



YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2025-yil 2-son

VOLUME 5 / ISSUE 2 / 2025

DOI: 10.51788/tsul.jurisprudence.5.2.



Crossref
Content
Registration

ISSN: 2181-1938

DOI: 10.51788/tsul.jurisprudence

MUASSIS: TOSHKENT DAVLAT YURIDIK UNIVERSITETI

“Jurisprudensiya” – “Юриспруденция” – “Jurisprudence” huquqiy ilmiy-amaliy jurnali O‘zbekiston matbuot va axborot agentligi tomonidan 2020-yil 22-dekabrda 1140-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.

Jurnal O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi 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:

E. Sharipov, Y. Yarmolik, E. Mustafayev, K. Abduvaliyeva, Y. Mahmudov, M. Sharifova, Sh. Beknazarova

Musahhih:

S. Rasulova

Texnik muharrir:

U. Sapayev

Dizayner:

D. Rajapov

Tahririyat manzili:

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

Veb-sayt: jurisprudence.tsul.uz

E-mail: lawjournal@tsul.uz

Obuna indeksi: 1387

Tasdiqнома

№ 174625, 29.11.2023-y.

Jurnal 28.04.2025-yilda bosmaxonaga topshirildi.
Qog‘oz bichimi: A4.
Shartli bosma tabog‘i: 15,8
Adadi: 100. Buyurtma: № 84.

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

© Toshkent davlat yuridik universiteti

BOSH MUHARRIR

B. Xodjayev – Toshkent davlat yuridik universiteti Ilmiy ishlar va innovatsiyalar bo‘yicha prorektori, yuridik fanlar doktori, professor

BOSH MUHARRIR O‘RINBOSARI

J. Allayorov – Toshkent davlat yuridik universiteti Ilmiy boshqarmasi boshlig‘i, yuridik fanlar bo‘yicha falsafa doktori, dotsent

MAS‘UL MUHARRIR

N. Ramazonov – Toshkent davlat yuridik universiteti O‘zbek tili va adabiyoti kafedrasini mudiri, filologiya fanlari bo‘yicha falsafa doktori, dotsent

TAHRIR HAY‘ATI A‘ZOLARI

J. Blum – Boston kolleji Huquq maktabi professori, huquq doktori (Boston, AQSh)

M. Vishovatiy – Gdansk universiteti professori (Gdansk, Polsha)

A. Hoshimxonov – Toshkent davlat yuridik universiteti professori, yuridik fanlar doktori (Toshkent, O‘zbekiston)

M. Axmedshayeva – Toshkent davlat yuridik universiteti professori, yuridik fanlar doktori (Toshkent, O‘zbekiston)

X. Xayitov – O‘zbekiston Respublikasi Prezidenti huzuridagi Davlat boshqaruvi akademiyasi professori, yuridik fanlar doktori (Toshkent, O‘zbekiston)

I. To‘raboyev – Toshkent davlat yuridik universiteti dotsenti v.b., yuridik fanlar bo‘yicha falsafa doktori (Toshkent, O‘zbekiston)

S. Xolboyev – O‘zbekiston Respublikasi Sudyalari oliy kengashi huzuridagi Sudyalari oliy maktabi dotsenti, yuridik fanlar nomzodi (Toshkent, O‘zbekiston)

N. Raxmonkulova – Jahon iqtisodiyoti va diplomatiyasi universiteti dotsenti, yuridik fanlar doktori (Toshkent, O‘zbekiston)

Z. Esanova – Toshkent davlat yuridik universiteti professori, yuridik fanlar doktori (Toshkent, O‘zbekiston)

J. Ne‘matov – Toshkent davlat yuridik universiteti professori, yuridik fanlar doktori (Toshkent, O‘zbekiston)

M. Kurbanov – Toshkent davlat yuridik universiteti dotsenti, yuridik fanlar bo‘yicha falsafa doktori (Toshkent, O‘zbekiston)

R. Kuchkarov – Toshkent davlat yuridik universiteti dotsenti v.b., filologiya fanlari nomzodi (Toshkent, O‘zbekiston)

**УЧРЕДИТЕЛЬ: ТАШКЕНТСКИЙ
ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ
УНИВЕРСИТЕТ**

Правовой научно-практический журнал «Юриспруденция» – «Yurisprudensiya» – «Jurisprudence» зарегистрирован Агентством печати и информации Узбекистана 22 декабря 2020 года с удостоверением № 1140.

Журнал включён в перечень журналов Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций 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:

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

Корректор:

С. Расулова

Технический редактор:

У. Сапаев

Дизайнер:

Д. Ражапов

Адрес редакции:

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

Веб-сайт: jurisprudence.tsul.uz

E-mail: lawjournal@tsul.uz

Подписной индекс: 1387

Свидетельство

от 29.11.2023 № 174625.

Журнал передан в типографию
28.04.2025.

Формат бумаги: А4.

Усл. п. л. 15,8. Тираж: 100 экз.

Номер заказа: 84.

Отпечатано в типографии

Ташкентского государственного
юридического университета.

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

© Ташкентский государственный
юридический университет

ГЛАВНЫЙ РЕДАКТОР

Б. Ходжаев – доктор юридических наук, профессор, проректор по научной работе и инновациям Ташкентского государственного юридического университета

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА

Ж. Аллаёров – доктор философии по юридическим наукам, доцент, начальник управления по науке Ташкентского государственного юридического университета

ОТВЕТСТВЕННЫЙ РЕДАКТОР

Н. Рамазонов – доктор философии по филологическим наукам, доцент, заведующий кафедрой узбекского языка и литературы Ташкентского государственного юридического университета

ЧЛЕНЫ РЕДКОЛЛЕГИИ

Дж. Блум – доктор права, профессор Школы права колледжа Бостона (Бостон, США)

М. Вишоватый – профессор Гданьского университета (Гданьск, Польша)

А. Хошимхонов – доктор юридических наук, профессор Ташкентского государственного юридического университета (Ташкент, Узбекистан)

М. Ахмедшаева – доктор юридических наук, профессор Ташкентского государственного юридического университета (Ташкент, Узбекистан)

Х. Хаитов – доктор юридических наук, профессор Академии государственного управления при Президенте Республики Узбекистан (Ташкент, Узбекистан)

И. Турабоев – доктор философии по юридическим наукам, и.о. доцента Ташкентского государственного юридического университета (Ташкент, Узбекистан)

С. Холбоев – кандидат юридических наук, доцент Высшей школы судей при Высшем судейском совете Республики Узбекистан (Ташкент, Узбекистан)

Н. Рахмонкулова – доктор юридических наук, доцент Университета мировой экономики и дипломатии (Ташкент, Узбекистан)

З. Эсанова – доктор юридических наук, профессор Ташкентского государственного юридического университета (Ташкент, Узбекистан)

Ж. Нематов – доктор юридических наук, профессор Ташкентского государственного юридического университета (Ташкент, Узбекистан)

М. Курбанов – доктор философии по юридическим наукам, доцент (Ташкент, Узбекистан)

Р. Кучкаров – кандидат филологических наук, и.о. доцента Ташкентского государственного юридического университета (Ташкент, Узбекистан)

**FOUNDER: TASHKENT STATE
UNIVERSITY OF LAW**

“Yurisprudensiya” – “Юриспруденция” – “Jurisprudence” legal scientific and practical journal was registered by the Press and Information Agency of Uzbekistan on December 22, 2020 with certificate No. 1140.

The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.

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

Agreed-upon price.

Publication Officer:

O. Choriev

Editors:

E. Sharipov, Y. Yarmolik, E. Mustafaev,
K. Abduvalieva, Y. Makhmudov,
M. Sharifova, Sh. Beknazarova

Proofreader:

S. Rasulova

Technical editor:

U. Sapaev

Designer:

D. Rajapov

Editorial office address::

100047. Tashkent city,
Sayilgokh street, 35.
Phone: (0371) 233-66-36 (1169)

Website: jurisprudence.tsul.uz

E-mail: lawjournal@tsul.uz

Subscription index: 1387.

Certificate

№ 174625, 29.11.2023.

The journal is submitted to the Printing house on 28.04.2025.

Paper size: A4.

Cond.p.f: 15,8.

Units: 100. Order: № 84.

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

© Tashkent State University of Law

EDITOR-IN-CHIEF

B. Xodjaev – Deputy Rector for Scientific Affairs and Innovations of Tashkent State University of Law, Doctor of Law, Professor

DEPUTY EDITOR

J. Allayorov – Head of the Scientific Department of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law, Associate Professor

EXECUTIVE EDITOR

N. Ramazonov – Head of the Department of Uzbek Language and Literature of Tashkent State University of Law, Doctor of Philosophy (PhD) in Philology, Associate Professor

MEMBERS OF THE EDITORIAL BOARD

J. Blum – Professor of Law School of Boston College, Doctor of Law (Boston, USA)

M. Vishovatiy – Professor of the University of Gdańsk (Gdansk, Poland)

A. Khoshimkhonov – Professor of Tashkent State University of Law, Doctor of Law (Tashkent, Uzbekistan)

M. Akhmedshaeva – Professor of Tashkent State University of Law, Doctor of Law (Tashkent, Uzbekistan)

Kh. Khayitov – Professor of the Academy of Public Administration under the President of the Republic of Uzbekistan, Doctor of Law (Tashkent, Uzbekistan)

I. Turaboev – Acting Associate Professor of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Tashkent, Uzbekistan)

S. Kholboev – Associate Professor of the Supreme School of Judges under the Supreme Judicial Council of the Republic of Uzbekistan, Candidate of Legal Sciences (Tashkent, Uzbekistan)

N. Rakhmonkulova – Associate Professor of the University of World Economy and Diplomacy, Doctor of Law (Tashkent, Uzbekistan)

Z. Esanova – Professor of Tashkent State University of Law, Doctor of Law (Tashkent, Uzbekistan)

J. Ne'matov – Professor of Tashkent State University of Law, Doctor of Law (Tashkent, Uzbekistan)

M. Kurbanov – Associate Professor of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Tashkent, Uzbekistan)

R. Kuchkarov – Acting Associate Professor of Tashkent State University of Law, Candidate of Philological Sciences (Tashkent, Uzbekistan)

MUNDARIJA

12.00.02 – KONSTITUTSIYAVIY HUQUQ. MA'MURIY HUQUQ. MOLIYA VA BOJXONA HUQUQI

- 8 **ALIYEV ILHOMJON MUROD O'G'LI**
Sun'iy intellekt texnologiyalarini O'zbekiston Respublikasi adliya organlari faoliyatiga tatbiq etish

12.00.03 – FUQAROLIK HUQUQI. TADBIRKORLIK HUQUQI. OILA HUQUQI.
XALQARO XUSUSIY HUQUQ

- 17 **RUSTAMBEKOV ISLAMBEK RUSTAMBEKOVICH, GULYAMOV SAID SAIDAXRAROVICH**
Zamonaviy kiberkorupsiya: tushunchasi, muammolari va Markaziy Osiyo hududida unga qarshi kurashish choralar
- 30 **JUMAG'ULOV ALISHER ERNAPASOVICH**
Sukuk: yangi huquqiy institutga tarixiy nazar
- 38 **INOYATOV NODIRBEK XAYITBOY O'G'LI**
Sun'iy intellekt va avtonom transport vositalari: raqamli davrda huquq subyektiligi masalalari
- 47 **KAN YEKATERINA EDUARDOVNA**
Sog'liqni saqlash sohasida sun'iy intellektni joriy etishdagi normativ to'siqlar
- 55 **SAIDOV BOBUR BAXROMJONOVICH**
Metaolamlarni huquqiy tartibga solish: virtual dunyoda yurisdiksiya va intellektual mulkni himoya qilish masalalari
- 81 **NABIRAYEVA ZARNIGOR AKMALOVNA**
AQShda robot-maslahatchilar faoliyatini tartibga solish xususiyatlari
- 91 **NURULLAYEV UMIDBEK XUDAYBERDIYEVICH**
O'zbekiston va xorijiy davlatlar qonunchiligida axborot vositachisining huquqiy maqomi masalalari

12.00.04 – FUQAROLIK PROTSESSUAL HUQUQI. IQTISODIY PROTSESSUAL HUQUQI.
HAKAMLIK JARAYONI VA MEDIATSIYA

- 101 **ABDULLAYEVA RISOLAT SUNNATOVNA**
Chet el fuqarolari bilan nikohni qayd etish masalalari va bu boradagi xalqaro qonunchilik asoslari

12.00.06 – TABIIY RESURLAR HUQUQI. AGRAR HUQUQ. EKOLOGIK HUQUQ

- 111 **ABDUSAMADOVA ZARINA SHOBIDDIN QIZI**
Xorijiy mamlakatlarda yer servitutining turlari va ularning huquqiy tabiati
- 125 **TURDIYEV BOBIR SOBIROVICH**
Atrof-muhitga oid qarorlar qabul qilishda jamoatchilik ishtiroki: xalqaro standartlar va xorij tajribasi

12.00.10 – XALQARO HUQUQ

- 141 **RAXMANOV SHUXRAT NAIMOVICH**
Xalqaro tashkilotlarning diplomatik huquqining umumiy xalqaro huquq tizimidagi o'ri: nazariy-metodologik yondashuvlar

12.00.13 – INSON HUQUQLARI

- 150 **NOSIROVA MARJONA NEGMAT QIZI**
Inson huquqlarini himoya qilishda nodavlat notijorat tashkilotlari ishtiroki tushunchasi va tavsifi

12.00.14 – HUQUQBUZARLIKLAR PROFILAKTIKASI. JAMOAT XAVFSIZLIGINI TA'MINLASH.
PROBATSIIYA FAOLIYATI

- 161 **XO'JAMBERDIYEV FARRUX KOMILOVICH**
Jamoat xavfsizligini ta'minlashni takomillashtirish: Turkiya tajribasi va O'zbekiston uchun istiqbollar

СОДЕРЖАНИЕ

12.00.02 – КОНСТИТУЦИОННОЕ ПРАВО. АДМИНИСТРАТИВНОЕ ПРАВО.
ФИНАНСОВОЕ И ТАМОЖЕННОЕ ПРАВО

8 АЛИЕВ ИЛХОМЖОН МУРОД УГЛИ

Внедрение технологий искусственного интеллекта в деятельность органов юстиции
Республики Узбекистан

12.00.03 – ГРАЖДАНСКОЕ ПРАВО. ПРЕДПРИНИМАТЕЛЬСКОЕ ПРАВО. СЕМЕЙНОЕ ПРАВО.
МЕЖДУНАРОДНОЕ ЧАСТНОЕ ПРАВО

17 РУСТАМБЕКОВ ИСЛАМБЕК РУСТАМБЕКОВИЧ, ГУЛЯМОВ САИД САИДАХРАРОВИЧ

Современная киберкоррупция: понятие, проблемы и пути противодействия
в Центральноазиатском регионе

30 ЖУМАГУЛОВ АЛИШЕР ЭРНАПАСОВИЧ

Сукук: исторический взгляд на новый правовой институт

38 ИНОЯТОВ НОДИРБЕК ХАЙИТБОЙ УГЛИ

Искусственный интеллект и автономные транспортные средства: вопросы правовой
субъектности в цифровую эпоху

47 КАН ЕКАТЕРИНА ЭДУАРДОВНА

Нормативные барьеры внедрения искусственного интеллекта в здравоохранении

55 САИДОВ БОБУР БАХРОМЖОНОВИЧ

Правовое регулирование метавселенных: вопросы юрисдикции и защиты интеллектуальной
собственности в виртуальных мирах

81 НАБИРАЕВА ЗАРНИГОР АКМАЛОВНА

Особенности регулирования деятельности роботов-консультантов в США

91 НУРУЛЛАЕВ УМИДБЕК ХУДАЙБЕРДИЕВИЧ

Правовой статус информационного посредника в законодательстве Узбекистана и зарубежных стран

12.00.04 – ГРАЖДАНСКОЕ ПРОЦЕССУАЛЬНОЕ ПРАВО. ЭКОНОМИЧЕСКОЕ
ПРОЦЕССУАЛЬНОЕ ПРАВО. АРБИТРАЖ И МЕДИАЦИЯ

101 АБДУЛЛАЕВА РИСОЛАТ СУННАТОВНА

Вопросы регистрации браков с иностранными гражданами и международно-правовые основы
в этой сфере

12.00.06 – ПРИРОДОРЕСУРСНОЕ ПРАВО. АГРАРНОЕ ПРАВО. ЭКОЛОГИЧЕСКОЕ ПРАВО

111 АБДУСАМАДОВА ЗАРИНА ШОБИДДИН КИЗИ

Типы сервитутов в зарубежных странах и их правовая природа

125 ТУРДИЕВ БОБИР СОБИРОВИЧ

Участие общественности в принятии решений, касающихся окружающей среды:
международные стандарты и зарубежный опыт

12.00.10 – МЕЖДУНАРОДНОЕ ПРАВО

141 РАХМАНОВ ШУХРАТ НАИМОВИЧ

Место дипломатического права международных организаций в системе международного права:
теоретико-методологические подходы

12.00.13 – ПРАВА ЧЕЛОВЕКА

150 НОСИРОВА МАРЖОНА НЕГМАТ КИЗИ

Понятие и характеристика участия некоммерческих негосударственных организаций
в защите прав человека

12.00.14 – ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПНОСТИ. ОБЕСПЕЧЕНИЕ ОБЩЕСТВЕННОЙ
БЕЗОПАСНОСТИ. ПРОБАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ

161 ХУЖАМБЕРДИЕВ ФАРРУХ КОМИЛОВИЧ

Совершенствование обеспечения общественной безопасности: опыт Турции и перспективы для
Узбекистана

CONTENTS

12.00.02 – CONSTITUTIONAL LAW. ADMINISTRATIVE LAW. FINANCIAL AND CUSTOMS LAW

- 8 **ALIEV ILKHOMJON MUROD UGLI**
Implementation of artificial intelligence technologies in the activities of the justice authorities of the Republic of Uzbekistan

12.00.03 – CIVIL LAW. BUSINESS LAW. FAMILY LAW. INTERNATIONAL PRIVATE LAW

- 17 **RUSTAMBEKOV ISLAMBEK RUSTAMBEKOVICH, GULYAMOV SAID SAIDAKHRAROVICH**
Modern cybercorruption: concept, challenges, and countermeasures in the Central Asian region
- 30 **JUMAGULOV ALISHER ERNAPASOVICH**
Sukuk: a historical view of the new legal institution
- 38 **INOYATOV NODIRBEK KHAYITBOY UGLI**
Artificial intelligence and autonomous vehicles: issues of legal subjectivity in the digital era
- 47 **KAN EKATERINA EDUARDOVNA**
Regulatory barriers to the implementation of artificial intelligence in healthcare
- 55 **SAIDOV BOBUR BAKHROMJONOVICH**
Legal regulation of metaverses: issues of jurisdiction and intellectual property protection in virtual worlds
- 81 **NABIRAYEVA ZARNIGOR AKMALOVNA**
Features of regulating robo-advisors in the USA
- 91 **NURULLAEV UMIDBEK KHUDAYBERDIYEVICH**
Issues of the legal status of an information intermediary in the legislation of Uzbekistan and foreign countries

12.00.04 – CIVIL PROCEDURAL LAW. ECONOMIC PROCEDURAL LAW. ARBITRATION PROCESS AND MEDIATION

- 101 **ABDULLAEVA RISOLAT SUNNATOVNA**
Issues of marriage registration with foreign citizens and the foundations of international legislation in this regard

12.00.06 – THE LAW OF NATURAL RESOURCES. AGRARIAN LAW. ENVIRONMENTAL LAW

- 113 **ABDUSAMADOVA ZARINA SHOBIDDINOVNA**
Types of servitudes in foreign countries and their legal nature
- 125 **TURDIEV BOBIR SOBIROVICH**
Public participation in environmental decision-making: international standards and foreign experience

12.00.10 – INTERNATIONAL LAW

- 141 **RAKHMANOV SHUKHRAT NAIMOVICH**
The role of the diplomatic law of international organizations in the general system of international law: theoretical and methodological approaches

12.00.13 – HUMAN RIGHTS

- 150 **NOSIROVA MARJONA NEGMAT KIZI**
The concept and descriptions of the participation of non-governmental non-profit organizations in the protection of human rights

12.00.14 – CRIME PREVENTION. ENSURING PUBLIC SAFETY. PROBATION ACTIVITY

- 161 **KHUJAMBERDIYEV FARRUKH KOMILOVICH**
Improving public safety ensuring: the experience of turkey and prospects for Uzbekistan

Kelib tushgan / Получено / Received: 20.03.2025
Qabul qilingan / Принято / Accepted: 19.04.2025
Nashr etilgan / Опубликовано / Published: 28.04.2025

DOI: 10.51788/tsul.jurisprudence.5.2./BUX05819

UDC: 343.352:004.056(045)(575.1)

СОВРЕМЕННАЯ КИБЕРКОРРУПЦИЯ: ПОНЯТИЕ, ПРОБЛЕМЫ И ПУТИ ПРОТИВОДЕЙСТВИЯ В ЦЕНТРАЛЬНОАЗИАТСКОМ РЕГИОНЕ

Рустамбеков Исламбек Рустамбекович,

доктор юридических наук, профессор,

врио ректора Ташкентского государственного юридического университета

ORCID: 0000-0002-8869-8399

e-mail: i.rustambekov@tsul.uz

Гулямов Саид Саидахарович,

доктор юридических наук, профессор,

председатель Совета молодых учёных

Академии наук Республики Узбекистан,

заведующий кафедрой «Киберправо»

Ташкентского государственного юридического университета

ORCID: 0000-0002-2299-2122

e-mail: said.gulyamov1976@gmail.com

Аннотация. В настоящем исследовании рассматривается феномен киберкоррупции – использование цифровых технологий в целях реализации коррупционных практик – в контексте Центральноазиатского региона. Целью работы является анализ сущности киберкоррупции, выявление её ключевых проявлений, а также разработка рекомендаций по противодействию данной угрозе. Методологическая основа исследования включает комплексный анализ правовых механизмов в области кибербезопасности и антикоррупционной политики, сравнительное изучение международного опыта и обобщение рекомендаций международных организаций. Полученные результаты свидетельствуют о повышающейся уязвимости региона перед лицом киберкоррупции, что обусловлено недостаточной адаптацией национальных правовых систем к условиям цифровой трансформации, ограниченными ресурсами правоохранительных органов и слабой региональной координацией. В числе предложенных мер: совершенствование нормативно-правовой базы, развитие институциональных механизмов и расширение форматов межгосударственного сотрудничества для эффективного предупреждения и пресечения киберкоррупции. Представленный анализ может служить основой для выработки комплексной политики в сфере цифровой безопасности и обеспечения прозрачности в странах Центральной Азии.

Ключевые слова: киберкоррупция, цифровые финансы, кибербезопасность, правовое регулирование, криптовалюты, цифровые активы, трансграничное сотрудничество, Центральная Азия

ZAMONAVIY KIBERKORRUPSIYA: TUSHUNCHASI, MUAMMOLARI VA MARKAZIY OSIYO HUDUDIDA UNGA QARSHI KURASHISH CHORALARI

Rustambekov Islambek Rustambekovich,
Toshkent davlat yuridik universiteti rektori v.v.b.,
yuridik fanlar doktori, professor

Gulyamov Said Saidaxrarovich,
Toshkent davlat yuridik universiteti Kiber huquq kafedrası mudiri,
O'zbekiston Respublikasi Fanlar akademiyasi huzuridagi
Yosh olimlar kengashi raisi, yuridik fanlar doktori, professor

Annotatsiya. Ushbu tadqiqotda raqamli texnologiyalar korrupsion amaliyotlarni amalga oshirish vositasi sifatida qo'llanadigan kiberkorrupsiya fenomeni Markaziy Osiyo mintaqasi kontekstida ko'rib chiqiladi. Tadqiqotning maqsadi – kiberkorrupsiyaning mohiyatini tahlil qilish, uning asosiy ko'rinishlarini aniqlash va ushbu tahdidga qarshi kurashish bo'yicha tavsiyalar ishlab chiqishdan iborat. Tadqiqotning metodologik asosi kiberxavfsizlik va korrupsiyaga qarshi kurash sohasidagi huquqiy mexanizmlarni kompleks tahlil qilish, xalqaro tajribaning qiyosiy o'rganilishi va xalqaro tashkilotlar tavsiyalarini umumlashtirishni o'z ichiga oladi. Olingan natijalar hududning kiberkorrupsiya oldida zaifligi ortib borayotganidan dalolat beradi, bu esa milliy huquqiy tizimlarning raqamli transformatsiya sharoitlariga yetarlicha moslashmaganligi, huquqni muhofaza qilish organlarining cheklangan resurslari va zaif mintaqaviy muvofiqlashtirilganligidandir. Taklif etilgan chora-tadbirlar qatoriga normativ-huquqiy bazani takomillashtirish, institutsional mexanizmlarni rivojlantirish va kiberkorrupsiyaning oldini olish hamda unga barham berishda davlatlararo hamkorlikni kengaytirish kiradi. Ushbu tahlil Markaziy Osiyodagi raqamli xavfsizlik va oshkoralikni ta'minlash bo'yicha kompleks siyosatni shakllantirishda muhim asos bo'lib xizmat qilishi mumkin.

Kalit so'zlar: kiberkorrupsiya, raqamli moliya, kiberxavfsizlik, huquqiy tartibga solish, kriptovalyutalar, raqamli aktivlar, transchegaraviy hamkorlik, Markaziy Osiyo

MODERN CYBERCORRUPTION: CONCEPT, CHALLENGES, AND COUNTERMEASURES IN THE CENTRAL ASIAN REGION

Rustambekov Islambek Rustambekovich,
Acting Rector of Tashkent State University of Law,
Doctor of Science in Law, Professor

Gulyamov Said Saidaxrarovich,
Head of the Department of Cyber Law,
Chairman of the Council of Young Scientists
at the Academy of Sciences of the Republic of Uzbekistan,
Tashkent State University of Law,
Doctor of Science in Law, Professor

Abstract. This study examines the phenomenon of cybercorruption—the use of digital technologies to implement corrupt practices—in the context of the Central Asian region. The purpose of the work is to analyze the essence of cybercorruption, identify its key manifestations, and develop recommendations for countering this threat. The methodological basis of the research includes a comprehensive analysis of legal mechanisms in the field of cybersecurity and anti-corruption policy, a comparative study of international experience, and the generalization of recommendations of international organizations.

The results indicate increasing vulnerability of the region to cybercorruption, which is due to insufficient adaptation of national legal systems to the conditions of digital transformation, limited resources of law enforcement agencies, and weak regional coordination. Among the proposed measures are improving the regulatory framework, developing institutional mechanisms, and expanding the formats of interstate cooperation for the effective prevention and suppression of cybercorruption. The presented analysis can serve as a foundation for developing a comprehensive policy in the field of digital security and ensuring transparency in Central Asian countries.

Keywords: cybercorruption, digital finance, cybersecurity, legal regulation, cryptocurrencies, digital assets, cross-border cooperation, Central Asia

Введение

Коррупция представляет собой многоаспектную глобальную проблему, которая налагает значительные социальные, экономические и политические издержки на общества во всём мире [1]. По оценкам Всемирного экономического форума, глобальные потери от коррупции составляют около 2,6 трлн долларов США, или 5 % мирового ВВП [2]. Однако в последние годы наблюдается качественная трансформация коррупционных практик, связанная с цифровизацией экономики и общества. Появление и распространение новых цифровых технологий, таких как криптовалюты, онлайн-банкинг, блокчейн и шифрованные коммуникации, создали условия для эволюции коррупции в новую форму – киберкоррупцию [3].

Киберкоррупция может быть определена как использование цифровых технологий и инфраструктуры для осуществления и сокрытия коррупционных действий, а также эксплуатация цифровых пространств и активов в качестве объектов коррупции. В отличие от традиционных форм коррупции, киберкоррупция характеризуется трансграничным характером, технологической сложностью и повышенной анонимностью, что создаёт значительные вызовы для существующих правовых систем и правоохранительных структур [4].

Государства Центральной Азии (Казахстан, Кыргызстан, Таджикистан, Туркменистан и Узбекистан) находятся в особенно уязвимом положении перед лицом

этой растущей угрозы. С одной стороны, эти страны активно продвигают цифровую трансформацию экономики, внедряя электронное правительство, цифровые финансовые услуги и развивая ИКТ-инфраструктуру, с другой – правовые и институциональные основы в области кибербезопасности и противодействия коррупции в регионе зачастую отстают от темпов технологических изменений [5]. Это создаёт благоприятные условия для распространения различных форм киберкоррупции.

Данное исследование направлено на решение следующих исследовательских вопросов:

1. Какова сущность киберкоррупции и каковы её ключевые проявления в Центральноазиатском регионе?
2. Каковы основные недостатки существующих правовых и институциональных основ, создающие условия для распространения киберкоррупции?
3. Какие нормативно-правовые акты и меры должны быть приняты в странах Центральной Азии для эффективного противодействия киберкоррупции?

Актуальность исследования обусловлена стремительным проникновением цифровых технологий во все сферы общественной жизни в регионе и необходимостью своевременной адаптации правовых и институциональных механизмов для предотвращения новых форм коррупции. Новизна исследования заключается в комплексном анализе киберкоррупции как междисциплинарной проблемы, находящейся

ся на пересечении правовых, технологических и социально-экономических аспектов.

Теоретические основы исследования киберкоррупции

Концептуализация киберкоррупции

Для формирования теоретической рамки анализа необходимо чётко разграничить понятия «киберкоррупция», «киберпреступность» и «кибермошенничество». Хотя эти термины часто используются взаимозаменяемо, они отражают разные, хотя и пересекающиеся феномены.

Киберпреступность представляет собой широкую категорию противоправных деяний, совершаемых с использованием компьютерных систем и сетей [6]. Это понятие охватывает разнообразные правонарушения от взлома компьютерных систем до кражи данных и распространения вредоносного программного обеспечения.

Кибермошенничество является подкатегорией киберпреступности и относится к деяниям, направленным на обман с целью получения финансовой или материальной выгоды в цифровой среде [7].

Киберкоррупция, в свою очередь, имеет специфические характеристики, отличающие её от других форм киберпреступности. Основываясь на классическом определении коррупции как «злоупотребления вверенной властью в частных интересах» [8], киберкоррупцию можно определить как использование цифровых технологий и систем для злоупотребления властью или доверием с целью получения неправомерных выгод. Ключевым отличием киберкоррупции от других форм киберпреступности является наличие элемента злоупотребления властью или доверием, обычно связанного с государственными или корпоративными институтами.

Киберкоррупция может проявляться в различных формах [9]:

1. Традиционная коррупция, фасилируемая цифровыми технологиями, – например, использование криптовалют для

выплаты взяток или шифрованных мессенджеров для организации коррупционных схем.

2. Коррупция в сфере управления цифровыми активами и системами – например, манипуляции с электронными системами государственных закупок или незаконное распределение цифровых ресурсов, таких как радиочастотный спектр.

3. Системный захват цифровой регуляторной среды – например, формирование законодательства в области кибербезопасности или защиты данных в интересах определённых групп.

Взаимосвязь цифровизации и коррупционных рисков

Процессы цифровизации создают двойственные эффекты в контексте коррупции. С одной стороны, внедрение цифровых технологий потенциально способствует прозрачности и подотчётности, сокращая возможности для коррупции [10]. Электронные системы государственных услуг, цифровые платформы государственных закупок и автоматизированные процессы принятия решений могут минимизировать человеческий фактор и снизить дискреционные полномочия, традиционно создающие почву для коррупции. С другой стороны, цифровизация также создаёт новые возможности для коррупции через [3]:

- *технологическую сложность* – многие цифровые системы и процессы сложны для понимания непрофессионалами, что создаёт информационную асимметрию и затрудняет общественный контроль;

- *цифровые монополии и олигополии* – концентрация контроля над цифровой инфраструктурой и ключевыми технологиями создаёт новые формы власти, которые могут стать объектом коррупции;

- *анонимность и трансграничность* – цифровые технологии облегчают анонимное и трансграничное перемещение средств, что усложняет отслеживание коррупционных транзакций.

Эмпирические исследования показывают, что связь между цифровизацией и снижением коррупции не является автоматической и зависит от качества институтов, правовой среды и политической воли [11]. В странах с сильными институтами цифровизация, действительно, способствует снижению коррупции, тогда как в странах со слабыми институтами эффект может быть противоположным – цифровизация может способствовать возникновению более сложных и трудно выявляемых форм коррупции.

Материалы и методы

В данном исследовании используются четыре взаимодополняющих методологических подхода для изучения тенденций киберкоррупции в государствах Центральной Азии и определения ответных мер на эту политическую проблему. Во-первых, проводится детальный обзор существующих правовых основ и политики управления, связанных с киберпреступностью, кибербезопасностью и противодействием коррупции на национальном уровне в Центральной Азии. Во-вторых, анализируется текущий дискурс и данные об измеренных и оценочных киберкоррупционных действиях, происходящих в регионе, подготовленные государственными органами, международными организациями и журналистами-исследователями. В-третьих, проводится сравнительный анализ политических основ и заявленных форм киберкоррупции в Центральной Азии с другими развивающимися странами. Наконец, обобщаются предлагаемые правовые, институциональные и технологические меры по противодействию рискам киберкоррупции, исходящие от глобальных органов по стандартизации, региональных организаций и национальных правительств.

Эти четыре источника доказательств интегрированы для определения контуров киберкоррупции как концепции,

картирования её текущих проявлений в Центральной Азии, изучения слабых мест, позволяющих ей расти, а также для выработки ответных мер, укоренённых в правовых прецедентах, передовой институциональной практике и технологических решениях, возникающих во всём мире.

Результаты исследования

Проявления киберкоррупции в глобальном контексте

Прежде чем анализировать специфику Центральноазиатского региона, целесообразно рассмотреть наиболее распространённые проявления киберкоррупции в мировой практике, уделяя особое внимание примерам из опыта развитых стран, которые могут служить предостережением для развивающихся экономик.

1. Манипуляции с системами электронных закупок

Системы электронных государственных закупок были внедрены во многих странах для повышения прозрачности и эффективности. Однако эти системы также становятся объектами киберкоррупции [12]. В Италии была выявлена схема, при которой технические спецификации в электронных тендерах формулировались таким образом, чтобы соответствовать возможностям конкретных поставщиков [13]. Такие манипуляции становятся возможными благодаря техническим уязвимостям систем электронных закупок, недостаточной защите против инсайдерских угроз и ограниченному пониманию цифровых процессов со стороны контролирующих органов.

2. Использование криптовалют в коррупционных схемах

Криптовалюты, обеспечивающие высокий уровень анонимности транзакций, становятся всё более популярным инструментом для коррупционных выплат. В США в 2022 году был раскрыт случай, когда федеральный служащий получал взятки в биткоинах за предоставление конфи-

денциальной информации [14]. Особую обеспокоенность вызывает использование так называемых «приватных» криптовалют, таких как Monero или Zcash, которые предоставляют повышенный уровень анонимности по сравнению с Bitcoin, что ещё больше усложняет отслеживание коррупционных транзакций [15].

3. Коррупция в управлении цифровыми активами

Распределение и управление цифровыми активами, такими как радиочастотный спектр, домены верхнего уровня и цифровые идентификаторы, также становится областью коррупционных рисков. В 2017 году было начато расследование в отношении нерегулярностей при распределении частот 4G, где определённые телекоммуникационные компании получили преференции [16]. В Испании в 2019 году был выявлен случай коррупции при распределении государственных контрактов на развитие цифровой инфраструктуры [17].

4. Манипуляции с цифровыми данными

Цифровые данные становятся ценным ресурсом, и их искажение или неправомерное использование может быть элементом коррупционных схем. В Великобритании в 2016 году были выявлены случаи манипуляций с данными о загрязнении воздуха, которые проводились в интересах определённых промышленных предприятий [18]. В Японии в 2018 году стало известно о манипуляциях с данными банковских стресс-тестов, что позволяло финансовым учреждениям избегать более строгого регулирования [19].

5. Коррупция в сфере кибербезопасности

Особую озабоченность вызывает коррупция в области кибербезопасности, которая подрывает цифровую защиту государства и общества. В США за последние годы были выявлены множественные случаи, связанные с киберкоррупцией и киберпреступлениями [20]. В Швеции в 2019 году был раскрыт случай, когда го-

сударственный служащий, ответственный за кибербезопасность, скрыл информацию о серьёзных уязвимостях в обмен на вознаграждение [21].

Эти примеры из опыта развитых стран демонстрируют разнообразие и сложность киберкоррупционных схем, а также подчёркивают необходимость комплексного подхода к их противодействию. Государства Центральной Азии, находящиеся на ранних стадиях цифровой трансформации, имеют возможность учесть эти уроки при формировании своих подходов к обеспечению цифровой прозрачности и безопасности.

Анализ правовых и институциональных основ в Центральной Азии

1. Современное состояние нормативно-правовой базы

Анализ законодательства стран Центральной Азии выявляет несколько ключевых проблем, которые ограничивают эффективность противодействия киберкоррупции.

Неадаптированные определения коррупционных преступлений: во многих странах региона законодательные определения коррупционных преступлений, таких как взяточничество и злоупотребление должностными полномочиями, сформулированы с акцентом на материальные активы. Например, в Уголовном кодексе Республики Узбекистан (статья 211) взятка определяется как «материальные ценности или имущественная выгода», что не всегда позволяет эффективно применять эту норму к цифровым активам, таким как криптовалюты или виртуальные товары [22]. Аналогичные проблемы наблюдаются в законодательстве Таджикистана и Кыргызстана.

Фрагментированность регулирования: наблюдается разрыв между законодательством о противодействии коррупции и законодательством о кибербезопасности и киберпреступности. Например, в Казахстане Закон «О противодействии корруп-

ции» и Закон «Об электронном документе и электронной цифровой подписи» функционируют параллельно, без достаточных механизмов интеграции [23]. Это создаёт правовые пробелы, которые могут быть использованы для киберкоррупционной деятельности.

Различия в региональных подходах: страны Центральной Азии демонстрируют разный уровень развития законодательства в области кибербезопасности и борьбы с коррупцией. Узбекистан и Кыргызстан приняли специальный закон о кибербезопасности, тогда как Таджикистан и Туркменистан регулируют эти вопросы преимущественно в рамках общего законодательства об информационной безопасности или через отдельные положения в различных нормативных актах [24]. Эта неоднородность затрудняет региональную координацию в борьбе с киберкоррупцией.

Ограниченное регулирование цифровых финансов: регулирование новых финансовых технологий, таких как криптовалюты и блокчейн, которые могут использоваться в коррупционных схемах, находится на начальном этапе развития во всех странах региона. Например, в Узбекистане криптовалюты были легализованы в 2018 году, но регуляторная база для мониторинга и контроля соответствующих транзакций остаётся недостаточно развитой [25].

2. Институциональные механизмы и их эффективность

Страны Центральной Азии создали различные институциональные механизмы для борьбы с коррупцией и обеспечения кибербезопасности, однако их эффективность в противодействии киберкоррупции вызывает вопросы.

Множественность и пересечение полномочий: во многих странах региона наблюдается дублирование функций между различными государственными органами. Например, в Казахстане вопросами кибербезопасности занимаются Комитет

национальной безопасности, Министерство цифрового развития и Государственная техническая служба, при этом чёткое разграничение полномочий между ними отсутствует [23]. Аналогичная ситуация наблюдается в сфере противодействия коррупции, где функции распределены между антикоррупционными агентствами, правоохранительными органами и специализированными подразделениями в различных министерствах.

Ограниченный технический потенциал: большинство антикоррупционных органов в регионе не обладают достаточными техническими возможностями для выявления и расследования сложных киберкоррупционных схем. Недостаток специалистов в области цифровой форензики, отсутствие современного оборудования и ограниченный доступ к специализированному программному обеспечению для анализа цифровых доказательств снижают эффективность борьбы с киберкоррупцией [11].

Недостаточное межведомственное взаимодействие: наблюдается ограниченное сотрудничество между органами, ответственными за кибербезопасность, и антикоррупционными структурами. Например, в Узбекистане Агентство по борьбе с коррупцией и Центр кибербезопасности функционируют относительно автономно, что затрудняет комплексный подход к проблеме киберкоррупции [6].

Ограниченное участие частного сектора и гражданского общества: в странах региона наблюдается недостаточное вовлечение частного сектора и гражданского общества в противодействие киберкоррупции. В развитых странах частные компании, особенно в финансовом и телекоммуникационном секторах, часто играют ключевую роль в выявлении подозрительных транзакций и кибератак, которые могут быть связаны с коррупцией [26].

3. Международное и региональное сотрудничество

Страны Центральной Азии участвуют в различных международных инициативах в области противодействия коррупции и кибербезопасности, однако уровень их вовлечённости различается.

Участие в международных конвенциях: все страны региона ратифицировали Конвенцию ООН против коррупции, что создаёт общую правовую основу для международного сотрудничества. Однако в отношении кибербезопасности ситуация менее однородна. Например, ни одна из стран Центральной Азии не является участником Будапештской конвенции о киберпреступности, которая обеспечивает международную правовую основу для борьбы с киберпреступностью [27].

Региональные инициативы: в рамках Шанхайской организации сотрудничества (ШОС), членами которой являются Казахстан, Кыргызстан, Таджикистан и Узбекистан, разрабатываются механизмы сотрудничества в области информационной безопасности. В 2019 году был принят план действий по реализации Стратегии развития ШОС до 2025 года, который включает меры по укреплению информационной безопасности [28]. Однако эти инициативы не всегда достаточно конкретны в отношении противодействия киберкоррупции.

Техническая помощь и обмен опытом: страны региона участвуют в программах технической помощи, реализуемых международными организациями, такими как ООН, ОБСЕ и Всемирный банк. Эти программы включают обучение специалистов, разработку методологий и предоставление технического оборудования для борьбы с коррупцией и киберпреступностью [6].

Анализ результатов исследования

Рекомендации по совершенствованию нормативно-правовой базы и институциональных механизмов

1. Совершенствование законодательства
Для эффективного противодействия киберкоррупции странам Центральной Азии рекомендуется:

- расширение определений коррупционных преступлений: необходимо адаптировать определения коррупционных преступлений, включив в них цифровые активы и нематериальные выгоды. Например, определение взятки должно охватывать не только традиционные материальные ценности, но и криптовалюты, виртуальные активы и доступ к цифровым данным. Это соответствует рекомендациям ОЭСР по модернизации антикоррупционного законодательства в цифровую эпоху [29];

- принятие специализированного законодательства о киберкоррупции: странам региона следует рассмотреть возможность принятия специализированных законов, направленных на противодействие киберкоррупции. Такие законы могли бы определить особые составы преступлений, такие как манипуляции с электронными системами государственных закупок, незаконное использование цифровых государственных ресурсов и коррупция в сфере распределения цифровых активов. Примером может служить Digital Trust Act Сингапура, который включает положения о противодействии цифровому мошенничеству и коррупции [30];

- гармонизация законодательства о кибербезопасности и противодействии коррупции: необходимо обеспечить согласованность законодательства в области кибербезопасности и противодействия коррупции, устранив существующие пробелы и противоречия. Это может включать создание единых терминологических стандартов, унификацию процедур расследования и согласование санкций за соответствующие правонарушения;

- регулирование цифровых финансов: странам Центральной Азии рекомендует-

ся разработать комплексное регулирование цифровых финансовых технологий, включая криптовалюты и блокчейн. Такое регулирование должно обеспечивать баланс между инновационным развитием и предотвращением использования этих технологий в коррупционных схемах. Модельной основой может служить Fifth Anti-Money Laundering Directive Европейского союза, которая устанавливает требования по идентификации клиентов и мониторингу транзакций для криптовалютных бирж [31];

- принятие законодательства о защите данных: учитывая, что киберкоррупция часто связана с неправомерным использованием данных, странам Центральной Азии рекомендуется принять современное законодательство о защите данных, соответствующее международным стандартам, таким как General Data Protection Regulation (GDPR) Европейского союза. Такое законодательство должно включать положения о прозрачности обработки данных, ограничении целей использования данных и ответственности за нарушения [32].

2. Укрепление институциональных механизмов:

Для эффективного противодействия киберкоррупции странам Центральной Азии рекомендуется:

- создание специализированных подразделений: в рамках существующих антикоррупционных органов целесообразно создать специализированные подразделения по борьбе с киберкоррупцией, укомплектованные экспертами в области информационных технологий, цифровой форензики и финансового анализа. Такой подход успешно реализован в Эстонии, где в составе Бюро по противодействию коррупции создан отдел по борьбе с цифровыми финансовыми преступлениями [33];

- развитие технического потенциала: необходимо инвестировать в развитие

технических возможностей антикоррупционных органов, включая приобретение современного оборудования для цифровой форензики, специализированного программного обеспечения для анализа данных и обучение персонала современным методам расследования киберкоррупции. Примером такого подхода может служить программа Digital Investigation Enhancement Program, реализуемая в Великобритании [34];

- создание механизмов межведомственной координации: рекомендуется создать формальные механизмы координации между антикоррупционными органами и структурами, ответственными за кибербезопасность. Это может быть реализовано в форме межведомственных рабочих групп, совместных оперативных центров или специализированных координационных советов. Такие механизмы успешно функционируют в Нидерландах, где создан National Cyber Security Centre, объединяющий усилия различных ведомств [35];

- вовлечение частного сектора и гражданского общества: необходимо разработать механизмы для активного участия частного сектора и гражданского общества в противодействии киберкоррупции. Это может включать создание платформ для обмена информацией о киберугрозах, разработку каналов для безопасного сообщения о случаях киберкоррупции и программы повышения осведомлённости населения. Успешным примером является Cyber Defense Alliance в Великобритании, объединяющий финансовые учреждения и правоохранительные органы [36];

- развитие системы цифрового мониторинга: рекомендуется внедрение систем цифрового мониторинга для выявления подозрительных действий в государственных информационных системах, особенно тех, которые связаны с распределением государственных ресурсов. Та-

кие системы могут использовать алгоритмы машинного обучения для выявления аномальных паттернов, которые могут указывать на коррупционную деятельность. Пример такого подхода – система ARACHNE, используемая Европейской комиссией для выявления рисков мошенничества и коррупции в проектах, финансируемых ЕС [37].

3. Расширение международного и регионального сотрудничества

Для эффективного противодействия трансграничной киберкоррупции странам Центральной Азии рекомендуется:

- присоединение к международным конвенциям: странам региона следует рассмотреть возможность присоединения к Будапештской конвенции о киберпреступности, которая обеспечивает международную правовую основу для сотрудничества в расследовании киберпреступлений. Членство в Конвенции не только предоставит доступ к международным механизмам сотрудничества, но и будет способствовать гармонизации национального законодательства с международными стандартами [27];

- развитие региональных механизмов сотрудничества: в рамках существующих региональных объединений, таких как ШОС или Содружество Независимых Государств, рекомендуется разработать специализированные механизмы для сотрудничества в противодействии киберкоррупции. Это может включать создание региональных центров обмена информацией о киберугрозах, совместных следственных групп и программ обмена опытом [38];

- создание региональной платформы для обмена информацией: рекомендуется создание региональной платформы для обмена информацией о киберугрозах и подозрительных транзакциях, которая могла бы объединить правоохранительные органы, финансовые учреждения и телекоммуникационные компании стран

Центральной Азии. Такая платформа могла бы функционировать по модели Financial Intelligence Units (FIUs), существующих в странах Европейского союза [39];

- участие в программах технической помощи: странам региона рекомендуется активно участвовать в программах технической помощи, предлагаемых международными организациями, такими как ООН, ОБСЕ и Всемирный банк. Эти программы могут предоставить доступ к передовым методикам, технологиям и знаниям в области противодействия киберкоррупции [40];

- сотрудничество с глобальными технологическими компаниями: рекомендуется развивать сотрудничество с глобальными технологическими компаниями, такими как Microsoft, Google и IBM, которые могут предоставить экспертную поддержку в области кибербезопасности и противодействия цифровому мошенничеству. Пример такого сотрудничества – партнёрство между Microsoft и правительством Сингапура в рамках программы Digital Crime Unit [41].

4. Внедрение технологических решений

Для повышения эффективности противодействия киберкоррупции странам Центральной Азии рекомендуется внедрение следующих технологических решений:

- блокчейн для обеспечения прозрачности: технология блокчейн может быть использована для обеспечения прозрачности и неизменности данных в критически важных государственных процессах, таких как государственные закупки, регистрация собственности и распределение государственных субсидий. Примером успешного применения блокчейн-технологий в государственном управлении является система e-Estonia в Эстонии [42];

- инструменты анализа больших данных: рекомендуется внедрение инструментов анализа больших данных для вы-

явления подозрительных паттернов и связей, которые могут указывать на коррупционную деятельность. Такие инструменты могут анализировать разнородные источники данных, включая государственные реестры, финансовые транзакции и социальные сети, для выявления необычных активностей. Пример такого подхода – система Corruption Hunter Network, разработанная Всемирным банком [43];

- системы мониторинга целостности данных: для предотвращения манипуляций с цифровыми данными рекомендуется внедрение систем мониторинга целостности данных, которые могут выявлять несанкционированные изменения в критически важных информационных системах. Такие системы используются в банковском секторе США для предотвращения мошенничества с финансовыми данными [44];

- автоматизированные системы проверки соответствия: рекомендуется внедрение автоматизированных систем для проверки соответствия действий государственных служащих и использования государственных ресурсов установленным нормам и правилам. Такие системы могут автоматически выявлять отклонения от стандартных процедур и сигнализировать о потенциальных рисках коррупции. Пример такого подхода – система SIIGAT, используемая в Мексике для мониторинга государственных контрактов [26];

- цифровые платформы для общественного контроля: рекомендуется создание цифровых платформ, позволяющих гражданам участвовать в мониторинге использования государственных ресурсов и сообщать о потенциальных случаях коррупции. Такие платформы могут повысить прозрачность государственного управления и способствовать формированию культуры нетерпимости к коррупции. Успешным примером является платформа I Paid A Bribe в Индии [45].

Выводы

Киберкоррупция представляет собой комплексную проблему, находящуюся на пересечении правовых, технологических и социально-экономических аспектов. В условиях ускоренной цифровой трансформации стран Центральной Азии эта проблема приобретает особую актуальность и требует соответствующих решений.

Анализ глобального опыта противодействия киберкоррупции демонстрирует многообразие её проявлений: от манипуляций с системами электронных закупок до использования криптовалют в коррупционных схемах и коррупции в сфере управления цифровыми активами. Примеры из развитых стран служат ценным предостережением для развивающихся экономик Центральной Азии, позволяя предвидеть потенциальные риски и своевременно разработать превентивные меры.

Оценка текущего состояния правовых и институциональных основ в странах Центральной Азии выявляет ряд ключевых проблем: неадаптированность определений коррупционных преступлений к цифровой реальности, фрагментированность регулирования, различия в региональных подходах и ограниченное регулирование цифровых финансов. На институциональном уровне наблюдается множественность и пересечение полномочий различных органов, ограниченный технический потенциал, недостаточное межведомственное взаимодействие и ограниченное участие частного сектора и гражданского общества в противодействии киберкоррупции.

Для эффективного решения этих проблем странам Центральной Азии рекомендуется комплексный подход, включающий совершенствование законодательства, укрепление институциональных механизмов, расширение международного и регионального сотрудничества и внедре-

ние современных технологических решений. Особое внимание следует уделить гармонизации и модернизации нормативно-правовой базы, созданию специализированных подразделений по борьбе с киберкоррупцией, развитию механизмов межведомственной координации и активному вовлечению частного сектора и гражданского общества.

Реализация предложенных рекомендаций позволит странам Центральной Азии не только эффективно противодействовать текущим проявлениям киберкоррупции, но и создать устойчивую основу для предотвращения новых форм коррупции, которые могут возникнуть в результате дальнейшего технологического развития. Это, в свою очередь, будет способствовать формированию благоприятной среды для

цифровой трансформации экономики и общества, повышению доверия к государственным институтам и укреплению позиций стран региона в глобальной цифровой экономике.

В конечном итоге успех в противодействии киберкоррупции будет зависеть не только от технических и правовых решений, но и от политической воли, институциональных возможностей и уровня цифровой грамотности общества. Страны Центральной Азии имеют уникальную возможность учесть опыт развитых стран и избежать многих проблем, с которыми те столкнулись в процессе цифровой трансформации, формируя свои собственные, адаптированные к местным условиям подходы к обеспечению цифровой прозрачности и безопасности.

REFERENCES

1. Mauro P. Corruption and growth. *The Quarterly Journal of Economics*, 1995, vol. 110(3), pp. 681–712.
2. Global Competitiveness Report: The Cost of Corruption. World Economic Forum, 2020.
3. Abbott J., Genschel P., Snidal D., Zangl B. *Orchestration: Global governance through intermediaries*. Oxford University Publ., 2022.
4. Burkert H. Legal aspects of cybersecurity. In *Cybersecurity in Digital Governance*, 2022, pp. 65–86.
5. Global Cybersecurity Index 2020. International Telecommunication Union, 2020.
6. Technical Assistance Programme for Countering Cybercrime in Central Asia. United Nations Office on Drugs and Crime, 2022.
7. Jaeger M.D. Globalization and cyber-corruption. *International Journal of Management, Accounting and Economics*, 2018, vol. 5(9), pp. 656–663.
8. Jain A.K. Corruption: A review. *Journal of Economic Surveys*, 2001, vol. 15(1), pp. 71–121.
9. Ramappa T., Aithal P.S. Digital Corruption: Forms, Causes and Consequences. *International Journal of Management, Technology, and Social Sciences*, 2022, vol. 7(1), pp. 120–135.
10. Chetwynd E., Chetwynd F., Spector B. *Corruption and poverty: A review of recent literature*. Management Systems International, 2003.
11. *Enhancing Government Effectiveness and Transparency: The Fight Against Corruption*. World Bank Group, 2020.
12. Annual Report UNCTAD. 2018.
13. Algorithm Watch. 2024. Available at: <https://algorithmwatch.org/en/entirely-automated-public-tenders-in-italy/>
14. TRM Labs. 2022. Available at: <https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022>
15. Cryptocurrency Financial Crime Report. Elliptic Research, 2021.
16. What is 4G BTS in the corruption case of the Minister of Communication and Information Johnny G Plat? VOI.ID, 2022. Available at: <https://voi.id/en/technology/280711>

17. El País Corruption in digital infrastructure contracts exposed. El País International, 2020. Available at: <https://english.elpais.com/>
18. Environmental Audit Committee. Report on Air Quality Data Manipulation. UK Parliament, 2017.
19. Regulation Asia. 2024. Available at: <https://www.regulationasia.com/fsa-japan-issues-order-over-use-of-falsified-data-in-stress-tests/>
20. Annual Report on Cryptocurrency-Related Crimes. Federal Bureau of Investigation, 2020.
21. Swedish National Council for Crime Prevention. Report on Corruption in Public Sector Cybersecurity. Government Offices of Sweden, 2020.
22. Analysis of Anti-Corruption Legislation in Central Asia. Organization for Security and Co-operation in Europe, 2019.
23. Cybersecurity in Central Asia: Policy Developments and Regional Cooperation. Organization for Security and Co-operation in Europe, 2020.
24. Cybersecurity Regulatory Frameworks in Central Asia. International Telecommunication Union, 2021.
25. Financial Sector Assessment Program: Regulatory Frameworks for Fintech. International Monetary Fund, 2019.
26. OECD Public Integrity. OECD Publ., 2020.
27. Council of Europe. Convention on Cybercrime (Budapest Convention). Council of Europe Treaty Office, 2021.
28. Shanghai Cooperation Organisation Strategy until 2025: Implementation Plan. SCO Secretariat, 2019.
29. Anti-Corruption Reforms in Eastern Europe and Central Asia. OECD Publ., 2021.
30. Government of Singapore. Digital Trust Act: Implementation Guidelines. Infocomm Media Development Authority, 2019.
31. European Commission. Fifth Anti-Money Laundering Directive. *Official Journal of the European Union*, 2018.
32. European Data Protection Board. Guidelines on GDPR Implementation. EDPB Secretariat, 2020.
33. Government of Estonia. Digital Crime Unit: Structure and Functions. Ministry of Justice of Estonia, 2020.
34. UK National Crime Agency. Digital Investigation Enhancement Program: Evaluation Report. National Crime Agency, 2021.
35. Government of the Netherlands. National Cyber Security Centre: Strategic Framework. Ministry of Justice and Security, 2021.
36. Cyber Defense Alliance. Annual Report 2021: Collaborative Defense Against Cyber Threats. CDA Publ., 2022.
37. European Commission. ARACHNE Risk Scoring Tool: Technical Guidelines. Publications Office of the European Union, 2021.
38. SCO. Cooperation in Information Security within the SCO Framework. SCO Secretariat 2020.
39. Egmont Group. Annual Report: Strengthening Financial Intelligence Cooperation. Egmont Group Secretariat, 2020.
40. UNODC Cybercrime and Anti-Corruption: Challenges and Responses in Central Asia. United Nations Office on Drugs and Crime, 2022.
41. Microsoft. Digital Crime Unit: Public-Private Partnerships in Cybersecurity. Microsoft Corporate Report 2022.
42. e-Estonia. Digital Government Blueprint: Blockchain Applications in Public Sector. e-Estonia Briefing Centre, 2022.
43. World Bank. Corruption Hunter Network: Leveraging Data Analytics. World Bank Group, 2021.
44. Financial Crimes Enforcement Network. Advisory on Cyber-Enabled Financial Crime. U.S. Department of the Treasury, 2020.
45. I Paid A Bribe. Citizen-Powered Anti-Corruption Platform: Impact Assessment. Janaagraha Centre for Citizenship and Democracy, 2021.

YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2025-YIL 2-SON

VOLUME 5 / ISSUE 2 / 2025

DOI: 10.51788/tsul.jurisprudence.5.2.