KIBERJINOYATLARNING KELIB CHIQISH VA RIVOJLANISH OMILLARI TAHLILI

O‘rinkulov Odiljon Naziraliyevich
O‘zbekiston Respublikasi Ichki ishlar vazirligi Akademiyasi
e-mail: ourinkulov@gmail.com
ORCID: 0000-0003-2392-9309

Annotatsiya. *Ushbu maqolada axborot texnologiyalari yordamida sodir etiladigan jinoyatlarning kelib chiqish va rivojlanish sabablari chuqur tahlil qilinadi. Kiberjinoyatlarga ta’sir qiluvchi texnologik, huquqiy va ijtimoiy omillar tahlil qilinadi hamda kiberjinoyatlarni oldini olish bo‘yicha tavsiyalar beriladi. Yangi turdagi jinoyat turlarining paydo bo‘lishi tadqiq etiladi va kiberjinoyatchilikka qarshi kompleks choralar majmuasini taklif etiladi. Tadqiqotning ilmiy-amaliy ahamiyati shundaki, unda kiberjinoyatlarning yangi shakllari paydo bo‘lishining “texnologik bo‘shliq - huquqiy bo‘shliq - ijtimoiy zaiflik - tezkor moslashuv” modeli asoslab beriladi. Ushbu xulosalar qonunchilikni takomillashtirish, bank va telekommunikatsiya sektorlarida preventiv nazoratni kuchaytirish, elektron dalillar bilan ishlash amaliyotini standartlashtirish hamda aholining kibermadaniyatini oshirish bo‘yicha amaliy tavsiyalar ishlab chiqishda qo‘llanishi mumkin.*

Kalit so‘zlar: *kiberjinoyat, kiberxavfsizlik, raqamlashtirish, ijtimoiy muhandislik, elektron dalil, fishing, sun'iy intellekt, deepfake, SIM-swap, account takeover.*

Annotation. *This article thoroughly analyzes the causes of the emergence and development of crimes committed using information technologies. Technological, legal, and social factors influencing cybercrimes are analyzed, and recommendations for the prevention of cybercrimes are given. The emergence of new types of crimes is investigated, and a complex of measures against cybercrime is proposed. The scientific and practical significance of the research lies in the fact that it substantiates the "technological gap - legal gap - social vulnerability - rapid adaptation" model of the emergence of new forms of cybercrime. These conclusions can be used in the development of practical recommendations for improving legislation, strengthening preventive control in the banking and telecommunications sectors, standardizing the practice of working with electronic evidence, and increasing the cyberculture of the population.*

Keywords: *cybercrime, cybersecurity, digitalization, social engineering, electronic evidence, phishing, artificial intelligence, deepfake, SIM-swap, account takeover.*

Аннотация. *В данной статье глубоко анализируются причины возникновения и развития преступлений, совершаемых с помощью информационных технологий. Проанализированы технологические, правовые и социальные факторы, влияющие на киберпреступления, а также даны рекомендации по предотвращению киберпреступлений. Исследуется возникновение новых видов преступлений и предлагается комплекс мер борьбы с киберпреступностью. Научная и практическая значимость исследования заключается в том, что в нем обоснована модель возникновения новых форм киберпреступности "технологический вакуум - правовой вакуум - социальная уязвимость - быстрая адаптация." Эти выводы могут быть использованы при разработке практических рекомендаций по совершенствованию законодательства, усилению превентивного контроля в банковском и телекоммуникационном секторах, стандартизации практики работы с электронными доказательствами и повышению киберкультуры населения.*

Ключевые слова: *киберпреступность, кибербезопасность, цифровизация, социальная инженерия, электронные доказательства, фишинг, искусственный интеллект, deepfake, SIM-swap, захват аккаунта.*

Kirish. Raqamli iqtisodiyot, elektron to‘lovlar, masofaviy identifikatsiya, davlat xizmatlarining onlayn shaklga o‘tishi va ijtimoiy tarmoqlar kommunikatsiyaning asosiy maydoniga aylanishi jinoyatchilikning shakllari va usullarini ham tubdan o‘zgartirdi. Rivojlangan davlatlar statistik ma’lumotlariga e’tibor qaratsak AQSH Federal qidiruv byurosining 2024-yilgi Internet Crime Report hisobotida 859 532 ta murojaat qayd etilgani va yo‘qotishlar 16 milliard AQSh dollaridan oshgani keltiriladi [1]. ENISA va Europol materiallari esa onlayn firibgarlik, ransomware, ma’lumotlarni o‘g‘irlash, shaxs biometrik ma’lumotlarini soxtalashtirish hamda AI bilan kuchaytirilgan hujumlar global xavfning markaziga aylanganini ko‘rsatadi [2]-[5].

O‘zbekistonda ham kiberjinoyatchilik periferik texnik muammo maqomidan chiqib, ommaviy huquqbuzarlik shakliga aylanmoqda. O‘zbekistonda 2023-yilning 11 oyida 5,5 mingta kiberjinoyat sodir etilgani, ularning qariyb 70 foizi bank kartalari bilan bog‘liq ekani yuqoridagi fikrlarning asosli ekanligini bildiradi [7]. IIVning 2025-yilgi rasmiy tahliliga ko‘ra, 2019-yilda axborot texnologiyalari yordamida 18 turdagi 863 ta jinoyat qayd etilgan bo‘lsa, 2024-yilda bu ko‘rsatkich 62 turdagi 58 800 ta holatga yetgan; umumiy jinoyatchilikdagi ulushi esa 2023-yildagi 6,2 foizdan 2024-yilda 44,4 foizga ko‘tarilgan [8].

Mavjud adabiyotlarda kiberjinoyatlarni tasniflash, alohida turlarini tavsiflash yoki ularning huquqiy jihatlarini ko‘rib chiqish yetarlicha uchrasa-da, ularning kelib

chiqish va rivojlanish sabablari ko‘pincha qismlarga ajratilgan holda yoritiladi. Ayniqsa, texnologik infratuzilma, huquqiy tartibga solish, ijtimoiy xulq-atvor va noqonuniy xizmat bozorlarining o‘zaro ta’siri kompleks tizim sifatida kamroq tadqiq etilgan [6], [12]-[16]. Shu bois kiberjinoyatchilikni faqat “texnik hujum” yoki faqat “firibgarlik” sifatida tushunish yetarli emas.

Mazkur tadqiqotning maqsadi kiberjinoyatlarning kelib chiqishi va rivojlanishini belgilovchi asosiy omillarni tizimli ravishda aniqlash, ularning O‘zbekiston sharoitidagi namoyon bo‘lish xususiyatlarini tahlil qilish va preventiv siyosat uchun amaliy xulosalar ishlab chiqishdan iborat.

Tadqiqot metodologiyasi. Tadqiqotning empirik va nazariy bazasini xalqaro rasmiy hisobotlar, milliy normativ-huquqiy hujjatlar, davlat organlarining ochiq statistik ma’lumotlari hamda mavzuga oid ilmiy maqolalar tashkil etadi [1]-[19]. Xususan, FBI, ENISA, Europol, UNODC, OSCE materiallari, shuningdek O‘zbekiston Respublikasi Ichki ishlar vazirligi, Markaziy bank va kiberxavfsizlik sohasiga oid milliy hujjatlar o‘rganildi.

Tadqiqotda tizimli tahlil, qiyosiy-huquqiy tahlil, statistik umumlashtirish, sabab-oqibat bog‘liqligini ochuvchi struktura-funktsional yondashuv hamda ilmiy adabiyotlarni sharhlash usullaridan foydalanildi. Kiberjinoyatlarning rivojlanish dinamikasi raqamli iqtisodiyotning kengayishi, qonunchilikdagi adaptatsiya sur’ati, ijtimoiy muhandislikka moyillik va kiberjinoyat infratuzilmasining xizmatlashuvi kabi mezonlar bo‘yicha tahlil qilindi.

Tadqiqotning asosiy cheklovi shundaki, kiberjinoyatlar yashirinligi yuqori bo‘lgan soha hisoblanadi. Shu sababli ochiq statistik ma’lumotlar real ko‘lamni to‘liq aks ettirmasligi mumkin. Biroq, turli manbalarni qiyoslash va mazmuniy verifikatsiya qilish natijasida asosiy tendensiyalarni aniqlash imkoniyati saqlanib qoladi.

Kiberjinoyatchilik dinamikasi va tarkibiy o‘zgarishi. Global va milliy ma’lumotlar kiberjinoyatchilikning miqdoriy o‘sishidan tashqari, uning sifat jihatdan murakkablashib borayotganini ham ko‘rsatadi. FBI hisobotida 2024-yilda eng ko‘p uchragan internet jinoyatlari sifatida phishing/spoofing, tovlamachilik va shaxsiy ma’lumotlardan noqonuniy foydalanish qayd etilgan [1]. Bu kiberjinoyatlar tobora ko‘proq ijtimoiy muhandislik, ma’lumotlarni ruxsatsiz egallash va masofadan boshqariladigan firibgarlik sxemalariga tayana boshlaganini bildiradi. Europolning IOCTA hisobotlari esa ransomware, onlayn firibgarlik, noqonuniy ma’lumot savdosi va dastlabki kirish huquqlarini sotish amaliyotining kuchayganini ko‘rsatadi [4], [5].

Jadval 1. O‘zbekistonda kiberjinoyat dinamikasining ayrim ko‘rsatkichlari

Ko‘rsatkich	2019	2023	2024
Qayd etilgan kiberjinoyatlar soni	863	5,5 ming (11 oy)	58 800
Aniqlangan turlar soni	18	-	62
Umumiy jinoyatchilikdagi ulushi	-	6,2 %	44,4 %
Bank kartalari bilan bog‘liq ulushi	-	qariyb 70 %	98 %

Manba: [7], [8] asosida muallif tomonidan tuzildi.

Jadval 1 ma’lumotlari O‘zbekistonda kiberjinoyatchilikning faqat son jihatidan emas, balki tarkib jihatidan ham o‘zgarganini ko‘rsatadi. 2019-yilda nisbatan tor ko‘lamli va texnik ko‘rinishdagi huquqbuzarliklar ustun bo‘lgan bo‘lsa, 2023-2024-yillarga kelib bank kartalari, mobil ilovalar, onlayn savdo platformalari va masofaviy tranzaksiyalar bilan bog‘liq firibgarliklar tez ko‘paygan [7], [8]. Demak, kiberjinoyatchilikning asosiy og‘irlik markazi korporativ tarmoq hujumlaridan keng iste'molchi segmentiga siljigan.

Texnologik omillar. Kiberjinoyatlarning birlamchi drayveri texnologik transformatsiya hisoblanadi. Yangi raqamli mahsulotlar va servislar foydalanuvchilar uchun qulaylik yaratadi, biroq ayni vaqtda yangi hujum omilini ham hosil qiladi. Mobil banking, masofaviy identifikatsiya, bulutli saqlash, API integratsiyasi, messenjerlar va marketplace platformalari orqali ma’lumotlar aylanishining tezlashishi jinoyatchiga ko‘proq kirish nuqtalarini taqdim etadi. Har bir yangi funksional imkoniyat - autentifikatsiya, tokenlash, SMS tasdiqlash, QR to‘lov, masofaviy kredit - alohida xavf vektori sifatida namoyon bo‘lishi mumkin.

Texnologik omil faqat “yangi texnologiya - yangi zaiflik” zanjiri bilan cheklanmaydi. So‘nggi yillarda kiberjinoyat infratuzilmasi takomillashdi: tayyor fishing to‘plamlari, zararli APK fayllar, botnet ijarasi, ma’lumotlar bazasi savdosi, hisoblarni egallash xizmatlari va kriptovalyutadan foydalanib pul yuvish sxemalari ommaviylashib bormoqda [12]. Bu holat kiberjinoyat sodir etish uchun zarur bo‘lgan texnik malaka to‘sig‘ini pasaytiradi. Natijada ilgari faqat yuqori malakali xakerlar sodir eta oladigan harakatlar endi yarim tayyor vositalar yordamida kengroq doiradagi shaxslar tomonidan amalga oshirilmoqda.

Sun’iy intellekt va generativ modellarning ommalashuvi ushbu jarayonni yanada tezlashtirmoqda. ENISA, Europol va chuqur tahliliy tadqiqotlar AI vositalari

ko‘p tilli firibgarlik xabarlarini yaratish, ovoz va video imitatsiyasi, shaxsni soxtalashtirish, deepfake asosidagi ishonch manipulyatsiyasi hamda fishing ssenariylarini avtomatlashtirish imkonini kengaytirayotganini ko‘rsatadi [3], [5], [13], [16]. Shu ma’noda texnologik omil nafaqat zaifliklar manbai, balki jinoyatchining unumdorligini oshiruvchi vosita hamdir.

Huquqiy va yurisdiksion omillar. Kiberjinoyatlarning rivojlanishiga ta’sir etuvchi ikkinchi omil - huquqiy va yurisdiksion murakkablikdir. An’anaviy jinoyatlardan farqli ravishda, kiberjinoyatda server, jabrlanuvchi, ijrochi va pul oqimlari turli davlatlarda joylashishi mumkin. Bu holat dalillarni tezkor yig‘ish, ma’lumotlarni saqlab qolish, IP va tranzaksiya izlarini kuzatish, shuningdek aybdorni ekstraditsiya qilish masalalarini murakkablashtiradi. Xalqaro darajadagi huquqiy me’yorlarning nomuvofiqligi, elektron dalillarni taqdim etish tartiblaridagi tafovutlar va so‘rovlarni ko‘rib chiqishdagi vaqt yo‘qotishlari jazo muqarrarligini pasaytiradi [12], [17].

O‘zbekistonda mazkur xavflarni jilovlash bo‘yicha normativ baza bosqichma-bosqich takomillashtirilmoqda. “Kiberxavfsizlik to‘g‘risida”gi Qonun, O‘zbekiston Respublikasi Prezidentining 2025-yildagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida” PQ-153-son qaror, shuningdek to‘lov tizimlarida axborot xavfsizligi va firibgarlikning oldini olish bo‘yicha Markaziy bank talablari buning yaqqol misolidir [9]-[11]. Biroq bu ijobiy siljishlarga qaramay, amaliyotda bir qator masalalar dolzarbligicha qolmoqda: elektron dalillarni tezkor aniqlash qilish va zanjirini saqlash, bank, telekom va platformalarning xabar berish majburiyatlarini aniq belgilash, kiberhodisa va kiberjinoyat statistikalarini yagona formatda yuritish, shuningdek tergov va sud amaliyotida maxsus kompetensiyalarni kuchaytirish.

Huquqiy omilning yana bir muhim ko‘rinishi - yangi texnologiya paydo bo‘lish tezligi bilan normativ moslashuv sur’ati o‘rtasidagi tafovutdir. Qonunchilik ko‘pincha zarar allaqachon sodir bo‘lgandan so‘ng reaksiya bildiradi. Deepfake yordamida firibgarlik, sintetik identifikatsiya, AI asosidagi ovozli aldov, investitsiya ilovalari ko‘rinishidagi soxta platformalar bunga misoldir. Shuning uchun kiberjinoyatlarning rivojlanishi ko‘p hollarda huquqiy “kechikish” bilan bevosita bog‘liq.

Ijtimoiy va psixologik omillar. Uchinchi yirik omil - ijtimoiy va psixologik zaifliklar. Kiberjinoyatlarning muhim qismi murakkab texnik ekspluatatsiyadan ko‘ra, foydalanuvchini chalg‘itish, shoshirish yoki ishonchga kiritish orqali sodir etiladi. Jinoyatchilar “bank xodimi”, “xavfsizlik bo‘limi”, “to‘lov operatori”, “marketplace sotuvchisi” yoki “investor-maslahatchi” sifatida namoyon bo‘lib, jabrlanuvchidan SMS-kod, karta rekviziti, ilova ruxsatlari yoki pul o‘tkazishni talab

qiladi. Bu yerda asosiy nishon tizim emas, insonning qaror qabul qilish mexanizmi bo‘ladi.

O‘zbekiston bo‘yicha rasmiy tahlillar kiberjinoyatlarning asosiy qismi zararli havolalar va dasturlar yuborish, SMS tasdiqlash kodlarini qo‘lga kiritish, onlayn kredit rasmiylashtirish hamda onlayn savdo maydonlaridagi firibgarliklar bilan bog‘liqligini ko‘rsatadi [8]. Mazkur ko‘rsatkichlar shuni anglatadiki, foydalanuvchi xatosi va past kibersavodxonlik kiberjinoyatchilikning markaziy omillaridan biridir. Demak, himoyani faqat texnik qatlamda emas, balki xulq-atvor darajasida ham qurish talab etiladi.

Ijtimoiy omilning yana bir jihati - latentlik. Ko‘plab jabrlanuvchilar sodir bo‘lgan hodisa haqida vaqtida xabar bermaydi, ayrimlar esa umuman murojaat qilmaydi. Bunga uyat, aybni o‘zidan ko‘rish, huquqni muhofaza qiluvchi organlar yordamiga ishonchsizlik yoki “pulni baribir qaytarib bo‘lmaydi” degan qarash sabab bo‘ladi. Natijada jinoyatchi bir xil sxemani ko‘p marotaba takrorlash imkoniga ega bo‘ladi, bu esa kiberjinoyatlarning ko‘payishiga qulay sharoit yaratadi.

Jadval 2. Kiberjinoyatlarning asosiy sabab omillari va ularning namoyon bo‘lishi

Omil guruhi	Asosiy mazmuni	Ko‘rinishlari	Ustuvor qarshi chora
Texnologik	Raqamli servislar, mobil ilovalar, API integratsiyasi, AI va xizmatlashgan kiberjinoyat bozori.	Fishing, zararli APK, hisobni egallash, deepfake, ransomware.	Xavfsiz dizayn, MFA, anti-fraud monitoring, fishingni erta aniqlash.
Huquqiy-yurisdiktsion	Transchegaraviylik, elektron dalillar bilan ishlashdagi murakkablik, normativ moslashuvning kechikishi.	Dalillarni yo‘qotish, javobgarlikdan qochish, soxta platformalar, anonim monetizatsiya.	Tezkor xalqaro hamkorlik, majburiy xabar berish, e-dalil protseduralarini standartlashtirish.
Ijtimoiy-psixologik	Ishonuvchanlik, shoshilish, savodxonlikning	SMS-kod berish, investitsiya aldovi,	Kibersavodxonlik, ommaviy

	pastligi, ijtimoiy muhandislikka moyillik.	marketplace firibgarligi, telefon manipulyatsiyasi.	ogohlantirish, xulq-atvor analitikasi.
Tashkiliy-iqtisodiy	Cybercrime-as-a-service, ma'lumotlar savdosi, noqonuniy pul oqimlari.	Fishing vositalari savdosi, ma'lumot brokerlari, gibrid investitsiya firibgarligi.	Pul oqimini kuzatish, bank-platforma hamkorligi, tezkor blokirovka va monitoring.

Manba: [1]-[5], [8], [12]-[16] asosida muallif tomonidan umumlashtirildi.

Yangi kiberjinoyat turlarining paydo bo‘lish mexanizmi. Tahlil natijalari yangi kiberjinoyat turlari, odatda, quyidagi mexanizm bo‘yicha paydo bo‘lishini ko‘rsatadi. Birinchi bosqichda yangi platforma yoki servis ommalashadi. Ikkinchi bosqichda uning xavfsizlik va nazoratdagi bo‘shliqlari aniqlanadi. Uchinchi bosqichda jinoyatchilar ushbu bo‘shliqni ekspluatatsiya qilib, sinov tariqasidagi sxemalarni ishga tushiradi. To‘rtinchi bosqichda muvaffaqiyatli sxemalar ommalashadi, ya’ni shablon, instruktsiya, bot yoki tayyor skript ko‘rinishida boshqalarga ham tarqala boshlaydi. Beshinchi bosqichda davlat va biznes himoya choralarini kuchaytiradi, natijada jinoyat boshqa vektorga ko‘chadi.

Deepfake firibgarligi, gibrid investitsiya-romantik firibgarlik (“pig butchering”), soxta mobil ilovalar, sintetik identifikatsiya, hisobni egallash hujumlari va cybercrime-as-a-service bozorlari aynan shu jarayonning mahsulidir [12]-[16]. Bunday sxemalarda texnik zaiflik, emotsional manipulyatsiya va transchegaraviy pul yuvish mexanizmlari birlashadi. Shu bois yangi kiberjinoyatni tushunish uchun uning alohida epizodini emas, balki butun ekotizimini tahlil qilish zarur.

Ushbu qonuniyat O‘zbekiston uchun ham dolzarb. Elektron to‘lovlar, davlat xizmatlari, onlayn kreditlash va ijtimoiy tarmoqlar integratsiyasi chuqurlashgani sari yangi firibgarlik ssenariylari paydo bo‘lish ehtimoli ortadi. Binobarin, kiberjinoyatga qarshi siyosat reaktiv emas, balki prognozli va oldindan ogohlantiruvchi xarakterga ega bo‘lishi lozim.

Muhokama. Kiberjinoyatlar kiber bog‘liq (cyber-dependent) va kiber qo‘llab-quvvatlanadigan (cyber-enabled) shakllarga bo‘linadi [6]. Biroq O‘zbekiston misolida aynan kiberqo‘llab-quvvatlanadigan firibgarliklar, ya’ni bank kartalari, mobil ilovalar, SMS kodlari va onlayn savdo bilan bog‘liq sxemalar yetakchi ekani kuzatiladi [7], [8]. Bu milliy kontekstda zaif nuqta ko‘proq “foydalanuvchi - to‘lov tizimi - aloqa kanali” kesishmasida joylashganini anglatadi.

Natijalar ENISA va Europolning so‘nggi tahdid misollari bilan hamohangdir. Ushbu manbalarda ham onlayn firibgarlik, ma’lumotlar savdosi, ransomware, dastlabki kirish huquqlarini sotish va AI bilan kuchaytirilgan hujumlar asosiy tendensiyalar sifatida ko‘rsatiladi [2]-[5]. Demak, O‘zbekistondagi holat alohida istisno emas; u global jarayonlarning mahalliy to‘lov va aloqa ekotizimiga moslashgan ko‘rinishidir.

Biroq milliy vaziyatning o‘ziga xos jihati ham mavjud. Kiberjinoyatlarning keskin o‘sishi qisman real xavfning kuchayganini, qisman esa raqamlashtirish ko‘lamining kengaygani va ro‘yxatga olish amaliyotining takomillashganini bildiradi. Shu sababli statistik o‘sishni faqat bitta omil bilan izohlash to‘g‘ri bo‘lmaydi. Ammo qanday talqin qilinmasin, ochiq ma’lumotlar kiberjinoyatchilikning endi e’tiborsiz qoldiriladigan hodisa emasligini, balki ommaviy va tizimli xavfga aylanganini aniq ko‘rsatadi.

Shundan kelib chiqib, samarali qarshi choralar ko‘p qatlamli bo‘lishi kerak. Birinchidan, normativ baza yangi tahdidlar paydo bo‘lishidan ortda qolmasligi lozim. Ikkinchidan, banklar, telekommunikatsiya operatorlari, marketplace platformalari va davlat axborot tizimlari o‘rtasida tezkor ma’lumot almashinuvi yo‘lga qo‘yilishi zarur [10], [11]. Uchinchidan, tergovchi, prokuror va sudyalar uchun elektron dalillar, deepfake, ma’lumotlarni autentifikatsiya qilish va transchegaraviy jinoyat ishlarini yuritish bo‘yicha maxsus o‘quv dasturlari kengaytirilishi kerak [18], [19]. To‘rtinchidan, kibersavodxonlikni oshirish uzluksiz ijtimoiy profilaktika vazifasi sifatida tashkil etilishi zarur.

2024-yilda BMT doirasida Kiberjinoyatlarga qarshi konvensiyaning qabul qilinishi xalqaro hamkorlik va elektron dalillar almashinuvi mexanizmlarini yanada tizimlashtirishga qaratilgan global burilish sifatida baholanishi mumkin [17]. Bu, ayniqsa, transchegaraviy firibgarlik, ma’lumot savdosi va ommalashgan kiberjinoyat bozorlariga qarshi kurashishda muhimdir.

Xulosa

Xulosa qilib aytganda, kiberjinoyatlarning kelib chiqishi va rivojlanishi biror yagona omilga emas, balki o‘zaro bog‘langan texnologik, huquqiy, ijtimoiy va tashkiliy omillar tizimiga tayanadi. Tadqiqot natijalari shuni ko‘rsatdiki, raqamlashtirish sur'atining tezlashuvi yangi hujum yuzalarini yaratadi; huquqiy tartibga solishdagi kechikish va transchegaraviy murakkabliklar jazo muqarrarligini pasaytiradi; past kibersavodxonlik va ijtimoiy muhandislik esa jinoyatchilar uchun eng qulay kiberjinoyatchilik amaliyotlarini amalga oshirish mexanizmini ta’minlaydi. Bularning barchasi ommalashgan kiberjinoyat bozori, tayyor zararli vositalar va AI asosidagi firibgarlik bilan birlashganda jinoyatlarning ko‘lami va xilma-xilligi keskin ortadi.

O‘zbekiston misolida kiberjinoyatchilikning markaziy og‘irlik nuqtasi bank kartalari, mobil ilovalar, SMS autentifikatsiya va onlayn savdo maydonlari bilan bog‘liq firibgarliklarga to‘g‘ri kelayotgani aniqlandi. Bu holat milliy preventiv siyosatni aynan foydalanuvchi xulqi, moliyaviy ekotizim, telekommunikatsiya xavfsizligi va tezkor axborot almashinuvi bilan bog‘liq choralar asosida qurish zarurligini ko‘rsatadi. Shu bilan birga, elektron dalillar bilan ishlash, sud va tergov amaliyotida maxsus kompetensiyalarni rivojlantirish, kiberhodisalar bo‘yicha xabar berish tizimini takomillashtirish va xalqaro hamkorlikni kuchaytirish strategik ahamiyatga ega.

Maqolaning ilmiy hissasi kiberjinoyatlarning yangi shakllari paydo bo‘lishining “texnologik bo‘shliq - huquqiy bo‘shliq - ijtimoiy zaiflik - xizmatlashgan ekspluatatsiya” modelini tizimlashtirishdan iborat. Kelgusida hududlar, yosh guruhlari va alohida jinoyat turlari kesimida empirik tadqiqotlarni kengaytirish kiberjinoyatchilikka qarshi yanada aniq va moslashuvchan siyosatni ishlab chiqish imkonini beradi.

Foydalanilgan adabiyotlar

[1] Federal Bureau of Investigation. Internet Crime Report 2024. Washington, DC: FBI Internet Crime Complaint Center, 2025. URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[2] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[3] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[4] Europol. IOCTA, Internet Organised Crime Threat Assessment 2024. Luxembourg: Publications Office of the European Union, 2024. DOI: 10.2813/442713.

[5] Europol. IOCTA, Internet Organised Crime Threat Assessment 2025. Luxembourg: Publications Office of the European Union, 2025. URL: https://op.europa.eu/en/publication-detail/-/publication/0a06109b-4b28-11f0-85ba-01aa75ed71a1/language-en

[6] Phillips K., Davidson J. C., Farr R. R., Burkhardt C., Caneppele S., Aiken M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2022, 2(2), pp. 379-398. DOI: 10.3390/forensicsci2020028.

[7] 11 oyda 5,5 mingta kiberjinoyat sodir etildi, ularning 70 foizi bank kartalari bilan bog‘liq. 20.12.2023. URL: https://www.gazeta.uz/oz/2023/12/21/cyber-crime/#:~:text=2023%2Dyilning%2011%20oyida%205%2C5%20mingta%20kiberji

noyat%20sodir,ham%20kiberxavfsizlik%20talablariga%20javob%20bermasligi%20qayd%20etildi.
[8] O‘zbekiston Respublikasi Ichki ishlar vazirligi. Creating a Safe Cyberspace by Combating Cybercrime. Uzbekistan's Experience in the Early Prevention of Cybercrime in the Context of Digital Transformation. 07.05.2025. URL: https://gov.uz/en/iiv/news/view/52319
[9] O‘zbekiston Respublikasining Qonuni. 'Kiberxavfsizlik to‘g‘risida’, O‘RQ-764, 15.04.2022. URL: https://lex.uz/docs/-5960604
[10] O‘zbekiston Respublikasi Prezidenti. 'Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida’, PQ-153, 30.04.2025. URL: https://lex.uz/pdffile/7716359
[11] O‘zbekiston Respublikasi Markaziy banki. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralarini ko‘rish to‘g‘risidagi nizomni tasdiqlash haqida, ro‘yxat raqami 3513, 21.05.2024. URL: https://lex.uz/pdffile/6933268
[12] United Nations Office of Counter-Terrorism, UNCCT, and UNICRI. Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks. New York: United Nations, 2024. URL: https://www.un.org/counterterrorism/events/report-dark-web-and-cyber-crime-service-and-its-impact-cyber-enabled-terrorism
[13] Sandoval M.-P., de Almeida Vau M., Solaas J., et al. Threat of deepfakes to the criminal justice system: a systematic review. Crime Science, 2024, 13, 41. DOI: 10.1186/s40163-024-00239-1.
[14] Han B., Button M. An Anatomy of 'Pig Butchering Scams': Chinese Victims' and Police Officers' Perspectives. Deviant Behavior, 2025. DOI: 10.1080/01639625.2025.2453821.
[15] Maras M.-H., Ives E. R. Deconstructing a form of hybrid investment fraud: Examining 'pig butchering‘ in the United States. Journal of Economic Criminology, 2024, 5, 100066. DOI: 10.1016/j.jeconc.2024.100066.
[16] Lin L. S. F. Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud. Laws, 2025, 14(4), 46. DOI: 10.3390/laws14040046.
[17] United Nations Office on Drugs and Crime. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crime. 2024. URL:

https://www.unodc.org/cld/en/treaties/status/australia/united_nations_convention_against_cybercrime.html
[18] OSCE Project Co-ordinator in Uzbekistan. National Training on Cybercrime for Judges Launched in Tashkent. 14.04.2025. URL: https://www.osce.org/project-coordinator-in-uzbekistan/589364
[19] Organization for Security and Co-operation in Europe. OSCE workshop in Uzbekistan supports development of national competency framework and training strategy on cybercrime and electronic evidence. 03.06.2025. URL: https://www.osce.org/secretariat/592076