat organlari huquqiy bazani takomillashtirib, kiberavfsizlik infratuzilmasini mustahkamlashi lozim. Tashkilotlar esa o'z axborot tizimlarini himoya qilish, xodimlarni muntazam ravishda kiberxavfsizlik bo'yicha o'qitish va xavf tahlilini olib borish orgali o'z mas'uliyatini oshirishi kerak. Fugarolar ham o'z navbatida raqamli savodxonlik darajasini oshirishi, shaxsiy ma'lumotlarini himoya qilish, shubhali havolalar va noma'lum manbalarga ishonmaslik madaniyatini shakllantirishi zarur. Huquqshunaslar ushbu vaziyatlarni oldini olishga kerakli normalarni yaratib berishlari, ushbu amaliyotlarni qonuniy qo'llanilishi uchun qonuniy asoslar yaratib berish kerak, kiberfiribgarliklarni oldini olish uchun barcha huquqiy harakatlarni amaga oshirish zarur.

Kiberjinoyatlarga qarshi samarali kurashish kompleks yondashuvni talab etadi. Bu esa jinoyat-huquqiy choralar, texnik vositalar, xalqaro hamkorlik va ma'rifiy ishlarning uyg'unligini taqozo etadi. Faqat shu holatda axborot xavfsizligini ta'minlash va jamiyatni kiberxavflardan himoya qilish mumkin.

Foydalanilgan adabiyotlar/ Литературы/ References

1. Wall D. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, 2015.
2. ISO/IEC 27001: Information Security Standards. <https://iso.org/standard/27001>
3. Brenner S. *Cybercrime and the Law*. 2012. https://www.researchgate.net/publication/287743943_Cybercrime_and_the_law_Challenges_issues_and_outcomes
4. Yar M. *Cybercrime and Society*. 2018. https://books.google.co.uz/books?id=_nN7DwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
5. O'zbekiston Respublikasi Jinoyat kodeksi. <https://lex.uz/mact/-111453>
6. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni. <https://lex.uz/mact/-83472>
7. O'zbekiston Respublikasining "Elektron hukumat to'g'risida"gi Qonuni. <https://lex.uz/mact/-2833860>
8. UNODC. *Comprehensive Study on Cybercrime*. 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
9. PF-38. <https://lex.uz/uz/docs/-8079286>.