ET DOCERE ET DISCERE SERVITUTE LEGIS

RAQAMLI KRIMINALISTIKA

O‘ZBEKISTON RESPUBLIKASI
HUQUQNI MUHOFAZA QILISH
AKADEMIYASI

ILMIY-AMALIY YURIDIK JURNALI

№1 (1) 2026

ЦИФРОВАЯ КРИМИНАЛИСТИКА

НАУЧНО-ПРАКТИЧЕСКИЙ ЮРИДИЧЕСКИЙ ЖУРНАЛ

DIGITAL FORENSIC

SCIENTIFIC-PRACTICAL LAW LOURNAL



PROACADEMY.UZ
ISSN 3093-9291

JURNAL O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI HUZURIDAGI OLIY ATTESTATSIYA KOMISSIYASI RAYOSATINING 2025-YIL 1-NOYABRDAGI QARORI BILAN ILMIY NASHRLAR RO‘YXATIGA KIRITILGAN

RAQAMLI KRIMINALISTIKA

O‘ZBEKISTON RESPUBLIKASI HUQUQNI MUHOFAZA QILISH AKADEMIYASI

Bosh muharrir:
Yevgeniy Kolenko

Mas’ul kotib:
Farxodjon Nazarov

Bosh muharrir o‘rinbosarlari:
Adham Odinayev
Durbek Turaxanov
Uyg‘un Nigmadjanov
Sardorbek Urozbayev

Tahrir hay’ati:
Baxtiyor Pulatov
Alisher Maxmudov
Alisher Imomnazarov
Abdulaziz Rasulev
Xurshid Karimov
Lyudmila Yugay
Umidjon Xamrakulov
Xagani Gadjiyev
Nasiba Norova
Bekzod Rajabov
G‘ayrat Musayev
Shoakrom Shomaxsudov
Xursanoy Mirzokulova
Asrorjon Turg‘unov
Anvar Xusanov
Yelena Rossinskaya
Vitaliy Vexov
Vladimir Mesheryakov
Kim Don Xyon
Savash Serkan
Vitaliy Kirvel
Richard Djoys

O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi huzuridagi Axborotlashtirish va telekommunikatsiyalar sohasida inspeksiyasida 2026-yil 18-mayda 1592102-sonli guvohnoma bilan olingan.
Jurnal O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2025-yil 1-noyabrdagi qarori bilan yuridik fanlar bo‘yicha dissertatsiyalar asosiy ilmiy natijalarini nashr qilish tavsiya etilgan ilmiy nashrlar ro‘yxatiga kiritilgan.

Muallif fikri tahririyat nuqtayi nazaridan farq qilishi mumkin.

Jurnalda chop etilgan materiallardan foydalanilganda "Raqamli kriminalistika" jurnalidan olindi deb ko‘rsatilishi shart. Tahririyat taqdim etilgan materiallarni taqriz qilish va qaytarish majburiyatini olmagan.

Manzil:
1001906 Toshkent shahri,
Rixsiliy ko‘chasi 9-uy
Veb-sayt: proacademy.uz
e-mail: info@proacademy.uz

MUNDARIJA

N. YO‘LDOSHEV	Yangi fikrlar, g‘oyalar va ilmiy qarashlarning muhim minbari	**3**
B. VALIEV	O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashda prokuratura organlarining o‘rni	**6**
G. MUSAYEV	Криминалистическая характеристика преступлений в Darknet	**13**
E. KOLENKO	Практико-ориентированная подготовка кадров в противодействии киберпреступности: опыт Правоохранительной академии Республики Узбекистан	**22**
H. GADJIYEV	Цифровая криминалистика в правоохранительной практике Республики Молдова: сравнительный анализ и перспективы применения опыта в Республике Узбекистан	**29**
L. YUGAY	Legal regulation of deepfake use: international and national experience	**39**
B. KUDRATOV	Raqamli davrda kiberjinoyatlarga qarshi kurashishning dolzarb masalalari	**45**
S. SAVASH	The potential and application areas of artificial intelligence in the effective fight against corruption	**50**
V. KIRVEL M. GALINSKIY	Судебная компьютерно-техническая экспертиза Республики Беларусь: современное состояние, проблемы и возможные пути решения	**68**

YANGI FIKRLAR, G‘OYALAR VA ILMIY QARASHLARNING MUHIM MINBARI



Avvalo shuni qayd etish o‘rinliki, bugun raqamlashtirish jamiyat ravnaqining asosiy mezonlaridan biriga aylandi.

Binobarin, mamlakatimiz iqtisodiyotining raqamli sektori kengayib, uning asosiy o‘sish omillari hisoblangan elektron tijorat platformalari, raqamli servislar, moliyaviy texnologiyalar shiddat bilan rivojlanmoqda.

Tabiiyki, bunday sharoitda kiberjinoyatlar oshishi xavfi ham kuzatiladi. Keyingi vaqtlarda bank kartalaridan foydalangan holda o‘g‘rilik yoki firibgarlik holatlarining ko‘payayotganining o‘ziyoq buning dalilidir.

Aholining raqamli moliyaviy savodxonligi hamda huquqni muhofaza qiluvchi organlar xodimlarining malakasi esa, afsuski, hali yetarli emas, tijorat banklari, to‘lov tizimi operatorlari va to‘lov tashkilotlarida huquqbuzarliklarning oldini olishning zamonaviy tizimlari ham to‘liq joriy etilmagan.

Bu omillar axborot texnologiyalaridan foydalangan holda sodir etilayotgan jinoyatlarni o‘z vaqtida aniqlash va samarali tergov qilishda maxsus raqamli usul va vositalardan foydalanishni, raqamli dalillar bilan ishlash texnikasini ishlab chiqishni, yuqori malakali mutaxassislar tayyorlash hamda bu borada tizimli ilmiy-tadqiqot bazasini yaratishni taqozo etmoqda.

Axborot texnologiyalari sohasidagi huquqbuzarliklarning o‘sishi, tergov organlarini zamonaviy uslublar bilan qurollantirish zaruriyati hamda raqamli kriminalistika sohasidagi xalqaro va mahalliy ilmiy yutuqlar, shuningdek, amaliy tajribalarni keng jamoatchilikka yetkazish esa har qachongidan ham dolzarb ahamiyatga ega.

Ma’lumki, O‘zbekiston Respublikasi Prezidentining 2024-yil 21-iyundagi “Raqamli kriminalistika sohasida ilmiy-tadqiqot faoliyatini tashkil etish chora-tadbirlari to‘g‘risida”gi 229-sonli qarori bilan Huquqni muhofaza qilish akademiyasi tarkibida Raqamli-kriminalistika ilmiy-tadqiqot instituti tashkil etilib, institut zimmasiga raqamli kriminalistikaga oid bir qator dolzarb vazifalar yuklatildi.

Institutning “Raqamli kriminalistika” xalqaro ilmiy-amaliy jurnalini ta’sis etish ana shunday ustuvor vazifalardan biri edi.

Bugun nishona soni taqdim etilayotgan ushbu jurnal O‘zbekistonda raqamli texnologiyalar sohasidagi ilmiy tadqiqotlar va amaliy ishlanmalarni yanada rivojlantirish, shuningdek, xalqaro hamkorlikni kengaytirish yo‘lidagi muhim qadamdir.

Ishonchimiz komilki, “Raqamli kriminalistika” jurnali raqamli kriminalistika sohasidagi ilmiy tadqiqotlar natijalarini tarqatish, xalqaro tajriba va eng ilg‘or amaliyotlarni O‘zbekiston mutaxassislari bilan ulashish, huquq-tartibot organlari, sud tizimi va ilmiy jamoatchilik o‘rtasida hamkorlikni mustahkamlash, yosh tadqiqotchilar va mutaxassislarni qo‘llab-quvvatlash, kiberxavfsizlik va raqamli jinoyatchilikka qarshi kurash bo‘yicha milliy salohiyatni oshirishga xizmat qiladi.

Jurnal raqamli dalillarni yig‘ish va tahlil qilish, kiberjinoyatchilikka qarshi kurashish, mobil qurilmalar va bulutli texnologiyalar kriminalistikasi, sun’iy intellekt va blokcheyn kabi texnologiyalarning kriminalistikada qo‘llanilishi, raqamli kriminalistikaning huquqiy jihatlari, tarmoq kriminalistikasi hamda ushbu sohada ta’lim va kadrlar tayyorlash masalalariga oid fikr-mulohazalar, ilmiy qarashlarning muhim minbari bo‘ladi degan umiddamiz.

Qolaversa, o‘zbek, ingliz va rus tillarida maqolalar chop etiladigan ushbu nashr milliy raqamli kriminalistika yutuqlarini keng ommaga yetkazishda benazir jarchi vazifasini ham o‘taydi.

“Raqamli kriminalistika”ning nishona soni chop etilayotgani munosabati bilan avvalo, keng o‘quvchilar ommasini, huquqshunoslar jamoatchiligini samimiy muborakbod etaman.

Tahririyat jamoasiga esa ijodiy barkamollik tilayman.

Nig‘matilla YO‘LDOSHEV,
O‘zbekiston Respublikasi Bosh prokurori

ВАЖНАЯ ТРИБУНА НОВЫХ ИДЕЙ, КОНЦЕПЦИЙ И НАУЧНЫХ ВЗГЛЯДОВ

Прежде всего, следует отметить, что сегодня цифровизация стала одним из основных критериев развития общества.

Соответственно, расширяется сектор цифровой экономики нашей страны, динамично развиваются платформы электронной коммерции, цифровые услуги, финансовые технологии, являющиеся основными факторами роста.

Закономерно, что в данных условиях наблюдается риск роста киберпреступлений. Сам факт увеличения случаев краж или мошенничества с использованием банковских карт в последнее время является тому доказательством.

Цифровая финансовая грамотность населения и квалификация сотрудников правоохранительных органов, к сожалению, пока недостаточны. В коммерческих банках, операторах платежных систем и платежных организациях также не полностью внедрены современные системы предупреждения правонарушений.

Эти факторы требуют использования специальных цифровых методов и средств для своевременного выявления и эффективного расследования преступлений, совершаемых с использованием информационных технологий, формирования техники работы с цифровыми доказательствами, подготовки высококвалифицированных специалистов, а также создания системной научно-исследовательской базы в этой области.

Рост правонарушений в сфере информационных технологий, необходимость вооружения следственных органов современными методами, а также доведение до широкой общественности международных и национальных научных достижений в области цифровой криминалистики, равно как и практического опыта, имеют как никогда актуальное значение.

В соответствии с Постановлением Президента Республики Узбекистан от 21 июня 2024 года № ПП-229 «О мерах по организации научно-исследовательской деятельности в области цифровой криминалистики» в составе Правоохранительной академии был создан Научно-исследовательский институт цифровой криминалистики, на который был возложен ряд актуальных задач в сфере цифровой криминалистики.

Учреждение Институтом международного научно-практического журнала «Цифровая криминалистика» определено в качестве одной из приоритетных задач.

Представляемый сегодня пилотный номер этого журнала является важным шагом на пути дальнейшего развития научных исследований и практических разработок в области цифровых технологий в Узбекистане, а также расширения международного сотрудничества.

Мы уверены, что журнал «Цифровая криминалистика» послужит распространению результатов научных исследований в области цифровой криминалистики, обмену международным опытом и передовыми практиками со специалистами Узбекистана, укреплению сотрудничества между правоохранительными органами, судебной системой и научным сообществом, поддержке молодых исследователей и специалистов, повышению национального потенциала в области кибербезопасности и борьбы с цифровой преступностью.

Надеемся, что журнал станет важной трибуной для мнений и научных взглядов по вопросам сбора и анализа цифровых доказательств, борьбы с киберпреступностью, криминалистики мобильных устройств и облачных технологий, применения в криминалистике таких технологий, как искусственный интеллект и блокчейн, правовых аспектов цифровой криминалистики, сетевой криминалистики, а также вопросов образования и подготовки кадров в данной области.

Кроме того, это издание, в котором будут публиковаться статьи на узбекском, английском и русском языках, будет выполнять и беспрецедентную роль проводника идей в донесении достижений национальной цифровой криминалистики до широких масс.

По случаю выхода в свет пилотного номера "Цифровой криминалистики" прежде всего искренне поздравляю широкую читательскую аудиторию, сообщество юристов.

Редакционной команде желаю творческих успехов!

Нигматилла ЙУЛДОШЕВ,
Генеральный прокурор
Республики Узбекистан

AN IMPORTANT PLATFORM FOR NEW IDEAS, CONCEPTS, AND SCIENTIFIC VIEWS

First and foremost, it should be noted that today digitalization has become one of the key indicators of societal development.

Consequently, the digital sector of our country's economy is expanding, and its principal drivers of growth—such as e-commerce platforms, digital services, and financial technologies—are developing at a rapid pace.

Naturally, in such circumstances, the risk of cybercrime also increases. The growing number of cases of theft and fraud committed through the use of bank cards in recent times is clear evidence of this trend.

Unfortunately, the level of digital financial literacy among the population, as well as the professional competence of law-enforcement personnel, remains insufficient. Moreover, modern systems for preventing violations have not yet been fully implemented in commercial banks, payment system operators, and payment institutions.

These factors necessitate the use of specialized digital methods and tools for the timely detection and effective investigation of crimes committed through information technologies. They also require the development of techniques for handling digital evidence, the training of highly qualified specialists, and the establishment of a systematic scientific-research base in this field.

The rise in offenses committed in the field of information technologies, the need to equip investigative bodies with modern methodologies, and the importance of disseminating international and domestic scientific achievements—as well as practical experience—in digital forensics to the wider public have become more relevant than ever.

As is known, by Decree No. 229 dated June 21, 2024, 'On Measures to Organize Scientific-Research Activities in the Field of Digital Forensics,' the Law Enforcement Academy of the Republic of Uzbekistan established the Scientific-Research Institute of Digital Forensics. The Institute has been assigned a number of pressing tasks related to digital forensics.

The establishment of the international scientific-practical journal 'Digital Forensics' was one of the Institute's priority tasks.

Today, with the presentation of its inaugural issue, this journal represents an important step towards further developing scientific research and practical developments in the field of digital technologies in Uzbekistan, as well as expanding international collaboration.

We are confident that the journal 'Digital Forensics' will serve to disseminate the results of scientific research in the field of digital forensics, share international experience and best practices with Uzbek specialists, strengthen cooperation among law enforcement agencies, the judicial system, and the scientific community, support young researchers and professionals, and enhance national capacity in cybersecurity and combating digital crime.

We hope that the journal will serve as an important platform for reflections and scholarly perspectives on issues such as the collection and analysis of digital evidence, combating cybercrime, forensics of mobile devices and cloud technologies, the application of technologies like artificial intelligence and blockchain in forensics, the legal aspects of digital forensics, network forensics, as well as education and personnel training in this field.

Furthermore, as a publication featuring articles in Uzbek, English, and Russian, this journal also performs a unique role in widely disseminating national achievements in digital forensics to the broader public.

On the occasion of the publication of the inaugural issue of 'Digital Forensics,' I would first like to extend my sincere congratulations to the wider readership and the community of legal professionals.

I wish the editorial team continued creativity and professional excellence.

Nigmatilla YULDOSHEV
Prosecutor General of the
Republic of Uzbekistan"

Baxriddin VALIEV,
O‘zbekiston Respublikasi
Bosh prokurorining birinchi o‘rinbosari

O‘ZBEKISTON RESPUBLIKASIDA KIBERJINOYATCHILIKKA QARSHI KURASHDA PROKURATURA ORGANLARINING O‘RNI

ANNOTATSIYA. *Mazkur maqolada O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishda prokuratura organlarining o‘rni va vazifalari tahlil qilingan. Axborot texnologiyalarining jadal rivojlanishi natijasida kiberxavfsizlikka tahdidlar tobora ortib borayotgani ta’kidlangan. Shu munosabat bilan prokuratura organlari tomonidan kiberjinoyatlarni aniqlash, ularning oldini olish va javobgarlikni ta’minlash bo‘yicha amalga oshirilayotgan chora-tadbirlar o‘rganilgan. Shuningdek, milliy qonunchilikni takomillashtirish, xalqaro hamkorlikni kuchaytirish va prokuratura xodimlarining kiberhuquq sohasidagi bilim va ko‘nikmalarini oshirish bo‘yicha takliflar ilgari surilgan.*

АННОТАЦИЯ. *В статье рассматривается роль и значение органов прокуратуры Республики Узбекистан в противодействии киберпреступности. Отмечается, что с развитием информационных технологий возрастает количество угроз в сфере кибербезопасности. Анализируются меры, принимаемые органами прокуратуры по выявлению, предупреждению и расследованию киберпреступлений, а также по обеспечению правовой ответственности виновных лиц. Особое внимание уделено вопросам совершенствования национального законодательства, расширения международного сотрудничества и повышения профессиональной подготовки прокурорских работников в области киберправа.*

ABSTRACT. *This article analyzes the role and functions of the Prosecutor’s Office of the Republic of Uzbekistan in combating cybercrime. It highlights that the rapid development of information technologies has led to an increase in cyber threats. The paper examines the measures taken by prosecutorial bodies to detect, prevent, and investigate cybercrimes, as well as to ensure accountability for offenders. Special attention is given to improving national legislation, strengthening international cooperation, and enhancing the professional capacity of prosecutors in the field of cyber law.*

Kalit so‘zlar: *kiberjinoyatchilik, prokuratura organlari, axborot xavfsizligi, kiberxavfsizlik, jinoyatchilikka qarshi kurash, huquqiy choralar, profilaktika, xalqaro hamkorlik.*

Ключевые слова: *киберпреступность, органы прокуратуры, информационная безопасность, кибербезопасность, борьба с преступностью, правовые меры, профилактика, международное сотрудничество.*

Key words: *cybercrime, prosecutor’s office, information security, cybersecurity, crime prevention, legal measures, international cooperation.*

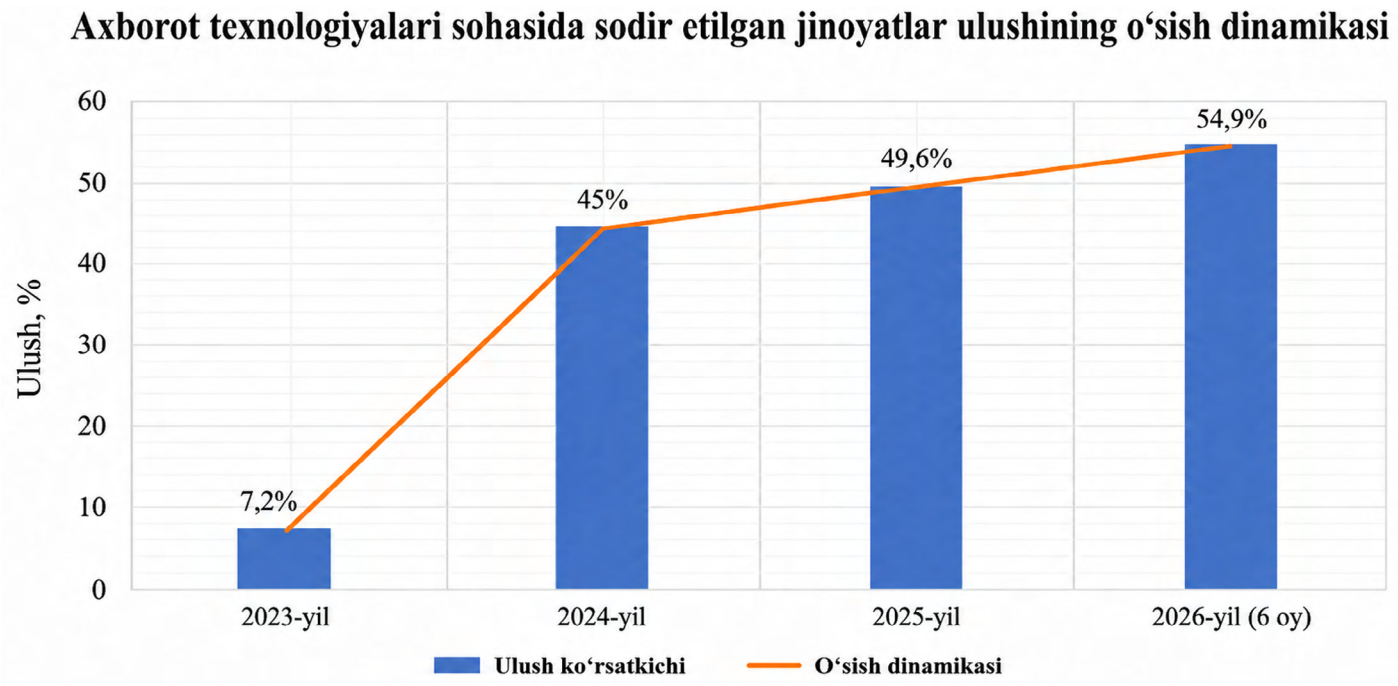
So‘nggi yillarda mamlakatimizda inson huquqlari va qonuniy manfaatlarini himoya qilish, ishning haqiqiy holatlarini har tomonlama, to‘liq va xolisona aniqlashga oid qonun talablariga so‘zsiz rioya etish, taraflarning tortishuvi hamda teng huquqliligi prinsiplarini amalda ta’minlash orqali inson huquq va erkinliklarini kompleks himoya qilish bo‘yicha keng ko‘lamli chora-tadbirlar amalga oshirilmoqda.

Shu bilan birga, jamiyat hayotining turli sohalarida raqamlashtirish jarayonlarining jadal sur’atlarda rivojlanishi, fuqarolar hamda tashkilotlarning axborot-kommunikatsiya texnologiyalaridan foydalangan holda o‘zaro munosabat va hamkorligi kengayib borishi natijasida raqamli muhitda jinoyatlar sodir etilishi, shuningdek, fuqarolar va tashkilotlarning huquqlari hamda qonuniy manfaatlariga tajovuz qilinishi holatlarining keng tarqalishi kuzatilmoqda, bu esa raqamli dalillarni institutsional jihatdan shakllantirishni va ular bilan bog‘liq protsessual harakatlarni amalga oshirishning huquqiy asoslarini yanada mustahkamlash zaruratini taqozo etmoqda.

Shuningdek, axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etilayotgan jinoyatlarni o‘z vaqtida aniqlash va tergov qilish maxsus raqamli vosita va usullarni qo‘llashni, raqamli dalillar bilan ishlashning ilmiy-texnikaviy asoslarini ishlab chiqishni, yuqori malakali mutaxassislar tayyorlashni hamda ushbu yo‘nalishda tizimli ilmiy-tadqiqot infratuzilmasini shakllantirishni talab etmoqda.

Xususan, respublikamizda axborot texnologiyalari sohasida sodir etilgan jinoyatlarning ulushi umumiy jinoyatlarning 2023-yilda 7,2 foizini, 2024-yilda 45 foizini, 2025-yilda 49,6 foizini hamda 2026-yilning 6 oyida 54,9 foizini tashkil etgan.

Hozirgi kunda axborot texnologiyalaridan foydalanib sodir etilayotgan jinoyatlar ulushi izchil ortib borayotganligi hamda ushbu toifadagi jinoyatlarni fosh etish va tergov qilish jarayonlarining murakkabligi sababli mazkur turdagi jinoyatlarning barvaqt oldini olishda boshqa huquqni muhofaza qiluvchi organlar bilan bir qatorda



1-diagramma. Axborot texnologiyalari yordamida sodir etilgan jinoyatlarning umumiy jinoyatchilikka nisbatan salmog‘i.

prokuratura organlarining o‘rni va rolini yanada kuchaytirishni zamonning o‘zi taqozo etmoqda. Shu munosabat bilan kiberjinoyatchilikka qarshi kurashishning huquqiy mexanizmlarini takomillashtirish, xususan, qonun ustuvorligini ta’minlashda prokuratura organlarining nazorat hamda muvofiqlashtirish vakolatlarini mustahkamlash dolzarb ahamiyat kasb etmoqda.

Zero, O‘zbekiston Respublikasining “Prokuratura to‘g‘risida”gi qonuniga muvofiq, prokuratura organlarining asosiy vazifalari qatorida qonun ijodkorligi faoliyatida hamda jamiyatda huquqiy madaniyatni yuksaltirish ishida ishtirok etish, qonunlarning ijro etilishi ustidan nazorat qilish va jinoyatchilikka qarshi kurashni muvofiqlashtirish kabi ustuvor yo‘nalishlar belgilangan[1].

Shuningdek, prokuratura organlari kiberjinoyatchilikka qarshi kurashish faoliyatining barcha bosqichlarida, ya’ni jinoyatlarning barvaqt oldini olishdan tortib, javobgarlik muqarrarligini ta’minlash bosqichigacha bo‘lgan jarayonlar ustidan prokurorlik nazoratini amalga oshiradi.

Ushbu maqolada mamlakatimizda keng tarqalgan kiberjinoyatlar va ularga qarshi kurashishda O‘zbekiston Respublikasi prokuratura organlarining o‘rni, huquqiy asoslari, amaldagi faoliyati hamda oldinda turgan muammolar va istiqbollar tahlil qilinadi.

Dastlabki o‘rinda tarixga nazar tashlaydigan bo‘lsak, O‘zbekistonda prokuratura organlarining tashkil etilib, taraqqiy etish davrini shartli ravishda to‘rt bosqichga bo‘lish mumkin.

Xususan, birinchi bosqich – sobiq Sovet Sotsialistik Respublikalari ittifoqi boshqaruviga to‘g‘ri keladi (1924 – 1991-yillar). O‘zbekistonda prokuratura organlari ilk bor 1924-yilda O‘zbekiston SSR tashkil topishi bilan tashkil etilgan. Bu tuzilma SSRI prokuraturasi tizimining bir qismi sifatida faoliyat yuritgan. Ushbu davrda O‘zbekiston SSR prokuraturasining asosiy vazifasi – sotsialistik qonunchilik ijrosini nazorat qilish bo‘lgan va prokuratura organlari sud ishlariga aralashmagan, lekin davlat siyosatiga xizmat qilgan.

Ikkinchi bosqichda – O‘zbekiston Respublikasining mustaqilligi qabul qilinib, islohotlar amalga oshirildi (1991 – 2000-yillar). O‘zbekiston mustaqil davlat sifatida o‘z prokuratura tizimini qayta tashkil etdi. Bu bosqichda prokuraturani milliy tizimga moslashtirish boshlandi. Jumladan, 1992-yilda O‘zbekiston Respublikasining Konstitutsiyasi qabul qilindi va bosh qomusimizning 118-moddasiga ko‘ra, prokuratura organlarining vazifalari va faoliyatining asosiy tamoyillari belgilandi hamda 1992-yil 9-dekabr kuni “Prokuratura to‘g‘risida”gi birinchi qonun qabul qilindi. Natijada prokuratura organlari davlatning mustaqil idorasi sifatida shakllanib, o‘z faoliyatini yurita boshladi.

1 O‘zbekiston Respublikasining 2001-yil 29-sentyabrdagi 257-II-sonli qonuni // https://lex.uz/uz/docs/106197.

Uchinchi bosqich – institutsional rivojlanish va ixtisoslashuv (2000 – 2016-yillar) davri bo‘lib, unda prokuratura organlari faoliyati nafaqat jinoyat ishi yuritishda, balki fuqarolar huquqlarini himoya qilish, tadbirkorlikni qo‘llab-quvvatlash, ma’muriy nazorat sohalarida ham kengaydi. Prokuratura organlarining jamiyatdagi ta’sirini kuchaytirishga qaratilgan qonunlar qabul qilindi va tizimga axborot texnologiyalari joriy etila boshlandi.

To‘rtinchi bosqich – yangi islohotlar va tizimni raqamlashtirish davri (2017-yildan hozirgi kungacha). Ushbu davrda O‘zbekiston Respublikasi Prezidentining tashabbusi bilan prokuratura organlarida tub islohotlar amalga oshirildi. Prokuratura organlari yanada xalqparvar, inson manfaatlari, uning qonuniy huquq va erkinliklarini himoya qilishga qaratilgan adolatli va shaffof tuzilma sifatida shakllandi. Jumladan, elektron hujjat almashinuvi va nazorat tizimlari joriy etildi, jamiyat bilan ochiq muloqot va fuqarolar murojaatlari bilan ishlash samaradorligi oshirildi, kiberjinoyatchilikka qarshi kurashda prokuraturaning alohida vakolat va funksiyalari belgilandi hamda xalqaro maydonda ham hamkorlik yo‘nalishlari kengaytirildi.

Hozirgi kunda axborot texnologiyalari yordamida sodir etilayotgan jinoyatlarning ulushi umumiy jinoyatlar hajmining 50 foizini tashkil etayotganligi jiddiy ahamiyatga ega. Mazkur tendensiyaning kelgusida yanada ortish ehtimoli mavjudligi ushbu toifadagi jinoyatlarga qarshi oldindan profilaktika choralarini kuchaytirish zarurligini ko‘rsatmoqda.

O‘z navbatida, hisobot hujjatlariga ko‘ra, 2026-yilning 6 oyida axborot texnologiyalari sohasida sodir etilgan jinoyatlar soni jami 41 466 tani tashkil etib, shundan 93,6 % yoki 38 817 tasi fuqarolarning bank kartalaridan pul mablag‘larini o‘g‘rilik va firibgarlik yo‘li bilan talon-toroj qilish jinoyatlari hissasiga to‘g‘ri kelgan.

Axborot texnologiyalari sohasidagi fosh etilmagan o‘g‘rilik va firibgarlik jinoyatlarining (38 817 ta) sodir etilish usullari tahlil qilinganda quyidagilar aniqlandi:

17 370 tasi yoki 44,75 foizi – soxta havola (zararli dastur) orqali karta yoki qurilma boshqaruvini qo‘lga kiritish orqali;

705 tasi yoki 1,82 foizi – soxta qo‘ng‘iroqlar orqali aldab, karta boshqaruvini qo‘lga kiritish orqali;

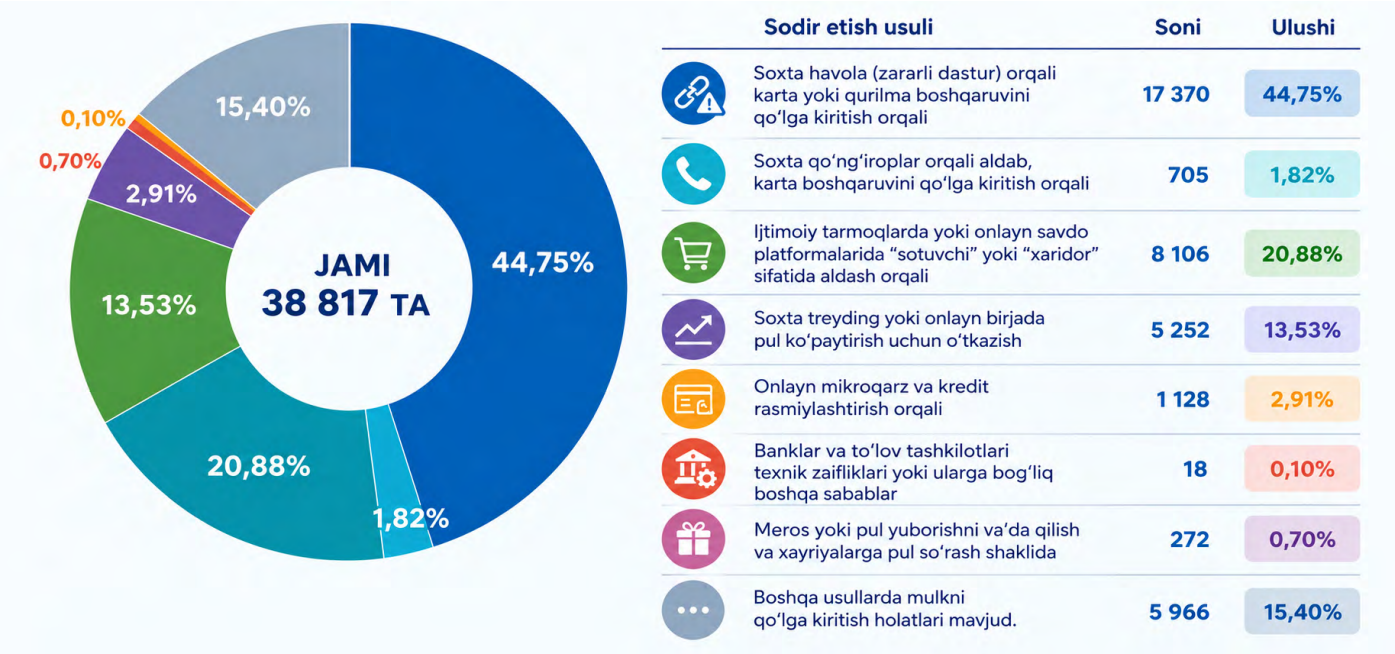
8 106 tasi yoki 20,88 foizi – ijtimoiy tarmoqlarda yoki onlayn savdo platformalarida “sotuvchi” yoki “xaridor” sifatida aldash orqali;

5 252 tasi yoki 13,53 foizi – soxta treyding yoki onlayn birjada pul ko‘paytirish uchun o‘tkazish;

1 128 tasi yoki 2,91 foizi – onlayn mikroqarz va kredit rasmiylashtirish orqali;

18 tasi yoki 0,1 foizi – banklar va to‘lov tashkilotlari texnik zaifliklari yoki ularga bog‘liq boshqa sabablar;

272 tasi yoki 0,7 foizi – meros yoki pul yuborish-



2-diagramma. Axborot texnologiyalari sohasidagi fosh etilmagan o‘g‘rilik va firibgarlik jinoyatlarining toifalari.

ni va’da qilish va xayriyalarga pul so‘rash shaklida;

5 966 tasi yoki 15,4 foizi – boshqa usullarda mulkni qo‘lga kiritish holatlari mavjud.

Bugungi kunda eng dolzarb kibertahdidlardan biri sifatida shaxsga doir ma’lumotlarni qo‘lga kiritish sanaladi. Bunga sabab shaxslar g‘ayriqonuniy yo‘l bilan boylik orttirish maqsadida o‘zgalarning mol-mulkini turli usullarda talon-toroj qilishga urinishadi va mazkur jinoiy rejalarning asosiy qismi mulk egasining shaxsiga doir ma’lumotlarni qo‘lga kiritishdan iborat bo‘ladi. Zero, shaxs to‘g‘risidagi axborotga ega bo‘lgach, jinoyatchilar aynan kim bilan aloqa qilayotganliklarini, uning zaif tomonlarini va eng asosiysi, jabrlanuvchini ishontirish uchun u haqidagi qator ma’lumotlarga ega bo‘ladilar.

O‘zbekiston Respublikasining 2019-yil 2-iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi 547-sonli qonuniga muvofiq, shaxsga doir ma’lumotlar tushunchasiga ta’rif berilgan bo‘lib, unga ko‘ra, muayyan jismoniy shaxsga taalluqli bo‘lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog‘ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot shaxsga doir ma’lumotlar hisoblanadi.

Bundan tashqari, shaxsga doir ma’lumotlar “qora bozor”da – “Darknet” tarmog‘i va boshqa noqonuniy savdo platformalarida yuqori baholanadi. Internetdagi ochiq manbalarni o‘rganish va tahlil qilish natijalari shuni ko‘rsatdiki, fuqarolarning shaxsiy ma’lumotlari turiga qarab turlicha narxlarda baholanadi.

Hozirda barcha sohalarni raqamlashtirish davr talabiga aylangan bir paytda shaxs haqidagi ko‘pgina ma’lumotlarni internetdagi ochiq manbalardan topish qiyin emas. Masalan, “Instagram”, “Facebook”, “YouTube”, “Tinder”, “X” va “Threads” kabi ijtimoiy tarmoqlar orqali foydalanuvchining shaxsiy ma’lumotlari, qiziqishlari, yaqinlari, kundalik hayoti va boshqa jihatlari haqida ma’lumot to‘plash mumkin.

Ijtimoiy tarmoqlar, messenjerlar va veb-sahifalardagi ochiq manbalardan ma’lumot to‘plash yoki shaxsga doir ma’lumotlarni noqonuniy platformalar orqali sotib olish natijasida kiberjinoyatlar sodir etilmoqda. Jinoyatchi to‘plangan ma’lumotlar asosida potensial jabrlanuvchiga uyali aloqa yoki messenjerlar orqali murojaat qilib, o‘zini vakolatli davlat organlari vakili sifatida tanishtirmoqda. Suhbat davomida jabrlanuvchining shaxsiy ma’lumotlarini (faqat rasmiy manbalarga ma’lum bo‘lishi kerak bo‘lgan) aytib berish orqali ishonchga kiradi va shaxsning psixologik-emotsional holatidan foydalanib, mol-mulkni talon-toroj qiladi yoki unga bo‘lgan huquqni qo‘lga kiritadi.

Tashvishli jihati shundaki, ayrim shaxslar boylik orttirish maqsadida g‘ayriqonuniy faoliyat bilan shug‘ullanmoqda. Xususan, xizmat mavqeyi yoki boshqa holatlar natijasida qo‘lga kiritilgan fuqarolarning shaxsiy ma’lumotlarini (F.I.SH., tug‘ilgan sanasi, yashash manzili, hujjatlar seriya raqamlari va boshqalar) noqonuniy sotuvga qo‘ymoqdalar. Bu ma’lumotlar esa mol-mulkka qarshi jinoyatlar sodir etuvchilar uchun muhim vosita bo‘lib xizmat qilmoqda.

Yana bir shiddat bilan tarqalib kelayotgan texnologiyalardan biri bu – “Deepfake” texnologiyasi, ya’ni sun’iy intellekt yordamida media mahsulotlarni, xususan, foto va videomateriallar hamda audioyozuvlarni tahrirlash va natijasidan jinoiy rejaga muvofiq foydalanish hisoblanadi.

“Deepfake” texnologiyasi asosida yaratilgan kontentlar yolg‘on axborot tarqatish, shaxs qadr-qimmatini kamsitish, obro‘yiga putur yetkazish hamda aholi orasida nizo keltirib chiqarish maqsadida telekommunikatsiya vositalari va internet tarmog‘i orqali tarqatilmoqda. Internetda foto va videomateriallari joylashtirilgan shaxslar asosiy xavf zonasiga kiradi.

Jinoiy maqsadda harakat qiluvchilar moddiy foydani ko‘zlab omma orasida tanilgan shaxslar yoki jabrlanuvchilar tanishlarining ishtirokidagi kontentlarni tahrirlash orqali, shantaj va tovlamachilik usullaridan foydalanmoqda. Bunda jabrlanuvchining xususiyatlariga qarab individual yondashuv qo‘llaniladi.

Tashvishlisi, ushbu noqonuniy harakatlar qurbonlarining ko‘pchiligi voyaga yetmaganlar bo‘lib, ularga psixologik bosim o‘tkazish va g‘arazli maqsadlarga yo‘naltirish nisbatan oson amalga oshiriladi.

Tergov amaliyoti va jinoyat to‘g‘risidagi ariza-xabarlar tahlili shuni ko‘rsatdiki, jabrlanuvchilar tomonidan ijtimoiy tarmoq va messenjerlarga joylashtirilgan fotosuratlarni uchinchi shaxslar to‘siqsiz yuklab olib, keyinchalik haqoratomuz izohlar yoki pornografik kontent bilan tahrirlash orqali jabrlanuvchini jinsiy aloqa qilishga majburlash va suratlarni tarqatish bilan shantaj qilish holatlari aniqlangan.

Mazkur texnologiya jamiyatdagi hodisalar yuzasidan jamoatchilik fikrini davlat tuzumiga qarshi yo‘naltirish yoki diniy, etnik, irqiy, jinsiy va boshqa qarashlar asosida aholining turli qatlamlari o‘rtasida nizolar va salbiy munosabatlarni shakllantirish maqsadida ham qo‘llanilishi mumkin.

Yuqorida sanab o‘tilgan kibertahdidlarga qarshi kurashish, axborot texnologiyalari yordamida sodir etilayotgan jinoyatlarni fosh etish va tergov qilishda qonun talablariga rioya etish muhim ahamiyat kasb etadi. Ushbu toifadagi jinoyatlarni tergov qilishning an’anaviy jinoyatlardan asosiy farqi shundaki, bunda isbotlash jarayonida raqamli dalillarni to‘plash ustuvor ahamiyat kasb etadi.

Ish uchun ahamiyatli elektron ma’lumotlarni to‘plash va ularni kelgusida maqbul raqamli dalil sifatida rasmiylashtirish protsessual harakatlarning qonun talablariga qat’iy rioya etilishini taqozo etadi. Bu borada prokuratura organlarining qonun ustuvorligini ta’minlash hamda huquqni muhofaza qiluvchi organlar faoliyatida qonun talablarining ijrosi ustidan nazorat olib borishdagi roli alohida ahamiyatga ega. Protsessual xatoliklar va qonunga zid ravishda olingan dalillar jinoyat sodir etgan shaxs foydasiga xizmat qilishi mumkinligi e’tiborga olingan holda, mazkur jarayonlarning qonuniyligi ta’minlanishi zarur.

Qayd etish lozimki, kibertahdidlar soni oshib borgan sari davlat rahbarining tashabbusi bilan kiberjinoyatchilikka qarshi kurashni samarali tashkil etish maqsadida keng ko‘lamli islohotlar amalga oshirilmoqda.

Jumladan, O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi 153-sonli qaroriga muvofiq Bosh prokuraturaning Ichki ishlar organlarida qonunchilik ijrosi ustidan nazorat boshqarmasi tuzilmasida *Kiberjinoyatlarga qarshi kurashishda qonuniylikni ta’minlash bo‘limi* tashkil etildi hamda hududiy prokuraturalar va Transport prokuraturasining Ichki ishlar organlarida qonunchilik ijrosi ustidan nazorat bo‘limlarida uning guruhlari faoliyati yo‘lga qo‘yildi.

Mazkur tuzilmalar zimmasiga ichki ishlar organlarining kiberjinoyatlarni tergov qilish va fosh etish faoliyatida qonunchilik ijrosi ustidan prokurorlik nazoratini amalga oshirish vazifasi yuklatildi.

Bosh prokuraturaning Kiberjinoyatlarga qarshi kurashishda qonuniylikni ta’minlash bo‘limi tomonidan o‘tgan qisqa davrda kiberjinoyatlarning oldini olish, ushbu toifadagi jinoyatlarni fosh etish va tergov qilishda tizimli ishlar amalga oshirildi. Shuningdek, muntazam ravishda hududiy guruh xodimlarining kiberjinoyatchilikka qarshi kurashish ko‘nikmalarini oshirish maqsadida o‘quv-seminar mashg‘ulotlari o‘tkazildi. Ichki ishlar organlari bilan hamkorlikda kiberjinoyatlarni fosh etish va tergov qilish amaliyotiga oid qo‘shma qarorlar qabul qilinib, xizmatda foydalanish uchun joylarga tarqatildi. Ushbu sohada prokurorlik nazorati kuchaytirildi va bevosita hududlarga chiqib, kiberjinoyatlarni fosh etish va tergov qilish yo‘nalishida amaliy yordam ko‘rsatilmoqda.

Bundan tashqari, so‘nggi yillarda prokuratura organlarida nafaqat qonuniylikni ta’minlash yo‘nalishida, balki kiberjinoyatchilikka qarshi kurashish sohasi samaradorligini oshirish maqsadida muammolarga innovatsion yondashgan holda ilmiy-amaliy islohotlar ham amalga oshirilmoqda.

Jumladan, davlat rahbarining 2024-yil 21-iyun kunidagi “Raqamli kriminalistika sohasida ilmiy-tadqiqot faoliyatini tashkil etish chora-tadbirlari to‘g‘risida”gi 229-sonli qaroriga muvofiq, Huquqni muhofaza qilish akademiyasida Raqamli kriminalistika ilmiy-tadqiqot instituti tashkil etildi.

Mazkur qarorga asosan institutga jinoyatlarni tergov qilish doirasida raqamli ma’lumotlarni izlaydigan, to‘playdigan va tahlil qiladigan, shuningdek, kripto-aktivlar, “bulutli texnologiyalar” va boshqalardan foydalangan holda sodir etilgan jinoyatlarni aniqlaydigan zamonaviy texnologiyalar va vositalarni joriy etish kabi bir qator vazifalar yuklatildi.

Hozirda institut xodimlari o‘zlariga yuklatilgan vazifalar ijrosi yuzasidan tezkor-qidiruv va tergov harakatlarida faol ishtirok etib, raqamli kriminalistika yo‘nalishida tergov organlariga amaliy ko‘mak ko‘rsatib kelmoqdalar.

Xususan, institut tashkil topgan kundan bugungi kunga qadar bo‘lgan davrda 900 dan ortiq murakkab turdagi raqamli ekspertizalar o‘tkazildi, shuningdek, tergov organlarining talabiga ko‘ra kripto-aktivlar aylanmasi sohasidagi xorijiy provayderlarga 394 ta rasmiy so‘rovlar yuborish orqali 683 nafar jinoyatga aloqador shaxsning akkaunt ma’lumotlari olindi hamda ushbu ma’lumotlar asosida blokcheyn tadqiqoti o‘tkazilib, huquqni muhofaza qilish organlariga 120 dan ortiq

mutaxassis fikri taqdim etildi.

Shuningdek, O‘zbekiston Respublikasi Prezidentining 2025-yil 30-aprel kunidagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi 153-sonli qaroriga muvofiq Huquqni muhofaza qilish akademiyasi Raqamli kriminalistika ilmiy-tadqiqot instituti tuzilmasida Kiberjinoyatlarga qarshi kurashishga va raqamli tergovga ko‘maklashish markazi tashkil etildi.

Markaz faoliyatining asosiy yo‘nalishlari sifatida tergovga qadar tekshiruv hujjatlarini, ma’muriy huquqbuzarliklar to‘g‘risidagi ishlarni hamda jinoyat ishlarini ilmiy yondashuvlar asosida o‘rganish orqali tavsiyalar ishlab chiqish va huquqni qo‘llash amaliyotiga tatbiq etish, shuningdek, kiberjinoyatlarni fosh etish va tergov qilish amaliyotida mavjud muammolarni aniqlab, ularni bartaraf etish bo‘yicha takliflar ishlab chiqish kabi yo‘nalishlar belgilandi.

Mazkur islohotlar mamlakatimizda prokuratura organlarining kiberjinoyatchilikka qarshi kurashish sohasidagi faoliyatini takomillashtirish yo‘nalishida amalga oshirilayotgan ishlarni ifodalaydi. Zamonaviy talablardan kelib chiqib, ixtisoslashtirilgan tuzilmalar tashkil etilmoqda hamda bu jarayonda barcha huquqni muhofaza qiluvchi organlar bilan samarali hamkorlik yo‘lga qo‘yilmoqda. Bu esa prokuratura organlarining jinoyatchilikka qarshi kurashishni muvofiqlashtiruvchi markaziy huquqiy institut sifatidagi maqomini yana bir bor tasdiqlaydi.

O‘z o‘rnida shuni ta’kidlash lozimki, axborot texnologiyalari yordamida sodir etilayotgan jinoyatlarning aksariyat qismi transchegaraviy jinoyatlar hisoblanib, ushbu jinoyatlarni fosh etish va tergov qilishda xalqaro hamkorlik doirasida o‘zaro huquqiy yordam mexanizmlarini ishlatish hamda bu jarayonni soddalashtirishda o‘ta muhim talablardan biridir.

Xususan, yuqorida keltirilgan 153-sonli qarorda Yevropa Ittifoqining “Kompyuter jinoyatlari to‘g‘risida”gi Budapesht konvensiyasiga muayyan shartlar asosida qo‘shilish masalasini har tomonlama o‘rganib chiqib, amaliy chora-tadbirlarni ko‘rish belgilangan.

Zero, Budapesht konvensiyasi kabi xalqaro hujjatlarni ratifikatsiya qilish orqali mamlakatimizda kiberjinoyatchilikka qarshi kurashish sohasida yangi imkoniyatlar yaratilib, ijobiy natijalarga erishiladi. Jumladan, mazkur konvensiyaga qo‘shilish, uni ratifikatsiya qilgan boshqa ishtirokchi davlatlar bilan xavfsiz aloqa kanali orqali uzluksiz tartibda o‘zaro ma’lumot almashinuvini amalga oshirishga imkon yaratadi, bu esa transchegaraviy raqamli dalillarni to‘plashning asosiy mexanizmlaridan biri hisoblanadi.

Hozirda Bosh prokuratura mas’ulligida huquqni muhofaza qiluvchi organlar xodimlaridan iborat idoralararo ishchi guruh tuzilib, kiberjinoyatchilikka qarshi kurash bo‘yicha milliy qonunchilikni xalqaro normalar talablariga muvofiqlashtirish va joriy etish yuzasidan jadal ishlar olib borilmoqda.

Tahlillarga ko‘ra, axborot texnologiyalari sohasidagi jinoyatlarning soni yildan-yilga ortib borishi, ushbu toifadagi jinoyatlarning fosh etilish darajasi pastligicha qolayotganligiga quyidagi omillar sabab bo‘lmoqda:

– raqamli transformatsiyaning jadal rivojlanishi va internetdan foydalanishning kengayishi – raqamlashtirish jarayoni ko‘plab imkoniyatlar yaratishi bilan birga, kiberxavfsizlik choralari lozim darajada ko‘rilmayotganligi jinoyatchilar uchun ham qulay shart-sharoitlar yaratmoqda;

– fuqarolarning raqamli savodxonlik darajasining yetarli emasligi va kiberxavfsizlik sohasidagi bilimlarining yo‘qligi – yengil daromad olish maqsadida raqamli gigiyena qoidalari va xavfsizlik talablariga rioya etmasliklari;

– banklar, to‘lov tizimlari operatorlari va to‘lov tashkilotlari himoya tizimlari*(antifrod)*ning kiberhujumlarning oldini olishda texnik jihatdan zaifligi;

– kiberxavfsizlik sohasida malakali mutaxassislarning yetishmasligi va ta’lim tizimining sifat jihatidan zaifligi – soha bo‘yicha tayyorlanayotgan mutaxassislar sonining cheklanganligi hamda yuqori malakali kadrlarning asosan xususiy sektor tomonidan jalb qilinishi;

– kiberjinoyatchilikka qarshi kurashish bilan shug‘ullanuvchi xodimlarning kasbiy ko‘nikmalari yetarli darajada shakllanmaganligi hamda zimmalariga yuklatilgan vazifalarni talab darajasida ijro etmayotganligi;

– banklar, to‘lov tashkilotlari va davlat organlari o‘rtasida tezkor ma’lumotlar almashinuvi va hamkorlikning zaifligi;

– jinoyatlarni fosh etish va tergovda muhim ahamiyatga ega bo‘lgan raqamli dalillar xorijiy davlatlarda joylashgan xizmat provayderlarining

serverlarida saqlanishi, o‘zaro huquqiy yordam mexanizmlarining amalda qo‘llanilmayotganligi, “Telegram”, “Meta” kompaniyasi *(Facebook, Instagram, WhatsApp)* kabi yirik ijtimoiy tarmoq provayderlari bilan rasmiy hamkorlik aloqalarining o‘rnatilmaganligi, shuningdek, jinoyatchilarning “Darknet” tarmog‘idan va noqonuniy yo‘l bilan olingan mablag‘larni yuvishda kripto-aktivlardan keng foydalanayotganligi;

Hozirda kiberjinoyatchilikka qarshi kurashish ahvolini yaxshilash va tizimli kamchiliklarni bartaraf etib, kelgusida ularning oldini olish choralarini ko‘rish maqsadga muvofiq hisoblanadi.

Yuqoridagilardan kelib chiqib:

– kiberjinoyatchilikka qarshi kurashish sohasida qonunchilikni takomillashtirish;

– axborot texnologiyalari sohasidagi jinoyatlarni barvaqt oldini olish;

– xodimlar malakasini oshirish;

– raqamli kriminalistika imkoniyatlaridan to‘liq foydalanish maqsadida zamonaviy axborot texnologiyalari asosida moddiy-texnik bazani takomillashtirish;

– transchegaraviy hamkorlikni rivojlantirish hamda bank va to‘lov tashkilotlarida xavfsizlik tizimini takomillashtirish chora-tadbirlarini jadallashtirish lozim bo‘ladi.

Xulosa o‘rnida shuni ta’kidlash joizki, kiberjinoyatchilikka qarshi kurashni ushbu yo‘nalishlarda takomillashtirish soha samaradorligini oshirishga va yanada ijobiy natijalarga erishishga xizmat qiladi.

#

Гайрат МУСАЕВ,
Администрация Президента Республики Узбекистан,
заведующий сектором, доцент

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В DARKNET

АННОТАЦИЯ. *В статье исследуется криминалистическая характеристика преступлений, совершаемых с использованием DarkNet. Автором критически анализируются классификации зарубежных исследователей а также рассматриваются типология субъектов DarkNet-преступлений, способы совершения преступлений и особенности формирования цифровых следов. В качестве практического примера анализируются международная операция по закрытию платформы AlphaBay.*

По результатам исследования автор предлагает многоуровневую концепцию криминалистической характеристики, включающую технологическую инфраструктуру, модифицированную субъектную характеристику, цифровую следовую картину и криптоэкономическую составляющую.

ANNOTATSIYA. *Maqolada "DarkNet" yordamida sodir etiladigan jinoyatlarning kriminalistik tavsifi tadqiq etiladi. Muallif xorijiy tadqiqotchilarning klassifikatsiyalarini tanqidiy tahlil qiladi, shuningdek, "DarkNet" jinoyatlari subyektlarining tipologiyasi, jinoyat sodir etish usullari va raqamli izlar shakllanishining xususiyatlari ko'rib chiqiladi. Amaliy misol sifatida "AlphaBay" platformasini yopish bo'yicha xalqaro operatsiya tahlil qilinadi. Tadqiqot natijalari asosida muallif texnologik infratuzilma, modifikatsiyalangan subyekt tavsifi, raqamli iz manzarasi va kriptoiqtisodiy tarkibiy qismni o'z ichiga olgan ko'p bosqichli kriminalistik tavsif konsepsiyasini taklif etadi.*

ABSTRACT. *The article examines the forensic characteristics of crimes committed using the DarkNet. The author critically analyzes classifications of foreign researchers and discusses the typology of DarkNet crime subjects, methods of committing crimes, and peculiarities of digital trace formation. The international operation to shut down the AlphaBay platform is analyzed as a practical example. Based on the research results, the author proposes a multi-level concept of forensic characterization that includes technological infrastructure, modified subject characteristics, digital trace pattern, and crypto-economic component.*

Ключевые слова: *цифровая криминалистика, киберпреступность, цифровые следы, технологии анонимизации, криптоактивы.*

Kalit so'zlar: *raqamli kriminalistika, kiberjinoyat, raqamli izlar, anonimlashtirish texnologiyalari, kripto-aktivlar.*

Key words: *digital forensics, cybercrime, digital evidence, anonymization technologies, crypto assets.*

Криминалистическая характеристика преступлений, совершаемых с использованием DarkNet, представляет собой систему криминалистически значимых признаков данной категории деяний, имеющую существенное теоретико-прикладное значение для оптимизации процесса их выявления, раскрытия и расследования. В условиях цифровизации криминальной среды формирование научно обоснованной криминалистической характеристики приобретает особую актуальность для правоприменительной практики, что обусловливает необходимость комплексного анализа структурных элементов данного криминалистического феномена.

Современное понимание криминалистической характеристики преступлений в цифровой среде формируется на основе классических криминалистических концепций с учетом специфики виртуального пространства. Фундаментальный вклад в разработку теории криминалистической характеристики внесли Р.С. Белкин и А.Н. Васильев, которые определили ее как систему данных о криминалистически значимых признаках преступлений определенного вида, отражающих закономерные связи между ними и служащих построению и проверке следственных версий при решении задач расследования[1]. Данная концепция получила дальнейшее развитие в работах Л.Я. Драпкина, который акцентировал внимание на вероятностном характере связей между элементами криминалистической характеристики[2].

Однако применение классических подходов к анализу преступлений в DarkNet требует существенной модификации в связи со спецификой виртуального пространства. Американский исследователь M. Chertoff справедливо отмечает, что традиционная криминалистическая характеристика не учитывает особенности виртуального пространства,

1 Белкин Р.С. Криминалистическая энциклопедия. М.: Мегатрон XXI, 2000. С. 144.

2 Драпкин Л. Я. Основы теории следственных ситуаций. — Свердловск: Издательство Уральского университета, 1987. — С. 67.

где отсутствуют физические границы, а преступная деятельность характеризуется высокой степенью технологической сложности[3]. В связи с этим он предлагает многоуровневую классификацию преступлений в DarkNet по степени их общественной опасности и структурированности:

Индивидуальные преступления низкой интенсивности - к данной категории M. Chertoff относит преступления, совершаемые одиночными субъектами без организационной структуры, характеризующиеся ограниченным масштабом воздействия и относительно низкой степенью общественной опасности. Типичными примерами являются индивидуальные покупки наркотических средств для личного потребления, разовые операции с поддельными документами. Отличительными признаками выступают: отсутствие долгосрочного планирования, ограниченное использование технологий анонимизации, минимальная вовлеченность в преступные сообщества.

Групповые преступления средней интенсивности включают преступную деятельность небольших групп (3-10 человек) с элементарным разделением ролей. Характерными примерами являются организация небольших интернет-магазинов по продаже наркотических средств, групповое мошенничество, коллективные схемы отмывания криптовалют. Данная категория характеризуется простейшей иерархией, использованием комбинированных методов анонимизации (TOR + VPN), регулярной преступной деятельностью в течение нескольких месяцев.

Организованные преступления высокой интенсивности представляют собой деятельность структурированных преступных организаций с четкой иерархией и долгосрочным планированием. К данной категории относятся крупные DarkNet-маркетплейсы, международные сети торговли наркотиками, профессиональные группы по продаже персональных данных. Отличительными характеристиками выступают строгая иерархическая структура, использование профессиональных технологий защиты, длительные периоды функционирования, значительные финансовые обороты.

Системные преступления критической интенсивности охватывают преступную деятельность, представляющую угрозу для критически важных инфраструктур государств. Сюда включаются государственный кибершпионаж через DarkNet-каналы, торговля оружием массового поражения, финансирование международного терроризма. Данная категория характеризуется государственным или квазигосударственным уровнем организации, использованием наиболее современных технологий анонимизации, потенциалом причинения ущерба национальной безопасности[4].

На наш взгляд, подход M. Chertoff имеет определенные достоинства, поскольку учитывает градацию сложности преступной деятельности в DarkNet и позволяет дифференцировать подходы к расследованию в зависимости от уровня организованности преступных групп. Вместе с тем представляется, что предложенная классификация чрезмерно упрощает многоаспектный характер преступлений в скрытом сегменте сети и не учитывает технологические особенности различных уровней DarkNet.

Более обоснованной представляется позиция американского исследователя Thomas J. Holt, который развивает технологически ориентированную классификацию, основанную на уровне сложности используемых инструментов анонимизации и шифрования[5]. Согласно его подходу, преступления в DarkNet следует классифицировать по следующим технологическим критериям:

Преступления базового технологического уровня - характеризуются использованием стандартных общедоступных инструментов анонимизации без их модификации. К данной категории относятся преступления, соверша-

3 Chertoff M. A public policy perspective of the Dark Web //Journal of Cyber Policy. – 2017. – Т. 2. – №. 1. – С. 26-38.

4 Chertoff M. Digital Transformation and Cybersecurity Challenges in Law Enforcement. Harvard National Security Journal. 2023. Vol. 14(2). P. 234-251.

5 Holt, Thomas J., and Adam M. Bossler. "An assessment of the current state of cybercrime scholarship." Deviant behavior 35.1 (2014): 20-40.

емые с использованием только TOR-браузера в стандартной конфигурации, применением общедоступных криптовалютных кошельков без дополнительных мер обеспечения анонимности, использованием популярных мессенджеров с базовым шифрованием. Субъекты данных преступлений обладают минимальными техническими навыками и полагаются на готовые решения.

Преступления продвинутого технологического уровня включают использование комбинированных методов анонимизации и модифицированного программного обеспечения. Характерно применение связки TOR + VPN + прокси-серверы, использование специализированных криптовалютных миксеров, применение модифицированных операционных систем (Tails, Whonix), использование кастомизированных мессенджеров с дополнительным шифрованием. Субъекты обладают серьезными техническими компетенциями и способны адаптировать существующие технологии под свои потребности.

Преступления экспертного технологического уровня предполагают разработку собственных технологических решений и использование профессиональных инструментов. Включают создание собственных анонимизирующих сетей, разработку кастомных криптографических протоколов, использование нулевых доказательств (zero-knowledge proofs) для обеспечения анонимности, применение квантово-устойчивых алгоритмов шифрования. Субъекты являются высококвалифицированными специалистами в сфере ИКТ, способными создавать инновационные технологические решения.

Преступления критического технологического уровня характеризуются использованием государственных или корпоративных ресурсов для создания сложнейших технологических инфраструктур. Субъекты обладают доступом к ресурсам государственного или крупного корпоративного уровня[6].

Технологически ориентированная классификация T.J. Holt представляется более практически значимой, поскольку она непосредственно коррелирует с методиками расследования и требуемыми техническими компетенциями следователей. Каждый технологический уровень требует специфических подходов к обнаружению следов, их фиксации и исследованию. Кроме того, данная классификация учитывает динамический характер развития технологий в DarkNet и позволяет прогнозировать появление новых форм преступной деятельности.

Критически оценивая обе представленные классификации, следует отметить, что они отражают различные аспекты одного явления и могут применяться комплексно. Классификация M. Chertoff больше подходит для криминологического анализа и оценки общественной опасности, тогда как подход T.J. Holt имеет большее значение для практики расследования и выбора технических средств противодействия преступности. На наш взгляд, оптимальным было бы создание интегрированной классификации, учитывающей как организационные, так и технологические критерии DarkNet-преступлений.

Развивая указанные теоретические подходы, следует отметить позицию европейских исследователей K. Kruithof и J. Aldridge, которые обосновывают необходимость включения в структуру криминалистической характеристики DarkNet-преступлений специфических элементов: *цифровая экосистема преступления, виртуальная преступная среда, технологическая инфраструктура правонарушения.*

Под *цифровой экосистемой преступления* авторы понимают совокупность взаимосвязанных цифровых платформ, сервисов и инструментов, обеспечивающих полный цикл преступной деятельности. Принципиальным отличием от традиционной преступной среды является глобальный характер, отсутствие географических границ и возможность быстрой реконфигурации.

Виртуальная преступная среда представляет социокультурную составляющую DarkNet-преступности, включающую нормы поведения, иерархии, системы репутации и доверия в анонимных сообществах.

Технологическая инфраструктура правона-

6 Martin J. Illuminating the dark net //Engaging with Ethics in International Criminological Research. – 2016. – С. 192.

рушения охватывает комплекс технических средств, обеспечивающих функционирование преступной деятельности: анонимизирующие сети, криптографические протоколы, технологии блокчейн. Анализ данной инфраструктуры позволяет установить уровень квалификации преступников и выявить уязвимости в их системах защиты[7].

С данной позицией следует согласиться, поскольку она отражает комплексный характер преступной деятельности в DarkNet, где технологические, социальные и экономические факторы образуют единую систему.

Переходя к анализу конкретных проявлений преступности в DarkNet, необходимо отметить, что типология данных преступлений характеризуется значительным разнообразием и постоянной эволюцией. Согласно данным отчета Европола Internet Organised Crime Threat Assessment (IOCTA) 2025, в структуре даркнет-преступности доминируют финансовые преступления (35%), торговля наркотическими средствами (28%), кибермошенничество (18%) и торговля личными данными (12%)[8]. При этом наблюдается устойчивая тенденция к усложнению схем преступной деятельности и повышению уровня организованности преступных групп.

Аналитическое исследование компании Market.us, проведенное в 2025 году на основе мониторинга активности даркнет-платформ, показывает несколько иную картину: кража личных данных составляет 65% всех отслеживаемых незаконных активностей, мошенничество с кредитными картами 15%, при этом объем компрометированных данных кредитных карт превысил 192 миллиона записей[9]. Однако представленные данные, требуют критического анализа, поскольку методология исследования Market.us не учитывает латентность значительной части преступлений в DarkNet, что может существенно исказить реальную картину преступности.

Критически оценивая представленную статистику, следует отметить определенные противоречия в данных различных исследований. На наш взгляд, расхождения в статистических показателях обусловлены различными методологическими подходами к мониторингу DarkNet-активности и неоднородностью исследуемых сегментов скрытой сети. Более объективную картину могли бы дать комплексные исследования, объединяющие данные *правоохранительных органов, академических исследований и коммерческого мониторинга.*

По официальным данным Департамента по борьбе с киберпреступностью МВД Республики Узбекистан, в 2025 году доля киберпреступлений достигла 49,6% от общего объема преступности в стране, принеся гражданам ущерб свыше 2 трлн сумов, а за первые 6 месяцев 2026 года (объявленного ведомством «Годом борьбы с киберпреступностью») правоохранительными органами было раскрыто 9 282 и инициативно выявлено 4 011 ИТ-преступлений, при этом совместные действия МВД и Центрального банка позволили заблокировать 18 838 мошеннических банковских карт и вернуть гражданам 120,49 млрд сумов[10].

Значительный рост показателей киберпреступности в Республике Узбекистан был обусловлен совершенствованием учетно-регистрационной дисциплины и изменением правоприменительной практики в части процессуальных решений о соединении уголовных дел. Ранее в органах внутренних дел сложилась отрицательная практика необоснованного соединения множественных эпизодов киберпреступлений в рамках одного уголовного дела под предлогом их совершения аналогичным способом или предполагаемой групповой принадлежности к одной преступной органи-

7 Kruithof K., Aldridge J. The Role of the 'Dark Net' in the Trade of Illicit Drugs. RAND Europe Research Report. Cambridge: RAND Corporation, 2020. P. 134-147.

8 EUROPOL. Internet Organised Crime Threat Assessment (IOCTA) 2024 // [Электронный ресурс]. — Режим доступа: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024. — Дата доступа: 11.01.2025.

9 Market.us. Dark Web Monitoring Market Report 2025 // [Электронный ресурс]. — Режим доступа: https://scoop.market.us/dark-web-statistics. — Дата доступа: 11.01.2025.

10 Ущерб от киберпреступлений в 2021–2024 годах в Узбекистане превысил 1,9 трлн сумов // [Электронный ресурс]. — Режим доступа: https://www.gazeta.uz/ru/2025/05/29/cybercrime/. — Дата доступа: 30.05.2025.
Retry

зации. Особенно негативной стороной указанной практики являлось последующее приостановление объединенных уголовных дел в соответствии со статьей 364 ч.1 УПК Республики Узбекистан по основанию неустановления лица, подлежащего привлечению в качестве обвиняемого. Такой подход приводил к тому, что сотни отдельных преступных деяний учитывались как одно приостановленное дело, что кардинально искажало реальную картину состояния преступности.

В связи с чем была пересмотрена практика процессуального оформления преступлений, совершаемых с использованием ИКТ. Даны разъяснения о недопустимости необоснованного соединения дел о киберпреступлениях и необходимости выделения каждого эпизода преступной деятельности в отдельное производство при отсутствии процессуальных оснований для их объединения. В результате корректировки учетно-регистрационной практики каждый факт киберпреступления стал учитываться отдельно, что привело к более объективному отражению реального состояния преступности в данной сфере и обеспечило соответствие статистической отчетности фактическим данным о количестве совершенных правонарушений.

Логическим продолжением типологического анализа является исследование субъектной характеристики лиц, совершающих преступления с использованием DarkNet. Данный элемент криминалистической характеристики имеет особое значение для построения версий о личности неустановленного преступника и выбора оптимальных тактических решений при расследовании.

Согласно результатам эмпирического исследования, проведенного Национальным агентством по борьбе с преступностью Великобритании (NCA), криминалистический портрет типичного субъекта DarkNet-преступлений включает следующие характеристики: лица мужского пола (89% случаев), возрастной диапазон 20-35 лет (72%), наличие высшего или неоконченного высшего образования (81%), владение несколькими языками (63%), наличие профессиональных навыков в области программирования (78%), отсутствие предшествующих судимостей (85%)[11].

Представленные статистические данные, вызывают определенные вопросы. В частности, остается неясным, каким образом исследователи получали достоверную информацию о субъектах преступлений в условиях высокого уровня анонимности DarkNet. Кроме того, выборка, основанная исключительно на выявленных и расследованных преступлениях, может не отражать реальную структуру субъектного состава, поскольку наиболее квалифицированные преступники имеют больше шансов избежать разоблачения.

Альтернативную точку зрения представляют французские исследователи D. Décary-Hétu и V. Mousseau, которые на основе анализа профилей продавцов на даркнет-маркетплейсах выделяют три основные категории субъектов.

Технические специалисты представляют собой высококвалифицированных специалистов в сфере ИКТ, обладающих глубокими знаниями в области программирования и криптографии. Данная категория характеризуется целенаправленной специализацией на киберпреступлениях, способностью разрабатывать собственные технологические решения, занимая ключевые позиции в иерархии DarkNet-сообществ в роли администраторов маркетплейсов и разработчиков специализированного программного обеспечения.

Традиционные преступники составляют категорию лиц, которые используют DarkNet как технологический инструмент для расширения традиционной преступной деятельности, не обладая глубокими техническими компетенциями. К данной группе относятся наркоторговцы, мошенники, торговцы оружием, которые адаптировали цифровые технологии для совершенствования традиционных преступных схем.

Случайные пользователи представляют наиболее многочисленную категорию участников DarkNet-преступности, характеризующуюся эпизодическим участием в незакон-

11 National Crime Agency. Cyber Crime Assessment 2023 // [Электронный ресурс]. — Режим доступа: https://nationalcrimeagency.gov.uk/images/NSA_2023_Website_-_PDF_Version_1.pdf. — Дата доступа: 12.01.2025.

ной деятельности. Данная группа включает лиц, обращающихся к ресурсам DarkNet для разовых покупок запрещенных товаров, не имея намерения заниматься систематической преступной деятельностью[12]. Отличительными признаками выступают минимальные технические навыки, использование базовых методов анонимизации, отсутствие долгосрочных планов преступной деятельности. На наш взгляд, данная классификация более точно отражает реальную структуру субъектного состава, поскольку учитывает различные мотивы и уровни вовлеченности в преступную деятельность, что имеет принципиальное значение для разработки дифференцированных методик расследования.

Развивая тему субъектной характеристики, следует отметить особую роль организованных преступных групп в структуре DarkNet-преступности. Согласно исследованиям А.К. Расулева в области киберпреступности в Республике Узбекистан, значительная часть выявленных преступлений в сфере информационных технологий совершается в составе организованных групп, при этом наблюдается четкая специализация участников по функциональным ролям. Данная тенденция подтверждается и международными исследованиями, что позволяет говорить о формировании специфической модели организованной преступности в виртуальном пространстве[13].

Анализ субъектной характеристики закономерно приводит к рассмотрению способов совершения преступлений в DarkNet, которые характеризуются высокой степенью технологической сложности и постоянной эволюцией. Американские исследователи N. Christin и K. Moore[14] выделяют следующие характерные черты механизма совершения DarkNet-преступлений:

Использование многоуровневых систем анонимизации представляет собой комплексное применение различных технологий сокрытия цифровой идентичности, включающее сеть TOR для маршрутизации трафика через множественные зашифрованные узлы, виртуальные частные сети (VPN) для дополнительного уровня защиты, прокси-серверы различных типов, а также специализированные операционные системы типа Tails, не оставляющие следов на локальном компьютере.

Применение криптографических методов защиты информации охватывает end-to-end шифрование коммуникаций, PGP-шифрование электронной почты, полнодисковое шифрование локальных данных, использование криптографических протоколов с совершенной прямой секретностью и стеганографию для сокрытия информации в обычных файлах. Данные технологии создают многослойную систему защиты, существенно усложняющую процесс деанонимизации для правоохранительных органов.

Использование криптовалют для финансовых операций стало стандартом DarkNet-экономики благодаря псевдонимности блокчейн-технологий, при этом преступники применяют Bitcoin как базовую валюту, приватные криптовалюты (Monero, Zcash) для повышенной анонимности, криптовалютные миксеры для перемешивания монет и затруднения отслеживания, а также сложные схемы отмывания через множественные кошельки и децентрализованные биржи.

Внедрение систем репутации и доверия адаптирует коммерческие механизмы к анонимной среде посредством рейтинговых систем оценки продавцов, эскроу-сервисов для блокировки средств до подтверждения сделки, систем арбитража для разрешения споров, механизмов страхования транзакций и программ лояльности для постоянных клиентов. Эти системы создают парадоксальную атмосферу «деловой этики» в преступной среде, обеспечивая долгосрочное функционирование нелегальных рынков и формируя

12 Décary-Hétu D., Mousseau V. Criminal Careers in Cryptomarkets. Criminology & Criminal Justice. 2022. Vol. 18(4). P. 78-96.

13 Расулев, А. 2022. Киберпреступность: причины и условия, личность преступника. in Library. 22, 1 (янв. 2022), 108–115.

14 Christin, N. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace // Proceedings of the 22nd International Conference on World Wide Web (WWW '13). — [Электронный ресурс]. — Режим доступа: https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf. — Дата доступа: 30.05.2025.

устойчивые экономические отношения между участниками преступной деятельности[15].

Показательным примером применения описанных технологических решений является международная операция «Bayonet» по закрытию DarkNet-маркетплейса AlphaBay в 2017 году. Данная платформа, функционировавшая с 2014 по 2017 год под управлением 25-летнего канадского гражданина Александра Казеса (псевдоним Alpha02), наглядно демонстрировала все характерные черты механизма совершения DarkNet-преступлений, выделенные N. Christin и K. Moore. AlphaBay использовал сложную многоуровневую систему анонимизации, включавшую функционирование как onion-сервис в сети TOR, так и узел в сети I2P, применял криптографические методы защиты всех коммуникаций через PGP-шифрование, принимал платежи исключительно в криптовалютах (Bitcoin, Monero, Ethereum), а также внедрил развитую систему репутации продавцов с обязательными эскроу-депозитами для обеспечения безопасности сделок[16].

С точки зрения криминалистической характеристики, случай AlphaBay демонстрирует типичные закономерности субъектного состава DarkNet-преступлений: *высокообразованный IT-специалист с техническими компетенциями, отсутствие предшествующих судимостей, использование устоявшегося псевдонима для создания репутационного капитала в преступной среде.* К моменту закрытия платформа обслуживала свыше 400 000 пользователей, более 40 000 продавцов, генерировала ежедневный оборот от 600 000 до 800 000 долларов США и содержала около 250 000 предложений о продаже наркотических средств. Обстановка совершения преступления характеризовалась глобальным масштабом деятельности с серверной инфраструктурой, распределенной по нескольким юрисдикциям (Литва, Канада, Таиланд), что создавало дополнительные сложности для правоохранительных органов[17].

Особый криминалистический интерес представляет анализ следообразования и причин разоблачения AlphaBay, которые наглядно иллюстрируют уязвимости даже высокотехнологичных преступных схем. Несмотря на применение сложных технологий анонимизации, администратор платформы совершил ряд критических ошибок:

- использовал личный email-адрес *pimp_alex_91@hotmail.com* для системных уведомлений платформы, который был связан с его профилем LinkedIn и легальным компьютерным бизнесом в Канаде;
- применял псевдоним Alpha02, который использовал в различных форумах с 2008 года;
- в момент ареста был авторизован в незашифрованном ноутбуке, выполняя административную перезагрузку сервера AlphaBay.

Данные обстоятельства позволили правоохранительным органам установить корреляционные связи между различными категориями цифровых следов и успешно деанонимизировать субъекта преступления. Координированные действия правоохранительных органов США, Канады, Таиланда, Нидерландов, Литвы, Великобритании и Франции при поддержке Европола привели к изъятию серверной инфраструктуры и криптовалютных активов, что стало одним из наиболее масштабных международных расследований в сфере DarkNet-преступности[18].

Рассмотрение способов совершения преступлений естественным образом приводит к анализу процессов следообразования в DarkNet как ключевого элемента криминалистической характеристики. Следообразование при совершении преступлений в DarkNet характеризуется рядом специфических особенностей, обусловленных цифровой средой функционирования и применением специали-

15 Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace // [Электронный ресурс]. — Режим доступа: https://www.semanticscholar.org/reader/79fb8e6bbcdafa0912b224dbba1bb41c8b96c85c. — Дата доступа: 31.05.2025.

16 AlphaBay Takedown [Электронный ресурс] / Federal Bureau of Investigation. – Режим доступа: https://www.fbi.gov/news/stories/alphabay-takedown (дата обращения: 21.02.2018).

17 AlphaBay, the Largest Online 'Dark Market,' Shut Down [Электронный ресурс] / U.S. Department of Justice, Office of Public Affairs. – Режим доступа: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (дата обращения: 20.07.2017

18 Operation Bayonet (darknet) [Электронный ресурс] // Wikipedia. – Режим доступа: https://en.wikipedia.org/wiki/Operation_Bayonet_(darknet) (дата обращения: 13.05.2025).

зированных технологий анонимизации, что требует переосмысления традиционных криминалистических подходов к обнаружению, фиксации и исследованию следов преступной деятельности.

В современной научной литературе существуют различные подходы к классификации следов DarkNet-преступлений. В.Б. Вехов и С.В. Зуева в своем фундаментальном труде по цифровой криминалистике выделяют иерархическую модель формирования цифровых следов, включающую четыре основных уровня.

Физический уровень включает следы на материальных носителях информации.

Логический уровень охватывает структуру организации данных: файловые таблицы, журналы изменений, удаленные файлы, фрагментированные данные, временные файлы операционных систем.

Системный уровень включает логи системных событий, записи реестра, кэши DNS-запросов, таблицы сетевых соединений, конфигурационные файлы приложений.

Прикладной уровень представляет наиболее содержательную категорию: история браузера, сохраненные пароли, файлы cookies, переписка в мессенджерах, кэши изображений, пользовательские документы[19].

Развитие теории цифрового следообразования в криминалистике связано также с работами В.А. Мещерякова, который выделил специфическую категорию «виртуальных следов», формирующихся в процессе функционирования компьютерных сетей. К данной категории относятся фрагменты зашифрованных данных в промежуточных узлах сети, временные метки установления и разрыва соединений, сигнатуры криптографических протоколов, метаданные сетевых пакетов, записи о туннелировании трафика через анонимизирующие сети. Выделение данной категории следов отражает специфику DarkNet как качественно новой среды следообразования, где традиционные подходы к локализации следов требуют существенной модификации.

Особое криминалистическое значение приобретают криптовалютные транзакции как специфический вид цифровых следов. Несмотря на то, что криптовалютные операции осуществляются с использованием буквенно-цифровых адресов кошельков без указания реальных имен владельцев, они сохраняют определенную доказательственную ценность благодаря публичной природе блокчейна. Неизменяемая запись всех транзакций с указанием адресов кошельков, сумм переводов, временных меток позволяет проводить анализ финансовых потоков. Современные методы криминалистического анализа блокчейна включают кластеризацию адресов, анализ паттернов поведения, корреляцию с данными криптовалютных бирж, что в ряде случаев позволяет установить связь между виртуальными кошельками и реальными личностями, о чем свидетельствует практика расследования крупных DarkNet-платформ.

Интегрированный подход к различным классификационным системам создает методологическую основу для разработки специализированных криминалистических методик, адекватных технологическим особенностям DarkNet-среды и учитывающих многоуровневый характер цифрового следообразования в анонимизированных сетях. Данный подход позволяет следователям и экспертам системно подходить к поиску, обнаружению и фиксации цифровых следов преступлений, совершенных с использованием скрытого сегмента сети Интернет.

По нашему мнению, криминалистическая характеристика преступлений, совершенных с использованием DarkNet, представляет собой систему взаимосвязанных криминалистически значимых признаков, отражающих закономерности преступной деятельности в анонимизированном сегменте сети Интернет и включающих как традиционные элементы криминалистической характеристики в их модифицированном виде, так и специфические элементы, обусловленные особенностями цифровой среды функционирования.

Структурно данная характеристика должна включать следующие основные элементы:

1. Технологическая инфраструктура пре-

19 Вехов, В. Б. Цифровая криминалистика : учебник для вузов / В. Б. Вехов, С. В. Зуева. – Москва : Юрайт, 2021. – 417 с

ступления - новый специфический элемент, включающий характеристику используемых анонимизирующих технологий, программного обеспечения, криптографических методов защиты, способов обеспечения анонимности финансовых операций. Данный элемент не имеет аналогов в традиционной криминалистической характеристике и отражает фундаментальную роль технологий в механизме совершения DarkNet-преступлений.

2. Модифицированная субъектная характеристика, учитывающая специфику личности DarkNet-преступника: высокий уровень технических компетенций, особенности социально-психологического портрета, функциональные роли в виртуальных преступных сообществах, модели поведения в анонимной среде. В отличие от традиционной субъектной характеристики, здесь принципиальное значение имеют не столько социально-демографические признаки, сколько цифровые компетенции и модели сетевого поведения.

3. Цифровая следовая картина - специализированный элемент, включающий характеристику процессов формирования и обнаружения цифровых следов в условиях применения технологий анонимизации. Включает классификацию следов по уровням цифровой инфраструктуры, временным характеристикам существования, степени защищенности от деанонимизации.

4. Виртуальная обстановка совершения преступления - элемент, характеризующий особенности цифровой среды, в которой реализуется преступная деятельность: типы используемых DarkNet-платформ, временные паттерны активности, географическое распределение узлов сети, особенности виртуальных преступных сообществ.

5. Трансформированный способ совершения преступления, интегрирующий физические и виртуальные действия преступника, включающий алгоритмы использования анонимизирующих технологий, схемы взаимодействия с DarkNet-платформами, методы обеспечения конспирации в цифровой среде.

6. Криптоэкономическая составляющая - новый элемент, отражающий особенности использования криптовалют и альтернативных платежных систем, включающий анализ финансовых потоков в блокчейне, способы отмывания криптовалютных активов, механизмы ценообразования на нелегальных рынках.

Принципиальной особенностью предлагаемой криминалистической характеристики является ее многоуровневая структура, отражающая иерархическую организацию цифровой среды DarkNet. На техническом уровне анализируются аппаратные и программные компоненты, на сетевом уровне - протоколы анонимизации и маршрутизации, на прикладном уровне - пользовательские интерфейсы и приложения, на социальном уровне - виртуальные преступные сообщества и их взаимодействие.

Важной характеристикой предлагаемой модели является динамичность и адаптивность. В отличие от традиционной криминалистической характеристики, которая формируется на основе анализа завершенных преступлений, характеристика DarkNet-преступлений должна учитывать быструю эволюцию технологий и постоянное изменение способов совершения преступлений. Это требует регулярного мониторинга и обновления элементов характеристики.

Таким образом, предлагаемая авторская концепция криминалистической характеристики преступлений, совершенных с использованием DarkNet, представляет собой комплексный научно-практический инструмент, позволяющий системно анализировать данную категорию преступлений и разрабатывать эффективные методы их расследования в условиях постоянной технологической эволюции цифровой преступности.

#

Евгений КОЛЕНКО,
Доктор философии (PhD) по юридическим наукам,
профессор, первый заместитель начальника
Правоохранительной академии Республики Узбекистан

ПРАКТИКО-ОРИЕНТИРОВАННАЯ ПОДГОТОВКА КАДРОВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: ОПЫТ ПРАВООХРАНИТЕЛЬНОЙ АКАДЕМИИ РЕСПУБЛИКИ УЗБЕКИСТАН

АННОТАЦИЯ. *В статье исследуется модель практико-ориентированной подготовки кадров в сфере расследования киберпреступлений, реализуемая Правоохранительной академией Республики Узбекистан. Показано, что отличительной чертой данной модели является органическая связь между экспертной деятельностью Научно-исследовательского института цифровой криминалистики и образовательным процессом Академии. Реальные уголовные дела становятся основой учебных программ, методических пособий и алгоритмов следственных действий. На основе анализа нормативно-правовой базы, статистики киберпреступности и конкретных экспертных случаев обосновывается вывод о том, что интеграция науки, практики и обучения в рамках единой институциональной структуры формирует воспроизводимую региональную модель подготовки специалистов в области цифровой криминалистики.*

ANNOTATSIYA. *Maqolada O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi tomonidan kiberjinoyatlarni tergov qilish sohasida amalga oshirilayotgan kadrlarni amaliyotga yo‘naltirilgan holda tayyorlash modeli tadqiq etilgan. Ushbu modelning o‘ziga xos xususiyati Raqamli kriminalistika ilmiy-tadqiqot institutining ekspertlik faoliyati hamda akademiya ta’lim jarayoni o‘rtasidagi uzviy bog‘liqlik ekanligi ko‘rsatib o‘tilgan. Real jinoiy ishlar o‘quv dasturlari, uslubiy qo‘llanmalar va tergov harakatlari algoritmlarining asosiga aylanmoqda. Normativ-huquqiy baza, kiberjinoyatchilik statistikasi va muayyan ekspertlik holatlari tahlili asosida yagona institutsional tuzilma doirasida ilm-fan, amaliyot va o‘qitishning integratsiyalashuvi raqamli kriminalistika sohasida mutaxassislar tayyorlashning takror ishlab chiqiluvchi mintaqaviy modelini shakllantirishi to‘g‘risidagi xulosa asoslangan.*

ABSTRACT. *The article examines the practice-oriented model of personnel training in cybercrime investigation implemented by the Law Enforcement Academy of the Republic of Uzbekistan. The distinctive feature of this model is the organic connection between the expert activities of the Institute of Digital Forensics and the Academy's educational process: real criminal cases form the basis of curricula, methodological manuals and investigative algorithms. Based on an analysis of the regulatory framework, cybercrime statistics and specific forensic cases, the article concludes that the integration of science, practice and education within a single institutional structure creates a replicable regional model for training digital forensics specialists.*

Ключевые слова: *киберпреступность, цифровая криминалистика, практико-ориентированное обучение, подготовка кадров, цифровые доказательства, Правоохранительная академия, НИИ цифровой криминалистики, блокчейн-аналитика, Даркнет.*

Kalit so‘zlar: *kiberjinoyatchilik, raqamli kriminalistika, amaliyotga yo‘naltirilgan o‘qitish, kadrlarni tayyorlash, raqamli dalillar, Huquqni muhofaza qilish akademiyasi, Raqamli kriminalistika ITI, blokcheyn-tahlil, Darknet.*

Key words: *cybercrime, digital forensics, practice-oriented training, personnel development, digital evidence, Law Enforcement Academy, blockchain analytics, Darknet.*

Стремительный рост киберпреступности в Республике Узбекистан за последние годы приобрёл характер, который точнее всего описывается не как количественное увеличение, а как структурная трансформация самой преступности. По данным официальной статистики МВД Республики Узбекистан, если в 2019 году с использованием информационных технологий в стране совершалось 863 преступления 18 видов, то в 2024 году этот показатель достиг 72 800 преступлений 62 видов — рост в 68 раз за пять лет[1]. Доля преступлений, совершённых с применением информационных технологий, в общей структуре преступности увеличилась с 7,2% в 2023 году до 49,6 % в 2025 году. Иными словами, сегодня почти каждое второе расследуемое уголовное дело содержит цифровой компонент. Столь стремительная трансформация криминальной среды с неизбежностью поставила вопрос о соответствии ей системы подготовки кадров. Как обоснованно констатирует профессор Б.Х. Пулатов, применительно к правоохранительной сфе-

1 Статистические данные Центра кибербезопасности МВД Республики Узбекистан // Официальный сайт Министерства внутренних дел Республики Узбекистан [Электронный ресурс]. – URL: https://gov.uz/ru/iiv/news/view/57775 (дата обращения: 27.06.2026).

ре существует острая необходимость в целенаправленной подготовке специализированных кадров и внедрении профильных образовательных программ[2].

Это наблюдение приобретает особую актуальность в контексте процессуальных изменений. Принятый в октябре 2024 года Закон Республики Узбекистан № ЗРУ-1003 впервые закрепил за цифровыми доказательствами самостоятельный процессуальный статус в Уголовно-процессуальном и смежных кодексах[3]. Правовое признание нового вида доказательств само по себе не порождает практической готовности следователей и прокуроров с ним работать. Прокурор, не способный оценить заключение эксперта о результатах цифровой экспертизы, не может надлежащим образом поддержать обвинение в суде даже при наличии полноценной доказательной базы.

Именно это противоречие между юридическим признанием цифровых доказательств и фактической готовностью правоохранительной системы к работе с цифровыми доказательствами определило логику институционального решения, закреплённого Постановлением Президента Республики Узбекистан № ПП-229 от 21 июня 2024 года. Данным актом на Правоохранительную академию Республики Узбекистан были возложены новые задачи по осуществлению инновационных исследований в сфере цифровой криминалистики, оказанию практической помощи правоохранительным органам в выявлении и исследовании цифровых следов, а также подготовке квалифицированных кадров, обладающих специальными знаниями и навыками в сфере борьбы с киберпреступностью[4].

Для реализации этих задач в структуре Академии был образован Научно-исследовательский институт цифровой криминалистики (далее — Институт). Принципиальная особенность избранной модели состоит в том, что экспертная практика и образовательный процесс не разделены организационно,

а объединены в рамках одной структуры: расследованный случай становится кейсом, разработанная методика — учебным алгоритмом, выявленный пробел — нормотворческим предложением.

Настоящая статья посвящена анализу этой модели в трёх взаимосвязанных измерениях: её нормативных и организационных оснований, содержания экспертной практики, питающей образовательный процесс, и конкретных форм трансляции этой практики в подготовку кадров.

Понять логику институционального устройства Академии невозможно без обращения к предшествующей нормативной базе. Путь к созданию НИИ цифровой криминалистики был подготовлен последовательным расширением государственной стратегии «Цифровой Узбекистан 2030». Постановление Президента Республики Узбекистан № ПП-122 от 8 февраля 2022 года предусмотрело внедрение принципиально новых видов исследований — экспертизы цифровых баз данных и экспертизы облачных сервисов[5]. Указ Президента Республики Узбекистан № УП-257 от 28 ноября 2022 года закрепил задачи развития Правоохранительной академии как ведущего центра подготовки кадров для правоохранительных органов[6]. Наконец, уже после создания Института, Указ Президента Республики Узбекистан № УП-204 от 3 ноября 2025 года

2 Пулатов Б.Х. Вопросы совершенствования системы подготовки и повышения квалификации кадров в сфере борьбы с преступностью // Вестник Академии Генеральной прокуратуры Республики Узбекистан. – 2021 г. – № 3. – С. 14–19.

3 Закон Республики Узбекистан ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами» от 21 ноября 2024 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/docs/7228823 (дата обращения: 27.06.2026).

4 Постановление Президента Республики Узбекистан № ПП-229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики» от 21 июня 2024 г. – [Электронный ресурс]. – Режим доступа: https://lex.uz/ru/docs/6977762.

5 Постановление Президента Республики Узбекистан № ПП-122 «О мерах по дальнейшему совершенствованию экспертно-криминалистической деятельности органов внутренних дел с широким внедрением достижений современной науки» от 8 февраля 2022 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/uz/docs/5851539 (дата обращения: 27.06.2026).

6 Указ Президента Республики Узбекистан № УП-257 «О мерах по внедрению передовых цифровых технологий в сферу государственного управления и коренному совершенствованию деятельности в данном направлении» от 28 ноября 2022 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/docs/6299079 (дата обращения: 27.06.2026).

«Об утверждении Стратегии „Цифровая прокуратура — 2030“» определил курс на перевод всей следственной и прокурорской деятельности в цифровую форму[7], а Указ Президента Республики Узбекистан № УП-38 от 10 марта 2026 года закрепил противодействие киберпреступности в качестве стратегической государственной задачи[8]. Таким образом, создание Института в 2024 году не было изолированным решением — оно стало закономерным этапом целенаправленной государственной политики, в рамках которой Академия последовательно наделялась всё более широким кругом полномочий.

Согласно Постановлению Президента Республики Узбекистан № ПП-229, в составе Института осуществляют деятельность четыре подразделения:

– Специализированный центр цифровых исследований;

– Центр содействия цифровому расследованию и борьбе с киберпреступлениями;

– Лаборатория цифровой криминалистики;

– Отдел оказания методической помощи[9].

Такое построение воспроизводит логику, хорошо известную в мировой практике. В частности, опыт формирования аналогичных структур в системе Верховной прокуратуры Республики Корея показал, что разграничение функций экспертизы, методического сопровождения и обучения внутри единой организации существенно сокращает разрыв между научной разработкой и её внедрением в следственную практику.

Существенным отличием от традиционной схемы, при которой экспертные учреждения и образовательные организации функционируют раздельно, является именно встроенность методической трансляции в текущую следственную практику. В условиях, когда специалист НИИ участвует в расследовании конкретного уголовного дела и одновременно является преподавателем или разработчиком методических материалов Академии, разрыв между экспертным знанием и его усвоением следователем и прокурором сокращается принципиально. Алгоритм, апробированный в ходе реального следственного действия, не проходит многолетний цикл от научной публикации до учебной программы — он становится учебным содержанием непосредственно по завершении дела.

Как справедливо отмечал Ж.Сремак применительно к мировой практике развития цифровой криминалистики, исторически эта дисциплина развивалась реактивно: специалисты вырабатывали приёмы работы, отвечая на конкретные вызовы преступности, в условиях отсутствия фундаментальной теоретической базы[10]. Академия, институционально объединив экспертизу и образование, создала механизм, при котором этот разрыв преодолевается системно, а не ситуативно.

Описанная организационная логика могла бы остаться декларацией, если бы не была подкреплена соответствующей материально-технической базой. Лаборатории Института выполняют двойную функцию: они одновременно являются местом проведения реальных экспертиз по уголовным делам и учебными полигонами для слушателей Академии. Это принципиально отличает их от стандартных учебных лабораторий, моделирующих условия работы: здесь условия работы являются реальными.

DarkWeb-лаборатория, открытая в 2021 году при поддержке Координатора проектов ОБСЕ в Узбекистане, стала первой подобной структурой в республике. Оснащённая выделенным сервером, специализированной

7 Указ Президента Республики Узбекистан № УП-204 «Об утверждении Стратегии "Цифровая прокуратура — 2030" и мерах по широкому внедрению цифровых технологий в деятельность органов прокуратуры» от 3 ноября 2025 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/docs/7813709 (дата обращения: 27.06.2026).

8 Указ Президента Республики Узбекистан № УП-38 «Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности» от 10 марта 2026 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/ru/docs/8079279 (дата обращения: 27.06.2026).

9 Постановление Президента Республики Узбекистан № ПП-229 «О мерах по организации деятельности Научно-исследовательского института цифровой криминалистики Правоохранительной академии Республики Узбекистан» от 18 мая 2026 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/ru/docs/6977762 (дата обращения: 27.06.2026).

10 Sremack J.C. AI Forensics: Investigation and Analysis of Artificial Intelligence Systems. – London; New York: Routledge, 2026. – P. 34–38.

сетевой инфраструктурой и программным обеспечением для мониторинга скрытых сегментов сети интернет (DarkWeb Monitor, Kodex Global, Project Arachnid, ICACCOPS), она используется одновременно для проведения реальных расследований и для обучения слушателей навыкам работы в Darknet.

Тренинги по расследованию преступлений в скрытых сетях и анализу криптовалютных транзакций проводятся на том же оборудовании, что и экспертная работа — различие лишь в процессуальном контексте, но не в технологии. Лаборатория Фарадея — первая в Узбекистане, её стены полностью экранированы металлом в соответствии с требованиями ISO/IEC 17025:2017 — решает иную, не менее важную задачу, исключая удалённое стирание данных с изъятых устройств, принудительное шифрование и несанкционированную синхронизацию, гарантируя процессуальную чистоту цифровых доказательств с момента их поступления на исследование.

Для слушателей Академии работа в условиях такого экранирования — навык, который невозможно получить нигде в регионе. Передвижная лаборатория, оснащённая резервным электроснабжением, системой видеофиксации и двумя типами БПЛА для аэрофотосъёмки, обеспечивает возможность криминалистического исследования непосредственно на месте происшествия. Её выезды на реальные следственные действия с участием слушателей превратились в один из наиболее востребованных форматов практических занятий.

Программно-аппаратный комплекс Института охватывает полный цикл цифровой криминалистики: извлечение данных с мобильных устройств (Cellebrite UFED, Tableau Forensic Imager, PC3000, Flash); криминалистический анализ цифровых следов (Magnet AXIOM, Belkasoft, PasswareKit Forensic, Autopsy, DFAS Pro); блокчейн-аналитику и мониторинг транзакций криптоактивов (Elliptic, Chainalysis). Именно эта совокупность инструментов — не смоделированная, а реально используемая в расследованиях, — составляет основу практических занятий. Тем самым слушатель ещё в процессе обучения приобретает компетенции, непосредственно востребованные в следственной практике.

Если инфраструктура создаёт условия для практико-ориентированного обучения, то его содержательным ядром являются конкретные уголовные дела, расследованные специалистами Института. Именно здесь модель Академии приобретает наибольшую специфику: каждое завершённое расследование анализируется с точки зрения методических уроков и в той или иной форме включается в учебный процесс. Рассмотрим несколько показательных примеров.

В рамках взаимодействия с Интерполом через платформу Project Arachnid и систему ICACCOPS специалисты Института выявили более 2000 веб-страниц с материалами сексуального насилия над детьми. В одном из дел на даркнет-форуме было обнаружено 603 видеоматериала с несовершеннолетними; лицо привлечено к уголовной ответственности. Принципиально важным с методической точки зрения стало дело в отношении гражданина Таджикистана: идентификация подозреваемого осуществлялась через хеш-значения медиафайлов по технологии Arthropod в совокупности с OSINT-анализом скрытого сегмента сети, что позволило суду вынести обвинительный приговор в виде пожизненного лишения свободы.

Деятельность Института в этом направлении отмечена официальной благодарностью Интерпола. Разработанная в ходе этих расследований методика хеш-идентификации медиаматериалов и алгоритм взаимодействия с международными платформами криминалистической разведки сегодня включены в учебные программы по расследованию преступлений против несовершеннолетних — прямой пример трансляции экспертного опыта в образовательный контент.

В сфере противодействия телефонному мошенничеству анализ сетевого трафика позволил выявить незаконный колл-центр в Фергане, использовавший VoIP-технологию Zoiper для хищений у граждан Российской Федерации; установленный ущерб составил 1,8 млн долларов США. Всего ликвидированы три незаконных колл-центра, к ответственности привлечены 34 лица. Отра-

ботанная в ходе этих расследований схема анализа сетевой инфраструктуры и порядок взаимодействия с иностранными правоохранительными органами в рамках международных поручений о правовой помощи легли в основу соответствующего раздела учебного пособия «Противодействие киберпреступности и основы цифровой криминалистики».

Особое методическое значение имеет первое в Центральной Азии извлечение данных из бортового компьютера электромобиля BYD. При расследовании уголовного дела специалисты Института столкнулись с задачей, для которой не существовало готового инструментария. Специализированное программное обеспечение было разработано самими сотрудниками Института; на его основе были получены геолокационные данные и маршруты движения, которые позволили полностью доказать вину подозреваемого. Этот случай наглядно демонстрирует механизм, при котором практическая необходимость порождает научную разработку, а научная разработка немедленно становится объектом учебного модуля в рамках дисциплин Академии.

При расследовании дел, связанных с незаконным оборотом наркотических средств, исследование мобильного устройства подозреваемого позволило проанализировать историю браузера Tor, установить источник приобретения и точки распространения. Методика работы с историей анонимных браузеров в сочетании с геолокационным анализом преподаётся слушателям в формате разбора данного конкретного дела. Аналогичным образом в делах, связанных с финансированием терроризма, отработанная специалистами Института методология установления личностей подозреваемых через открытые источники OSINT и анализ транзакций криптоактивов составила основу соответствующего учебного модуля.

Описанные кейсы были бы изолированными достижениями, если бы Академия не выстроила системные механизмы их устойчивости в образовательном процессе. Эти механизмы реализуются на нескольких взаимосвязанных уровнях.

На уровне высшего профессионального образования с 2025/2026 учебного года в Академии открыта магистратура «Правовое обеспечение кибербезопасности» — первая подобная программа в Узбекистане.

С 2026/2027 учебного года в соответствии с Указом Президента Республики Узбекистан № УП-204 от 3 ноября 2025 года вводится бакалавриат «Киберправо», предусматривающий подготовку по профилям «киберпрокурор» и «киберследователь»[11]. Учебные планы обеих программ формировались с прямым участием экспертов Института, а практические занятия проходят на лабораторной базе Академии — то есть на том самом оборудовании, которое используется в реальных расследованиях.

На уровне дополнительного профессионального образования действует образовательный портал «ProAcademy.uz», объединяющий 52 элективных курса по цифровой криминалистике, киберправу и информационной безопасности. По итогам 2025 года обучение прошли свыше 5000 слушателей — следователи, прокуроры и сотрудники правоохранительных органов со всей республики. Портал включает систему диагностики цифровых компетенций с формированием индивидуальной матрицы и персонализированной образовательной траектории, что позволяет перейти от унифицированного повышения квалификации к компетентностному подходу. Именно этот переход от усвоения нормативных требований к формированию практических умений является сутью модели.

На уровне учебно-методического обеспечения изданы учебное пособие «Квалификация и тактика расследования киберпреступлений», учебник «Цифровая криминалистика», более 20 методических пособий по тематике криптовалют, Darknet и OSINT, завершена работа над пособием «Типология киберпреступлений». По всем регионам ре-

11 Указ Президента Республики Узбекистан № УП-204 «Об утверждении Стратегии "Цифровая прокуратура — 2030" и мерах по ее эффективной реализации» от 3 ноября 2025 г. [Электронный ресурс]. – Режим доступа: https://lex.uz/ru/docs/7813709 (дата обращения: 27.06.2026).

спублики распространён «специальный криминалистический чемодан» для следователей и прокуроров.

Этот инструмент заслуживает отдельного внимания: в нём воплощена сама идея практической трансляции — набор средств обеспечивает побитовое копирование носителей (bit-by-bit imaging), работу с блокировщиком записи (write-blocker), восстановление удалённых файлов с форматированных носителей, обход экранной блокировки персональных компьютеров и изъятие криптоактивов. Иными словами, следователь в любой точке республики получает возможность работать с цифровыми доказательствами по тем же стандартам, что применяются в лабораториях Института — разрыв между центральной экспертизой и периферийной следственной практикой сокращается не только через обучение, но и через унификацию инструментария.

Органическая связь между практикой и обучением имеет ещё одно измерение, которое нередко упускается при анализе образовательных моделей: практика питает не только учебный процесс, но и нормотворческую деятельность. Институтом подготовлено более 30 предложений по совершенствованию законодательства в области цифровых доказательств и расследования киберпреступлений, а также свыше 50 практических рекомендаций, направленных в Генеральную прокуратуру Республики Узбекистан. В стадии согласования находится разработанный при участии Института проект Постановления Пленума Верховного суда Республики Узбекистан о квалификации киберпреступлений. Этот нормотворческий выход закрывает контур, в котором практика расследований выявляет пробелы в праве, Институт формулирует предложения по их устранению, а принятые нормы возвращаются в учебные программы как новое содержание.

В научном отношении в Академии функционирует диссертационный совет по специальностям ВАК 12.00.16 «Правовое обеспечение кибербезопасности» и 12.00.18 «Цифровое право». В рамках инновационного гранта реализуется проект «Единый реестр цифровых доказательств» — межведомственная автоматизированная система централизованного сбора, учёта, хранения и анализа цифровых доказательств, одобренная Постановлением № ПП-229. Зарегистрирован первый в Узбекистане специализированный научный журнал по цифровой криминалистике «Рақамли криминалистика», утверждённый ВАК при Академии наук Республики Узбекистан. Журнал выполняет функцию академической площадки для обмена опытом между практиками и исследователями, завершая тем самым институциональный цикл: практика → методика → норма → наука → практика.

Описанная модель не осталась незамеченной на международном уровне. На 35-м заседании Совета Генеральных прокуроров СНГ Академия номинирована базовой организацией по подготовке кадров в сфере киберпреступности для государств Содружества. Стажировки и обучение в Институте проходят сотрудники из России, Казахстана, Кыргызстана, Таджикистана и Азербайджана, то есть практико-ориентированная модель Академии воспринимается соседними государствами как воспроизводимый образец, а не как уникальный национальный феномен. В мае 2026 года состоялся международный форум Cyberlex-2026 с участием ОБСЕ, UNODC, GIZ, Интерпола и ECTEG, а также делегаций из США, Великобритании, Японии, Республики Корея, Молдовы, Казахстана и ряда других государств, что свидетельствует о признании Ташкента в качестве площадки регионального уровня для обсуждения вопросов противодействия киберпреступности и цифровой криминалистики.

В 2026 году Академия вошла в топ-100 международного рейтинга WURI (World University Rankings for Innovation) по направлению «Industrial Application» — международное признание именно практической составляющей научно-образовательной деятельности.

Проведённый анализ позволяет сформулировать несколько выводов, имеющих как теоретическое, так и практическое значение.

Избранная Правоохранительной академией модель практико-ориентированной под-

готовки кадров основана на принципе, который можно назвать институциональным замыканием цикла, где экспертная практика порождает методику, методика становится учебным содержанием, учебное содержание возвращается в практику через подготовленных специалистов. Этот цикл не может быть воспроизведён в условиях организационного разделения экспертных учреждений и образовательных структур.

Нормативная база, складывавшаяся последовательно с 2022 по 2026 год, свидетельствует о том, что данная модель является результатом целенаправленной государственной политики, а не случайным организационным решением. Создание Научно-исследовательского института цифровой криминалистики в структуре Академии стало не точкой отсчёта, а закономерным этапом в развитии этой политики.

Опыт Правоохранительной академии имеет значение, выходящее за рамки Узбекистана. Государства Центральноазиатского региона, перед которыми стоят аналогичные задачи в сфере цифровой криминалистики, располагают сегодня работающим прецедентом институционального строительства, апробированным в условиях реальной правоохранительной практики и получившим международное признание.

#

Хагани ГАДЖИЕВ,
Начальник Специализированного центра цифровых исследований Научно-исследовательского института цифровой криминалистики Правоохранительной академии Республики Узбекистан, доктор философии по юридическим наукам (PhD)

ЦИФРОВАЯ КРИМИНАЛИСТИКА В ПРАВООХРАНИТЕЛЬНОЙ ПРАКТИКЕ РЕСПУБЛИКИ МОЛДОВА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ОПЫТА В РЕСПУБЛИКЕ УЗБЕКИСТАН

АННОТАЦИЯ. *В данной статье представлено комплексное исследование состояния и перспектив развития цифровой криминалистики в правоохранительной системе Республики Молдова с позиции возможного применения данного опыта в Республике Узбекистан. На основе анализа нормативно-правового регулирования, организационной структуры и технического обеспечения криминалистических подразделений исследуется процесс международной аккредитации лабораторий цифровой криминалистики по стандарту ISO/IEC 17025 и его влияние на эффективность противодействия киберпреступности. Проводится сравнительный анализ с ситуацией в Узбекистане, выявляются ключевые проблемы и определяются перспективные направления развития данной сферы в контексте евразийской интеграции и цифровизации правоохранительных систем.*

ANNOTATSIYA. *Ushbu maqolada Moldova Respublikasi huquqni muhofaza qilish tizimida raqamli kriminalistikaning holati va rivojlanish istiqbollarini O‘zbekiston Respublikasida ushbu tajribani qo‘llash imkoniyatlari nuqtayi nazaridan kompleks tadqiqoti taqdim etilgan. Normativ-huquqiy tartibga solish, kriminalistik bo‘linmalarning tashkiliy tuzilishi va texnik ta’minoti tahlili asosida raqamli kriminalistika laboratoriyalarining ISO/IEC 17025 standarti bo‘yicha xalqaro akkreditatsiyasi jarayoni va uning kiberjinoyatchilikka qarshi kurashish samaradorligiga ta’siri o‘rganildi. O‘zbekistondagi vaziyat bilan qiyosiy tahlil o‘tkazilib, asosiy muammolar aniqlanmoqda va Yevroosiyo integratsiyasi va huquqni muhofaza qilish tizimlarining raqamlashtirilishi kontekstida ushbu sohani rivojlantirishning istiqbolli yo‘nalishlari belgilanmoqda.*

ABSTRACT. *This article presents a comprehensive study of the state and development prospects of digital forensics in the law enforcement system of the Republic of Moldova from the perspective of possible application of this experience in the Republic of Uzbekistan. Based on the analysis of legal regulations, organizational structure, and technical support of forensic units, the process of international accreditation of digital forensics laboratories according to the ISO/IEC 17025 standard and its impact on the effectiveness of combating cybercrime is examined. A comparative analysis with the situation in Uzbekistan is conducted, key problems are identified, and promising directions for the development of this field are determined in the context of Eurasian integration and digitalization of law enforcement systems.*

Ключевые слова: *цифровая криминалистика, киберпреступность, цифровые доказательства, ISO/IEC 17025, международная аккредитация, правоохранительная деятельность.*

Kalit so‘zlar: *raqamli kriminalistika, kiberjinoyatchilik, raqamli dalillar, ISO/IEC 17025, xalqaro akkreditatsiya, huquqni muhofaza qilish faoliyati.*

Key words: *digital forensics, cybercrime, digital evidence, ISO/IEC 17025, international accreditation, law enforcement.*

ВВЕДЕНИЕ (INTRODUCTION)

Глобальная цифровая трансформация общественных отношений фундаментально изменила характер преступной деятельности, которая все активнее переходит в виртуальное пространство. Киберпреступления представляют серьезную угрозу национальной безопасности, экономической стабильности и правам граждан как в Республике Молдова[1], так и в Республике Узбекистан. Данная тенденция объективно требует адекватного ответа со стороны правоохранительных систем посредством развития специализированного направления – цифровой криминалистики.

Цифровая криминалистика представляет собой систему научно обоснованных методов обнаружения, фиксации, изъятия, со-

1 Постановление Парламента Республики Молдова № HP391/2023 "Стратегия национальной безопасности Республики Молдова" от 15. декабря 2023 г. – [Электронный ресурс]. – Режим доступа: https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023_Ru.pdf. – Дата доступа: 27.10.2025г.

хранения и анализа цифровых данных для их последующего использования в качестве доказательств[2]. Особую актуальность данное направление приобретает для Республики Молдова и Республики Узбекистан, где процессы информатизации общества развиваются ускоренными темпами, требуя соответствующего развития правоохранительных механизмов.

Выбор Республики Молдова в качестве объекта исследования обусловлен несколькими факторами. Во-первых, данное государство демонстрирует системный подход к развитию цифровой криминалистики, включая нормативно-правовое регулирование, организационную структуру и техническое оснащение.

Во-вторых, международная аккредитация лабораторий цифровой криминалистики Молдовы по стандарту ISO/IEC 17025 представляет особый интерес в контексте стремления Узбекистана к повышению качества криминалистических исследований.

В-третьих, как Молдова, так и Узбекистан являются постсоветскими государствами со схожими правовыми системами, что позволяет эффективно адаптировать положительный опыт.

Актуальность исследования обусловлена комплексом взаимосвязанных факторов, подтверждаемых объективными статистическими данными. Официальная статистика демонстрирует не только устойчивую тенденцию роста числа киберпреступлений, но и их структурную трансформацию в общем массиве правонарушений. Так, в Республике Узбекистан наблюдается стремительный рост доли киберпреступлений в общей структуре преступности: если в 2023 году они составляли лишь 7,2 % от общего количества правонарушений, то в 2024 году данный показатель вырос до 45 %, сохранив аналогичную пропорцию (45 %) в 2025 году[3].

В Республике Молдова ситуация не менее тревожная – в 2024 году зарегистрировано более 10000 киберпреступлений, что обусловило 15-е место страны в мировом рейтинге киберпреступности согласно Всемирному индексу 2025 года (из 97 оцениваемых государств).

Стратегия «Цифровой Узбекистан-2030» и процесс европейской интеграции Молдовы, в свою очередь, детерминируют необходимость системного совершенствования правоохранительных механизмов в соответствии с международными стандартами. Динамичное развитие информационных технологий и их криминальное использование предъявляют качественно новые требования к техническому оснащению и методическому обеспечению правоохранительных органов обеих стран. Данные обстоятельства обусловливают необходимость комплексного научного анализа передового опыта в сфере цифровой криминалистики с целью его возможной адаптации в национальных правоохранительных системах.

Присоединение Молдовы к Будапештской конвенции о киберпреступности[4] стало важнейшим шагом в развитии национальной системы противодействия киберпреступности, обязав государство имплементировать нормы, регламентирующие процедуры работы с цифровыми доказательствами. Узбекистан, хотя и не является участником данной Конвенции, активно изучает международный опыт для совершенствования собственного законодательства в данной сфере.

Подтверждением этого служит принятие Закона Республики Узбекистан № ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами» от 21.11.2024 года, который знаменует существенный прогресс в нормативном регулировании процедур по-

2 Casey E. Digital evidence and computer crime: Forensic science, computers, and the internet. – Academic press, 2011.

3 Ущерб от киберпреступлений в 2021–2024 годах в Узбекистане превысил 1,9 трлн сумов [Электронный ресурс]: Режим доступа: https://www.gazeta.uz/ru/2025/05/29/cybercrime/. – Дата доступа: 27.10.2025 г.

4 Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) – [Электронный ресурс]. – Режим доступа: https://rm.coe.int/1680081580. – Дата доступа: 27.10.2025 г.

лучения, хранения и использования цифровых доказательств в уголовном процессе.

Целью настоящего исследования является комплексный анализ современного состояния и перспективных направлений развития цифровой криминалистики в правоохранительной практике Республики Молдова для возможного применения данного опыта в Республике Узбекистан. Для достижения указанной цели поставлены следующие задачи: проанализировать нормативно-правовую базу цифровой криминалистики в Молдове в сравнении с национальным законодательством, исследовать организационную структуру специализированных подразделений, изучить процесс международной аккредитации лабораторий цифровой криминалистики, оценить уровень технического оснащения, проанализировать международное сотрудничество в сфере цифровой криминалистики, выявить проблемные аспекты и определить перспективные направления совершенствования данной сферы в обеих странах.

МЕТОДЫ (METHODS)

Методологической основой исследования является комплекс взаимодополняющих общенаучных и частных методов, обеспечивающих объективность и достоверность результатов. Системно-структурный подход позволил рассмотреть цифровую криминалистику как комплексное явление, включающее взаимосвязанные элементы: нормативно-правовую базу, организационную структуру, техническое оснащение и методическое обеспечение. Данный подход особенно важен при сравнительном анализе систем цифровой криминалистики Молдовы и Узбекистана, имеющих различную степень развития.

Сравнительно-правовой метод применялся при сопоставлении законодательства Молдовы и Узбекистана с международными стандартами в сфере цифровой криминалистики. Это позволило выявить сходства и различия в правовом регулировании, определить степень гармонизации национальных нормативных актов с международными нормами и идентифицировать области, требующие дальнейшего совершенствования.

Формально-юридический метод использовался при анализе нормативных актов, регламентирующих деятельность в сфере цифровой криминалистики. Этот метод обеспечил точность юридических формулировок и корректность интерпретации правовых норм, что особенно важно при исследовании законодательства разных стран.

Историко-правовой метод позволил проследить эволюцию развития цифровой криминалистики в Республике Молдова и Республике Узбекистан, выявить закономерности и тенденции этого развития, что имеет существенное значение для прогнозирования дальнейших перспектив.

Статистический метод применялся при обработке и анализе количественных показателей, характеризующих состояние киберпреступности и эффективность деятельности подразделений цифровой криминалистики в обеих странах, что позволило сформировать объективное представление о масштабе проблемы и результативности принимаемых мер.

Метод экспертной оценки использовался при анализе качественных характеристик технического оснащения и методического обеспечения цифровой криминалистики в Молдове и Узбекистане, что обеспечило достоверность выводов относительно практических аспектов функционирования соответствующих систем.

Прогностический метод применялся для определения перспективных направлений развития цифровой криминалистики в обеих странах с учетом выявленных тенденций, проблемных аспектов и международного опыта.

Эмпирическую базу исследования составили: нормативно-правовые акты Республики Молдова и Республики Узбекистан, международные документы (Будапештская конвенция, стандарты ISO/IEC), научные публикации, статистические данные, материалы официальных сайтов правоохранительных органов обеих стран, отчеты международных организаций. Данная методологическая основа обеспечила всестороннее и объективное изучение предмета исследования.

РЕЗУЛЬТАТЫ (RESULTS)

Нормативно-правовые основы цифровой криминалистики

Правовой фундамент цифровой криминалистики в Республике Молдова формируется многоуровневой системой нормативных актов. Фундаментальное значение имеет Конвенция о киберпреступности (Будапештская конвенция)[5], которая обязала Молдову имплементировать положения о работе с цифровыми доказательствами. В Узбекистане, не являющемся участником данной Конвенции, правовая основа представлена несколькими ключевыми актами:

Законом Республики Узбекистан №ЗРУ-764 «О кибербезопасности» от 15 апреля 2022 года[6];

Законом Республики Узбекистан №ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами» от 21.11.2024 года, который существенно расширил правовое регулирование вопросов цифровой криминалистики, в частности, процедур получения, исследования и использования цифровых доказательств[7].

На национальном уровне в Молдове ключевую роль играет Закон «О судебной экспертизе и статусе судебного эксперта» № 68 от 14.04.2016[8], регламентирующий организационные и процессуальные аспекты экспертиз, включая цифровые. В Узбекистане аналогичные вопросы регулируются Законом Республики Узбекистан № ЗРУ-249 «О судебной экспертизе» от 1 июня 2010 года[9], который, однако, содержит лишь общие положения без специфических норм относительно цифровых экспертиз. Это создает определенные правовые пробелы в регулировании процедур сбора и исследования цифровых доказательств.

Уголовно-процессуальный кодекс Молдовы[10] содержит детализированные положения о процедурах сбора, фиксации и использования цифровых доказательств, в то время как УПК Узбекистана[11], хотя и оперирует понятием цифровых доказательств, но не регламентирует конкретные процессуальные механизмы и методики работы с ними, что создает определенные правоприменительные сложности при документировании киберпреступлений.

Положение о Центре технико-криминалистических и судебных экспертиз (ЦТКСЭ) Молдовы[12] создало организационно-правовую основу функционирования специализированных подразделений цифровой криминалистики. В Узбекистане аналогичные функции регламентируются Положением о Республиканском центре судебной экспертизы имени Х. Сулаймоновой и Положением о Главном экспертно-криминалистическом центре МВД Республики Узбекистан, которые, однако, имеют единичные лаборатории цифровой криминалистики в отличие от молдавской модели в которой присутствуют целые дирекции по линии циф-

5 Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) – [Электронный ресурс]. – Режим доступа: https://rm.coe.int/1680081580. – Дата доступа: 27.10.2025 г.

6 Закон Республики Узбекистан №ЗРУ-764 «О кибербезопасности» от 15 апреля 2022 года – [Электронный ресурс]. – Режим доступа: https://lex.uz/ru/docs/5960609. – Дата доступа: 28.10.2025 г.

7 Закон Республики Узбекистан №ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами» от 21.11.2024 года – [Электронный ресурс]. – Режим доступа: https://lex.uz/ru/docs/7228823. – Дата доступа: 29.10.2025 г.

8 Закон Республики Молдова № 68 «О судебной экспертизе и статусе судебного эксперта» от 14.04.2016 – [Электронный ресурс]. – Режим доступа: https://www.legis.md/cautare/getResults?doc_id=106005&lang=ro. – Дата доступа: 29.10.2025 г.

9 Закон Республики Узбекистан № ЗРУ-249 «О судебной экспертизе» от 1 июня 2010 года – [Электронный ресурс]. – Режим доступа: https://www.lex.uz/acts/1633100. – Дата доступа: 28.10.2025 г.

10 Уголовно-процессуальный кодекс Республики Молдова № 122 от 14.03.2003 // Monitorul Oficial al Republicii Moldova. – 2003 г. – № 104-110. – Ст. 447.

11 Уголовно-процессуальный кодекс Республики Узбекистан от 22 сентября 1994 года // Национальная база данных законодательства, 21.09.2024 г., № 03/24/963/0735.

12 Положение о Центре технико-криминалистических и судебных экспертиз Генерального инспектората полиции, утвержденное Постановлением Правительства Республики Молдова № 1033 от 16.12.2013 // Monitorul Oficial al Republicii Moldova. – 2013 г. – № 304-310.

ровых экспертиз.

Важным шагом в развитии нормативной базы Молдовы стало принятие Постановления Правительства «О мерах по реализации Закона о судебной экспертизе и статусе судебного эксперта»[13], установившего требования к аккредитации экспертных учреждений в соответствии со стандартом ISO/IEC 17025. В Узбекистане процесс международной аккредитации экспертных учреждений находится на начальной стадии, что создает перспективу для изучения и адаптации молдавского опыта.

Как отмечает О.А. Зайцев[14], в законодательстве Молдовы сохраняются пробелы в отношении регламентации новейших технологий цифровой криминалистики. Аналогичную проблему для Узбекистана отмечает Х.Гаджиев[15], указывая на необходимость совершенствования нормативной базы с учетом международных стандартов и передового опыта.

Центральным звеном в системе цифровой криминалистики Молдовы является Центр технико-криминалистических и судебных экспертиз при Генеральном инспекторате полиции. В его структуре функционирует Дирекция экспертизы информационных средств, включающая Секцию информационных экспертиз, которая непосредственно осуществляет экспертизы в области цифровой криминалистики[16].

В Узбекистане аналогичные функции распределены между несколькими ведомствами. Главный экспертно-криминалистический центр МВД Узбекистана имеет отдел цифровых экспертиз, В Республиканском центре судебных экспертиз имени Х. Сулаймоновой функционирует отдел судебной компьютерно-технической экспертизы, в соответствии с постановлением Президента Республики Узбекистан №ПП-229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики» от 21 июня 2024 г., в Правоохранительной академии образован Научно-исследовательский институт цифровой криминалистики одной из основных задач которого является проведение судебные экспертизы и исследования по цифровой криминалистике однако их организационная структура и функциональные возможности существенно отличаются от молдавской модели. ГУП «Центр кибербезопасности Узбекистана» также выполняет судебные экспертизы в сфере цифровой криминалистики[17].

Миссия ЦТКСЭ Молдовы заключается в реализации полномочий Генерального инспектората полиции в сфере предупреждения и борьбы с преступностью. В контексте цифровой криминалистики это предполагает не только реактивное реагирование на совершенные киберпреступления, но и проактивную деятельность по предупреждению и раннему выявлению потенциальных киберугроз. В Узбекистане функционирует развитая система специализированных подразделений, занимающихся как расследованием киберпреступлений, так и проведением судебных экспертиз в сфере цифровой криминалистики. Ключевое отличие заключается в организационной модели: в Молдове преобладает централизованный подход с единым координирующим центром, в то время как узбекистанская модель характеризуется более диверсифицированной структурой с распределением функций между различными ведомственными под-

13 Закон Республики Молдова № 68 «О судебной экспертизе и статусе судебного эксперта» от 14 апреля 2016 года // Monitorul Oficial al Republicii Moldova. – 2017. – № 92-102.

14 Зайцев О.А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства //Журнал зарубежного законодательства и сравнительного правоведения. – 2019 г. – №. 4. – С. 42-57.

15 Гаджиев Х.М., Югай Л.Ю. Методика компьютерно-технической экспертизы по преступлениям в сфере цифровых технологий // Противодействие правонарушениям в сфере цифровых технологий и вопросы организационно-правового обеспечения информационной безопасности. – 2022 г. – №1 (1). – С. 68-76

16 Официальный сайт Центра технико-криминалистических и судебных экспертиз Генерального инспектората полиции Республики Молдова [Электронный ресурс]. – Режим доступа: https://ctcej.politia.md/ro

17 Постановление Президента Республики Узбекистан №ПП-229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики» от 21 июня 2024 г. [Электронный ресурс] – Режим доступа: https://lex.uz/ru/docs/6977762– Дата доступа: 29.10.2025 г.

разделениями, что имеет как свои преимущества (специализация), так и недостатки (потенциальное дублирование полномочий).

Секция информационных экспертиз ЦТКСЭ Молдовы выполняет широкий спектр функций, включая экспертизы компьютерной техники и мобильных устройств, восстановление удаленных данных, анализ программного обеспечения, выявление следов несанкционированного доступа[18].

В Узбекистане реализована более специализированная модель, при которой данные функции распределены между профильными экспертными подразделениями различных ведомств, что обеспечивает углубленную специализацию экспертов, повышенную точность и достоверность результатов исследований. Такая организационная структура позволяет экспертным подразделениям эффективно решать сложные задачи в области цифровой криминалистики, нередко достигая более высоких результатов за счет концентрации ресурсов на узкоспециализированных направлениях.

В Молдове для обеспечения территориальной доступности экспертных услуг, помимо центрального аппарата, функционируют территориальные центры Аналогичный подход применяется в Узбекистане, где экспертно-криминалистические подразделения имеются во всех региональных управлениях МВД, при этом их техническое оснащение для проведения цифровых экспертиз находится в процессе планомерной модернизации в соответствии с динамично развивающимися технологическими стандартами и современными требованиями цифровой криминалистики.

Важным аспектом организации деятельности подразделений цифровой криминалистики в Молдове является внедрение системы менеджмента качества, соответствующей стандарту ISO/IEC 17025, что обеспечивает достоверность результатов экспертиз и их международное признание. В Узбекистане множество лабораторий по традиционным видам судебных экспертиз уже успешно функционируют с внедренными и сертифицированными системами менеджмента качества, однако специализированные лаборатории цифровых экспертиз находятся в процессе подготовки к внедрению данного стандарта. Планомерная и целенаправленная работа в этом направлении активно ведется с учетом как международного опыта, так и национальных особенностей организации экспертно-криминалистической деятельности.

Ключевым событием в развитии цифровой криминалистики в Молдове стала аккредитация ЦТКСЭ по стандарту ISO/IEC 17025. В 2018 году Центр получил сертификат аккредитации от Национального центра по аккредитации "МОЛДАК", подтверждающий соответствие международным требованиям к компетентности испытательных лабораторий. ЦТКСЭ получил аккредитацию по шести направлениям, включая цифровую криминалистику[19].

Процесс подготовки к аккредитации начался за шесть лет до ее получения с подписания соглашения с Правительством США и продолжился в рамках проекта "Поддержка реформы полиции в Республике Молдова", реализуемого ПРООН. В рамках подготовки ЦТКСЭ получил международную консультативную поддержку по разработке системы менеджмента качества, криминалистические лаборатории были оснащены современным оборудованием, а сотрудники прошли специализированное обучение.

В Узбекистане процесс международной аккредитации экспертных учреждений ответственных за производство судебных экспертиз в сфере цифровой криминалистики находится на начальной стадии. Как отмечает Л.Ю. Югай, внедрение международных стандартов качества в деятельность экспертно-криминалистических подразделений Узбекистана является одним из приоритетных направлений развития. В этом контексте опыт Молдовы представляет зна-

18 Официальный сайт Центра технико-криминалистических и судебных экспертиз Генерального инспектората полиции Республики Молдова [Электронный ресурс]. – Режим доступа: https://ctcej.politia.md/ro

19 Centrul tehnico-criminalistic şi expertize judiciare a fost dotat cu echipament performant oferit de UE [Электронный ресурс]. – Режим доступа: https://moldova.md/ro/content/centrul-tehnico-criminalistic-si-expertize-judiciare-fost-dotat-cu-echipament-performant.

чительный интерес, особенно в части подготовки к аккредитации и внедрения системы менеджмента качества[20].

Аккредитация обеспечивает повышение доверия к результатам экспертиз, стандартизацию процедур обработки цифровых доказательств, расширение возможностей международного сотрудничества и признание результатов экспертиз в международных судебных инстанциях. Это особенно важно в условиях транснационального характера многих киберпреступлений, затрагивающих интересы нескольких государств.

Благодаря поддержке международных партнеров, ЦТКСЭ Молдовы получил современное оборудование для проведения цифровых экспертиз. В 2017 году Европейский Союз предоставил специализированное оборудование для лабораторий цифровой криминалистики[21], а в 2018 году с помощью ПРООН и правительства США Дирекция экспертизы информационных средств получила высокопроизводительный компьютер, сокративший время анализа цифровых устройств с 24 часов до примерно одного часа.

В Узбекистане техническое оснащение подразделений цифровой криминалистики также развивается с международной поддержкой, однако существуют значительные различия в уровне оснащения центральных и региональных подразделений. Как отмечает Л.Ю. Югай, модернизация технического оснащения является одним из приоритетов развития экспертно-криминалистических подразделений Узбекистана[22].

Важным шагом в развитии технических возможностей Молдовы стало вступление ЦТКСЭ в 2023 году в Европейскую сеть институтов судебной экспертизы (ENFSI) и создание специализированной лаборатории для расследования киберпреступлений при поддержке ЕС[23].

Узбекистан также активно развивает международное сотрудничество в данной сфере, но в иных региональных форматах. Значимым достижением стало присоединение Узбекистана к Азиатской сети судебных экспертиз (Asian Forensic Sciences Network), что открыло доступ к обширному региональному опыту, технологическим стандартам и методикам, применяемым в странах Азиатско-Тихоокеанского региона, а также создало платформу для профессионального обмена и повышения квалификации экспертов[24].

Методики цифровой криминалистики, применяемые в Молдове, основываются на международных стандартах ISO/IEC 27037:2012 и ISO/IEC 27041:2015[25]. Процесс цифровой экспертизы включает последовательные этапы: идентификацию, сбор, сохранение, анализ и отчетность. В Узбекистане функционирует комплексная система методического обеспечения цифровой криминалистики, формализованная в Государственном реестре судебных экспертиз. Данный реестр содержит детально разработанные и официально утвержденные методики проведения различных видов цифровых исследований, включая компьютерно-техническую экспертизу, экспертизу мобильных устройств, аналитику больших данных (Big Data) и другие актуальные направления. Такая системная методологическая база обеспечивает высокое качество и юридическую обоснованность проводимых экспертиз, а также способствует единообра-

20 Югай Л.Ю., Гаджиев Х.М. Использование цифровой экспертизы при доказывании факта распространения ложной информации в интернете // Юрист ахборотномаси. – Вестник юриста. – Lawyer herald. – № 1 (2021). – С. 208-218.

21 Forensic and Judicial Expertise Centre (CTCEJ), Chisinau [Электронный ресурс] // European Network of Forensic Science Institutes. – URL: https://enfsi.eu/member/forensic-and-judicial-expertise-centre-ctcej-chisinau/ (дата обращения: 28.10.2025).

22 Югай Л.Ю., Гаджиев Х.М. Использование цифровой экспертизы при доказывании факта распространения ложной информации в интернете // Юрист ахборотномаси. – Вестник юриста. – Lawyer herald. – № 1 (2021). – С. 208-218.

23 Forensic and Judicial Expertise Centre (CTCEJ), Chisinau [Электронный ресурс]. – Режим доступа: https://enfsi.eu/member/forensic-and-judicial-expertise-centre-ctcej-chisinau/

24 Sud ekspertlik faoliyatining rivojida xalqaro sud ekspertiza tashkilotlarning o'rni – [Электронный ресурс]. – Режим доступа: https://sudex.uz/?p=7090. – Дата доступа: 28.10.2025 г.

25 ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence // International Organization for Standardization. – 2012.

зию экспертной практики на всей территории страны.

Международное сотрудничество играет ключевую роль в развитии цифровой криминалистики как в Молдове, так и в Узбекистане. Основными партнерами Молдовы выступают Европейский Союз, США, ПРООН, ENFSI и CEPOL[26]. Узбекистан развивает сотрудничество с Россией, Китаем, странами Центральной Азии, а также с международными организациями, включая ОБСЕ и ШОС.

Сотрудничество осуществляется по нескольким направлениям: техническая помощь, обучение и повышение квалификации специалистов, консультативная помощь при разработке нормативных актов и стандартов, обмен информацией о киберугрозах, участие в международных проектах. Особое значение для Молдовы имеет сотрудничество в рамках имплементации Будапештской конвенции о киберпреступности, в то время как Узбекистан развивает сотрудничество в рамках региональных организаций, включая ШОС и СНГ.

Важным аспектом является гармонизация законодательства с международными стандартами, что облегчает сотрудничество с зарубежными партнерами и повышает эффективность борьбы с киберпреступностью. В этом контексте опыт Молдовы по имплементации международных стандартов представляет значительный интерес для Узбекистана.

ОБСУЖДЕНИЕ (DISCUSSION)

Проблемы развития цифровой криминалистики в Молдове и Узбекистане.

Сравнительный анализ систем цифровой криминалистики Молдовы и Узбекистана позволил выявить общие и специфические проблемы. Ключевой проблемой для обеих стран является ограниченность кадрового потенциала – дефицит высококвалифицированных специалистов, особенно в региональных подразделениях. В Молдове, как отмечает Чеботарь А.С.[27], это связано с недостаточной подготовкой специалистов в вузах и оттоком кадров в частный сектор. Аналогичные проблемы характерны и для Узбекистана.

Финансовые ограничения затрудняют своевременное обновление технического оснащения в обеих странах, что особенно критично в области, где технологии развиваются стремительно. Зависимость от международной помощи создает риски для устойчивого развития в долгосрочной перспективе.

А.С. Чеботарь указывает на пробелы в нормативно-правовом регулировании цифровой криминалистики в Молдове, что характерно и для Узбекистана. Отсутствие четкой регламентации процедур работы с данными в облачных сервисах и виртуальных средах затрудняет сбор и использование цифровых доказательств в судебном процессе.

Технологические вызовы связаны с постоянным совершенствованием методов киберпреступлений. Преступники используют современные технологии шифрования и анонимизации, что затрудняет экспертную работу в обеих странах. В Молдове вопросы координации между различными правоохранительными органами при расследовании киберпреступлений решаются относительно эффективно благодаря централизованной организационной структуре и сравнительно небольшой территории страны.

В Узбекистане для преодоления координационных барьеров и оптимизации работы с цифровыми доказательствами разрабатывается и внедряется инновационная межведомственная автоматизированная система «Единый реестр цифровых доказательств». Данный реестр призван решать комплекс стратегических задач:

26 Совместная декларация по итогам 8-го заседания совета ассоциации республики молдова - европейского союза – [Электронный ресурс]. – Режим доступа: https://old.gov.md/ru/content/sovmestnaya-deklaraciya-po-itogam-8-go-zasedaniya-soveta-associacii-respubliki-moldova. – Дата доступа: 28.10.2025г.

27 Чеботарь А.С. О современных тенденциях преступлений, совершенных посредством использования информационно-телекоммуникационных технологий или в сфере компьютерной информации в Российской Федерации //Вестник ВГУ. Серия: Право. – 2024 г. – №. 2. – С. 294-300.

централизованный сбор, учет, хранение и исследование поступающих из правоохранительных органов материалов по уголовным делам цифровых данных, обеспечение надежных механизмов хранения, обработки, защиты данных. Внедрение данной системы представляет собой качественно новый подход к обеспечению межведомственного взаимодействия в сфере цифровой криминалистики, значительно повышающий эффективность расследования киберпреступлений.

На основе выявленных проблем и сравнительного анализа определены следующие перспективные направления развития цифровой криминалистики в Молдове и Узбекистане:

1. Совершенствование нормативно-правовой базы – для Молдовы это дальнейшая гармонизация законодательства с европейскими стандартами, для Узбекистана – разработка комплексного законодательства в сфере цифровой криминалистики с учетом международного опыта, включая опыт Молдовы по имплементации стандартов Будапештской конвенции.

2. Развитие кадрового потенциала – создание системы подготовки и повышения квалификации специалистов, включая специализированные образовательные программы. Узбекистан может адаптировать молдавский опыт с учетом национальной специфики системы образования.

3. Техническая модернизация – для обеих стран актуально регулярное обновление оборудования и программного обеспечения, внедрение новых технологий для автоматизации процессов анализа цифровых данных. Узбекистан может изучить опыт Молдовы по привлечению международной технической помощи.

4. Организационное совершенствование – для Узбекистана перспективным является создание централизованной структуры по образцу ЦТКСЭ Молдовы, что позволит оптимизировать ресурсы и повысить эффективность экспертной деятельности.

5. Международная аккредитация – опыт Молдовы по подготовке и прохождению аккредитации по стандарту ISO/IEC 17025 представляет особую ценность для Узбекистана, планирующего аналогичный процесс.

6. Укрепление международного сотрудничества – для обеих стран важно расширение участия в международных проектах и развитие механизмов оперативного обмена информацией, хотя и в разных региональных форматах.

7. Совершенствование методического обеспечения – для Узбекистана особенно актуальна адаптация международных стандартов и методик цифровой криминалистики, успешно внедренных в Молдове.

8. Улучшение межведомственного взаимодействия – создание эффективных механизмов координации между правоохранительными органами, формирование межведомственных рабочих групп и единых протоколов обмена информацией.

Реализация указанных направлений требует комплексного подхода и координации усилий всех заинтересованных сторон, с учетом национальных особенностей и международного опыта.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволяет сделать вывод о том, что цифровая криминалистика в Республике Молдова демонстрирует системное развитие, обусловленное как внутренними потребностями правоохранительной системы, так и процессом европейской интеграции. Достигнутые результаты включают формирование нормативно-правовой базы, создание централизованной организационной структуры с ЦТКСЭ в качестве ключевого элемента, проведение международной аккредитации по стандарту ISO/IEC 17025, модернизацию технического оснащения и развитие международного сотрудничества.

В Республике Узбекистан развитие цифровой криминалистики находится на другой стадии, характеризующейся формированием нормативной базы, совершенствованием организационной структуры и начальным этапом международной аккредитации. При этом опыт Молдовы представляет значительный интерес для Узбекистана с точки зрения возможной адап-

тации, особенно в части организационной структуры, международной аккредитации и методического обеспечения.

Выявленные проблемы развития цифровой криминалистики в обеих странах (ограниченность кадрового потенциала, финансовые ограничения, нормативно-правовые пробелы, технологические вызовы) имеют как общий характер, так и специфические особенности, обусловленные национальным контекстом. Определенные перспективные направления развития предполагают комплексный подход, включающий совершенствование законодательства, развитие кадрового потенциала, техническую модернизацию и укрепление международного сотрудничества.

Адаптация опыта Молдовы в условиях Узбекистана требует учета национальных особенностей правовой системы, организационной структуры правоохранительных органов и региональных форматов международного сотрудничества. При этом базовые принципы и подходы, успешно реализованные в Молдове, могут быть эффективно применены в Узбекистане с соответствующей адаптацией.

В целом, проведенное исследование демонстрирует значительный потенциал международного обмена опытом в сфере цифровой криминалистики и перспективность адаптации успешных практик с учетом национальных особенностей, что способствует повышению эффективности борьбы с киберпреступностью, обеспечению защиты прав граждан в цифровом обществе.

#

Lyudmila YUGAY,
Law Enforcement Academy of the Republic of Uzbekistan,
Scientific Research Institute of Digital Forensics,
Head of Methodological support division, DSc., Associate Professor

LEGAL REGULATION OF DEEPFAKE USE: INTERNATIONAL AND NATIONAL EXPERIENCE

ABSTRACT. *The article provides a comprehensive analysis of the experience of foreign countries and the Republic of Uzbekistan in regulating the use of deepfake technologies. The author substantiates the issue's relevance in light of the growing cybercrime rate and the increasing number of unlawful cases involving the distribution of synthetic audio and video content capable of causing economic, political, reputational, and moral harm to individuals and the state. The study covers the regulatory approaches of the United States, the European Union, China, Singapore, Australia, the CIS countries, and other states. Special attention is given to current initiatives and legislative processes in the Republic of Uzbekistan, including the review of draft laws. Based on the study's results, practical recommendations are proposed to improve national legislation.*

ANNOTATSIYA. *Maqola xorijiy mamlakatlar va O'zbekiston Respublikasining "deepfake" texnologiyalaridan foydalanishni tartibga solish sohasidagi tajribasini kompleks tahlil qilishga bag'ishlangan. Muallif tomonidan kiberjinoyatchilikning o'sishi, fuqarolar va davlatga iqtisodiy, siyosiy, obro'-e'tibor va ma'naviy zarar yetkazishi mumkin bo'lgan sintetik audio va video kontentni tarqatishning noqonuniy holatlari ko'payishi bilan bog'liq muammoning dolzarbligi asoslab berilgan. Tadqiqotda AQSH, Yevropa Ittifoqi, Xitoy, Singapur, Avstraliya, MDH va boshqa davlatlarning me'yoriy yondashuvlari qamrab olingan. O'zbekiston Respublikasidagi zamonaviy tashabbuslar va qonunchilik jarayonlariga, shu jumladan, qonun loyihalarini ko'rib chiqishga alohida e'tibor qaratildi. Tadqiqot yakunida milliy qonunchilikni takomillashtirish bo'yicha amaliy tavsiyalar shakllantirilgan.*

АННОТАЦИЯ. *Статья посвящена комплексному анализу опыта зарубежных стран и Республики Узбекистан в сфере регулирования использования технологий дипфейков. Автором обоснована актуальность проблемы в связи с ростом киберпреступности и увеличением числа противоправных случаев распространения синтетического аудио- и видео-контента, способного причинять экономический, политический, репутационный и моральный ущерб гражданам и государству. Исследование охватывает нормативные подходы США, Европейского Союза, Китая, Сингапура, Австралии, стран СНГ и других государств. Особое внимание уделено современным инициативам и законодательным процессам в Республике Узбекистан, включая рассмотрение законопроектов. По итогам исследования сформулированы практические рекомендации по совершенствованию национального законодательства.*

Key words: *artificial intelligence, cybercrime, disinformation, digital rights, personal data, online platforms, content labeling, liability for deepfakes.*

Kalit so'zlar: *sun'iy intellekt, kiberjinoyatchilik, dezinformatsiya, raqamli huquqlar, shaxsiy ma'lumotlar, onlayn platformalar, kontentni belgilash, "deepfake" uchun javobgarlik.*

Ключевые слова: *искусственный интеллект, киберпреступность, дезинформация, цифровые права, персональные данные, онлайн-платформы, маркировка контента, ответственность за дипфейки.*

Introduction. Article 31 of the renewed Constitution of the Republic of Uzbekistan, for the first time, established the right of everyone to the protection of their personal data. Article 33 further defines the state's obligation to create conditions that ensure access to the global information network, the Internet, which has significantly expanded and strengthened citizens' digital rights[1].

It should be noted that the transition of all spheres of public life into the digital domain, on the one hand, introduces positive opportunities, such as remote access to banking, governmental, medical, and other services, saving time, broadening access to public services, and minimizing corruption risks. On the other hand, it has led to an increase in personal data leaks, as information stored in databases may be altered, while the risks of cybercrime and related threats are growing.

In the Republic of Uzbekistan, more than 12 million cyberattack attempts were recorded in 2024, compared to about 11 million in 2023.

According to data from the Ministry of Internal Affairs, over the past five years, Uzbekistan has witnessed a surge in cybercrime – from 863 cases in 2019 to nearly 59,000 in 2024. Within just the last year, the number of such crimes has in-

1 Constitution of the Republic of Uzbekistan. – T.: Uzbekistan, 2023. – P. 19-21.
A press tour was organized for media representatives and the public, dedicated to the activities of the Cybersecurity Center of the Operational-Investigative Department of the Ministry of Internal Affairs of the Republic of Uzbekistan. URL: https://gov.uz/ru/iiv/news/view/57775. (access date 01.11.2025).

creased ninefold, while their share in the overall crime structure has risen from 6.2% to 44.4%[2].

Currently, cases of deepfake dissemination have become increasingly frequent in the Republic of Uzbekistan. The term "deepfake" comes from two English words: deep learning and fake. In most cases, the method is based on generative adversarial neural networks. A deepfake is an artificially generated audio or video recording of real people that is almost indistinguishable from the original in terms of facial features, voice, mannerisms, accent, and other traits.

Considering its global spread and the accompanying risks and threats, the issue of deepfakes has become the subject of academic research by numerous scholars, including Christopher Doss, Jared Mondschein, Dule Shu, Tal Wolfson, Denise Kopecky, Valerie A. Fitton-Kane, Lance Bush, Conrad Tucker[3], Bahar Uddin Mahmud, Afsana Sharmin[4], M.B. Dobrobaba[5], I.N. Arkhiptsev, A.N. Alexandrov, A.V. Maksimenko, K.I. Ozerov[6], M.A. Falaleev, N.A. Sitdikova, E.E. Nechai[7], M.A. Zheludkov, A.P. Alekseeva[8], and others.

Main part. Experts identify the most well-known examples of unlawful uses of deepfake technology:

– creation of pornographic videos (98% of all deepfakes are pornographic in nature; on the ten most popular specialized platforms, pornographic deepfakes have been viewed over 303 million times; 99% of such videos feature female characters)[9];

– creation of audio and video recordings for fraud or extortion[10];

– political manipulation.

The damage caused by crimes involving deepfakes is significantly greater than that resulting from traditional offenses. Their consequences may be economic, political, reputational, moral, and others.

While early deepfakes in Uzbekistan were primarily created for fraudulent purposes, more recent examples involving well-known media figures, athletes, politicians, businesspeople, and others often serve as attempts at political manipulation[11]. Such cases can undoubtedly undermine public order, infringe on citizens' legitimate rights and interests, and pose a threat to national security and social stability.

One of the state's key priorities in countering the malicious use of deepfakes is improving the relevant legal framework.

Foreign Experience.

In the United States, the TAKE IT DOWN Act (enacted on May 19, 2025) requires online platforms and websites to promptly remove pornographic deepfakes that have been posted without the consent of the depicted individual. Offenders are obliged to compensate for damages and are subject to criminal penalties, including imprisonment and/or fines. Threats to publish intimate visual depictions of a person are likewise prohibited by law and carry criminal liability.

Platforms must establish procedures that al-

2 A press tour was organized for media representatives and the public, dedicated to the activities of the Cybersecurity Center of the Operational-Investigative Department of the Ministry of Internal Affairs of the Republic of Uzbekistan. URL: https://gov.uz/ru/iiv/news/view/57775. (access date 01.11.2025).

3 Christopher Doss, Jared Mondschein, Dule Shu, Tal Wolfson, Denise Kopecky, Valerie A.Fitton-Kane, Lance Bush, Conrad Tucker. Deepfakes and scientific knowledge dissemination // Scientific Reports. – volume 13, Article number: 13429 (2023). URL: https://www.nature.com/articles/s41598-023-39944-3.

4 Bahar Uddin Mahmud, Afsana Sharmin. Deep Insights of Deepfake Technology: A Review // DUJASE. – 2020. – Vol. 5. – (1 & 2). (January & July) – p.p. 13-23.

5 Dobrobaba M.B. Deepfakes as a Threat to Human Rights// LEX RUSSICA. – 2022. – T.75. – No. 11. – P. 112-119.

6 Arkhiptsev I.N., Alexandrov A.N., Maksimenko A.V., Ozerov K.I. Pornographic Deepfake: Fiction or Reality? // Socio-Political Sciences. – 2021. – T.11. – No. 1. – P. 69-74.

7 Falaleev M.A., Sitdikova N.A., Nechai E.E. Deepfake as a Phenomenon of Political Communication // Bulletin of Transbaikal State University. – 2021. – T. 27. – No. 6. – P. 101-106.

8 Zheludkov M.A., Alekseeva A.P. Ensuring the Security of Biometric Personal Data Against Criminal Use // Bulletin of the Saint Petersburg University of the Ministry of Internal Affairs of Russia. – 2025. – No. 2 (106). – P. 159-169.

9 2023 State of Deepfakes Realities, Threats and Impact. Access mode: URL: https://www.securityhero.io/state-of-deepfakes/. (access date: 01.11.2025).

10 Dolgieva M.M. Qualification of Deepfake Fraud and Cyber Kidnapping // Actual Problems of Russian Law. – 2024. – T. 19. – No. 11 (168). – P. 106-113.

11 Attention, Fake! Deepfake videos appeared on behalf of public figures, urging people to join the Russian Army. URL: https://kun.uz/ru/87868316. (access date: 01.11.2025).

low individuals featured in intimate visual depictions to notify the platform of their existence and request the removal of such content if it has been published without their consent. Online platforms must delete the identified images within 48 hours of receiving such notification. According to the Act, covered platforms include public websites, online services, and applications[12].

As early as 2018, California enacted Assembly Bill No. 602 (AB 602) and Assembly Bill No. 730 (AB 730), which prohibit the creation and distribution of deepfakes depicting individuals in pornographic contexts without their consent, as well as those produced for the purpose of causing harm, deception, or manipulation, particularly in the contexts of pornography and political elections[13]. Although the term "deepfake" is not explicitly used in California law, liability is established for "forgeries created with the use of artificial intelligence" and for "misleading videos intended to portray someone in a negative light".

For reference: On January 22, 2024, the Office of the Attorney General of New Hampshire launched an investigation into a series of automated voice messages (so-called "robocalls") received by thousands of state residents and linked to S. Kramer. The voice of U.S. President Joe Biden in these recorded messages had been cloned using a neural network algorithm. Under RSA 659:40, III (Criminal violation related to voter suppression), it is established that "No person shall engage in voter suppression by knowingly attempting to prevent or deter another person from voting or registering to vote based on fraudulent, deceptive, misleading, or spurious grounds or information". In connection with the incident, 13 administrative offenses were recorded under RSA 666:7-a (Impersonation of Candidates). Following the Federal Communications Commission's (FCC) decision, the telecommunications company Lingo Telecom, whose equipment was used to carry out the robocalls, was fined. Charges were filed against S. Kramer, with the penalty estimated at $6 million[14].

In Singapore, the Protection from Online Falsehoods and Manipulation Act (POFMA) was adopted in 2019 to protect society from the dissemination of deepfakes and other forms of misinformation[15].

The Act prohibits the spread of false statements of fact or misleading information online.

China was among the first countries to introduce specific measures to regulate the distribution of deepfake content. A system of mandatory labeling was established to help identify synthetic media and reduce the risk of misinformation.

Since January 1, 2020, criminal liability has been introduced for the distribution of deepfakes without proper labeling. Compliance with this requirement is monitored and enforced by the Cyberspace Administration of China.

In November 2022, China adopted the Provisions on the Administration of Deep Synthesis Internet Information Services[16]. Together with the laws "On Cybersecurity", "On Data Security", "On Personal Information Protection", "On the Administration of Internet Information Services", and other regulatory legal acts of the People's Republic of China, these provisions establish prohibitions on the use of deepfakes for purposes that may threaten national security and national interests, damage the nation's image, infringe upon public interests, disrupt economic or social order; or violate the lawful rights and interests of other individuals.

The Provisions on the Administration of Deep Synthesis Internet Information Services include the following key requirements:

– companies must obtain the consent of individuals before creating deepfakes and must verify the authenticity of users' real identities;

– service providers must establish and improve mechanisms for rumor refutation;

– created deepfakes may not be used for ac-

12 S.146 - TAKE IT DOWN Act. URL: https://www.congress.gov/bill/119th-congress/senate-bill/146 (access date: 01.11.2025).

13 URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20192 0200AB730 (access date: 01.11.2025).

14 Consultant behind deepfaked Biden robocall fined $6m as new charges filed. US elections 2024. Retrieved from https://www.theguardian.com/us-news/article/2024/may/23/biden-robocall-indicted-primary.

15 Introduction to Foreign Interference (Countermeasures) Act (FICA). URL: https://www.mha.gov.sg/fica (access date: 01.11.2025).

16 Provisions on the Administration of Deep Synthesis Internet Information Services. Documents of the State Council Department. Government Network of China. URL: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm (access date: 01.11.2025).

tivities prohibited by laws or administrative regulations;

– providers of deep synthesis services must add a signature or watermark indicating that the work is synthetic, to prevent public confusion or misidentification[17].

In the European Union, regulatory frameworks for artificial intelligence are under consideration and may address deepfakes. In particular, the Artificial Intelligence Act 2024 (AI Regulation)[18] introduces the concept of deepfakes and includes provisions addressing the high risks associated with data manipulation. The Regulation allows the use of deepfakes but sets forth minimum requirements to ensure transparency and openness. Creators of deepfake content must label their materials accordingly. Violations of the Regulation entail penalties for governmental bodies, institutions, agencies, and AI model providers.

The Digital Services Act (DSA) (2024) establishes the obligation to label synthetic or manipulated content, for instance, through watermarks or metadata. The DSA grants citizens the right to notify online platforms of illegal deepfakes and requires platforms to remove or restrict access to such content upon verification. Regulators have been given enforcement mechanisms, including fines of up to 6% of global turnover, for platforms that fail to take adequate measures against deepfakes and other forms of disinformation.

In Australia, legislation addressing deepfakes has been adopted to counter cyberbullying, the distribution of non-consensual pornography, and the spread of disinformation[19]. The Criminal Code Amendment (Deepfake Sexual Material) Act 2024 establishes criminal liability for distributing pornographic deepfakes via online services. The creation of a deepfake and its subsequent dissemination are treated as aggravating circumstances that increase the severity of the penalty.

In France, criminal penalties are prescribed for the publication, by any means, of photo or video material that uses a person's image or words without their consent, unless it is clearly apparent that the material is a montage or explicitly stated to be so. The punishment includes up to one year of imprisonment and a fine of 15,000 euros.

In 2018, France adopted the Law on Combating Information Manipulation, which strengthens oversight of social-media publications and the operations of foreign media outlets. In particular, it enables a registered candidate, political party, or civic association to request, through the courts, the removal from social networks or the media of information they deem false. The court must review such a complaint within 48 hours and "suspend the dissemination of false information".

In the United Kingdom, the Online Safety Act was adopted in 2023. This legislation covers the protection of children, cyberbullying and harassment, privacy and data security, and other aspects of online safety. One of its provisions prohibits the sharing of intimate images created using deepfakes without consent (Ministry of Justice, 2022).

The Data (Use and Access) Act 2025 introduces a set of amendments ranging from data-access rules to enhanced protections aimed at combating deepfakes. Under this legal framework, the creation of sexually explicit deepfakes without consent, whether for personal gratification or for the purpose of causing harm, is punishable by an unlimited fine.

In South Korea, the Special Act on the Punishment of Sexual Crimes 2024 establishes liability for the creation and distribution of sexual deepfakes without consent, prescribing up to 7 years of imprisonment, regardless of the creator's intention to disseminate the material. Moreover, the purchase, possession, or viewing of such deepfakes is also criminalized, carrying penalties of up to 3 years of imprisonment or a fine of up to 30 million Korean won.

In 2023, amendments to the Public Official Election Act prohibited the publication of manipulative media, including deepfakes, during the 90 days preceding elections. Violations of this provision may result in up to 7 years' imprisonment

17 URL: https://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm. (access date: 01.11.2025).

18 2024 European Union Artificial Intelligence Regulation, Autonomous Non-Profit Organization "Digital Economy". URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikhstranakh/2024_reglament_evropeyskogo_soyuza _ob_iskusstvennom_intellekte_ano_cifrovaya_ekonomika_/ (access date: 01.11.2025).

19 Lexology Search. URL: https://www.lexology.com/ (access date: 01.11.2024).

and a fine of 50 million won. Election campaigns are additionally required to disclose any use of AI-generated content.

In the State Duma of the Russian Federation, Draft Law No. 718538-8 is under consideration. It proposes classifying the use of deepfakes (images, voice, biometric data) as an aggravating circumstance for several criminal offenses, including defamation (Art. 128.1), fraud (Art. 159), theft (Art. 158), and extortion (Art. 163).

The second package of measures to combat cyber fraud introduces direct criminal liability for acts related to deepfakes. For fraudulent activities involving AI, a fine of 100,000 to 500,000 rubles may be imposed. Imprisonment for up to six years, accompanied by a fine of up to 80,000 rubles, is also permitted. If money is stolen from a bank account using neural networks, the penalty may include 3 to 8 years of imprisonment, as well as a fine of up to 100,000 rubles. Extortion committed using AI is punishable by a fine of 100,000 to 500,000 rubles or imprisonment for up to five years. Malicious interference with information systems, computer data, or communication networks using AI is punishable by a fine of up to 500,000 rubles or up to 4 years' imprisonment.

The creation of deepfakes, per se, is not unlawful. In Russian judicial practice, there are precedents recognizing deepfakes as objects of copyright[20]. However, it is essential to note that a person's image is protected under civil law. Therefore, when creating and distributing deepfakes involving a real person, these legal considerations must also be taken into account.

In Kazakhstan, the dissemination of knowingly false information is regulated by the Law "On Online Platforms and Online Advertising" (2023). False information is understood as anything that distorts facts and misleads the public, creating a false perception of events, people, and phenomena.

Liability for false information may be administrative (Article 456-2 of the Code of Administrative Offenses) or criminal (Article 274 of the Criminal Code of the Republic of Kazakhstan). The latter provides for a fine of 3,000 MCI, correctional labor, community service of up to 800 hours, or imprisonment for up to 3 years.

In May 2025, the Mazhilis approved at first reading the draft law "On Artificial Intelligence", which introduces liability measures for the creation of deepfakes. According to the draft, the use of AI constitutes an aggravating circumstance. Kazakhstan plans to introduce administrative liability for the creation and dissemination of deepfakes, with fines ranging from 15 to 100 MCI.

For reference: In June this year, politically oriented deepfakes were widely circulated in Kazakhstan involving the Akim of the Kostanay region, Kumar Aksakalov, the Akim of the North Kazakhstan region, Gauez Nurmukhambetov, Member of the Senate of the Parliament of the Republic of Kazakhstan from the East Kazakhstan region, Olga Bulavkina, and others[21].

In Kyrgyzstan, in June 2024, a draft law was published on the official website of the Jogorku Kenesh, proposing amendments to existing national regulations to counter threats posed by deepfakes.

The legislative initiative aims to protect citizens' rights and state interests from the risks of public opinion manipulation, targeted discreditation, and disinformation.

National Practice.

In the Republic of Uzbekistan, the issue of introducing liability for the use of artificial intelligence in the commission of crimes has been raised repeatedly.

In November 2025, the Senate of the Oliy Majlis approved the draft Law of the Republic of Uzbekistan "On Regulating Relations Arising from the Use of Artificial Intelligence", which establishes the obligation to label deepfakes and introduces liability for the unlawful processing and dissemination of deepfakes[22].

In addition, the draft Law of the Republic of Uzbekistan "On the Protection of the Rights of Users of Online Platforms and Websites" has completed the public discussion stage. The draft obliges internet platforms to promptly remove unlawful

20 Lexology Search. URL: https://www.lexology.com/ (access date: 01.11.2024)

21 Deepfakes are rapidly spreading in Kazakhstan. URL: https://stopfake.kz/ru/archives/24326. (access date: 01.11.2025).

22 Information on the Eleventh Plenary Session of the Senate of the Oliy Majlis of the Republic of Uzbekistan. Access mode: https://senat.uz/plenary-sessions/post-4333 . (access date: 05.11.2025)

content, including fake news, drug-related advertising, and offensive materials. It also strengthens the protection of personal data. Platforms are prohibited from providing user information to third parties without the user's consent.

Conclusion. Taking into account advanced foreign experience, legislation, and law-enforcement practice, it is considered advisable to:

1. Establish administrative liability for the creation and dissemination of deepfakes without proper labeling;

2. Define the commission of a crime (fraud, extortion, politically motivated offenses, etc.) using deepfakes as an aggravating circumstance;

3. Introduce a separate criminal offense for the creation and dissemination of pornographic deepfakes and require platforms to remove such materials without delay (within 48 hours of notification);

4. Provide for the liability of digital platforms for hosting unlabeled deepfakes to ensure that users can identify such content. Require platforms to use deepfake detection systems before uploading video and audio materials to their resources.

5. Clearly specify in the Civil Code of the Republic of Uzbekistan who holds the rights to use a person's image and voice, including cases involving deceased individuals (the right to sound and image);

6. Introduce clarifications into the Law of the Republic of Uzbekistan "On Personal Data" regarding how deepfake technologies relate to personal data protection, to prevent the use of images without consent;

7. Develop guidelines and standards for the use of deepfake technologies in media and advertising to ensure transparency and integrity;

8. Include information on deepfake technologies, their capabilities, and risks in educational programs to increase public awareness;

9. Establish a regulatory authority or committee to monitor the use of deepfake technologies and their impact on society. These measures will help create a safer and more ethical environment for the use of deepfake technologies.

#

Bunyod KUDRATOV,
Huquqni muhofaza qilish akademiyasi Raqamli kriminalistika ilmiy-tadqiqot instituti Kiberjinoyatlarga qarshi kurashishga va raqamli tergovga ko‘maklashish markazi boshlig‘i

RAQAMLI DAVRDA KIBERJINOYATLARGA QARSHI KURASHISHNING DOLZARB MASALALARI

ANNOTATSIYA. *Maqolada zamonaviy sharoitda kiberjinoyatchilikning o‘sib borayotganligi va unga qarshi kurashishning dolzarb muammolari tahlil qilingan. Tadqiqotda O‘zbekiston Respublikasida axborot texnologiyalari yordamida sodir etilayotgan jinoyatlarning holati, ularni tergov qilishdagi nazariy va amaliy qiyinchiliklar, jinoyat-protsessual qonunchilikning mavjud kamchiliklari ko‘rib chiqilgan. Global va milliy statistik ma’lumotlar asosida kiberjinoyatchilikning iqtisodiy va ijtimoiy oqibatlari baholangan. Muallif tomonidan raqamli dalillarni protsessual tartibda yig‘ish va baholash, xalqaro huquqiy hamkorlikni takomillashtirish, malakali kadrlar tayyorlash hamda milliy qonunchilikni isloh qilish bo‘yicha ilmiy-amaliy tavsiyalar ishlab chiqilgan.*

АННОТАЦИЯ. *В статье анализируются проблемы роста киберпреступности в современных условиях и актуальные вопросы противодействия ей. В исследовании рассматривается состояние преступлений, совершаемых с использованием информационных технологий в Республике Узбекистан, теоретические и практические трудности их расследования, существующие недостатки уголовно-процессуального законодательства. На основе глобальных и национальных статистических данных оценены экономические и социальные последствия киберпреступности. Автором разработаны научно-практические рекомендации по процессуальному сбору и оценке цифровых доказательств, совершенствованию международного правового сотрудничества, подготовке квалифицированных кадров и реформированию национального законодательства.*

ABSTRACT. *The article analyzes the issues of cybercrime growth in contemporary conditions and the urgent problems of combating it. The study examines the state of crimes committed through information technologies in the Republic of Uzbekistan, theoretical and practical difficulties in their investigation, and existing deficiencies in criminal procedural legislation. Based on global and national statistical data, the economic and social consequences of cybercrime are assessed. The author has developed scientific and practical recommendations on the procedural collection and evaluation of digital evidence, improvement of international legal cooperation, training of qualified personnel, and reform of national legislation. The article is intended for legal scholars, law enforcement officers, and researchers.*

Kalit so‘zlar: *kiberjinoyatchilik, raqamli dalillar, jinoyat-protsessual qonunchilik, axborot texnologiyalari, raqamli kriminalistika, xalqaro hamkorlik.*

Ключевые слова: *киберпреступность, цифровые доказательства, уголовно-процессуальное законодательство, информационные технологии, цифровая криминалистика, международное сотрудничество.*

Key words: *cybercrime, digital evidence, criminal procedural law, information technologies, digital forensics, international cooperation.*

Zamonaviy jamiyatning raqamli transformatsiyasi sharoitida jinoyatchilikning tabiati va ko‘rinishlari tubdan o‘zgarib bormoqda. Axborot-kommunikatsiya texnologiyalarining jadal sur’atlar bilan rivojlanishi, internet tarmog‘ining globallashuvi va kibermakonning kengayib borishi jinoyatchilikka qarshi kurashish sohasida yangi qiyinchiliklarni keltirib chiqarmoqda.

Bugungi kunda an’anaviy jinoyatlarning kibermakonga ko‘chishi kuzatilmoqda. Uyushgan jinoiy guruhlar hamda transmilliy jinoiy tashkilotlar zamonaviy axborot texnologiyalaridan jinoyatlarni rejalashtirish, sodir etish, ularning izlarini yo‘qotish hamda jinoiy javobgarlikdan qochish maqsadida samarali foydalanib kelmoqda. Global internet tarmog‘ining chegarasizligi, kriptografik texnologiyalar va anonimlashtirish vositalarining mavjudligi kiberjinoyatchilarning huquq-tartibot idoralari tomonidan aniqlanishi ehtimolini sezilarli darajada kamaytirish imkoniyatini bermoqda.

Xalqaro tahliliy manbalar prognozlariga ko‘ra, kiberjinoyatchilik oqibatida yetkaziladigan global iqtisodiy zarar 2025-yilda yiliga 10,5 trillion AQSH dollariga yetganligi, 2031-yilga borib esa 12,2 trillion AQSH dollarigacha oshishi kutilmoqda. Ushbu ko‘rsatkichlar kiberjinoyatchilikning nafaqat axborot xavfsizligi, balki global iqtisodiy barqarorlikka ham bevosita tahdid solayotganini ko‘rsatadi[1].

Bugungi kunda insoniyatning Internet jahon axborot tarmog‘iga ijtimoiylashuvi jarayonlari tobora kuchayib borib, eng yuqori cho‘qqiga chiqqan. Xususan, yer yuzi aholisining 60 foizi bir kunda o‘rtacha 6 soat vaqtini internetda o‘tkazmoqda.

1 Cybersecurity Ventures. Official Cybercrime Report: Cybercrime To Cost The World $12.2 Trillion By 2031. 2025.

Shu bilan birga, so‘nggi besh yilda global tarmoqda axborot almashish hajmi ikki karraga oshgan[2].

Ayrim hukmron davlatlar o‘rtasidagi siyosiy o‘yinlar va qarama-qarshiliklarda iqtisodiy sanksiyalar, energetik va boshqa resurslardan bosim ko‘rsatuvchi vosita sifatida foydalanish bilan bir qatorda, maxsus kiberhujumlar qo‘llanilmoqda. Xususan, “@War: The Rise of the Military-Internet Complex” asari muallifi amerikalik olim SH.Xarris (Shane Harris) kibermakonni havo, quruqlik, dengiz va koinotdan keyingi harbiy harakatlarning beshinchi teatr maydoni sifatida ta’riflaydi[3].

Kiberjinoyatchilik, xususan, kiberfiribgarlik bugungi kunda oddiy mahalliy jinoyat doirasidan chiqib, global xavfga aylangan. Professor S.Uoll Devid) ta’kidlaganidek[4], huquqni muhofaza qiluvchi organlar ko‘p hollarda kiberjinoyatchilardan bir qadam ortda qolmoqda. Bu esa mazkur jinoyatlarni fosh etish va tergov qilishda raqamli izlarning tez yo‘qolishi, jinoyatchilarning texnik vositalar orqali shaxsini yashirishi hamda mablag‘larni transchegaraviy tarzda harakatlantirishi bilan izohlanadi. Shuningdek, professor Mixael Levi va hammualliflar kiberfiribgarlikning muhim xususiyati uning “globallashish qobiliyatiga ega” ekanligini ta’kidlaydi[5]. Demak, kiberfiribgarlik bir vaqtning o‘zida jabrlanuvchi, bank-moliya tizimi, internet provayderlar, kripto-platformalar va turli davlatlar yurisdiksiyasini qamrab oladigan murakkab transmilliy jinoyat hisoblanadi.

Dunyoning nufuzli tadqiqot markazlarida kiberfiribgarlikka qarshi kurashishning nazariy va amaliy asoslarini konseptual o‘rganish bo‘yicha ilmiy izlanishlar olib borilmoqda. Xususan, Oksford universiteti tadqiqotchilari ishtirok etgan xalqaro ilmiy loyiha — Jahon kiberjinoyatchilik indeksida (World Cybercrime Index) eng katta kibertahdid manbalari bo‘lgan davlatlar ko‘rsatilgan bo‘lib, unga ko‘ra Rossiya (58.39), Ukraina (36.44), Xitoy (27.86), AQSH (25.01)[6] davlatlari ushbu ro‘yxatda yetakchilik qilgan.

O‘zbekiston Respublikasi ham bu jahon miqyosidagi jarayondan chetda qololmaydi - davlat va xususiy sektorlarning raqamlashuvi, elektron davlat xizmatlarining joriy etilishi, moliyaviy tizimning raqamli transformatsiyasi yangi turdagi xavf-xatarlarni yuzaga keltirmoqda.

O‘zbekiston Respublikasi Milliy statistika qo‘mitasining uy xo‘jaliklari tanlanma kuzatuvi ma’lumotlariga ko‘ra, 2025-yil yanvar-avgust oylarida mamlakatda internetdan foydalanuvchi aholi ulushi 94,2 foizni tashkil etgan. Shuningdek, 2025-yilda 100 ta uy xo‘jaligiga o‘rtacha 359 ta mobil telefon to‘g‘ri kelgani aholining raqamli kommunikatsiya vositalari va onlayn xizmatlardan foydalanish imkoniyatlari kengayganini ko‘rsatadi. Mazkur holat kibermakonda sodir etiladigan huquqbuzarliklar, kiberfiribgarlik va shaxsiy ma’lumotlar xavfsizligi bilan bog‘liq tahdidlarning dolzarbligini yanada oshirmoqda[7].

Shu nuqtayi nazardan raqamli muhitdan foydalanish ko‘lamining kengayishi kiberjinoyatchilikka qarshi kurashishning huquqiy va tashkiliy asoslarini takomillashtirish zaruratini obyektiv ravishda yuzaga keltirmoqda. Zero, aholining internet, mobil aloqa vositalari, elektron davlat xizmatlari, onlayn to‘lov tizimlari va ijtimoiy platformalardan faol foydalanishi bir tomondan jamiyatda raqamli qulayliklarni oshirsa, ikkinchi tomondan kibermakonda sodir etiladigan firibgarlik, shaxsiy ma’lumotlarni noqonuniy qo‘lga kiritish, moliyaviy operatsiyalarga aralashish, zararli dasturlardan foydalanish hamda transchegaraviy kiberjinoyatlar xavfini kuchaytirmoqda.

Bunday sharoitda kiberjinoyatchilikka qarshi kurashish faqat jinoyat sodir etilgandan keyin uni fosh etish bilan cheklanmasdan, balki huquqiy normalarni zamonaviy axborot texnologiyalari rivojiga moslashtirish, vakolatli organlar o‘rtasida tezkor axborot almashinuvini ta’minlash, raqamli dalillarni yig‘ish va saqlashning yagona protsessual mexanizmlarini joriy etish ham-

2 Global Business Platform Statista. https://www.statista.com/statistics/631151/worldwide-data-collected-by-smart-buildings/.

3 Харрис Шейн. Кибервойн@. Пятый театр военных действий. М.: Альпина нон-фикшн, 2016. - 390 с.

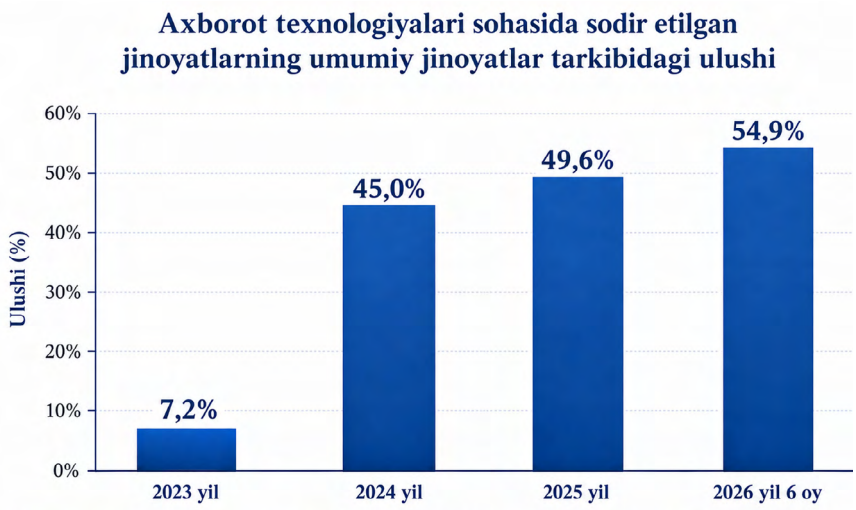
4 Wall, D.S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.

5 Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. (2017). "Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research." Crime, Law and Social Change, 67(1), 77-96.

6 Miranda Bruce, Jonathan Lusthaus, Ridhi Kashyap Nigel Phair, Federico Varese. Mapping the global geography of cybercrime with the World Cybercrime Index Published: April 10, 2024. https://doi.org/10.1371/ journal.pone.0297312;

7 https://nsdg.stat.uz/publication/2025/uz.pdf

da profilaktik va tashkiliy choralarni kuchaytirishni talab etadi.



Manba: "Elektron jinoyiy-huquqiy statistika" yagona axborot tizimi hisobot hujjatlari asosida tayyorlandi.

Xususan, respublikamizda axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarning umumiy jinoyatchilik tarkibidagi ulushi so‘nggi yillarda izchil va sezilarli darajada ortib bormoqda. Jumladan, mazkur turdagi jinoyatlar 2023-yilda jami qayd etilgan jinoyatlarning 7,2 foizini tashkil etgan bo‘lsa, 2024-yilda ushbu ko‘rsatkich 45 foizga, 2025-yilda 49,6 foizga yetgan. 2026-yilning olti oyi yakunlariga ko‘ra esa axborot texnologiyalari sohasida sodir etilgan jinoyatlarning ulushi 54,9 foizni tashkil etib, umumiy jinoyatlarning yarmidan ortig‘i mazkur toifaga to‘g‘ri kelayotganini ko‘rsatmoqda. Ushbu statistik dinamika raqamli texnologiyalarning jamiyat hayotiga keng kirib borishi bilan bir qatorda, kiberjinoyatchilikning ko‘lami va ijtimoiy xavflilik darajasi ortib borayotganini hamda unga qarshi kurashishning huquqiy, tashkiliy va kriminalistik mexanizmlarini yanada takomillashtirish zaruratini yaqqol namoyon etadi[8].

Mavzuning dolzarbligi quyidagi obyektiv omillar bilan asoslanadi:

birinchidan, respublikamizda jinoyat-protsessual qonunchilikning kiberjinoyatchilik bilan bog‘liq huquqbuzarliklarni tergov qilish va sud tomonidan ko‘rib chiqish xususiyatlarini to‘liq inobatga olmasligi, tergov organlari tomonidan xorijiy mamlakatlarda saqlanayotgan raqamli dalillarni xizmat ko‘rsatuvchi provayderlardan to‘g‘ridan-to‘g‘ri so‘rab olish mexanizmlari mavjud emasligi kuzatilmoqda;

ikkinchidan, huquqni muhofaza qiluvchi idoralar xodimlarining kiberjinoyatchilik bilan bog‘liq ishlarni yuritish bo‘yicha maxsus bilim va malakaga ega emasligi, zamonaviy texnik vositalar va dasturiy ta’minotdan foydalanish ko‘nikmalarining yetarli emasligi muammosi mavjud;

uchinchidan, kiberhujumlarning transchegaraviy xususiyatga ega ekanligi xalqaro huquqiy hamkorlik mexanizmlarini takomillashtirish, jinoiy-protsessual yordam ko‘rsatish tartibotini oddiylashtirish va tezlashtirishni taqozo etmoqda;

to‘rtinchidan, kibermakondagi dalillarning o‘ziga xos xususiyatlari — ularning oson o‘zgaruvchanligi, yo‘qoluvchanligi, joylashish joyining noaniqligi — jinoyat-protsessual isbotlashning an’anaviy nazariyasi doirasida mazkur muammolarga yechim topishni qiyinlashtirmoqda.

Bu jihatdan kibermakonda sodir etilgan jinoyatlar bo‘yicha sudgacha ish yuritish jarayonida yuzaga keladigan muammolarni hal etish, mazkur toifadagi jinoyatlarga qarshi kurashishning yanada samarali mexanizmlarini ishlab chiqish, sudgacha ish yuritish davomida shaxsning huquq va erkinliklarini samarali himoya qilish, shuningdek, kibermakonda sodir etiladigan jinoyatlar sonini kamaytirish bo‘yicha ko‘rilayotgan chora-tadbirlar samaradorligini oshirishning ilmiy asoslangan yechimlarini izlashga qaratilgan tadqiqotlar tobora dolzarb bo‘lib bormoqda.

Quyidagi omillar axborot texnologiyalari yordamida sodir etilgan jinoyatlar bo‘yicha amaliyotdagi dolzarb muammolarni ko‘rsatadi.

Birinchidan, bugungi kunda kiberjinoyatni sodir etishda o‘z nomidagi bank kartasidan, bank hisobraqamidan, SIM-kartasidan hamda elektron hamyonidan (elektron akkauntlar) foydalanishga yo‘l qo‘ygan shaxslar (drop) uchun ma’muriy yoki jinoiy javobgarliklar mavjud emasligi.

Ikkinchidan, kiberjinoyatlar bo‘yicha, xususan, raqamli dalillar bilan ishlash, blokcheyn texnologiyalari, zararli dasturiy ta’minotlar bo‘yicha mu-

8 “Elektron jinoiy-huquqiy statistika” yagona axborot tizimi hisobot hujjatlari.

taxassis fikri yoki ekspert xulosasi berish uchun maxsus bilimlarga ega mutaxassislar soni respublika miqyosida juda kamligi, raqamli dalillar bilan bog‘liq jinoyatlarni tergov qilishda jiddiy to‘siq yaratmoqda.

Uchinchidan, bu toifadagi jinoyatlar kibermakonda sodir etilishi, jinoyatchilar o‘zlarining shaxsini imkon qadar oshkor qilmasliklari, transchegaraviy xususiyatdagi elektron dalillarni protsessual tartibda olish mexanizmlarining takomillashmaganligi, JPKdagi normalarda raqamli dalillarni xorijiy mamlakatlardan so‘rab olishning protsessual jihatlari murakkabligi, xorijiy mamlakatlarda joylashgan xizmat ko‘rsatish provayderlari va ijtimoiy tarmoqlardan elektron ma’lumotlarni so‘rab olishda qator muammolar mavjudligi tergov organlarining bu toifadagi jinoyatlarni fosh etish amaliyotiga o‘zining salbiy ta’sirini ko‘rsatmoqda.

Kiberjinoyatchilikka qarshi kurashishning huquqiy asoslarini takomillashtirishda avvalo, sohani tartibga soluvchi yagona va tizimli yondashuvni shakllantirish muhim ahamiyat kasb etadi. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-sonli qarori bilan Ichki ishlar vazirligi kiberjinoyatlarga qarshi kurashish yo‘nalishida yagona ishlash amaliyotini yo‘lga qo‘yish, mas’ul davlat organlari va muassasalari faoliyatini muvofiqlashtirish hamda manzilli hamkorlikni tashkil etish bo‘yicha vakolatli organ etib belgilandi. Bu esa kiberjinoyatchilikka qarshi kurashishda parokandalikni bartaraf etish, idoralararo ma’lumot almashinuvini kuchaytirish va yagona huquqni qo‘llash amaliyotini shakllantirishga xizmat qiladi.

Mazkur sohadagi muhim huquqiy yangiliklardan biri — bu axborot texnologiyalaridan foydalanib sodir etilayotgan jinoyatlarga qarshi kurashish bo‘yicha alohida qonun loyihasini ishlab chiqish vazifasining belgilanganidir. Ushbu qonun loyihasida kiberjinoyatlarning oldini olish va fosh etishda davlat organlari, banklar, to‘lov tizimi operatorlari hamda to‘lov tashkilotlarining aniq mas’uliyatini belgilash nazarda tutilgan. Shuningdek, kiberjinoyat sodir etilishida o‘z bank kartasi, hisobraqami, SIM-kartasi yoki elektron hamyonidan foydalanishga yo‘l qo‘ygan shaxslar, ya’ni “drop”lar uchun ma’muriy va jinoiy javobgarlikni belgilash, axborot texnologiyalari sohasidagi jinoyatlar uchun jazo choralarini kuchaytirish, axborot texnologiyalaridan foydalanishni javobgarlikni og‘irlashtiruvchi holat sifatida belgilash kabi masalalar ham huquqiy islohotlarning muhim yo‘nalishlari hisoblanadi.

Tashkiliy jihatdan kiberjinoyatchilikka qarshi kurashish faqat jazolash mexanizmlari bilan cheklanmasligi lozim. Bu borada profilaktika, barvaqt aniqlash, tezkor to‘xtatish va raqamli dalillarni ishonchli tadqiq etish tizimlari o‘zaro uyg‘un holda ishlashi zarur.

153-sonli qarorda banklar va to‘lov tashkilotlarining kiberxavfsizlik talablariga rioya etish bo‘yicha mas’uliyatini kuchaytirish, kiberjinoyatlar ko‘p qayd etilgan bank va to‘lov tashkilotlari ro‘yxatini ommaga e’lon qilish, moliyaviy piramidalarni tranzaksiyalar monitoringi orqali aniqlash hamda markazlashgan antifrod tizimlarini joriy etish choralari belgilangan. Bu mexanizmlar kiberjinoyatlarning oqibati bilan emas, balki ularning kelib chiqish sabablari va shart-sharoitlari bilan kurashishga qaratilganligi bilan ahamiyatlidir.

Raqamli kriminalistika institutsional jihatdan alohida o‘rin tutadi. O‘zbekiston Respublikasi Prezidentining 2024-yil 21-iyundagi 229-sonli qarori bilan Raqamli kriminalistika ilmiy-tadqiqot instituti tashkil etilgani sohada ilmiy-texnik salohiyatni kuchaytirishga xizmat qiladi. Ushbu hujjatda axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etilayotgan jinoyatlarni o‘z vaqtida aniqlash va samarali tergov qilish uchun maxsus raqamli usullar, raqamli dalillar bilan ishlash texnikasi, yuqori malakali mutaxassislar va tizimli ilmiy-tadqiqot bazasi zarurligi alohida ta’kidlangan. Institutga raqamli kriminalistika bo‘yicha sud ekspertizalari va tadqiqotlar o‘tkazish, jinoyatlarning raqamli izlarini aniqlash, olib qo‘yish, saqlash va tadqiq qilish, shuningdek, mutaxassislarni zamonaviy ekspertiza turlari bo‘yicha o‘qitish vakolatlari berilgan.

Kiberjinoyatlarni fosh etishda raqamli dalillarning protsessual maqomi, ularni yig‘ish, saqlash, tahlil qilish va sudda baholash masalalari alohida ahamiyat kasb etadi. 229-sonli qarorda “Raqamli dalillar yagona reyestri” idoralararo avtomatlashtirilgan tizimini joriy etish vazifasi belgilangan bo‘lib, uning asosiy maqsadi jinoyatlarni fosh etish, tergov samaradorligini oshirish va uyushgan jinoiy guruhlarni tezkor aniqlash uchun jinoyat ishlari bo‘yicha materiallarni yig‘ish, hisobga olish, saqlash va tahlil qilishdan iborat. Bu esa raqamli dalillar bilan ishlashda zanjirli saqlash,

ma’lumotlarning yaxlitligi va ishonchliligini ta’minlash, tergov organlari o‘rtasida axborot almashinuvini tezlashtirish imkonini beradi.

Kadrlar tayyorlash tizimi ham kiberjinoyatchilikka qarshi kurashishning muhim tashkiliy asoslaridan biridir. O‘zbekiston Respublikasi Prezidentining 2025-yil 22-yanvardagi 17-sonli qarori bilan IIV Akademiyasida “Raqamli texnologiyalar sohasida jinoyatlarga qarshi kurashish faoliyati” bakalavriat yo‘nalishi, Huquqni muhofaza qilish akademiyasida esa “Kiberxavfsizlikni huquqiy ta’minlash” magistratura mutaxassisligini joriy etish belgilangan. Shuningdek, o‘quv jarayonini huquqbuzarliklar profilaktikasi, tezkor-qidiruv va ekspert-kriminalistika faoliyatlariga ixtisoslashgan holda dual ta’lim tizimi asosida tashkil etish nazarda tutilgan. Bu huquqni muhofaza qiluvchi organlar uchun nazariy bilim va amaliy ko‘nikmalarga ega bo‘lgan professional kadrlarni tayyorlashga xizmat qiladi.

Yuqoridagilarga ko‘ra quyidagi xulosaga kelish mumkin.

1. Kiberjinoyatchilik bugungi kunda nafaqat alohida shaxslar yoki tashkilotlarga, balki davlatning axborot xavfsizligi, moliyaviy barqarorligi va huquq-tartibot tizimiga bevosita tahdid soluvchi transmilliy xavf sifatida namoyon bo‘lmoqda. Shu sababli kiberjinoyatlarga qarshi kurashishda milliy qonunchilikni zamonaviy raqamli tahdidlarga moslashtirish, axborot texnologiyalari orqali sodir etiladigan jinoyatlar bo‘yicha alohida huquqiy tartibotlarni belgilash hamda “drop”lar, noqonuniy elektron operatsiyalar va kripto-aktivlar bilan bog‘liq huquqbuzarliklarga nisbatan javobgarlik choralarini kuchaytirish zarur.

2. Raqamli dalillar kiberjinoyatlarni fosh etish va tergov qilishda hal qiluvchi ahamiyat kasb etadi. Shu bois ularni aniqlash, olib qo‘yish, saqlash, tahlil qilish va sudda baholashning yagona protsessual mexanizmlarini joriy etish, “Raqamli dalillar yagona reyestri” kabi idoralararo tizimlarni rivojlantirish hamda raqamli kriminalistika imkoniyatlaridan keng foydalanish tergov samaradorligini oshirishning muhim sharti hisoblanadi.

3. Kiberjinoyatchilikka qarshi kurashish faqat jazolash choralari bilan cheklanmasdan, profilaktika, tezkor aniqlash, idoralararo axborot almashinuvi, bank va to‘lov tashkilotlari mas’uliyatini oshirish, xalqaro huquqiy hamkorlikni kuchaytirish hamda yuqori malakali mutaxassislar tayyorlash bilan uzviy bog‘liq holda amalga oshirilishi lozim. Aynan huquqiy, tashkiliy, texnik va kadrlar salohiyatini kompleks rivojlantirish orqali kiberjinoyatlarning oldini olish, ularni tezkor fosh etish va raqamli muhitda qonuniylikni ta’minlash mumkin bo‘ladi.

#

Serkan SAVAŞ,
Kırıkkale University, Türkiye. Associate Professor of Department of Computer Engineering, Faculty of Engineering and Natural Science, PhD

THE POTENTIAL AND APPLICATION AREAS OF ARTIFICIAL INTELLIGENCE IN THE EFFECTIVE FIGHT AGAINST CORRUPTION

ABSTRACT. *Corruption is a global problem that causes profound damage to the economic, cultural, and social structures of both developed and developing countries. This study examines the potential and application areas of artificial intelligence (AI) technologies in the fight against corruption. AI offers significant advantages in detecting and preventing corruption through techniques such as big data analysis, anomaly detection, natural language processing, and machine learning. The research highlights four key roles of AI in the fight against corruption: (1) Identifying irregularities in public tenders and financial transactions through data analysis and anomaly detection, (2) Real-time analysis of suspicious financial activities through fraud and money laundering detection, (3) Enabling proactive intervention through preventive measures and risk management, (4) Promoting citizen participation by increasing transparency and accountability. The study provides examples of successful AI applications in areas such as public procurement, tax auditing, personnel management, and document forgery detection. It also addresses the ethical, legal, and political dimensions of AI. Challenges such as data privacy, algorithmic bias, and accountability are critical to the responsible use of AI systems. In conclusion, while AI is a powerful tool in the fight against corruption, its effectiveness requires international cooperation, transparent policies, and strong legal frameworks. This study serves as a guide for future research and policy recommendations.*

ANNOTATSIYA. *Korrupsiya rivojlangan va rivojlanayotgan mamlakatlarning iqtisodiy, madaniy va ijtimoiy tuzilmalariga jiddiy zarar yetkazadigan global muammodir. Ushbu tadqiqot korrupsiyaga qarshi kurashda sun'iy intellekt (SI) texnologiyalarining potensiali va qo'llash sohalarini ko'rib chiqadi. SI katta ma'lumotlarni tahlil qilish, anomaliyalarni aniqlash, tabiiy tilni qayta ishlash va mashinani o'rgatish kabi usullar orqali korrupsiyani aniqlash va oldini olishda sezilarli afzalliklarni taklif etadi. Tadqiqot korrupsiyaga qarshi kurashda SIning to'rtta asosiy rolini ajratib ko'rsatadi: (1) ma'lumotlarni tahlil qilish va anomaliyalarni aniqlash orqali davlat xaridlari va moliyaviy operatsiyalardagi qoidabuzarliklarni aniqlash; (2) firibgarlik va pul yuvishni aniqlash orqali shubhali moliyaviy faoliyatni real vaqt rejimida tahlil qilish; (3) profilaktika choralari va xavflarni boshqarish orqali proaktiv aralashuvni ta'minlash; (4) shaffoflik va hisobdorlikni oshirish orqali fuqarolarning ishtirokini rag'batlantirish. Tadqiqot davlat xaridlari, soliq auditi, kadrlarni boshqarish va hujjatlar qalbakilashtirilishini aniqlash kabi sohalarda SIning muvaffaqiyatli qo'llanilishi misollarini taqdim etadi. Shuningdek, u SIning axloqiy, huquqiy va siyosiy jihatlarini ko'rib chiqadi. Ma'lumotlar maxfiyligi, algoritmik tarafkashlik va hisobdorlik kabi muammolar SI tizimlaridan mas'uliyat bilan foydalanish uchun hal qiluvchi ahamiyatga ega. Xulosa qilib aytganda, SI korrupsiyaga qarshi kurashda kuchli vosita bo'lsa-da, uning samaradorligi xalqaro hamkorlik, shaffof siyosat va mustahkam huquqiy bazani talab qiladi. Ushbu tadqiqot kelajakdagi tadqiqotlar va siyosat tavsiyalari uchun qo'llanma bo'lib xizmat qiladi.*

АННОТАЦИЯ. *Коррупция является глобальной проблемой, которая наносит серьезный ущерб экономическим, культурным и социальным структурам как развитых, так и развивающихся стран. Данное исследование рассматривает потенциал и области применения технологий искусственного интеллекта (ИИ) в борьбе с коррупцией. ИИ предлагает значительные преимущества в обнаружении и предотвращении коррупции с помощью таких методов, как анализ больших данных, обнаружение аномалий, обработка естественного языка и машинное обучение. Исследование выделяет четыре ключевые роли ИИ в борьбе с коррупцией: (1) Выявление нарушений в государственных закупках и финансовых транзакциях посредством анализа данных и обнаружения аномалий, (2) Анализ подозрительных финансовых операций в режиме реального времени посредством обнаружения мошенничества и отмывания денег, (3) Обеспечение проактивного вмешательства посредством превентивных мер и управления рисками, (4) Содействие участию граждан путем повышения прозрачности и подотчетности. Исследование приводит примеры успешного применения ИИ в таких областях, как государственные закупки, налоговый аудит, управление персоналом и обнаружение подделки документов. Оно также рассматривает этические, правовые и политические аспекты ИИ. Такие проблемы, как конфиденциальность данных, алгоритмическая предвзятость и подотчетность, имеют решающее значение для ответственного использования систем ИИ. В заключение, хотя ИИ является мощным инструментом в борьбе с коррупцией, его эффективность требует международного сотрудничества, прозрачной политики и прочных правовых рамок. Данное исследование служит руководством для будущих исследований и политических рекомендаций.*

Key words: *anti-corruption, artificial intelligence, transparency, anomaly detection, data analysis.*

Kalit so'zlar: *korrupsiyaga qarshi kurash, sun'iy intellekt, shaffoflik, anomaliyalarni aniqlash, ma'lumotlarni tahlil qilish.*

Ключевые слова: *борьба с коррупцией, искусственный интеллект, прозрачность, обнаружение аномалий, анализ данных.*

1. Introduction

Corruption is defined in the dictionary as "abuse of power or authority; irregularity"[1]. Corruption is a widespread problem in both developed and developing countries, and it causes deep damage to economic, cultural, and social structures for various reasons. Corruption is a problem encountered all over the world, and as shown in Figure 1, the Corruption Perceptions Index (CPI) varies from country to country[2].

1 Türk Dil Kurumu Sözlükleri [Online resource] / Türk Dil Kurumu. — URL: https://sozluk.gov.tr/ (date of access: 21.05.2026).

2 Corruption Perceptions Index 2024 // Transparency International [Online resource]. – 2024. – URL: https://www.transparency.org/en/cpi/2024 (date of access: 21.04.2026).

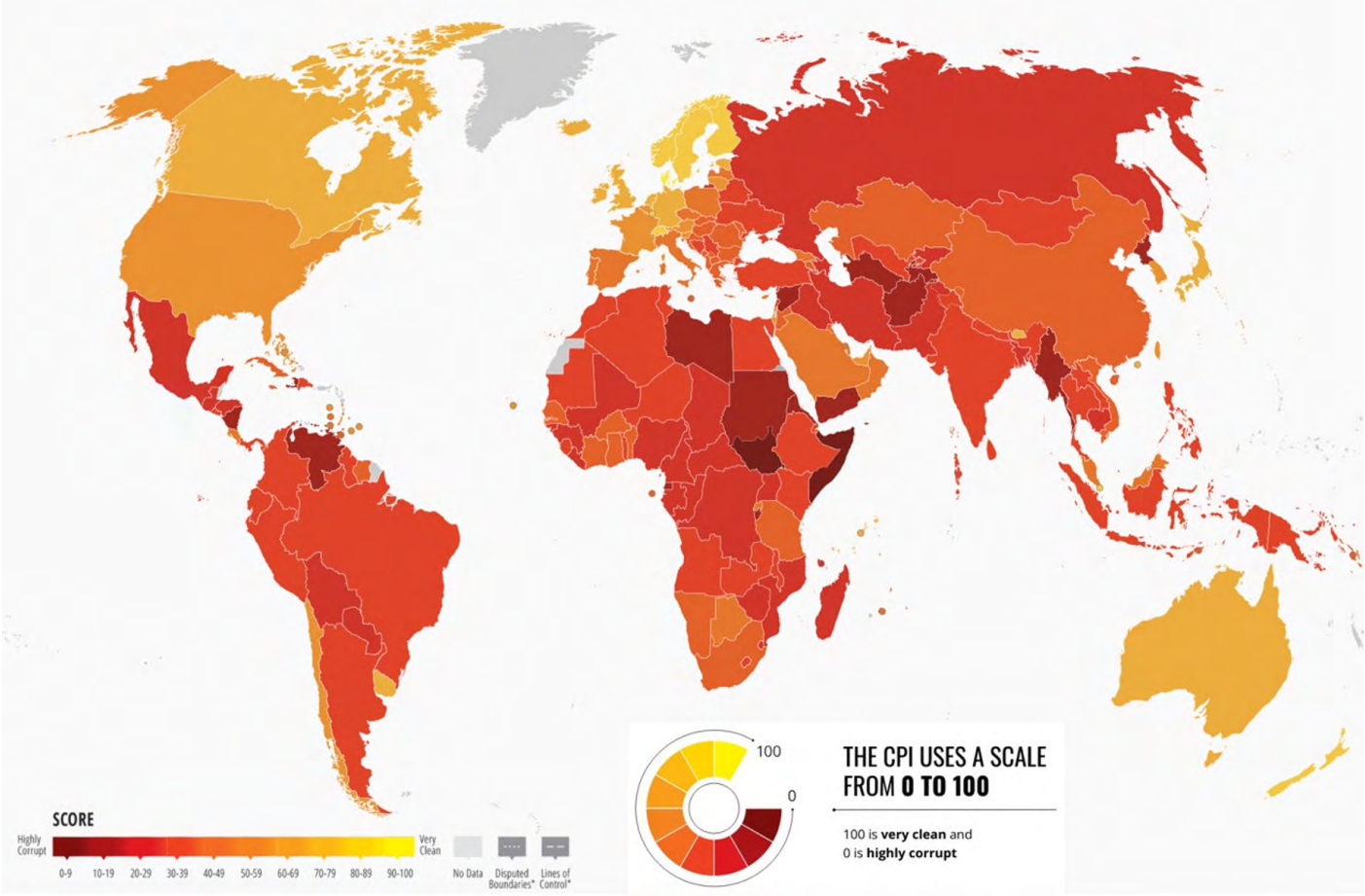


Figure 1. The 2024 Corruption Perceptions Index (CPI). Transparency International is licensed under CC-BYND 4.0. Image Disclaimer: The designations employed and the presentation of material on Transparency International maps showing disputed boundaries and lines of control follow the UN practice to the best of our knowledge and as of January 2023. They do not imply the expression of any opinion on the part of Transparency International concerning the legal status of any country, territory, city or area or of its authorities or concerning the delimitation of its frontiers or boundaries. Maps of Kosovo are without prejudice to positions on status and are in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence[3].

The CPI, obtained as a result of the research shown in Figure 1, ranks 180 countries and regions worldwide according to the level of perceived corruption in the public sector. The CPI is the most widely used global corruption ranking in the world. According to experts and businesspeople, it measures the perception of how corrupt each country's public sector is. Each country's score is based on a combination of at least three data sources from 13 different corruption surveys and assessments. These data sources are collected by various reputable institutions such as the World Bank and the World Economic Forum. The results are presented on a scale from 0 (high level of corruption) to 100 (very clean). While 32 countries have significantly reduced their corruption levels since 2012, 148 countries have remained at the same level or deteriorated during the same period. The global average is 43. While this rate has remained at the same level for many years, more than two-thirds of countries score below 50. Changes in the corruption perception index for Türkiye and Uzbekistan are shown in Figure 2, respectively[4].

3 Corruption Perceptions Index 2024 // Transparency International [Online resource]. – 2024. – URL: https://www.transparency.org/en/cpi/2024 (date of access: 21.04.2026).

4 Corruption Perceptions Index 2024 // Transparency International [Online resource]. – 2024. – URL: https://www.transparency.org/en/cpi/2024 (date of access: 21.04.2026).

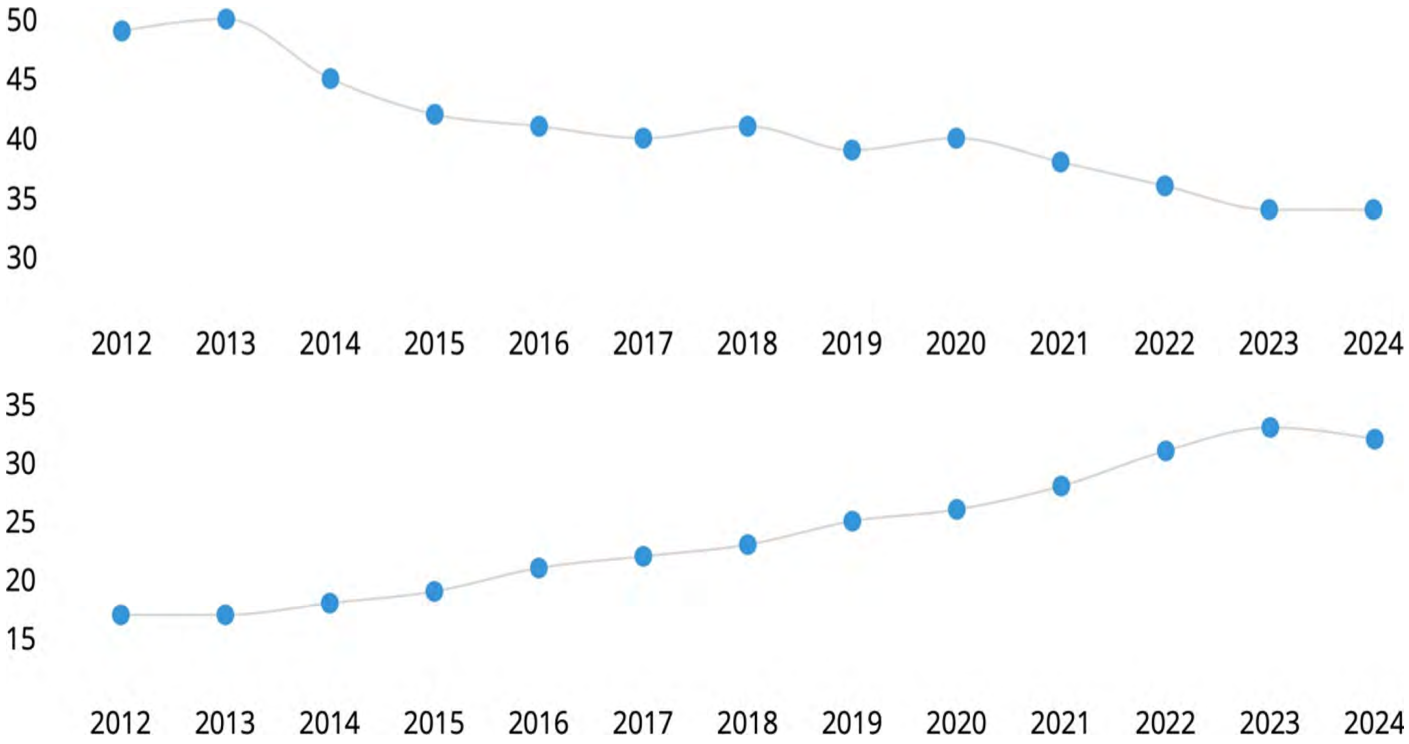


Figure 2. Change in corruption expectations index between 2012 and 2024 (a) Türkiye, (b) Uzbekistan[5].

When examining Türkiye's 2024 CPI data in Figure 2, it can be seen that it has an index of 34 out of 100. With this score, Türkiye ranks 107th among the 180 countries included in the dataset. There has been no change between Türkiye's 2023 and 2024 data. Uzbekistan has an index of 32. With this index value, it ranks 121st among 180 countries. Uzbekistan's score has changed by -1 between 2023 and 2024[6].

Corruption is a multifaceted problem that can manifest itself in various forms. The main types of corruption include bribery, embezzlement, fraud, extortion, and favoritism. Structurally, corruption can be divided into two main categories: political and bureaucratic-judicial corruption. Political corruption involves the benefits obtained by high-level decision-makers through large contracts and large-scale bribery aimed at influencing policy processes. In contrast, bureaucratic and judicial corruption refers to corruption that arises during daily transactions between public officials and citizens and during the implementation of existing policies[7] In addition to these, there are various forms of corruption such as black-market trading, collusion, fraud, kickbacks, match fixing, money laundering, bribery funds, tax evasion, and offshore investments.

Corruption is a global phenomenon that causes poverty, hinders development, and deters investment. It also weakens judicial and political systems that are supposed to work for the public good. As the rule of law weakens and the voice of the people goes unheard, citizens' trust in government officials and national institutions also declines[8]. For this reason, various methods are being used, and steps are being taken to combat corruption today. Legal and institutional reforms are one such method, involving the strengthening of laws, regulations, and institutions to detect, prevent, and punish corruption. Initiatives such as anti-corruption agencies, independent judiciary, and whistleblower protection laws are

5 Corruption Perceptions Index 2024 // Transparency International [Online resource]. – 2024. – URL: https://www.transparency.org/en/cpi/2024 (date of access: 21.04.2026).

6 Corruption Perceptions Index 2024 // Transparency International [Online resource]. – 2024. – URL: https://www.transparency.org/en/cpi/2024 (date of access: 21.04.2026).

7 Berksoy T., Yıldırım N. E. Yolsuzluk Kavramına Genel Bir Bakış: Problemler ve Çözüm Önerileri // Journal of Awareness (JoA). – 2017. – Vol. 2, No. 1. – P. 1–18.; Swaleheen M. Economic growth with endogenous corruption: an empirical study // Public Choice. – 2011. – Vol. 146, No. 1. – P. 23–41. – DOI: 10.1007/s11127-009-9581-1.

8 Countering the global problem of corruption // United Nations Office on Drugs and Crime [Online resource]. – 2006. – URL: https://www.unodc.org/newsletter/200601/page004.html (date of access: 21.04.2026).

being implemented within this scope[9]. Another method is transparency and open government practices. In this context, it is recommended that transparency in government activities be encouraged to reduce opportunities for corruption. Initiatives such as transparency in public procurement, open data portals, budget transparency, and freedom of information laws are examples of practices that are in line with this method[10]. E-government applications and digital tools are other methods used to combat corruption. These applications involve the use of technology to reduce face-to-face interactions, automate processes, and increase traceability. This method includes many digital applications, from online tax returns to e-auction systems, digital land registry records, and blockchain transactions for public contracts[11]. Efforts to combat corruption are also being carried out through civil society and media participation. These efforts include combating corruption by supporting civil society organizations, investigative journalism, and citizen participation to expose and suppress corrupt practices[12]. Another method of combating corruption is to promote honesty in public administration through honesty pacts, ethics commissions, and values-based education, as well as through ethics training and codes of conduct[13]. Another method of combating corruption is through international agreements and peer pressure. In this context, participation in international frameworks and agreements for combating cross-border corruption is being implemented. The United Nations Convention against Corruption (UNCAC), the OECD Anti-Bribery Convention, and FATF (Financial Action Task Force) regulations are among these[14]. Efforts are also being made to combat corruption through merit-based bureaucratic reforms or public financial management reforms. Thus, while the aim is to reduce discretionary power in public employment and promotions and to professionalize public services, the goal is also to strengthen budget systems, audits, and financial controls[15].

The fight against corruption has recently begun to benefit from innovative technologies. Artificial intelligence (AI) applications, which are becoming widely used in all disciplines and are beginning to yield successful results, have also begun to offer opportunities in the fight against corruption. AI is defined as the ability to mimic human-like intelligence processes in machines and is currently creating transformation in many sectors, particularly education, healthcare, transportation, and defense[16]. AI is not just a single technology; it has a wide range of applications supported by numerous sub-technologies such as machine learning (ML), deep learning (DL), computer vision (CV), natural language processing (NLP), and big data analytics. ML consists of algorithms that enable predictions by learning patterns from data, while DL is a more com-

9 Meagher P. Anti-corruption agencies: Rhetoric versus reality // The Journal of Policy Reform. – 2005. – Vol. 8, No. 1. – P. 69–103. – DOI: 10.1080/1384128042000328950.; Rose-Ackerman S., Palifka B. J. Corruption and Government: Causes, Consequences, and Reform. – Cambridge: Cambridge University Press, 2016. – DOI: 10.1017/CBO9781139962933.

10 Bauhr M., Grimes M. Indignation or Resignation: The Implications of Transparency for Societal Accountability // Governance. – 2014. – Vol. 27, No. 2. – P. 291–320. – DOI: 10.1111/gove.12033.; Fox J. The Uncertain Relationship between Transparency and Accountability // Development in Practice. – 2007. – Vol. 17, No. 4/5. – P. 663–671. – URL: http://www.jstor.org/stable/25548267 (date of access: 21.04.2026).

11 Andersen T. B. E-Government as an anti-corruption strategy // Information Economics and Policy. – 2009. – Vol. 21, No. 3. – P. 201–210. – DOI: 10.1016/j.infoecopol.2008.11.003.; e-Devlet Kapısı. Official website [Online resource]. – 2025. – URL: https://www.turkiye.gov.tr/ (date of access: 21.04.2026).

12 Grimes M. The Contingencies of Societal Accountability: Examining the Link Between Civil Society and Good Government // Studies in Comparative International Development. – 2013. – Vol. 48, No. 4. – P. 380–402. – DOI: 10.1007/s12116-012-9126-3.; The Media's Role in Curbing Corruption. – Washington, D.C.: World Bank Group, 2000. – URL: https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/893191468766225068/the-medias-role-in-curbing-corruption (date of access: 21.04.2026).

13 Huberts L. W. J. C. Integrity: What it is and Why it is Important // Public Integrity. – 2018. – Vol. 20, Suppl. 1. – P. S18–S32. – DOI: 10.1080/10999922.2018.1477404.; Maesschalck J., Bertok J. Towards a Sound Integrity Framework: Instruments, Processes, Structures and Conditions for Implementation // SSRN Electronic Journal. – 2009.

14 United Nations Convention against Corruption. – New York: United Nations Office on Drugs and Crime, 2004.

15 Andrews M. The Limits of Institutional Reform in Development. – Cambridge: Cambridge University Press, 2013. – DOI: 10.1017/CBO9781139060974.; Dahlström C., Lapuente V., Teorell J. The Merit of Meritocratization: Politics, Bureaucracy, and the Institutional Deterrents of Corruption // Political Research Quarterly. – 2012. – Vol. 65, No. 3. – P. 656–668. – DOI: 10.1177/1065912911408109.

16 Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – 4th ed. – Harlow: Pearson, 2020.

plex form of this approach developed with artificial neural networks[17]. NLP, which has become more popular thanks to generative AI technologies[18], involves machines' ability to understand, produce, and interpret human language. This creates a wide range of applications, from text analysis to translation systems.

The development of AI technologies has gained momentum alongside big data analytics; in particular, the ability to process high-volume, diverse, and fast-moving data has increased the accuracy and effectiveness of AI systems[19]. When combined, these technologies enable the development of intelligent systems that go beyond traditional software systems and offer autonomous decision-making capabilities. Therefore, AI should be considered not only as an engineering field but also as a strategic technology that shapes the transformation of contemporary societies. Due to these capabilities, it also offers great potential in the fight against corruption.

Thanks to AI, more effective, faster, and scalable solutions can be offered in the fight against corruption, going beyond traditional control and monitoring mechanisms. While traditional methods often rely on manual control, complaint mechanisms, and retrospective investigations, AI-based systems can detect suspicious transactions in advance by performing real-time analyses on large data sets[20]. ML algorithms have made it easier to analyze patterns in complex data sets such as public tenders, budget expenditures, and tender data, enabling anomalies that might escape human observation to be identified more quickly and accurately. Thus, AI technologies can be used not only to detect corruption but also to carry out useful work in creating preventive mechanisms.

Thanks to its scalability, AI can overcome the time and resource constraints faced by human inspectors when processing large and multidimensional data much more effectively. In addition, with NLP technologies, traces of unethical behavior can be analyzed more systematically and dynamically through public officials' communication records, documents, or social media content. Thanks to the recent proliferation of explainable artificial intelligence (XAI) studies, it has become possible to establish more transparent and accountable management systems in the fight against corruption. For these technologies to be successful, complementary elements such as access to accurate data, ethical use principles, and strengthening institutional capacity must also be taken into consideration[21].

Based on this, this study aims to explain the potential, opportunities, and advantages of AI technologies in the fight against corruption, as well as their areas of application. In addition, the ethical, legal, and political dimensions that need to be considered in this context are also discussed. Various studies in the literature are discussed, and recommendations for the future are made. The study aims to serve as a guide for future research on AI in the fight against corruption.

2. The Role of Artificial Intelligence in Combating Corruption

The roles of AI in the fight against corruption can be explained from different perspectives. The studies conducted in this research were clustered according to their purpose and examined under four different subheadings. In addition, the opportunities and advantages of using AI in the fight against corruption are also discussed in this section.

2.1. Data Analysis and Anomaly Detection

Algorithms are at the heart of AI studies, and the raw material used by these algorithms is data. Therefore, data analysis is also very important in the fight against corruption. AI, especial-

17 Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge, MA: MIT Press, 2016.

18 Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative Adversarial Nets // Advances in Neural Information Processing Systems / eds. Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, K. Q. Weinberger. – 2014. – Vol. 27. – URL: https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf (date of access: 21.04.2026).

19 Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. – Boston: Houghton Mifflin Harcourt, 2013.

20 Wirtz B. W., Weyerer J. C., Geyer C. Artificial Intelligence and the Public Sector—Applications and Challenges // International Journal of Public Administration. – 2019. – Vol. 42, No. 7. – P. 596–615. – DOI: 10.1080/01900692.2018.1498103.

21 Meske C., Bunde E., Schneider J., Gersch M. Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities // Information Systems Management. – 2022. – Vol. 39, No. 1. – P. 53–63. – DOI: 10.1080/10580530.2020.1849465.

ly through data analysis, enables auditing, prediction, and early warning systems, providing the opportunity to enrich data-based methods. This is where approaches and disciplines such as data mining, big data, and anomaly detection come into play. Thanks to these techniques, it has become possible to perform automatic analyses on multi-dimensional and high-volume data sets such as public expenditures, tender processes, financial transactions, and company records. Through algorithms, anomalies can be identified, and various detections can be made, such as excessive price fluctuations, different pricing for similar items, and continuous tenders awarded to the same supplier[22]. These findings can also be used to identify areas of risk in the future. Predictive analytics can enable proactive measures to be taken in high-risk sectors, thereby serving as a kind of predictive measure[23].

Thanks to recent advances in AI tools, particularly large language models (LLMs), document analysis has become more accessible and accurate. As a result, many tasks can now be performed using NLP techniques, such as examining public documents such as contracts and legal texts, reviewing legal documents, identifying ambiguous expressions, and determining implicit provisions. Text mining, another NLP technique, also holds potential in the fight against corruption. When data obtained from platforms such as public complaint forms, media news, and website forms is subjected to text mining processes using AI techniques, it will be possible to obtain automatic sentiment analysis, complaint analysis, and user opinions from this data. This will enable solutions to be produced quickly and effectively.

AI-supported network analysis is another potential technique that enables the comprehensive modeling of relationships at the personal and institutional levels in the fight against corruption. Financial, legal, or communication-based relationships between public institutions, companies, individuals, and suppliers can be analyzed graphically, and suspicious connections or conflicts of interest can be detected through AI[24]. These techniques have been shown to be effective in unraveling the complex web of international relationships revealed in documents such as the Panama Papers[25]. In this context, AI automatically identifies central actors, intermediary structures, and hidden connections within multi-node networks, thereby enabling the illumination of risk areas that cannot be reached through traditional control methods.

Social network analysis considers not only the visible connections between individuals and organizations, but also the patterns that emerge over time[26]. These analyses make it possible to identify close ties between public officials or decision-makers and certain interest groups, hidden trends in tender distribution, or capital flows within the same structures. Thus, unethical situations such as conflicts of interest, abuse of position, and insider information leaks can be detected at an early stage before they even arise. These technologies have become important components in the establishment of transparency, accountability, and preventive governance mechanisms, particularly in public administration.

2.2. Fraud and Money Laundering Detection

Another potential benefit of AI is innovative solutions for understanding the complex structure of financial systems in the detection of fraud and money laundering. In financial monitoring processes, AI- based algorithms perform real-time analysis on millions of transactions to

22 Köbis N., Starke C., Rahwan I. Artificial Intelligence as an Anti-Corruption Tool (AI-ACT): Potentials and Pitfalls for Top-down and Bottom-up Approaches [Online resource]. – 2021. – URL: https://arxiv.org/pdf/2102.11567 (date of access: 21.04.2026).; Wirtz B. W., Weyerer J. C., Geyer C. Artificial Intelligence and the Public Sector—Applications and Challenges // International Journal of Public Administration. – 2019. – Vol. 42, No. 7. – P. 596–615. – DOI: 10.1080/01900692.2018.1498103.

23 Bertot J. C., Jaeger P. T., Grimes J. M. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies // Government Information Quarterly. – 2010. – Vol. 27, No. 3. – P. 264–271. – DOI: 10.1016/j.giq.2010.03.001.

24 Krempel L. Network Visualization // The SAGE Handbook of Social Network Analysis / eds. J. Scott, P. J. Carrington. – London: SAGE, 2009.

25 Joaristi M., Serra E., Spezzano F. Inferring Bad Entities Through the Panama Papers Network // 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). – 2018. – P. 767–773. – DOI: 10.1109/ASONAM.2018.8508497.; Zhuhadar L., Ciampa M. Leveraging learning innovations in cognitive computing with massive data sets: Using the offshore Panama Papers leak to discover patterns // Computers in Human Behavior. – 2019. – Vol. 92. – P. 507–518. – DOI: 10.1016/j.chb.2017.12.013.

26 Savaş S., Topaloğlu N. Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri // ISCTURKEY 2015: VIII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. – 2015. – P. 62–69.

detect suspicious activities (anomaly detection). For example, anomaly detection algorithms used in the banking sector can flag sudden and large-scale transactions that are inconsistent with a customer's past spending habits as red flags[27]. In addition, AI systems analyze transaction networks to identify risky movements through complex connections and implicit relationships to detect terrorist financing. For example, HSBC has been conducting AI-supported financial crime detection since 2021. The bank checks approximately 1.35 billion transactions per month across 40 million customer accounts for signs of financial crime and uses AI to assist in this process[28].

AI can analyze the accuracy of documents (IDs, invoices, etc.) submitted during customer registration processes, prevent the use of fake IDs by using biometric data (face recognition), and quickly identify inconsistencies or potential fraud indicators (e.g., multiple accounts opened with the same address or phone number) in the data submitted during new account openings or credit applications. As such fraudulent activities have become more prevalent in recent times, AI algorithms can help prevent them. Another risk is the use of mobile devices by others for fraudulent purposes. Thanks to AI, behavioral data such as user device interactions, typing speeds, mouse movements, or location information can be analyzed to detect unauthorized access or account takeover attempts. For example, deviations from a user's typical login behavior (access from a different location, abnormal keyboard usage) can be interpreted as a fraud attempt.

Tax audit processes are one of the areas where AI is most effectively used in finance. AI can detect anomalies that may indicate tax evasion by cross-checking millions of tax returns and financial reports. Modern tax audit systems use big data analysis and ML techniques to identify inconsistencies among taxpayers. These systems process millions of tax returns simultaneously to identify suspicious patterns[29]. AI-based systems analyze taxpayers' income statements and commercial reports from different years to assess trends and inconsistencies. This allows tax auditors to focus on high-risk groups and conduct more effective audits. For example, if there are significant discrepancies between a company's reported income and its bank account transactions or supplier invoices, AI can flag this as a risk. Additionally, AI technologies combined with big data analytics can also identify smuggling activities conducted through international trade and offshore accounts[30].

In traditional audits, tax auditors typically work with limited resources and identify taxpayers to be audited using manual methods. AI analyzes factors such as past audit results, industry data, economic indicators, and taxpayer behavior patterns to identify taxpayers or industries with the highest risk of tax evasion. This allows audit resources to be used in a more targeted and efficient manner, thereby achieving higher success rates in the fight against corruption[31]. AI can detect fake or manipulated documents by digitizing invoices, receipts, and other financial documents using optical character recognition (OCR) technology and then analyzing their content. For example, the use of the same invoice by multiple taxpayers, anomalies in invoice numbers, or unusual document formats can be flagged by AI[32].

2.3. Preventive Measures and Risk Management

Another potential offered by AI is to play a key role in preventive measures and risk management

27 Ngai E. W. T., Hu Y., Wong Y. H., Chen Y., Sun X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature // Decision Support Systems. – 2011. – Vol. 50. – P. 559–569. – DOI: 10.1016/j.dss.2010.08.006.

28 Calvery J. Harnessing the power of AI to fight financial crime [Online resource]. – 2025. – URL: https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime (date of access: 21.04.2026).

29 De Roux D., Pérez B., Moreno A., Villamil M. del P., Figueroa C. Tax fraud detection for under-reporting declarations using an unsupervised machine learning approach // Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2018. – P. 215–222. – DOI: 10.1145/3219819.3219878.

30 Fille M. B., Dominique H., Joseph N., Francis K., Ignace K. Predicting tax fraud using supervised machine learning approach // African Journal of Science, Technology, Innovation and Development. – 2023. – Vol. 15, No. 6. – P. 731–742. – DOI: 10.1080/20421338.2023.2187930.

31 Muthalagu R., Malik J., Pawar P. M. Detection and prevention of evasion attacks on machine learning models // Expert Systems with Applications. – 2025. – Vol. 266. – Art. 126044. – DOI: 10.1016/j.eswa.2024.126044.

32 Nuryani N., Mutiara A. B., Wiryana I. M., Purnamasari D., Putra S. N. W. Artificial Intelligence Model for Detecting Tax Evasion Involving Complex Network Schemes // Aptisi Transactions on Technopreneurship. – 2024. – Vol. 6. – DOI: 10.34306/att.v6i3.436.

strategies that enable intervention before corruption occurs. Thanks to its big data analysis capabilities, AI has the potential to be much more effective and efficient in combating corruption by identifying potential risks in advance and enabling proactive measures to be taken.

Corruption usually occurs under certain conditions or when certain system weaknesses exist[33]. Analyzing these conditions and vulnerabilities and creating powerful risk models that predict future corruption risks has now become a solvable problem for AI algorithms. Thanks to the ML models created, the foundations for anti-corruption strategies can be laid for public institutions, private sector organizations, and even non-governmental organizations. A flowchart like the one in Figure 3 can be created for these models.

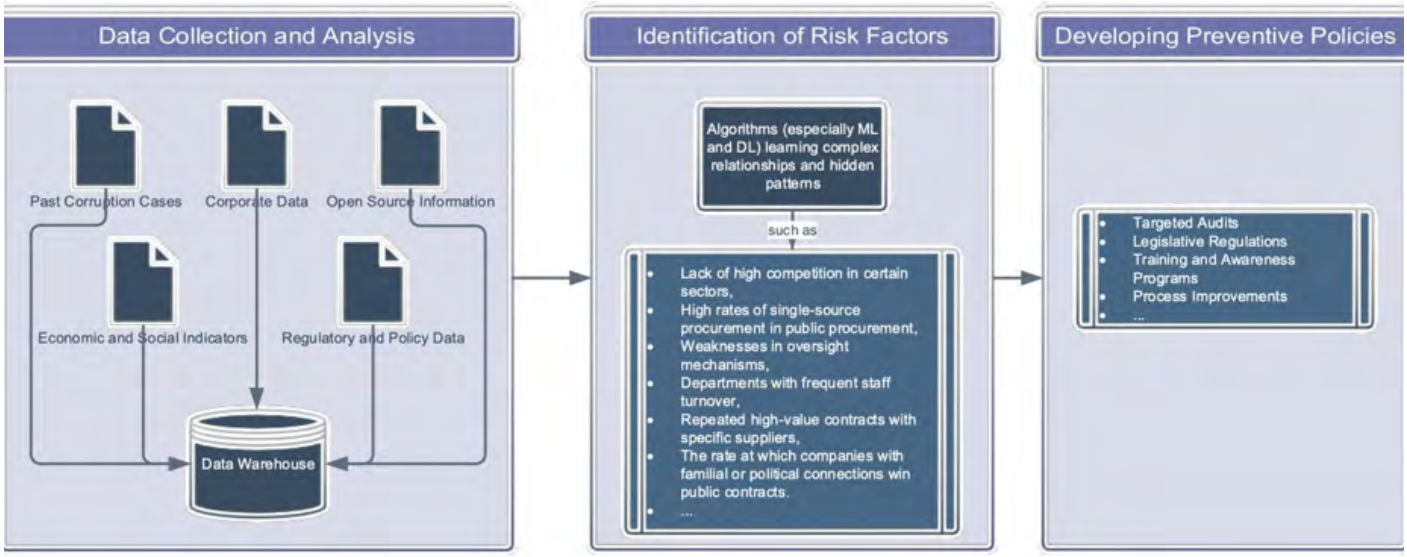


Figure 3. Steps for applying AI in anti-corruption and risk management

As shown in Figure 3, the AI-supported anti-corruption process operates in three main stages: First, heterogeneous data sets such as past corruption cases, corporate data (tenders, budget expenditures, internal audit reports), macroeconomic indicators, legislation analyses, and open-source data are systematically collected and structured. Next, ML and DL algorithms analyze this data to uncover complex patterns associated with corruption risk (e.g., single-source tenders, audit weaknesses, politically connected companies) and develop risk scoring models. In the final stage, these models optimize resource allocation and strengthen proactive mechanisms by providing policymakers with evidence-based preventive strategies such as targeted audits, regulatory improvements, ethics training programs, and process optimizations. This process aims to increase transparency and accountability in the prevention of corruption through data-driven decision-making.

Risk models show general trends and potential risk areas, while automated alert systems instantly detect suspicious situations and directly notify authorities. These systems play a critical role in preventing corruption from reaching a larger scale or spreading. AI-supported automatic alert systems for risk management are an innovative technology that strengthens early warning and intervention mechanisms in the fight against corruption. These systems facilitate time-sensitive decision-making by sending automatic notifications to authorities when they detect suspicious behavior or transactions. Such systems go beyond the limitations of manual monitoring in detecting corruption. Automatic alert systems are of critical importance, especially in areas where there are very large volumes of data. The financial sector is one such area. Here, AI algorithms reduce the burden of oversight, creating opportunities to focus human

33 De Graaf G. Causes of Corruption: Towards a Contextual Theory of Corruption // Public Administration Quarterly. – 2007. – Vol. 31, No. 1/2. – P. 39–86. – URL: http://www.jstor.org/stable/41288282 (date of access: 21.04.2026).

resources on more complex and analytical decision-making processes. Various technologies can be used in these systems. These can be structured in many ways, from rule-based systems to real-time monitoring, anomaly detection, and risk mapping.

2.4. Transparency and Accountability

Transparency and accountability are among the most important elements in the fight against corruption. AI has the potential to provide support in these areas as well. Public institutions are structures that operate with taxes paid by citizens and provide public services[34]. Transparent disclosure of data such as the financial activities, tender processes, budget expenditures, and asset declarations of these institutions reduces the risk of corruption and facilitates citizen oversight. However, raw data is often very large, complex, and difficult to understand. This is where AI comes in, transforming raw data into meaningful and accessible information, making it one of the most important actors in transparency.

AI can use big data and visualization methods to instantly generate answers to many questions and problems. It can also shed light on many issues in public institutions' financial processes, such as recurring suppliers, anomalies in bids, process violations, and the identification of affiliated companies.

Thanks to AI, citizen participation in administrative processes becomes more feasible. It has become possible to comprehensively address reporting mechanisms; process data obtained from different data sources together and ensure accountability by conducting the process in a more transparent manner. In recent years, developments in NLP techniques have also made it possible for AI algorithms to evaluate reports from different sources and perform relational analyses.

2.5. Opportunities and Advantages Brought by Artificial Intelligence

The use of AI technologies in various fields brings with it many opportunities and advantages. There are also limitations and disadvantages, which will be discussed in the section on ethical and legal dimensions. The opportunities and advantages offered using AI in the fight against corruption can be examined in several sub-items.

Firstly, from the perspective of "efficiency and speed," AI algorithms analyze large data sets that exceed human capacity in seconds, offering significant time savings compared to traditional audit processes. Tasks that would take weeks to complete manually can be completed in a much shorter time. This saves time and provides a significant advantage in the fight against corruption.

"Objectivity" is another opportunity offered by AI. ML algorithms can provide impartial and objective analyses by making decisions based entirely on data, without being influenced by human biases or emotional factors. This enables more fair and reliable results to be obtained. The absence of human bias is an advantage here, but it should be noted that bias can also arise in machines depending on the data set.

Another opportunity offered by AI is the "detection of hidden patterns." Patterns that are not visible to the human eye at first glance can be detected by AI algorithms, thus providing an advantage in combating corruption that has been overlooked or hidden.

"Resource optimization" can also be mentioned as an opportunity offered by AI. The most efficient use of limited audit and investigation resources is of critical importance. AI ensures that resources are directed to the areas with the highest risk of corruption by accurately targeting risky areas, transaction groups, or individuals. It also offers advantages to auditors by performing much more than what can be done with a limited number of personnel.

The "early warning system" is one of the most important opportunities AI offers in the fight against corruption. This allows corruption to be detected at the earliest stage and prevented before it causes greater damage. This provides a vital advantage in preventing corruption by offering the possibility of proactive intervention.

Finally, the opportunity for "comprehensive analysis" can also be mentioned. AI can perform in-depth and holistic analysis by processing very large and diverse data sets simultaneously, which

34 Pratt D. What Are Public Institutions? // Fairness, Globalization, and Public Institutions. – 2006. – P. 35.

is not possible with traditional methods. This advantage makes it possible to understand all dimensions of corruption and develop effective countermeasures.

3. Application Areas and Examples

This section discusses areas of application where AI techniques can be used to combat corruption (Figure 4). Examples of its use in different countries are also provided.

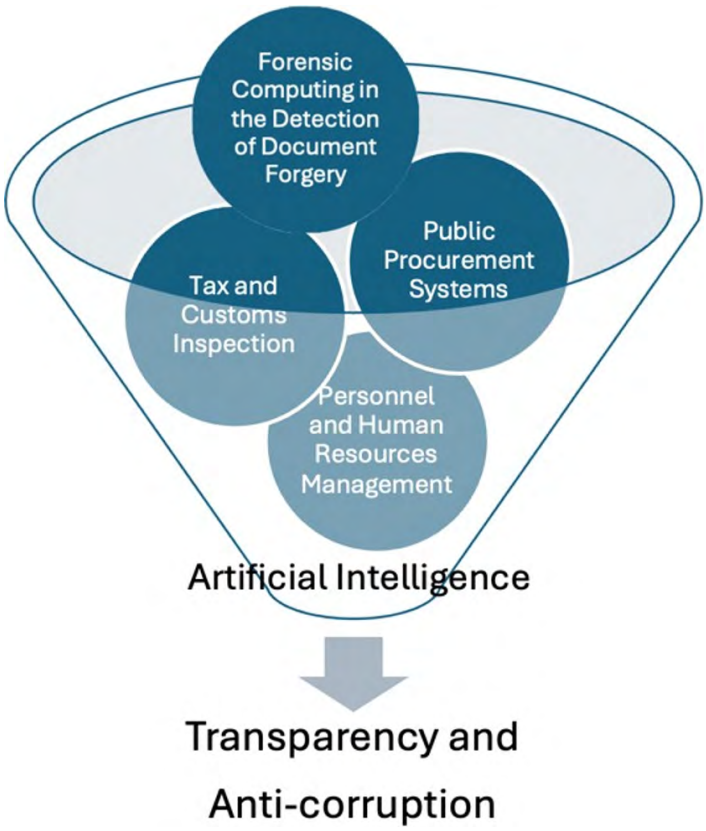


Figure 4. Areas of application in the fight against corruption

3.1. Artificial Intelligence Applications in Public Procurement Systems

Public procurement is one of the areas with the highest risk of corruption since it accounts for a significant portion of government spending and involves large sums of money. Traditional audit methods may be insufficient in the face of the complexity of procurement processes, the large volume of data, and the increasing sophistication of corruption methods. In these processes, AI can play an important role in both increasing transparency and preventing potential corruption through big data analytics and ML algorithms. AI-based systems used in tender processes can identify potential conflicts of interest by analyzing the relationships between bidding companies. They also have the capacity to detect potential irregularities, anti-competitive behavior, and conflicts of interest by analyzing tender data.

AI has also made it possible to scan tender documents using NLP techniques to detect manipulative statements or customized specifications. This method enables the automatic identification of restrictive conditions (e.g., unnecessary technical specifications) that have been prepared in favor of a particular company. Furthermore, supplier network analysis can reveal the tendency of interconnected companies to participate in the same tenders. Such analyses are effective in detecting cartel formation or nepotism cases[35].

Another application of AI in public procurement systems is data analysis and anomaly detection. AI models can automatically identify situations that deviate from the norm or match predefined risk indicators by analyzing large amounts of procurement data (bids, contracts, company profiles, tender specifications, payment records, etc.). For example, situations such as bids from companies participating in a tender being abnormally close to each other, a particular company consistently winning tenders, a tender being awarded to a single company, or the tender period being unusually short can be flagged as suspicious by AI algorithms. Additionally, AI can combine different datasets to identify potential connections between relevant public officials and the companies that win tenders (such as shared addresses, board memberships, or family ties), thereby uncovering potential conflicts of interest[36].

3.2. Artificial Intelligence Applications in Tax and Customs Auditing

Tax and customs control is of great importance

35 Wallimann H., Imhof D., Huber M. A Machine Learning Approach for Flagging Incomplete Bid-Rigging Cartels // Computational Economics. – 2023. – Vol. 62, No. 4. – P. 1669–1720. – DOI: 10.1007/s10614-022-10315-w.

36 Torres Berru Y., López Batista V. F., Torres-Carrión P., Jimenez M. G. Artificial Intelligence Techniques to Detect and Prevent Corruption in Procurement: A Systematic Literature Review // Applied Technologies / eds. M. Botto-Tobar et al. – Cham: Springer International Publishing, 2020. – P. 254–268.

in terms of securing state revenue sources and preventing illegal commercial activities. Tax evasion and customs fraud are significant forms of corruption that cause serious erosion of state revenues worldwide, threatening economic stability and creating an unfair competitive environment. The complex processes and large volumes of data in these areas are becoming increasingly difficult to effectively audit using traditional methods. ML algorithms can identify inconsistencies and abnormal patterns in tax returns, operating with a much higher accuracy rate compared to traditional methods[37]. AI algorithms can analyze large amounts of financial data to uncover suspicious transaction patterns. For example, cross-check analyses of tax returns are commonly used to detect anomalies or inconsistencies in income declarations[38].

AI also plays a critical role in combating fraud and smuggling in customs inspections. These systems cross-verify and analyze large datasets from various sources, such as bank transactions, e-commerce records, social media data, and past customs declarations, to identify tax evasion, customs fraud, and tax and customs losses resulting from unauthorized goods sales. In customs operations, AI automatically analyzes documents such as import/export declarations, loading manifests, and market prices to identify risky shipments, counterfeit products, or undervalued declarations, while machine learning algorithms predict the likelihood of fraudulent declarations. This integrated approach not only makes audit processes more effective by detecting irregularities but also improves the international trade environment and increases compliance rates by shortening shipment customs clearance times and reducing costs.

According to a technical report by the International Monetary Fund (IMF), the use of AI in tax and customs administrations means more effective fraud detection, improved compliance rates, and more personalized services for both taxpayers and foreign trade operators. The integration of AI into customs processes significantly reduces shipment customs clearance times, lowers costs, accelerates product transportation, and improves the international trade environment[39].

3.3. Artificial Intelligence Applications in Personnel and Human Resources Management

Personnel and human resources processes, particularly stages such as recruitment, promotion, and performance evaluation, are areas where there is a high risk of favoritism, nepotism, and political patronage. When recruitment processes are shaped by personal relationships or discriminatory criteria rather than individual qualifications, this results in a violation of the principle of meritocracy and a decline in organizational efficiency. Such corruption undermines the principle of meritocracy in the public sector, lowering service quality, while in the private sector, it leads to unfair competition and inefficiency.

Detecting such situations using traditional methods is quite difficult due to subjective decisions and limited human oversight. Personnel recruitment processes in the public and private sectors represent one of the areas with the highest potential for AI technologies to increase meritocracy and prevent favoritism. For example, AI-based systems can eliminate personal biases from hiring decisions by automatically evaluating qualifications in resumes or analyzing patterns in hiring processes to reveal systematic exclusion or discrimination against certain demographic groups. For example, an organization may identify that a particular gender or ethnic group is consistently at a disadvantage. Such analyses are made possible by reviewing past hiring decisions[40]. This makes it possible to implement reforms within the organization and restructure recruitment processes. In addition, making deci-

37 Tax Administration 3.0: The Digital Transformation of Tax Administration. – Paris: OECD Publishing, 2020. – URL: https://www.oecd.org/en/publications/tax-administration-3-0-the-digital-transformation-of-tax-administration_ca274cc5-en.html (date of access: 21.04.2026).

38 Belahouaoui R., Attak E. H. Digital taxation, artificial intelligence and Tax Administration 3.0: improving tax compliance behavior – a systematic literature review using textometry (2016–2023) // Accounting Research Journal. – 2024. – Vol. 37. – P. 172–191. – DOI: 10.1108/ARJ-12-2023-0372.

39 Aslett J., Hamilton S., Gonzalez I., Hadwick D., Hardy M. A. Understanding Artificial Intelligence in Tax and Customs Administration // Technical Notes and Manuals. – 2024. – No. 1. – DOI: 10.5089/9798400290435.005.

40 Binns R. Fairness in Machine Learning: Lessons from Political Philosophy // Proceedings of Machine Learning Research. – 2018. – Vol. 81. – P. 149–159.; Raghavan M., Barocas S., Kleinberg J., Levy K. Mitigating bias in algorithmic hiring: Evaluating claims and practices // Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. – 2020. – P. 469–481. – DOI: 10.1145/3351095.3372828.

sions in the candidate selection process transparent increases the perception of fairness among employees, thereby strengthening motivation and commitment in the workplace[41].

Thanks to AI, human resources systems provide data-driven insights into candidates' past performance, skill sets, and suitability for job positions, guiding decision-makers. These applications increase objectivity and accountability in human resources processes. AI-supported systems provide data-driven information to hiring committees to evaluate candidates solely based on predefined criteria. This reduces the influence of subjective decisions and external interference, ensuring the more effective application of the merit principle[42].

3.4. Artificial Intelligence Applications in Forensic Computing for Detecting Document Forgery

Document forgery (invoices, contracts, bank statements, identity documents, official correspondence, etc.), which is frequently encountered in corruption cases, is a critical part of this process. Forensic computing is a field concerned with the collection, examination, and use of digital evidence in legal proceedings[43]. The field of forensic computing contributes to the fight against corruption thanks to the advantages offered by AI techniques. AI offers innovative solutions in the fight against document forgery, accelerating investigation processes and increasing accuracy rates. ML and DL algorithms can detect signs of forgery by digitally analyzing documents. For example, inconsistencies in font types on a document, digital signature manipulations, or inconsistencies in the timestamps of electronic records can be automatically analyzed by AI. In digital forensics, mobile forensics, and cloud forensics investigations, AI demonstrates superior performance in filtering through large amounts of evidence material to identify and pinpoint relevant data in automatic searches of images, videos, language, and audio files[44].

The primary role of AI in detecting document forgery is to reveal anomalies and manipulations in documents using image processing, NLP, and pattern recognition techniques. AI algorithms can analyze the visual integrity of a document (font types, alignment, logos, seals, signatures) and identify any inconsistencies or alterations. AI applications in document forgery detection adopt a multi-layered analysis approach. At the primary level, OCR systems detect textual inconsistencies in documents, while at the secondary level, spectral imaging techniques analyze the physical and chemical properties of documents[45].

The practical results of AI applications in detecting digital fraud provide significant advantages in the fight against corruption. In the banking sector, bank statements, invoices, payroll, and invoice documents can be automatically verified using AI, which can detect fraud that is invisible to the human eye. The combination of AI and blockchain technologies enables the creation of digital identity cards for physical objects, thereby detecting counterfeiting. Advanced technologies such as deepfake content detection and image forgery analysis accelerate the evidence collection and analysis processes of forensic computing experts and increase accuracy rates. These technological developments play a critical role in the proactive detection of document-based corruption attempts, particularly in public institutions, and go beyond the limitations of traditional manual review methods[46].

41 Cappelli P., Tambe P., Yakubovich V. Artificial Intelligence in Human Resources Management: Challenges and a Path Forward // SSRN Electronic Journal. – 2018. – DOI: 10.2139/ssrn.3263878.

42 Zhang N., Wang M., Xu H. et al. Reducing subgroup differences in personnel selection through the application of machine learning // Personnel Psychology. – 2023. – Vol. 76. – P. 1125–1159. – DOI: 10.1111/peps.12593.

43 Orakcı M., Çakır H., Kök İ. Adli Bilişim Eğitiminin Gereksinimi ve Genel Olarak Değerlendirilmesi [Online resource]. – 2016. – URL: https://dergipark.org.tr/en/pub/gazibtd/issue/26690/280769 (date of access: 21.04.2026).

44 Barash M., McNevin D., Fedorenko V., Giverts P. Machine learning applications in forensic DNA profiling: A critical review // Forensic Science International: Genetics. – 2024. – Vol. 69. – Art. 102994. – DOI: 10.1016/j.fsigen.2023.102994.; Yılmaz F., Çakır H. Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bir Öneri Çalışması // Uluslararası Bilgi Güvenliği Mühendisliği Dergisi. – 2021. – Vol. 7, No. 1. – P. 24–45. – URL: https://dergipark.org.tr/en/pub/ubgmd/issue/64040/851997 (date of access: 21.04.2026).

45 Yang P., Fang W., Zhang F., Bai L., Gao Y. Document Image Forgery Detection Based on Deep Learning Models // 2022 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE). – 2022. – P. 36–41. – DOI: 10.1109/ISEEIE55684.2022.00014.

46 Sukhija R., Kumar M., Jindal M. K. Document forgery detection: a comprehensive review // International Journal of Data Science and Analytics. – 2025. – DOI: 10.1007/s41060-025-00723-0.

3.5. Examples of Using Artificial Intelligence in the Fight Against Corruption

Different AI applications are used in the fight against corruption in different countries around the world. These examples are increasing day by day. Concrete applications implemented by countries and institutions around the world demonstrate the transformative impact AI can have in combating different forms of corruption.

3.5.1. Examples of financial monitoring and tax/customs control

The detection and prevention of financial crimes is one of the important areas of application for AI. Singapore is among the countries working on this issue by creating AI-supported financial surveillance systems. A system developed in Singapore has successfully uncovered fraud networks by analyzing unusual cash transfers between different institutions. Similarly, the Monetary Authority of Singapore (MAS) is collaborating with fintech companies under "Project Greenprint" to develop AI solutions for sustainable finance and money laundering detection[47]. JPMorgan Chase in the US uses the COIN (Contract Intelligence) platform to leverage AI in the analysis of legal documents. The system can analyze thousands of contracts in seconds to identify suspicious clauses and potential inconsistencies[48].

Cross-checking systems of AI detect suspected tax evasion by integrating different sources such as bank transactions, e-commerce records, and social media data. The Indian Income Tax Department has launched the "Project Insight" initiative to strengthen tax audits and expand the tax base, aiming to prevent tax evasion through big data analysis and provide taxpayers with online compliance solutions[49]. The Indian Goods and Services Tax Network uses AI to detect types of tax fraud such as false invoicing, circular trading, and input tax refund fraud[50]. The UK Revenue and Customs Authority has begun combating tax evasion and collecting additional taxes by integrating numerous data sources through its "Connect" platform[51]. The United States Internal Revenue Service (IRS) aims to successfully detect tax crimes such as identity theft, refund fraud, and underreporting by conducting AI-supported tax audits using the "CADE (Customer Account Data Engine) 2" system[52]. In customs control, some AI tools used in the European Union's customs control processes automatically identify risky commercial actors by analyzing import and export data.

The Dutch Customs Administration's "Datalab" project has generated additional tax revenue and significantly reduced irregularities in customs processes through AI-based analyses[53]. AI-powered systems used by U.S. Customs and Border Protection (CBP) can analyze import- export data to detect illegal trade activities in real time[54].

3.5.2. Examples in public procurement processes

The risk of corruption in public procurement can be significantly reduced with AI-based solutions. Ukraine's "ProZorro" e-procurement platform has significantly reduced corruption cases through transparent procurement processes

47 Krause D. The Rise of Online Scams and Consumer Protections: A Comparative Analysis of the U.S. and Singapore // SSRN. – 2025. – DOI: 10.2139/ssrn.5134496.; Money Laundering National Risk Assessment Report. – Singapore: Monetary Authority of Singapore, 2024.

48 J.P. Morgan COiN: A Case Study of AI in Finance // Superior Data Science [Online resource]. – 2024. – URL: https://superiordatascience.com/jp-morgan-coin-a-case-study-of-ai-in-finance/ (date of access: 21.04.2026).

49 Income Tax Department signs contract with L&T Infotech Ltd for implementation of Project Insight / Press Information Bureau, Government of India [Online resource]. – 2016. – URL: https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=147283 (date of access: 21.04.2026).

50 Goods and Services Tax Network. Technology Backbone for GST in India [Online resource]. – 2025. – URL: https://www.gstn.org.in/home (date of access: 21.04.2026).

51 HMRC Annual Report and Accounts: 2023 to 2024 [Online resource]. – 2024. – URL: https://www.gov.uk/government/publications/hmrc-annual-report-and-accounts-2023-to-2024 (date of access: 21.04.2026).

52 CADE-2 / Internal Revenue Service [Online resource]. – 2021. – URL: https://www.irs.gov/pub/irs-pia/cade-2-pia.pdf (date of access: 21.04.2026).

53 Rukanova B., Tan Y. H., Slegt M. et al. Identifying the value of data analytics in the context of government supervision: Insights from the customs domain // Government Information Quarterly. – 2021. – Vol. 38. – Art. 101496. – DOI: 10.1016/j.giq.2020.101496.

54 United States Customs and Border Protection: AI Use Cases / U.S. Department of Homeland Security [Online resource]. – 2025. – URL: https://www.dhs.gov/ai/use-case-inventory/cbp (date of access: 21.04.2026).

thanks to AI-supported analyses[55]. Studies conducted using AI in the European Union's "TED (Tenders Electronic Daily)" database have yielded successful results in identifying suspicious tender participation[56]. The "KONEPS" platform in South Korea uses AI algorithms to analyze the reliability of companies participating in tenders and alerts authorities by flagging high-risk candidates[57]. Brazil's anti-corruption agency CGU (Controladoria-Geral da União) uses the "ALICE" (Análise de Licitações e Editais) system to perform AI-supported risk analysis in public tenders. In 2024, the system scanned over 118,000 processes, initiated 214 audits totaling 26.17 billion R$, and prevented 1.25 billion R$ in resource waste through its findings[58]. Similarly, the South Korean Audit and Inspection Board's AI-supported "K- IFRS" system detects irregularities in public institutions' financial statements with a high degree of accuracy and provides transparency[59].

3.5.3. Examples in personnel and human resources

Nepotism in hiring and promotion processes is another important area of corruption that AI intervenes in. The European Union's "AI-Recruiter" project automatically analyzes skills and experience in CVs to identify the most suitable candidates in the applicant pool, thereby significantly reducing the risk of nepotism[60]. This system aims to create a more equitable process by eliminating the influence of factors such as gender, ethnic origin, or social connections, particularly in public sector hiring. The Canadian Federal Government's "Talent Cloud" platform analyzes employees' project contributions, skill development, and impact on team performance to provide unbiased evaluations, thereby increasing transparency in performance-based promotion processes and reducing suspicions of favoritism[61].

3.5.4. Forensic computing and sample applications in document forgery detection

Document forgery is an area frequently encountered in corruption cases and one that AI effectively combats with its image processing and NLP capabilities. Europol aims to use DL-based image processing systems to detect forged documents across Europe. These systems can analyze font variations, ink distribution anomalies, and digital manipulation traces on identity documents, diplomas, and official certificates[62]. The Document and Benefit Fraud Task Forces (DBFTF) used by US Immigration and Customs Enforcement (ICE) have significantly reduced the time required to detect fraudulent documents compared to traditional methods by automatically checking security features in passports and visa documents[63]. Estonia's "KSI Blockchain"-based document management system aims to reduce the use of fake documents by instantly verifying the authenticity of educational diplomas and professional certificates[64]. Similarly, the United Arab Emirates' "Emirates Blockchain Document Verification" system ensures the security of all official documents in the public and private sectors and

55 International Bank for Reconstruction and Development and/or International Development Association: Project Document / World Bank. – 2022. – URL: https://documents1.worldbank.org/curated/en/099210502092310651/pdf/P1801260cf71a208082c0081a69939ad85.pdf (date of access: 21.04.2026).

56 Preparatory Action on Transparency in Public Procurement // Tenders Electronic Daily [Online resource]. – 2024. – URL: https://ted.europa.eu/en/preparatory-action (date of access: 21.04.2026).

57 Kuris G. Creating a Level Playing Field for Public Procurement: The Korea Online E-Procurement System, 1996–2002 [Online resource]. – 2021. – URL: https://www.effectivecooperation.org/system/files/2021-09/CS_KoreaProcurement.pdf (date of access: 21.04.2026).

58 Controladoria-Geral da União. Alice [Online resource]. – 2025. – URL: https://www.gov.br/cgu/pt-br/assuntos/auditoria-e-fiscalizacao/alice (date of access: 21.04.2026).

59 IFRS Foundation. Official website [Online resource]. – 2025. – URL: https://www.ifrs.org/ (date of access: 21.04.2026).

60 Preparatory Action on Transparency in Public Procurement // Tenders Electronic Daily [Online resource]. – 2024. – URL: https://ted.europa.eu/en/preparatory-action (date of access: 21.04.2026).

61 Talent Cloud. Talent Cloud Results Report [Online resource]. — Government of Canada, 2021. — URL: https://talent.canada.ca/static/tc-report/en/talent-cloud/report (date of access: 21.03.2026).

62 Europol Programming Document. – The Hague: Europol, 2023.

63 Identity and Benefit Fraud // U.S. Immigration and Customs Enforcement [Online resource]. – 2025. – URL: https://www.ice.gov/about-ice/hsi/investigate/identity-benefit-fraud (date of access: 21.04.2026).

64 KSI Blockchain // e-Estonia [Online resource]. – 2025. – URL: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ (date of access: 21.04.2026).

minimizes cases of fraud[65].

3.5.5. Examples in transparency and citizen participation

AI indirectly but powerfully contributes to the fight against corruption by making public data more transparent and encouraging citizen participation. The Finnish Government has developed an AI- supported platform that allows citizens to determine their own budget priorities and automatically generates policy recommendations by analyzing citizen preferences[66]. Georgia's e-government platform has increased transparency and citizen satisfaction between 2018 and 2023 with AI-supported automated transparency reports and proactive information sharing[67]. Uruguay's open data platform, the "Datos.gub.uy Project," has increased citizen participation with AI features such as semantic search and automatic visualization[68]. The "Ushahidi" platform used in Kenya allows citizens to report cases of corruption on a map, while AI systems can categorize these reports and prioritize them[69].

3.5.6. Developments in Türkiye and Uzbekistan

In Türkiye, significant steps are being taken to combat corruption using AI applications. The Revenue Administration (GİB) is implementing AI-supported tax audit systems as part of the "Digital Türkiye" vision. Anomaly detection algorithms are run by integrating e-declaration, e-invoice, and e-ledger data on the Digital Tax Office, and inconsistencies between taxpayer declarations and invoice amounts are automatically flagged. Applications such as e-Inspection, e-Ledger, e-Invoice, e-Archive Invoice, VAT Refund Risk Analysis System, Labeled Product Tracking System, and Counterfeit Document Risk Analysis Program have the capacity to detect counterfeit document use, tax evasion, and other irregularities by analyzing large volumes of tax data in real time[70]. The Supreme Audit Institution of the Republic of Türkiye is developing AI-supported risk analysis systems as part of its "Digital Transformation and AI in Auditing" project, working on cross-checking algorithms for financial statements, NLP techniques for contract analysis, and anomaly detection systems for personnel movements[71]. The Public Procurement Authority conducts AI-supported tender analysis using data collected through EKAP (Electronic Public Procurement Platform), utilizing copy detection algorithms in technical specifications, anomaly analysis in bidding patterns, and price comparison/market analysis modules[72]. In addition, Türkiye's e-Government platform also benefits indirectly from AI by providing many services online and transparently[73].

Uzbekistan, on the other hand, has taken significant steps in recent years to combat corruption and increase transparency in public administration, and has begun to actively use AI technologies in this process. In particular, the Anti-Corruption Agency of the Republic of Uzbekistan has made significant investments in digitalization to increase transparency and reduce the risk of cor-

65 Document Verification (Blockchain) / UAE Ministry of Climate Change and Environment [Online resource]. – 2025. – URL: https://www.moccae.gov.ae/en/e-participation/blockchain-apostilles.aspx (date of access: 21.04.2026).

66 Finland AI Strategy Report / Finnish Ministry of Economic Affairs and Employment [Online resource]. – 2017. – URL: https://ai-watch.ec.europa.eu/countries/finland/finland-ai-strategy-report_en (date of access: 21.04.2026).

67 My.gov.ge. Public services portal [Online resource]. – 2025. – URL: https://my.gov.ge/ka-ge/services/10 (date of access: 21.04.2026).

68 Datos Abiertos // gub.uy [Online resource]. – 2025. – URL: https://www.gub.uy/datos-estadisticas (date of access: 21.08.2026).

69 Ushahidi. Official website [Online resource]. – 2025. – URL: https://www.ushahidi.com/ (date of access: 21.04.2026).

70 Dijital Vergi Dairesi. Official website [Online resource]. – 2025. – URL: https://dijital.gib.gov.tr/ (date of access: 21.04.2026).; Gelir İdaresi Başkanlığı. Official website [Online resource]. – 2025. – URL: https://www.gib.gov.tr/ (date of access: 21.04.2026).

71 Kurban S., Çığman M. Z., Pekel A. Büyük Veri Çağında Sayıştay Başkanlığı'nın Dijitalleşen Denetimi // Denetişim. – 2023. – P. 39–52. – DOI: 10.58348/denetisim.1282034.

72 Gürbüz A. E-İhale Kapsamında Avrupa Birliği ve Türk Kamu Alımları'nda Dinamik Alım Sistemi'nin Karşılaştırmalı Analizi // Çanakkale Onsekiz Mart Üniversitesi Uluslararası Sosyal Bilimler Dergisi. – 2019. – Vol. 4. – P. 333–356. – DOI: 10.31454/usb.634613.; Pınar Ö. G. Yerel Yönetimlerde Elektronik İhale (E-İHALE) Sistemleri ve Yapı Bilgi Modellemesi (YBM) Entegrasyonu // Yapı Bilgi Modelleme. – 2022. – Vol. 3. – P. 64–75. – DOI: 10.53033/ybm.1112607.

73 Dede A. Dijital Vatandaşlığın Dokuz Boyutu ve E-Devlet Uygulamaları // EKEV Akademi Dergisi. – 2024. – P. 15–27. – DOI: 10.17753/sosekev.1365162.

ruption[74] (ACA, 2025; UNODC, 2024).

In this context, Uzbekistan has launched an electronic platform inspired by Korea to monitor and evaluate anti-corruption measures[75]. Through platforms such as "E-Anticor.uz," corruption risks in public institutions are assessed and programs are developed to eliminate these risks. AI algorithms analyze data in sectors prone to corruption, such as capital construction, education, and public procurement, to identify potential irregularities and optimize audit processes[76]. In addition, Uzbekistan has risen to a leading position in Central Asia in terms of the use of AI in public services and has adopted the goal of using AI to improve interactions between citizens and government agencies[77]. These initiatives support the goals of improving the country's overall governance quality and its position in international transparency indices by making anti-corruption strategies more data-driven and proactive.

4. Ethical, Legal, and Political Dimensions

Although AI holds significant potential in the fight against corruption, the implementation of these technologies also brings with it several ethical and legal responsibilities and political challenges. These dimensions must not be overlooked, as neglecting them could undermine the reliability and social acceptance of AI systems. Furthermore, such neglect could negatively impact the fight against corruption. Therefore, these challenges must be carefully addressed to ensure the responsible and sustainable integration of AI.

At the core of AI systems are algorithms. The quality and privacy of the data that forms the raw material and foundation of these algorithms is one of the most critical issues. Insufficient, incomplete, corrupted, erroneous, or dirty data can cause AI algorithms to produce incorrect results and thus lead to false detections or unjust accusations[78]. In addition, large data sets used to combat corruption often contain sensitive personal information, which has the potential to conflict with data protection regulations such as the General Data Protection Regulation (GDPR) in the European Union or the Personal Data Protection Law (KVKK) in Türkiye. The use of personal data and AI's extensive surveillance capabilities raise serious concerns about individuals' privacy rights by increasing the risk of a surveillance society[79]. Therefore, it is vitally important to ensure absolute compliance with transparency, anonymization, and security standards in data collection, storage, and processing processes.

Another important issue in AI algorithms is bias. AI models can inherit social, institutional, or systematic biases from the historical data they are trained on[80]. This situation can cause algorithms to produce discriminatory results against certain groups or make unfair decisions. For example, a tax audit algorithm that disproportionately flags certain demographic groups as risky can lead to discrimination, or biased algorithm training against a particular country can cause problems at that country's customs checkpoints. These algorithmic biases can also be susceptible to political manipulation, as certain interest groups may attempt to manipulate data sets or models to influence algorithmic decisions in their favor. To mitigate these risks, algorithms must be regularly audited, tested with

74 Anti-Corruption Agency of the Republic of Uzbekistan. Official website [Online resource]. – URL: https://anticorruption.uz/en (date of access: 21.04.2026).; UNODC and the Anti-Corruption Agency of Uzbekistan have signed an Action Plan for joint activities aimed at countering corruption in the country // United Nations Office on Drugs and Crime [Online resource]. – 2024. – URL: https://www.unodc.org/roca/en/NEWS/news_2024/june/unodc-and-the-anti-corruption-agency-of-uzbekistan-have-signed-an-action-plan-for-joint-activities-aimed-at-countering-corruption-in-the-country-.html (date of access: 21.04.2026).

75 Uzbekistan launches electronic platform for monitoring and evaluation of anti-corruption measures inspired by Korean tool // United Nations Development Programme [Online resource]. – 2022. – URL: https://www.undp.org/policy-centre/seoul/news/uzbekistan-launches-electronic-platform-monitoring-and-evaluation-anti-corruption-measures-inspired-korean-tool (date of access: 21.04.2026).

76 E-Antikorrupsiya. E-ANTICOR.UZ [Online resource]. – 2025. – URL: https://e-anticor.uz/oz (date of access: 21.04.2026).

77 Grau G. Harnessing AI for development: Uzbekistan's progress towards becoming a regional IT hub // Oxford Insights [Online resource]. – 2024. – URL: https://oxfordinsights.com/insights/harnessing-ai-for-development-uzbekistans-progress-towards-becoming-a-regional-it-hub/ (date of access: 21.04.2026).

78 Crawford K. The Atlas of AI. – New Haven: Yale University Press, 2021. – DOI: 10.2307/j.ctv1ghv45t.

79 Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. – New York: PublicAffairs, 2019.

80 O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. – New York: Crown Publishing Group, 2016.

diverse data sets, and verified to ensure they produce fair outcomes[81].

Due to the black box operating principle of AI systems, accountability and traceability pose significant legal and ethical challenges. Some AI models, such as DL, cannot fully explain how they make decisions; that is, it is difficult to interpret their outputs and understand their decision-making mechanisms. This makes it difficult to prove or challenge the rationale behind a decision in legal proceedings when an AI system detects corruption or flags an individual as risky. While research on XAI offers solutions to address this issue, practical applications are still in their infancy. The question of who is responsible for an erroneous detection or decision made by AI necessitates the urgent clarification of legal and regulatory frameworks.

Beyond all these technical and legal challenges, strong political will and overcoming institutional resistance are critical to the success of AI-based anti-corruption systems. The adoption of new technologies may conflict with traditional management cultures and encounter resistance to technological transformation. The development, implementation, and maintenance of AI systems require high costs and necessitate collaboration between qualified AI experts and anti-corruption specialists. Additionally, the potential for corrupt individuals to similarly use AI technologies for their own gain or manipulate AI systems necessitates the continuous development and enhancement of security measures for these systems. Shortcomings in existing legal and regulatory frameworks necessitate the filling of legal gaps and the updating of existing legislation to enable AI to be used effectively in the fight against corruption.

Comprehensive policy recommendations should be developed to overcome these challenges. The establishment of clear legal and ethical standards governing the use of AI is an important factor. These standards should ensure data privacy, algorithmic impartiality, transparency, and accountability. In addition, high-quality and accessible data sets must be created and data infrastructure strengthened to ensure the reliability of AI systems. To combat corruption globally and maintain technological advantage, international cooperation and cross-border sharing of knowledge and experience in AI-based anti-corruption strategies should be encouraged. Capacity building in all institutions should be targeted through the training of AI experts and anti-corruption specialists. Meanwhile, to preserve the impact of the human factor, a human-AI collaboration model should be adopted, in which AI is positioned as a supportive tool rather than a replacement for human auditors, and the audit sector should be transformed into a changing sector. Citizens' education and awareness regarding the use of AI-supported transparency platforms should also be increased.

5. Conclusions and Recommendations

Corruption is one of the most destructive and complex problems facing modern societies. Today, AI technologies offer important tools in the fight against this problem, with potential for detecting and preventing corruption in many areas, from public procurement to tax audits, human resources processes, and forensic computing. It has capabilities that go beyond human capacity, especially in areas with high data volumes. International examples have proven AI's success in detecting financial anomalies, tender irregularities, tax evasion, and document forgery. However, it should not be forgotten that AI is not a "complete solution" to combating corruption, but rather a powerful "force multiplier." It should be acknowledged that AI possesses transformative qualities in audit mechanisms and that AI-supported solutions, through human-AI collaboration, constitute a significant force. In this way, AI will be positioned not as a replacement for human auditors but as a supportive and productivity-enhancing tool. Additionally, the effective use of this technology must be supported by a robust ethical and legal framework, transparent policies, and strong political will. To fully realize AI's potential in the fight against corruption, the ethical, legal, and technical challenges encountered must be overcome.

Strengthening legal regulations for the use of AI technologies in the fight against corruption is a

81 Jobin A., Ienca M., Vayena E. The global landscape of AI ethics guidelines // Nature Machine Intelligence. – 2019. – Vol. 1, No. 9. – P. 389–399. – DOI: 10.1038/s42256-019-0088-2.

fundamental priority. AI-supported audit systems must have a clear legal framework in terms of data privacy (GDPR/KVKK compliance), algorithmic impartiality, transparency, and accountability. Issues such as the legal validity of decisions made by AI and their admissibility as evidence in courts must be clearly defined in legislation. Additionally, public officials must be trained in AI technologies to enhance their capabilities and improve their AI literacy.

Several important steps must be taken to ensure the effective use of AI in future anti-corruption strategies. International cooperation is critical in terms of data sharing and the development of common standards in the fight against global corruption networks. International organizations such as the OECD and the UN should play a leading role in determining AI ethics and application standards. Academic research should continue to thoroughly examine the delicate balance between data privacy and corruption investigations, the risks of algorithmic bias leading to false accusations, and the legal compliance of AI-supported decisions. The development of data sharing models between governments, the private sector, and civil society organizations will increase innovation and effectiveness in this area. AI is not only a powerful technological tool but also a catalyst supporting the principles of transparency, civil society participation, and accountability, thereby facilitating the beginning of a new era in the fight against corruption.

#

Виталий КИРВЕЛЬ,
Академия управления при Президенте Республики Беларусь,
доцент кафедры конституционного и административного права, к.ю.н., доцент
Михаил ГАЛИНСКИЙ,
Министерство внутренних дел Республики Беларусь

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА РЕСПУБЛИКИ БЕЛАРУСЬ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ

АННОТАЦИЯ. *В статье рассмотрены актуальные вопросы назначения и проведения судебной компьютерно-технической экспертизы сотрудниками органов дознания и предварительного следствия, а также государственными судебными экспертами Республики Беларусь с целью обеспечения прав и законных интересов граждан, юридических лиц и государства, дальнейшего совершенствования и повышения эффективности правоохранительной деятельности по противодействию преступности.*

ANNOTATSİYA. *Maqolada fuqarolar, yuridik shaxslar va davlatning huquqlari hamda qonuniy manfaatlarini ta'minlash, jinoyatchilikka qarshi kurashish bo'yicha huquqni muhofaza qilish faoliyatini yanada takomillashtirish va samaradorligini oshirish maqsadida tergov va dastlabki tergov organlari xodimlari, shuningdek, Belarus Respublikasining davlat sud ekspertlari tomonidan sud kompyuter-texnik ekspertizasini tayinlash va o'tkazishning dolzarb masalalari ko'rib chiqilgan.*

ABSTRACT. *The article discusses the current issues of appointment and conduct of forensic computer and technical expertise by employees of the bodies of inquiry and preliminary investigation, as well as by state forensic experts of the Republic of Belarus, in order to ensure the rights and legitimate interests of citizens, legal entities, and the state, and to further improve and enhance the effectiveness of law enforcement activities aimed at combating crime at combating crime.*

Ключевые слова: *судебная экспертиза, судебные инженерно-технические экспертизы, судебная компьютерно-техническая экспертиза, информационно-коммуникационные технологии, информационные технологии, цифровые технологии, специальные знания.*

Kalit so'zlar: *sud ekspertizasi, sud muhandislik-texnik ekspertizalari, sud kompyuter-texnik ekspertizasi, axborot-kommunikatsiya texnologiyalari, axborot texnologiyalari, raqamli texnologiyalar, maxsus bilimlar.*

Key words: *forensic expertise, forensic engineering and technical expertise, forensic computer and technical expertise, information and communication technologies, information technology, digital technologies, special knowledge.*

Введение (Introduction).

Компьютеризация всех сфер жизнедеятельности человека, активное внедрение информационно-коммуникационных технологий (далее – ИКТ), цифровых технологий (далее – ЦТ) в течение нескольких десятилетий привели не только к положительным результатам – беспрецедентному научно-техническому прогрессу, но и к отрицательным – так называемым «компьютерным или киберпреступлениям».

Под компьютеризацией следует понимать широкое внедрение электронно-вычислительных машин в различные сферы человеческой деятельности (например, для управления технологическими и производственными процессами, транспортом; планирования, учёта и обработки статистических данных, организационно-административного управления; проведения научных исследований, образования, диагностирования и т. д.)[1].

Под ИКТ следует понимать совокупность информационных технологий и технологий электросвязи, обеспечивающих сбор, обработку, хранение, распространение, отображение и использование информации в интересах ее пользователей[2].

Информационная технология (далее – ИТ) – совокупность процессов, методов осуществления поиска, получения, передачи, сбора,

1 Большой энциклопедический словарь: Компьютеризация [сайт]. – М., 2000. – URL : https://dic.academic.ru/dic.nsf/enc3p/161134 (дата обращения: 10.11.2025).

2 Концепция обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года : постановление Совета Министров Респ. Беларусь от 31 дек. 2024 г. № 1074 // Национальный правовой Интернет-портал Республики Беларусь, 15.01.2025, 5/54484.

обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации[3].

Под ЦТ следует понимать технологию, в отличие от аналоговой, работающей с дискретными, а не с непрерывными сигналами[4]. [4]

Беларусь ежегодно улучшает свои позиции в ИКТ Международного союза электросвязи (далее – МСЭ). Индекс развития ИКТ, формируемый МСЭ, в Беларуси растет в последние годы:

в 2023 году он составлял – 86,9, в 2024 году – 88,5, в 2025 году – 90,7 балла. По итогам 2024 года доля ИКТ в ВВП Беларуси достигла 4,9%. Для сравнения, в 2023 году этот показатель равнялся 4,5%[5]. Указанные достижения достигнуты в рамках Государственной программы «Цифровое развитие Беларуси» на 2021–2025 годы.

25 апреля 2024 года Решением № 5 Всебелорусского народного собрания утверждена «Концепция национальной безопасности Республики Беларусь» (далее – Концепция), в которой определены национальные интересы в социальной и информационной сферах, в том числе:

обеспечение общественной безопасности и безопасности жизнедеятельности населения, снижение уровня преступности и криминализации общества,

дальнейшее развитие безопасной информационной среды и информационного общества.

Концепцией также определены внутренние источники угроз национальной безопасности

в информационной сфере, в том числе:

активное использование ИКТ для совершения правонарушений;

расширение возможностей для неправомерных действий в отношении персональных данных;

низкий уровень правосознания и безопасного поведения пользователей ИКТ.

Согласно действующему законодательству Республики Беларусь, содержание понятия «компьютерная или киберпреступность» включает:

1) преступления против компьютерной безопасности (Глава 31 Уголовного кодекса Республики Беларусь (далее – УК)), а именно: ст. 349 УК «Несанкционированный доступ

к компьютерной информации», ст. 350 УК «Уничтожение, блокирование или модификация компьютерной информации», ст. 352 УК «Неправомерное завладение компьютерной информацией», ст. 354 УК «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств», ст. 355 УК «Нарушение правил эксплуатации компьютерной системы или сети» и ст. 212 УК «Хищение имущества путем модификации компьютерной информации»;

2) иные преступления, связанные с использованием средств компьютерной техники:

ст. 179 УК «Незаконные собирание либо распространение информации о частной жизни»,

ст. 188 УК «Клевета», ст. ст. 203, 2031 и ст. 2032 УК «Нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений», «Незаконные действия в отношении информации о частной жизни и персональных данных», «Несоблюдение мер обеспечения защиты персональных данных», ст. 208 УК «Вымогательство», ст. 209 УК «Мошенничество», ст. 216 УК «Причинение имущественного ущерба без признаков хищения»; ст. 254 УК «Коммерческий шпионаж», ст. ст. 343, 3431 УК «Изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего, ст. 368 УК «Оскорбление Президента Республики Беларусь», ст. 369 УК «Оскорбление представителя власти» и др.

Таким образом, к компьютерным или киберпреступлениям относятся правонарушения,

при совершении которых средства компьютерной техники выступают как орудия

3 Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10 ноябр. 2008 г. № 453-З // Национальный реестр правовых актов Республики Беларусь, 2008 г., № 279, 2/1552.

4 Цифровая трансформация. Термины и определения: СТБ 2583-2020. – Введ. 2021–03–01. – Мн. : Госстандарт, 2020 г. – 16 с.

5 ИКТ_(рынок_Белоруссии) [сайт]. – М., 2025. – URL: https://www.tadviser.ru/index.php/ (дата обращения: 10.11.2025).

совершения преступления либо как предмет преступного посягательства.

Непосредственное установление факта и обстоятельств совершения правонарушений, при которых средства компьютерной техники выступали как орудия совершения преступления либо как предмет преступного посягательства невозможно без использования специальных знаний, что обуславливает необходимость назначения и проведения судебной компьютерно-технической экспертизы (далее – СКТЭ) по всем уголовным делам данных категорий.

Под специальными знаниями следует понимать знания в определенной области человеческой деятельности (исключая знания в области материального и процессуального права), полученные в результате профессиональной подготовки, научной деятельности и опыта практической работы, которые используются с целью собирания, исследования, оценки и использования доказательств при раскрытии и расследовании преступлений[6].

По мнению ведущих российских ученых в области компьютерно-технических исследований Россинской Е.Р. и Усова А.И. под СКТЭ следует понимать вид деятельности, который представляет собой процессуальное действие, направленное на установление достоверных фактов и обстоятельств по компьютерной информации, хранящейся на компьютерных носителях. СКТЭ представляет собой отдельный род судебной экспертизы, относящейся к классу судебных инженерно-технических экспертиз[7].

Предметом СКТЭ являются факты (обстоятельства), устанавливаемые на основе исследования закономерностей разработки и эксплуатации компьютерных средств и систем, обеспечивающих реализацию информационных процессов[8].

Объектами СКТЭ являются:

1) персональные компьютеры (стационарные, переносные);

2) машинные носители информации, периферийные устройства, сетевые аппаратные средства, интегрированные системы, комплектующие всех указанных компонентов (аппаратные блоки, машинные носители информации, платы расширения и др.);

3) видеорегистраторы, цифровые фотоаппараты, программы для ЭВМ, текстовые и графические документы (в электронной форме), изготовленные с использованием компьютерных средств;

4) журналы (протоколы) работы специализированных программ.

Задачами СКТЭ являются:

1) определение статуса объекта как компьютерного средства, выявление и изучение его роли в расследуемом событии, а также получение доступа к информации на носителях данных с последующим всесторонним ее исследованием;

2) определение вида (типа, марки), свойств аппаратного средства, его технических и функциональных характеристик, фактического состояния;

3) поиск информации на машинных носителях по техническим критериям, например, форматам файлов, атрибутам, ключевым словам, образцам;

4) определение основных характеристик операционной системы;

5) выявление и исследование функциональных свойств и настроек программного обеспечения, времени его инсталляции; 6) диагностирование алгоритма программного продукта;

7) поиск на машинных носителях сведений об активности пользователя в сети Интернет (Интернет-переписки, истории о посещении сайтов сети Интернет)[9].

Расследование уголовных дел о преступле-

6 Кирвель В.К. Использование специальных знаний в раскрытии и расследовании преступлений. Тактика назначения и проведения судебной экспертизы : Лекция / В. К. Кирвель; М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Мн. : Акад. МВД Респ. Беларусь, 2010 г. – С.5.

7 Россинская, Е. Р. Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. – М. : Право и закон, 2001 г. – С.213.

8 Сборник методических рекомендаций по вопросам назначения экспертиз, проводимых в Государственном комитете судебных экспертиз Республики Беларусь. – Мн. : Гос. комитет суд. экспертиз Респ. Беларусь, 2023 г. – С.88-89.

9 Сборник методических рекомендаций по вопросам назначения экспертиз, проводимых в Государственном комитете судебных экспертиз Республики Беларусь. – Мн. : Гос. комитет суд. экспертиз Респ. Беларусь, 2023 г. – С.88-89.

ниях против компьютерной безопасности и иных преступлений, связанных с использованием средств компьютерной техники, которые выступают как орудия совершения преступления либо как предмет преступного посягательства является одним из актуальных направлений правоохранительной деятельности на современном этапе.

Подтверждением вышеизложенного тезиса являются информационно-справочные данные Национального статистического комитета Республики Беларусь о количестве зарегистрированных преступлений[10] и Управления по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома о количестве, зарегистрированных компьютерных или киберпреступлений в Республике Беларусь за прошедшие 5 лет[11].

Республики Беларусь в период времени с 2011 по 2023 год[12]. [11]

Таким образом, вследствие недостаточности существующих теоретических исследований и разработанных практических рекомендаций по вопросам межведомственного взаимодействия сотрудников органов дознания и предварительного следствия с государственными судебными экспертами при назначении и проведении СКТЭ, при обеспечении прав и законных интересов граждан, юридических лиц и государства, по мнению авторов, невозможно в полной мере удовлетворить насущные потребности общества в создании эффективного правового механизма противодействия преступности, укреплении правопорядка, повышении доверия граждан к органам власти и управления. Одним

Год	Количество зарегистрированных преступлений	Количество зарегистрированных компьютерных или киберпреступлений	Прирост / снижение к предыдущему году	Процент от всех зарегистрированных преступлений
2020	95 478	25 561	+15 022	26,8
2021	87 696	16 446	-9 115	18,8
2022	88 555	14 839	-1 607	16,8
2023	85 374	18 321	+3 482	21,5
2024	73 270	20 135	+1 814	27,5

Необходимо отметить, что современное состояние, проблемы при назначении и проведении СКТЭ и возможные пути их решения в Республике Беларусь оказались вне поля зрения отечественных исследователей и практиков. В Беларуси отсутствуют публикации, посвященные данной теме. Имеются только Методические рекомендации по проведению СКТЭ, разработанные Государственным комитетом судебных экспертиз

из приоритетных решений данной проблемы является разработка и совершенствование теоретико-правовых положений и практических рекомендаций

для правоохранительных органов при назначении и проведении СКТЭ.

Вышеизложенное обусловливает актуальность, научную новизну и практическую значимость исследования современного состояния, выявления проблем при назначении и

10 Официальный сайт Национального статистического комитета Республики Беларусь: Статистика правосудия и правонарушений [сайт]. – Мн., 2025. – URL: https://dataportal.belstat.gov.by/osids/rubric-info/10620 (дата обращения: 10.11.2025).

11 Современная киберпреступность [сайт]. – Мн., 2025. – URL: https://dokshitsy.vitebsk-region.gov.by/uploads/files/29-05-25-29.pdf (дата обращения: 10.11.2025).

12 Официальный сайт Государственного комитета судебных экспертиз Республики Беларусь : Реестр методических материалов в сфере судебно-экспертной деятельности [сайт]. – Мн., 2025. – URL: https://sudexpert.gov.by/ru/registry-materials.html (дата обращения: 10.11.2025).

проведении СКТЭ и предложения возможных путей их решения.

Материалы и методы (Methods)

Целью исследования является анализ современного состояния, выявление проблем и предложение возможных путей их решения в ходе межведомственного взаимодействия сотрудников органов дознания внутренних дел (Министерство внутренних дел / далее – МВД), органов предварительного следствия (Следственный комитет / далее – СК) и государственных судебных экспертов (Государственный комитет судебных экспертиз Республики Беларусь / далее – ГКСЭ) Республики Беларусь на этапе назначения и проведения СКТЭ и повышения эффективности правоохранительной деятельности по противодействию преступности в Республике Беларусь.

Предметом проведённого исследования являются объективные закономерности действительности, выявляемые в результате межведомственного взаимодействия органов дознания и предварительного следствия с государственными судебными экспертами при назначении и проведении СКТЭ.

Методологической основой проведенного исследования послужил всеобщий диалектический метод научного познания, носящий универсальный характер, а также общенаучные (логические, структурный, функциональный, системный), частно-научные (статистический, социологический, синергетический) и специальные методы (формально-юридический).

Результаты (Results)

С целью изучения современного состояния, проблем назначения и проведения СКТЭ, предложения возможных путей их решения в Республике Беларусь, с декабря 2023 года по март 2024 года в рамках проведения дипломного исследования было проведено анкетирование 257 сотрудников правоохранительных органов. Из них:

230 сотрудников МВД республиканского, регионального и территориального уровня (подразделения по противодействию киберпреступности),

14 сотрудников СК регионального уровня (подразделения по противодействию преступлениям против компьютерной безопасности),

13 сотрудников ГКСЭ (государственные судебные эксперты республиканского уровня).

Опросом 230 сотрудников МВД установлено, что 64% из них имеют возраст от 20 до 30 лет, 31% имеют возраст от 30 до 40 лет и 5% имеют возраст от 40 до 50 лет. 72% сотрудников МВД имеют высшее юридическое образование, 30% имеют высшее техническое образование и 3% имеют педагогическое образование. Стаж работы в должности до 1 года у 7% сотрудников, от 1 года до 3 лет у 34%, от 3 до 5 лет у 13%, от 5 до 10 лет у 20%, от 10 до 15 лет у 26%, от 15 до 20 лет у 8% сотрудников.

Опросом 14 сотрудников СК установлено, что 72% из них имеют возраст от 20 до 30 лет, 28% имеют возраст от 30 до 40 лет, 10% имеют возраст от 40 до 50 лет. 100% сотрудников СК имеют высшее юридическое образование. Стаж работы в должности до 1 года у 20% сотрудников, от 1 года до 3 лет у 28%, от 3 до 5 лет у 22%, от 5 до 10 лет у 20%, от 10 до 15 лет у 7%, от 15 до 20 лет у 3% сотрудников.

Опросом 13 сотрудников ГКСЭ установлено, что 7% из них имеют возраст от 20 до 30 лет, 38% имеют возраст от 30 до 40 лет, 47% имеют возраст от 40 до 50 лет и 8% имеют возраст старше 50 лет. 100% сотрудников ГКСЭ имеют высшее техническое образование. Стаж работы в должности от 5 до 10 лет у 8%, от 10 до 15 лет у 54%, от 15 до 20 лет у 15% сотрудников и более 20 лет у 23%.

Анкетируемым было предложено ответить на следующие вопросы.

1. При проведении Вами следственных и иных процессуальных действий возникала ли необходимость в привлечении специалиста в области компьютерной техники (для следователей и сотрудников МВД):

да, всегда – 8% сотрудников МВД, 29% следователей;

да, только в случаях, когда имеется необходимость в обнаружении, фиксации и изъятии следовой информации – 65% сотрудников МВД, 42% следователей;

нет – 27% сотрудников МВД, 29% следователей.

2. Какие затруднения возникали при привлечении специалистов ГКСЭ в области компьютерной техники для проведения след-

ственных и иных процессуальных действий по материалам и уголовным делам (для следователей и сотрудников МВД):

затруднения, связанные с занятостью специалиста, как судебного эксперта для проведения СКТЭ – 65% сотрудников МВД, 35% следователей;

малочисленность сотрудников специализированных подразделений ГКСЭ – 29% сотрудников МВД, 57% следователей;

отсутствие возможности у специалиста принять участие в проведении следственных и иных процессуальных действий по другим причинам – 6% сотрудников МВД, 8% следователей.

3. Можете ли Вы без участия специалиста в области компьютерной техники эффективно применить технико-криминалистические средства для обнаружения, фиксации и изъятия следов преступления, обеспечения их сохранности (для следователей и сотрудников МВД):

да – 53% сотрудников МВД, 29% следователей;

нет – 23% сотрудников МВД, 43% следователей;

не всегда – 24% сотрудников МВД, 28% следователей.

4. Были ли в Вашей практике случаи, когда в ходе применения Вами технико-криминалистических средств произошло изменение или уничтожение следов преступления:

да – 0% сотрудников МВД, 0% следователей, 0% сотрудников ГКСЭ;

нет – 100% сотрудников МВД, 100% следователей, 100% сотрудников ГКСЭ.

5. Как часто Вы применяете технико-криминалистические средства (за исключением фототехники):

постоянно (ежедневно) – 42% сотрудников МВД, 0% следователей, 100% сотрудников ГКСЭ;

часто (еженедельно) – 28% сотрудников МВД, 0% следователей, 0% сотрудников ГКСЭ;

иногда (ежемесячно) – 17% сотрудников МВД, 0% следователей, 0% сотрудников ГКСЭ;

не применяю – 13% сотрудников МВД, 100% следователей, 0% сотрудников ГКСЭ.

6. Укажите, достаточно ли Вам специальных знаний в области ИКТ для проведения СКТЭ (для сотрудников ГКСЭ):

да – 73% сотрудников ГКСЭ;

нет – 0% сотрудников ГКСЭ;

не всегда – 27% сотрудников ГКСЭ.

7. Обращаетесь (обращались) ли Вы к сотрудникам ГКСЭ за помощью

при назначении СКТЭ (для следователей и сотрудников МВД):

да – 55% сотрудников МВД, 50% следователей;

нет – 23% сотрудников МВД, 36% следователей;

не всегда – 22% сотрудников МВД, 14% следователей.

8. Привлекали ли сотрудников ГКСЭ для проведения занятий в рамках служебной подготовки непосредственно в Вашем подразделении с освещением вопросов использования криминалистических средств, приемов и методов сбора доказательственной информации при проведении проверок и расследовании уголовных дел в области компьютерной техники (для следователей и сотрудников МВД):

если да, то укажите название – 5% сотрудников МВД, 0% следователей;

нет – 95% сотрудников МВД, 100% следователей.

9. Имеется ли в Вашем пользовании централизованная информационная база данных (удаленного доступа), содержащая и накапливающая методические рекомендации, разъяснения, информационные письма ГКСЭ, СК, и т.д., касающиеся сбора доказательственной информации при проведении проверок и расследовании уголовных дел в области компьютерной техники (для следователей и сотрудников МВД):

если да, то укажите название – 0% сотрудников МВД, 0% следователей;

нет – 100% сотрудников МВД, 100% следователей.

10. Имеется ли в Вашем распоряжении все необходимое программное обеспечение для проведения СКТЭ (для сотрудников ГКСЭ):

если да, то укажите название – 54% сотрудников ГКСЭ («Encase», «R-Studio», «Passware Kit», «Desktop», «Мобильный криминалист»);

если нет, то какое необходимо – 46% сотрудников ГКСЭ (отвечающее современным

возможностям и способное обновляться).

11. Достаточно ли, по Вашему мнению, имеющихся научно-методических рекомендаций ГКСЭ или необходима разработка дополнительных методик (для сотрудников ГКСЭ):

да – 77% сотрудников ГКСЭ;

нет – 23% сотрудников ГКСЭ.

12. Укажите, назначали ли Вы СКТЭ по материалам проверки и уголовным делам (для следователей и сотрудников МВД):

да – 86% сотрудников МВД, 93% следователей;

нет – 14% сотрудников МВД, 7% следователей.

13. Укажите, на все ли поставленные Вами вопросы, в соответствии с методическими рекомендациями ГКСЭ и СК, получены ответы в заключении эксперта по СКТЭ (для следователей и сотрудников МВД):

да, на все – 40% сотрудников МВД, 43% следователей;

нет – 18% сотрудников МВД, 16% следователей;

частично – 42% сотрудников МВД, 43% следователей.

14. Укажите, в течение какого времени Вами получено заключение эксперта по СКТЭ (для следователей и сотрудников МВД):

до 15 календарных дней – 3% сотрудников МВД, 8% следователей;

до 30 календарных дней – 81% сотрудников МВД, 78% следователей;

свыше 30 календарных дней –16% сотрудников МВД, 14% следователей.

15. Укажите, в каких областях криминалистического обеспечения проведения СКТЭ Вы видите проблемы (отметьте один или несколько вариантов) (для сотрудников ГКСЭ):

теоретическое исследование, в том числе проблема употребления понятий, терминов – 15% сотрудников ГКСЭ;

область криминалистической техники (например, наличие и состояние технико-криминалистических средств и методов обнаружения компьютерной информации) – 31% сотрудников ГКСЭ;

область криминалистической тактики (например, вопросы назначения и проведения СКТЭ) – 54% сотрудников ГКСЭ.

16. Как Вы считаете, вследствие каких проблем отсутствует развитие СКТЭ (отметьте один или несколько вариантов) (для сотрудников ГКСЭ):

недостаточное теоретическое и научное исследование проблем в данной области – 18% сотрудников ГКСЭ;

недостаточное внимание, а также неэффективная организация встреч по обмену опытом между Республикой Беларусь и другими странами – 22% сотрудников ГКСЭ;

проблемы в данном вопросе отсутствуют, так как криминалистическое обеспечение развито на должном уровне – 60% сотрудников ГКСЭ.

Обсуждение результатов (Discussion)

1. Основные результаты анкетирования сотрудников МВД и СК.

1.1 86% сотрудников МВД и 93% сотрудников СК назначали СКТЭ по материалам проверки и уголовным делам.

1.2 73% сотрудников МВД и 71% сотрудников СК отметили необходимость в привлечении специалиста (специальных знаний) в области компьютерной техники при проведении следственных и иных процессуальных действий, связанных с обнаружением, фиксацией и изъятием следов преступления, обеспечения их сохранности.

1.3 23% сотрудников МВД и 43% сотрудников СК подтвердили возможность самостоятельного применения специальных знаний в области компьютерной техники без участия специалиста для обнаружения, фиксации и изъятия следов преступления, обеспечения их сохранности.

1.4 77% сотрудников МВД и 64% сотрудников СК при назначении СКТЭ обращались за консультацией к сотрудникам ГКСЭ по вопросам определения рода и вида СКТЭ, объема необходимых для проведения СКТЭ материалов и объектов, их правильного обнаружения, фиксации, изъятия и упаковки, компетентной формулировке вопросов, необходимых для решения определенных судебно-экспертных задач и т.д.

1.5 5% сотрудников МВД привлекали сотрудников ГКСЭ для проведения занятий в рамках служебной подготовки непосредственно с освещением вопросов использования технико-криминалистических средств,

приемов и методов сбора доказательственной информации при проведении проверок по материалам и расследовании уголовных дел в области компьютерной техники.

1.6 65% сотрудников МВД и 35% сотрудников СК отметили затруднения при привлечении специалистов ГКСЭ в области компьютерной техники для проведения следственных и иных процессуальных действий по материалам и уголовным делам, связанные с организационно-штатной структурой подразделений ГКСЭ.

1.7 82% сотрудников МВД и 86% сотрудников СК отметили, что получили ответы на сформулированные вопросы в заключении эксперта по СКТЭ, в соответствии с методическими рекомендациями ГКСЭ и СК.

1.8 84% сотрудников МВД и 86% сотрудников СК получили заключение эксперта по СКТЭ в установленные законодательством сроки (до 30 дней).

1.9 100% сотрудников МВД и сотрудников СК отметили отсутствие централизованной информационной базы данных (удаленного доступа), содержащей и накапливающей методические рекомендации, разъяснения, информационные письма ГКСЭ, СК и МВД, касающиеся сбора доказательственной информации при проведении проверок по материалам и расследовании уголовных дел в области компьютерной техники.

2. Основные результаты анкетирования сотрудников ГКСЭ.

2.1 27% сотрудникам ГКСЭ не всегда достаточно специальных знаний в области компьютерной техники для проведения СКТЭ.

2.2 54% сотрудников ГКСЭ отметили, что в их распоряжении имеется все необходимое программное обеспечение для проведения СКТЭ;

2.3 23% сотрудников ГКСЭ отметили необходимость разработки дополнительных методик и методических рекомендаций по проведению СКТЭ.

2.4 15% сотрудников ГКСЭ указали на недостаточную разработку теоретико-правовых аспектов назначения и проведения СКТЭ, в том числе на проблему употребления дефиниций.

2.5 31% сотрудников ГКСЭ указали на недостаточную разработку технико-криминалистических аспектов назначения и проведения СКТЭ, в том числе на проблему наличия и состояния технико-криминалистических средств и методов обнаружения компьютерной информации.

2.6 54% сотрудников ГКСЭ указали на недостаточную разработку тактических аспектов назначения и проведения СКТЭ.

Выводы (Conclusion/Recommendations)

Проведенный анализ современного состояния, выявление проблем и предложение возможных путей их решения в ходе межведомственного взаимодействия сотрудников органов предварительного следствия (СК) и органов внутренних дел (МВД) с государственными судебными экспертами (ГКСЭ) Республики Беларусь на этапе назначения и проведения СКТЭ позволили сделать следующие выводы:

1) современное состояние и проблемы межведомственного взаимодействия сотрудников СК и МВД с ГКСЭ были изучены и выявлены с помощью статистических, социологических и синергетических методов исследования;

2) анализ полученных при анкетировании сотрудников правоохранительных органов результатов указывает на целесообразность дальнейшего проведения исследования теоретико-прикладных аспектов указанной темы;

3) необходимость разработки методических рекомендаций о форме, порядке и регламенте межведомственного взаимодействия сотрудников СК и МВД с ГКСЭ;

4) представляется обоснованным предложить следующие направления совершенствования межведомственного взаимодействия сотрудников МВД, СК и ГКСЭ:

4.1) создать централизованную информационную базу (удаленный доступ), назвав ее «Цифровые технологии», накапливающую методические рекомендации, разъяснения, информационные письма МВД, СК, и ГКСЭ, касающуюся сбора доказательственной информации при проведении проверок по материалам и расследовании уголовных дел в области компьютерной техники;

4.2) привлекать наиболее подготовленных в профессиональном плане и обладаю-

щих педагогическими умениями общения с аудиторией сотрудников ГКСЭ для проведения занятий в рамках служебной подготовки в МВД и СК, непосредственно в подразделениях с освещением вопросов использования криминалистических средств, приемов и методов сбора доказательственной информации при проведении проверок материалов и расследовании уголовных дел в области компьютерной техники, а также для правильности постановки вопросов при назначении СКТЭ. Данных специалистов следует привлекать не только к проведению лекционных занятий, но и к проведению семинарских занятий по типу круглых столов с целью консультаций;

4.3) создать группу исследователей и практиков для разработки национальных методик проведения СКТЭ, не используя адаптированные методики других стран;

4.4) осуществить адаптирование программного обеспечения тех стран, которые не наложили санкции на Республику Беларусь (Российская Федерация, Китай и другие), с возможностью обновления;

4.5) проводить повышение квалификации и переподготовку государственных судебных экспертов, специализирующихся на проведении СКТЭ, в вузах Российской Федерации и других странах для получения новых знаний и практических умений всестороннего исследования компьютерной техники.

В заключение следует отметить, что авторы не претендуют на бесспорность высказанных суждений и выводов. Представляется, что данная публикация вызовет интерес и дискуссию у теоретиков и практиков, а также тех, кому небезразлична данная проблема. Они полагают, что публикация может вызвать интерес у читателей и приглашают к дискуссии теоретиков и практиков, а также предлагают проведение совместных комплексных теоретико-прикладных исследований по указанной проблематике.

#

RAQAMLI KRIMINALISTIKA
ILMIY-AMALIY YURIDIK JURNALI

Jurnalda nashr etiladigan maqolaga quyidagi talablar qo‘yiladi:

– maqolada jamiyatni demokratlashtirish va yangilash, mamlakatni modernizatsiyalash va isloh etishning umumnazariy, ijtimoiy-siyosiy, huquqiy masalalari, mazkur sohalarda amalga oshirilgan ishlarning tizimli tahlili hamda aniq yangi nazariy va amaliy takliflar aks etishi;

– matn takrorlarsiz, mantiqiy izchil, bayon qilingan fikrlar aniq, qisqa va lo‘nda bo‘lishi;

– keltirilayotgan ma’lumotlar ishonchli va to‘g‘ri bo‘lishi;

– maqolaga jurnalda nashr qilish mumkinligi haqida shu sohadagi yetakchi huquqshunos olim va mutaxassisning, muallif ishlaydigan yoki tadqiqotchi hisoblanadigan oliy o‘quv muassasasi kafedrasi yoki instituti rahbari taqrizi;

– matn o‘zbek va rus tilida taqdim etilishi;

– matn kompyuterda Wordning "Times New Roman"ida 14 shriftda 1,5 intervalda A4 formatli standart oq qog‘ozning bir tomonida yozilishi, elektron nusxada taqdim etilishi hamda matnning chap qismi 3 sm, o‘ng qismi 1,5 sm, tepa va pastki qismlari 2 sm bo‘lishi;

– maqolada ilmiy bahs-munozara, iqtiboslarning mavjud bo‘lishi; iqtiboslar 12 shriftda 1,0 intervalda yozilishi;

– maqolaning hajmi 8 betdan 10 betgacha bo‘lishi;

– maqolaning so‘nggi sahifasida muallifning ism-sharifi, ilmiy darajasi va unvoni, ish joyi va lavozimi, yashash va xizmat manzili, telefon raqamlari yozilgan;

– o‘zbek, rus va ingliz tilidagi qisqa annotatsiya hamda tayanch so‘zlar bo‘lishi lozim.

На статьи, публикуемые в журнале, распространяются следующие требования:

– обзор общих политических, общественно-политических, правовых и практических вопросов темы, а также систематический анализ работы, проделанной в этих областях, новых теоретических и практических выводов, предложений и рекомендаций;

– постановка проблем, полнота теоретических и методологических аспектов материала, достоверность предоставленной информации, обоснованность проблемы, выводов, предложений и рекомендаций;

– логическое, последовательное, точное и лаконичное изложение идей, предложений и рекомендаций;

– отсутствие информации, не подлежащей публикации в открытой печати.

Статьи публикуются на узбекском, русском и английском языках.

Текст набирается на компьютере, шрифт «Times New Roman», размер шрифта 14 пт, межстрочный интервал 1.5, общий размер не более 8-10 страниц, напечатан на одной стороне стандартного формата бумаги А4, поля слева 3 сантиметра, справа 1,5 сантиметра, сверху и снизу 2 сантиметра;

– научные дискуссии, цитаты (ссылки) на использованные источники, цитаты, написанные шрифтом 12 пт, в однострочном интервале.

Первая страница статьи должна содержать следующую информацию:

– имя, фамилия и отчество (полное) автора (ов), место работы и должность, ученая степень и звание, почетное звание, номер телефона (сотового), адрес электронной почты;

– краткая аннотация и ключевые слова на узбекском, английском и русском языках.

Статья не будет принята к рассмотрению и публикации в следующих случаях:

– статья не соответствует вышеуказанным требованиям;

– наличие отрицательных рецензий;

– в случае принятия на заседаниях редколлегии решения не публиковать научную статью;

– если выявлено научное мнение другого автора, выводы и взгляды (плагиат).

Авторы и рецензенты несут ответственность за содержание представленных статей и достоверность фактов. Рукописи не рассматриваются и не возвращаются.

