



KRIMINOLOGIYA VA JINOIY ODIL SUDLOV

ILMIY-AMALIY JURNAL

2026-yil 3-son

VOLUME 6 / ISSUE 3 / 2026
ISSUE DOI: [HTTPS://DX.DOI.ORG/10.51788/TSUL.CCJ.63](https://dx.doi.org/10.51788/TSUL.CCJ.63)

ISSN 2181-2179
DOI: [HTTPS://DX.DOI.ORG/10.51788/TSUL.CCJ](https://dx.doi.org/10.51788/TSUL.CCJ)



Crossref
Content
Registration

**MUASSIS:
TOSHKENT DAVLAT YURIDIK
UNIVERSITETI**

“Kriminologiya va jinoiy odil sudlov” ilmiy-amaliy jurnali O‘zbekiston matbuot va axborot agentligi tomonidan 2021-yil 18-martda 1160-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.

Ushbu jurnal O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi bilan hamkorlikda tashkil etilgan.

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

Mualliflik huquqlari Toshkent davlat yuridik universitetiga tegishli. Barcha huquqlar himoyalangan. Jurnal materiallaridan foydalanish, tarqatish va ko‘paytirish muassis ruxsati bilan amalga oshiriladi.

Sotuvda kelishilgan narxda.

Nashr bo‘yicha mas‘ul:
O. Choriyev

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

Musahhih:
R. Yunusova
Texnik muharrir:
U. Sapayev
Dizayner:
D. Rajapov

Tahririyat manzili:
100047. Toshkent shahri,
Sayilgoh ko‘chasi, 35.

Tel.: (0371) 233-66-36, 233-41-09.
Faks: (0371) 233-37-48.
Veb-sayt: www.ccj.tsul.uz
E-mail: criminologyjournal@tsul.uz

Obuna indeksi: 1386.

Nashriyot litsenziyasi
№ 174625, 29.11.2023.

Jurnal 2026-yil 24-sentabrda bosmaxonaga topshirildi.
Qog‘oz bichimi: A4.
Shartli bosma tabog‘i: 18.
Adadi: 100. Buyurtma: № 99.

Bosmaxona litsenziyasi
29.11.2023 № 174626

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

© Toshkent davlat yuridik universiteti

TAHRIR HAY’ATI

BOSH MUHARRIR

Q. Abdurasulova – Toshkent davlat yuridik universiteti Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish sho‘basi professori, yuridik fanlar doktori

Y. Kolenko – O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi boshlig‘ining birinchi o‘rinbosari

BOSH MUHARRIR O‘RINBOSARI

D. Bazarova – Toshkent davlat yuridik universiteti Jinoyat-protsessual huquqi sho‘basi professori, yuridik fanlar doktori

MAS‘UL MUHARRIR

Sh. Xaydarov – Toshkent davlat yuridik universiteti Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish sho‘basi mudiri o‘rinbosari, yuridik fanlar doktori, professor

TAHRIR HAY’ATI A‘ZOLARI

M. Rustambayev – O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti boshlig‘i, yuridik fanlar doktori, professor

A. Otajonov – Toshkent davlat yuridik universiteti Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish sho‘basi professori, yuridik fanlar doktori

O. Mahkamov – Toshkent davlat yuridik universiteti Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish sho‘basi dotsent v.b., yuridik fanlar doktori

N. Salayev – O‘zbekiston Respublikasi Odil sudlov akademiyasi prorektori, yuridik fanlar doktori, professor

S. Niyozova – Toshkent davlat yuridik universiteti Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish sho‘basi professori, yuridik fanlar doktori

V. Davlyatov – O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi huzuridagi Parlament tadqiqotlari instituti direktorining o‘rinbosari, yuridik fanlar doktori, professor

A. Baratov – Toshkent davlat yuridik universiteti Kriminalistika va sud ekspertizasi sho‘basi mudiri, yuridik fanlar nomzodi

D. Musayev – Bojxona institutining Umumhuquqiy fanlar kafedrasini boshlig‘i, yuridik fanlar bo‘yicha falsafa doktori, dotsent

I. Nikonov – O‘zbekiston Respublikasi Prezidenti Administratsiyasi boshqarma boshlig‘i, yuridik fanlar bo‘yicha falsafa doktori

N. Hojiyev – Toshkent davlat yuridik universiteti O‘quv-uslubiy boshqarma (Registrator ofisi) boshlig‘i

P. Xojabekov – Toshkent davlat yuridik universiteti Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish sho‘basi katta o‘qituvchisi, yuridik fanlar nomzodi

D. Nurumov – Toshkent davlat yuridik universiteti Sud hokimiyati, advokatura va huquqni muhofaza qiluvchi organlar sho‘basi professori, yuridik fanlar bo‘yicha falsafa doktori



**УЧРЕДИТЕЛЬ:
ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ
ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ**

Научно-практический журнал «Криминология и уголовное правосудие» зарегистрирован Агентством печати и информации Узбекистана 18 марта 2021 года с удостоверением № 1160.

Журнал создан при сотрудничестве с Правоохранительной академией Республики Узбекистан.

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

Авторские права принадлежат Ташкентскому государственному юридическому университету. Все права защищены. Использование, распространение и воспроизведение материалов журнала осуществляется с разрешения учредителя.

Реализуется по договорной цене.

Ответственный за выпуск:

О. Чориев

Редакторы:

Е. Ярмолик, Э. Мустафаев, М. Шарифова,
Ш. Бекназарова, К. Абдувалиева,
Э. Шарипов, Х. Юлдашева, Й. Махмудов

Корректор:

Р. Юнусова

Технический редактор:

У. Сапаев

Дизайнер:

Д. Ражапов

Адрес редакции:

100047. Город Ташкент,
улица Сайилгох, 35.

Тел.: (0371) 233-66-36, 233-41-09.

Факс: (0371) 233-37-48.

Веб-сайт: www.ccj.tsul.uz

E-mail: criminologyjournal@tsul.uz

Подписной индекс: 1386.

Издательская лицензия от

29.11.2023, № 174625.

Журнал передан в типографию
24.09.2026.

Формат бумаги: А4.

Усл. п. л. 18. Тираж: 100 экз.

Номер заказа: 99.

Лицензия типографии от

№ 174626, 29.11.2023.

Отпечатано в типографии

Ташкентского государственного
юридического университета.

100047, г. Ташкент, ул. Сайилгох, дом 37.

© Ташкентский государственный
юридический университет

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

ГЛАВНЫЙ РЕДАКТОР

К. Абдурашулова – профессор сектора уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета, доктор юридических наук

Е. Коленко – первый заместитель начальника Правоохранительной академии Республики Узбекистан

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА

Д. Базарова – профессор сектора уголовно-процессуального права Ташкентского государственного юридического университета, доктор юридических наук

ОТВЕТСТВЕННЫЙ РЕДАКТОР

Ш. Хайдаров – заместитель заведующего сектором уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета, доктор юридических наук, профессор

ЧЛЕНЫ РЕДКОЛЛЕГИИ

М. Рустамбаев – начальник Университета общественной безопасности Республики Узбекистан, доктор юридических наук, профессор

А. Отажонов – профессор сектора уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета, доктор юридических наук

О. Махкамов – и. о. доцента сектора уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета, доктор юридических наук

Н. Салаев – проректор Академии правосудия Республики Узбекистан, доктор юридических наук, профессор

С. Ниёзова – профессор сектора уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета, доктор юридических наук

В. Давлятов – заместитель директора Института парламентских исследований при Законодательной палате Олий Мажлиса Республики Узбекистан, доктор юридических наук, профессор

А. Баратов – заведующий сектором криминалистики и судебной экспертизы Ташкентского государственного юридического университета, кандидат юридических наук

Д. Мусаев – начальник кафедры общеправовых дисциплин Таможенного института, доктор философии по юридическим наукам, доцент

И. Никонов – начальник управления Администрации Президента Республики Узбекистан, доктор философии по юридическим наукам

Н. Хожиев – начальник учебно-методического управления Ташкентского государственного юридического университета

П. Хожобеков – старший преподаватель сектора уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета, кандидат юридических наук

Д. Нурумов – профессор сектора судебной власти, адвокатуры и правоохранительных органов Ташкентского государственного юридического университета, доктор философии по юридическим наукам

**FOUNDER:
TASHKENT STATE UNIVERSITY OF LAW**

The scientific-practical journal "Criminology and Criminal Justice" was registered by the Press and Information Agency of Uzbekistan on March 18, 2021, with certificate No. 1160.

This journal was founded in cooperation with the Law Enforcement Academy of the Republic of Uzbekistan.

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

Copyright belongs to Tashkent State University of Law. All rights reserved. Use, distribution and reproduction of materials of the journal are carried out with the permission of the founder.

Agreed-upon price.

Publication Officer:
O. Choriev

Editors:
E. Yarmolik, E. Mustafaev, M. Sharifova,
Sh. Beknazarova, K. Abduvaliyeva,
E. Sharipov, Kh. Yuldasheva, Y. Makhmudov

Proofreader:
R. Yunusova

Technical editor:
U. Sapaev

Designer:
D. Rajapov

Editorial office address:
100047. Tashkent city,
Sayilgoh street, 35.

Phone: (0371) 233-66-36,
233-41-09.

Fax: (0371) 233-37-48.

Website: www.ccj.tsul.uz

E-mail: criminologyjournal@tsul.uz

Subscription index: 1386.

Publishing license
№ 174625, 29.11.2023.

The journal is submitted to the Printing house on 24.09.2026.

Paper size: A4. Cond.p.f: 18.

Units: 100. Order: № 99.

Printing house license
№ 174626, 29.11.2023.

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

© Tashkent State University of Law

EDITORIAL BOARD

EDITOR-IN-CHIEF

Q. Abdurasulova – Professor of the Department of Criminal Law, Criminology and Anti-Corruption of Tashkent State University of Law, Doctor of Law

Y. Kolenko – First Deputy Head of the Law Enforcement Academy of the Republic of Uzbekistan

DEPUTY EDITOR-IN-CHIEF

D. Bazarova – Professor of the Department of Criminal Procedural Law of Tashkent State University of Law, Doctor of Law

EXECUTIVE EDITOR

Sh. Khaydarov – Deputy Head of the Department of Criminal Law, Criminology and Anti-Corruption of Tashkent State University of Law, Doctor of Law, Professor

MEMBERS OF THE EDITORIAL BOARD

M. Rustambayev – Head of the University of Public Security of the Republic of Uzbekistan, Doctor of Law, Professor

A. Otajonov – Professor of the Department of Criminal Law, Criminology and Anti-Corruption of Tashkent State University of Law, Doctor of Law

O. Mahkamov – Acting Associate Professor of the Department of Criminal Law, Criminology and Anti-Corruption of Tashkent State University of Law, Doctor of Law

N. Salaev – Deputy Rector of the Academy of Justice of the Republic of Uzbekistan, Doctor of Law, Professor

S. Niyozova – Professor of the Department of Criminal Law, Criminology and Anti-Corruption of Tashkent State University of Law, Doctor of Law

V. Davlyatov – Deputy Director of the Institute of Parliamentary Research under the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan, Doctor of Law, Professor

A. Baratov – Head of the Department of Criminalistics and Forensic Examination of Tashkent State University of Law, Candidate of Legal Sciences

D. Musaev – Head of the Department of General Legal Sciences of the Customs Institute, Doctor of Philosophy (PhD) in Law, Associate Professor

I. Nikonov – Head of a Department of the Administration of the President of the Republic of Uzbekistan, Doctor of Philosophy (PhD) in Law

N. Hojiyev – Head of the Educational and Methodological Department (Registrar's Office)

P. Khojabekov – Senior Lecturer of the Department of Criminal Law, Criminology and Anti-Corruption of Tashkent State University of Law, Candidate of Legal Sciences

D. Nurumov – Professor of the Department of Judiciary, Advocacy and Law Enforcement Agencies of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law



MUNDARIJA

12.00.08 – JINOYAT HUQUQI. JINOYAT-IJROIYA HUQUQI

Otajonov Abrorjon Anvarovich

JINOYATGA PROVOKATSIYA QILISH INSTITUTINI HUQUQIY TARTIBGA SOLISHNI
TAKOMILLASHTIRISH ISTIQBOLLARI11

Primov Baxtiyor Olim o'g'li

KRIPTO-AKTIVLAR BILAN BOG'LIQ JINOYATLARNING JINOIY-HUQUQIY TARTIBGA
SOLINISHI: XORIJIY TAJRIBA VA MILLIY QONUNCHILIK ISTIQBOLLARI26

12.00.09 – JINOYAT PROTSESSI. KRIMINALISTIKA, TEZKOR-QIDIRUV HUQUQ VA SUD EKSPERTIZASI

Xikmatov Aziz Bobonarovich

SO'ROQ QILISHNI TASNIFLASHNING NAZARIY VA PROTSESSUAL-HUQUQIY
MASALALARI33

Qaybar Malik Sungatuli

TRANSCHEGARAVIY YO'NALISHLAR SHAROITIDA TRANSPORT JINOYATLARINI
TERGOV QILISHDA HUQUQNI MUHOFAZA QILUVCHI ORGANLARNING O'ZARO
HAMKORLIGI MUAMMOLARI48

Nosirov Amirxon Bahodir o'g'li

AXBOROT TEXNOLOGIYALARIDAN FOYDALANIB SODIR ETILGAN FIRIBGARLIK
JINOYATINI TERGOV QILISHDA TERGOV VA TEZKOR-QIDIRUV FAOLIYATINING
O'ZARO HAMKORLIGINI TAKOMILLASHTIRISH MASALALARI58

Hasanov Abdulmannon Mamatmurodovich

JINOYAT PROTSESSIDA SUD MUHOKAMASI BOSQICHIDA JABRLANUVCHI VA
FUQAROVIIY DA'VOGARGA MALAKALI YURIDIK YORDAM KO'RSATISH
KAFOLATLARI69

12.00.10 – XALQARO HUQUQ

Umarov Rustam Zulfukarovich

"MARKAZIY OSIYO – KOREYA RESPUBLIKASI" FORMATINING XALQARO-HUQUQIY
INSTITUTIONALLASHUVI79

12.00.12 – KORRUPSIYA MUAMMOLARI

Xomidov Shuxrat Gafurjonovich

KORRUPSIYA VA JINOIY DAROMADLARNI LEGALLASHTIRISH: BOG'LIQLIK VA
FARQLASH MEZONLARI95

Ahmadov Alimardon Ahmadovich

CHEGARALARARO AKTIVLARNI QAYTARISHDA GLOBE TARMOG'INING O'RNI:
INSTITUTSIONAL TUZILISH, HUQUQIY CHEKLOVLAR VA MINTAQAVIY HAMKORLIK 105

**12.00.14 – HUQUQBUZARLIKLAR PROFILAKTIKASI. JAMDAT XAVFSIZLIGINI TA'MINLASH.
PROBATSIIYA FAOLIYATI**

Abdullayev Akbarjon Azamovich

TOSHKENT SHAHRINING KRIMINOGEN VAZIYATINI MONITORING QILISH BO'YICHA
GEOINFORMATSION XARITASINING DASTURIY TA'MINOTINI YARATISH VA
FAZOVIIY-TOPOGRAFIK TAHLIL USULLARI 117

12.00.15 – KRIMINOLOGIYA

Tairova Gulmira Murodjonovna

JINOYATCHILIKKA QARSHI KURASHISH TIZIMI VA UNING AYRIM MODELLARI 123

Allambergenov Islambek Sadatdinovich, Ibragimova Gozzal Maratovna

KIBERTAHIDIDLAR TRANSFORMATSIYASI SHAROITIDA O'ZBEKISTON
RESPUBLIKASIDA KIBERFIRIBGARLIKKA QARSHI KURASHISH TIZIMINI
TAKOMILLASHTIRISH 132

Xursanov Shamsiddin Allamurod o'g'li

KORRUPSIYANING OLDINI OLIISHDA SUN'IY INTELLEKTNI QO'LLASHNING
O'ZIGA XOS JIHATLARI 147



СОДЕРЖАНИЕ

12.00.08 – УГОЛОВНОЕ ПРАВО. УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

Отажонов Абдоржон Анварович

ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ
ИНСТИТУТА ПРОВОКАЦИИ ПРЕСТУПЛЕНИЯ11

Примов Бахтиёр Олим угли

УГОЛОВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ
С КРИПТОАКТИВАМИ: ЗАРУБЕЖНЫЙ ОПЫТ И ПЕРСПЕКТИВЫ
НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА26

12.00.09 – УГОЛОВНЫЙ ПРОЦЕСС. КРИМИНАЛИСТИКА, ОПЕРАТИВНО-РОЗЫСКОЕ ПРАВО И СУДЕБНАЯ ЭКСПЕРТИЗА

Хикматов Азиз Бобонарович

ТЕОРЕТИЧЕСКИЕ И ПРОЦЕССУАЛЬНО-ПРАВОВЫЕ ВОПРОСЫ КЛАССИФИКАЦИИ
ДОПРОСА33

Кайбар Малик Сунгатулы

ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ РАССЛЕДОВАНИИ ТРАНСПОРТНЫХ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ
ТРАНСГРАНИЧНЫХ МАРШРУТОВ48

Носиров Амирхон Баходир угли

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ВЗАИМОДЕЙСТВИЯ СЛЕДСТВЕННЫХ
ОРГАНОВ И ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ
ДЕЯТЕЛЬНОСТЬ, ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВА
С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ58

Хасанов Абдулманнон Маматмуродович

ГАРАНТИИ ОКАЗАНИЯ КВАЛИФИЦИРОВАННОЙ ЮРИДИЧЕСКОЙ
ПОМОЩИ ПОТЕРПЕВШЕМУ И ГРАЖДАНСКОМУ ИСТЦУ НА СТАДИИ СУДЕБНОГО
РАЗБИРАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ69

12.00.10 – МЕЖДУНАРОДНОЕ ПРАВО

Умаров Рустам Зульфукарович

МЕЖДУНАРОДНО-ПРАВОВАЯ ИНСТИТУЦИОНАЛИЗАЦИЯ ФОРМАТА
«ЦЕНТРАЛЬНАЯ АЗИЯ – РЕСПУБЛИКА КОРЕЯ»79

12.00.12 – ПРОБЛЕМЫ КОРРУПЦИИ

Хомидов Шухрат Гафуржонович

КОРРУПЦИЯ И ЛЕГАЛИЗАЦИЯ ПРЕСТУПНЫХ ДОХОДОВ: ВЗАИМОСВЯЗЬ И
КРИТЕРИИ РАЗГРАНИЧЕНИЯ95

Ахмадов Алимардон Ахмадович

СЕТЬ GLOBE В ТРАНСГРАНИЧНОМ ВОЗВРАТЕ АКТИВОВ: ИНСТИТУЦИОНАЛЬНОЕ
УСТРОЙСТВО, ПРАВОВЫЕ ОГРАНИЧЕНИЯ И РЕГИОНАЛЬНОЕ СОТРУДНИЧЕСТВО 105

12.00.14 – ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПНОСТИ. ОБЕСПЕЧЕНИЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ. ПРОБАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ

Абдуллаев Акбаржон Азамович

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ГЕОИНФОРМАЦИОННОЙ
КАРТЫ МОНИТОРИНГА КРИМИНОГЕННОЙ ОБСТАНОВКИ В ГОРОДЕ ТАШКЕНТЕ И
МЕТОДЫ ПРОСТРАНСТВЕННО-ТОПОГРАФИЧЕСКОГО АНАЛИЗА 117

12.00.15 – КРИМИНОЛОГИЯ

Таирова Гулмира Муроджоновна

СИСТЕМА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ И НЕКОТОРЫЕ ЕЁ МОДЕЛИ 123

Алламбергенов Исламбек Садатдинович, Ибрагимова Гоззал Маратовна

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ
В РЕСПУБЛИКЕ УЗБЕКИСТАН В УСЛОВИЯХ ТРАНСФОРМАЦИИ КИБЕРУГРОЗ 132

Хурсанов Шамсиддин Алламурод угли

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
В ПРЕДУПРЕЖДЕНИИ КОРРУПЦИИ 147



CONTENTS

12.00.08 – CRIMINAL LAW. CRIMINAL-EXECUTIVE LAW

Otajonov Abrorjon Anvarovich

PROSPECTS AND IMPROVEMENT OF THE REGULATION OF THE INSTITUTION
OF CRIME PROVOCATION11

Primov Bakhtiyor Olim ugli

CRIMINAL LAW REGULATION OF CRIMES RELATED TO CRYPTO-ASSETS:
FOREIGN EXPERIENCE AND PROSPECTS OF NATIONAL LEGISLATION26

12.00.09 – CRIMINAL PROCEEDINGS. FORENSICS, INVESTIGATIVE LAW AND FORENSIC EXPERTISE

Hikmatov Aziz Bobonarovich

THEORETICAL AND PROCEDURAL-LEGAL ISSUES OF CLASSIFYING INTERROGATION33

Kaybar Malik Sungatuli

PROBLEMS OF INTERACTION BETWEEN LAW ENFORCEMENT AGENCIES
IN INVESTIGATING TRANSPORT CRIMES UNDER TRANSBOUNDARY ROUTE
CONDITIONS48

Nosirov Amirkhon Bahodir ugli

ISSUES OF IMPROVING THE INTERACTION BETWEEN INVESTIGATIVE
AUTHORITIES AND OPERATIONAL-SEARCH ACTIVITIES IN THE INVESTIGATION
OF FRAUD CRIMES COMMITTED USING INFORMATION TECHNOLOGIES58

Khasanov Abdulmannon Mamatmurodovich

GUARANTEES FOR PROVIDING QUALIFIED LEGAL ASSISTANCE TO THE
VICTIM AND CIVIL PLAINTIFF AT THE STAGE OF TRIAL IN CRIMINAL
PROCEEDINGS69

12.00.10 – INTERNATIONAL LAW

Umarov Rustam Zulfukarovich

INTERNATIONAL LEGAL INSTITUTIONALIZATION OF THE “CENTRAL ASIA –
REPUBLIC OF KOREA” FORMAT79

12.00.12 – CORRUPTION PROBLEMS

Khomidov Shukhrat Gafurjonovich

CORRUPTION AND MONEY LAUNDERING: CORRELATION AND DIFFERENTIATION
CRITERIA95

Ahmadov Alimardon Akhmadovich

THE GLOBE NETWORK IN CROSS-BORDER ASSET RECOVERY: INSTITUTIONAL DESIGN, LEGAL LIMITS AND REGIONAL COOPERATION	105
--	-----

12.00.14 – CRIME PREVENTION. ENSURING PUBLIC SAFETY. PROBATION ACTIVITY

Abdullaev Akbarjon Azamovich

DEVELOPMENT OF GEOINFORMATION MAP SOFTWARE FOR MONITORING THE CRIMINOGENIC SITUATION OF TASHKENT CITY AND METHODS OF SPATIAL-TOPOGRAPHIC ANALYSIS	117
---	-----

12.00.15 – CRIMINOLOGY

Tairova Gulmira Murodjonovna

CRIME CONTROL SYSTEM AND ITS CERTAIN MODELS	123
---	-----

Allambergenov Islambek Sadatdinovich, Maratovna Gozzal Ibragimova

IMPROVING THE ANTI-CYBER FRAUD SYSTEM IN THE REPUBLIC OF UZBEKISTAN UNDER CONDITIONS OF TRANSFORMATION	132
---	-----

Khursanov Shamsiddin Allamurod ugli

SPECIFIC FEATURES OF USING ARTIFICIAL INTELLIGENCE IN PREVENTING CORRUPTION	147
--	-----

Kelib tushgan / Получено / Received: 17.07.2026
Qabul qiligan / Принято / Accepted: 26.08.2026
Nashr etilgan / Опубликовано / Published: 24.09.2026

DOI: <https://dx.doi.org/10.51788/tsul.ccj.63012>

UDC: 343.72:004.738.5(045)(575.1)

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ В РЕСПУБЛИКЕ УЗБЕКИСТАН В УСЛОВИЯХ ТРАНСФОРМАЦИИ КИБЕРУГРОЗ

Алламбергенов Исламбек Садатдинович,
самостоятельный соискатель,
научный сотрудник Исследовательского института
криминологии Республики Узбекистан
ORCID: <https://orcid.org/0009-0001-7511-9781>
e-mail: islambek_ais_0920@mail.ru

Ибрагимова Гоззал Маратовна,
самостоятельный соискатель
Правоохранительной академии Республики Узбекистан,
сотрудник УКД ОВД Мирзо-Улугбекского района города Ташкента
ORCID: <https://orcid.org/0009-0007-2390-4175>
e-mail: gozzalibragimova0208@gmail.com

Аннотация. В статье исследованы современное состояние, основные тенденции и детерминанты кибермошенничества в Республике Узбекистан. С применением статистического, системного, сравнительно-правового и формально-юридического методов проанализированы формы и способы совершения кибермошенничества, виктимологические факторы, организационно-правовые механизмы его предупреждения и пресечения, а также зарубежный опыт. Обоснована модель детерминации кибермошенничества, основанная на взаимодействии преступного потенциала правонарушителя, виктимологический уязвимости потерпевшего и возможностей цифровой среды. Определены направления совершенствования национальной системы предупреждения кибермошенничества и противодействия ему с учётом современных форм, способов и технологий его совершения.

Ключевые слова: кибермошенничество, киберпреступность, предупреждение преступности, детерминанты, виктимологическая уязвимость, социальная инженерия, искусственный интеллект

KIBERTAHIDDLAR TRANSFORMATSIYASI SHAROITIDA O'ZBEKISTON RESPUBLIKASIDA KIBERFIRIBGARLIKKA QARSHI KURASHISH TIZIMINI TAKOMILLASHTIRISH

Allambergenov Islambek Sadatdinovich,

O'zbekiston Respublikasi
Kriminologiya tadqiqot instituti
ilmiy xodimi, mustaqil izlanuvchi

Ibragimova Gozzal Maratovna,

O'zbekiston Respublikasi
Huquqni muhofaza qilish akademiyasi
mustaqil izlanuvchisi,
Toshkent shahar Mirzo Ulug'bek tuman IIO FMB xodimi

Annotatsiya. Maqolada O'zbekiston Respublikasida kiberfiribgarlikning zamonaviy holati, asosiy tendensiyalari va determinantlari tadqiq etilgan. Statistik, tizimli, qiyosiy-huquqiy va formal-yuridik metodlar asosida kiberfiribgarlikni sodir etish shakllari va usullari, viktimologik omillari, uning oldini olish va chek qo'yishning tashkiliy-huquqiy mexanizmlari, shuningdek, xorijiy tajriba tahlil qilingan. Huquqbuzarning jinoiy salohiyati, jabrlanuvchining viktimologik zaifligi va raqamli muhit imkoniyatlarining o'zaro ta'siriga asoslangan kiberfiribgarlik determinantlarining modeli asoslangan. Kiberfiribgarlikni sodir etishning zamonaviy shakllari, usullari va texnologiyalarini hisobga olgan holda uning oldini olish va unga qarshi kurashish bo'yicha milliy tizimni takomillashtirish yo'nalishlari belgilab berilgan.

Kalit so'zlar: kiberfiribgarlik, kiberjinoyatchilik, jinoyatchilikning oldini olish, determinantlar, viktimologik zaiflik, ijtimoiy muhandislik, sun'iy intellekt

IMPROVING THE ANTI-CYBER FRAUD SYSTEM IN THE REPUBLIC OF UZBEKISTAN UNDER CONDITIONS OF TRANSFORMATION

Allambergenov Islambek Sadatdinovich,

Research Fellow at the Research Institute of Criminology
of the Republic of Uzbekistan, Independent Researcher

Ibragimova Gozzal Maratovna,

Independent Researcher at the Law Enforcement Academy
of the Republic of Uzbekistan,
Officer of the Department of Internal Affairs of Mirzo-Ulugbek District
of Tashkent

Abstract. The article examines the current state, main trends, and determinants of cyber fraud in the Republic of Uzbekistan. Using statistical, systematic, comparative-legal, and formal-legal methods, the forms and methods of committing cyberfraud, victimological factors,

organizational and legal mechanisms for its prevention and suppression, as well as foreign experience, were analyzed. A determination model for cyberfraud is substantiated, based on the interaction of the offender's criminal potential, victimological vulnerability, and digital environment capabilities. Directions for improving the national system for preventing and countering cyber fraud have been defined, taking into account modern forms, methods, and technologies of its commission.

Keywords: *cyber fraud, cybercrime, crime prevention, determinants, victimological vulnerability, social engineering, artificial intelligence*

Введение

Стремительная цифровизация общественных отношений не только расширила возможности социально-экономического развития, но и сформировала новые условия для совершения преступлений в киберпространстве.

Динамика киберпреступности в Узбекистане подтверждает данную тенденцию: в 2021–2025 годах число зарегистрированных киберпреступлений возросло более чем в 12 раз – с 4 865 до 62 440 случаев, а причинённый гражданам материальный ущерб достиг 3,73 трлн сумов, при этом 1,89 трлн сумов пришлось на первые 11 месяцев 2025 года. Число поступивших обращений также увеличилось в 34 раза (Ministry of Internal Affairs of the Republic of Uzbekistan, 2025).

При этом за последние пять лет наблюдается не только количественный рост киберпреступности, но и качественная трансформация её структуры, выражающаяся в появлении новых форм и способов кибермошенничества, обусловленных развитием цифровых технологий и расширением сферы электронных услуг.

В настоящее время формируется противоречие между динамичностью изменения форм и способов кибермошенничества, с одной стороны, и недостаточной адаптацией отдельных организационно-правовых и профилактических механизмов к темпам и характеру происходящих изменений – с другой. Указанное противоречие затрудняет своевременное выявление и пресечение кибермошенничества, установление виновных лиц, снижение уровня его латентности, защиту потерпевших, блокирование используемой преступной инфраструктуры и возврат похищенных денежных средств.

Таким образом, ключевая проблема заключается не столько в отсутствии в Республике Узбекистан нормативно-правовой и организационной основы предупреждения кибермошенничества и противодействия ему, сколько в необходимости её постоянной адаптации к динамике преступных практик, развитию цифровых технологий и изменению характера виктимологической уязвимости пользователей.

Цель исследования заключается в криминологическом анализе состояния, динамики и детерминант кибермошенничества, а также в разработке предложений по совершенствованию системы противодействия ему.

Для достижения поставленной цели определены следующие задачи:

проанализировать динамику и основные тенденции киберпреступности в Узбекистане за 2021–2025 годы и определить место кибермошенничества в её структуре;

выявить основные криминогенные и виктимологические факторы, способствующие совершению и распространению кибермошенничества;



исследовать действующие в Узбекистане организационно-правовые механизмы предупреждения кибермошенничества и противодействия ему, а также выявить основные проблемы их применения;

изучить зарубежный опыт предупреждения кибермошенничества и разработать предложения по совершенствованию национальной системы его предупреждения и пресечения.

В научной литературе проблема кибермошенничества и его предупреждения рассматривается с различных позиций. Р. Смит и Г. Урбас акцентируют внимание на обмане и причинении имущественного ущерба посредством интернет-технологий (Smith & Urbas, 2001). А. Гиллеспи относит кибермошенничество к преступлениям против собственности, совершаемым с использованием цифровых технологий (Gillespie, 2019).

Существенное внимание в исследованиях уделяется человеческому фактору и социальной инженерии. Б. Шнайер подчёркивает значение поведения человека в обеспечении информационной безопасности, а Конте и Шмик рассматривают социальную инженерию как способ получения конфиденциальной информации посредством психологического воздействия (Schneier, 2000; Conteh & Schmick, 2016). В исследовании Вэнь и соавторов также отмечается роль эмоциональных и поведенческих факторов в побуждении пользователей к совершению действий вопреки их интересам (Wen et al., 2022). О. Бовть раскрывает понятие кибержертвы, а В. Плешаков и Т. Склярова исследуют сущность кибервиктимности (Bovt, 2017; Pleshakov & Sklyarova, 2020).

Указанные исследователи в большей степени сосредоточены на раскрытии содержания и сущности кибермошенничества, анализе способов его совершения, роли человеческого фактора и социальной инженерии, а также виктимологической уязвимости. При этом каждый из рассмотренных авторов акцентирует внимание преимущественно на отдельных аспектах данного явления. Несмотря на значительный объём исследований, комплексный подход, объединяющий анализ динамики и структуры кибермошенничества, современных способов его совершения и применяемых технологических инструментов, детерминант и виктимологических факторов с оценкой механизмов противодействия в условиях Узбекистана, остаётся недостаточно разработанным. Именно данная совокупность взаимосвязанных вопросов определяет научную проблему настоящего исследования.

Научная новизна исследования состоит в разработке авторского подхода к криминологическому анализу кибермошенничества, предусматривающего разграничение формы преступного посягательства, способа его совершения и используемых для этого цифровых технологий и ресурсов. Кроме того, обоснована модель детерминации кибермошенничества, основанная на взаимодействии преступного потенциала правонарушителя, виктимологической уязвимости потерпевшего и возможностей цифровой среды.

В ходе исследования изучены современное состояние и основные тенденции кибермошенничества в Республике Узбекистан, систематизированы формы, способы и детерминанты его совершения, проанализированы действующие организационно-правовые и профилактические меры. На этой основе выявлены существующие проблемы и разработаны предложения по совершенствованию механизмов противодействия кибермошенничеству.

Объектом исследования является кибермошенничество как социально-правовое и криминологическое явление в условиях цифровой трансформации общественных отношений.

Предметом исследования являются состояние, динамика, структура, формы и способы совершения кибермошенничества, его детерминанты и виктимологические факторы, а также организационно-правовые и профилактические механизмы его предупреждения и пресечения в Республике Узбекистан.

В исследовании использованы статистический, системный, сравнительно-правовой и формально-юридический методы, а также методы анализа и синтеза. Статистический метод применён для оценки состояния и динамики киберпреступности в Республике Узбекистан за 2021–2025 годы. Системный метод позволил рассмотреть кибермошенничество как совокупность взаимосвязанных элементов, включающих формы преступного посягательства, способы его совершения, технологические инструменты, характеристики преступника и потерпевшего, а также условия цифровой среды. Сравнительно-правовой метод использован при сопоставлении зарубежных моделей предупреждения кибермошенничества и противодействия ему, а формально-юридический – при анализе национального законодательства и организационно-правовых механизмов. Методы анализа и синтеза применены для систематизации представленных в научной литературе теоретических подходов к пониманию сущности, детерминации и виктимологии кибермошенничества.

Основная часть

Кибермошенничество является одним из наиболее распространённых и динамично развивающихся видов киберпреступности. Его распространение и постоянная трансформация обуславливают необходимость прежде всего определить содержание данного явления. Под кибермошенничеством в настоящем исследовании предлагается понимать умышленное завладение чужим имуществом либо приобретение права на него путём обмана, злоупотребления доверием или иного введения потерпевшего в заблуждение с использованием информационно-коммуникационных технологий, цифровых платформ и иных средств цифрового взаимодействия.

В рамках настоящего исследования предлагается аналитически разграничивать три взаимосвязанных элемента кибермошеннической деятельности: *форму преступного посягательства, способ его совершения и используемые для реализации преступного умысла цифровые технологии и ресурсы.*

Форма характеризует содержание и направленность мошеннической схемы и может выражаться в инвестиционном мошенничестве, мошенничестве в электронной торговле, мошенничестве с использованием корпоративной электронной почты, мошенничестве, основанном на романтических или доверительных отношениях, мошенничестве под видом технической поддержки, мошенничестве, связанном с непоставкой товаров или неоказанием услуг, и иных разновидностях цифрового мошенничества.

Способ отражает непосредственный механизм воздействия на потерпевшего и включает фишинг, голосовой фишинг и СМС-фишинг, выдачу себя за другое лицо или представителя организации, применение методов социальной инженерии, получение неправомерного доступа к учётным записям, а также иные способы введения потерпевшего в заблуждение или получения незаконного доступа к цифровым ресурсам.



Цифровое средство реализации преступного умысла представляет собой конкретную технологию, сервис, платформу или ресурс, посредством которых применяется выбранный способ совершения преступления. К таким средствам относятся электронная почта, веб-сайты, мобильная связь, мессенджеры, социальные сети, вредоносное программное обеспечение, технологии искусственного интеллекта, цифровые платёжные системы и криптовалютные инструменты.

Таким образом, одна и та же форма кибермошенничества может реализовываться различными способами и посредством разных технологических инструментов. Данная взаимосвязь позволяет рассматривать трансформацию кибермошенничества не только как появление новых видов мошеннических схем, но и как изменение способов преступного воздействия и применяемых технологий.

Кибермошенничество и киберкражи относятся к числу наиболее значимых по имущественным последствиям форм киберпреступности, характеризуются высокой латентностью и способностью быстро адаптироваться к новым технологическим условиям.

Для оценки масштабов и динамики данных явлений целесообразно проанализировать динамику киберпреступности за 2021–2025 годы, её удельный вес, темпы роста и структурные изменения. Тем не менее ограниченная доступность детализированных официальных статистических данных, в том числе об отдельных видах киберпреступлений и кибермошенничестве, снижает возможности проведения углублённого криминологического анализа.

Вместе с тем имеющиеся статистические данные позволяют в определённой степени проследить динамику и основные тенденции кибермошенничества.

Так, если в 2019 году с использованием информационных технологий было совершено 863 преступления 18 видов, то в 2024 году было зарегистрировано 58,8 тыс. преступлений 62 видов. Таким образом, наблюдается значительный рост как количества, так и видового разнообразия киберпреступлений.

Согласно официальным данным, в 2024 году основную часть киберпреступлений (98 %) составляли мошенничества и кражи, связанные с использованием банковских карт.

Установлено, что указанные преступления совершались преимущественно посредством рассылки вредоносных ссылок и программ с целью получения контроля над банковскими картами или мобильными устройствами (60 %). В 16 % случаев злоумышленники с помощью различных способов обмана получали СМС-коды, обеспечивающие доступ к банковским счетам и мобильным приложениям. На долю мошеннических действий на платформах электронной торговли приходилось 11 %, различных схем обмана, направленных на завладение денежными средствами граждан, – 9 %, а оформления онлайн-кредитов на имя граждан – 4 % (Ministry of Internal Affairs of the Republic of Uzbekistan, 2025).

Перечисленные способы совершения преступлений объединяет общий признак: по механизму воздействия на потерпевшего и способу завладения денежными средствами они преимущественно соответствуют признакам кибермошенничества. Однако в зависимости от конкретных обстоятельств содеянного такие деяния в ходе предварительного расследования могут быть квалифицированы как киберкражи.

Использование в 60 % зарегистрированных киберпреступлений вредоносных ссылок и программ для получения контроля над банковскими картами или

мобильными устройствами свидетельствует не только о распространённости данного способа среди преступников, но и о виктимологической уязвимости пользователей, проявляющейся в недостаточной способности распознавать потенциально вредоносный контент и избегать взаимодействия с ним.

В условиях стремительного развития цифровых технологий в последние годы всё более заметным становится использование технологий искусственного интеллекта (далее – ИИ). Вместе с тем объективные ограничения эмпирической базы, обусловленные недостаточной доступностью детализированных статистических данных, не позволяют в полной мере оценить масштабы и динамику кибермошенничества, совершаемого с применением ИИ. В связи с этим для характеристики данной тенденции целесообразно обратиться к международным аналитическим данным.

Согласно исследованию международной компании Sumsb, основанному на анализе более 3 млн попыток мошенничества в 2023–2024 годах, в 2024 году дипфейки составили 7 % выявленных случаев мошенничества, связанного с идентификацией личности, а их количество по сравнению с 2023 годом увеличилось в четыре раза. Среди выявленных видов мошенничества, связанного с идентификацией личности, дипфейки занимали четвёртое место после подделки документов, злоупотребления процедурой чарджбэка и захвата учётных записей (Sumsb, 2025).

По данным Центра приёма жалоб на интернет-преступления Федерального бюро расследований США (Internet Crime Complaint Center – IC3), в 2025 году было зарегистрировано 22 364 жалобы, содержащие сведения, связанные с использованием ИИ, а совокупный скорректированный размер ущерба по ним составил 893,3 млн долл. США. Хотя статистика IC3 не отражает ситуацию в глобальном масштабе, она позволяет оценить значительность ущерба от преступлений, связанных с использованием ИИ (Federal Bureau of Investigation, 2026).

По оценке INTERPOL, мошеннические схемы, усиленные технологиями ИИ, могут быть в 4,5 раза более прибыльными по сравнению с традиционными методами. Масштабы распространения таких схем продолжают увеличиваться вследствие снижения барьеров для их массового применения (INTERPOL, 2026).

Таким образом, приведённые данные свидетельствуют о расширении применения ИИ в преступной деятельности, увеличении числа дипфейк-атак и размера причиняемого ущерба, а также повышении прибыльности мошеннических схем. ИИ постепенно становится фактором масштабирования и усложнения кибермошенничества, что обуславливает необходимость совершенствования механизмов его предупреждения.

Анализ отечественной и зарубежной научной литературы показывает, что в настоящее время не выработан единый подход к определению и систематизации детерминант кибермошенничества. Исследователи рассматривают данную проблему с различных позиций, акцентируя внимание на отдельных факторах и условиях, влияющих на возникновение и распространение рассматриваемого вида преступности. В связи с этим представляется необходимым рассмотреть и сопоставить различные научные подходы отечественных и зарубежных исследователей.

А. Расулев выделяет уязвимость информационно-технологических систем, недостаточную эффективность законодательства и отдельных институтов, недостаток профессионализма, а также человеческий фактор. При рассмотрении личности киберпреступника автор обращает внимание на сочетание личностных характеристик,



технических знаний и навыков, социальных особенностей и мотивирующих факторов (Rasulev, 2022).

В исследовании А. Сабырбаевой отмечается, что развитие технологий, модернизация предпринимательской деятельности, появление новых способов заработка и цифровых форм взаимодействия существенно изменили возможности совершения мошенничества. Использование Интернета, информационно-коммуникационных технологий, программного обеспечения, социальных сетей и мессенджеров позволяет преступникам расширять географию преступной деятельности и круг потенциальных потерпевших, что отличает современные формы мошенничества от традиционных (Sabyrbaeva, 2021).

По мнению Г. Меша и М. Доделя, низкий уровень самоконтроля и характер онлайн-активности повышают вероятность раскрытия персональной информации в интернете. В свою очередь, раскрытие такой информации и определённые повседневные онлайн-практики увеличивают вероятность того, что человек станет адресатом мошеннического предложения. Авторы также установили связь между низким уровнем самоконтроля и непосредственной реакцией на такое предложение (Mesch & Dodel, 2018).

Й. ван Вилсем установил, что повышенный риск интернет-мошенничества связан с низким уровнем самоконтроля, активным совершением покупок в Интернете и участием в онлайн-форумах. Причём влияние низкого уровня самоконтроля проявляется как непосредственно, так и опосредованно: импульсивные лица чаще участвуют в рискованных формах онлайн-деятельности, тем самым повышая собственную подверженность мошенничеству (van Wilsem, 2013).

В исследовании Кюн-Шик Чоя, проведённом с участием 204 студентов, применены положения теории повседневной деятельности. Автор показал, что особенности поведения пользователя в цифровой среде и эффективность механизмов компьютерной защиты связаны с вероятностью стать жертвой компьютерных преступлений. В качестве наиболее значимых факторов он выделяет цифровую защищённость, уровень компьютерной безопасности и характер онлайн-деятельности. Практический вывод исследования заключается в необходимости повышения цифровой грамотности, обучения безопасному поведению в Интернете и использования эффективных средств защиты (Choi, 2008).

В исследовании 2026 года Ю Чжоу, Дж. Р. Ли, К. Линь и М. Тивари изучили виктимизацию от кибермошенничества среди 929 китайских учащихся старших классов. Авторы объединили положения общей теории преступности, теории образа жизни и повседневной деятельности, а также концепции рискованного поведения в Интернете. Они пришли к выводу, что девиантный онлайн-образ жизни является наиболее сильным предиктором на обеих стадиях виктимизации: как при попадании в поле зрения мошенников, так и при последующем причинении финансового ущерба (Zhou et al., 2026).

Таким образом, анализ отечественных и зарубежных исследований показывает, что детерминация кибермошенничества имеет комплексный характер и формируется под воздействием взаимосвязанных факторов, относящихся к личности и деятельности преступника, цифровой среде и потенциальному потерпевшему. Одни исследователи преимущественно связывают распространение кибермошенничества с технологическими и институциональными условиями, другие акцентируют внимание

на виктимологическом поведении и особенностях онлайн-активности потерпевших, а третьи рассматривают значение личностных характеристик и профессиональных навыков преступника. Следовательно, сведение детерминант кибермошенничества исключительно к техническим возможностям цифровой среды либо к поведению потерпевшего представляется недостаточным.

На основе обобщения рассмотренных научных подходов в настоящем исследовании предлагается авторская трёхкомпонентная модель детерминации кибермошенничества, включающая *преступный потенциал лица, уязвимость потенциального потерпевшего и возможности цифровой среды*.

Под преступным потенциалом в рамках предлагаемой модели понимается совокупность мотивационных, личностных и профессионально-технических характеристик лица, объективно повышающих его способность к совершению кибермошенничества. Уязвимость потерпевшего определяется особенностями его поведения в цифровой среде, уровнем цифровой и финансовой грамотности, а также степенью осторожности при обращении с персональными и платёжными данными. Цифровая среда, в свою очередь, создаёт условия для анонимизации, удалённого взаимодействия и масштабирования преступной деятельности, а также обеспечивает доступ к современным инструментам, включая технологии искусственного интеллекта.

В связи с актуализацией современных угроз в сфере кибербезопасности в Республике Узбекистан последовательно осуществляются системные и институциональные реформы, направленные на совершенствование данной сферы.

Принятые в 2022–2026 годах нормативно-правовые акты, включая Закон Республики Узбекистан «О кибербезопасности» и соответствующие решения Президента Республики Узбекистан, сформировали правовую основу дальнейшего развития национальной системы кибербезопасности.

Основополагающее значение имеет Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности», закрепивший правовые основы обеспечения кибербезопасности и организации деятельности соответствующих субъектов (Republic of Uzbekistan, 2022). Правовые и организационные механизмы в данной сфере получили дальнейшее развитие в постановлении Президента Республики Узбекистан от 30 ноября 2023 года № ПП-381 «О мерах по усилению защиты прав потребителей цифровой продукции (услуг) и борьбы с правонарушениями, совершаемыми посредством цифровых технологий». Документом предусмотрены меры по усилению защиты прав потребителей цифровой продукции и услуг, а также совершенствованию деятельности по противодействию правонарушениям, совершаемым посредством цифровых технологий (President of the Republic of Uzbekistan, 2023).

В целях совершенствования кадрового обеспечения постановлением Президента Республики Узбекистан от 22 января 2025 года № ПП-17 «О мерах по внедрению системы подготовки профессиональных кадров для сферы противодействия преступлениям, совершаемым с использованием цифровых технологий» предусмотрено внедрение соответствующей системы подготовки специалистов (President of the Republic of Uzbekistan, 2025a).

Дальнейшее усиление правоохранительных и организационных механизмов предусмотрено постановлением Президента Республики Узбекистан от 30 апреля



2025 года № ПП–153 «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий». Документом определён комплекс мер по совершенствованию деятельности по выявлению, предупреждению и пресечению таких преступлений (President of the Republic of Uzbekistan, 2025b).

Следующим этапом развития национальной системы стало принятие Указа Президента Республики Узбекистан от 10 марта 2026 года № УП–38 «Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности», утвердившего Стратегию кибербезопасности Республики Узбекистан на 2026–2030 годы и определившего приоритетные направления дальнейшего совершенствования системы кибербезопасности и предупреждения киберпреступности (President of the Republic of Uzbekistan, 2026).

Таким образом, анализ нормативно-правовой базы свидетельствует о последовательном формировании в Узбекистане организационно-правовых и институциональных основ противодействия киберпреступности, охватывающих предупреждение таких преступлений, подготовку специализированных кадров, повышение цифровой грамотности населения и совершенствование механизмов выявления и раскрытия преступлений. Вместе с тем появление новых форм кибермошенничества и развитие технологий социальной инженерии требуют постоянной адаптации существующих механизмов, повышения кадрового потенциала и расширения технологических возможностей компетентных органов.

Особое значение в данном контексте приобретает совершенствование системы подготовки специализированных кадров. Для обеспечения её соответствия современным требованиям целесообразно ориентировать образовательные программы организаций высшего образования правоохранительных органов и силовых структур на международные стандарты и передовые зарубежные практики. При этом основное внимание следует уделять развитию практико-ориентированного обучения, повышению квалификации преподавателей и расширению возможностей прохождения стажировок в ведущих зарубежных учреждениях с последующей адаптацией эффективных образовательных моделей к национальным условиям.

Поскольку кибермошенничество по своей природе носит трансграничный характер, особый интерес представляет опыт государств, накопивших значительный опыт предупреждения преступлений, совершаемых с использованием цифровых технологий, и противодействия им, в частности государств – членов Европейского союза (ЕС), Республики Корея и Японии.

В государствах – членах ЕС превентивные механизмы преимущественно ориентированы на предупреждение мошеннических платёжных операций до их завершения. В частности, Директивой (ЕС) 2015/2366 (PSD2) предусмотрено применение усиленной аутентификации клиентов при иницировании электронных платёжных операций, а Регламентом (ЕС) 2024/886 – проверка соответствия имени получателя и идентификатора его платёжного счёта (European Parliament & Council of the European Union, 2015; European Parliament & Council of the European Union, 2024). Одновременно противодействие онлайн-мошенничеству обеспечивается посредством межгосударственной координации правоохранительных органов при участии Европола и в рамках Европейской междисциплинарной платформы по борьбе

с преступными угрозами (European Multidisciplinary Platform Against Criminal Threats – EMPACT) (Europol, 2026).

В Республике Корея противодействие кибермошенничеству основывается на специальном законодательстве, устанавливающем обязанности финансовых организаций по предупреждению телекоммуникационного финансового мошенничества. Существенное значение имеют механизмы оперативного приостановления операций по подозрительным счетам, межведомственного обмена информацией и последующего возврата потерпевшим похищенных денежных средств (Republic of Korea, 2023).

В Японии сформирована государственно-частная модель, основанная на взаимодействии Национального полицейского агентства, Агентства финансовых услуг и финансовых организаций. Основными инструментами являются мониторинг и выявление подозрительных операций, оперативная приостановка операций или замораживание счетов, использованных в мошеннических схемах, а также обмен информацией между правоохранительными органами и финансовыми организациями (Financial Services Agency, 2025; National Police Agency, 2022).

Зарубежный опыт показывает, что дальнейшее совершенствование национальной системы противодействия кибермошенничеству целесообразно ориентировать преимущественно на повышение эффективности уже действующих механизмов. Приоритетными направлениями являются предварительная проверка данных получателя при осуществлении электронных платежей, внедрение риск-ориентированных систем мониторинга транзакций, автоматизированный обмен информацией между банками, операторами связи и цифровыми платформами, а также ускорение процедур блокирования подозрительных операций и возврата денежных средств потерпевшим. Перспективным направлением также является применение технологий искусственного интеллекта для проактивного выявления мошеннических схем.

Заключение

Проведённое исследование позволило получить следующие основные результаты. Установлено, что киберпреступность в Республике Узбекистан характеризуется существенным количественным ростом и расширением видового разнообразия, при этом изменение её структуры сопровождается появлением новых форм и способов кибермошенничества.

Систематизация изученных материалов позволила разграничить форму преступного посягательства, способ его совершения и используемые для реализации преступного умысла цифровые технологии и ресурсы как взаимосвязанные элементы механизма кибермошенничества. Выявлено широкое использование вредоносных ссылок и программ для получения контроля над банковскими картами и мобильными устройствами, что свидетельствует как о распространённости соответствующего преступного инструментария, так и о сохраняющейся виктимологической уязвимости пользователей.

Обобщение отечественных и зарубежных исследований позволило установить комплексный характер детерминации кибермошенничества. Обоснована модель, учитывающая взаимодействие преступного потенциала правонарушителя, виктимологической уязвимости потерпевшего и возможностей цифровой среды. Установлено, что развитие технологий искусственного интеллекта дополнительно расширяет возможности масштабирования и усложнения мошеннических схем.



Анализ нормативно-правовой и институциональной базы показал, что в Республике Узбекистан сформированы основные организационно-правовые механизмы противодействия киберпреступности. Вместе с тем их дальнейшая результативность зависит от своевременной адаптации к изменению форм, способов и технологических средств совершения кибермошенничества.

Сравнительно-правовой анализ показал, что в зарубежной практике существенное значение имеют проактивные механизмы предупреждения и пресечения мошеннических операций, включая предварительную проверку данных получателя платежа, риск-ориентированный мониторинг транзакций, оперативный обмен информацией между правоохранительными органами и субъектами финансовой и цифровой инфраструктуры, а также ускоренное блокирование подозрительных операций.

В целях совершенствования системы противодействия кибермошенничеству с учётом выявленных в ходе исследования тенденций и проблем предлагаются следующие меры:

1. Внедрение знака доверия «CyberSafe» для цифровых сервисов

В целях снижения виктимизации пользователей предлагается внедрить знак доверия «CyberSafe» для онлайн-платёжных сервисов, интернет-магазинов, Telegram-ботов, мобильных банковских приложений, порталов государственных услуг и иных цифровых сервисов. Предоставление знака по результатам проверки уровня защищённости данных, наличия критических уязвимостей и правового статуса владельца с возможностью подтверждения его подлинности посредством индивидуального QR-кода позволит повысить надёжность выбора цифровых сервисов и снизить риск использования поддельных ресурсов.

2. Введение в образовательные программы 10–11-х классов курса «Кибериммунитет и медиакультура»

С учётом виктимологических факторов, обусловленных недостаточной осведомлённостью пользователей о цифровых угрозах, предлагается ввести в образовательные программы 10–11-х классов курс «Кибериммунитет и медиакультура», направленный на формирование навыков защиты персональных данных, распознавания фишинга и иных мошеннических схем, проверки достоверности информации и безопасного поведения в цифровой среде.

3. Внедрение системы картирования киберрисков на территориях с высоким уровнем зарегистрированного кибермошенничества

Предлагается в пилотном порядке внедрить систему криминологического картирования киберрисков в пяти регионах Республики Узбекистан с наиболее высоким уровнем зарегистрированного кибермошенничества. Такая система позволит выявлять территории повышенного риска и устанавливать особенности распространения отдельных форм и способов кибермошенничества, в том числе фишинга, мошенничества на онлайн-площадках и хищения денежных средств с банковских карт. Для оперативного реагирования целесообразно обеспечить обмен соответствующей информацией между органами внутренних дел, банками и операторами мобильной связи.

4. Внедрение в банковские приложения интеллектуального механизма предупреждения о мошенничестве

Предлагается внедрить в банковские приложения интеллектуальный механизм предупреждения о мошенничестве с применением методов социальной инженерии.

При выявлении признаков характерного мошеннического сценария система должна автоматически уведомлять клиента о возможных рисках непосредственно в момент совершения операции и предоставлять ему возможность оперативно связаться с банком.

5. *Создание единого межведомственного аналитического модуля на основе искусственного интеллекта*

Предлагается создать единый межведомственный аналитический модуль, который по каждому зарегистрированному факту кибермошенничества будет автоматически осуществлять поиск совпадений по номерам телефонов, банковским реквизитам, электронным кошелькам, IP-адресам и иным цифровым следам, формируя карту связей между преступными аккаунтами и финансовыми операциями. Результаты такого анализа могут использоваться следственными подразделениями для установления взаимосвязанных эпизодов и определения приоритетных направлений расследования.

REFERENCES

Bovt, O. B. (2017). Kiberviktimologiya kak napravlenie borby s kiberprestupnostyu [Cybervictimology as a direction in combating cybercrime]. *Scientific Notes of the Crimean Engineering and Pedagogical University. Series: Pedagogy. Psychology*, (4), 34–36.

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1), 308–333. https://www.researchgate.net/publication/238621672_Computer_Crime_Victimization_and_Integrated_Theory_An_Empirical_Assessment

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31–38. <https://doi.org/10.19101/IJACR.2016.623006>

European Parliament, & Council of the European Union. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market*. EUR-Lex. <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>

European Parliament, & Council of the European Union. (2024). *Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro*. EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2024/886/oj>

Europol. (2026). *EMPACT 2026–2029: Fighting crime together*. <https://www.europol.europa.eu/how-we-work/empact>

Federal Bureau of Investigation. (2026). *2025 IC3 annual report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Financial Services Agency. (2025). *Information on the number of cases of provision of information concerning fraudulent use of deposit accounts, etc.* <https://www.fsa.go.jp/news/r6/ginkou/20250530.html>

Gillespie, A. A. (2019). *Cybercrime: Key issues and debates* (2nd ed.). Routledge. <https://doi.org/10.4324/9781351010283>



INTERPOL. (2026). *Global financial fraud threat assessment* (2nd ed.). <https://www.interpol.int/content/download/24291/file/INTERPOL%20Global%20Financial%20Fraud%20Threat%20Assessment%202026.pdf>

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, 62(10), 1356–1371. <https://doi.org/10.1177/0002764218787854>

Ministry of Internal Affairs of the Republic of Uzbekistan. (2025, May 7). *Kiberjinoyatlarni jilovlash orqali xavfsiz kiber makon yaratish. Raqamli transformatsiya sharoitida kiberjinoyatlarning barvaqt oldini olishda O'zbekiston tajribasi* [Creating a safe cyberspace by curbing cybercrime: Uzbekistan's experience in early prevention of cybercrime in the context of digital transformation]. Gov.uz. <https://gov.uz/oz/iiv/news/view/52319>

National Police Agency. (2022). *Threats in cyberspace in 2021*. https://www.npa.go.jp/english/bureau/cyber/document/Threats_in_Cyberspace_in_2021.pdf

Pleshakov, V. A., & Sklyarova, T. V. (2020). Fors-mazhornaya kibepedagogika [Force majeure cyberpedagogy]. *Homo Cyberus*, (1), 1–8. <http://journal.homocyberus.ru/Pleshakov&SklyarovaTV12020>

President of the Republic of Uzbekistan. (2023, November 30). *On measures to strengthen consumer rights protection in the field of digital products (services) and to combat offenses committed through digital technologies (Resolution No. RP-381)*. Lex.uz. <https://lex.uz/ru/docs/6681115>

President of the Republic of Uzbekistan. (2025a, January 20). *On measures to introduce a system for training professional personnel in the field of combating crimes committed through digital technologies (Resolution No. RP-17)*. Lex.uz. <https://lex.uz/ru/docs/7340341>

President of the Republic of Uzbekistan. (2025b, April 30). *On measures aimed at further strengthening efforts to combat crimes committed using information technologies (Resolution No. RP-153)*. Lex.uz. <https://lex.uz/ru/docs/7511168>

President of the Republic of Uzbekistan. (2026, March 10). *On defining the Cybersecurity Strategy of the Republic of Uzbekistan and improving the system for preventing cybercrime (Decree No. DP-38)*. Lex.uz. <https://lex.uz/ru/docs/8079279>

Rasulev, A. (2022). Kiberprestupnost: prichiny i usloviya, lichnost prestupnika [Cybercrime: Causes and conditions, identity of the perpetrator]. *Bulletin of Legal Sciences*, 22(1), 108–115. <https://inlibrary.uz/index.php/archive/article/view/9133>

Republic of Korea. (2023). *Teukbyeolbeop on jeontongsinhaegeumyung sagijiloeui sonshilbangji mit sonshilhwan-geup-e gwanhan beop* [Special Act on the prevention of loss caused by telecommunications-based financial fraud and refund for loss]. Korean Law Information Center. <https://www.law.go.kr/LSW/lsInfoP.do?chrClsCd=010203&lsiSeq=251011&urlMode=engLsInfoR&viewCls=engLsInfoR>

Republic of Uzbekistan. (2022, April 15). *On cybersecurity (Law No. LRU-764)*. Lex.uz. <https://lex.uz/ru/docs/5960609>

Sabyrbaeva, A. B. (2021). On measures to counter fraud (using the example of phishing). *State and Law*, (12), 181–185. <https://doi.org/10.31857/S102694520017465-2>

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. John Wiley & Sons.

Smith, R., & Urbas, G. (2001). *Controlling fraud on the Internet: A CAPA perspective*. Australian Institute of Criminology. <https://www.aic.gov.au/publications/rpp/rpp39>

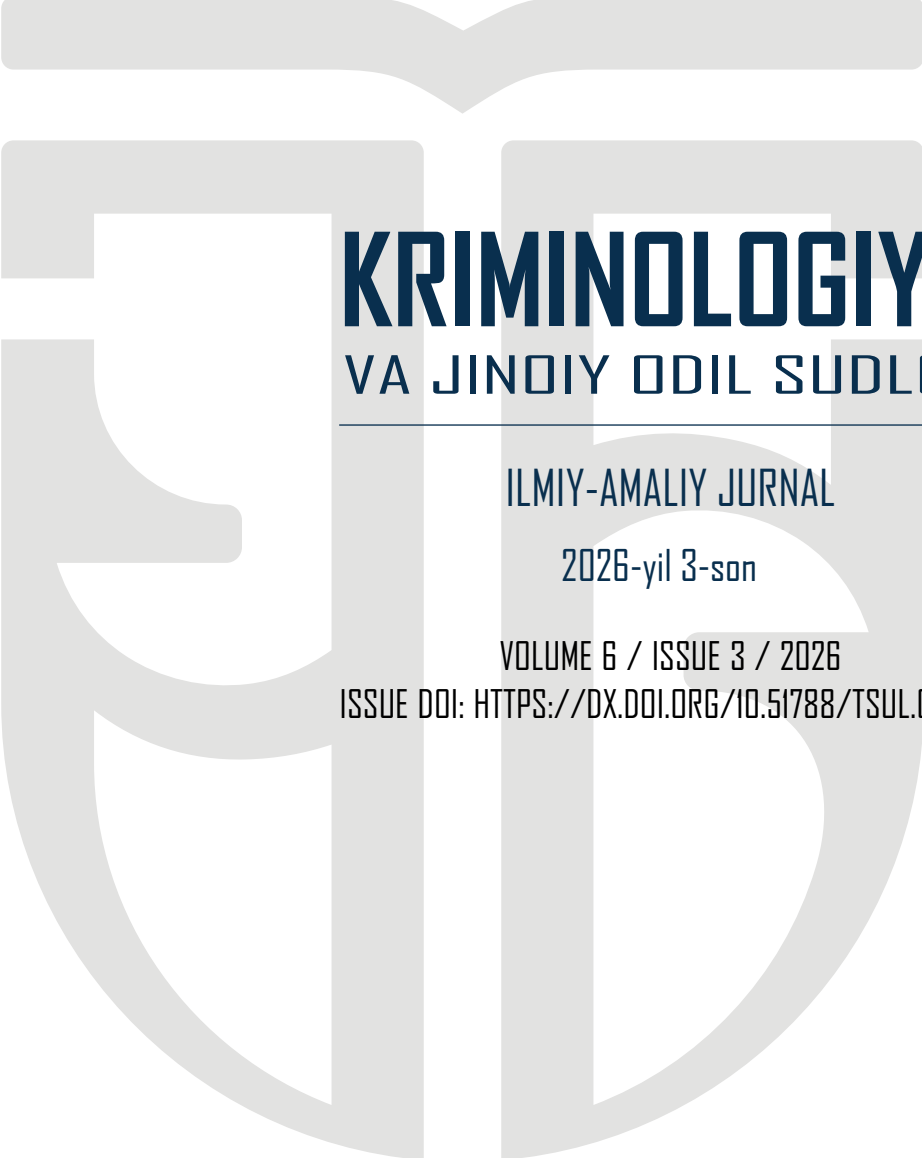
Sumsub. (2025). *Identity fraud report 2024–2025*. <https://sumsub.com/blog/guides-reports/identity-fraud-report-2024-2025/>

UzNews. (2025, December 23). *Ushcherb grazhdan ot kiberprestupleniy za poslednie pyat let prevysil 3,7 trln sumov* [Damage to citizens from cybercrime over the past five years exceeded 3.7 trillion soums]. <https://www.uznews.uz/ru/news/106012>

Van Wilsem, J. (2013). 'Bought it, but never got it': Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, 29(2), 168–178. <https://doi.org/10.1093/esr/jcr053>

Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental states: A key point in scam compliance and warning compliance in real life. *International Journal of Environmental Research and Public Health*, 19(14), 8294. <https://doi.org/10.3390/ijerph19148294>

Zhou, Y., Lee, J. R., Lin, K., & Tiwari, M. (2026). Examining cyber fraud victimization among Chinese adolescents: An integrated test of criminological theories. *Crime & Delinquency*, 72(11), 3373–3408. <https://doi.org/10.1177/00111287261440144>



KRIMINOLOGIYA VA JINOIY ODIL SUDLOV

ILMIY-AMALIY JURNAL

2026-yil 3-son

VOLUME 6 / ISSUE 3 / 2026

ISSUE DOI: [HTTPS://DX.DOI.ORG/10.51788/TSUL.CCJ.63](https://dx.doi.org/10.51788/TSUL.CCJ.63)