YURIDIK FANLAR AXBOROTNOMASI
ВЕСТНИК ЮРИДИЧЕСКИХ НАУК
REVIEW OF LAW SCIENCES

huquqiy ilmiy-amaliy jurnal

правовой научно-практический журнал

legal scientific-practical journal

2026-yil maxsus son

VOLUME 10 / SPECIAL ISSUE / 2026
DOI: HTTPS://DX.DOI.ORG/10.51788/TSUL.ROLS.2026.10.SI.

ISSN 2181-919X
E-ISSN 2181-1148
DOI: HTTPS://DX.DOI.ORG/10.51788/TSUL.ROLS

Crossref
Content
Registration

MUASSIS: TOSHKENT DAVLAT YURIDIK UNIVERSITETI

"Yuridik fanlar axborotnomasi – Вестник юридических наук – Review of law sciences" huquqiy ilmiy-amaliy jurnali O'zbekiston matbuot va axborot agentligi tomonidan 2020-yil 22-dekabrda 0931-sonli guvohnoma bilan davlat ro'yxatidan o'tkazilgan.

Jurnal O'zbekiston Respublikasi Fanlar akademiyasi huzuridagi Oliy attestatsiya komissiyasi jurnallari ro'yxatiga kiritilgan.

Sotuvda kelishilgan narxda.

Nashr bo'yicha mas'ul:
O. Choriyev

Muharrirlar:
E. Mustafayev, Y. Yarmolik, M. Sharifova, Sh. Beknazarova, X. Yuldasheva, E. Sharipov

Musahhih:
M. Tursunov

Texnik muharrir:
U. Sapayev

Dizayner:
D. Rajapov

Tahririyat manzili:
100047. Toshkent shahri, Sayilgoh ko'chasi, 35.
Tel.: (0371) 233-66-36 (1169)

Veb-sayt: review.tsul.uz
E-mail: reviewjournal@tsul.uz

Obuna indeksi: 1385.

Nashriyot litsenziyasi
№ 174625, 29.11.2023.

Jurnal 2026-yil 7-iyulda bosmaxonaga topshirildi.
Qog'oz bichimi: A4.
Shartli bosma tabog'i: 24,2
Adadi: 100. Buyurtma: № 77.

Bosmaxona litsenziyasi
29.11.2023 № 174626

TDYU bosmaxonasida chop etildi.
Bosmaxona manzili:
100047. Toshkent shahri, Sayilgoh ko'chasi, 37.

TAHRIR HAY'ATI

УЧРЕДИТЕЛЬ: ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ

Правовой научно-практический журнал «Вестник юридических наук – Yuridik fanlar axborotnomasi – Review of Law Sciences» зарегистрирован Агентством печати и информации Узбекистана 22 декабря 2020 года с удостоверением № 0931.

Журнал включён в перечень журналов Высшей аттестационной комиссии при Академии наук Республики Узбекистан.

Реализуется по договорной цене.

Ответственный за выпуск:
О. Чориев

Редакторы:
Э. Мустафаев, Е. Ярмолик, М. Шарифова, Ш. Бекназарова, Х. Юлдашева, Э. Шарипов

Корректор:
М. Турсунов

Технический редактор:
У. Сапаев

Дизайнер:
Д. Ражапов

Адрес редакции:
100047. Город Ташкент,
улица Сайилгох, 35.
Тел.: (0371) 233-66-36 (1169)

Веб-сайт: review.tsul.uz
E-mail: reviewjournal@tsul.uz

Подписной индекс: 1385.

Издательская лицензия
№ 174625, от 29.11.2023.
Журнал передан в типографию 07.07.2026.
Формат бумаги: А4.
Усл. п. л. 24,2 Тираж: 100 экз.
Номер заказа: 77.

Лицензия типографии
№ 174626, от 29.11.2023.
Отпечатано в типографии Ташкентского государственного юридического университета.
100047, г. Ташкент, ул. Сайилгох, 37.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

FOUNDER: TASHKENT STATE UNIVERSITY OF LAW

"Yuridik fanlar axborotnomasi – Вестник юридических наук – Review of law sciences" legal scientific-practical journal was registered by Press and Information Agency of Uzbekistan on December 22, 2020, with certificate number 0931.

The journal is included in the list of journals of the Supreme Attestation Commission under the Akademy of Sciences of the Republic of Uzbekistan.

Agreed-upon price.

Publication Officer:
O. Choriev

Editors:
E. Mustafaev, E. Yarmolik, M. Sharifova, Sh. Beknazarova, Kh. Yuldasheva, E. Sharipov

Proofreader:
M. Tursunov

Technical editor:
U. Sapaev

Designer:
D. Rajapov

Publishing department address:
100047. Tashkent city,
Sayilgoh street, 35.
Phone: (0371) 233-66-36 (1169)

Website: review.tsul.uz
E-mail: reviewjournal@tsul.uz

Subscription index: 1385.

Publishing license
№ 174625, 29.11.2023.

The journal is submitted to the Printing house on 07.07.2026.
Paper size: A4.
Cond.p.f: 24,2.
Units: 100. Order: № 77.

Printing house license
№ 174626, 29.11.2023.

Published in the Printing house of Tashkent State University of Law.
100047. Tashkent city, Sayilgoh street, 37.

EDITORIAL BOARD

MUNDARIJA

12.00.10 – XALQARO HUQUQ

12.00.14 – HUQUQBUZARLIKLAR PROFILAKTIKASI. JAMOAT XAVFSIZLIGINI TA’MINLASH. PROBATSIYA FAOLIYATI

E-ISSN 2181-1148
ISSN 2181-919X

СОДЕРЖАНИЕ

12.00.10 – МЕЖДУНАРОДНОЕ ПРАВО

12.00.14 – ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПНОСТИ. ОБЕСПЕЧЕНИЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ. ПРОБАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ

E-ISSN 2181-1148
ISSN 2181-919X

CONTENTS

12.00.14 – CRIME PREVENTION. ENSURING PUBLIC SAFETY. PROBATION ACTIVITY

E-ISSN 2181-1148
ISSN 2181-919X

Kelib tushgan / Получено / Received: 05.05.2026
Qabul qilingan / Принято / Accepted: 01.06.2026
Nashr etilgan / Опубликовано / Published: 07.07.2026

DOI: 10.51788/10.51788/10.51788/tsul.rols.2026.10.SI./DAWG1633
UDC: 343:004(045)(575.1)

O‘ZBEKISTONDA KIBERJINOYATLARNING RIVOJLANISHI HAMDA ULARNI TERGOV QILISH MUAMMOLARI

Nodirov Muzaffar Axmadovich,
Toshkent davlat yuridik universiteti
Jinoiy odil sudlov fakulteti dekani o‘rinbosari,
yuridik fanlar bo‘yicha falsafa doktori
ORCID: https://orcid.org/0000-0003-3970-2985
e-mail: m.nodirov@tsul.uz

Usmonov Ibrohim Alisher o‘g‘li,
Toshkent davlat yuridik universiteti
Jinoiy odil sudlov fakulteti
2-bosqich talabasi
ORCID: https://orcid.org/0009-0000-1322-0641
e-mail: usmonov8712@gmail.com

Annotatsiya. *Maqolada kiberjinoyatchilikning zamonaviy jamiyatdagi o‘rni, uning kriminologik, ijtimoiy-iqtisodiy va huquqiy jihatlari kompleks hamda tizimli tahlil qilingan. Mavzuning dolzarbligi kiberjinoyatlarni tergov qilish jarayonida yuzaga kelayotgan muammolar: texnik ta’minotning yetarli emasligi, malakali kadrlar tanqisligi, raqamli dalillarni aniqlash, saqlash va baholashdagi murakkabliklar bilan belgilanadi. Tadqiqot davomida O‘zbekistonda kiberjinoyatlarning rivojlanish dinamikasi, ularning sodir etilish usullari, tarkibiy tuzilmasi hamda yetkazilgan iqtisodiy zarar hajmi rasmiy statistik ma’lumotlar asosida o‘rganilgan. Shuningdek, kiberjinoyatlarning “cyber-dependent” va “cyber-enabled” kabi turlari, ularning ijtimoiy xavflilik darajasi, jumladan, sun’iy intellekt texnologiyalaridan foydalangan holda sodir etilayotgan jinoyatlar atroflicha tahlil etilgan. Maqolada kiberjinoyatchilikning kelib chiqish sabablari psixoanalitik yondashuv hamda kognitiv xulq-atvor nazariyasi asosida ilmiy jihatdan asoslab berilgan. Xalqaro tajriba, xususan, Budapesht konvensiyasi normalari o‘rganilgan va O‘zbekiston Respublikasi milliy qonunchiligi bilan qiyosiy tahlil qilingan. Xulosada kiberjinoyatlarning rivojlanishiga qarshi kurashish va tergov qilish tizimini takomillashtirishga qaratilgan ilmiy asoslangan takliflar, amaliy tavsiyalar ishlab chiqilgan. Tadqiqot natijalaridan kiberxavfsizlikni ta’minlash, huquqni muhofaza qilish organlari faoliyatini takomillashtirish hamda raqamli muhitda huquqbuzarliklarning oldini olishda foydalanish mumkin.*

Kalit so‘zlar: *kiberjinoyatchilik, kiberxavfsizlik, raqamli tergov, kiberfiribgarlik, sun’iy intellekt, raqamli dalillar, kriminologik nazariya, Budapesht konvensiyasi*

РАЗВИТИЕ КИБЕРПРЕСТУПНОСТИ В УЗБЕКИСТАНЕ И ПРОБЛЕМЫ ЕЁ РАССЛЕДОВАНИЯ

Нодиров Музаффар Ахмадович,
доктор философии по юридическим наукам,
заместитель декана факультета уголовного правосудия
Ташкентского государственного юридического университета

Усмонов Иброхим Алишер угли,
студент 2-го курса факультета уголовного правосудия
Ташкентского государственного юридического университета

Аннотация. *В статье комплексно и системно проанализированы место киберпреступности в современном обществе, а также её криминологические, социально-экономические и правовые аспекты. Актуальность темы обусловлена проблемами, возникающими в процессе расследования киберпреступлений, включая недостаточность технического обеспечения, дефицит квалифицированных кадров, а также сложности выявления, хранения и оценки цифровых доказательств. В ходе исследования на основе официальных статистических данных изучены динамика развития киберпреступности в Республике Узбекистан, способы совершения киберпреступлений, их структура и объём причинённого экономического ущерба. Кроме того, подробно проанализированы такие виды киберпреступлений, как киберзависимые (cyber-dependent) и кибероопосредованные (cyber-enabled) преступления, степень их общественной опасности, а также преступления, совершаемые с использованием технологий искусственного интеллекта. В статье причины возникновения киберпреступности научно обоснованы с позиций психоаналитического подхода и теории когнитивного поведения. Изучен международный опыт, в частности положения Будапештской конвенции, и проведён их сравнительный анализ с национальным законодательством Республики Узбекистан. В заключение разработаны научно обоснованные предложения и практические рекомендации, направленные на совершенствование системы противодействия и расследования киберпреступлений. Результаты исследования могут быть использованы для обеспечения кибербезопасности, совершенствования деятельности правоохранительных органов и предупреждения правонарушений в цифровой среде.*

Ключевые слова: *киберпреступность, кибербезопасность, цифровое расследование, кибермошенничество, искусственный интеллект, цифровые доказательства, криминологическая теория, Будапештская конвенция*

THE DEVELOPMENT OF CYBERCRIME IN UZBEKISTAN AND PROBLEMS OF THEIR INVESTIGATION

Nodirov Muzaffar Akhmadovich,
Deputy Dean of the Faculty of Criminal Justice,
Tashkent State University of Law,
Doctor of Philosophy (PhD) in Law

Usmonov Ibrohim Alisher ugli,
2nd-year Student at the Faculty of Criminal Justice,
Tashkent State University of Law

Abstract. *The article provides a comprehensive and systematic analysis of the role of cybercrime in modern society, its criminological, socio-economic, and legal aspects. The relevance of the topic is determined by the problems arising in the process of investigating cybercrimes – insufficient technical support, shortage of qualified personnel, and difficulties in identifying, storing, and evaluating digital evidence. During the study, the dynamics of the development of cybercrime in Uzbekistan, the methods of their commission, the structural structure and the amount of economic damage caused were studied on the basis of official statistical data. Additionally, types of cybercrimes such as "cyber-dependent" and "cyber-enabled," their level of social danger, including crimes committed using artificial intelligence technologies, are analyzed in detail. The article provides a scientific justification for the causes of cybercrime based on a psychoanalytical approach and cognitive-behavioral theory. International experience, in particular, the norms of the Budapest Convention, have been studied and compared with the national legislation of the Republic of Uzbekistan. The conclusion develops scientifically grounded proposals and practical recommendations aimed at improving the system of combating and investigating the development of cybercrime. The research results can be used to ensure cybersecurity, improve the activities of law enforcement agencies, and prevent offenses in the digital environment.*

Keywords: *cybercrime, cybersecurity, digital investigation, cyber fraud, artificial intelligence, digital evidence, criminological theory, Budapest Convention*

Kirish

Internet xizmatlarining tez sur'atlarda rivojlanishi inson hayoti, iqtisodiy faoliyat va davlat institutlari faoliyatini tubdan o'zgartirdi. Statistik ma'lumotlarga ko'ra, 2005-yilda dunyo aholisining atigi 16% internetdan foydalangan

bo‘lsa, 2023-yilga kelib bu ko‘rsatkich 67%ga yetgan (Tila, 2026). Bu o‘sish nafaqat texnologik taraqqiyotni, balki jamiyatning raqamli muhitga to‘liq integratsiyalashuvini ko‘rsatadi. Internet iqtisodiy qiymat yaratdi, bandlikni oshirdi va tranzaksion xarajatlarni kamaytirdi. Shu bilan birga, aynan shu ochiqlik va keng qamrov jinoyatchilik uchun yangi imkoniyatlar maydonini ham yaratdi.

Kiberjinoyatchilik bugungi kunda global iqtisodiyot uchun jiddiy tahdidga aylangan. 2024-yilga kelib kiberjinoyatlar tufayli yetkazilgan zarar trillionlab dollar bilan baholanmoqda. Biroq eng ahamiyatli jihati shundaki, kiberjinoyat faqat davlatlar va korporatsiyalar darajasida emas, balki individual darajada ham chuqur ijtimoiy oqibatlarga ega. Ayniqsa, rivojlanayotgan davlatlarda ishsizlik, tengsizlik va iqtisodiy marginalizatsiya yoshlarni kiberjinoyatchilikka undovchi omil sifatida namoyon bo‘lmoqda. Demak, kiberjinoyatni faqat texnologik xavfsizlik muammosi sifatida emas, balki ijtimoiy tengsizlik va strukturaviy muammolar bilan bog‘liq hodisa sifatida ham ko‘rish zarur.

O‘zbekistonda ham mazkur turdagi jinoyatlar soni yildan yilga ortib bormoqda. Xususan, Ichki ishlar vazirligi tomonidan berilgan axborotda 2023-yilda kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 6,2%ni tashkil etgan bo‘lsa, bu raqam 2024-yilda 44,4 %ga yetganligi, deyarli har ikkita jinoyatning biri axborot texnologiyalari orqali sodir qilinganligi, o‘tgan yili 58 800 ta jinoyat ishi qo‘zg‘atilganligi keltirilgan (Gazeta.uz, 2025).

Metodlar

Tadqiqot bir qator o‘zaro bog‘liq ilmiy metodlar asosida amalga oshirildi. Normativ-huquqiy hujjatlar tahlili yordamida O‘zbekiston Respublikasi Jinoyat kodeksi (Republic of Uzbekistan, 1994), O‘zbekiston Respublikasi Prezidentning 2025-yil 30-apreldagi PQ–153-sonli qarori (President of the Republic of Uzbekistan, 2025) hamda kiberxavfsizlik sohasidagi tegishli qonun hujjatlari tahlil qilindi. Qiyosiy-huquqiy tahlil metodi orqali kiberjinoyatchilikni tartibga soluvchi xalqaro hujjatlar, xususan, 2001-yilda qabul qilingan Budapesht konvensiyasi (Council of Europe, 2001) va bir qator xorijiy davlatlar qonunchiligi o‘rganildi hamda O‘zbekiston milliy qonunchiligi bilan taqqoslandi. Statistik tahlil metodi yordamida O‘zbekiston Ichki ishlar vazirligi Kiberxavfsizlik markazi tomonidan taqdim etilgan 2021–2024-yillar ko‘rsatkichlari, jumladan, kiberjinoyatlarning dinamikasi, sodir etilish usullari va moddiy zarar hajmi miqdoriy jihatdan baholandi. Tadqiqot jarayonida milliy qonun hujjatlari, xalqaro shartnomalar, huquqni muhofaza qilish organlarining rasmiy statistik ma’lumotlari va ilmiy adabiyotlar asosiy manbalar sifatida xizmat qildi.

Natijalar

Tadqiqot doirasida O‘zbekistonda kiberjinoyatchilikning rivojlanish dinamikasi tizimli ravishda tahlil qilindi. Olingan ma’lumotlar kiberjinoyatlarning nafaqat son jihatdan keskin ortib borayotganini, balki ularning tuzilmasi va sodir etilish usullari ham sezilarli darajada transformatsiyaga uchrayotganini ko‘rsatadi. Xususan, 2023–2024-yillar oralig‘ida kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi keskin oshgani raqamli muhitning kriminalizatsiya darajasi yuqorilayotganini tasdiqlaydi. Statistik ko‘rsatkichlar kiberjinoyatlarning asosiy qismi moliyaviy firibgarlik bilan bog‘liqligini, ayniqsa, bank kartalari orqali sodir etiladigan jinoyatlar ustunlik qilayotganini ko‘rsatadi. Bu esa raqamli to‘lov tizimlarining kengayishi bilan birga, ularning xavfsizlik zaifliklaridan faol foydalanilayotganini anglatadi. Tahlil natijalari shuni ham ko‘rsatadiki, kiberjinoyatchilikda yangi tendensiyalar, xususan, sun’iy intellekt texnologiyalaridan foydalangan holda sodir etilayotgan jinoyatlar shakllanib bormoqda.

Yuqoridagi 1-jadval ma’lumotlari kiberjinoyatchilikning O‘zbekistonda qanday tez sur’atlar bilan kengayib borayotganini raqamlar orqali yaqqol namoyon etadi. Mazkur turdagi jinoyat natijasida 2021–2024-yillar mobaynida yetkazilgan jami moddiy zarar 1 trln 909 mlrd so‘mni tashkil etgan bo‘lib, shundan 603 mlrd so‘mi, ya’ni umumiy zararning qariyb 32% faqat 2024-yilda qayd etilgan. Bu holat kiberjinoyatlarning nafaqat sonida, balki ularning iqtisodiy ta’sir ko‘lamida ham keskin o‘sish kuzatilayotganini ko‘rsatadi.

1-jadval

O‘zbekistonda kiberjinoyatchilikning asosiy statistik ko‘rsatkichlari (2021–2024-y.)

Ko‘rsatkich	Qiymat	Davr / Izoh
Jami moddiy zarar	**1 909 mlrd so‘m**	2021–2024-y.
Zarar (2024-yil)	**603 mlrd so‘m**	2024-y.
Kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi	**6,2 %**	2023-y.
Kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi	**44,4 %**	2024-y.
Qo‘zg‘atilgan jinoyat ishlari soni	**58 800 ta**	2024-y.
Bank kartalari bilan bog‘liq kiberjinoyatlar ulushi	**98 %**	Umumiy kiberjinoyatlardan

Ayniqsa, e’tiborga molik ko‘rsatkich – kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi.

2023-yilda bu ulush 6,2 foizni tashkil etgan bo‘lsa, 2024-yilga kelib u 44,4%ga yetgan, ya’ni bir yil ichida taxminan 7 barobarga oshgan. Boshqacha aytganda, 2024-yilda sodir etilgan har ikkita jinoyatdan biri axborot texnologiyalari orqali amalga oshirilgan. Qo‘zg‘atilgan 58 800 ta jinoyat ishi ham ushbu tendensiyani tasdiqlaydi. Bank kartalari bilan bog‘liq kiberjinoyatlarning umumiy kiberjinoyatlardagi ulushining 98 foizga yetgani esa jinoyatchilarning asosiy nishoni moliyaviy-raqamli tizimlar ekanini ko‘rsatib, raqamli to‘lov infratuzilmasining himoya mexanizmlarini zudlik bilan takomillashtirish zaruratini belgilaydi.

2-jadval

Kiberjinoyatlarning sodir etilish usullari bo‘yicha taqsimoti

Ulushi (%)	Sodir etilish usuli	Mexanizm
60	Zararli havolalar va dasturlar yuborish	Bank kartasi yoki qurilma boshqaruvini egallash
16	Soxta qo‘ng‘iroqlar orqali SMS-kod o‘g‘irlash	Bank ilovasi va karta boshqaruvini qo‘lga kiritish
11	Onlayn savdo platformalaridagi firibgarlik	“OLX.uz”, “Olcha” va boshqa platformalar orqali aldash
9	Soxta elektron birja va onlayn treyding	Qiziqtirish orqali mablag‘ o‘tkazdirib olish
4	Noqonuniy onlayn kredit rasmiylashtirish	O‘zgalar nomiga kredit olish
31	*Dipfeyk* (sun‘iy intellekt orqali soxta video hamda rasmlar)	Insonlar qiyofasidan foydalanib onlayn kredit rasmiylashtirish

2-jadval kiberjinoyatlarning sodir etilish usullari bo‘yicha taqsimotini aks ettiradi va jinoyatchilar qo‘llayotgan metodlarning xilma-xilligidan darak beradi. Ular ichida eng keng tarqalgan usul zararli havolalar va dasturlar yuborish orqali bank kartasi yoki qurilma boshqaruvini egallash bo‘lib, u umumiy kiberjinoyatlarning 60 foizini tashkil etadi. Bu usulning bunday keng qo‘llanishi foydalanuvchilarning raqamli savodxonligi va kibergigiyena ko‘nikmalarining hali yetarli darajada shakllanmaganidan dalolat beradi.

Ikkinchi o‘rinda soxta qo‘ng‘iroqlar orqali SMS-kodlarni olish usuli turadi (16 %). Onlayn savdo platformalaridagi firibgarlik (11%) va soxta elektron birja hamda onlayn treyding (9%) holatlari esa raqamli savdo muhitidagi ishonchning yo‘qolishiga olib keladi. Jadvalda sun’iy intellekt texnologiyasi asosidagi *dipfeyk* usuli (31%) alohida ko‘rsatilgan. Bu esa kiberjinoyatlar zamonaviy texnologiyalar bilan hamohang rivojlanayotganini anglatadi.

E-ISSN 2181-1148
ISSN 2181-919X

Fikrimizcha, amaliyotda sun'iy intellekt texnologiyasi asosidagi dipfeyk usulining kengayishi huquqni muhofaza qiluvchi organlardan jinoiy maqsadda generatsiya qilingan biometrik ma'lumotlarni (ovoz va tasvir) haqiqiysidan ajratish uchun o'ta yuqori texnik ekspertizani talab qiladi.

Muhokama

Kiberjinoyatlar kompyuter tizimlari, tarmoqlar va boshqa raqamli texnologiyalardan foydalanib sodir etiladigan jinoyatlar bo'lib, ular shaxsiy, korporativ yoki davlat ma'lumotlariga zarar yetkazishi mumkin. Kiberjinoyat tushunchasi ko'pincha kompyuter orqali sodir etiladigan jinoyat, raqamli jinoyat, texnologik jinoyat, elektron jinoyat, shuningdek, "cyber dependent crime" kabi atamalar bilan o'zaro almashtirib qo'llanadi. Olimlar kiberjinoyatni odatda kompyuterlar, internet yoki smartfonlar kabi zamonaviy texnologiyalar yordamida sodir etiladigan har qanday jinoiy xatti-harakat sifatida ta'riflaydi (Onwuadiamu, 2025). Kiberjinoyatlar asosan ikki kategoriya bo'yicha tasniflanadi. Birinchi guruh, ya'ni "cyber-dependent crimes" faqat raqamli texnologiyalar orqali yuz beradigan jinoyatlar bo'lib, virus va zararli dasturlarni tarqatish, ruxsatsiz kirish (*hacking*), DDoS hujumlar va ma'lumotlar manipulyatsiyasini o'z ichiga oladi. Ikkinchi guruh, ya'ni "cyber-enabled crimes" an'anaviy jinoyatlarning internet orqali kengaytirilgan shakli bo'lib, firibgarlik, fishing (*phishing* – aldov yo'li bilan foydalanuvchilarning maxfiy ma'lumotlarini qo'lga kiritish), shaxsiy ma'lumotlarni o'g'irlash, moliyaviy firibgarlik va tahdidlar kabi jinoyatlarni o'z ichiga oladi. Shuningdek, manbalarda kiberjinoyatlar boshqa jihatlarga qarab ham farq qilishi mumkin.

Bolalar pornografiyasi – noqonuniy onlayn pornografiya voyaga yetmaganlarning jinsiy faoliyatga jalb etilishini o'z ichiga oladi. Bunday noqonuniy faoliyatga bolalarni pornografik mahsulotlar yaratishda ishtirok ettirish, jinsiy ko'rgazmalar, fohishalik, jinsiy qullik, tasvir va videolarni tarqatish, chatlar, tanishuv saytlari, "Webcam Child Sex Tourism (WCST)", jinsiy o'yinchoqlar, telefon orqali jinsiy xizmatlar va jinsiy shoular kiradi. Pornografiya bilan shug'ullanuvchilar voyaga yetmaganlar tasvirini boshqa tasvirlar bilan birlashtirish uchun raqamli dasturlardan foydalanadi – bu "morphing" deb ataladi.

Intellektual mulkka qarshi kiberhuquqbuzarliklar – patentlar, tijorat sirlari, tovar belgilari va mualliflik huquqlarini buzuvchi har qanday kiberhuquqbuzarlik. Bu turdagi jinoyatlar tarmoqlar va kompyuter xavfsizligi bilan bog'liq bo'lib, dasturiy ta'minot, ma'lumotlar bazalari, raqamli kontent, algoritmlar va xom ma'lumotlarni ham qamrab oladi.

Kiberbulling – aloqa texnologiyalari orqali shaxslarni tahqirlash yoki bezovta qilish. Asosan bolalar va o'smirlarga ta'sir qiladi. Turlari: kibershantaj, uyatsiz tasvirlarni tarqatish, tahdid qilish, masxara qilish, jabrlanuvchi nomidan chiqish.

Kibershpionaj ma'lumotlarni noqonuniy qo'lga kiritish, kuzatish va o'g'irlash. Josuslar spayver (*spyware* – josus dasturlar, kilogger (*keylogger* – klaviatura tugmalarini qayd qiluvchi yashirin dastur) trafikni kuzatish va kommunikatsiyani monitoring qilish vositalaridan foydalanadi. Kibershantaj – jabrlanuvchini zarar yetkazish bilan qo'rqitib, moliyaviy foyda talab qilish. Ko'pincha tovlamachilik dasturlari – *ransomware* orqali bitcoin to'lov talab qilinadi.

Raqamli texnologiyalar orqali firibgarlik. Masalan: onlayn auksionda, aksiyalar bilan bog'liq firibgarlik, kredit karta firibgarligi, soxta reklama, lotereya firibgarligi, SMS firibgarligi va boshqalar. Kibergruming (*cyber-grooming* – pedofilning jabrlanuvchi bilan ishonchli munosabat o'rnatib, asta-sekin jinsiy ekspluatatsiyaga o'tishi. Kibertalonchilik *(cyberheist)* – banklar yoki moliyaviy institutlardan keng ko'lamli o'g'irlik. Zararli dasturiy ta'minot (*malware)*, fishing usullari qo'llanadi. Pul yuvish (*cyberlaundering*) – jinoiy mablag'larni elektron to'lov tizimlari va raqamli pul orqali legallashtirish. Kiberterrorizm – jamiyat infratuzilmasiga zarar yetkazish maqsadida kompyuter tizimlaridagi zaifliklardan foydalanish. Sabablari siyosiy, diniy yoki shaxsiy bo'lishi mumkin. Fishing (*phishing*) – soxta vebsaytlar orqali maxfiy ma'lumotlarni qo'lga kiritish jarayoni (Sabillon et al., 2016).

Kiberjinoyatlarning tarkibi ijtimoiy va iqtisodiy xavflilik darajasiga ko'ra turlicha ko'rinishga ega. Xususan, moliyaviy firibgarliklar, kibershantaj (*ransomware*) va kibero'g'riliklar (*cyberheist*) global iqtisodiyotga sezilarli zarar yetkazayotgan bo'lsa, kibershpionaj va kiberterrorizm davlat xavfsizligi va infratuzilmasiga jiddiy tahdid

solmoqda. Shuningdek, shaxsning huquq va erkinliklariga qarshi qaratilgan kiberbulling, kibergruming hamda voyaga yetmaganlarning ekspluatatsiyasi bilan bog‘liq jinoyatlar raqamli muhitda inson huquqlarini himoya qilish tizimini takomillashtirishni talab etadi. Intellektual mulk obyektlariga qarshi kiberhuquqbuzarliklar esa raqamli iqtisodiyotda mualliflik huquqi va patentlarni himoya qilish mexanizmlarining zaifligini ko‘rsatmoqda. Kiberjinoyatchilikka qarshi kurashish nafaqat texnologik choralarni, balki jinoiy-huquqiy normalarni ushbu dinamik o‘zgaruvchan tahdidlarga moslashtirishni taqozo etadi.

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va raqamli makonning globallashuvi natijasida kiberjinoyatchilik transmilliy va chegarasiz xususiyat kasb etdi. Internet tarmog‘i orqali sodir etilayotgan huquqbuzarliklar bir vaqtning o‘zida bir nechta davlat hududini qamrab olishi, jinoyatchi va jabrlanuvchining turli yurisdiksiyalarda joylashishi bilan murakkablashmoqda. Shu bois kiberjinoyatlarga qarshi samarali kurashish faqat milliy qonunchilik doirasida emas, balki xalqaro hamkorlik va yagona huquqiy mexanizmlarni shakllantirishni talab etadi. Aynan shu zarurat xalqaro miqyosda kiberjinoyatchilikning oldini olish, jinoyatlarni tergov qilish va davlatlar o‘rtasida huquqiy yordamni ta’minlashga qaratilgan bir qator konvensiyalar va normativ-huquqiy hujjatlarning qabul qilinishiga asos bo‘ldi. Ushbu xalqaro hujjatlarning eng muhimlaridan biri 2001-yilda qabul qilingan Kiberjinoyatlar to‘g‘risidagi Budapesht konvensiyasi (*Convention on Cybercrime*) hisoblanadi. Budapesht konvensiyasi (Council of Europe, 2001) shunchaki huquqiy hujjat emas; u ishtirokchi davlatlarning yuzlab mutaxassislariga o‘zaro tajriba almashish va ushbu konvensiyada ko‘zda tutilgan muayyan qoidalardan tashqari, xususan, favqulodda vaziyatlarda hamkorlikni osonlashtiradigan aloqalarni o‘rnatish imkonini beruvchi tizimdir. Istalgan davlat Budapesht konvensiyasidan yo‘riqnoma, nazorat ro‘yxati (*check list*) yoki namunaviy qonun sifatida foydalanishi mumkin. Bundan tashqari, ushbu shartnomaga a’zo bo‘lish qo‘shimcha afzalliklarni ham taqdim etadi. Qozog‘iston Respublikasiga Budapesht konvensiyasiga qo‘shilish taklif qilindi (Council of Europe, 2023), ammo mamlakatda u hali ratifikatsiya qilinmagan.

Konvensiya (Council of Europe, 2001) jinoyat tarkiblarini uyg‘unlashtirish tamoyiliga asoslanadi. U o‘zining normalari orqali ishtirokchi davlatlardan milliy qonunchilikda quyidagi xatti-harakatlarni jinoyat deb belgilashni talab qiladi: kompyuter tizimlariga noqonuniy kirish (*illegal access*) (Budapesht konvensiyasining, 2-moddasi), ma’lumotlarni noqonuniy qo‘lga kiritish (*illegal interception*, (3-modda), ma’lumotlarga zarar yetkazish (*data interference*, (4-modda), tizim faoliyatiga aralashish (*system interference*, (5-modda), qurilmalar va dasturlarni noqonuniy qo‘llash (*misuse of devices*, (6-modda), kompyuter orqali firibgarlik va qalbakilashtirish (6-modda), shuningdek, bolalar pornografiyasi bilan bog‘liq jinoyatlar (9-modda). Shu bilan birga, konvensiya protsessual-huquqiy mexanizmlarni belgilaydi. Jumladan, elektron dalillarni saqlab qolish (*preservation of stored data*), tezkor ravishda trafik ma’lumotlarini saqlash, kompyuter tizimlarini tintuv qilish va ma’lumotlarni musodara qilish, real vaqt rejimida trafikni kuzatish kabi choralar nazarda tutilgan. Bu normalar raqamli dalillarning tez yo‘qolib ketish xususiyatini inobatga olgan holda ishlab chiqilgan. Qolaversa, konvensiya xalqaro hamkorlikni kuchaytirishga alohida e’tibor qaratadi. Unda ekstraditsiya, o‘zaro huquqiy yordam, tezkor aloqa kanallari orqali axborot almashish mexanizmlari belgilangan. Kiberjinoyatlarning transmilliy tabiati aynan shunday muvofiqlashtirilgan hamkorlikni talab etadi.

Budapesht konvensiyasi ochiq va global xarakterga ega. U nafaqat Yevropa davlatlari, balki boshqa mintaqa mamlakatlari uchun ham ochiq bo‘lib, bugungi kunda ko‘plab davlatlar tomonidan ratifikatsiya qilingan.

O‘zbekiston Respublikasi Jinoyat kodeksi ham konvensiya talablariga qisman mos keladi. Biroq konvensiyaning 16–21-moddalarida nazarda tutilgan protsessual mexanizmlar: raqamli dalillarni tezkor saqlash majburiyati, real vaqt rejimida trafikni kuzatish va xalqaro tezkor ma’lumot almashish tartibi O‘zbekiston qonunchiligida hali to‘liq mustahkamlanmagan.

Kiberjinoyatlarni tergov qilishdagi amaliy muammolarning asosi aynan shu bo‘shliq bilan bog‘liq. Raqamli dalillarning tez yo‘qolib ketish xususiyatini inobatga olsak, ularni saqlash muddati va qonuniy jihatdan tartibga soluvchi alohida protsessual normalar mavjud bo‘lmaganda tergov

E-ISSN 2181-1148
ISSN 2181-919X

samaradorligi sezilarli darajada pasayadi. Shu sababli konvensiya normalarining milliy qonunchilikka integratsiya qilinishi yoki kamida ularga muvofiq protsessual qoidalarning alohida qonun bilan mustahkamlanishi maqsadga muvofiq, deb hisoblaymiz.

Kiberjinoyatlar tahlil qilinar ekan, jinoyatchilarning xulq-atvori, ularni jinoyat sodir etishga undagan sabablarni o‘rganish alohida ahamiyatga ega. Ijtimoiy o‘rganish nazariyasiga ko‘ra, insonlar yangi xulq-atvorni ijtimoiy muhitni kuzatish orqali o‘rganadilar. Kiberjinoyatchilik kontekstida bu onlayn guruhlar va tengdoshlarning ta’sirini anglatadi. Shaxs boshqalarning kiberhujumlari muvaffaqiyatli chiqqanini yoki foyda keltirganini ko‘rsa, ularga taqlid qilishga moyil bo‘ladi. Psixoanalitik nazariyada insonning ongsiz istaklari, ichki nizolari hamda “ID”, “Ego” va “Superego” o‘rtasidagi muvozanatga e’tibor qaratiladi. Kiberjinoyat bu yerda ichki muammolar, jinoyat sodir etayotgan shaxsning qondirilmagan mayllarini namoyon qilish, vaziyatni nazorat ostiga olish yoki o‘zini tasdiqlash vositasi sifatida ko‘riladi. Virtual olamdagi anonimlik shaxsdagi yashirin va qachondir e’tiborga olinmagan his-tuyg‘ularning yuzaga chiqishiga yo‘l ochadi. Ya’ni jinoyat sodir etayotgan shaxs o‘zining harakatlarini tushunadi, raqamli muhitda anonimlik orqali o‘zining barcha xohishlarini namoyon qiladi. Kognitiv xulq-atvor nazariyasiga ko‘ra, kiberjinoyat sodir etgan shaxslar ko‘pincha oson daromad topish va “yo‘qolib qolish” imkoniyati haqidagi noto‘g‘ri xulosaga boradi. Shuningdek, eng muhim jihatlaridan biri shundaki, real hayotda har doim huquq doirasida yashagan shaxslar kibermakonda anonimlik va nazorat kamligi sababli huquqbuzarliklarni amalga oshiradi (Raed et al., 2024, p. 263).

Kiberjinoyatlarni tahlil qilishda shaxsning psixologik xususiyatlari, ijtimoiy muhiti va fikrlash jarayonlari muhim omil hisoblanadi. Jinoyatchining xulq-atvori ko‘pincha u yashayotgan yoki faoliyat yuritayotgan ijtimoiy muhit ta’sirida shakllanadi. Shuningdek, kiberjinoyat ayrim hollarda shaxsning ichki psixologik ehtiyojlari, o‘zini tasdiqlash istagi yoki nazorat hissini boshdan kechirishga intilishi bilan bog‘liq bo‘lishi mumkin. Bundan tashqari, kiberjinoyatchilar o‘z harakatlarini oson daromad olish, anonim qolib, javobgarlikdan qochish kabi noto‘g‘ri tasavvurlar orqali oqlashga moyil bo‘ladilar. Ayniqsa, real hayotda huquq doirasida yashagan shaxslar ham kibermakonda anonimlik va aniqlanish ehtimolining pastligi sababli huquqbuzarlik sodir etishga jur’at topishi mumkin.

COVID-19 pandemiyasi, moliyaviy inqiroz va masofaviy ishga o‘tish kiberjinoyatlarning, ayniqsa, ijtimoiy muhandislikdan foydalangan holda moliyaviy firibgarliklarning keskin ko‘payishiga olib keldi (Rossiyada 2020-yilda kredit tashkilotlari mijozlarining hisob raqamlariga kiberhujumlar 2019-yilga nisbatan 88 %ga oshgan (Central Bank of the Russian Federation, 2021). Shu bilan birga, feyk kompensatsiyalar, soxta vaksinalar va dorilar savdosi kabi yangi turdagi kiberfiribgarliklar yuzaga keldi.

COVID-19 pandemiyasi kiberjinoyatchilarning ish uslublariga ta’sir qilgan: qurbonlarning ko‘rsatishicha, jinoyatlarning muhim qismi, ayniqsa, onlayn firibgarlik holatlarida aynan COVID-19 pandemiyasi bilan bog‘liq bo‘lgan (Weijer et al., 2024, p. 10).

Keltirilgan kriminologik va psixologik nazariyalarni milliy kontekstda baholar ekanmiz, fikrimizcha, O‘zbekistonda kiberjinoyatchilikning o‘sishiga faqatgina virtual anonimlik emas, balki real hayotdagi iqtisodiy va ijtimoiy omillar ham jiddiy ta’sir ko‘rsatmoqda. Xususan, raqamli infratuzilmaning jadal rivojlanishi aholining huquqiy va raqamli madaniyati darajasidan o‘zib ketdi. Binobarin, kiberjinoyatchilarning xulqini kognitiv xulq-atvor nazariyasi doirasida tahlil qilganda milliy qonunchilikda jazo muqarrarligi mexanizmlarini virtual makonda ham xuddi real hayotdagidek qat’iy ta’minlash choralari yetarli emas, degan xulosaga kelamiz.

Kiberjinoyatchilikka qarshi samarali kurashish bugungi kunda huquqni muhofaza qiluvchi organlar oldida turgan eng murakkab vazifalardan biridir. Raqamlashtirish jarayonining jadallashuvi, davlat boshqaruvi, bank-moliya tizimi va kundalik ijtimoiy munosabatlarning internet makoniga ko‘chishi kiberjinoyatlarning ko‘lamini kengaytirdi. Bunday sharoitda samaradorlikni oshirish uchun bir qator tizimli muammolarni hal etish zarur.

Avvalo, texnik jihozlash masalasi alohida ahamiyatga ega. Kiberjinoyatlarni tergov qilish an’anaviy jinoyatlardan farqli ravishda moddiy emas, balki raqamli dalillar bilan ishlashni talab etadi. Shu sababli huquqni muhofaza qiluvchi or-

ganlar zamonaviy texnik vositalar majmuasi bilan ta’minlanishi lozim. Bu vositalar kompyuter-texnik ekspertizalarni (apparat, dasturiy, tarmoq darajasida) o‘tkazish, ma’lumotlarni tiklash, zararli dasturlarni tahlil qilish hamda yuridik ahamiyatga ega dalillar bazasini shakllantirish imkonini berishi kerak. Raqamli dalillar tez yo‘qolishi yoki o‘zgartirilishi mumkinligi sababli tezkorlik va aniqlik muhim omil hisoblanadi. Bundan tashqari, kiberjinoyatlar monitoringi, kiberrazvedka va kibertahdidlarni tahlil qilish tizimini yo‘lga qo‘yish zarur.

Yana bir asosiy muammo kadrlar salohiyati bilan bog‘liq. Kiberjinoyatlarni fosh etish va tergov qilish yuqori darajadagi texnik bilim va ko‘nikmalarni talab etadi. Amaliyot shuni ko‘rsatadiki, ko‘plab tergovchilar va tezkor xodimlarning AT-texnologiyalar sohasidagi bilimlari yetarli darajada emas. Faqat ofis dasturlaridan foydalanish yoki internet xizmatlarini bilish kiberjinoyatni ochish uchun yetarli emas. Tergovchi tarmoq arxitekturasi asoslarini, raqamli izlar tabiatini, ma’lumotlarni tiklash usullarini va ekspert xulosalarini baholash mezonlarini tushunishi lozim. Texnologiya rivojlanib borar ekan va jinoyatchilar kiberjinoyatlarni sodir etishning yangi usullarini ishga solar ekan, huquqni muhofaza qiluvchi organlar ham bilim, ko‘nikma va ekspertiza jihatidan ular bilan hamqadam bo‘lishi shart. Kiberjinoyatlarga javob berish bo‘yicha an’anaviy tergov modellari ko‘pincha murakkab kibermuhitda samarali emas, degan fikrlar mavjudligi bu vaziyatni yanada murakkablashtiradi. Huquqni muhofaza qilish organlari duch keladigan muammolar va qiyinchiliklar spektrini hisobga olganda, kiberjinoyatlarni tergov qilish oddiy politsiya kuchlari tomonidan samarali tarzda amalga oshirilishi qiyin va murakkab vazifa bo‘lishi mumkin. Shu sababli keng qamrovli hamkorlik va sheriklik ishlari huquqni muhofaza qilish jamoasi orasida kiberjinoyatlarga samarali javob berish uchun muhim deb e’tirof etilmoqda (Hunton, 2011). Xorijiy tajribada murakkab kiberjinoyatlarni tergov qiluvchi xodimlarning yuridik va texnik yo‘nalish bo‘yicha ikki oliy ma’lumotga ega bo‘lishi maqsadga muvofiq deb hisoblanadi. Bu esa tergovchiga AT-mutaxassislarga aniq vazifa qo‘yish, ularning xulosalarini mustaqil tahlil qilish va sud jarayonida asosli pozitsiya bildirish imkonini beradi. Shuningdek, doimiy ravishda malaka oshirish va qayta tayyorlash tizimini yo‘lga qo‘yish zarur, chunki texnologiyalar tez sur’atlarda yangilanib bormoqda.

Xorijiy tajribada kiberjinoyatlarni tergov qilishning ikki usuli alohida keltiriladi. Ularning biri an’anaviy tergov bo‘lsa, ikkinchisi – raqamli tergov. Kiberjinoyatchilar ham raqamlar va domenlar o‘rtasida qandaydir izlarni qoldirib ketadilar va aynan shular jinoyatni ochishda muhim ahamiyatga ega.

An’anaviy tergov – uzoq vaqt davomida shakllangan jarayon bo‘lib, adolatni ta’minlashga qaratilgan bir qator muhim bosqichlarni o‘z ichiga oladi. Ushbu usulning asosiy elementi gumondorlarni tizimli kuzatish, ular bilan aloqa va so‘roq qilishdir. Bu elementlar jinoyatchini qo‘lga olish jarayonida muhim rol o‘ynaydi. Gumondorning jinoiy xatti-harakatlarini batafsil tahlil qilish orqali huquqni muhofaza qilish organlari jinoyat tafsilotlarini aniqlash va gumondor harakatlaridagi sabablarni tushunish uchun asos yaratadi. Bundan tashqari, tergov orqali gumondorning oldingi qilmishlari, shaxslararo munosabatlari va butun faoliyati batafsil o‘rganiladi. Texnologiya va forensika metodlaridagi yutuqlarga qaramay, an’anaviy tergov texnikalarining asosiy tamoyillari barqarorligicha qoladi.

Raqamli tergov jarayoni raqamli forensika tamoyillariga asoslanib, turli raqamli artefaktlardan dalillarni tizimli ravishda chiqarishni o‘z ichiga oladi. Ushbu jarayon maxsus bilim va jihozlarni talab qiladi va odatda huquqni muhofaza qiluvchi organ xodimlari tomonidan qo‘llanadigan an’anaviy ma’lumot yig‘ish, saqlash usullaridan farq qiladi. Raqamli tergovning asosiy maqsadi ikki qirrali: birinchidan, jinoyatga aloqador shaxsni aniqlash, ikkinchidan, jinoyat ishini ochishga xizmat qiladigan dalillarni taqdim etishdir. Jinoyatlarni sodir etishga imkon beradigan texnologiya nazorat va monitoring vazifalarida ham ishlatilishi mumkin. Kiberjinoyat sohasida raqamli artefaktlar muhim axborot manbayi hisoblanadi. Shu sababli raqamli tergovdan samarali foydalanish dalillarni aniqlik bilan to‘plash va ishlarni muvaffaqiyatli hal qilishda muhim ahamiyatga ega (Sarkar & Shukla, 2023, p. 16).

Kiberjinoyatlar turlari, ularni tergov qilish hamda muammolarini tahlil qilish barobarida kiberjinoyatlarning oldini olish va uning jabrlanuvchisi bo‘lib qolmaslik uchun nimalar qilish lozim-

E-ISSN 2181-1148
ISSN 2181-919X

ligini ham keltirish lozim. Avvalo, kiberjinoyatlarning oldini olish uchun foydalanuvchilarning xabardorligini oshirish zarur. Kiberjinoyatlarga qarshi kurashishda o‘rnatilgan xavfsizlik tizimlaridan foydalangan holda foydalanuvchilarni xabardor qilish va ularni ma’lumotlarni himoya qilish bo’yicha maxsus o‘qitish katta o‘rin tutadi. Kiberjinoyatlarning oldini olish uchun tizimli yondashuvlar, jumladan, yaxshilangan xavfsizlik protokollari, global qonunchilik va foydalanuvchilarning onlayn xavfsizligini oshirish bo‘yicha choralar samarali hisoblanadi. Kiberxavfsizlikning texnologik, huquqiy va ijtimoiy jihatlarini birlashtirgan yondashuvlar muhim ahamiyatga ega. Ayniqsa, kiberjinoyatlar bilan kurashishda yirik kompaniyalar va davlatlar o‘rtasidagi hamkorlikni kuchaytirish zarurati ortib bormoqda. Kiberjinoyatlar nafaqat individual shaxslar, balki kompaniyalar va davlatlar uchun jiddiy xavf tug‘dirmoqda (Kodirov & Tursunova, 2025). Shuningdek, kiberxavfsizlik bo‘yicha qattiq standartlar joriy etish – korxona va tashkilotlar uchun minimal xavfsizlik talablarini belgilash, IoT (*Internet of Things* – Buyumlar interneti) qurilmalarini ishlab chiqaruvchi kompaniyalar uchun esa qattiq xavfsizlik me’yorlarini joriy etish lozim.

Xorijiy mamlakatlarning kiberxavfsizlik sohasidagi ilg‘or tajribasini o‘rganish asnosida shuni ta’kidlashimiz lozimki, O‘zbekistonda kiberjinoyatlarning oldini olish tizimi proaktiv (oldindan ogohlantiruvchi) emas, balki reaktiv (jinoyat sodir bo‘lib bo‘lgandan keyin harakat qiluvchi) xarakterga ega. Muallif sifatida taklif qilamizki, profilaktika samaradorligini oshirish uchun tijorat banklari va to‘lov tizimlari zimmasiga shubhali tranzaksiyalarni avtomatik ravishda bloklash bo‘yicha majburiyat yuklanishi shart. Kibermakonda profilaktika faqatgina raqamli va avtomatlashgan nazorat orqali real natija berishi mumkin.

Ilmiy tadqiqotlarni qo‘llab-quvvatlash – kiberxavfsizlik bo‘yicha ilmiy tadqiqotlar va yangi texnologik yechimlarni yaratish uchun davlat va xususiy sektor hamkorligini kuchaytirish kerak (Siroyev, 2025). Qolaversa, buzib kirishning murakkabligi turli xavfsizlik choralarini joriy qilish orqali yuzaga keladi, jumladan, kirish nazorati, tarmoqlararo ekran (*firewall)*lar, buzilishlarni aniqlash/oldini olish tizimlari, ko‘p bosqichli autentifikatsiya (MFA), tarmoqni segmentlash va sezgir ma’lumotlarni himoya qilish uchun “demilitarizatsiya qilingan zonalar”ni tashkil etish (Sarkar & Shukla, 2024, p. 11) samarali choradir.

Xorijiy manbalarda kompaniya va tashkilotlar uchun ham kiberhujumlar orqali yetkazilishi mumkin bo‘lgan ziyonlarni bartaraf etish uchun yetarli shart-sharoitlar yaratish lozimligi keltiriladi. Masalan, ma’lumotlarni himoya qilishda yuqori darajadagi kirish ehtiyojiga ega shaxslarni belgilab olish lozim, bu jarayonlar va texnologiyalarni himoya qilishda muhim. Kirish huquqlarini berishda qat’iy choralar qo‘llanadi, bu esa texnik infratuzilmaga tahdidlarni kamaytiradi (Tubaishat & AlAleeli, 2024).

Davlat-xususiy sheriklik kiberxavfsizlikni yaxshilashda samarali bo‘lishi mumkin. Hukumat kiberxavfsizlik siyosati va tashabbuslarini ishlab chiqish va amalga oshirish uchun xususiy sektor bilan hamkorlik qilishi kerak (Primov, 2024). Ushbu vositalar orqali muqarrar hujumlarning oldi olinib qolishi mumkin. Kiberxavfsizlik sohasida yuqori natijalarga erishgan mamlakatlar bir necha asosiy tamoyillarga amal qiladilar: zamonaviy va moslashuvchan qonunchilik, maxsus tuzilmalar va yuqori malakali kadrlar, texnologik kompaniyalar bilan hamkorlik, xalqaro standartlarga muvofiqlik va proaktiv yondashuv. O‘zbekiston uchun ushbu tajribadan o‘rganish va milliy xususiyatlarni inobatga olgan holda eng yaxshi amaliyotlarni joriy etish muhim ahamiyatga ega (Makhmudov, 2025).

Shu o‘rinda, O‘zbekiston Respublikasining qonunchiligida mazkur turdagi jinoyatlar uchun jazo tayinlash masalasi hamda kiberjinoyatlarni tergov qilish amaliyotini, bu borada amalga oshirilgan ishlarni ham keltirish lozim. O‘zbekiston Respublikasi Jinoyat kodeksining XX[1] bobi aynan “Axborot texnologiyalari sohasidagi jinoyatlar” deb nomlanadi hamda o‘zida to‘qqizta moddani qamrab oladi (Republic of Uzbekistan, 1994). Unda axborotlashtirish qoidalarini buzish, kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish, kompyuter tizimidan, shuningdek, telekommunikatsiya tarmoqlaridan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish, kompyuter axborotini modifikatsiyalashtirish, kompyuter sabotaji, zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish, telekommu-

nikatsiya tarmog‘idan qonunga xilof ravishda (ruxsatsiz) foydalanish, kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzish, mayning faoliyatini qonunga xilof ravishda amalga oshirish kabi qilmishlar uchun jinoiy javobgarlik belgilangan. Yuqorida sanalganlarning ba’zilari kompyuter tizimlariga oflayn tarzda shikast yetkazishni nazarda tutsa, zararli dasturlar yaratish kabi normalar aynan virtual muhitda sodir etiladigan qilmishlarni nazarda tutadi. Qolaversa, O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ–153-sonli qarori (President of the Republic of Uzbekistan, 2025) bilan Markaziy bank, Ichki ishlar vazirligi, Bosh prokuratura, Davlat xavfsizlik xizmati kabi huquqni muhofaza qiluvchi organlar zimmasiga bir nechta muhim vazifalar yuklatildi. Unga ko‘ra, shubhali pul o‘tkazma amaliyotlariga aloqador bank kartalari haqidagi ma’lumotlarni zudlik bilan ichki ishlar organlari mas’ul bo‘linmalariga taqdim etiladi va agar ular so‘rov kiritsa bank kartasi bloklanadi; prokuratura tuzilmasida kiberjinoyatlarga qarshi kurashishda qonuniylikni ta’minlash yo‘nalishida tashkil etilayotgan tuzilmalar xodimlarini 2025-yil 1-iyulga qadar Huquqni muhofaza qilish akademiyasida maxsus qayta tayyorlash kurslarida o‘qitiladi. Mazkur qaror bilan Huquqni muhofaza qilish akademiyasi Raqamli kriminalistika ilmiy-tadqiqot instituti tuzilmasida Kiberjinoyatlarga qarshi kurashishga va raqamli tergovga ko‘maklashish markazi tashkil etilgan. Markaz kiberjinoyatlarni fosh etish va ularni tergov qilish amaliyotidagi mavjud muammolarni aniqlash va ularni bartaraf etish bo‘yicha ilmiy asoslantirilgan takliflarni ishlab chiqish, kiberjinoyatlar yo‘nalishida tergov faoliyati samaradorligini oshirish hamda ta’lim jarayonini takomillashtirishni ilmiy va uslubiy jihatdan ta’minlash kabi muhim vazifalarni amalga oshiradi.

Xulosa

Mazkur tadqiqot kiberjinoyatchilikning O‘zbekistonda miqdor va sifat jihatdan tubdan o‘zgarib borayotganini ko‘rsatadi. 2023-yilda umumiy jinoyatchilikdagi ulushi 6,2 %ni tashkil etgan kiberjinoyatlar 2024-yilga kelib 44,4 %ga yetgan. Bir yilda 58 800 ta jinoyat ishining qo‘zg‘atilishi va moddiy zararning 603 mlrd so‘mga yetgani muammoning ijtimoiy-iqtisodiy ko‘lamini yaqqol namoyon etadi (Gazeta.uz, 2025).

Tadqiqot davomida kiberjinoyatlarning tarkibiy tahlili shuni ko‘rsatdiki, sodir etilgan jinoyatlarning 98% bank kartalari bilan bog‘liq, eng ko‘p qo‘llanadigan usul esa zararli dasturlar va havolalar orqali moliyaviy ma’lumotlarni o‘g‘irlashdir. Bundan tashqari, sun’iy intellekt texnologiyalari asosidagi dipfeyk usulidan foydalangan holda sodir etilayotgan jinoyatlarning 31% lik ulushi alohida tashvish uyg‘otadi. Bunday jinoyatlar an’anaviy tergov usullari orqali fosh etilishi qiyin bo‘lib, maxsus texnik bilim va jihozlarni talab etadi.

Jinoyatchilarning xulq-atvorini psixoanalitik va kognitiv xulq-atvor nazariyalari asosida tahlil qilish esa muhim xulosaga olib keldi: kibermakondagi anonimlik va aniqlanish ehtimolining pastligi shaxsni jinoiy xatti-harakatga undovchi asosiy omillar hisoblanadi. Ayniqsa, real hayotda qonunlarga amal qilib yashaydigan shaxslar ham raqamli muhitda anonim bo‘lgani bois huquqbuzarlik sodir etishga moyil bo‘ladi.

Tergov amaliyotida uchraydigan muammolar ham tadqiqotda keltirildi. Texnik infratuzilmaning yetarli emasligi, malakali kadrlar tanqisligi va raqamli dalillarni protsessual talablar doirasida to‘g‘ri olish, saqlash hamda baholash mexanizmlarining hali to‘liq shakllanmagani tergov samaradorligiga salbiy ta’sir ko‘rsatmoqda. Raqamli dalilning o‘ziga xos xususiyati shundaki, u moddiy izdan farqli ravishda bir zumda yo‘q qilinishi yoki o‘zgartirilishi mumkin. Shu sababli dalillarni zudlik bilan olish ham operativ, ham huquqiy jihatdan zarur talabga aylanishi lozim.

Budapesht konvensiyasi normalari (Council of Europe, 2001) bilan O‘zbekiston Respublikasi milliy qonunchiligi o‘rtasida tahlil amalga oshirilganda farqlarni anglash mumkin. Konvensiyada nazarda tutilgan kompyuter tizimlariga noqonuniy kirish, ma’lumotlarni noqonuniy qo‘lga kiritish, tizim faoliyatiga aralashish kabi qilmishlarning bir qismi O‘zbekiston Jinoyat kodeksining XXI bobida (Republic of Uzbekistan, 1994) aks ettirilgan bo‘lsa-da, protsessual-huquqiy mexanizmlar – xususan, raqamli dalillarni real vaqt rejimida kuzatish, trafik ma’lumotlarini saqlash va davlatlararo tezkor huquqiy yordam tartiblari – hali yetarli darajada qonunchilikka kiritilmagan. Kiberjinoyatlarning transmilliy tabiati esa ushbu

E-ISSN 2181-1148
ISSN 2181-919X

bo‘shliqlarni tezroq to‘ldirishni talab etmoqda. Tadqiqot doirasida quyida bir nechta takliflar ilgari suriladi:

Birinchidan, kiberjinoyatlarni tergov qiluvchi xodimlarni tayyorlashda yuridik va axborot texnologiya tizimlari borasidagi bilimlarni birlashtirgan ixtisoslashgan ta’lim tizimi shakllantirilishi lozim. Xorijiy amaliyotda keng qo‘llanadigan ikki yo‘nalishli – huquqiy va axborot texnologiyalari – oliy ma’lumot modeli O‘zbekiston uchun ham samarali yechim bo‘lib xizmat qiladi. 2025-yil 30-apreldagi PQ–153-sonli qaror (President of the Republic of Uzbekistan, 2025) bilan tashkil etilgan Kiberjinoyatlarga qarshi kurashishga va raqamli tergovga ko‘maklashish markazi ushbu yo‘nalishda muhim qadam bo‘ldi, biroq bu yetarli emas – tizimli kadrlar tayyorlash mexanizmi uzoq muddatli strategiya asosida qurilishi kerak.

Ikkinchidan, qo‘shni Qozog‘iston Respublikasining 2023-yil 19-aprelda Budapesht konvensiyasiga qo‘shilish uchun rasmiy taklif olgani (Council of Europe, 2023) va bu yo‘nalishda integratsiyalashayotgani MDH mintaqasida kiberjinoyatlarni tergov qilish standartlarini o‘zgartirmoqda. O‘zbekiston transmilliy kiberfiribgarliklar qurboniga aylanayotgan o‘z fuqarolarining huquqlarini himoya qilish uchun ushbu konvensiyaning tezkor aloqa kanallariga ulanishi va xorijiy provayderlar (masalan, “Telegram”, “Meta”, “Google”) bilan to‘g‘ridan to‘g‘ri huquqiy hamkorlik mexanizmini yo‘lga qo‘yishi shart. Bu elektron dalillarni olish vaqtini bir necha oydan bir necha daqiqaga qisqartiradi.

Xulosa o‘rnida aytish mumkinki, hozirgi kunda mamlakatimiz ushbu jabhada salmoqli qadamlar qo‘ymoqda. Tergov va sud amaliyoti ham tobora zamonaviy dunyo talablariga, aniqlanayotgan kiberjinoyatlarning shakli va usullariga moslashib bormoqda. Ammo bu yangilanishlar soha rivojlanishini to‘xtatib qo‘yishi kerak emas. Shu boisdan, raqamli muhitda sodir etiladigan jinoyatlar yanada tezroq va aniqroq fosh etilishi uchun malakali kadrlar hamda mukammal qonunchilik tizimi muhim ahamiyat kasb etadi.

REFERENCES

Central Bank of the Russian Federation. (2021). *Osnovnye tipy kompyuternykh atak v kreditno-finansovoy sfere v 2019–2020 godakh* [Main types of computer attacks in the credit and financial sphere in 2019–2020]. Bank of Russia Official Report. https://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf

Council of Europe. (2001, November 23). *Convention on Cybercrime* (Budapest Convention, ETS No. (185) and its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (2023, April 19). *Kazakhstan invited to join the Convention on Cybercrime*. https://www.coe.int/en/web/cybercrime/-/kazakhstan-invited-to-join-the-convention-on-cybercrime

Gazeta.uz. (2025, November 5). *O‘zbekistonda kiberjinoyatlar umumiy jinoyatlarning salkam yarmini tashkil qilyapti: IIV ularning sodir etilish usullarini ochiqladi* [Cybercrimes account for nearly half of all crimes in Uzbekistan: The Ministry of Internal Affairs disclosed methods of their commission]. https://www.gazeta.uz/oz/2025/11/05/cybercrime/

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review, 27*(1), 61–67. https://doi.org/10.1016/j.clsr.2010.11.001

Kodirov, F., & Tursunova, S. (2025, April 1). Kiberjinoyatlar va ularning oldini olish yo‘llari [Cybercrimes and ways of preventing them]. *Science, 3*(7), 151–157. https://doi.org/10.5281/zenodo.15119685

Mahmudov, M. (2025). Kiberjinoyatlarga qarshi kurashishning huquqiy asoslarini takomillashtirish [Improving the legal foundations of combating cybercrime]. *Modern Science and Research, 4*(11), 914–918. https://doi.org/10.5281/zenodo.17770356

Onwuadiamu, G. (2025). Cybercrime in criminology: A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology, 8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

President of the Republic of Uzbekistan. (2025, April 30). On measures aimed at further strengthening efforts to combat crimes committed using information technologies (Resolution No. RP-153). https://lex.uz/uz/docs/7511145

Primov, B. (2024). Kiberjinoyatchilikka qarshi immunitetni hosil qilish masalalari [Issues of developing immunity against cybercrime]. *Central Asian Journal of Education and Innovation, 3*(5), 164–179. https://doi.org/10.5281/zenodo.11394491

Raed, S., Faqir, A., & Arfaoui, D. (2024). Psychological insights into the behavior of cybercriminals: A theoretical perspective. *Pakistan Journal of Criminology, 16*(2), 263–276. https://www.pjcriminology.com/wp-content/uploads/2024/04/19-Psychological-Insights-into-the-Behavior.pdf

Republic of Uzbekistan. (1994). *Criminal Code of the Republic of Uzbekistan (with amendments and additions up to 2026).* https://lex.uz/docs/111453

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165–176. http://www.ijcncs.org

Sarkar, G., & Shukla, S. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 2*, 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Sarkar, G., & Shukla, S. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology, 4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Siroyev, N. (2025). Kiberjinoyatlar va ularga qarshi samarali kurashish strategiyalari [Cybercrimes and effective strategies for combating them]. *Science, 3*(4), 134–137. https://doi.org/10.5281/zenodo.14964074

Tila, C. (2026). Global number of internet users 2005–2025. *Statista*. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Tubaishat, A., & AlAleeli, H. (2024). A framework to prevent cybercrime in the UAE. *Procedia Computer Science, 238*, 558–565. https://doi.org/10.1016/j.procs.2024.06.060

Weijer, S., Leukfeldt, R., & Moneva, A. (2024). Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Computers & Security, 139*, 103693. https://doi.org/10.1016/j.cose.2023.103693

E-ISSN 2181-1148
ISSN 2181-919X

YURIDIK FANLAR AXBOROTNOMASI
ВЕСТНИК ЮРИДИЧЕСКИХ НАУК
REVIEW OF LAW SCIENCES

Huquqiy ilmiy-amaliy jurnal

Правовой научно-практический журнал

Legal scientific-practical journal

2026-yil maxsus son

VOLUME 10 / SPECIAL ISSUE / 2026

DOI: HTTPS://DX.DOI.ORG/10.51788/TSUL.ROLS.2026.10.SI.