O‘ZBEKISTON RESPUBLIKASI HUQUQNI MUHOFAZA QILISH AKADEMIYASI

TOSHKENT DAVLAT YURIDIK UNIVERSITETI

KIBERHUQUQ: MUAMMOLAR VA RIVOJLANTIRISH ISTIQBOLLARI

konferensiya materiallari

ТОШКЕНТ 2024

O‘ZBEKISTON RESPUBLIKASI
HUQUQNI MUHOFAZA QILISH AKADEMIYASI

Tezkor-qidiruv faoliyati va kiberhuquq kafedrasi

“KIBERHUQUQ: MUAMMOLAR VA RIVOJLANTIRISH ISTIQBOLLARI”

mavzusidagi xalqaro ilmiy-amaliy

KONFERENSIYA

materiallari

TOSHKENT- 2025

UO‘K 343. 98+343.2/.7(575.1)

BBK 67.408

K 43

Mazkur to’plam O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasida 2024-yilning 25-sentabr kuni “Kiberhuquq: muammolar va rivojlantirish istiqbollari” mavzusida otkazilgan xalqaro ilmiy-amaliy konferensiyasi yakunlari doirasida tayyorlangan.

To’plam O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi kengashining 2024-yilning “24”-dekabr kungi “14”-sonli qarori bilan nashrga tavsiya etilgan.

Kiberhuquq: muammolar va rivojlantirish istiqbollari. Xalqaro ilmiy-amaliy konferensiyasi materiallari. /Mas’ul muxarrir M.M.Mamasiddiqov. “Lesson press”. 2025. – 402 b.

Mas’ul muharrir: **M.M.Mamasiddiqov**

Tahrir hay’ati:

kafedra boshlig’i	**F.A.Nazarov**
yu.f.d.prof.	**V.Karimov**
yu.f.d.prof.	**I.R.Astanov**
yu.f.f.d., dotsent	**Sh.I.Shayzakov**

Nashrga tayyorlovchilar: **A.A. Turg‘unov**
J.R.Shukurov

To’plamda O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasida 2024-yilning 25-sentabr kuni “Kiberhuquq: muammolar va rivojlantirish istiqbollari” mavzusida o’tkazilgan xalqaro ilmiy-amaliy konferensiyasi materiallari o’rin olgan. Unda kiberhuquqni rivojlantirishning dolzarb nazariy va tashkiliy-amaliy masalalari hamda ushbu soha bo’yicha tadqiqot natijalarini amaliyotda qo’llash muammolariga bag‘ishlangan konferensiya maqola va maqola ilmiy-ommabop tarzda bayon etilgan.

To’plam fan va ta’lim sohasini boshqarishga vakolatli davlat organlari, yuridik fan va huquqni qo’llash amaliyoti bilan bog’liq mutasaddi tashkilotlar xodimlari, oliy o’quv yurtlari professor-o’qituvchilari, doktorantlar, mustaqil izlanuvchilar, magistrlar hamda ushbu masalalarda qiziquvchi mutaxassislar va keng jamoatchilik uchun mo’ljallangan.

Mazkur to’plamga kiritilgan materiallarning mazmuni, undagi statistik va boshqa ma’lumotlar, me’yoriy hujjatlar sanasinng to’g‘riligiga hamda tanqidiy fikr-mulohazalarga mualliflarning o’zlari mas’uldir.

@ O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi, 2025.

PROKURATURA ORGANLARINING KORRUPSIYAGA QARSHI KURASHISH FAOLIYATIDA SUN'IY INTELLEKT IMKONIYATLARIDAN FOYDALANISHNING AYRIM MASALALARI

Samadov Salom Ismatovich,
O'zbekiston Respublikasi Bosh prokurori o'rinbosari,
Huquqni muhofaza qilish akademiyasi boshlig'i v.v.b.,
3-darajali Davlat adliya maslahatchisi

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi tufayli jamiyatimiz yangi davrga – raqamli inqilob davriga qadam qo'ymoqda. Har bir sohada yuz bergan tub o'zgarishlar bizdan yangi, innovasion yondashuvlarni talab qilmoqda. Ana shunday sharoitda kiberhuquq mavzusi ayniqsa muhim ahamiyat kasb etmoqda. Hozirgi xalqaro ilmiy-amaliy konferensiyamizda Huquqni muhofaza qilish akademiyasining professor-o'qituvchilari va ilmiy xodimlari, Hindiston Milliy sud ekspertizasi universiteti, Qozog'iston Respublikasi Huquqni muhofaza qilish akademiyasi va boshqa nufuzli ta'lim va ilmiy tadqiqot muassasalari vakillari ishtirok etishmoqda.

Hayotimizning deyarli barcha jabhalari raqamli texnologiyalar bilan bog'liq holda o'zgarmoqda. Bu o'zgarishlar nafaqat odamlar o'rtasidagi muloqot shakllarini, balki iqtisodiyot, ta'lim, sog'liqni saqlash va davlat boshqaruvi kabi muhim sohalarni ham qamrab olmoqda. Ammo bu yangi imkoniyatlar bilan bir qatorda, yangi xavf-xatarlarni ham keltirib chiqardi.

Raqamli dunyoda paydo bo'layotgan yangi tahdidlar orasida kiberxavfsizlik, shaxsiy ma'lumotlarni himoya qilish, axborot maxfiyligi va kiberjinoyatchilik kabi masalalar alohida o'rin tutadi. Shuning uchun kiberhuquq sohasini rivojlantirish va kiberxavfsizlikni ta'minlash nafaqat milliy, balki xalqaro miqyosda ham muhimdir. Jamiyatlar va davlatlar o'rtasida raqamli xavf-xatarlarga qarshi samarali kurash olib borish uchun umumiy huquqiy normalarni ishlab chiqish va davlatlar o'rtasidagi hamkorlikni mustahkamlash zarur bo'lmoqda.

Yangi raqamli reallikda, davlatlarning mustaqil yondashuvlari axborot xavfsizligini ta'minlashda muhim o'rin tutadi. Shu bilan birga, kiberjinoyatchilik va raqamli xavf-xatarlarning global xarakterga ega ekanligi sababli, davlatlar o'rtasidagi integrasiya va hamkorlikning ahamiyati kun sayin ortib bormoqda. Bu konferensiya, kiberhuquq sohasida global hamkorlikni mustahkamlash uchun platforma vazifasini o'taydi.

Bugungi tadbirning asosiy maqsadi – raqamli rivojlanishning huquqiy oqibatlarini chuqur o‘rganish, kiberhuquq sohasida mavjud muammolarni aniqlash va ularga amaliy echimlar topishdir. Umid qilamizki, ushbu konferensiya kiberhuquq sohasida yangi fikrlar va amaliy echimlar ishlab chiqishga yo‘naltirilgan ilmiy muhokamalar va mulohazalarni ilgari suradi.

Ayni vaqtda prokurorlik faoliyatida sun’iy intellektdan foydalanish masalasi alohida ahamiyat kasb etmoqda. Uning dolzarbligi, avvalo, nazorat faoliyatini optimallashtirishga, ya’ni birlamchi ma’lumotlarni qayta ishlashga, qonun ustuvorligini ta’minlashga, prokuratura organlarining nazorat faoliyatining sifat va samaradorligini oshirish nuqti nazaridan o‘ta muhim hisoblanadi.

Buning uchun nazarimizda prokuratura organlarining nazorat faoliyatida sun’iy intellektni joriy etish bo‘yicha davlat vazifalarini bajarishda prokuratura xodimlarining yagona yondashuvini ishlab chiqish zarur. Nazorat amaliyoti tajribasi va prokurorlik nazorati sohasidagi mavjud ilmiy muammolarni tezroq hal etish zaruratini hisobga olgan holda, nazorat faoliyatini takomillashtirish uchun tegishli tadbirlarni amalga oshirish maqsadga muvofiqdir. Bu prokuratura faoliyatining ustuvor yo‘nalishlaridan biri bo‘lib, nazariy-huquqiy va texnologik xarakterdagi chora-tadbirlarni o‘z ichiga oladi.

Bu yerda prokuratura organlarini tashkil etish va faoliyatini huquqiy tartibga solish; prokurorlik nazorati nazariyasini takomillashtirish (prokurorlik nazoratining ilmiy muammolarini nazariy-amaliy tadqiqotlar orqali o‘rganish); nazorat faoliyatini tashkil etish va amalga oshirishning shakl va usullarini takomillashtirish, shu jumladan ilmiy va amaliy tadqiqotlar natijalariga asoslangan holda amalga oshirish; raqamli texnologiyalar, jumladan sun’iy intellektni qo‘llash orqali nazorat faoliyatini optimallashtirish nazarda tutiladi. Buning doirasida ilmiy va amaliy tajribalar natijalariga asoslangan harakatlar algoritmini maxsus dastur orqali bajarish, vujudga kelgan vaziyatlarda samarali qarorlar qabul qilish, ushbu qarorlarni to‘plash, saqlash, qo‘llash va ma’lumotlarni himoya qilishni ta’minlash kabi tadbirlar amalga oshiriladi.

Ma’lumki, nazorat faoliyatini tashkil etish va amalga oshirishda raqamli texnologiyalardan foydalanish samaradorligi tegishli huquqiy va nazariy bazaning mavjudligiga ko‘proq bog‘liq bo‘ladi. Bu esa o‘z navbatida ushbu yo‘nalishdagi nazorat amaliyotining ijobiy tajribasi va prokuratura nazorat faoliyatining sifat va natijadorligini oshirishga qaratilgan ilmiy tadqiqotlar natijalari orqali shakllanadi.

Bu yerda, ayniqsa, ilmiy tadqiqotlarning nazorat faoliyatini takomillashtirishdagi rolini alohida ta’kidlash zarur. Ilmiy tadqiqotlar

nazorat faoliyatini tashkil etish va amalga oshirishning yangi shakl va usullarini, shu jumladan sun’iy intellektdan foydalangan holda, ishlab chiqishga yordam beradi.

O‘zbekiston Respublikasi Konstitutsiyasining 53-moddasiga ko‘ra, har kimga ilmiy, texnikaviy va badiiy ijod erkinligi, madaniyat yutuqlaridan foydalanish huquqi kafolatlanadi. Intellektual mulk qonun bilan muhofaza qilinadi. Davlat jamiyatning madaniy, ilmiy va texnikaviy rivojlanishi haqida g‘amxo‘rlik qiladi.[1]

Biz so‘z bilan aytganda, jamiyatning ilmiy rivojlanishi masalasi ham davlat vazifalari doirasiga kiradi.

Qonun ustuvorligini ta’minlash prokurorlik nazorati samaradorligini talab etadi, bu esa nazorat faoliyatining sifati va natijadorligiga bog‘liq holda amalga oshiriladi. Nazorat faoliyati sifati esa faqatgina nazorat tadbirlarining hajmi va chuqurligi, ya’ni nazorat mavzusi bilan belgilangani bilan emas, balki nazorat jarayonining o‘ziga xos xususiyati bilan ham belgilanadi. Bu, avvalo, prokuror tomonidan amalga oshiriladigan harakatlarning bosqichma-bosqichligi, izchilligi va nazorat faoliyatining har bir bosqichida belgilangan maqsad va vazifalarning to‘liq amalga oshirilishi bilan tavsiflanadi.

Biz prokuratura organlarining nazorat faoliyatini tizimli ravishda tashkil etilgan va izchil amalga oshiriladigan prokuror harakatlari majmui sifatida tushunamiz. Ushbu harakatlar belgilangan maqsad va vazifalar bilan bog‘liq bo‘lib, qonun buzilishlari va ularga olib keluvchi holatlarni aniqlash hamda bartaraf etishga qaratilgan. Qonun ustuvorligini to‘liq tiklash uchun ushbu harakatlar amalga oshiriladi.

Nazorat faoliyati samaradorligi va sifatiga erishishda asosiy omillardan biri taktikani to‘g‘ri qo‘llashdir. Taktika prokuror harakatlarining mufassal va tizimli bo‘lishini ta’minlaydi, nazorat holatining mavjud sharoitlarini doimiy tahlil qilish orqali tanlangan usul va harakatlar tartibini ishlab chiqish va amalga oshirish uchun asos bo‘ladi.

Hozirgi kunda prokurorlik faoliyati taktikasi nazariya va amaliyotda yetarli darajada o‘rganilmagan va bu raqamli texnologiyalar asrida tezkor yechim talab etuvchi ilmiy muammo hisoblanadi. Ushbu ilmiy muammoni hal etish maqsadida biz muayyan harakatlarni amalga oshirdik va prokurorning nazorat faoliyatini tashkil etish hamda amalga oshirishda taktikadan foydalanish borasida ilmiy-amaliy tadqiqot o‘tkazdik. Ushbu tadqiqot natijasida dastlabki asosiy xulosalar qo‘lga kiritildi.

[1] O‘zbekiston Respublikasi Konstitutsiyasi // https://lex.uz/docs/6445145

Biz prokurorlik nazorat faoliyati taktikasi tushunchasini nazorat faoliyatini tashkil etish va amalga oshirishda eng maqsadga muvofiq usul va harakatlarni ishlab chiqish uchun zarur bo‘lgan oqilona yechimlarni topish va amalga oshirish jarayoni sifatida tushunamiz.

Yuridik adabiyotlar tahlili shuni ko‘rsatadiki, prokurorlar faoliyatini optimallashtirish maqsadida, qonun ustuvorligi holati to‘g‘risida obyektiv ma’lumotlarni yig‘ish uchun maxsus elektron kartalarni yaratish taklif etilmoqda. Ushbu kartalarda nazorat faoliyati yo‘nalishlari bo‘yicha har bir nazoratdagi obyektga tegishli ma’lumotlar alohida qayd etiladi.

Nazorat obyektining ma’lumotlarini tizimli va kompleks tahlil qilish hamda ularni doimiy ravishda yangilash quyidagilarga yordam beradi:

tekshiruvlarni tashkil qilish va o‘tkazish bo‘yicha oqilona taktikani ishlab chiqish va amalga oshirish;

nazorat ostidagi obyektda qonun ustuvorligi holati va prokuratura nazorati samaradorligi to‘g‘risida dolzarb ma’lumot-larni olish va saqlash, shuningdek, nazorat faoliyatini tashkil qilish va amalga oshirishning ratsional usullarini ishlab chiqish.

Ushbu tahlil natijalari nazorat faoliyatini rejalashtirish, nazorat holatlarini prognoz qilish, qonun ustuvorligi holati va uning dinamikasiga ta’sir etuvchi omillarni aniqlash va ma’lum bir davrdagi statistik va tahliliy ma’lumotlarga asoslangan qonun ustuvorligi holatini shakllantirish uchun asos bo‘ladi.

Qonun ustuvorligi holati bo‘yicha dastlabki ma’lumotlarni qayta ishlashdan tashqari, elektron kartada aniq nazorat obyektiga doir barcha yakuniy ma’lumotlar saqlanishi tavsiya etiladi. Ushbu ma’lumotlar tekshiruv va profilaktik faoliyat natijalarini, idoralararo hamkorlik samaradorligi baholarini hamda har bir tekshiruv tadbiri natijalarini o‘z ichiga oladi.

Elektron karta mazmunini prokuraturaning nazorat faoliyati sifatini, samaradorligini va natijadorligini oshirish maqsadida dasturiy mahsulot sifatida joriy etish mumkin. Ilgari ayrim olimlar prokurorlarning tahliliy faoliyatida yordam beradigan tizimli kompyuter dasturlaridan foydalanishni taklif qilgan. Ushbu dasturiy ta’minotga quyidagi asosiy masalalarni tahlil qilish kiritilgan: qonun ustuvorligi holati, mintaqaning ijtimoiy-iqtisodiy ahvoli, prokurorlik aralashuvini talab etuvchi ma’lumotlar va h.k.

Elektron kartada prokurorlar tomonidan nazorat obyekti va mavzulari bo‘yicha quyidagi ma’lumotlarni qayd etish tavsiya etiladi:

Nazorat obyekti to‘g‘risidagi ma’lumotlar (faoliyat sohasi, huquqiy tartibga solish, tuzilma va h.k.);

Prokurorlik tekshiruvlarini o‘tkazish asoslari va davriyligi;

Prokuror tomonidan amalga oshirilgan ishlar xususiyati (tekshiruv o‘tkazish, nazorat ostidagi obyekt tashabbusi bilan o‘tkazilayotgan tekshiruvda qatnashish, profilaktik tadbirlar, obyektga tashrif buyurish, qo‘shma yig‘ilishlarda ishtirok etish, profilaktik faoliyat va h.k.).

Bunday ma’lumotlar bazasini yuritish prokurorlarning faoliyatini sezilarli darajada yengillashtiradi va quyidagi jarayonlarda zarur ma’lumotlarni tezkor olishni ta’minlaydi:

tekshiruvlarni tashkil qilish va o‘tkazishda;

yuqori prokuraturalar tomonidan berilgan shoshilinch topshiriqlarni bajarishda;

amalga oshirilgan tekshiruvlar sifatini va prokurorlik ta’sir choralarini tahlil qilishda;

qonun ustuvorligi holatini prognoz qilish va nazorat tadbirlarini rejalashtirishda;

tanlangan taktika va nazorat tadbirlarining samaradorligini baholashda va boshqalarda.

Elektron kartalarni yuritishni prokuratura tizimining barcha bo‘g‘inlarida, yuqoridan boshlab quyi darajalargacha, amalga oshirish maqsadga muvofiqdir. Elektron kartalarga o‘zgartish kiritish huquqi tegishli prokurorlar kompetensiya va vakolatlariga muvofiq ravishda amalga oshirilishi lozim.

Biroq, elektron kartalardan to‘liq foydalanish prokuratura nazorat faoliyati taktikasi ishlab chiqilmasdan imkonsizdir. Nazorat faoliyati taktikasi prokurorlik nazoratining sifat va samaradorligining asosiy omili hisoblanadi.

Shu munosabat bilan prokurorlik nazorati taktikasi asoslarini ilmiy-amaliy o‘rganish bo‘yicha tadqiqotlarni davom ettirish zarur. Bunday tadqiqotning asosiy maqsadi – prokuratura nazorat faoliyati taktikasi ishlab chiqish va amalga oshirishda yagona algoritmni yaratishdir. Ushbu algoritm (yoki taktikani ishlab chiqish va amalga oshirish formalizatsiyasi) prokuratura organlari nazorat faoliyatiga sun’iy intellektni joriy etish uchun asos sifatida tavsiya etiladi.

Prokuratura organlari nazorat faoliyatini takomillash-tirish uchun sun’iy intellektdan foydalanish bo‘yicha takliflar O‘zbekiston Respublikasi Prezidentining 2024 yil 14 oktyabrdagi “Sun’iy intellekt texnologiyalarini 2030 yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PQ-358-son qarori bilan tasdiqlangan Sun’iy intellekt texnologiyalarini 2030 yilga qadar rivojlantirish strategiyasi[2]ga muvofiq keladi.

[2] O‘zbekiston Respublikasi Prezidentining 2024 yil 14 oktyabrdagi “Sun’iy intellekt texnologiyalarini 2030 yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PQ-358-son qarori // https://www.lex.uz/docs/7158604

Prokuratura organlari nazorat faoliyatiga sun’iy intellektni joriy etish uchun quyidagilarni amalga oshirish maqsadga muvofiqdir:

Qonunchilik darajasida:

prokuratura organlarining nazorat faoliyatining asosiy bosqichlarini, ularning maqsad va vazifalarini belgilash;

prokuratura organlari faoliyatini tashkil qilish va amalga oshirish to‘g‘risidagi amaldagi qonunchilikni takomillashtirish va uni tekshiruvlar o‘tkazishda nazorat faoliyati taktikasidan foydalanish bo‘yicha qoidalar bilan to‘ldirish. Taktikani ishlab chiqish va amalga oshirish algoritmini O‘zbekiston Respublikasi Bosh prokurorining buyrug‘i bilan tasdiqlash.

Prokuratura organlari amaliyotida:

nazorat obyektlarining elektron karta ma’lumotlarini qayta ishlash bo‘yicha dasturni joriy etish va ma’lumotlarni himoya qilish bo‘yicha choralarni ko‘rish.

Prokuror nazorati nazariyasida:

prokuror nazorati taktikasi asoslari bo‘yicha ilmiy-amaliy tadqiqotlarni davom ettirish va ularning natijalarini prokuratura organlari amaliyotiga joriy etish, nazorat faoliyatining sifat va samaradorligini oshirish.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ОХРАНЫ ПРАВОПОРЯДКА

Коленко Евгений Вячеславович
Первый заместитель начальника Правоохранительной академии Республики Узбекистан, PhD, доцент

Аннотация. *The article analyzes current innovative technologies in law enforcement activities. It examines the role of artificial intelligence (AI) in the legal protection system, as well as the legal and ethical aspects of its application. The contribution of AI to the development of legal norms, crime fighting, law enforcement activities, and legal analysis is described. The article also highlights the challenges and prospects of using AI to safeguard human rights and ensure the objectivity of judicial processes. The legal foundations for implementing AI in practice and the need for its legal regulation are discussed. The study is relevant and important for legal professionals, policymakers, and anyone interested in innovative technologies.*

Ключевые слова: *искусственный интеллект, цифровая криминалистика, киберпреступность, киберправо, цифровые доказательства, международное сотрудничество, образовательные программы, цифровая безопасность.*

Аннотация. *Мақолада ҳуқуқни муҳофаза қилиш фаолиятида замонавий инновацион технологияларни таҳлил этади. Унда сунъий интеллект (СИ)нинг ҳуқуқни муҳофаза қилиш тизимларидаги ролини, шунингдек, ушбу технологиянинг қонуний ва этик жиҳатларини кўриб чиқиш мумкин. Мақолада*

сунъий интеллектнинг ҳуқуқий нормалар, жиноятчиликка қарши кураш, полиция фаолияти ва ҳуқуқий таҳлил соҳасидаги амалиётларга қўшган ҳиссаси тавсифланади. Яна, инсон ҳуқуқларини ҳимоя қилиш ва суд жараёнларидаги объективликни таъминлашда СИнинг муаммолари ва истиқболларига эътибор қаратилган. Мақола, шунингдек, сунъий интеллектни амалиётда жорий қилишнинг ҳуқуқий асосларини ва қонуний тартибга солишнинг зарурлигини муҳокама қилади. Бу тадқиқот, ҳуқуқий соҳадаги профессионаллар, сиёсатчилар ва инновацион технологиялар билан қизиқувчилар учун долзарб ва муҳим аҳамиятга эга.

Калит сўзлар: *суниий интелект, рақамли криминалистика, кибержиноятчилик, киберҳуқуқ, рақамли далиллар, халқаро ҳамкорлик, таълим дастурлари, рақамли хавфсизлик.*

Abstract. *The article examines the current issues of digital forensics development in the Republic of Uzbekistan through the example of the Law Enforcement Academy's activities. It analyzes modern challenges and threats in the field of cybercrime, as well as measures taken to counter them. Special attention is paid to describing the Academy's technical and methodological equipment, including specialized software and hardware for digital investigations. The article discusses educational programs for training specialists in cyber law and digital forensics, including plans to introduce a new master's program. The Academy's international cooperation and its role in developing methodological materials and regulatory legal acts are highlighted. Specific examples of successful assistance to law enforcement agencies in solving cybercrimes are presented. The article emphasizes the importance of further developing capabilities in digital forensics for effectively countering modern cyber threats.*

Keywords: *artificial intelligence, digital forensics, cybercrime, cyber law, digital evidence, international cooperation, educational programs, digital security.*

Искусственный интеллект (ИИ) становится важным инструментом для повышения эффективности работы правоохранительных органов. Его потенциал позволяет улучшить анализ данных, автоматизировать рутинные процессы и ускорить расследование преступлений. В этой статье рассматриваются основные преимущества ИИ для правоохранительной деятельности и его вклад в обеспечение безопасности общества.

Осознавая важность этих угроз, 13 января 2023 года на расширенном заседании Совета безопасности Президент Республики Узбекистан Шавкат Мирзиёев отметил, что в условиях растущих геополитических противостояний обостряются проблемы в различных сферах — экономической, социальной, политической, а также информационной безопасности. Президент подчеркнул, что защита информационной безопасности становится одной из приоритетных задач для обеспечения стабильности и устойчивости страны в условиях увеличивающейся цифровой уязвимости.

Применение ИИ делает возможным более точное и быстрое проведение оперативных мероприятий. Алгоритмы позволяют правоохранительным органам эффективно управлять временем, выделять приоритетные задачи и принимать меры на основе анализа в реальном времени.

Для безопасного и справедливого использования ИИ необходимо соблюдать этические нормы и стандарты. Органам важно обеспечивать защиту конфиденциальности данных и исключать предвзятость алгоритмов. Прозрачность и независимые проверки помогут минимизировать риски и повысить доверие общества.

Искусственный интеллект открывает новые возможности для правоохранительных органов, способствуя повышению их эффективности и обеспечению безопасности. При этом важно учитывать этические и правовые аспекты, чтобы технологии использовались справедливо и защищали права граждан. Умное и ответственное внедрение ИИ в работу органов правопорядка станет залогом улучшения качества услуг и укрепления общественной безопасности.

К примеру, программное обеспечение «Magnet Axiom» обеспечивает комплексный подход к обработке цифровых данных, интегрируя информацию из различных источников в единую систему анализа. Это повышает точность и удобство работы с разрозненными цифровыми доказательствами. Также НИИ цифровой криминалистики получила доступ к специализированным информационным системам, таким как DarkWebMonitor, Elliptic ICAC-COPS и Arthropod. Эти системы позволяют отслеживать незаконную активность в даркнете, анализировать криптовалютные транзакции и существенно расширяют возможности расследования киберпреступлений, связанных с незаконными операциями в онлайн-пространстве, включая борьбу с распространением детской порнографии и другими серьёзными угрозами.

Для создания криминалистических копий цифровой информации и защиты данных было приобретено специализированное оборудование — комплекты дубликаторов и блокираторов Tableau, которые позволяют выполнять побитовое копирование данных без риска их повреждения или изменения. Это особенно важно при работе с цифровыми доказательствами, где

требуется максимальная точность и сохранность данных.[3] С целью восстановления данных с повреждённых и сложных носителей информации академия приняла в эксплуатацию аппаратно-программный комплекс PC-3000 Portable PRO, обладающий высокой функциональностью для работы с физическими носителями данных, что позволяет восстанавливать информацию даже с повреждённых или частично неработоспособных устройств.

Такие программные продукты и оборудование значительно расширяют технический потенциал академии и обеспечивает возможность эффективной работы с широким спектром цифровых носителей, что повышает качество и достоверность анализа цифровых доказательств.

В Академии ведется подготовка специализированной лаборатории для работы с цифровыми носителями, отвечающей международным стандартам ISO/IEC 17025-201[4] и ISO 14644-1:201[5]. Лаборатория будет оборудована герметичной конструкцией, обеспечивающей защиту от проникновения пыли и внешнего электромагнитного излучения. Такая защита необходима для создания стабильных условий, в которых можно проводить анализ цифровых данных и экспертизы без риска внешнего воздействия на информацию.

Правоохранительная академия Республики Узбекистан придает особое значение методическому сопровождению деятельности правоохранительных органов, что позволяет эффективно интегрировать новые подходы и технологии в повседневную работу по противодействию цифровой преступности.

Несмотря на относительно короткую историю работы, академия уже имеет ряд успешных примеров содействия в раскрытии преступлений. Так, проведено изучение, направленное на противодействие распространению детской порнографии. В ходе этого исследования специалисты академии сосредоточились на выявлении и анализе каналов распространения данного контента на территории Республики Узбекистан. По результатам работы полученные сведения были оперативно переданы в правоохранительные органы для принятия необходимых мер. Этот

[3] Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. – 2018. – №1 – С. 450-260.

[4] ISO/IEC 17025:2019 General requirements for the competence of testing and calibration laboratories [Электронный ресурс] – https://www.iasonline.org/wp-content/uploads/2021/02/ISO-IEC-17025-2017-IAS.pdf Дата доступа: 05.11.2024 г.

[5] ISO 14644-1:2015 General requirements for the competence of testing and calibration laboratories [Электронный ресурс] – https://antoandoluong.com/Files/Docs/20203181613304.pdf Дата доступа: 05.11.2024 г.

подход позволил не только выявить в двух регионах станы источники распространения и привлечь виновных лиц к ответственности, но и наладить эффективное взаимодействие с правоохранительными органами для защиты общества и особенно уязвимых категорий граждан.

Также, был проведен анализ вредоносного программного обеспечения, используемого для несанкционированного доступа к банковским картам через фиктивные сайты транспортных компаний, инициированы исследования, направленные на изучение активности денежных мулов и предотвращение незаконных транзакций и др. Исследования выявили методы, применяемые злоумышленниками для обмана пользователей и хищения данных. Полученная информация и методики противодействия были также переданы правоохранительным органам.

Сотрудники института совместно с экспертами-криминалистами Министерства внутренних дел разработали, утвердили и внесли в государственный реестр методику проведения экспертных исследований мобильных устройств. Эта методика стандартизирует процесс исследования мобильных устройств, обеспечивая высокий уровень качества и точности проводимых экспертиз.[6]

В настоящее время ведется разработка методики экспертно-криминалистического анализа больших данных (Big Data). Эта методика направлена на повышение эффективности обработки и анализа цифровой информации, что имеет особое значение при расследовании преступлений, связанных с большими массивами данных, например, в случаях киберпреступности или финансовых преступлений.

Особое значение придается базовой подготовке следователей и прокуроров на основе программ бакалавриата. В рамках образовательных направлений «Следственная деятельность» и «Прокурорская деятельность» на протяжении всего обучения осуществляется преподавание дисциплин, посвященных киберправу, расследованию киберпреступлений и другим ключевым аспектам цифровой криминалистики. Эти предметы позволяют студентам овладеть теоретическими знаниями и практическими навыками, необходимыми для успешной работы в условиях стремительно меняющегося цифрового мира.

[6] Sud-ekspertlik ilmiy-tadqiqot instituti tomonidan tanqidiy ko’rib chiqilgan va sud-ekspertlik sohasiga oid yagona reestrga kiritilgan uslubiy qo‘llanmalar [Электронный ресурс]. - https://sudex.uz/?page_id=4801 Дата доступа: 06.11.2024 г.

В учебный процесс Правоохранительной академии внедрен модуль «Киберправо», который охватывает 60 учебных часов в рамках 6 курсов общей продолжительностью 360 часов. В рамках модуля «Киберправо» в учебный процесс включены специализированные курсы «Основы цифровой криминалистики в борьбе с киберпреступностью», «Информационные технологии», «Параллельное расследование», «Оперативно-розыскное право», «Киберправо» и др.

Введение профильных учебных дисциплин по киберправу и кибербезопасности, а также их постоянное обновление с учетом актуальных вызовов, позволит будущим следователям и прокурорам эффективно противостоять современным угрозам и активно участвовать в развитии правовой системы для обеспечения цифровой безопасности.

Аналогичная работа проводится и по образовательным программам магистратуры, включающих такие направления, как «Прокурорская деятельность», «Следственная деятельность», «Международное право прав человека» и «Противодействие коррупции». Эти программы дают слушателям возможность углубленно изучать специфику различных аспектов правоприменительной практики в цифровой среде, осваивать современные методики и подходы, а также развивать навыки аналитической и исследовательской работы.

В соответствии с решением Президента Республики Узбекистан, с 2025/2026 учебного года в Правоохранительной академии планируется внедрение программы магистратуры по новой специальности «Киберправо». Это нововведение позволит готовить высококвалифицированных специалистов, обладающих углубленными знаниями в области правового регулирования цифровой среды и кибербезопасности и обеспечит их актуальными навыками для работы с новейшими технологиями, а также для создания и реализации правовых норм, направленных на защиту интересов государства и общества в условиях цифровизации.[7]

Так, в 2024 году авторским коллективом Правоохранительной академии и Ташкентского государственного юридического университета подготовлен учебник «Киберправо», ставшим важным шагом в создании современной образовательной базы для

[7] Постановление Президента Республики Узбекистан № ПП-381 «О мерах по усилению защиты прав потребителей цифровой продукции (услуг) и борьбы с правонарушениями, совершаемыми посредством цифровых технологий» от 1 декабря 2024 г. [Электронный ресурс]. - https://lex.uz/docs/6681115 Дата доступа: 06.11.2024 г.

подготовки специалистов в области киберправа и цифровой криминалистики. Учебник охватывает ключевые аспекты правового регулирования киберпространства и знакомит читателей с отраслевыми международными стандартами, практиками и правовыми нормами.[8]

Планируется, что в ближайшем будущем учебник будет опубликован на английском и узбекском языках, что позволит использовать его как на национальном уровне, так и в международной академической среде. Двухъязычное издание сделает учебник доступным для широкого круга специалистов, обучающихся и работающих в сфере киберправа, и будет способствовать укреплению сотрудничества с зарубежными партнерами в области цифровой безопасности и правоприменительной деятельности в киберпространстве.

Ранее, при технической поддержке Офиса координатора проектов в Узбекистане ОБСЕ создано первое учебное пособие по цифровой криминалистике, являющийся уникальным учебным пособием для специалистов в этой области. Это издание, подготовленное на русском и узбекском языках, стало важнейшим инструментом для формирования базовых и углубленных знаний среди следователей, занимающихся расследованием преступлений в цифровой среде. Пособие включает в себя основные методы и приемы цифрового анализа, принципы сбора, сохранения и обработки цифровых доказательств, а также раскрывает особенности расследования киберпреступлений.[9]

Пособие было распространено среди всех следователей республики, что позволило обеспечить их необходимыми знаниями и практическими навыками для эффективного противодействия киберпреступности.

Разработано и внедрено в учебный процесс пособие по исследованию мобильных устройств, которое включает в себя научно обоснованные алгоритмы и протоколы исследования информации в мобильных устройствах.

Правоохранительная академия Республики Узбекистан стала одним из разработчиком законопроекта о введении в национальное законодательство понятия «электронное (цифровое)

[8] O’zbekiston Respublikasi Huquqni muhofaza qilish akademiyasida Kiberhuquq bo’yicha xalqaro konferensiya o’tkazildi. [Электронный ресурс]. - https://gulyamov.org/ru/international-conference-on-cyber-law-held-at-the-academy-of-law-enforcement-of-uzbekistan/ Дата доступа: 06.11.2024 г.

[9] Г. Ф. Мусаев [ва бошқ.]. Ахборот технологиялари соҳасидаги жиноятлар (кибержиноятлар): турлари, квалификацияланиши ва уларга нисбатан тергов ҳаракатларини ўтказиш тактикаси. [Электронный ресурс] - https://proacademy.uz/ru/e-library/index?alias=628 Дата доступа: 06.11.2024 г.

доказательство». Этот законопроект призван урегулировать правовой статус цифровых данных, используемых в качестве доказательств в уголовных и других видах производства, что является важным шагом в обеспечении правовой определенности и эффективности расследования преступлений, связанных с использованием цифровых технологий.[10]

Особое внимание в Правоохранительной академии Республики Узбекистан уделяется укреплению основ международного сотрудничества, что позволяет эффективно реагировать на глобальные вызовы, связанные с цифровой криминалистикой и киберпреступностью. Академия активно взаимодействует с международными организациями и правоохранительными структурами других стран, что способствует обмену знаниями, опытом и передовыми технологиями.

Развитие международного сотрудничества позволяет академии интегрировать в учебный процесс лучшие мировые практики, а также адаптировать международные стандарты к национальной правовой системе. Укрепление таких связей играет ключевую роль в повышении квалификации узбекских специалистов и создает основу для формирования надежной системы противодействия киберпреступности на глобальном уровне.

В Правоохранительной академии Республики Узбекистан были проведены многочисленные конференции, семинары и тренинги по тематике расследования киберпреступлений, использования OSINT, работы с цифровыми активами, а также проблем Darkweb, криптовалют и блокчейн, с участием ведущих экспертов из США, Великобритании, России, Беларуси, Латвии, Казахстана, Турции, Грузии, Республики Корея и других стран[11]. Эти мероприятия стали важной площадкой для обмена знаниями и передовыми практиками в области цифровой криминалистики, кибербезопасности и правового регулирования в цифровой среде.

Участие международных экспертов позволило студентам и сотрудникам академии ознакомиться с различными подходами к расследованию киберпреступлений, освоить новейшие методы и технологии, применяемые в других странах, а также укрепить профессиональные связи с зарубежными коллегами.

---

[10] Депутаты приняли закон о цифровых доказательствах с третьего раза. [Электронный ресурс] - https://www.gazeta.uz/ru/2024/08/27/digital-evidence/ Дата доступа: 06.11.2024 г.

[11] Состоялся семинар-тренинг по проведению следственных действий в отношении криптоактивов // Официальный сайт правоохранительной Академии Республики Узбекистан [Электронный ресурс] – https://proacademy.uz/ru/news/view?alias=1775 Дата доступа: 06.11.2024 г.

В заключение необходимо отметить, что Правоохранительной академией проделана определенная работу по формированию потенциала в развитии и укреплении цифровой криминалистики, заложив фундамент для подготовки высококвалифицированных специалистов, способных эффективно противостоять современным цифровым угрозам.

Однако, несмотря на все достигнутые результаты, многое еще предстоит сделать. В условиях стремительно развивающихся технологий и постоянного появления новых форм киберпреступности академии необходимо продолжать совершенствовать свои программы, расширять научно-исследовательскую деятельность и укреплять международное сотрудничество. Предстоит работа по созданию дополнительных методик, внедрению практики использования современного оборудования и развитию комплексных образовательных программ, чтобы соответствовать глобальным стандартам и новейшим достижениям в сфере цифровой криминалистики. Эти усилия позволят академии и в дальнейшем эффективно содействовать обеспечению правопорядка и верховенства права, готовя специалистов, способных решать сложные задачи правоохранительной деятельности в цифровом пространстве на самом высоком уровне.

ПРОКУРАТУРА ОРГАНЛАРИ ФАОЛИЯТИНИ РАҚАМЛИ ТРАНСФОРМАЦИЯ ҚИЛИШНИНГ ТАШКИЛИЙ-ҲУҚУҚИЙ АСОСЛАРИНИ ТАКОМИЛЛАШТИРИШ

Бобоев Миршод Муротович,
Ўзбекистон Республикаси Бош прокуратураси
Ахборот-коммуникация технологияларини жорий
этиш ва ахборот хавфсизлигини таъминлаш бошқармаси бошлиғи,
юридик фанлар бўйича фалсафа доктори (PhD)

Аннотация: *Мақолада прокуратура органлари фаолиятини рақамли трансформация қилишнинг мақсадлари, вазифалари, асосий йўналишлари ҳамда ташкилий-ҳуқуқий асослари ўрин олган. Прокуратура органлари фаолиятига ахборот-коммуникация технологияларини жорий этиш бўйича норматив-ҳуқуқий ҳужжатлар ижроси таҳлил қилинган. Прокуратура органлари ахборот тизимлари вазифалари, уларда фаолият шаффофлигини таъминловчи механизмлар кўриб чиқилган. Прокуратура органлари инфратузилмасининг жорий этилган элементлар кўрсатилган. Бош прокуратуранинг ихтисослаштирилган бошқармаси ҳақида маълумот берилган. Вазирлик, идоралар ахборот тизимлари ва ресурслари билан интеграция қилиш зарурати, бу борада*

қабул қилинган норматив-ҳуқуқий ҳужжатлар ва бажарилган ишлар таҳлил қилинган.

Калит сўзлар: *рақамли трансформация, прокуратура органлари, ахборот-коммуникация технологиялари, тенденциялар, миллий қонунчилик, Маълумотларни қайта ишлаш маркази, корпоратив ҳисоблаш тармоғи, ахборот тизимлари.*

Аннотация: *В статье учтены цели, задачи, основные направления, организационно-правовые основы цифровой трансформации деятельности органов прокуратуры. Проанализировано исполнение нормативно-правовых актов по внедрению информационно-коммуникационных технологий в деятельность органов прокуратуры. Рассмотрены задачи информационных систем и механизмы, обеспечивающие прозрачность деятельности. Показаны внедренные элементы инфраструктуры органов прокуратуры. Дана информация о специализированном управлении Генеральной прокуратуры. Проанализирована необходимость интеграции с информационными системами и ресурсами министерств и ведомств, принятых в этой связи нормативно-правовых актов и выполненные работы.*

Ключевые слова: *цифровая трансформация, органы прокуратуры, информационно-коммуникационные технологии, тенденции, национальное законодательство, Центр обработки данных, корпоративная вычислительная сеть, информационные системы.*

Abstract: *The article considers the goals, objectives, main directions, and organizational and legal foundations of the digital transformation of the activities of the prosecutor's offices. It analyzes the implementation of regulatory acts on the introduction of information and communication technologies in the activities of the prosecutor's offices. The tasks of information systems and mechanisms ensuring transparency of activities are examined. The implemented elements of the prosecutor's office infrastructure are presented. Information is provided about the specialized department of the General Prosecutor's Office. The necessity of integration with the information systems and resources of ministries and departments, the regulatory acts adopted in this regard, and the work carried out are analyzed.*

Keywords: *digital transformation, prosecutor’s offices, information and communication technologies, trends, national legislation, Data processing center, corporate computer network, information systems.*

Сўнгги йилларда республикамизда суд-ҳуқуқ соҳасини демократ-лаштириш ва либераллаштириш, ижтимоий-иқтисодий ислоҳотларни амалга оширишда прокуратура органларининг ролини кучайтириш борасида кенг кўламли ишлар амалга оширилди. Ислоҳотлар самараси ўлароқ жисмоний ва юридик шахсларнинг судлар ва ҳуқуқни муҳофаза қилувчи органларга ишончи ортиб, мурожаатлар кўпайиб бораётганида ҳам яққол намоён бўлмоқда.

Дарҳақиқат, барча соҳа ва тармоқларда, энг аввало, давлат бошқаруви, таълим, соғлиқни сақлаш ва қишлоқ хўжалигида

фаолият шаффофлигини ошириш, коррупция хатарларини камайтириш ва ҳуқуқбузарликларнинг олдини олиш ҳамда аҳоли учун қулайлик яратиш мақсадида маъмурий жараёнларни рақамлаштириш бўйича ислоҳотлар олиб борилмоқда.

Шу билан бирга, мамлакатимизнинг, шунингдек хорижий ва халқаро ҳуқуқни муҳофаза қилувчи идоралар фаолияти натижадорлигини фаол жорий этилаётган ахборот-коммуникация технологияларисиз тасаввур этиб бўлмайди.

Албатта, бу тенденциялар Ўзбекистон прокуратура органлари фаолиятини рақамли трансформация қилинишини тақозо этади.

“Прокуратура тўғрисида”ги Қонунда прокуратура органлари фаолиятининг 9 та асосий йўналишлари белгиланган.

Ушбу йўналишларни рақамли трансформация қилишдан кўзланган мақсадлар фаолият самарадорлиги, тезкорлиги ва шаффофлигини ошириш, қонун ҳужжатлари ижроси устидан назоратни амалга ошириш усулларини такомиллаштириш, фуқаролар ва тадбиркорлик субъектларининг ҳуқуқлари ҳамда қонуний манфаатлари ҳимоя қилинишини таъминлашдан иборат.

Шундан келиб чиқиб, прокуратура органлари фаолиятини рақамлаштириш бўйича бир қатор норматив-ҳуқуқий ҳужжатлар қабул қилинган.

Фаолиятни рақамлаштириш билан боғлиқ дастлабки ҳуқуқий ҳужжатлар бу Ўзбекистон Республикаси Президентининг 2015 йил 16 ноябрдаги ПҚ-2433-сонли Қарори билан тасдиқланган “Прокуратура органлари фаолиятига замонавий ахборот-коммуникация технологияларини жорий этиш бўйича чора-тадбирлар дастури” бўлди.

Ундан кейин эса Ўзбекистон Республикаси Президентининг 2016йил 29 июлдаги ПҚ-2568-сонли қарорига мувофиқ, Бош прокуратура тузилмасида Ахборот-коммуникация технология-ларини жорий этиш ва ахборот хавфсизлигини таъминлаш бошқармаси ва унинг жойлардаги тармоқлар ташкил этилди.

Ўзбекистон Республикаси Президентининг юқорида қайд этилган ҳужжат ларига ҳамда Бош прокурорнинг буйруқ ва топшириқлари билан прокуратура органларининг ахборот инфратузилмаси яратилиб, фаолиятнинг асосий йўналишларини рақамлаштириш бўйича чора-тадбирлар амалга оширилди.

Хусусан, Бош прокуратурада замонавий, барча талабларга жавоб берадиган Маълумотларни қайта ишлаш маркази ташкил этилди.

Прокуратура органларида локал ҳисоблаш тармоқлари яратилди. Уларни ўзаро боғлаш учун оптик толали линиялар ўтказилиб, корпоратив тармоқ ишга туширилди. IP-телефония ва аудио-конференцалоқа тизимлари яратилиб, республика миқёсида жорий этилди, видео-конференцалоқа тизимлари ишга туширилди. Ишчи ўринлар замонавий компьютер ва офис техникаси билан жиҳозланди.

Ушбу чоралар 2019-2024 йилларда 35 та ахборот тизими ишлаб чиқишга ва 100 дан ортиқ ахборот тизимлари билан интеграция қилинишига ҳамда уларни узлуксиз ва барқарор ишлаши учун асос бўлди.

Прокуратура органларининг тузилмаси ва фаолияти ўзига хос хусусиятларини инобатга олган ҳолда “Электрон ҳужжат айланиши” тизими ишлаб чиқилди. Ахборот тизимининг жорий этилиши ҳужжатлар билан ишлашнинг шаффофлиги, тезкорлиги, самарадорлиги ва ҳужжатлар ижроси устидан назоратни оширди, уларни йўқотиш хавфини олдини олиб, ҳужжатларни жўнатиш ва журналларда рўйхатдан ўтказиш каби қиммат ва кўп вақт талаб қилувчи жараёнларни бартараф этди.

Ўтган 5 йил давомида 22 млн. 283 мингта ҳужжат кирим қилиниб, бу билан 21 млрд. сўмдан ортиқ яъни 667 тонна офис қоғози иқтисод қилинди.

Қайд этиш жоизки, фаолиятга жорий этилган ахборот-коммуникация технологиялари нафақат прокуратура, балки бошқа ҳуқуқни муҳофаза қилувчи органлар фаолиятига ҳам ижобий таъсир қилди.

Биринчидан, 2019 йилгача жиноий-ҳуқуқий статистика тизими ва жиноятлар ҳисобини юритиш жараёнлари рақамлаштирилмаган эди.

Ўзбекистон Республикаси Президентининг 2018 йил 31 октябрдаги ПФ-5566-сонли Фармони ижроси доирасида “Электрон жиноий-ҳуқуқий статистика” ягона ахборот тизими ишлаб чиқилди ва ҳуқуқни муҳофаза қилувчи органлар фаолиятига жорий қилинди.

Иккинчидан, Ўзбекистон Республикаси Президентининг 13.12.2019 йилдаги ПҚ-4551-сонли Қарори ижроси доирасида 2020 йил 1 июлдан бошлаб процессуал мажбурлов чоралар электрон шаклда ҳисобга олиниши бошланди.

Учинчидан, 2021 йилгача жиноятга оид ариза, хабар ва бошқа маълумотларни электрон рўйхатга олиш ва уларни кўриб чиқиш

натижаларининг ҳисобини юритиш махсус рўйхатга олиш китобларида қайд қилиш билан кирим қилиниб келинган.

Ўзбекистон Республикаси Президентининг 10.08.2020 йилдаги ПФ-6041-сонли Фармонидан кейин эса 2021 йил 1 январдан бошлаб барча терговга қадар текширув материаллари ва уларнинг натижалари ҳақидаги маълумотлар рақамлаштирилиб, “E-material” ахборот тизими жорий этилди.

Тўртинчидан, 2022 йилгача ҳуқуқни муҳофаза қилувчи органлар ҳамда вазирлик ва идораларнинг ахборот тизимлари ўртасида интеграция бўлмаган. Шу боис, жиноятлар ҳақида хабарларни кўриб чиқиш ва жиноят ишларини юритишда суриштирув ва дастлабки тергов органлари томонидан зарур маълумотлар қоғоз шаклида олинар эди.

Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПҚ-105-сонли Қарори ижроси доирасида 2022 йил 1 августдан бошлаб суриштирув ва дастлабки тергов органлари учун жиноятни тезкор фош этиш учун муҳим бўлган маълумотларни ягона ахборот тизими орқали тезкор олиш имконияти яратилди.

Ушбу тизим орқали жиноятни тезкор ва тўлиқ фош этиш учун муҳим бўлган маълумотларни тезкор олиш мақсадида ўтган 2 йил давомида 1 млн.дан ортиқ сўров юборилди.

Бешинчидан, 2023 йилга қадар Бош прокуратура ва Олий суд ахборот тизимлари ўртасида ўзаро ҳужжат алмашинуви рақамлаштирилмаган.

Ўзбекистон Республикаси Президентининг 2023 йил 16 январдаги ПФ-12-сонли Фармони ижроси доирасида Бош прокуратура ва Олий суд ахборот тизимлари ўртасида ҳужжат алмашинуви йўлга қўйилди ҳамда “Судларда прокурор иштироки" ахборот тизими яратилди. Бу судларда жиноят ишлари, фуқаролик ишларини, маъмурий ҳуқуқбузарликлар тўғрисидаги ишларни ҳамда иқтисодий низоларни кўришда ҳужжатлар билан алмашинувига имконият берди.

Олтинчидан, Ўзбекистон Республикаси Президентининг 2023 йил 24 майдаги ПФ-77-сонли Фармони ижроси доирасида "Прокурор назорати" ахборот тизими ишга туширилди. Қонунчилик ижроси устидан прокурор назорати тадбирлари ҳамда уларнинг натижаси бўйича қўлланилган прокурор назорати ҳужжатларининг ҳисобини юритиш имконияти яратилди.

Прокуратура органлари фаолиятини рақамли трансформация қилиш бўйича амалдаги қонунчиликни такомиллаштириш бўйича таклиф ва тавсиялар:

Биринчи, прокуратура органлари фаолиятини рақамли трансформация қилишни изчил давом эттириш мақсадида бу борадаги Стратегияни қабул қилиш. Бош прокуратура томонидан Ўзбекистон Республикаси Президентининг "Рақамли прокуратура — 2030" стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида" ги Фармони лойиҳаси ҳам ишлаб чиқилди.

Иккинчи, прокуратура органлари фаолиятини рақамли трансформация қилишнинг яна бир мақсади – давлат органларида коррупция хатарларини камайтириш, коррупцияга оид қонун бузилишларининг олдини олишдир. Бироқ, вазирлик, идора, ҳокимликларда ахборот тизимлари ва ресурслари мавжуд бўлсада, улар ва прокуратура органлари билан электрон ҳамкорлик ҳанузгача тўлақонли йўлга қўйилмаган. Бунинг сабаблари бири – интеграция жараёнлари давлат органларидан меҳнат ресурслари, вақт ва маблағ сарфлашни талаб қилади.

Шунга кўра, интеграция қилиш жараёнларини жадаллаштириш ҳамда техник топшириқларда "рақамли назорат"ни таъминлаш бўйича алоҳида тартиб жорий қилиш назарда тутилган норматив-ҳуқуқий ҳужжатларни қабул қилиш ҳамда айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш таклиф этилади.

Учинчи, ҳуқуқни муҳофаза қилувчи органлар ўртасида электрон ҳужжатлар айланишини ягона ахборот тизимини яратиш.

Тўртинчи, ҳуқуқни муҳофаза қилувчи органлар билан биргаликда "Электрон жиноят иши" ахборот тизимлари комплексини ишлаб чиқиш.

Бешинчи, жиноятга оид ариза, хабар ва бошқа маълумотларни электрон рўйхатга олиш ва уларни кўриб чиқиш тартиби жиноят процессуал қонунчилигида ўз аксини топмаганлигидан келиб чиқиб, Ўзбекистон Республикасининг Жиноят-процессуал кодексига жиноятга оид ариза, хабар ва бошқа маълумотлар бўйича "электрон реестри" тушунчасини киритиш.

Олтинчи, жисмоний ва юридик шахсларнинг мурожаатларини электрон тарзда қабул қилиш ва кўриб чиқиш, мурожаатларни сунъий интеллект ёрдамида таҳлил қилиш, ҳуқуқни муҳофаза қилиш органлари ўртасида тақсимлаш ҳамда етказиб бериш

тартибини ўрнатиш бўйича норматив-ҳуқуқий ҳужжатларни қабул қилиш.

Ушбу мақола якунида таъкидлаш мумкинки, Ўзбекистон прокуратура органлари фаолиятини рақамли трансформация қилиш стратегик аҳамиятга эга жараён бўлиб, уларнинг шаффофлиги, самарадорлиги ва тезкорлигини ошириш учун зарур қадам ҳисобланади.

Ахборот-коммуникация технологияларини жорий этиш марказлашган маълумотларни қайта ишлаш маркази ва локал ҳамда корпоратив тармоқларни ривожлантириш каби сезиларли ўзгаришларга олиб келди. Шу билан бирга, турли ахборот тизимларини жорий қилиш асосий жараёнларни автоматлаштириш, ҳужжатларни бошқаришни яхшилаш ва фаолиятнинг шаффофлигини ошириш имконини берди.

Бу чора-тадбирлар ҳужжатларни бошқаришни яхшилашга, маъмурий вазифаларни бажаришга кетадиган вақтни қисқартиришга, қонун ижроси устидан назоратни мустаҳкамлашга, фуқаролар ва тадбиркорларнинг ҳуқуқларини ҳимоя қилишни кучайтиришга хизмат қилмоқда. Натижада, прокуратура органларига бўлган ишонч ошмоқда.

Бизнинг фикримизча, рақамли трансформацияни муваффақиятли давом эттириш учун норматив-ҳуқуқий базани такомиллаштириш ва бошқа давлат органларининг ахборот тизимлари билан интеграция қилиш ишларини давом эттириш зарур.

Шунингдек, фақат комплекс ва мувофиқлаштирилган ёндашув орқали рақамлаштириш жараёнидаги технологияларнинг тўлиқ салоҳиятини очиш мумкин. Шу муносабат билан, барча ҳуқуқни муҳофаза қилувчи органлар учун ягона ахборот тизимини яратиш муҳим вазифалардан бири бўлиб, бу тизим улар ўртасидаги ҳамкорликни яхшилашга, маълумот ва жараёнларни самарали бошқаришни таъминлашга имкон беради.

CYBERCRIME AND CYBER LAW

Naeem AllahRakha
Tashkent State University of Law
Chaudharynaeem133@gmail.com

Abstract: *This study examines the evolving landscape of cybercrime and cyber law in the global digital era. Against a background of rapidly advancing technology and increasing cyber threats, we aim to analyze the effectiveness of international cyber law frameworks in combating cybercrime. Using qualitative research methods, including doctrinal and document analysis of current regulations and official databases, we investigate the challenges and opportunities in cyber legislation across various jurisdictions. Our results reveal significant disparities in cyber law implementation and enforcement capabilities worldwide, with 80% of countries having some form of cybercrime legislation. Key findings include the emergence of specialized cyber courts, the integration of AI-specific provisions in recent legal amendments, and the crucial role of public-private partnerships in cybercrime prevention. We recommend establishing an international cybercrime tribunal, enhancing global legislative harmonization, and investing in capacity-building programs to address jurisdictional challenges and strengthen cross-border cooperation. This research contributes to the ongoing effort to create a more secure and resilient global digital environment through improved legal frameworks and international collaboration.*

Keywords*: Cybercrime, Cyber Law, International Cooperation, Digital Security, Legal Harmonization*

Introduction

The rapid advancement of digital technologies has led to an unprecedented interconnectedness in our global society. While this digital revolution has brought numerous benefits, it has also given rise to a new frontier of criminal activity: cybercrime. As our reliance on digital platforms for communication, commerce, and governance increases, so does the potential for malicious actors to exploit vulnerabilities in these systems. Cybercrime encompasses a wide range of illegal activities carried out through digital means, from financial fraud and identity theft to cyber espionage and attacks on critical infrastructure (Chen et al., 2023). The pervasive nature of these threats has necessitated the development of cyber laws and international cooperation to combat this growing menace.

Despite the increasing sophistication of cybersecurity measures, cybercrime continues to evolve at an alarming rate, outpacing legal and regulatory frameworks. The borderless nature of the internet poses significant challenges for law enforcement agencies, as traditional jurisdictional boundaries become blurred in cyberspace (Menon & Guan

Siew, 2012). Moreover, the technical complexity of cyber-attacks often makes it difficult to attribute crimes to specific perpetrators, complicating prosecution efforts. The lack of harmonized international legal standards and the varying levels of cybercrime legislation across countries create loopholes that cybercriminals can exploit. This global disparity in cyber laws and enforcement capabilities has resulted in safe havens for cybercriminals, hindering effective cross-border cooperation in combating these digital threats.

Recent research has shed light on various aspects of cybercrime and cyber law. The importance of international cooperation in combating cybercrime, emphasizing the need for harmonized legal frameworks across nations (Cerezo et al., 2007). Their study found that disparities in national cyber laws often impede effective cross-border investigations and prosecutions. The challenges of attributing cybercrimes to specific actors, revealing that the anonymity afforded by the internet and the use of sophisticated obfuscation techniques make it difficult for law enforcement to identify and prosecute cybercriminals (Isaac Abiodun et al., 2022). In a comprehensive analysis of global cybercrime legislation, discovered that while 80% of countries have some form of cybercrime laws, the scope and enforcement of these laws vary significantly, creating potential safe havens for cybercriminals (Mphatheni & Maluleke, 2022).

The role of artificial intelligence in both perpetrating and combating cybercrimes (Pasha et al., 2022). Their research indicated that AI-powered cyber-attacks are becoming increasingly sophisticated, necessitating equally advanced defensive measures and legal frameworks. Focusing on the economic impact of cybercrime, (Cremer et al., 2022) estimated that global losses due to cybercrime reached $6 trillion in 2022, highlighting the urgent need for more robust cyber law enforcement and international cooperation. The challenges of digital evidence collection and preservation in cybercrime cases, emphasizing the need for standardized procedures and international protocols to ensure the admissibility of evidence across jurisdictions (Azam et al., 2023).

The effectiveness of the Budapest Convention on Cybercrime, finding that while it has improved international cooperation, significant gaps remain in addressing emerging cyber threats and technologies (Etta et al., 2022). Examining the intersection of privacy rights and cybercrime investigations, (Granovetter, 1973) identified tensions between data protection laws and the need for cross-border information sharing in cybercrime cases. (Kacou et al., 2022) studied the impact of capacity-building programs in developing countries, revealing that such initiatives

significantly improve a nation's ability to combat cybercrime and implement effective cyber laws. And, (Tropina, 2015) investigated the role of public-private partnerships in cybercrime prevention, concluding that collaboration between government agencies and tech companies is crucial for developing comprehensive cybersecurity strategies and legal frameworks.

While existing research has made significant strides in understanding various aspects of cybercrime and cyber law, there remains a notable gap in comprehensively analyzing the interplay between technological advancements, legal frameworks, and international cooperation in combating cybercrime. Most studies focus on specific regions or particular types of cybercrimes, leaving a need for a holistic, global perspective that addresses the dynamic nature of cyber threats and the legal challenges they pose. Furthermore, there is limited research on the effectiveness of current international cyber law instruments in addressing emerging technologies such as artificial intelligence, blockchain, and the Internet of Things. This gap underscores the need for a multidisciplinary approach that combines legal, technical, and policy perspectives to develop more adaptive and resilient cyber law frameworks.

The primary objective of this research is to conduct a comprehensive analysis of the current state of global cyber laws and their effectiveness in combating cybercrime. This study aims to identify key challenges in the implementation and enforcement of cyber laws across different jurisdictions and evaluate the impact of international cooperation mechanisms. By examining case studies of successful cybercrime prosecutions and analyzing the factors that contribute to their success, this research seeks to propose a framework for harmonizing cyber laws and enhancing cross-border collaboration. Additionally, the study will explore the potential of emerging technologies in both perpetrating and combating cybercrimes, with the goal of recommending adaptations to legal frameworks to address these evolving threats.

How can international cyber law frameworks be enhanced to effectively address the evolving nature of cybercrime in a globalized digital landscape, considering technological advancements, jurisdictional challenges, and the need for cross-border cooperation?

This research holds significant importance for policymakers, law enforcement agencies, and cybersecurity professionals worldwide. By providing a comprehensive analysis of the current cyber law landscape and identifying key areas for improvement, this study will contribute to the development of more effective legal frameworks and international

cooperation mechanisms. The findings will help inform policy decisions and legislative efforts aimed at closing legal loopholes and harmonizing cyber laws across jurisdictions. Furthermore, the research will offer valuable insights into the integration of emerging technologies in both cybercrime prevention and law enforcement, potentially leading to more robust and adaptive cybersecurity strategies. Ultimately, this study aims to contribute to the global effort in creating a safer digital environment, reducing the economic and social impacts of cybercrime, and fostering trust in digital technologies and e-governance initiatives.

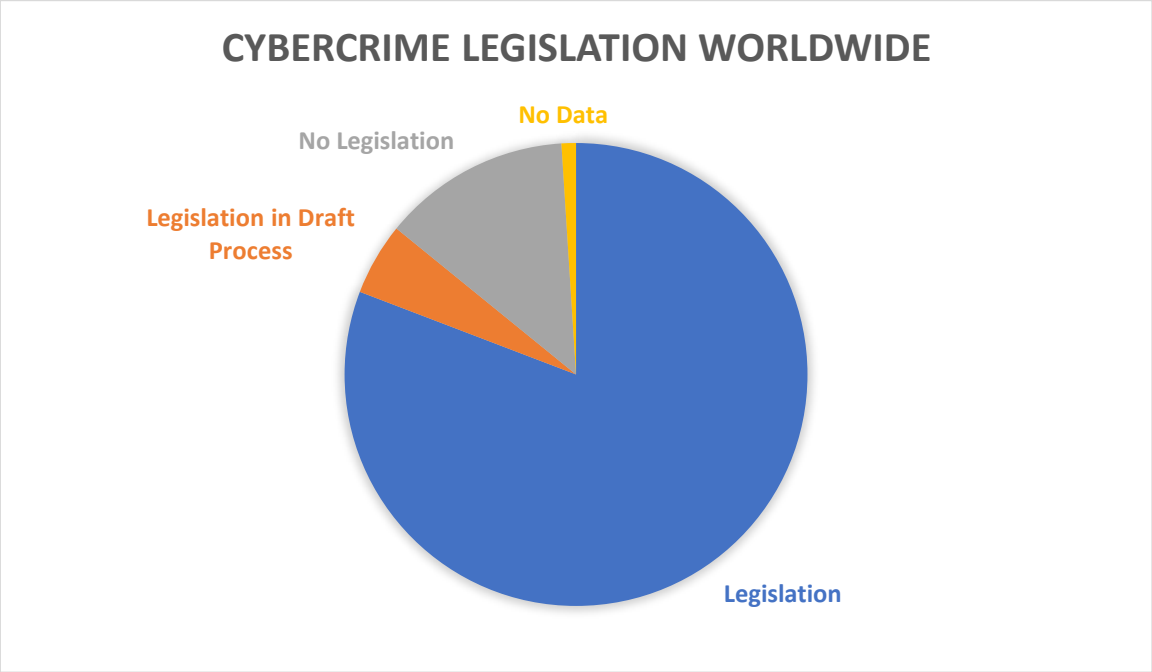
Methodology

This study employs a qualitative research design, utilizing doctrinal and document analysis approaches to examine the current landscape of cybercrime legislation and enforcement. The research population consists of existing cyber law regulations across various jurisdictions, with a focus on international agreements and national legislations enacted or updated since 2020. Sampling is purposive, selecting regulations and case studies that represent diverse geographical regions and legal systems. Data collection involves accessing official databases of legal documents, including but not limited to the United Nations Office on Drugs and Crime (UNODC) repository, the Council of Europe's treaty office, and national legislative databases. To ensure validity and reliability, the study relies on primary sources of law and official government publications, cross-referencing these with recent academic literature and reports from reputable international organizations.

The data analysis technique primarily involves content analysis of legal documents, identifying key themes, provisions, and enforcement mechanisms in cyber law regulations. This approach allows for a comprehensive comparison of different legal frameworks and their effectiveness in addressing cybercrime. Ethical considerations are addressed by utilizing publicly available data and ensuring proper citation of all sources. The study acknowledges limitations such as the potential for rapid changes in cyber law legislation that may occur during the research period and the challenges in accessing comprehensive data from all jurisdictions, particularly those with limited online resources. Additionally, the qualitative nature of the study means that findings may not be generalizable to all contexts. Despite these limitations, this methodology provides a robust framework for analyzing the current state of cyber law and identifying areas for potential improvement in the global fight against cybercrime.

Results

The analysis of global cyber law frameworks and their effectiveness in combating cybercrime revealed a complex landscape of legal challenges and international cooperation efforts. Our examination of cybercrime legislation across various jurisdictions, international agreements, and enforcement mechanisms provided insights into the current state of cyber law and its ability to address evolving digital threats. The results highlight significant disparities in legislative approaches, enforcement capabilities, and international cooperation, reflecting the diverse priorities and resources of different nations. This section presents key findings from our doctrinal and document analysis, offering a comprehensive overview of the global cyber law ecosystem and its impact on cybercrime prevention and prosecution.



Cybercrime Legislation Chart

Our research revealed that while 80% of countries have implemented some form of cybercrime legislation, the scope and effectiveness of these laws vary significantly. Advanced economies generally have more comprehensive cyber laws and better enforcement mechanisms compared to developing nations. However, even among developed countries, there are notable differences in approach, particularly in areas such as data privacy, encryption policies, and cross-border data sharing. We found that countries with more robust cyber laws and active participation in international cooperation efforts reported higher success rates in cybercrime investigations and prosecutions. Notably, nations that have ratified the Budapest Convention on

Cybercrime showed improved capabilities in addressing transnational cybercrimes through enhanced legal harmonization and mutual assistance protocols.

An intriguing discovery was the emergence of AI-specific provisions in recent cyber law amendments across several jurisdictions. These provisions aim to address the unique challenges posed by AI-driven cybercrimes, such as deep fakes and automated hacking attempts. Additionally, we observed a growing trend towards public-private partnerships in cybercrime prevention and investigation. Countries that fostered close collaboration between law enforcement agencies and tech companies demonstrated greater agility in responding to emerging cyber threats. Another interesting finding was the increasing role of cryptocurrency regulations in cybercrime legislation, with several countries implementing strict Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements for crypto exchanges to combat ransomware attacks and other crypto-facilitated cybercrimes (Darmawansyah et al., 2023).

Our analysis identified several key findings that shed light on the current state of global cyber law. First, there is a significant gap between the rapid evolution of cybercrime techniques and the often-slow process of legislative updates, creating vulnerabilities in legal frameworks. Second, jurisdictional challenges remain a major obstacle in prosecuting transnational cybercrimes, despite efforts to improve international cooperation. Third, countries with comprehensive data protection laws tend to have more effective cybercrime prevention measures, highlighting the interconnectedness of privacy and security in the digital realm. Fourth, the adoption of technologies like blockchain for digital evidence management is improving the integrity and admissibility of electronic evidence in court proceedings. Lastly, capacity-building initiatives in developing countries have shown positive results in enhancing cybercrime legislation and enforcement capabilities (Khan et al., 2022).

One unexpected finding was the emergence of "cyber courts" in several jurisdictions, specialized judicial bodies equipped to handle complex cybercrime cases. These courts have shown promising results in expediting cybercrime trials and improving conviction rates. Another surprising discovery was the increasing use of alternative dispute resolution mechanisms, such as online mediation platforms, for resolving certain types of cybercrimes, particularly in cases of online defamation and intellectual property infringement. We also found an unexpected trend of some countries incorporating "ethical hacking" provisions into their cyber laws, providing legal protections for security researchers who

discover and report vulnerabilities in good faith. This approach has led to improved cybersecurity in these jurisdictions by encouraging responsible disclosure of system weaknesses.

Our findings directly address the research question by illustrating how international cyber law frameworks can be enhanced to effectively combat evolving cybercrimes. The results suggest that a multi-faceted approach is necessary, combining legislative harmonization, technological innovation, and international cooperation. Successful strategies include: 1) Regular updates to cyber laws to address emerging technologies and threats; 2) Strengthening international cooperation mechanisms, particularly in evidence sharing and joint investigations; 3) Investing in capacity-building programs to reduce global disparities in cybercrime fighting capabilities; 4) Encouraging public-private partnerships to leverage industry expertise in law enforcement efforts; 5) Developing specialized cyber courts and training programs for judiciary members; and 6) Implementing comprehensive data protection regulations as a foundation for effective cybercrime prevention. These findings provide a roadmap for policymakers to enhance the resilience and effectiveness of global cyber law frameworks in the face of rapidly evolving digital threats.

Discussion

The results of our study reveal a complex and evolving landscape of cybercrime legislation and enforcement globally. The high percentage (80%) of countries with some form of cybercrime legislation indicates a growing recognition of the threat posed by digital crimes. However, the significant variations in the scope and effectiveness of these laws suggest that mere presence of legislation is insufficient. The emergence of specialized cyber courts and the incorporation of AI-specific provisions in recent legal amendments demonstrate an adaptive response to technological advancements. The positive correlation between robust cyber laws, active international cooperation, and successful cybercrime prosecutions underscores the importance of a comprehensive, globally coordinated approach. These findings collectively suggest that while progress has been made, there remains a critical need for further harmonization of legal frameworks and enhancement of cross-border cooperation mechanisms to effectively combat the borderless nature of cybercrime.

Our findings both corroborate and extend previous research in the field of cybercrime and cyber law. Consistent with (Cerezo et al., 2007),

we found that disparities in national cyber laws continue to impede effective cross-border investigations. However, our research goes further by identifying emerging trends such as the establishment of specialized cyber courts, which were not prominent in earlier studies. While (Mphatheni & Maluleke, 2022) highlighted the variability in cybercrime legislation across countries, our study provides updated statistics and a more nuanced understanding of the factors contributing to these differences. Our findings on the role of public-private partnerships in combating cybercrime align with and expand upon the work of (Cremer et al., 2022), offering new insights into the practical implementation and effectiveness of such collaborations. Additionally, our research provides fresh perspectives on the integration of AI and blockchain technologies in cyber law frameworks, areas that were not extensively covered in previous studies.

The findings of this study have several important theoretical implications for the field of cyber law and criminology. First, they challenge the traditional notion of territorial jurisdiction in law enforcement, suggesting a need for a more fluid, borderless conceptualization of legal frameworks in cyberspace. This aligns with and extends theories of transnational law and global governance. Second, the emergence of AI-specific provisions in cyber laws introduces new dimensions to theories of criminal liability and intent, particularly in cases where AI systems are involved in or used to commit cybercrimes. Third, our findings on the effectiveness of public-private partnerships in cybercrime prevention contribute to theories of collaborative governance and regulatory capitalism in the digital age. Lastly, the observed relationship between data protection laws and cybercrime prevention efficacy supports theories linking privacy rights to broader issues of digital security and resilience.

The practical implications of our research are far-reaching for policymakers, law enforcement agencies, and cybersecurity professionals. For policymakers, our findings highlight the urgent need for regular updates to cyber laws to keep pace with technological advancements and emerging threats. The success of specialized cyber courts suggests that investing in such institutions could significantly improve the efficiency of cybercrime prosecutions. Law enforcement agencies should prioritize international cooperation and capacity building, particularly in developing countries, to address the global nature of cybercrime effectively. The positive impact of public-private partnerships underscores the importance of fostering collaboration between government agencies and tech companies in cybercrime prevention and

investigation (Etta et al., 2022). For cybersecurity professionals, our findings emphasize the need for a multidisciplinary approach that combines technical expertise with an understanding of legal and regulatory frameworks to develop more effective cybersecurity strategies.

A key strength of this study lies in its comprehensive analysis of global cyber law frameworks, providing an up-to-date overview of the current legislative landscape. The inclusion of diverse jurisdictions and the examination of recent legal amendments offer a nuanced understanding of global trends in cybercrime legislation. Additionally, the study's focus on emerging technologies and their impact on cyber laws contributes valuable insights to the field (AllahRakha, 2024). However, the research also has limitations. The rapid pace of technological change and legislative updates means that some findings may become outdated quickly. The reliance on publicly available data might have resulted in the underrepresentation of countries with limited online resources or non-English language documents. Furthermore, the qualitative nature of the study, while providing rich insights, limits the generalizability of findings. Future research could benefit from a mixed-methods approach, incorporating quantitative analysis of cybercrime rates and conviction statistics to complement the qualitative findings.

Based on our findings, we propose several recommendations to enhance the effectiveness of global cyber law frameworks. First, we advocate for the establishment of an international cybercrime tribunal to address jurisdictional challenges in prosecuting transnational cybercrimes. Second, we recommend the development of a global cyber law harmonization initiative, similar to the Budapest Convention but with broader scope and participation. Third, countries should invest in continuous education and training programs for legal professionals, focusing on emerging technologies and their implications for cyber law. Fourth, we suggest the creation of a global cybercrime database to facilitate information sharing and trend analysis among law enforcement agencies worldwide. Fifth, governments should incentivize the adoption of privacy-enhancing technologies and security-by-design principles in software development to proactively reduce cybercrime vulnerabilities. Lastly, we recommend the establishment of international working groups to develop legal frameworks for emerging technologies like quantum computing and advanced AI systems, anticipating future challenges in the cybercrime landscape.

Conclusion

This study has examined the critical intersection of cybercrime and cyber law in our increasingly digital world. The importance of this topic cannot be overstated as cybercrime continues to evolve, threatening individuals, businesses, and nations alike. With the global cost of cybercrime reaching trillions of dollars annually and affecting millions of people, the need for effective legal frameworks to combat these digital threats is paramount. Our research has underscored the crucial role that well-crafted cyber laws and international cooperation play in safeguarding the digital landscape and ensuring the trust and security necessary for the continued growth of our global digital economy.

Our research affirms that while significant progress has been made in developing cyber laws globally, there remains a pressing need for greater harmonization and enhanced international cooperation to effectively combat cybercrime. We assert that the current patchwork of national legislation and varying levels of enforcement capabilities create vulnerabilities that cybercriminals exploit. Furthermore, we maintain that addressing these challenges requires a multifaceted approach that combines legislative updates, technological innovation, capacity building, and robust public-private partnerships. Only through such comprehensive efforts can we hope to create a resilient global framework capable of adapting to the rapidly evolving nature of cyber threats.

The core thesis of this study is that enhancing international cyber law frameworks is essential for effectively addressing the evolving nature of cybercrime in our globalized digital landscape. Our research has demonstrated that this enhancement must consider technological advancements, overcome jurisdictional challenges, and foster cross-border cooperation. We have shown that countries with more robust cyber laws and active participation in international cooperation efforts have greater success in combating cybercrime. This thesis underscores the need for a unified, adaptive approach to cyber legislation that can keep pace with technological innovations and provide a strong foundation for global cybersecurity efforts.

Our research has highlighted several key points supporting our thesis. First, the significant disparity in cyber law sophistication across nations creates exploitable weaknesses in the global cybersecurity landscape. Second, the emergence of AI-driven cybercrimes and the use of cryptocurrencies in illegal activities necessitate continual updates to legal frameworks. Third, specialized cyber courts and public-private partnerships have shown promise in improving cybercrime prosecution and prevention. Fourth, strong data protection laws correlate with more

effective cybercrime prevention measures. Lastly, capacity-building initiatives in developing countries have demonstrated positive outcomes in enhancing cybercrime legislation and enforcement capabilities.

In our introduction, we highlighted the pervasive nature of cybercrime and the challenges it poses to traditional legal frameworks. As we conclude, we reaffirm the critical importance of addressing these challenges through enhanced international cooperation and adaptive legal mechanisms. The journey from recognizing the threat of cybercrime to developing effective global counter-measures has been long and complex, but our research demonstrates that progress is being made. The evolving landscape of cyber threats that we initially described is being met with increasingly sophisticated legal and technological responses, as evidenced by our findings on specialized cyber courts and AI-specific legal provisions.

Our research offers valuable insights into the future of cyber law and cybercrime prevention. The trend towards specialized cyber courts and the integration of AI and blockchain technologies in legal frameworks suggest a future where the lines between technology and law become increasingly blurred. This convergence may lead to more agile and responsive legal systems capable of addressing cyber threats in real-time. Moreover, the growing emphasis on public-private partnerships indicates a shift towards a more collaborative approach to cybersecurity, where government regulations and private sector innovations work in tandem to create a more secure digital environment.

Some may argue that stringent cyber laws and increased international cooperation could infringe on individual privacy rights or hinder technological innovation. However, our research suggests that well-crafted cyber laws actually enhance privacy protections and create a more secure environment for innovation to flourish. We contend that the benefits of a harmonized global approach to cybercrime far outweigh the potential drawbacks. By aligning with our position, stakeholders can contribute to creating a safer digital world without sacrificing the values of privacy and innovation that are fundamental to our digital society.

We call upon policymakers, law enforcement agencies, and technology companies to intensify their collaborative efforts in developing and implementing harmonized cyber laws. Future research should focus on quantifying the impact of different cyber law approaches on cybercrime rates, exploring the ethical implications of AI in cyber law enforcement, and developing predictive models for emerging cyber threats. Additionally, we encourage studies on the long-term effects of specialized cyber courts and the potential for a global cybercrime tribunal.

By building on this research, we can work towards a future where our digital interactions are secured by a robust, adaptive, and globally coordinated legal framework.

ИЛМИЙ ФАОЛИЯТДА СУНЪИЙ ИНТЕЛЛЕКТДАН ФОЙДАЛАНИШНИНГ ДОЛЗАРБ МАСАЛАЛАРИ

Мамасиддиқов Музаффаржон Мусажонович,
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси бошлиғининг ўринбосари, ю.ф.д., проф.

Сунъий интеллект (СИ) тизими — бу инсон фикрлаш жараёнини компьютерда тақлид қиладиган дастурий тизимдир. Бундай тизимни яратиш учун нафақат ушбу жараён алгоритмини ўрганиш ва уни компьютерда қайта ишлашга мос дастурий воситаларни ишлаб чиқиш, балки инсон фикрлаш жараёнини ҳам ўрганиш зарур. Демак, СИ методлари қарор қабул қилиш тизимларини ишлаб чиқишга оддий тузилмавий ёндашувни таклиф этади ва инсон ақли талаб этиладиган вазифаларни бажара оладиган интеллектуал тизимларни яратишни кўзлайди.

“Сунъий интеллект” тушунчасини 1956 йилда биринчи бўлиб америкалик информатик **Жон Маккарти** таклиф қилган. Ушбу тушунча бундан олдин ишлатилган “машиналарни ўқитиш” тушунчасини алмаштирди. Сунъий интеллект атамаси компьютернинг катта ҳажмдаги маълумотларни қайта ишлаш ва маълум алгоритмлар асосида қарорлар таклиф қилиш қобилиятини англатади.

Тадқиқотларга кўра, 2024 йилга келиб, дунёдаги компанияларнинг ярмидан кўпи сунъий интеллектдан фойдаланмоқда. Беш миллиарддан ортиқ инсон турли даражада ушбу технологиялардан фойдаланади. Генератив сунъий интеллектнинг пайдо бўлиши инсоният ҳаётида электр энергияси, ядро технологиялари ва космосни ўзлаштириш билан тенг даражадаги прорыв бўлди.

Сўнгги 10 йил ичида СИ соҳасида улкан ривожланиш кузатилди, бу эса бир қатор омиллар билан боғлиқ. Биринчидан, кучли компьютерлар ва ҳисоблаш технологияларининг пайдо бўлиши ва ривожланиши катта ҳажмдаги маълумотларни қайта ишлаш ва мураккаб ҳисоб-китобларни реал вақтда бажариш имконини берди. Бу эса мураккаброқ алгоритмлар ва машинани ўргатиш моделларидан фойдаланиш имконини яратди, натижада СИ самарадорлиги сезиларли даражада яхшиланди. Иккинчидан,

маълумотлардан фойдаланиш имконияти ва уларнинг ҳажми сезиларли даражада ошди. Йирик компания ва ташкилотлар СИ ўқитиш учун ишлатилиши мумкин бўлган катта ҳажмдаги маълумотларни тўплайди ва сақлайди. Бу эса аниқроқ ва самаралироқ СИ моделларини яратишга имкон беради.

Сунъий интеллект (СИ) – бугунги кунда ўқув жараёнлари, ижодий ва илмий фаолиятда актив қўлланилаётган инновацион технологиялардан бири ҳисобланади. СИ орқали олимлар учун янги имкониятлар эшиги очилмоқда. Бироқ, бу жараёнда қандай афзалликлар ва камчиликлар мавжудлиги каби долзарб масалалар ҳозирги кунда кўпчилик илмий жамоатчиликни қизиқтириши табиий.

Машинани ўргатишнинг янги алгоритмларидан бири бўлмиш **(deep learning) чуқур ўрганиш** маълумотлар ичидаги қонуният-ларни мустақил ўрганиш ва топиш имконини берди, бу эса СИнинг юқори аниқлиги ва самарадорлигига ижобий таъсирини кўрсатди.

Инновацион технологиялар кундан-кунга шиддат билан ривожланиб бораётган ҳозирги даврда **илмий фаолиятда СИдан фойдаланиш масаласи** долзарб бўлиб қолмоқда. Ушбу жараёнларда сунъий интеллектдан фойдаланиш самаралими ёки йўқми, деган савол кўпчиликни ўйлантириб қўйди. Сўнгги йилларда СИдан фойдаланиш масаласига нисбатан қизиқиш ошиб, бу борада кўплаб баҳс-мунозаралар олиб борилмоқда. Айримлар бу технологияни қўллаб-қувватласа, бошқалар унга қарши чиқмоқда. Қуйида афзалликлар ва камчиликлар таҳлил қилинади.

Илмий жамоатчиликнинг илмий фаолиятда СИдан фойдаланиш юзасидан фикрлари нима учун турлича?

Шубҳасиз, СИ илмий тадқиқотларда янги имкониятлар ва истиқболларни яратади. У қуйидагиларда ёрдам беради:

- Илмий тадқиқотларнинг самарадорлигини ошириш;
- Ахборотга кириш имкониятларини кенгайтириш;
- Вақтни тежаш;
- Тадқиқот ишининг кучли ва заиф томонларини аниқлаш;
- Мутахассислардан фикр ва таклиф олиш имкониятини яратиш.

Бир гуруҳ олимлар СИнинг катта салоҳиятини таъкидлаб, унинг илмий тадқиқотлар ва ишлар ёзишда фойдали жиҳатларини кўрсатади. Шу билан бирга, бошқалар СИ қўлланилиши мумкин бўлган зарарли томонлар ҳақида огоҳлантирмоқда. Уларга кўра, СИ орқали тақдим этилган маълумотлар нотўғри ёки эскирган бўлиши

мумкинлиги, шунингдек, бу технология иш сифатига салбий таъсир кўрсатиши ҳам айтилади.

АФЗАЛЛИКЛАРИ:

1. Маълумотларни таҳлил қилиш

СИ катта ҳажмдаги маълумотларни таҳлил қилиш имкониятини беради. Бу жараён янги тенденциялар ва қонуниятларни аниқлашга ёрдам беради, бу ўз навбатида анъанавий усуллар орқали аниқланиши бир мунча мураккаб жараён ҳисобланади. Шунингдек, маълумотларни тезкор таҳлил қилиш жараёни вақтни тежашга ҳам имкон яратади.

2. Янги ғоялар яратиш

Одатда, илмий иш жараёнида янги ғоялар топишда қийинчиликка дуч келинади. СИ, шу жумладан ҳозирги кунда кўпчилик тадқиқотчилар томонидан фойдаланиб келинаётган ChatGPT (генератив олдиндан тайёрланган трансформатор) янги мавзулар ва тадқиқот йўналишларини таклиф этмоқда. Ундаги айрим таклифлар тадқиқотчилар учун йўналиш сифатида хизмат қилиши мумкин.

Ҳозирда **Робот олимлар** яратилаётганлиги ҳақида маълумотлар мавжуд. Робот олимлар сунъий интеллект (СИ) ва машина ўқитиш (МО) алгоритмлари ҳамда лаборатория роботларини бирлаштириб, асосий илмий тадқиқотларни мустақил равишда амалга оширадиган сунъий яратилган объектдир.

Сунъий интеллект илмфанга сезиларли таъсир кўрсатиши учун , у тажриба тадқиқотлари ҳақиқатан ҳам амалга ошириладиган ла бораторияларга кириши керак.

Илмфан фақат дунё ҳақида ўйлаш эмас, балки гипотезаларни т ажриба орқали синаб кўришдир.

Робот олим гипотеза ишлаб чиқади;
гипотезани синаб кўриш учун тажрибаларни ишлаб чиқади; лабора тория робототехникасидан фойдаланган ҳолда тажрибаларни баж аради; натижаларни таҳлил қилади ва турли гипотезалар эҳтимол ини ўзгартиради; сўнгра циклни такрорлайди. Шунингдек, робот оли м альтернатив гипотезалар ўртасида қарор қабул қилиш учун сама рали тажрибаларни (вақти ва пул жиҳатидан) танлашнинг автом атлаштирилган усулига эга.

Дастлабки робот олим Адам эди, бу илмий билимни мустақил р авишда кашф этган биринчи машина эди. У хамиртуруш метаболиз мида генлар ва ферментлар ўртасидаги муносабатни аниқлаш учун мўлжалланган эди. Адам фақат лаборатория сарф материалларин

и қўшиш ва чиқиндиларни олиб ташлаш учун вақти-вақти билан техник ходимларга муҳтож эди. Ҳар бир тажриба кўп кун давомида ва тинимсиз ишлади. Адам кунига 100 дан ортиқ янги тажрибани яратиб, 1000 дан ортиқ хамиртуруш штаммлари ва ўсиш шароитларидан танлов қилган.[1]

3. Тадқиқот жараёнини оптималлаштириш

ChatGPT илмий иш ёзиш жараёнини осонлаштириши мумкин. У манбалар таҳлилини амалга ошириб, тадқиқотчига долзарб маълумотларни тақдим этади.

4. Манбалар танлаш ва расмийлаштириш

ChatGPT ёрдамида тадқиқотчи ўз иши учун керакли манбаларни топиши ва уларни маълум бир услубда расмийлаштириши мумкин.

5. Тавсиялар тақдим этиш

ChatGPT тадқиқотчига янги гипотезалар, номаълум саволлар ва тадқиқот йўналишлари бўйича тавсиялар тақдим этиши мумкин.

6. График материаллар яратиш

ChatGPT диаграмма, тасвирлар ёки 3D моделлар яратишда ёрдам бера олади.

7. Таржима қилиш

ChatGPT 100 дан ортиқ тилда таржима қилиш имкониятига эга.

8. Матн сифатини яхшилаш

ChatGPT грамматик, орфографик ёки услубий хатоларни аниқлашда қўл келади.

КАМЧИЛИКЛАР

1. Махфийлик ва муаллифлик ҳуқуқлари

СИдан фойдаланишда махфийлик қоидаларига амал қилиш зарур. Ахборот хавфсизлиги таъминланмаса, бу муаллифлик ҳуқуқлари бузилишига олиб келиши мумкин.

2. Эскирган маълумотлар

ChatGPT кўпинча эски маълумотларни тақдим этади. Шунинг учун долзарб статистик маълумотларни унинг орқали эмас, балки ишончли манбалардан олиш тавсия этилади.

3. Илмий этика бузилиши

ChatGPT тадқиқотни тўлиқ бажаришига ишониб қолиш илмий этикага зиддир.

4. Маълумотлар таҳлилининг чуқур эмаслиги

ChatGPTнинг маълумотларни таҳлили чуқур эмас ва бу илмий ишлар учун етарли бўлмаслиги мумкин.

[1] R. King, Chalmers University, Sweden. O. Peter, Idorsia, Switzerland. P. Courtney, tec-connection, Germany. Robot scientists: From Adam to Eve to Genesis // ARTIFICIAL INTELLIGENCE IN SCIENCE © OECD 2023. P. 129-139.

5. Академик ҳалоллик билан боғли муаммолар

Сунъий интеллектнинг тез ривожланиши университетларда академик ҳалолликка таҳдид солмоқда. Чет эл олий таълим муассасалари хавотирда – ChatGPT каби технологияларнинг тараққиёти плагиатни аниқлашни қийинлаштириб, ўқув жараёнининг асосий мантиғини йўққа чиқармоқда.

Яқин-яқингача тадқиқотчи диссертация ишини кафедрага ёки илмий семинарга топширса, ушбу диссертацияни плагиатга текшириш учун махсус дастурлардан фойдаланиб, ундаги кўчирмакашлик ҳолатлари аниқланса, ишни қайта ёзилар, то ишнинг катта қисми **уникал (яъни ноёб, нодир, ягона)** бўлмагунича, тадқиқотчи диссертация устида иш олиб борар эди.

Бироқ, ChatGPT пайдо бўлиши билан иш айрим ўринларда тадқиқотчи томонидан мустақил равишда бажарилганини аниқлаш деярли имкониятсиз бўлиб қолди. Ушбу янги технология орқали яратилган матнлар осонгина плагиатга қарши дастурлардан ўтади. Шу муносабат билан чет эл университетлари биринчилардан бўлиб бу борада ўз хавотирларини билдирдилар.

"Агар бизнинг олдимиздаги ягона ҳужжат ёзма матн бўлса, уни машинанинг ёзганини исботлаш қийин. Чунки унинг тилга оид стандартлари аксарият ҳолларда юқори даражада, грамматикаси эса кўпинча тадқиқотчиникидан яхшироқ бўлади", – дейди Лондон Қироллик коллежининг компьютер илми мутахассиси ва плагиатга қарши эксперт **Томас Ланкастер**.

Шунингдек, бир неча хорижий университетлар сунъий интеллект ёрдамида ёзилган ишлар учун талабаларни ўқишдан чиқаришини маълум қилди. Бундан ташқари, университетлар энди талабалар билимларини баҳолашнинг анъанавий усулларини қайта кўриб чиқишга мажбур бўлмоқдалар.

Қўшни **Қозоғистон**да экспертлар (Сергей Пен) томонидан "бу воситанинг ўрнини аниқлаш ва қоидаларини ишлаб чиқиш зарурлиги, агар талабгор ChatGPTдан фойдаланган бўлса, худди манбаларга ҳавола бергани каби буни қайд этиш талабини жорий этиш кераклигини таклиф қилмоқдалар.

Мутахассислар (Сейфуллин номидаги ҚозАТУнинг факультет декани Ержар Ибишев) фикрига кўра, қозоғистонлик талабаларга ChatGPT ёрдамида диплом ёзиш учун ҳали камида беш йил кутишга тўғри келади. Чунки сунъий интеллект асосан **инглиз тилидаги маълумотларни яхши қабул қилади ва қайта ишлайди**".

ИЛМИЙ ЖАМОАТЧИЛИКНИНГ ҚАРАШЛАРИ:

Россия Федерацияси Ҳукумати қошидаги Қонунчилик ва қиёсий ҳуқуқшунослик институти директори, академик **Хабриева Талия Ярулловна**:

“Сунъий интеллект шиддат билан ривожланмоқда. Ҳуқуқий илм консерватив бўлишига қарамай, тезда СИ ни инкор қилишдан фрагментли ўзлаштиришга ва кейинчалик ҳуқуқ тизимида тўлиқ қўлланилишига ўтди.”

Шу ўринда академик сунъий интеллектни ҳуқуқий субъекти сифатида тан олиш масаласига тўхталиб, "Сунъий интеллектни ҳуқуқий субъект сифатида кўриш инқилобий таклифдир. Бир вақтлар инсон мол-мулк сифатида кўрилган бўлса, эндиликда мол-мулк инсонга айланишига гувоҳ бўлишимиз мумкин", – деб таъкидлайди.

"Сунъий интеллектни ҳуқуқий тартибга солиш воситаси сифатида кўриш мумкин. Белгородда **2021 йилда ўтказилган экспериментда суд буйруқларини сунъий интеллект ишлаб чиқди**", – дейди Талия Хабриева.

Ҳуқуқий тартибга солиш зарурияти

Cognitive Technologies асосчиси ва президенти Ольга Ускованинг фикрича, ҳозироқ СИ учун ҳуқуқий тартибга солишни жорий этиш зарур.

Григорий Ивлиевнинг фикрича, сунъий интеллект учун қонунчилик заруриятини аниқлаш давлатнинг вазифасидир. Бу юристлар учун эмас, давлат учун умумий вазифадир.

Сунъий интеллект тушунчасининг аниқ таърифи йўқ

“Юристлар сунъий интеллектни инсон ҳаётига интеграция қилиш учун инновацион ечимларни топа олмасалар, фантаст ёзувчиларнинг, масалан, Айзек Азимовнинг сценарийлари ҳаётимизда амалга ошиши мумкин. Ҳозирги кунда қонунчиликда сунъий интеллектнинг аниқ таърифи йўқ. Шунингдек, уни қўллаш, контентни верификация қилиш ва сунъий интеллект ёрдамида қабул қилинган қарорлар учун жавобгарлик бўйича тизимли ёндашув мавжуд эмас. Сунъий интеллект бугунги кунда инсон билан рақобатлашибгина қолмай, кўпинча уни енгмоқда", – дейди Просвещение” компаниялари гуруҳи бош директори Наталья Третьяк.

ХУЛОСА

СИ, шу жумладан ChatGPT илмий тадқиқотлар учун қулай восита бўлиб, вақтни тежашга ёрдам беради. Бироқ, ундан фойдаланишда муаллифлик ҳуқуқлари, илмий этика ва ахборотнинг

ишончлилигига алоҳида эътибор бериш керак. ChatGPT тадқиқотчига ёрдамчи восита бўлиши мумкин, аммо асосий иш инсон томонидан амалга оширилиши лозим.

“КИБЕРҲУҚУҚ СОҲАСИДА КАДРЛАР ТАЙЁРЛАШ: ИМКОНИЯТЛАР ВА ҲАМКОРЛИК ИСТИҚБОЛЛАРИ”

Назаров Фарходжон Абдувахобович
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси Тезкор-қидирув фаолияти ва киберҳуқуқ кафедраси бошлиғи

Аннотация: *Дунёда ахборот технологияларининг юқори суратда тараққий этиб бораётганлиги, интернетнинг глобаллашуви ва рақамли иқтисодиётнинг ўсиши бу соҳадаги ижтимоий муносабатларни ҳуқуқий тартибга солиш механизмларини мунтазам такомиллаштириб боришни тоқазо этмоқда. Бу жараёнда ҳуқуқий тизимнинг янги тармоғи киберҳуқуқ йўналишида профессионал кадрлар тайёрлаш муҳим аҳамиятга эга. Ушбу мақолада киберҳуқуқ соҳасида кадрлар тайёрлашнинг долзарб масалалари, бу борадаги имкониятлар ва ҳамкорлик истиқболлари ҳақида сўз юритилган ҳамда соҳани такомиллаштиришга қаратилган таклиф ва тавсиялар ишлаб чиқилган.*

Калит сўзлар: *кадр, интернет, рақамли, кибермакон, киберҳуқуқ, киберхавфсизлик, кибержиноят, мутахассис, прокурор, соҳа, муаммо, маблағ, ресурс.*

Аннотация: *Стремительное развитие информационных технологий в мире, глобализация Интернета и рост цифровой экономики требуют регулярного совершенствования механизмов правового регулирования общественных отношений в этой сфере. В этом процессе важна подготовка профессиональных кадров в области киберправа – новой отрасли правовой системы. В данной статье рассматриваются актуальные вопросы подготовки кадров в сфере киберправа, возможности и перспективы сотрудничества в этом направлении, а также разрабатываются предложения и рекомендации, направленные на совершенствование сферы.*

Ключевые слова: *персонал, интернет, цифра, киберпространство, киберправо, кибербезопасность, киберпреступность, специалист, прокурор, отрасль, проблема, финансирование, ресурс.*

Abstract. *The rapid development of information technology in the world, the globalization of the Internet and the growth of the digital economy require regular improvement of the mechanisms of legal regulation of public relations in this area. In this process, it is important to train professional personnel in the field of cyber law - a new branch of the legal system. This article examines current issues of training personnel in the field of cyber law, the possibilities and prospects for cooperation in this area, and also develops proposals and recommendations aimed at improving the field.*

Keywords: *personnel, Internet, digital, cyberspace, cyberlaw, cybersecurity, cybercrime, specialist, prosecutor, industry, problem, financing, resource.*

Инсоният тарихида XX аср – бу рақамли даврга дастлабки қадам сифатида қоладиган бўлди. Бугунги кунда ахборот-технологияларидан фойдаланиш кўлами ўтган даврларга нисбатан мисли кўрилмаган даражага чиқмоқда. Рақамлаштириш ижтимоий ҳаётнинг барча соҳаларини тез суратларда қамраб олмоқда.

Дунёда рақамли борлиқнинг шиддат билан кенгайиб бораётганлиги ўз навбатида кибермакондаги ижтимоий муносабатларни ҳуқуқий тартибга солиш механизмларини ҳам ривожлантириб боришни тақозо қилмоқда.

Маълумки, кибермакон - бу дунё бўйлаб одамлар ўзаро таъсирлашиши ва ғоялар ва ресурсларни бўлишиши мумкин бўлган онлайн муҳит бўлиб, у интернет орқали содир бўладиган барча рақамли алмашувларни, шу жумладан, веб-сайтлар, ижтимоий тармоқлар ва онлайн бозорларни ўз ичига олади. Кибермакон бошқа ижтимоий маконлардан фарқли ўлароқ, жисмоний ҳудудий жиҳатдан чегараланмаган ва бутун дунё бўйлаб фойдаланувчилар учун мавжуд ҳисобланади.

Кибермаконда компьютерлар ва тармоқлар орқали яратилган рақамли муҳитдаги ижтимоий муносабатларни тартибга солувчи ҳуқуқий соҳа –киберҳуқуқ ҳуқуқий тизимнинг янги ривожланиб бораётган тармоғи ҳисобланади.

Хорижий адабиётларда “киберуқуқ” атамаси билан биргаликда “интернет ҳуқуқи” (Internet Law), “кибермакон ҳуқуқи” (Cyberspace Law)[2], “веб-ҳуқуқ” (Web Law), “компьютер ҳуқуқи” (Computer Law)[3], “электрон тижорат ҳуқуқи” (Electronic Commerse Law) [4], “электрон савдо ҳуқуқи” (E-merchant Law)[5], “ахборот технологиялари ҳуқуқи” (Information Technology Law (IT Law))[6], “ахборот ҳуқуқи”

[2] Bird R. and Others. Cyber Law: Text and Cases. Cengage, 2011 ; Rosenoer J. Cyber Law: The Law of the Internet. Springer, 1997 ; Ku R. S. R., Lipton J. (eds). Cyberspace Law: Cases and Materials. 3rd edn. Aspen Publisher, 2010 ; Travis H. (ed). Cyberspace Law: Censorship and Regulation of the Internet. Routledge, 2013.

[3] Reed C., Angel J. (eds). Computer Law: The Law and Regulation of Information Technology. Oxford University Press, 2011 ; Bainbridge D. Introduction to Computer Law. 5th edn. Pearson Education Limited, 2004 ; Raysman R. Computer Law: Drafting and Negotiating Forms and Agreements // Law Journal Press. 1984.

[4] Wild Ch., Weinstein S., MacEwan N., Geach N. Op. cit.

[5] Trakman L. E. From the Medieval Law Merchant to E-Merchant Law // The University of Toronto Law Journal. 2003. Vol. 53. No. 3. Pp. 265—304.

[6] Murray A. Information Technology Law: The Lawand Society.Oxford University Press, 2010 ; Lloyd I. Information Technology Law. 6th edn. Oxford University Press, 2011 ; Rowland D., Kohl U., Charlesworth A. Information Technology Law. 4th edn. Routledge, 2012 ; Mooney Cotter A.-M., Babe C. (eds). Information Technology Law. Cavendish, 2004

(Информационное право)[7], “тармоқ ҳуқуқи” (Сетовая право) [8], “рақамли ҳуқуқ” (Цифровое право)[9] атамалари ҳам қўлланиб келинмоқда.

Таъкидлаш лозимки, киберҳуқуқнинг предмети, ўзига хос жиҳатлари ва мустақиллиги бўйича тадқиқотчилар турли ёндашувларни илгари суришади.

Юридик фаннинг айрим олимлари, жумладан, росссиялик олимлар М.В.Мажорина[10], М.А.Рожкова[11], америкалик юрист Ж.Амброги[12] ва бошқалар киберҳуқуқни ҳали алоҳида мустақил тармоқ сифатида эътироф этишмайди.

И.М.Рассолов эса, киберҳуқуқ таърифида “халқаро хусусий ҳуқуқ, ахборот ҳуқуқи ва бошқа ҳуқуқ соҳалари нормаларини ўзида бирлаштирган соҳалараро комплекс ҳуқуқий институт” сифатида қайд этган[13].

Таъкидлаш лозимки, аксарият россиялик олимлар киберҳуқуқни “рақамли ҳуқуқ” (Цифровое право) сифатида таърифлашиб, улардан бири, “Рақамли ҳуқуқ. Умумий қисм" (2022) дарслиги муаллифи В.Е.Волков, рақамли ҳуқуққа рақамли жамият тараққиётини таъминловчи, ҳуқуқий тартибга солишнинг янги йўналиши сифатида кенг маънода таъриф беради. Тор маънода эса, В.Е.Волковнинг фикрича, рақамли ҳуқуқ – рақамли маълумотларни қидириш, олиш, етказиш, ишлаб чиқариш ва тарқатиш, шунингдек, рақамли ахборот технологияларини қўллаш билан боғлиқ муносабатларни тартибга солувчи ҳуқуқнинг асосий тармоқлари

---

[7] Рассолов И. М. Информационное право : учебник для магистров. 2-е изд., испр. и доп. М. : Юрайт, 2013 ; Бачило И. Л. Актуальные проблемы информационного права // НТИ (теоретические проблемы информационного права). 2001. № 9; Бачило И. Л. Информационное право. М., 2001 ; Тедеев А. А. Информационное право (право Интернета). М., 2005 ; Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : дис. канд. юрид. наук. Екатеринбург, 2003.

[8] Голоскоков Л. В. Теория сетевого права / под ред. А. В. Малько. СПб., 2006. С. 32.

[9] Радченко М. Ю., Горбунов В.П. Цифровое право будущего // Третья Всероссийская конференция «Право и Интернет: теория и практика», 28—29 ноября 2000. С. 47—53. URL: http://www.hostcentre.ru/hosting/ files/5_2/pr_int.pdf.

[10] Мажорина М.В. “Цифровые платформы и международное частное право, или Есть ли будущее у киберправа”. https://cyberleninka.ru/article/n/tsifrovye-platformy-i-mezhdunarodnoe-chastnoe-pravo-ili-est-li-buduschee-u-kiberprava/viewer

[11] Рожкова М.А. “Цифровая право (Digital law) - что это такое и чем она отличается от киберправо / интернет право / компьютерного право?” “Является ли цифровое право отраслью права и ожидать ли появления цифрового кодекса?)”.

[12] Ambrogi, Robert J.Chapter 12: Net Law: The Internet's Rules of the Road //The essential guide to the best (and worst) legal sites on the Web. -2nd edition. -N.Y.: ALM Publishing, 2004. - P 139. -417 p.

[13] Рассолов И.М. Право и интернет: Теоретические проблемы // Центр социальных научно информационных исследований Социальные и гуманитарные науки: Реферативный журнал. -М.: ИНИОН РАН, 2004. -№ 3. -С. 48.

нормаларини бирлаштирувчи, тармоқлараро тўлақонли ҳуқуқий институтдир[14].

Ёки, В.С.Белых ва М.А.Егороваларга кўра, рақамли ҳуқуқ (цифровое право) рақамли технологияларни қўллаш ёки рақамли маълумотлардан фойдаланишдан келиб чиқадиган муносабатларни тартибга солувчи комплекс ҳуқуқ институти сифатида намоён бўлади[15]. Худди шундай, А.А.Карцхия рақамли ҳуқуқни мустақил тармоқ сифатида белгилайди[16]. Шу каби, В.С.Белых, М.О.Болобоновалар ҳам рақамли ҳуқуқни мустақиллик, автономлик билан тавсифланишини қайд этишади[17].

Бундан ташқари, “Рақамли ҳуқуқ” дарслиги муаллифлари В.В.Блажеева ва М.А.Егороваларга кўра, рақамли ҳуқуқ – бу рақамли технологияларни қўллаш ёки уларни қўллаш ёрдамида шаклланадиган соҳада давлат томонидан кафолатланган умумий мажбурий, расмий белгиланган хатти-ҳаракатлар қоидалари тизими бўлиб, рақамли маълумотлар, технологиялар ёки ахборот технологияларидан фойдаланиш билан боғлиқ муносабатларни тартибга солади[18].

С.Гулямов И.Рустамбеков фикрича, “ҳуқуқнинг янги комплекс соҳаси – “Кибер-ҳуқуқ” вужудга келганини ишонч билан қайд этиш мумкин. Кибер-ҳуқуқнинг ҳуқуқий тартибга солиш предметига кибермаконда юзага келадиган ва турли ҳуқуқ соҳаларининг нормалари билан тартибга солинадиган ижтимоий муносабатлар мажмуи ёки йиғиндиси киради.” [19]

Умумий тарзда қайд этишимиз мумкинки, киберҳуқуқ – бу кибермакондаги ижтимоий-ҳуқуқий муносабатларни тартибга солувчи алоҳида ҳуқуқ тармоғи сифатида шаклланиб улгурди ва ривожланиб бормоқда. Ушбу соҳадаги ҳуқуқнинг аҳамияти шундаки, у технологиялардан кенг фойдаланиш натижасида келиб чиқадиган мураккаб муаммоларни бошқариш ва тартибга солиш имкониятига эга ҳамда жамиятдаги ахборот хавфсизлиги, шахсий маълумотларни ҳимоя қилиш, кибержиноятларга қарши курашиш

---

[14] Волков В.Э. Цифровое право. Общая часть: учебное пособие / В. Э. Волков. – Самара: Издательство Самарского университета, 2022. – С. 24.

[15] Цифровое право: учебник / под общ. ред. В.В.Блажеева, М.А.Егоровой. М.: Проспект, 2020. С. 640.

[16] Карцхия А.А. Цифровые права и правоприменение // Мониторинг правоприменения. 2019. № 2(31). С. 45.

[17] Белых В. С., Болобонова М. О. Понятие, значение и тенденции развития цифрового права // Юрист. 2020. №1. С. 10–11.

[18] Цифровое право. Учебник / Под ред. В.В. Блажеева, М.А. Егоровой. – М.: Проспект, 2023.

[19] С.Гулямов, И.Рустамбеков “Кибер-ҳуқуқ” - янги комплекс ҳуқуқ соҳаси сифатида”. “Ўзбекистон қонунчилиги таҳлили” журнали. 2020 №4.

ва интернетдаги фаолиятнинг қонунийлигини таъминлаш вазифаларини бажаради.

Киберҳуқуқ шахслар ва ташкилотларни кибер таҳдидлардан ҳимоя қилиш, рақамли операцияларнинг махфийлиги ва хавфсизлигини таъминлаш ҳамда кибер маконда этика ва ҳуқуқий фаолиятга йўл-йўриқлар кўрсатиш учун асос яратади.

Рақамли дунё ривожланиб боргани сари, киберҳуқуқнинг аҳамияти ортиб бормоқда ва у рақамли ресурслардан масъулиятли ва қонунчиликка мувофиқ фойдаланиш учун пойдевор сифатида хизмат қилади.

Маълумки, киберҳуқуқ киберхавфсизлик, интеллектуал мулк, махфийлик, маълумотларни ҳимоя қилиш, электрон ҳукумат, электрон тижорат, электрон контрактлар, блокчейн ва сунъий интелект, солиқлар ва реклама, кибержиноятчилик, рақамли криминалистика ва бошқа кўплаб ҳуқуқнинг турли соҳаларини ўз ичига олади.

Мамлакатимизда киберҳуқуқ дунёдаги трансформацияларга узвий равишда ривожланиб бормоқда. Биргина, қонунчилик мисолида кўрадиган бўлсак, рақамли технологияларни тартибга солувчи 16 та қонун, ушбу соҳага дахлдор Ўзбекистон Республикаси Президенти, Вазирлар Маҳкамасининг 100 дан ортиқ қарорлари амал қилмоқда.

Киберҳуқуқ соҳасида профессионал кадрларни тайёрлаш бугунги кунда айни долзарб масала ҳисобланади. Бу соҳада етук мутахассисларнинг етишмаслиги киберҳуқуқий муносабатларда мураккабликларнинг келиб чиқишига олиб келиши мумкин. Профессионал кадрларнинг тайёрланганлиги эса жамиятда киберхавфсизликни таъминлаш, кибержиноятларни камайтириш ва қонунчиликни ривожлантиришга ёрдам беради.

Таъкидлаш лозимки, дунёда кибержиноятлар, кибертерроризм ва кибертаҳдидлар тобора ортиб бормоқда.

Экспертларнинг хулосасига кўра, кибержиноятлардан кўрилган зарар дунё бўйича 2022 йилда 8 триллион АҚШ долларини ташкил этган бўлса, йўқотишлар миқдори 2025 йилда 10,5 триллион долларга етиши прогноз қилинган.

Биргина, 2017 йилда WannaCry номли киберҳужум бутун дунё бўйлаб 150 дан ортиқ давлатдаги компьютер тизимларини зарарлантирган. Ушбу ҳужумнинг оқибатида катта иқтисодий зарар келтирилган. Кибертерроризм эса давлатларнинг ахборот тизимларига ҳужум қилиш ва уларни издан чиқариш орқали катта

таҳдид солмоқда. Кибертаҳдидлар эса ҳар куни янгича кўринишда намоён бўлиб, жамиятнинг барча соҳаларига салбий таъсир кўрсатмоқда.

Мамлакатимизда бу турдаги жиноятлар сўнгги уч йилда қарийб 25 баробарга ошган. Биргина, 2022 йилда АКТдан фойдаланган ҳолда 4 080 та жиноят содир этилган.

Ушбу маълумотлар таҳлили соҳадаги ижтимоий эҳтиёж ва заруратнинг кўламини кўрсатадиган омиллардан бири ҳисобланади.

Маълумки, соҳада кадрларни тайёрлаш деганда учта йўналиш назарда тутилади. Жумладан:

Биринчи йўналиш – амалиёт кадрларни тайёрлаш.

Иккинчи йўналиш – педагог ходимларни тайёрлаш, қайта тайёрлаш.

Учинчи йўналиш – илмий салоҳиятли кадрларни етиштириш.

Тадқиқотлар натижаларига кўра, киберҳуқуқ соҳасида кадрлар тайёрлаш жараёни ўзига хос хусусиятларга эгалиги кўринади.

Киберҳуқуқ соҳасида кадрлар тайёрлаш жараёни ҳам ўзига хос хусусиятларига эга:

киберҳуқуқ соҳасида кадрлар тайёрлашда ихтисосликка эътибор қаратиш жуда муҳим. Мутахассислар киберҳуқуқнинг турли йўналишларида билим ва кўникмаларга эга бўлишлари лозим;

киберҳуқуқ соҳасидаги мутахассислар нафақат ҳуқуқий билимларга, балки техник билимларга ҳам эга бўлишлари керак. Бу уларга кибержиноятларни таҳлил қилиш, киберхавфсизлик чораларини кўриш ва соҳага оид бошқа жараёнларни амалга оширишда ёрдам беради;

киберҳуқуқ соҳасида мутахассисларни тайёрлаш жараёнида таҳлил ва тадқиқот фаолиятига алоҳида эътибор қаратиш зарур. Бу уларнинг соҳадаги янгиликлар ва трендларни кузатиб боришлари ва таҳлил қилишлари учун муҳимдир.

Киберҳуқуқ соҳаси ривожланиб бориш билан биргаликда, бу йўналишда фаолият юритувчи кадрлар билан боғлиқ қатор муаммолар ҳам сақланиб қолмоқда.

Бугунги кунда киберҳуқуқ соҳасида профессионал кадрларнинг етишмаслиги долзарб муаммо ҳисобланади.

Ҳар соҳада бўлганидек, киберҳуқуқ соҳасида кадрлар тайёрлаш масаласига комплекс ёндашув зарур ва соҳа ривожи учун аниқ

вазифа ва механизмларни назарда тутувчи яхлит концепция ишлаб чиқилиши керак.

Бу соҳадаги кадрларни тайёрлаш учун етарли даражада маблағ ва ресурсларни ажратиш керак.

Шунингдек, кадрлар тайёрлашда таълим сифатига эътибор қаратиш муҳим. Бунинг учун замонавий ўқув дастурлари, малакали ўқитувчилар ва илғор технологиялардан фойдаланиш лозим.

Айниқса, соҳасида кадрлар тайёрлашда амалий машғулотлар ва тажриба алмашиш жараёнларига кўпроқ эътибор қаратиш зарур. Бу уларнинг назарий билимларини амалда қўллаш кўникмаларини оширишга ёрдам беради.

Ваҳоланки, киберҳуқуқ соҳасида кадрлар тайёрлаш масаласи дунё бўйлаб кўплаб давлатларда юқори даражада аҳамият касб этмоқда. Хусусан, АҚШ, Европа Иттифоқи мамлакатлари, Япония ва Жанубий Корея каби ривожланган давлатларда киберҳуқуқ соҳасида кадрлар тайёрлашга катта эътибор қаратилмоқда. Бу давлатларда киберҳуқуқ бўйича махсус ўқув дастурлари, таълим муассасалари ва тадқиқот марказлари ташкил этилган.

Маълумки, киберҳуқуқни ривожлантириш, кибержиноятларни тергов қилиш илмий методлар орқали махсус билимлардан фойдаланиш асосида амалга оширилади.

Шу боис, хорижий давлатларда бу борадаги илмий-амалий тадқиқотларга, кадрларларни тайёрлашга жиддий эътибор қаратилган.

Тергов амалиётини илмий жиҳатдан таъминлаш учун алоҳида илмий марказ ва тадқиқот институтлари ташкил этилиб, юриспруденция ва замонавий ахборот технологиялари соҳасида малакали мутахассислар тайёрлаш тизими шакллантирилган.

Масалан, Италияда Европа рақамли тадқиқот институти (European Institute for Digital Investigation, EIDI) рақамли криминалистика, киберхавфсизлик ва рақамли тергов соҳасида қўшма тадқиқотлар олиб бориш учун Европанинг турли давлатларидан мутахассисларни бирлаштирган, худди шундай вазифадаги халқаро нотижорат ташкилот – Рақамли криминалистика институти (Digital Forensics Institute, DFI) ҳам ҳуқуқни муҳофаза қилиш органлари ва хусусий компаниялар учун рақамли криминалистика соҳасида мутахассислар тайёрлаш билан шуғулланади.

Шу каби, Европа кибержиноятчиликка қарши ўқитиш ва таълим гуруҳи (ECTEG – European Cybercrime Training and Education

Group) Европа Иттифоқига аъзо давлатларнинг ҳуқуқни муҳофаза қилиш идоралари, Европа иқтисодий зонаси, халқаро ташкилотлар, илмий доиралар, хусусий бизнес ва экспертлардан иборат.

Ўзбекистонда ҳам киберҳуқуқ соҳасида кадрлар тайёрлаш масаласига алоҳида эътибор қаратилмоқда. Бу соҳада кадрлар тайёрлаш учун махсус ўқув дастурлари ишлаб чиқилмоқда ва улар амалга оширилмоқда.

2023 йилда Ўзбекистондаги нуфузли олий таълим муассасаларидан Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси, Тошкент давлат юридик университетида киберҳуқуқ бўйича махсус кафедралар ташкил қилиниб, бу соҳада мутахассислар тайёрланишни бошлаган. Бу қадам Ўзбекистоннинг киберҳуқуқ соҳасидаги салоҳиятини оширишга ёрдам бермоқда.

Ўзбекистон Республикаси Президентининг 2024 йил 21 июндаги “Рақамли криминалистика соҳасида илмий-тадқиқот фаолиятини ташкил этиш чора-тадбирлари тўғрисида”ги ПҚ-229-сонли Қарорига асосан Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академиясига рақамли криминалистика соҳасида инновацион тадқиқотлар олиб бориш, катта ҳажмдаги маълумотлар (“Big Data”), сунъий интеллект ва бошқа илғор технологияларни таҳлил қилиб, амалиётга жорий этиш вазифаси юклатилди[20].

Ҳозирда, Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академиясида талабалар ва тингловчиларга киберҳуқуқ, киберхавфсизлик ва рақамли криминалистика йўналишларида таълим берилмоқда.

Таъкидлаш лозимки, бакалавр йўналишида киберҳуқуқ модулини муваффақиятли тамомлаган талабалар киберҳуқуқ соҳасидаги асосий қонунчиликни тушуниш ва уни амалий ҳаётда қўллаш, кибер жиноятлар ва уларга қарши кураш усулларини билиш, интернетда шахсий маълумотларни муҳофаза қилиш бўйича билимларга эга бўлиш, халқаро киберҳуқуқий меъёрларни ва уларнинг миллий қонунчиликка таъсирини тушуниш, электрон тижорат ва онлайн хизматлар учун ҳуқуқий асосларни тушуниш ва уларни қўллаш назарий ва амалий компетенцияларга эга бўлишлари зарур.

Бу йўналишда ўқув дастурларини такомиллаштириш зарурати вужудга келган. Киберҳуқуқ соҳасида кадрлар тайёрлаш учун ўқув дастурларини замонавий талабларга, жаҳон стандартларига мос

[20] (Қонунчилик маълумотлари миллий базаси, 22.06.2024 й., 07/24/229/0438-сон)

равишда такомиллаштириш лозим. Бунинг учун илғор хорижий тажрибаларни ўрганиш ва амалиётга жорий этиш муҳим.

Малакали ўқитувчилар тайёрлаш ҳам бу йўналишдаги долзарб масалалардан биридир. Киберҳуқуқ соҳасида кадрлар тайёрлашда малакали ўқитувчиларни тайёрлаш ва уларнинг билимларини доимий равишда ошириб бориш керак. Бу уларнинг талабаларга сифатли таҳсил беришини таъминлайди.

Мамлакатимиздаги киберҳуқуқ йўналишида ўқув-таълимни амалга ошираётган тармоқлар фаолиятини такомиллаштириш, уларнинг штат бирликларини кенгайтириш, амалдаги ходимларнинг малакасини ошириш тизимини йўлга қўйиш, ушбу тармоқлар ишига юқори малакали хорижий эксперт ва мутахассисларни жалб қилиш кечиктириб бўлмас энг долзарб вазифалардан бири ҳисобланади.

Шу ўринда, Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академиясида киберҳуқуқ йўналишида бакалавриат ва магистратура факультетлари фаолиятини йўлга қўйиш соҳада кадрлар тайёрлашдаги навбатдаги илдам қадам бўлади.

Бундан ташқари, соҳавий тармоқларнинг моддий-техника базасини тубдан яхшилаш, профессор-ўқитувчиларни замонавий ўқув, илмий ресурслар ва техник воситалар билан таъминлаш муҳим мақсаддир.

Киберҳуқуқ соҳасида кадрлар тайёрлашда халқаро ҳамкорликка алоҳида эътибор қаратиш зарур. Хорижий университетлар ва тадқиқот марказлари билан ҳамкорлик қилиш, тажриба алмашиш жараёнларини кучайтириш лозим.

Ушбу соҳадаги илғор илмий мактаблар билан мулоқотни йўлга қўйиш, соҳада фаолият олиб бораётган профессор-ўқитувчиларни бу йўналишда илғор тажрибага эга бўлган хорижий таълим муассасаларида малакасини оширишга юбориш мақсадга мувофиқдир. Киберҳуқуқ соҳасида кадрлар тайёрлашда амалий машғулотлар ва стажировкаларни ташкил қилиш жуда муҳим. Бу талабаларнинг амалиётдаги кўникмаларини оширишга ёрдам беради.

Таъкидлаш лозимки, Ҳуқуқни муҳофаза қилиш академиясида ўтказилаётган халқаро конференция киберҳуқуқни ривожлантириш учун қулай платформа вазифасини ўтайди.

Хулоса ўрнида шуни айтишимиз мумкинки, киберҳуқуқ соҳасида кадрлар тайёрлаш бугунги кунда жамиятнинг долзарб масалаларидан бири ҳисобланади. Бу соҳада етук мутахассисларни

тайёрлаш учун ўқув дастурларини такомиллаштириш, малакали ўқитувчиларни тайёрлаш, халқаро ҳамкорликни кучайтириш ва амалий машғулотларга алоҳида эътибор қаратиш зарур.

Бу орқали киберҳуқуқ соҳасида профессионал кадрларни тайёрлашни самарали амалга оширишни таъминлаш ва соҳада ҳуқуқий тартиботни мустаҳкамлаш мумкин.

ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМУ ЭЛЕКТРОННОГО УГОЛОВНОГО ДЕЛА В УЗБЕКИСТАНЕ

Тургунов Асроржон Анварович
Старший преподаватель кафедры
Оперативно-розыскной деятельности и киберправа
Правоохранительной академии Республики Узбекистан.
E-mail: turgunov.a.a@proacademy.uz

Аннотация: *В статье рассматриваются актуальные вопрос внедрение искусственного интеллекта в систему электронного уголовного дела в Узбекистане, Освещаются основные ключевые аспекты, такие как правовые, технические и организационные барьеры, с которыми сталкивается система, а также перспективы ее развития.*

Ключевые слова: *Электронное уголовное дело, информационные технологии, искусственный интеллект, законодательство, безопасность данных, перспективы.*

Аннотация: *Мақолада Ўзбекистонда сунъий интеллект технологияларидан фойдаланишга эътибор қаратиилган ҳолда жиноят ишларининг электрон тизимини жорий этишнинг долзарб масалалари кўриб чиқилган. Тизимда дуч келадиган ҳуқуқий, техник ва ташкилий тўсиқлар, шунингдек унинг ривожланиш истиқболлари каби асосий асосий жиҳатлар таъкидланган.*

Таянч сўзлар: *Электрон жиноят иши, ахборот технологиялари, сунъий интеллект, қонунчилик, маълумотлар хавфсизлиги, истиқболлар*

Annotation: *The article examines the current issues of implementing artificial intelligence in the electronic criminal case system in Uzbekistan. It highlights the main key aspects, such as legal, technical, and organizational barriers faced by the system, as well as its development prospects*

Keywords: *Electronic criminal case, information technology, artificial intelligence, legislation, data security.*

В нашей стране реализуются комплексные меры по широкому внедрению современных информационно-коммуникационных технологий во все сферы жизни, созданию дополнительных удобств для граждан, обеспечению оперативности и прозрачности в деятельности государственных органов. В Узбекистане применение

технологий искусственного интеллекта имеет особое значение при использовании современных информационных технологий.

В соответствии со Стратегией «Цифровой Узбекистан — 2030» и в целях создания благоприятных условий для ускоренного внедрения технологий искусственного интеллекта и их широкого применения в стране, обеспечения доступности и высокого качества цифровых данных в указанной сфере утверждено ряд мер по изучению и внедрению технологий искусственного интеллекта.

Искусственный интеллект (ИИ) – это область компьютерных наук, направленная на создание систем и программ, способных выполнять задачи, требующие человеческого интеллекта. Эти задачи включают обучение, понимание речи, принятие решений, решение проблем и распознавание объектов. ИИ может имитировать различные аспекты человеческого мышления и поведения, что позволяет системам взаимодействовать с внешней средой и самостоятельно адаптироваться к новым данным.

Технологии искусственного интеллекта формируют комплекс технологических решений, позволяющих имитировать когнитивные функции человека (в том числе, самообучение и поиск решений при отсутствии заранее заданного алгоритма) и при выполнении задач достигать результатов, как минимум сопоставимых с результатами интеллектуальной деятельности человека, а как максимум значительно превосходящих человеческие возможности[1].

Под ИИ понимаются платформы, обеспечивающие анализ и прогнозирование в судебной и правоохранительной сферах на основе обработки больших данных с использованием машинного обучения, нейронных сетей и методов распознавания образов с выводом результатов в визуальном или любом ином понятном для конечных пользователей виде. Выделяется несколько направлений практического использования ИИ в судебной и правоохранительной сферах. Конкретно речь идет о:

- продвинутых семантических корпоративных поисковых системах;

- системах поиска и анализа ситуаций, содержащихся в юридических документах;

- системах поддержки разработки юридических документов на основе автоматического генерирования шаблонов;

[1] Филипова И.А. Правовое регулирование искусственного интеллекта: учебное пособие Нижний Новгород: Нижегородский госуниверситет, 2020. – 90 с.

- системах предиктивной судебной аналитики, ориентированных на адвокатские компании;

- юридических чат ботах, осуществляющих информирование сторон в ходе первоначальных контактов по тем или иным делам на естественных языках[2].

Искусственный интеллект может переводить допросы и очных ставок в текст, а также может помочь установить ведомственный контроль и прокурорский надзор за проведением доследственной проверки и уголовного расследования.

Но главная проблема использования ИИ в судебной практике – это то, что ИИ базируется не на ситуационной логике, а на вычислительных процедурах. ИИ не умеет работать с контекстами. Соответственно, в каждом государстве политические силы должны прийти к компромиссу и установить, в каких сферах и в каких аспектах судебной системы и правоохранительной деятельности можно использовать ИИ, а в каких использование этого инструмента опасно для политического консенсуса[3].

Искусственный интеллект невозможно реализовать в простой информационной системе. Одним из шагов к внедрению искусственного интеллекта является его обучение. Искусственный интеллект должен изучить ранее введенные данные и документы, выполненные действия.

Для обучения искусственного интеллекта документы должны быть в читаемой цифровой форме, и должно быть достаточно данных (реквизитов), описывающих документы.

В условиях современного мира, где цифровизация охватывает все сферы жизни, системы уголовного правосудия также требуют изменений. Системы электронного уголовного дела (далее – ЭУД) становятся неотъемлемой частью современного правосудия во многих странах мира.

Электронное уголовное дело представляет собой цифровую систему, которая позволяет автоматизировать процессы сбора, хранения и обработки информации, связанной с уголовными делами. Основные компоненты ЭУД включают электронные

---

[2] Б.Исмаилов, А.Атажанов. «Зарубежный опыт внедрения современных технологий в систему правосудия» Жамият ва инновациялар – Общество и инновации – Society and innovations Special Issue - 2, №01 (2020) / ISSN 2181-1415 https://cyberleninka.ru/article/n/zarubezhnyy-opyt-vnedreniya-sovremennyh-tehnologiy-v-sistemu-pravosudiya/viewer

[3] 3 Goodman B., Harder J. Four areas of legal ripe for disruption by smart startups (англ.). Law Technology Today. ABA Journal (16 December 2014).

документы, базы данных, системы управления делами и платформы для обмена информацией между участниками уголовного процесса.

Внедрение искусственного интеллекта в систему электронного уголовного дела в Узбекистане открывает новые горизонты для повышения эффективности и качества правосудия. Рассмотрим ключевые сферы, где ИИ может быть применен:

1. Автоматизация обработки данных.

ИИ может значительно ускорить процесс обработки больших объемов данных, связанных с уголовными делами. Системы на основе машинного обучения способны анализировать текстовые документы, выявлять ключевые факты и автоматически классифицировать материалы.

2. Предсказательная аналитика.

Использование алгоритмов предсказательной аналитики позволяет прогнозировать вероятность совершения преступлений на основе исторических данных. Это может помочь правоохранительным органам в планировании патрулирования и профилактических мерах.

3. Анализ судебной практики.

ИИ может анализировать судебные решения и выявлять тенденции в практике судов. Это поможет юристам и судьям принимать более обоснованные решения, основываясь на предыдущих делах и их исходах.

4. Поддержка расследований.

Системы ИИ могут помочь в расследовании преступлений, анализируя данные из различных источников (например, социальных сетей, финансовых транзакций) и выявляя связи между подозреваемыми и жертвами.

5. Улучшение доступа к правосудию.

Чат-боты и виртуальные помощники на базе ИИ могут предоставлять гражданам информацию о процессе уголовного дела, их правах и обязанностях, а также помогать в подготовке необходимых документов.

6. Обнаружение мошенничества.

Алгоритмы машинного обучения могут быть использованы для выявления аномалий в финансовых данных, что поможет в борьбе с экономическими преступлениями и мошенничеством.

7. Обработка жалоб и обращений.

Системы ИИ могут автоматизировать процесс обработки жалоб граждан, анализируя их содержание и направляя на соответствующие уровни для дальнейшего рассмотрения.

Ожидаемые результаты от внедрения искусственного интеллекта в ЭУД включают повышение доступности правосудия, улучшение защиты прав граждан и сокращение временных затрат на рассмотрение дел. Президент Республики Узбекистан Ш.М.Мирзиёев, в своих выступлениях, также уделил этому особое внимание. “Мы должны укреплять открытости и прозрачности деятельности судов, реализации концепции "электронных и цифровых судов"[4].

Использование технологий ИИ позволит повысить уровень прозрачности судебных процессов. Это может снизить уровень коррупции и повысить доверие граждан к судебной системе. Применение аналитических инструментов для оценки работы судов, поможет выявить возможные проблемы и устранить их.

А также могут значительно упростить процесс сбора, хранения и обработки информации, что приведет к более быстрой и эффективной работе правоохранительных органов. Автоматизация процессов позволит сократить время на обработку дел и снизить вероятность ошибок. Это приведет к более быстрому разрешению дел и сокращению нагрузки на сотрудников.

В органах прокуратуры Республики Узбекистан началась работа по внедрению современных технологий и искусственного интеллекта в информационные системы. Основная цель внедрения технологий искусственного интеллекта – оптимизация нагрузки сотрудников.

В 2023 году начато разработка новую версию информационной системы «E-material», а также в опытном порядке внедрить технологии искусственного интеллекта.

Сегодня существует необходимость цифровизации доследственной проверки и уголовного расследования. Процесс регистрации преступлений автоматизирован, но остальные процессуальные действия не фиксируются в электронной форме. В настоящее время для работы информационных систем и интеграций требуется много ресурсов.

Если искусственный интеллект внедрится в информационные системы типа «электронное уголовное дело», то он может

[4] Ш.М.Мирзиёев “Янги Ўзбекистон стратегияси” Тошкент – “Ўзбекистон” нашриёти - 2021 й. 464-бет. Ст. 109.

предоставлять следователям и дознавателям рекомендации по первоначальной квалификации преступлений.

В перспективе планируется в органах прокуратуры создать совершенно новую систему распознавания, классификации, распределения и направления, анализа и рассмотрения поступивших обращений, обобщения повторных обращений с помощью технологий искусственного интеллекта.

Открывает возможности для разработки новых решений на базе ИИ, таких как автоматизированные системы предсказания исходов дел или анализатор судебной практики. Эти инструменты могут помочь юристам в подготовке дел и повышении качества правовой помощи.

Но внедрение новых технологий требует подготовки специалистов, что может привести к повышению квалификации сотрудников правоохранительных органов. Перспективы международного сотрудничества также открывают новые возможности для обмена опытом и лучшими практиками. Важно отметить, что успешная внедрения искусственного интеллекта в ЭУД может стать основой для дальнейших реформ в области уголовного правосудия. Тем не менее, реализация этих перспектив потребует значительных инвестиций в инфраструктуру, обучение персонала и разработку безопасных технологий для защиты данных.

Внедрение искусственного интеллекта в электронное уголовное дело в Узбекистане имеет потенциал для значительного улучшения работы правоохранительных органов и судебной системы. Однако важно учитывать этические аспекты и необходимость обеспечения прозрачности и справедливости при использовании ИИ-технологий.

Одним из ключевых аспектов внедрения ИИ в уголовное судопроизводство является обеспечение справедливости и недискриминационного подхода в принимаемых решениях. Алгоритмы ИИ могут унаследовать предвзятости или ошибки, заложенные в исходных данных, что приводит к искажению результатов. Поэтому важна прозрачность алгоритмов и возможность их проверки, чтобы избежать дискриминации по половым, расовым или другим признакам. Также встает вопрос о том, кто несет ответственность за решения, принятые ИИ, что требует ясного правового регулирования.

Уголовные дела обычно содержат множество конфиденциальной информации, включая личные данные участников процесса. Безопасность данных становится критически важной задачей при внедрении ИИ в уголовное производство. Необходимо разработать системы защиты, которые предотвратят утечку данных или их несанкционированное использование. Особое внимание уделяется шифрованию данных, а также регламентации доступа к ним, чтобы минимизировать риски вмешательства в правовые процессы.

Для эффективного и безопасного применения ИИ в уголовном правосудии требуется разработка четкой правовой базы. Это включает регулирование использования технологий, определение ролей и ответственности всех участников, а также стандартизацию методов обработки данных и принятия решений. Правовая система должна адаптироваться к новым вызовам, которые ставят перед ней технологии ИИ, чтобы обеспечить баланс между автоматизацией процессов и защитой прав граждан.

КИБЕРЖИНОЯТЧИЛИККА ВА БОШҚА ТУРДАГИ ЖИНОЯТЛАРГА ҚАРШИ КУРАШДА СУНЪИЙ ИНТЕЛЛЕКТ: ИМКОНИЯТЛАР ВА ҲУҚУҚИЙ ЧЕКЛОВЛАР, ЭРИШИШ МУМКИН БЎЛГАН НАТИЖАЛАР

Шукуров Жахонгир Раббонаевич
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси
Тезкор-қидирув фаолияти ва киберҳуқуқ кафедраси ўқитувчиси

Аннотация *Ҳозирги рақамли асрда интернет ва ахборот технологиялари ҳаётимиздаги аксарият соҳаларни қамраб олди. Инсонларнинг турмуш тарзи, иш жараёнлари, бизнес фаолияти ва давлат бошқаруви интернет ва рақамли воситалар орқали амалга оширилиб, бу орқали жамиятдаги самарадорлик ва инновациялар юксалмоқда. Бироқ, бу ривожланиш кибержиноятчиликнинг ортишига ҳам сабаб бўлмоқда.*

Сунъий интеллект (СИ) киберхавфлардан ҳимоя қилишда муҳим восита сифатида жорий этилмоқда. Унда автоматлаштирилган таҳлил, хулоса чиқариш ва паттернларни аниқлаш қобилиятлари орқали киберҳужумларни олдиндан аниқлаш ва уларнинг олдини олиш бўйича самарали ечимлар ишлаб чиқилмоқда. Бу тезисда кибержиноятчиликка қарши курашда СИнинг имкониятлари, ҳуқуқий чекловлар ва жаҳондаги қатор илғор давлатларнинг бу йўналишдаги тажрибалари кўриб чиқилади.

Калит сўзлар: *кибермакон, кибержиноят, интеллект, сунъий интеллект, киберхавф, таҳлил, фишинг, DDoS, машинавий ўрганиш,*

автоматлаштирилган таҳлил, дастур, паттерн, прогнозлаш, реал вақт, ҳужум.

Аннотация *В настоящее цифровое время интернет и информационные технологии охватывают большинство сфер нашей жизни. Образ жизни людей, рабочие процессы, бизнес-деятельность и государственное управление осуществляются через интернет и цифровые инструменты, что способствует повышению эффективности и внедрению инноваций в обществе. Однако этот рост также привёл к увеличению киберпреступности.*

Искусственный интеллект (ИИ) внедряется как важный инструмент для защиты от киберугроз. Благодаря возможностям автоматизированного анализа, выводов и выявления паттернов разрабатываются эффективные решения для заблаговременного обнаружения кибератак и их предотвращения. В данной работе рассматриваются возможности ИИ в борьбе с киберпреступностью, правовые ограничения и опыт ряда передовых стран в этой сфере.

Ключевые слова: *киберпространство, киберпреступление, интеллект, искусственный интеллект, киберугроза, анализ, фишинг, DDoS, машинное обучение, автоматизированный анализ, программа, паттерн, прогнозирование, реальное время, атака.*

Annotation *In today's digital era, the internet and information technologies have permeated most aspects of our lives. People's lifestyles, work processes, business activities, and government administration are carried out through the internet and digital tools, enhancing efficiency and fostering innovation in society. However, this development has also contributed to the rise of cybercrime.*

Artificial Intelligence (AI) is being introduced as a vital tool for protecting against cyber threats. Through automated analysis, inference, and pattern recognition capabilities, AI enables the early detection of cyberattacks and provides effective solutions for their prevention. This thesis explores the potential of AI in combating cybercrime, the legal limitations, and the experiences of several leading countries in this field.

Keywords: *cyberspace, cybercrime, intelligence, artificial intelligence, cyber threat, analysis, phishing, DDoS, machine learning, automated analysis, software, pattern, forecasting, real-time, attack.*

Аввалambор, кибержиноятчиликнинг моҳиятига тўхталиш ва унинг тушунчасини кўриб чиқиш муҳим масаладир.

Кибержиноятчилик — бу интернет ёки ахборот технологияларидан фойдаланган ҳолда амалга ошириладиган жиноий фаолиятлар тоифаси бўлиб, у шахсий маълумотларни ўғирлашдан тортиб, корпоратив маълумотларга тажовуз қилиш, давлат ва бизнес маълумотларини бузиш, молиявий фирибгарлик, тижорат ва давлат сирларига тажовуз қилишгача бўлган кенг қамровли жиноятларни ўз ичига олади. Бу ҳужумлар замонавий технологиялардан кенг фойдаланган ҳолда амалга оширилади ва уларни аниқлаш ҳамда олдини олишни жуда қийинлаштиради.

Бунинг натижасида киберхавфсизликни таъминлаш ҳар бир замонавий давлатлар ва мавжуд бизнес соҳаси вакилларининг энг муҳим вазифаларидан бирига айланиб бормоқда.

Бугунги кунда кибержиноятчилик бир қанча турларга бўлинади, жумладан:

Фишинг – бу фирибгарлик йўли билан фойдаланувчининг шахсий ёки молиявий маълумотларини олиш мақсадида фирибгар электрон хабарлар ёки веб-саҳифалардан фойдаланиши.

DDoS (Distributed Denial of Service) - бу тизимга орттиқча юкламани юбориш орқали уни ишдан чиқариш ёки ишлаш қобилиятини пасайтириш.

Зарарли дастурлар орқали маълумотларни бузиш ёки шифрлаш орқали уларни қайтариб бериш учун товон талаб қилиш.

Зарарли дастурлар - бу компьютер ёки серверларга кириб, уларни бузиш ёки маълумотларни ўғирлашга қаратилган дастурий таъминот.

Кибержиноятлар ёки бошқа турдаги жиноятлар бўладими уларга қарши курашишда ривожланиб бораётган рақамли воситалар, айниқса, сунъий интеллектнинг имкониятларидан кенг фойдаланиш зарурияти ортиб бормоқда.

Сунъий интеллект технологиялари киберхавфларга қарши курашишда инсоннинг когнитив қобилиятларини автоматлаштириш орқали катта кўламдаги маълумотларни тез ва самарали таҳлил қилиш имкониятини беради. Машинавий ўрганиш алгоритмлари ва катта маълумотлар таҳлили (big data) жиноятчиликка қарши курашда ҳамда киберхавфсизликни таъминлашда муҳим воситалар ҳисобланади. СИ имкониятларидан кибержиноятларга, умуман кибертаҳдидларга қарши курашда фойдаланишимиз юқори афзалликларга эришишда қўл келиши мумкин. Жумладан:

Машинавий ўрганиш ва автоматлаштирилган таҳлил.

Бу анъанавий инсоннинг ўзидаги бу қобилятларига қараганда анча тез ҳамда аниқликда амалга оширилади.

СИ дастурлари кенг миқдордаги маълумотларни инсон аралашувисиз таҳлил қилиш ва улар асосида таҳдидларни аниқлаш имконини беради. Ҳар бир ҳужумни қўлда таҳлил қилиш инсон қобилиятидан ташқари бўлиши мумкин, аммо СИ бу жараённи автоматлаштириб, тезкорлик билан маълумотлар орасидаги аномалияларни (ноўрин ёки кутилмаган ҳолат) аниқлаб беради. Мисол тариқасида, IBMнинг “Watson for Cybersecurity” тизими катта

маълумотларни таҳлил қилиб, кибержиноятларга қарши ҳимоя стратегияларини ишлаб чиқишда фойдаланилади.

Паттернларни аниқлаш ва таҳдидларни олдиндан кўриш.

Паттерн — бу муайян қонун-қоидалар, қонуниятлар ёки такрорланувчи схемалар асосида намоён бўладиган тузилма ёки тенденция.

СИнинг муҳим имкониятларидан бири — паттернларни аниқлаш ва таҳдидларни олдиндан кўра олиш қобилиятидир. Машинавий ўрганиш алгоритмлари турли сценарийлар орқали киберҳужумларга хос бўлган паттернларни топади ва уларнинг қайталанишини олдиндан аниқлайди.

Паттернларни аниқлаш ва жиноятларни олдиндан кўриш – бу маълумотларни таҳлил қилиш (data analytics) ва сунъий интеллект (AI) соҳасидаги концепция бўлиб, у инсоннинг қонунбузарлик ёки хавфли ҳаракатларини олдиндан тахмин қилишни мақсад қилади. Бу тушунчани яхшироқ тушуниш учун уни икки қисмга ажратиб кўрамиз: **паттернларни аниқлаш** ва **жиноятларни прогноз қилиш**.

Паттернларни аниқлаш. Тасаввур қилинг, сиз изқуварсиз ва шаҳарда жиноятлар билан боғлиқ юзлаб ҳодисалар юз беради. Ҳар бир жиноятни алоҳида қараганда, улар фақат битта ҳодиса бўлиб туюлади, аммо сиз ҳамма маълумотни тўплаб таҳлил қила бошласангиз, маълум қонуниятларни (паттернлар) аниқлайсиз. Бу худди ҳаётингизда оддий юз берадиган одатларни кузатишга ўхшайди. Бу жараёнда маълумотлар орасидан такрорланувчи қонунлар, алоқадорликлар ва тенденцияларни излаймиз. Масалан, бир маҳалладаги жиноятлар асосан кечки соат 20-22 лар атрофида юз бериши ва улар асосан пайшанба куни содир бўлишини кузатсак, бу паттерн ҳисобланади. Демак, бу вақт ва жойда хавф юқори бўлишини кутиш мумкин.

Жиноятларни олдиндан кўриш (прогнозлаш). Энди паттернлар аниқлангандан сўнг, компьютер моделлари ва статистикадан фойдаланиб, қайси вақтда ва қаерда жиноят содир бўлиши мумкинлигини тахмин қилиш (прогнозлаш) мумкин. Бу концепция хорижда “Predictive Policing” деб аталади, яъни – прогноз асосида полицияни ташкил этиш номи билан танилган.

Масалан, сиз ҳар куни эрталаб ҳароратга қараб қачон ёмғир ёғишини прогноз қиласиз.

Энди тахминлаш моделлари қандай ишлайди?-деган саволга қуйидагича жавоб беришимиз мумкин.

Биринчи қадам, машинавий ўқитиш (machine learning). Бунда моделлар тарихий маълумотларни ўрганиб, паттернларни аниқлайди. Масалан, ўтмишда ўғирликлар асосан якшанба кунлари маълум бир ресторан яқинида ёки ҳудудда юз берган бўлса, алгоритмлар шу каби ҳолатлар яна содир бўлиш эҳтимолини ҳисоблайди.

Иккинчи қадам, таҳлил ва қарор қабул қилиш. Агар маълум бир жой ва вақтда жиноят содир бўлиши эҳтимоли юқори бўлса, хизматга жалб этилган ходимлар ва кучларни ўша ерга олдиндан жўнатиш мумкин.

Техник жараён мураккаб ҳисобланиб, жиноятлар ҳақидаги тарихий маълумотлар, видеокамералардан олинган маълумотлар, ижтимоий тармоқлардаги хабарлар ва бошқалар маълумотлар манбасини ташкил этиши мумкин.

Бироқ, бундай прогнозларда хато эҳтимоли мавжуд. Тўпланган маълумотларда хатолик ҳам бўлиши мумкин. Ҳар доим тўғри маълумотлар йиғилмайди. Нотўғри маълумотлар нотўғри прогнозларга олиб келиши мумкин. Масалан, компьютерга тақдим этилган нотўғри маълумот асосида нотўғри қарорлар қабул қилиниши мумкин. Шунинг учун, бундай тизимлар ҳар доим инсон кузатуви ва аниқ таҳлил билан бирга қўлланилиши керак.

Реал вақтда жиноятларга, ҳужумларга қарши кураш.

Реал вақтда ҳужумларга қарши кураш – бу жиноятлар содир бўлишидан олдин ёки уни содир бўлаётган вақтда тезкорлик билан чора кўришни англатади. Бундай тизимлар маълумотларни доимий равишда кузатиб боради, таҳлил қилади ва тезкор қарорлар қабул қилишга ёрдам беради. Бундай тизимлар жуда катта миқдордаги маълумотлар билан ишлаш ва сунъий интеллект орқали таҳлил қилиш қобилиятига эга.

СИ воситалари ҳужумлар рўй берган вақтда уларни тезкорлик билан аниқлайди ва олдини олиш чораларини кўради.

Бу тизимлар ҳужумлар ва жиноятлар содир бўлиши мумкин бўлган жойларни онлайн кузатиб, хавф пайдо бўлиши биланоқ ҳушёрлик билан реакция қилади. Бундай жараёнлар асосан

4 босқичда амалга оширилади:

маълумотларни реал вақтда йиғиш;

хавфларни аниқлаш ва таҳлил қилиш;

автоматик хавф сигналларини бериш;

тезкор чора кўриш ва қарорлар қабул қилиш;

маълумотларни реал вақтда йиғиш;

Маълумотлар турли хил манбалардан, яъни видеокамералар ва дронлар, сенсорлар ва сигнализациялар, GPS қурилмалари, ижтимоий тармоқлардан доимий равишда тушиб туради.

Юзага келиши мумкин бўлган хавфларни аниқланиб, таҳлил қилинади. Маълумотлар катта миқдорда йиғилгани учун сунъий интеллект алгоритмлари бу маълумотни таҳлил қилади. Бундай тизимлар паттернларни аниқлаб, шубҳали фаолиятни топади.

Реал вақтдаги хавфни аниқлаш ҳам шундай ишлайди. Агар одамларнинг ҳаракати одатдаги оқимдан кескин фарқ қилса (масалан, инсонлар номувофиқ тезликда юра бошласа), алгоритмлар буни хавф сифатида баҳолайди. “Machine Learning” моделлари жиноятларни олдинги маълумотлар асосида таҳлил қилиб, анъанавий ва шубҳали фаолиятни ажратиб беради.

Автоматик хавф сигналларини беришда агар камералар кўп одам йиғилишини ёки кутилмаган тезликда ҳаракатларни кузатса, автоматик равишда хабар берилади. Банк ёки бирор-бир омборхонада сигнализация ёқилса, қўриқлаш гуруҳи реал вақтда ўша ерга жўнатилади.

Тезкор чора кўриш ва қарорлар қабул қилишда маълумотлар таҳлил қилинганидан сўнг, тизим ички ишлар ёки маълум бир хавфсизликни таъминловчи хизматларига чора кўриш бўйича тавсиялар беради. Бундай тавсиялар автоматик ёки қўлда бажарилиши мумкин.

Автоматик реакцияларларда, овозли огоҳлантириш тизимлари ёқилади, сигнализациялар автоматик ишга тушади ёки камералар хавфли объектни яқинлаштириб суръатга олади ва бошқалар.

Қўлда реакцияда эса, ички ишлар идораси навбатчилик қисми воқеа жойига экипажни жўнатади ёки бошқа чораларни кўришга қарор қилади.

Бугун бу тизимлардан реал ҳаётда шаҳар хавфсизлиги таъминлашда, банк ва молия муассасаларида, жамоат тадбирларида қўллаш мумкин.

Масалан, Лондон каби шаҳарларда кўчалардаги камералар реал вақтда одамлар оқимини кузатади. Агар шубҳали ҳаракатлар ёки нотўғри ҳаракатлар кузатилса, полицияга жўнатилади.

Бундан ташқари, банк ва молиявий муассасаларида сигнализациялар ва сенсорлар ёрдамида ўғриликлар ва турли ҳужумлар олдини олиш мумкин. Жамоат тадбирларида, яъни стадионлар ёки концертларда одамларнинг шубҳали ҳаракатлари

кузатиб борилиб, хавф содир бўлишидан олдин чора кўрилиши мумкин.

Тадбиқ этиш жараёнида айрим хавф ва чекловларни ҳам инобатга олиш муҳим. Ҳар доим ҳам автоматик тизимлар аниқ прогноз бера олмаслиги мумкин. Доим инсон омилидан фойдаланиш керак. Масалан, камера нотўғри таҳлил қилиб, одамларнинг оддий ҳаракатини хавф сифатида баҳолаши мумкин. Натижа шахсий ҳаётнинг бузилишига олиб келиши, ижтимоий тармоқлар ва камералар орқали кузатувлар баъзида одамларнинг шахсий ҳаётини чеклаб қўйиши мумкин.

СИ имкониятларидан фойдаланиб жиноятчиликка қарши курашни амалга ошириш жараёнида ҳуқуқий чекловлар ва муаммолар юзага келиши эҳтимолдан ҳоли эмас. Жараёнда маълумотларнинг махфийлиги ва шахсий ҳаёт дахлсизлиги, алгоритмларнинг шаффофлиги ҳамда халқаро ҳуқуқий меъёрларга алоқадор муаммолар юзага келиши мумкин. Бу чеклов ва муаммоларни бартараф этишда миллий қонунчилик ва халқаро ҳужжатларга асосланган ҳолда чоралар кўриш лозим бўлади.

СИдан киберхавфларга қарши курашда фойдаланиш жараёнида маълумотлардан кенг фойдаланиш талаб этилади. Кўпгина давлатларда шахсий маълумотларни ҳимоя қилиш тўғрисидаги қонунлар мавжуд. Бу қонунлар маълумотларни қайта ишлаш жараёнида шахсий ҳаёт дахлсизлигини таъминлашга қаратилган.

СИ алгоритмлари мураккаб ва кўпинча тушунарсиз бўлиб, улар қандай қарорлар қабул қилаётганини тушуниш қийин. Бу ҳолат ҳуқуқий муаммоларни келтириб чиқаради, чунки инсон ҳуқуқлари бузилиши ёки номақбул қарорлар қабул қилиниши мумкин. Бу муаммолар ҳозирда халқаро даражада муҳокама қилинмоқда. Европа Комиссияси СИ алгоритмларининг шаффофлигини ошириш учун қонунларни такомиллаштириш устида ишламоқда.

Кибержиноятчиликнинг глобал характери халқаро ҳуқуқий меъёрларнинг ишлаб чиқилишини талаб этади. Аммо ҳозирги кунда турли давлатлар ўртасида ушбу йўналишда ягона қонунчилик базаси йўқ. Масалан, АҚШ, Хитой ва Европа Иттифоқи ўртасидаги СИ ва киберхавфсизликни тартибга солиш бўйича қонунлар бир-биридан фарқ қилади, бу эса халқаро киберхавфларга қарши самарали курашишга тўсқинлик қилади.

Тезис доирасида илғор давлатларнинг кибержиноятларга қарши курашдаги тажрибалари тўхталиш аҳамиятлидир.

Дунё миқёсида киберхавфсизликка эътибор қаратган ва бу соҳада илғор технологияларни жорий қилган давлатларнинг тажрибаси муҳим ҳисобланади.

АҚШ дунёдаги энг кучли киберхавфсизлик инфратузилмаларига эга давлатлардан бири ҳисобланади. АҚШ Миллий хавфсизлик агентлиги (NSA) ва ФТБнинг сунъий интеллектдан фойдаланиб амалга оширадиган киберхавфларга қарши дастурлари катта миқдордаги маълумотларни таҳлил қилиш ва ҳужумларни олдиндан аниқлаш имконини яратмоқда. Шунингдек, Хитой, Исроил, Германия, Япония, Буюк Британия, Канада, Франция, Корея, Сингапур каби давлатларнинг соҳадаги илғор тажрибаларини тадқиқ этиш ва эришилган ютуқларидан республикамизда бу борадаги ислоҳотларни амалга оширишда фойдаланишимиз мумкин.

СИ имкониятларидан фойдаланиш кибержиноятлар ва бошқа жиноятларга, киберхавфларга қарши курашда қатор ижобий натижаларга эришишни таъминлайди.

СИ технологиялари ёрдамида киберхавфсизлик тизимларини автоматлаштириш орқали инсон аралашувисиз тезкор ҳимояни амалга оширади. Бу эса давлат ва компанияларнинг хавфсизлик харажатларини сезиларли даражада камайтиради.

Ҳужумларни реал вақтда аниқлаш ва тўхтатиш имконини бериб, янги таҳдидларга тезкор жавоб қайтаришни таъминлайди. Бу эса катта муваффақиятларга эришиш имкониятини яратади.

Халқаро даражада СИ ва киберхавфсизлик бўйича ҳамкорликни кучайтириш билан хавфларни олдиндан аниқлаш ва уларга қарши самарали чоралар кўриш мумкин.

Хулоса қиладиган бўлсак, сунъий интеллект кибер-жиноятчиликка қарши курашишда катта имкониятларга эга бўлиб, унинг автоматлаштириш, тезкорлик ва аниқлик каби хусусиятлари давлатлар ва хусусий сектор учун жуда фойдали. Аммо ҳуқуқий муаммолар, хусусан, маълумотларнинг махфийлиги ва алгоритмларнинг шаффофлиги масалалари ҳал қилиниши керак. Илғор давлатлар тажрибаси шуни кўрсатадики, СИ технологияларини жорий қилиш орқали кибержиноятларга ва киберхавфларга қарши самарали курашиш мумкин.

КИБЕРХАВФСИЗЛИК СОҲАСИДАГИ ХАЛҚАРО ҲАМКОРЛИК ИМКОНИЯТЛАРИДАН КИБЕРЖИНОЯТЛАРГА ҚАРШИ КУРАШДА ФОЙДАЛАНИШ ИСТИҚБОЛЛАРИ

Убайдуллаев Қудратилла Хабибуллаевич
сиёсий фанлар доктори (DSc), катта илмий ходим

Аннотация. *Ушбу мақолада киберхавфсизлик соҳасидаги хорижий давлатлар тажрибасидан Ўзбекистонда фойдаланиш имкониятлари ўрганилган. Хусусан, кибержиноятларга қарши курашда халқаро ҳамкорлик қилиш билан боғлиқ муаммолар тадқиқ этилган.*

Калит сўзлар: *киберхавфсизлик, кибермакон, кибертаҳдидлар, кибержиноятлар, халқаро ҳамкорлик, ҳуқуқ-тартибот органлари, киберҳужумлар, трансчегаравий жиноятла*

Аннотация. *В данной статье изучена возможности использования опыта зарубежных стран в Узбекистане в сфере кибербезопасности. В частности, исследованы проблемы, связанные с международным сотрудничеством в борьбе с киберпреступностью.*

Ключевые слова: *кибербезопасность, киберпространство, киберугрозы, киберпреступления, международное сотрудничество, правоохранительные органы, кибератаки, трансграничные преступления.*

Abstract. *This article examines the possibilities of using the experience of foreign countries in cybersecurity field in Uzbekistan. In particular, the problems related to international cooperation in the fight against cybercrime were studied.*

Keywords: *cybersecurity, cyberspace, cyberthreats, cybercrimes, international cooperation, law enforcement agencies, cyberattacks, cross-border crimes.*

Дунё цивилизацияси XXI асрнинг чорак қисмига яқинлашиб борар экан, кибермакондаги ижтимоий-иқтисодий ва ҳарбий-сиёсий муносабатлар тобора фаоллашиб, рақамли технологиялар билан ер шари аҳолиси ўртасидаги ўзаро трансформациялашув жараёнлари янада кучлироқ давом этишини кўрсатмоқда.

Инсониятнинг глобал Интернет тармоққа ижтимоийлашув жараёнлари тобора кучайиб бормоқда. Хусусан, ер юзи аҳолисининг 60 фоизи ва уларнинг суткалик ўртача 6 соат вақти Интернетда ўтмоқда. Шу билан бирга, сўнгги беш йилда глобал тармоқда ахборот алмашиш ҳажми икки каррага ошган.[1]

Айрим ҳукмрон давлатлар ўртасидаги сиёсий ўйинлар ва қарама-қаршиликларда иқтисодий санкциялар, энергетик ва бошқа ресурслардан босим кўрсатувчи восита сифатида фойдаланиш билан бир қаторда, махсус киберҳужумлар қўлланилмоқда.

[1] Global Business Data Platform Statista. https://www.statista.com/statistics/631151/worldwide-data-collected-by-smart-buildings/: 30.08.2024 йилда мурожаат қилинди.

Америкалик таниқли журналист Ш.Харрис кибермаконни ҳаво, қуруқлик, денгиз ва космосдан кейинги ҳарбий ҳаракатларнинг бешинчи театр майдони сифатида таърифлайди.[2]

БМТ Бош котиби А. Гутерриш таъкидлаганидек, “Афсуски, бугунги кунда давлатлар ўртасида киберуруш билан боғлиқ ҳолатлар кўзга ташланмоқда. Энг ёмони, бу каби урушларга чек қўядиган ва уларни тартибга соладиган универсал халқаро нормалар мавжуд эмас”.[3]

Биргина сунъий интеллектнинг амалиётда мақсадли қўлланилиши, кибержиноятларнинг анонимлик ва трансчегаравийлик хусусиятларига сезиларли туртки берди. Жумладан, кибержиноятчилар электрон манзилларни клонлаштирган ҳолда, исталган давлат фуқаросининг қиёфасида муҳим ахборот инфратузилмаси объектларига ёки персонал маълумотлар базасига киберҳужум уюштириш имкониятига эга бўлмоқда.

Бугунги кунда киберхавфсизликни таъминлаш ва кибержиноятларга қарши кураш масалалари ҳуқуқ-тартибот идораларнинг энг долзарб вазифаларидан бири ҳисобланади. Айниқса, ушбу соҳада миллий қонунчиликни тўлиқ ишлаб чиқилмаганлиги ҳамда халқаро нормаларнинг тартибга солинмаганлиги трансчегаравий кибержиноятларга қарши кураш бўйича саъй-ҳаракатларни мувофиқлаштиришда ўзига хос муаммоларни келтириб чиқармоқда.

Жумладан, ривожланган давлатлар тажрибасининг таҳлили шуни кўрсатмоқда-ки, иқтисодий соҳадаги кибержиноятларга (киберфирибгарлик, ўғирлик) қарши курашда Интерпол ва Европол каби халқаро полициянинг имкониятларидан самарали фойдаланган ҳолда, ўз вақтида зарур бўлган тезкор-қидирув ва махсус тергов ҳаракатларини амалга оширишни талаб этмоқда. Шунингдек, ноқонуний халқаро пул ўтказмалари билан боғлиқ банк транзакция операцияларини “музлатиб қўйиш” ҳамда уларнинг ҳақиқий эгаларини аниқлаш муаммоси сақланиб қолмоқда.

Хусусан, Ўзбекистонда киберфирибгарликлар билан боғлиқ жиноятларни содир этилиши натижасида, тўпланган пул маблағларини хорижий валюта пластик карталарига ўтказиш ва криптовалютага айирбошлаш операцияларидан сўнг, ўғирланган маблағларни ўзлаштирувчи шахсларга нисбатан тезкор-қидирув ва

[2] Харрис Шейн. Кибервойн@. Пятый театр военных действий. Пер. с англ. - М.: Альпина нон-фикшн, 2016. - 390 с.

[3] https://dfnc.ru/security/kibervojny-v-seroj-zone/: 30.08.2024 йилда мурожаат қилинган.

тергов ҳаракатларини амалга ошириш жараёнларида халқаро ҳамкорлик муаммолари юзага келмоқда.

Мазкур ҳолатларда, шунингдек, терроризмни молиялаштириш, кибертерроризм билан боғлиқ трансчегаравий жиноятларни фош этишда юқоридаги имкониятлар билан бир қаторда, халқаро ташкилотлар, давлат-хусусий шерикчилик секторидан фойдаланиш, хорижий давлатларнинг ҳуқуқ-тартибот идоралари ёрдамида гумонланаётган шахслар, уларнинг яқин алоқалари, электрон манзиллари, банк-ҳисоб рақамларини текширишдаги ҳамкорлик ишлари суст олиб борилмоқда.

Киберхавфсизлик муаммоси глобал аҳамиятга эга бўлганлиги боис, ривожланган давлатларда киберхавфсизлик стратегиялари қабул қилиниб, киберқуроллардан ҳарбий-сиёсий мақсадларда фойдаланилмоқда. Қолаверса, бугунги кунда 130 га яқин давлатларда киберхавфсизлик стратегиялари қабул қилинган.

Бу соҳада хорижий мамлакатларда илмий-тадқиқот институтлари ҳамда таҳлилий марказлар фаолият кўрсатмоқда. Жумладан, АҚШ, Буюк Британия, Хитой, Россия каби давлатларда квант криптографияси, кибернетик қурилларнинг замонавий турларини яратиш, графлар назариясини қўллаган ҳолда, кибермакондаги аноним фойдаланувчиларни аниқлаш, сунъий интеллектдан гибрид урушларда фойдаланиш бўйича фундаментал тадқиқотлар олиб борилмоқда.[4]

Ундан ташқари, глобал киберхавфсизлик муаммоларини тадқиқ этувчи марказларда, хусусан Европа Иттифоқи (ЕИ) давлатлари бўйича Интернетдан хавфсиз ва эркин фойдаланиш жамияти (Internet Society), тармоқлар ва ахборот хавфсизлиги бўйича ЕИ агентлиги (ENISA), АҚШ ички хавфсизлик вазирлиги таркибидаги миллий киберхавфсизликни бошқариш маркази (National Cyber Security Division) ва бошқа илмий-тадқиқот марказларида киберхавфсизликнинг амалий масалалари ўрганилмоқда.[5]

---

[4] Расторгуев С.П. Литвиненко М.В. Информационные операции в сети Интернет. – М.: 2014. – 133 с.; Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: 2017. – 546 с.; Yoko Nitta. Review of the Japan Cybersecurity Strategy. ISPSW Strategy Series: Focus on Defense and International Security Review of the Japan Cybersecurity Strategy. Issue No. 290. September 2014. 1-8 pp.; Melissa E. Hathaway, Alexander Klimburg. National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. 2012. – 44 p.

[5] Мелисса Хатауэй, Крис Демчак, Джейсон Кербен, Дженнифер МакАрдл, Франческа Спидальери. Киберготовность США: краткая информация. Сентябрь 2016, - 53 с. Опубликовано Потомакским Институтом политических исследований (Potomac Institute for Policy Studies) 901 N. Stuart St, Suite 1200 Arlington, VA 22203. potomacinstitute.org.; Keir Giles. Conflict Studies Research Centre, UK. Legitimation of Online Surveillance and Monitoring. Eighth International Forum “Partnership of State Authorities, Civil Society

Ўзбекистон Республикасида ҳам киберхавфсизликни таъминлаш соҳасига давлат сиёсати даражасида алоҳида эътибор қаратилмоқда. Хавфсизлик кенгашининг 2023 йилдаги кенгайтирилган йиғилишида Президент Ш. Мирзиёев томонидан сўзланган нутқда ахборот ва киберхавфсизликни таъминлаш миллий хавфсизлик соҳасидаги муҳим вазифа бўлиб қолишига урғу берилди.[6]

Сўнгги вақтларда, маҳаллий олимлар томонидан киберхавфсизликни таъминлашнинг сиёсий ва ҳуқуқий муаммоларини тадқиқ этиш бўйича бир қатор илмий тадқиқотлар амалга оширилди. Жумладан, А.У. Анорбоев, А.А. Матчанов, А.К. Расулев ва бошқалар томонидан кибержиноятларни олдини олиш ва киберхавфсизликни таъминлашнинг норматив-ҳуқуқий асосларини такомиллаштириш бўйича илмий изланишлар олиб борилди.[7]

2020 йилда ЕИнинг янги киберхавфсизлик стратегияси қабул қилинди. Мазкур ҳужжатда ЕИ киберхавфсизлигини таъминлаш принциплари, рақамли иқтисодиётга ўтишда миллий қадриятларни сақлаш, сўз, ахборот эркинлиги, шахсий маълумотлар дахлсизлиги, конфиденциал маълумотларни ҳимоялаш, кибертерроризмга қарши кураш, кибержиноятларни олдини олиш, соҳадаги стратегик устувор йўналишлар, фуқаролар учун барқарор кибермаконни яратиш каби мақсадлар мужассамлаштирилган.[8]

Шунингдек, ЕИ киберстратегиясида хавфсизлик учун жавобгар ташкилотлар, киберҳужумларга қарши курашнинг мувофиқлаштириш механизмлари, киберхавфсизликни таъминлашда хусусий секторнинг роли, халқаро ҳамкорлик, аҳоли ўртасида кибертаҳдидлардан ҳимояланиш бўйича тушунтириш-профилактик ишларни олиб бориш, кибержиноятларга қарши курашда тезкор маълумот алмашиш, Европол, Интерпол, адлия идоралари ва бошқа ҳуқуқ-тартибот органлари билан ҳамкорлик қилиш учун ҳужжатни ратификация қилиш талаблари белгилаб берилди.

---

and the Business Community in Ensuring International Information Security" Ninth Scientific Conference of the International Information Security Research Consortium. April 21-24, 2014. Garmisch-Partenkirchen, Munich, Germany. 240-247 pp.; Lech J. Janczewski, Andrew M. Colarik. Cyber Warfare and Cyber Terrorism. University of Auckland, New Zealand. New York, 2008. – 565 p.

[6] president.uz/uz/list/view/6967: 25.08.2024 йилда мурожаат қилинган.

[7] Анорбоев А.У. Кибержиноятчилик, унга қарши қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари. Монография. – Т.: 2020. – 324 б.; Матчанов А.А. Жиноятчиликка қарши курашда халқаро хамкорлик истиқболлари. Монография. – Т.: 2012. – 135 б.; Расулев А.К. Совершенствование уголовно-правовых и криминалистических мер борьбы с преступлениями в сфере информационных технологий и безопасности. Дис. докт. юрид. наук. – Т.: 2018. – 250 с.

[8] The EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec. europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

2023 йилда Ж. Байден томонидан тасдиқланган АҚШ миллий киберхавфсизлик стратегияси беш қисмдан иборат бўлиб, унинг асосий мақсади глобал кибермаконда АҚШ миллий манфаатларини ҳимоя қилиш ва мустаҳкамлашдан иборат.

Унинг биринчи қисми - муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини таъминлаш, иккинчиси - хавфли акторларга қарши чоралар кўриш, учинчиси - рақамли экотизим хавфсизлигини таъминлаш, киберхавфсизлик соҳасида бозор муносабатларини кучайтириш ҳамда соҳага самарали инновацияни тадбиқ этиш, тўртинчиси - Федерал грант лойиҳалари ва маблағлар ҳисобига соҳани молиялаштириш ва ниҳоят бешинчиси - киберхавфсизликни таъминлаш ҳамда кибержиноятчиликка қарши курашда халқаро ҳамкорликни кучайтириш кўзда тутилган.

Мазкур ҳужжатда кибермакондаги қуйидаги тенденциялар эътиборга олинган:

дунё цивилизацияси рақамли қарамликнинг чуқурлашган босқичига ўтиб бормоқда;

ривожланаётган IT-технологиялар билан бир қаторда, тизимли хавф-хатарлар пайдо бўлмоқда;

ишлаб чиқилаётган дастурий таъминот ва тизимлар мураккаблашиб, фойдаланувчиларнинг уларга бўлган ишончсизлиги кучайиб бормоқда;

сунъий интеллект тизимларининг кенг миқёсда жорий этилиши, ҳаттоки унинг яратувчилари учун ҳам жиддий хавфларни келтириб чиқармоқда;

Интернет тармоғи шахс, жамият ва давлатнинг ахборот алмашинув жараёнларини тезлаштириш билан бирга, ўзаро боғланган таҳдидларни ҳам вужудга келтирмоқда;

шахсга тегишли маълумотларни тўплаш ва улардан жиноий мақсадларда фойдаланиш имкониятлари ортиб бормоқда;

жисмоний чегаралар тобора ўз кучини йўқотиб, муҳим ахборот инфратузилмалари объектларига нисбатан кибертаҳдидлар кучайиб бормоқда;

булутли ва IoT-технологиялар оммалашиб, фуқаролар ҳамда ҳарбий объектларни жойлашув локацияси ва навигациясини аниқлаш имкониятлари кенгаймоқда.

Шу билан бирга, 2001 йилда қабул қилинган ЕИ Конвенциясининг тўртта моддасида “соф” турдаги кибержиноятлар (ноқонуний кириш, ахборотларни ноқонуний тутиб олиш,

компьютер тизимлари ва тармоқларидан ноқонуний фойдаланиш, тизимга ҳалақит бериш) аниқлаб берилди.[9]

Шунингдек, мазкур конвенцияда турли зарарли дастурларни киритиш йўли билан компьютер тизимларининг бир меъёрда ишлашига тўсқинлик қилиш (5-модда), компьютер қурилмалари ҳимоя тизими ва паролларидан жиноий мақсадларда фойдаланиш, зарарли дастурлар, қурилмалар ва бошқа воситаларни яратиш, тарқатиш ёки сотиш (6-модда), компьютер маълумотларини сохталаштириш - қасддан ўзгартириш, қалбакилаштириш, ўчириш ва йўқ қилиш (7-модда), компьютер фирибгарлиги (8-модда), болалар порнографияси боғлиқ жиноятлар (9-модда), муаллифлик ҳуқуқи ва бошқа турдош ҳуқуқларни бузилиши (10-модда) ҳамда жиноят содир этишга суиқасд қилиш, ёрдам бериш ва далолатчи бўлиш (11-модда) каби жиноий ҳаракатлар кўзда тутилган.

Шу билан бирга, конвенциянинг 11-моддасида белгиланган ҳолатлар бўйича 2-10 моддалари билан боғлиқ қилмишларни содир этганлик учун қонуний чораларни белгилаш мумкинлиги қайд этилган.

Ушбу конвенциянинг айнан 11-моддасида белгиланган ҳолатларни Ўзбекистон Республикаси Жиноят Кодексининг тегишли моддаларига, яъни кибержиноятларни содир этиш мақсадида кибермакондан восита сифатида фойдаланиш ҳолатлари билан уйғунлаштирилганда, замонавий кибертаҳдид манбаларини шакллантирувчи жиноятларга нисбатан ҳуқуқий баҳо бериш имкониятлари пайдо бўлади.

Хусусан, Ўзбекистон Республикаси ЖКнинг 28-моддасида “Жиноятни бажарувчи билан бир қаторда ташкилотчи, далолатчи ва ёрдамчилар ҳам жиноят иштирокчилари ҳисобланади” деб белгилаб қўйилган (1-хат боши). Шунингдек, мазкур моддада далолатчи, ёрдамчи ва кодекснинг 25-моддасида жиноятни содир этишга суиқасд қилувчи шахсларнинг тоифасига аниқлик киритилган.[10]

Шу ўринда, кодексда ёрдамчи шахсга берилган таърифни кибержиноятчиларга нисбатан қўлланилишига алоҳида эътибор қаратиш лозим бўлади. Жумладан, кибермакондаги мавжуд ҳимоя тизимларини бузиб кириш, унинг имкониятларидан восита ёки жиноят содир этиш қуроли сифатида фойдаланишга кўмаклашувчи шахсни - ёрдамчи деб ҳисоблаш мумкин.

---

[9] Европейская Конвенция по киберпреступлениям (преступления в киберпространстве) Будапешт, 23 ноября 2001 года.

[10] Ўзбекистон Республикаси Жиноят Кодекси. –Т.: Адолат, 2019. – Б. 9-10.

Маълумки, кибермакондан террорчилик мақсадларида фойдаланиш кибертерроризм тушунчасини ифодалайди. Darknet орқали виртуал валюталарни айирбошлашга, терроризмни молиялаштиришга ҳамда уларга тегишли материалларини ушбу тизимларда яширин сақлашга кўмакчи бўлаётган кимсаларни айнан юқоридаги ёрдамчи шахслар тоифасига киритиш ўринли бўлади.

Демак, кибержиноятлар бўйича ЕИ Конвенциясини Ўзбекистонда ратификация қилиниши, унинг санаб ўтилган моддаларини ЖКнинг тегишли бандларига имплементация этилиши келгусида замонавийлашиб бораётган кибержиноятларни аниқ жиноий-ҳуқуқий баҳолаш ҳамда уларга нисбатан ҳаққоний жазо чораларини белгилаш имкониятини беради.

Юқоридаги қисқа таҳлил натижаларини эътиборга олган ҳолда, қуйидаги таклифларни илгари суриш мақсадга мувофиқ ҳисобланади:

миллий кибермаконда хизмат кўрсатиш, киберхавфсизликни таъминлаш инфратузилмасини ривожлантириш, ушбу соҳадаги инновацион халқаро ҳамкорликни фаоллаштириш ва хусусий секторнинг ролини ошириш;

кибержиноятларга қарши кураш бўйича ҳуқуқ-тартибот идораларининг тезкор-қидирув тадбирлари самарадорлигини ошириш мақсадида минтақавий ва халқаро доирадаги ҳамкорлик муносабатларини ривожлантириш, бу борада халқаро ташкилотлар томонидан қабул қилинган келишувлар ва конвенцияларни ратификация қилиш;

кибертерроризмга ва трансчегаравий кибержиноятларга қарши кураш бўйича республика ҳуқуқ-тартибот органлари билан Интерпол ҳамда Европол доирасида глобал Интернет тармоғида фаолият кўрсатувчи йирик IT-компаниялар ўртасидаги ҳамкорлик муносабатларини ривожлантириш;

замонавий кибержиноятларни содир этилиш эҳтимоли ва кўламидан келиб чиққан ҳолда, ривожланган хорижий давлатларнинг ушбу соҳадаги тажрибаси асосида киберсуғурта механизмини ишлаб чиқишни Ўзбекистон Республикаси киберхавфсизлик стратегиясида эътиборга олиниши лозим. Яъни, Ўзбекистонда қайд этилаётган кибержиноятлардан келадиган моддий зарар миқдорини баҳолаш, киберхатарларни суғурталаш, етказилган моддий ва маънавий зарарларни қоплаш тизими (норматив-ҳуқуқий асослари) ишлаб чиқилиши зарур.

AI-DRIVEN WEB SECURITY: NLP-BASED LOG ANALYSIS IN FIREWALLS

***Aliyev Abdurahmon**, (PhD),*
Turin polytechnical university in Tashkent, Dotsent,
e-mail: aliyev95.uz@mail.ru,
phone: +998 91 2198319,

***Makhamatov Nurilla**, (DSc),*
Turin polytechnical university in Tashkent, Professor, Head of department
e-mail: n.mahamatov@new.polito.uz,
phone: +998 71 2467082,

***Annotatsiya** ushbu maqolada veb-ilovalar xavfsizlik devorlarida (WAF) loglarini tahlil qilish uchun sun'iy intellektga asoslangan veb-xavfsizlik yondashuvi taklif etiladi. Biz server loglarini tahlil qildik va zararli harakatlar loglarini aniqlash uchun ularni mashina o'rganish (ML) modellari yordamida tasnifladik. NLP va turli tasniflagichlardan foydalanish tahdidlarni aniqlash aniqligini oshirib, kiberhujumlardan avtomatlashtirilgan himoyani ta'minlash samaradorligini oshiradi.*

***Kalit so'zlar.** Veb xavfsizligi, jurnal tahlili, NLP, WAF.*

***Аннотация.** В статье представлен подход к веб-безопасности на основе технологий искусственного интеллекта, использующий обработку естественного языка (NLP) для анализа логов в межсетевых экранах веб-приложений (WAF). Мы проанализировали логи серверов и классифицировали их с помощью моделей машинного обучения для выявления вредоносных шаблонов. Применение методов NLP и различных классификаторов повысило точность обнаружения угроз, обеспечивая автоматическую и проактивную защиту от кибератак.*

***Ключевые слова.** Веб-безопасность, анализ журналов, NLP, WAF.*

***Abstract.** This paper presents an AI-driven approach to web security using Natural Language Processing (NLP) for log analysis in Web Application Firewalls (WAFs). We analyzed server logs and classified them with machine learning models to detect malicious patterns. The use of NLP techniques and various classifiers improved the accuracy of threat detection, providing an automated and proactive defense against cyber-attacks.*

***Keywords.** Web security, log analysis, NLP, WAF.*

1. Introduction

In an increasingly connected world, web applications serve as the backbone of numerous services, from e-commerce and banking to social media and cloud computing. However, with this growing reliance on web applications comes an escalating threat landscape. Cybercriminals continuously evolve their tactics, making it challenging for traditional

security measures to keep up. This has led to a demand for more advanced and intelligent security solutions.

Artificial Intelligence (AI) has emerged as a key player in enhancing cybersecurity, particularly in the realm of Web Application Firewalls (WAFs). By integrating Natural Language Processing (NLP) techniques, AI can revolutionize how we analyze logs, detect potential threats, and respond to malicious activities in real-time. This article explores how NLP-based log analysis can be leveraged within AI-driven WAFs to predict and prevent cyber-attacks on web applications, ensuring a more robust defense against an ever-evolving array of threats.

2. The Role of NLP in Web Security

Natural Language Processing (NLP), a branch of AI, has significant potential in cybersecurity, especially in log analysis. While typically used in chatbots and language translation, NLP can enhance security systems by understanding the context of log entries, distinguishing between normal and suspicious activities.

For example, NLP can identify patterns like repeated failed logins or unusual data access, enabling more accurate threat detection and fewer false positives. In a scenario where an e-commerce platform sees a spike in login attempts from multiple IPs, traditional tools might flag it as suspicious. However, NLP-based AI could analyze log content to identify a coordinated brute-force attack and automatically implement defenses like CAPTCHA or IP blocks.

NLP can also detect data exfiltration attempts by analyzing unusual data access patterns, allowing AI to restrict access and prevent breaches.

3. Literature Survey

Research has extensively explored the application of machine learning and AI in web application security, particularly for firewall log analysis. Below are key studies that provide a foundation for the NLP-based approach discussed in this article.

Fatih Ertam et al.[1] classified firewall log files using various SVM kernels, with the RBF kernel achieving a 76.4% F1 score. The study did not employ preprocessing or feature engineering, indicating potential for improvement, particularly with advanced techniques like NLP-based log analysis.

Faizan Ahmad's GitHub repository presents a machine learning approach to web application firewalls, using TF-IDF vectorization on a dataset of 1,000,000 positive and 50,000 negative queries. While the

[1] F. Ertam and M. Kaya, "Classification of firewall log files with multiclass support vector machine,"2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-4,

logistic regression model claimed 99% accuracy, the absence of detailed performance metrics like the F1 score leaves room for further validation[2].

Shilpa Balan applied random forest regression to the CICDS2017 dataset for network intrusion detection, achieving an F1 score of 0.965. This study highlights the effectiveness of machine learning in network security, serving as a benchmark for AI applications in web security[3].

4. Dataset Context and Composition

In the context of AI-driven web security, particularly for the detection and prevention of malicious actions in web application firewalls, understanding the nature of the dataset is crucial. The dataset used in this study reflects a wide range of common web application security vulnerabilities, such as HTTP request injections, SQL injections, and Cross-Site Scripting (XSS) attacks, which have been extensively documented in the literature.

HTTP Request Injections: As described by Chandramouli et al.[4], HTTP request injections are a form of web application vulnerability where the content or headers of an HTTP request are dynamically generated based on user input. This creates an opportunity for attackers to inject malicious payloads into requests, leading to potential security breaches. *SQL Injections:* According to Clarke[5] and Halfond et al.[6], SQL injections involve inserting a malicious text string into input data that is then executed as part of a SQL query. This type of attack allows attackers to manipulate or retrieve data from the database in unauthorized ways. The dataset includes various types of SQL injection techniques. *XSS Attacks:* As highlighted by Fonseca et al.[7]

XSS attacks involve injecting malicious scripts into trusted websites, with the goal of compromising users who visit these sites. The dataset also captures various XSS injection techniques.

To enhance model robustness, the dataset was created by merging university firewall logs with public datasets, ensuring diverse web security threats for effective AI training.

---

[2] Faizan Ahmad, Machine Learning-Driven Web Application Firewall, *https://github.com/faizann24/Fwaf-Machine-Learning-driven-Web-Application-Firewall*

[3] Shilpa Balan A Machine Learning Approach for Network Traffic Analysis using Random Forest Regression, 2019, *https://api.semanticscholar.org/CorpusID:209372369*

[4] *Chandramouli, S. P., Bajan, P. M., Kruegel, C., Vigna, G., Zhao, Z., Doupe, A., & Ahn, G.-J. (2018). Measuring e-mail header injections on the world wide web. In* Proceedings of the 33rd Annual ACM Symposium on Applied Computing *(pp. 1647–1656). ACM.*

[5] *Clarke, J. (2009).* SQL injection attacks and defense*. Elsevier.*

[6] *Halfond, W. G., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. In* Proceedings of the IEEE International Symposium on Secure Software Engineering *(pp. 13–15). IEEE.*

[7] *Fonseca, J., Vieira, M., & Madeira, H. (2007). Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. In* 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007) *(pp. 365–372). IEEE.*

5. Methodology

In this study, we focus on using Natural Language Processing (NLP) techniques to analyze firewall logs in order to detect and classify various types of attacks, such as SQL injection and Cross-Site Scripting (XSS). The goal is to create a real-time attack detection system that can identify malicious activities at their onset and take appropriate actions to prevent further exploitation.

Dataset and Preprocessing

The dataset comprises HTTP requests and associated attack types, such as SQL injection and XSS, as well as normal traffic. Each log entry contains details about the request, such as HTTP headers and parameters. We utilized the Term Frequency-Inverse Document Frequency (TF-IDF) vectorizer to convert the textual HTTP requests into numerical features that could be used for training machine learning models.

Model Training

A Support Vector Classifier (SVC) with a linear kernel was selected for the classification task. The dataset was split into training and testing sets, with 70% of the data used for training and the remaining 30% for testing. The model was trained to classify the HTTP requests into categories like "SQL Injection," "XSS," and "Normal Traffic."

6. Results

The model's performance across five datasets—command injection, path traversal, SQL injection, valid (non-attack traffic), and cross-site scripting (xss) is summarized in Table 1.

Table 1: Model Performance Metrics

Dataset	**Precision**	**Recall**	**F1-score**
Command Injection	0.97	0.98	0.97
Path Traversal	0.99	0.98	0.98
SQL Injection	1.0	0.99	1.0
Valid	1.0	1.0	1.0
Cross-Site Scripting	1.0	1.0	1.0

The model consistently performed well across all datasets, achieving near-perfect precision, recall, and F1-scores, especially for SQL injection, valid traffic, and cross-site scripting.

КРИПТО АКТИВЛАР ТУШУНЧАСИ, МАЗМУН-МОҲИЯТИ ВА ЎЗИГА ХОС ХУСУСИЯТЛАРИ

Атаниязов Жасурбек Курбанбаевич
Ўзбекистон Республикаси Жамоат хавфсизлиги университети, "Жиноий-ҳуқуқий фанлар" кафедраси доценти, ю.ф.б.ф.д.(PhD)
телефон: +998972249998
jasurbekataniyazov91@gmail.com
ORCID: 0000-0003-39-53-3800

Азизхонов Шоҳруҳ Мадилханович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети мустақил изланувчиси
телефон: +998915019119
azizkhanovshokhruh@gkuul.com
ORCID: 0009-0009-3488-8697

Аннотация: *Ушбу мақолада крипто-активларнинг ривожланиш тарихи, крипто-активларнинг турлари ва уларнинг ўзига хос хусусиятлари, дунё ҳамжамияти ва молиявий бозорга таъсири, Ўзбекистон Республикасида крипто-активлар айланмаси соҳасининг тартибга солиниши ҳамда крипто-активлар айланмасида хорижий давлатлар тажрибаси тадқиқ этилган. Тадқиқотда анализ, синтез, индукция, дедукция, қиёсий-ҳуқуқий таҳлил каби методлар қўлланилган.*

Калит сўзлар: *Крипто-активлар, "IOU" (Мен Сизга қарздорман), Сатоши Накамото, Bitcoin, Ethereum, Altcoin, Lightcoin, Stabilkoin, Токен, хусусий криптовалюталар.*

Аннотация: *В данной статье история развития крипто-активов, виды крипто-активов и их характеристики, влияние на мировое сообщество и финансовый рынок, регулирование сферы обращения крипто-активов в Республике Узбекистан. и изучен опыт зарубежных стран в обращении крипто-активов. В исследовании использованы такие методы, как анализ, синтез, индукция, дедукция, сравнительно-правовой анализ.*

Ключевые слова: *Крипто-активы, долговые расписки (IOU), Сатоши Накамото, Bitcoin, Ethereum, Altcoin, Lightcoin, Stabilkoin, Токен, Частные криптовалюты.*

Abstract: *This article describes the history of crypto-assets development, types of crypto-assets and their characteristics, impact on the global community and financial market, regulation of the sphere of crypto-assets circulation in the Republic of Uzbekistan. and studies the experience of foreign countries in the circulation of crypto-assets. The study uses methods such as analysis, synthesis, induction, deduction, comparative legal analysis.*

Keywords: *Crypto assets, IOUs, Satoshi Nakamoto, Bitcoin, Ethereum, Altcoin, Lightcoin, Stabilkoin, Token, Private cryptocurrencies*

Бугунги кунга келиб ҳеч кимга сир эмаски, дунё ҳамжамиятида замонавий рақамли технологияларнинг ривожланиши инсонларнинг ўз мақсадлари ва эҳтиёжларига эришишда энг самарали воситага айланиб улгурди.

Тарихга назар солсак, пул – йил ўтиши билан жисмоний ишлаб чиқарилган тангалардан рақамли кўринишга ўз шаклини ўзгартириб келган. милоддан аввалги X минг йилликда гўшт, туз, дон каби маҳсулотлар савдоси товар айирбошлаш кўринишида бўлган бўлса, II минг йиллик атрофида қимматбаҳо металларни пул ўрнида ишлатиш бошланган. Метал буюмлар орасида олтин 3500 йилдан ортиқ вақт давомида, пул муносабатларида ўз мавқеини сақлаб турган. Кейинчалик фирибгарлар томонидан бошқа арзон металларни олтинга аралаштириши натижасида таннарҳининг пасайиши кузатилган. Шу тариқа олтин билан қийматланадиган қоғоз пуллар пайдо бўлишига эҳтиёж пайдо бўлган.

XVI асрга келиб, олтиннинг қиймати тушиши натижасида, оддий одамлар томонидан олтин тангаларнинг ҳақиқий эканлигини ажратиш мураккаблашган. Шу даврга келиб, инсонлар ўзларидаги олтин ва кумушларни банкларга бериб, ўрнига ундан “Мен Сизга қарздорман” (IOU) [1] деб номланган ҳужжат олган. Шу тариқа пулнинг дастлабки қоғоз кўринишлари пайдо бўлган. Бу қоғоз пуллар қиймати унинг банкда бўлган олтинлари билан қийматланган (олтин стандарти). 1950 йилга келиб, дунёнинг аксарият давлатлари “олтин стандарти”дан воз кечиб, пулни олтиндан ажратган. АҚШ пул сиёсатида бу жараён 1971 йилда содир бўлган.

XX аср ўрталарига қадар пул олтин билан қийматланди [2] ва давлатлар томонидан “олтин стандарти”дан воз кечиб, пул муомаласи ва унинг миқдорини назорат қилишга ҳаракатлар бошланди. Марказий банклар томонидан пулни ишлаб чиқаришни ошириш ва камайтириш мустақил белгиланишга ўтиши натижада “пул инфляцияси” ва “пул дефляцияси” каби тушунчалар пайдо бўлиши билан бирга пул тизимида аста-секин марказлаштириш амалга оширила бошланди.

Вақт ўтиши билан, қоғоз пул муомалага чиқарилиши натижасида, пулни компьютер ёрдамида нусхалаш ва кўпайтириш билан боғлиқ жиноятлар авж ола бошлади. Жиноятларни олдини олиш учун давлатлар пулни марказлашган ҳолда электрон ҳисобини

юритишга ўта бошлади ва электрон пулнинг дастлабки шакли пайдо бўлди.

Бунда, бутун дунёда марказий банклар маҳаллий банклар билан биргаликда ҳисоб рақамлардаги пулларни бошқариш бошланди, яъни:

- банкдаги ҳисоб рақамларга кириш мумкин бўлган вақт *(душанба – жума, соат 09:00-17:00 гача)*;
- пулни нақдлаштириш ва ўтказмалар учун комиссия тўлови;
- пул ечиб олиш чегараси;
- ҳисоб рақами фойдаланувчиларини чегаралаш;
- ҳисоб рақамдаги пуллар ҳаракатини чеклаш;
- муомалага чиқарилган пуллар миқдори.

Пул тизимининг марказлаштирилиши, электрон пул пайдо бўлиши натижасида, эндиликда инсонларни пулдан фойдаланишини назорат қилиш бошланди.

Кўпчиликда савол туғила бошлади. Яъни, ҳеч қандай жисмоний элементларсиз, марказлашмаган, барча афзалликларга эга рақамли пул,

- ундан фойдаланишни хоҳловчилар учун тўлиқ очиқ бўлиши;
- ҳеч қандай чегара (ҳудуд) ёки транзакция назорати йўқлиги;
- 24/7 режимида ишлайдиган;
- ҳамма учун аниқ ишлаб чиқилган қоидаларга амал қилиниши;
- давлатлар томонидан бошқарилмайдиган, тизим орқали фойдаланиш;
- пулни ўғирлаш жуда қийин ва пул сақланадиган марказий орган йўқ бўлган тизимни яратиш бўйича ҳаракатлар бошланди.

Натижада, 2008 йилда Сатоши Накамото томонидан “Bitcoin: A Peer-to-Peer Electronic Cash System” номли лойиҳа нашр этилди [3].

Шундан сўнг, электрон пул тизимида ҳисоб рақамлар ўртасида пул ўтказиш йўлга қўйилди. Учинчи томондан ўтказмаларни тасдиқлаши кераклиги, ҳисоб-китобларни бекор қилиш каби имкониятлар натижасида, пулни қайтариб олиш ёки бир вақтда иккита ҳисобга ўтказиш, яъни пулни икки марта сарфлаш билан боғлиқ фирибгарлик ҳолатлари ҳам пайдо бўлаш бошлади.

Ушбу муаммони хал этиш учун Сатоши томонидан тақдим этилган лойиҳада “рақамли имзолар занжири” тизими асосида ҳар икки томон ҳам транзакцияни мустақил тасдиқлашлари учун марказий банклар томонидан назорат қилинмайдиган блокчейн технологияси назарда тутилган эди.

Криптовалюта - бу фақат Интернетда мавжуд бўлган рақамли ёки виртуал шаклдаги электрон валютадир. Бу тизимда транзакциялар банклар аралашувисиз блокчейн тизими асосида амалга оширилади. Блокчейн тизими рақамли пулларни воситачисиз бир бирига ўтказиш учун хизмат қилади.

Транзакцияларни қайд этиш ва янги бирликларни ишлаб чиқаришда марказлашмаган тизим хизмат кўрсатади.

Криптовалюта савдо операцияларни амалга оширишда хавфсизликнинг юқорилиги, тизимнинг криптографияга асосида қурилганлиги сабаблидир. Бунда ҳар бир маълумот шифрланган ҳолда махфий узатилади.

Крипто-активлар тарихига назар солсак, “Биткоин” криптовалютаси пайдо бўлишидан анча олдин бошланган, яъни 1980 ва 1990-йилларда “Диги Саш” ва “Ҳашсаш” каби рақамли пулларни яратишга уринишлар кўп бўлди. Ушбу лойиҳалар келажакдаги криптовалюталар учун асос яратди, аммо ишонч, хавфсизлик ва тартибга солиш билан боғлиқ муаммолар туфайли муваффақиятли бўлмади. Крипто-активлар тарихидаги асосий момент Биткоиннинг пайдо бўлиши эди. 2008 йилда кимлиги номаълум бўлиб қолаётган Сатоши Накамото марказлаштирилмаган рақамли валютанинг ишлаш принципини тавсифловчи оқ қоғозни нашр этди. 2009 йил январ ойида биринчи блокчейн тармоғи яратилди ва Сатоши “генезис блоки” деб номланувчи биринчи Биткоин блокини яратди. Биткоин икки марта сарфлаш муаммосига ноёб ечим таклиф қилди ва криптовалюта концепциясининг биринчи муваффақиятли амалга оширилиши бўлди.

“Биткоин” - бу ҳеч қандай моддий қийматга эга бўлмаган, майнинг қурилмалар ёрдамида ишлаб чиқарилувчи, алгоритм ёзувлари жамланмасидан иборат виртуал пул ҳисобланади.

Биткоин мавжудлигининг биринчи йиллари ишқибозлар ва ишлаб чиқувчиларнинг кичик доираси орасида ўтди. 2010 йилда реал иқтисодиётда Биткоиндан фойдаланган ҳолда биринчи транзакция амалга оширилди, яъни 10 000 БТСга пица сотиб олинди, бу кейинчалик афсонавий воқеага айланади. Аста-секин криптовалюталарни сотиш ва айирбошлаш учун инфратузилмани шакллантириш бошланди. 2011 йилда “Mt. Gox” каби биринчи биржалар яратилди.

Бугунги кунга келиб, биткоиндан ташқари мавжуд криптовалюталар – “алткоин” ёки “алт” атамаси билан номланади.

Алткоин *(англ. Altcoins)* барча криптовалюталарнинг умумий номини англатади *(фақат биткоиндан ташқари)*.

Дастлабки алткоин 2011 йилда яратилган бўлиб, ҳозирги кунда алткоинлар дунё бўйича 1000 дан зиёдни ташкил этади.

“Coinmarketcap.com” [4] портали бугунги кунда 9 878 алткоинларни ўз ичига олиб, уларнинг савдодаги кўрсаткичларини эълон қилиб боради.

Алткоинларга қуйидагиларни келтиришимиз мумкин:

“Ethereum” криптовалютаси. “Эфир” капитализация бўйича биткоиндан кейинги 2-ўринда туради. Ethereum 2015 йилда “ақлли шартнома”лар тузиш учун платформа сифатида ишлаб чиқарилган.

“Bitcoin Cash” криптовалютаси. 2017 йил 1 августда чиқарилган. Биткоиндан фарқли томони унда 8 мб блок мавжуд.

“Lightcoin” криптовалютаси. 2011 йилда ишлаб чиқарилган энг биринчи алткоин. Биткоиндан деярли фарқ қилмайди. Бунда асосан блок занжирларда операциялар тезроқ амалга оширилади.

“Monero” криптовалютаси. Бу “DarkNet”даги энг машҳур тўлов воситаси ҳисобланади. Шунинг учун у жиноятларда ва жиноий даромадларни легаллаштиришда кўпроқ фойдаланилади.

“Dash” криптовалютаси. Анонимликка қаратилган бошқа яна бир алткоин. 2014 йил январь ойидан бошлаб, муомалада ишлатилиб келинади.

“Ripple” криптовалютаси. Пул алмашинуви билан боғлиқ транзакцияларга қаратилган тўлов тизими платформаси. 2012 йилда “Ripple” компанияси томонидан ишлаб чиқилган бўлиб, кўпроқ банк соҳасида машҳурдир.

21 асрнинг энг кўп муҳокама қилинадиган ва молиявий воситаларига айланган крипто-активларнинг асосий турлари ва кўринишлари қуйидагилардан иборат.

- “Bitcoin” ва “altkoin” – булар биринчи криптовалюталар. 2009 йилда яратилган бўлиб, Bitcoin ҳозирда энг машҳури ҳисобланади. Алткоинлар эса, биткоин бўлмаган бошқа барча криптовалюталар ҳисобланади. Масалан, Ethereum, Ripple, Litecoin;

- “Stabilkoin” – бу криптовалюта нархини барқарорлаштириш учун “фиат пуллар” (АҚШ доллари, евро) ёки бошқа активларга боғланган кўринишидир. Масалан, Tether (USDT), USD Coin (USDC), TrueUSD (TUSD);

- Хусусий криптовалюталар. Буларга Monero (XMR) ва Zcash (ZEC) мисол бўла олади. Бу турларда транзакция маълумотлари яшириш бўлиб, унинг эгалари учун махфийликни таъминлайди;

- Платформа токени – бу марказлашмаган иловалар ва ақлли шартномаларни ишлаб чиқиш учун платформаларда яратилган токенлар. Мисол учун Ethereum токени, у ўз тармоғидаги тўловларни тўлаш ва ақлли шартномаларни амалга ошириш учун керак;

- Utility tokens – ушбу токенлар платформалар ёки лойиҳалар ичида муайян хизматлар ёки хусусиятларга кириш учун фойдаланилади. Мисол учун, Binance Coin (BNB) “Binance” биржасидаги тўловлар учун керак.

Вақтлар ўтиши билан крипто-активларининг асосий муаммоси назоратсизлик ва ўзгарувчанлик бўлиб қолди ва “стабилкоин”лар яратилиши билан курснинг тез ўзгариши билан муаммони ҳал бўлди.

Одатда, стабилкоинлар курси валюта ёки олтин қийматига қиёсланади.

Шахсий даромадини хавфсиз сақлаш ёки кўпайтиришни хоҳлаганларнинг кўпчилиги пулларини стабилкоинга айлантиришмоқда.

Бугунги кунда стабилкоинлар яна қуйидаги мақсадларда ишлатилади:

- кундалик валюта операциялари учун;
- комиссиясиз халқаро пул ўтказмаларида;
- миллий валютани инфлациядан ҳимоялаш;
- крипто актив биржасида биткоиннинг ролини камайтириш;
- такрорий ўтказмаларни оптималлаштириш.

Ҳозирда энг машҳур стабилкоинлар курси – АҚШ доллари қийматига боғланган бўлиб, уларнинг энг ишончлиси USDTдир.

Стабилкоинларни кўпайтиришдан асосий мақсад, уларни марказлаштириш ҳисобланади. Энг машҳур ва барқарор стабилкоинлар: USDT, USDC, BUSD, DAI, FRAX, TUSD, USDP, USDN, USDD ва FEI [5].

Ўз навбатида, крипто-активлардан фойдаланишда бир қанча қулайликлар ҳам мавжуд. Булар,

- марказлашмаганлиги – яъни, блокчейн технологиясига асосланган бўлиб, назорат қилувчи ёки тартибга солувчи марказий ҳокимиятнинг йўқлиги, фойдаланувчиларга эркинлик ва мустақилликни таъминлайди;

- шаффофлиги – криптовалюталар ёрдамида амалга оширилган барча операциялар одатда барча фойдаланувчилар

кўриши мумкин бўлган оммавий тақсимланган дафтарда қайд этилади ва бу фирибгарлик хавфини камайтиради;

- тўловлар камлиги – анъанавий молиявий тизимлар (банк ва тўлов ташкилотлари иловалари) билан солиштирганда, воситачилик ҳақи йўқ бўлиб, юборувчи ва қабул қилувчи ўртасида ўтказмалар учун ҳақ олинмайди;

- ўтказмаларнинг тезлиги – криптовалюта операциялари одатда анъанавий банк операцияларига қараганда сезиларли даражада тезроқ қайта ишланади, айниқса халқаро ўтказмалар учун;

- глобал кириш – крипто-биржалардан дунёнинг исталган жойидан интернетга уланган ҳолда фойдаланиш мумкин;

- инвестицион имконият – баъзи криптовалюталар инвесторларга юқори даражадаги ўзгарувчанлик ва потенциал юқори даромадни таклиф этади.

Шу билан бир қаторда, крипто-активлардан фойдаланишдаги айрим камчиликлар ҳам мавжуд. Хусусан,

- юқори ўзгарувчанлиги – криптовалюта нархлари қисқа вақт ичида кескин ўзгариши, яъни юқорига кўтарилиши ёки тушиб кетиши мумкин;

- тартибга солинмаганлиги – криптовалюталар оддий пуллар каби қатъий тартибга солинмаганлиги сабабли, кўпинча фирибгарлик ҳолатларида фойдаланувчилар учун ҳимоя таъминланмайди;

- техник заифликлар – блокчейн технологияси юқори даражадаги хавфсизликни таъминлаши билан бир қаторда, криптовалюта платформалари киберҳужумларга техник томонлама мойил бўлиши мумкин, бу эса маълумотларнинг сизиб чиқиши ва маблағларни ўғирланишига олиб келади;

- легаллаштиришдаги муаммолар – айрим давлатларда крипто-активлар муомаласи қонун билан тақиқланиши ёки чекланиши мумкин, бу эса криптовалюта эгалари ва ихтисослашган компаниялар учун ҳуқуқий хавф туғдиради;

- йўқотиш хавфи – агар хатога йўл қўйиб, бошқа ҳисобга ўтказилган “коин”ларни қайтариш эҳтимоли жуда ҳам паст ҳисобланади.

Дунё тажрибасини ўрганган ҳолда ҳозирга келиб крипто-актиклар билан боғлиқ муносабатларга турлича ёндашувлар мавжуд бўлиб, баъзи давлатларда бутунлай тақиқланган, айримларида эса лицензиялаш орқали тартибга солинган. Лекин, бир нечта мамлакатлар томонидан тўлиқ қонунийлаштириб,

ҳаттоки улардан расмий пул айирбошлаш воситаси сифатида фойдаланилади. Масалан,

- Хитойда бу бўйича қатъий чора-тадбирлар белгиланган бўлиб, крипто-биржалар фаолияти қонун билан тақиқланган бўлиб, 10 йилдан ортиқ озодликдан маҳрум қилиш жазоси белгиланган;

- Ҳиндистонда ҳам ушбу фаолият тури тақиқланган, лекин расмий ҳужжат мавжуд эмас. Ҳозирда тақиқловчи қонун ишлаб чиқилмоқда;

- Бангладешда 2021 йил 11 май куни крипто-актив фаолиятини тақиқловчи қонун қабул қилинган ва ушбу қонун амал қилиши жиҳатидан энг қаттиқ қонун ҳисобланади;

- Россия Федерациясида крипто-активлар муомаласи бутунлай тақиқланмаган бўлиб, лицензиялаш орқали тартибга солинган;

- АҚШда крипто-активлар фаолияти билан шуғулланиш тартибга солинган бўлиб, бу кўплаб йирик компаниялар ва инвесторларни крипто-биржа соҳасида фаол иштирокини таъминлайди;

- Салвадор дунёда биринчи бўлиб, “bitcoin”ни расман тўлов воситаси сифатида тан олган давлат ҳисобланади. Бу Салвадор учун меҳнат мигрантларининг хориждан пул ўтказишдаги комиссион харажатлар учун йилига 400 млн. доллар тежашга олиб келади.

- Ўзбекистонда ҳам ушбу фаолият қонун билан тартибга солинган бўлиб, крипто-активлар айланмаси соҳасида лицензиялаш ва рухсат бериш тартиби белгиланган.

Республикамизда, крипто-активлар фаолиятининг тартибга солинишига назар солсак, Ўзбекистон Республикасининг 2023 йил 6 сентябрдаги ЎРҚ-866-сонли Қонунига [6] мувофиқ, крипто-активлар айланмаси соҳасидаги фаолият (майнинг ва крипто-активлар айланмаси соҳасидаги хизматлар провайдерлари) турлари Истиқболли лойиҳалар миллий агентлиги томонидан лицензиялаш ва рухсат бериш тартиб-таомиллари асосида амалга оширилиши белгиланган.

Яъни, хизматлар провайдерлари турлари сифатида,

- крипто-биржа;

- майнинг-пул;

- крипто-депозитарий;

- крипто-дўконлар фаолияти учун лицензия ҳамда майнинг фаолиятини амалга ошириш учун рухсатнома олиш кераклиги айтилган.

Ушбу қонунга кўра, юқоридаги фаолият турлари билан шуғулланиш учун лицензия ёки рухсатнома олиш фақат юридик шахслар учун бўлиб, жисмоний шахс сифатида ҳар иккала фаолият тури билан шуғулланиш тақиқланган.

Ўзбекистон Республикасининг 2024 йил 19 январдаги ЎРҚ-899-сонли Қонунига [7] мувофиқ, Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодекси 155^4 ва 155^5 ҳамда Жиноят кодекси 278^8 ва 278^9-моддалари билан тўлдирилган бўлиб, бунинг учун маъмурий ва жиноий жавобгарлик белгиланган.

Хулоса ўрнида шуни айтиш мумкинки, бугунги кунга келиб крипто-активлар замонавий жамиятда тобора муҳим рол ўйнаб, молия, технология ва ҳуқуқий жиҳатларга ёндашувларни ўзгартирмоқда. Уларнинг асосий вазифаси воситачиларсиз тез ва хавфсиз транзакцияларни амалга ошириш имконини берувчи анъанавий валюталар ва молиявий воситаларга марказлашмаган муқобиллигини сақлаб қолмоқда.

Бундан ташқари, крипто-активлар блокчейн технологиясидан фойдаланган ҳолда логистика ва соғлиқни сақлаш каби турли соҳаларда шаффофлик ва бухгалтерия ҳисобини яхшилаш учун ишлатилиши мумкин. Шу билан бирга, улар ноқонуний операцияларда қўлланилиши ва уларнинг юқори ўзгарувчанлиги сабабли хавотирларни келтириб чиқаради, бу эса давлат ва инвесторлар учун қийинчиликлар туғдиради.

Шундай қилиб, крипто-активлар рақамли иқтисодиётнинг муҳим элементига айланиб, глобал миқёсда пул ва активлар билан ўзаро алоқада янги ёндашувларни шакллантирмоқда.

TERAN O’RGANISHGA ASOSLANGAN TARMOQ HUJUMLARINI ANIQLASH USULLARI

G‘ulomov Sherzod Radjaboyevich
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik” fakulteti dekani, dotsent, tel:+998909708464

Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi assistenti, tel:+998997481489

Annotatsiya: *Teran o’rganish asl tuzilmalari va domenga yo’naltirilgan ilovalar murakkab bo’lganligi sababli, ushbu maqola teran o’rganish usullaridan foydalangan*

holda tarmoq xavfsizligini o'rganishni maqsad qilganlar uchun soda qilib yozilgan. Asosan, teran o'rganish usullaridan foydalangan holda hujumlarni aniqlashga qaratilgan ko'plab ishlar mavjud.

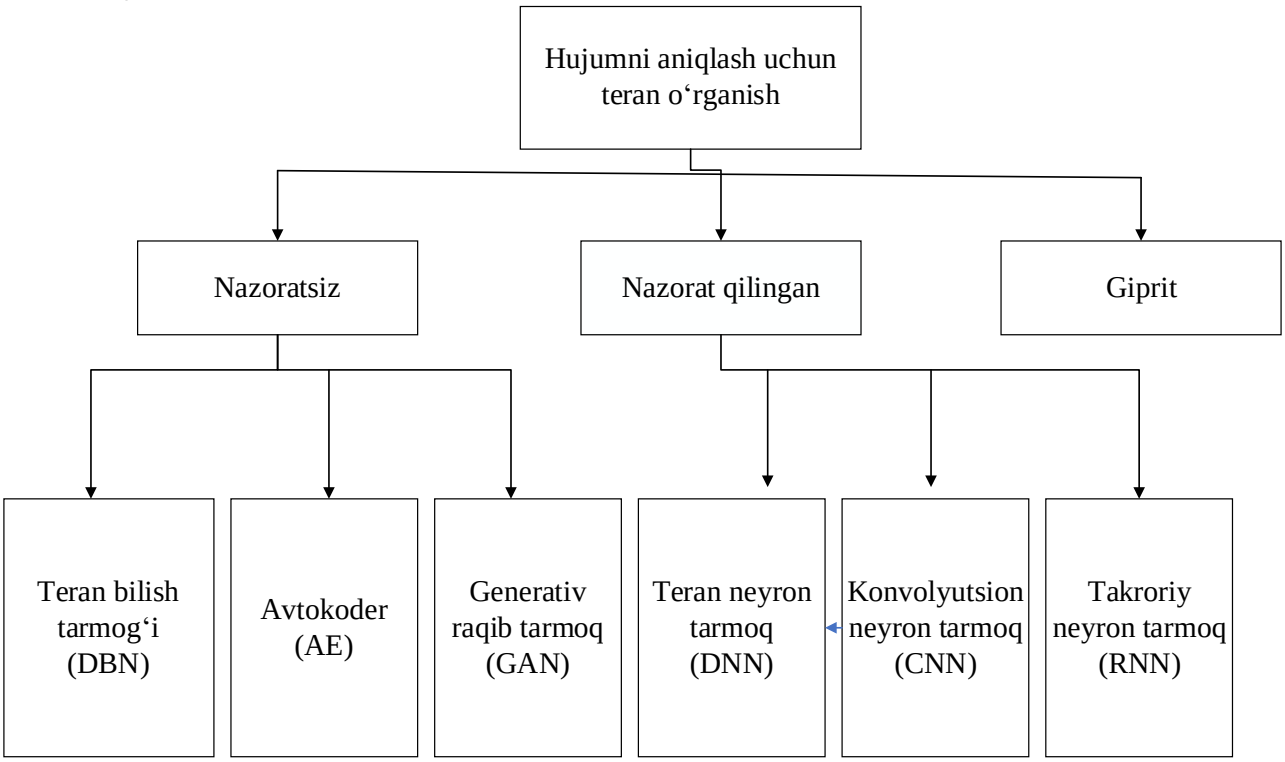
Kalit so'zlar: *Hujumni aniqlash, zararli dasturlar, domen yaratish algoritimlari, kiberxavfsizlik, tarmoq xavfsizligi, kompyuterlar, tarmoqlar, dasturlar, turli ma'lumotlar.*

Abstract: *Since deep learning is complex in its original structure and domain-specific applications, this article is written to explain it to those who intend to study network security using deep learning techniques. Basically, there is a lot of work on detecting attacks using deep learning techniques.*

Аннотация: *Поскольку глубокое обучение является сложным по своей исходной структуре и приложениям, специфичным для предметной области, эта статья написана для того, чтобы объяснить его тем, кто собирается изучать сетевую безопасность с использованием методов глубокого обучения. По сути, ведется большая работа по обнаружению атак с использованием методов глубокого обучения.*

Internetning uzluksiz rivojlanishi, tarmoq foydalanuvchilariga ko'p jihatdan foyda keltirmoqda. Ular batafsil xususiyatlari haqida oldindan ma'lumotga ega bo'lmagan hujumlar makoni hisoblanadi. Biroq, an'anaviy mashinali o'rganish usullari modelning murakkabligidagi cheklovlar tufayli hujumni aniqlash muammosini tavsiflash uchun o'ziga xos xususiyat deskriptorlarini taqdim eta olmaydi. Yaqinda mashinali o'rganish murakkab muammolarni hal qilish uchun teran o'rganish usullari deb ataladigan neyron tarmoqlarning tuzilishi bilan inson miyasini taqlid qilish orqali katta yutuqga ega bo'lishdi. Ushbu muvaffaqiyatli ilovalar orasida Google AlphaGo "go" o'yini uchun eng ajoyib sinovlardan biri bo'lib, Teran o'rganishning tipik turi, ya'ni konvolyutsion neyron tarmoqlari kuchini o'z ichiga oladi. Shu bilan birga, tarmoqdan keng foydalanish bilan tarmoq xavfsizligi yanada muhimroq hisoblanadi. Tarmoq xavfsizligi kompyuterlar, tarmoqlar, dasturlar, turli ma'lumotlar va boshqalar bilan chambarchas bog'liq bo'lib, bu yerda himoyaning maqsadi ruxsatsiz kirish va o'zgartirishlarning oldini olishdir [1]. Biroq, moliya, elektron tijorat va harbiy sohalarda internetga ulangan tizimlar sonining ortib borishi ularni tarmoq hujumlari nishoniga aylantiradi, bu esa katta miqdordagi xavf va zararga olib keladi. Asosan, hujumlarni aniqlash, himoya qilish va tarmoq xavfsizligini ta'minlash uchun samarali strategiyalarni taqdim etish kerak. Bundan tashqari, har xil turdagi hujumlar odatda turli yo'llar bilan qayta ishlanishi kerak. Har xil turdagi tarmoq hujumlarini qanday aniqlash, tarmoq xavfsizligi sohasida hal qilinishi kerak bo'lgan asosiy muammoga aylanadi, ayniqsa, ilgari hech qachon ko'rilmagan hujumlar bularga misol bo'la oladi.

Hujumni aniqlash. Bosqinlarni aniqlash tizimi tarmoqdagi xatti-harakatlar, xavfsizlik jurnali va tarmoqda va ulangan kompyuterlar orasida mavjud bo'lgan boshqa ma'lumotlarni to'plash va tahlil qilish orqali zararli faoliyatni aniqlay oladi [16]. Biz Teran o'rganish usulining amaliyligini taqdim etish uchun ba'zi tipik ilovalarni taqdim etamiz, bu yerda biz ushbu ilovalarni multimediya bilan ishlash [13], signalni qayta ishlash [14] va hokazo [15] domenlarida amalga oshirish mumkin deb hisoblaymiz.



1-rasm. Hujumni aniqlash uchun mavjud Teran o'rganish usullarining toifalari

Asosan, tajovuzni aniqlash tizimi, tizim xavfsizlik siyosatiga qarshi g'ayritabiy xatti-harakatlarning mavjudligini va tizimdagi hujum belgilarini tekshiradi, bu tizimni real vaqtda javoblar bilan himoya qilishga qodir. An'anaviy tizim sozlamalarida hujumni aniqlash tizimi xavfsizlik devoriga oqilona, faol va samarali qo'shimcha sifatida ishlaydi, bu aslida hujumlardan passiv himoya vositasi sifatida ishlashini anglatadi.

An'anaviy tajovuzni aniqlash tizimi birinchi navbatda tajovuzni aniqlash texnologiyasidan noto'g'ri foydalanishga asoslangan bo'lib, u asosan tajovuzkor xatti-harakatlarning xususiyatlarini yoki qoidalarini chiqaradi. Mashinali o'rganishning an'anaviy modellari bilan g'ayritabiy xatti-harakatlarni aniqlash texnologiyasi paydo bo'lgandan so'ng, tajovuzni aniqlash tizimi odatdagi xatti-harakatlar uchun ehtimollik statistik modellashtirishni amalga oshirish uchun rivojlanadi, bu esa katta

og‘ishlar bilan normal xatti-harakatlarni tahlil qilishi va ogohlantirishi mumkin.

Biroq, bunday tizim muammoli maydonni aniqlash qobiliyatining pastligi va zararli faoliyatni modellashtirishning murakkabligi tufayli qoniqarsiz natijalarga olib kelishi mumkin.

Tegishli hisoblash funksiyasi matnini chiqarish texnologiyasini olish uchun PE metadata xususiyatlaridan foydalanish mumkin.

Biz zararli dasturlarni aniqlash usullarini ikkita toifaga ajratamiz:

- imzoga asoslangan
- anomaliyaga asoslangan

An’anaviy antivirus dasturlari birinchi toifaga kiritilishi mumkin. Bu fayl imzosi asosida zararli fayllarni aniqlaydi. Biroq, biroz deformatsiyalangan zararli kodlarni chetlab o’tish mumkin, bu esa ko’p sonli noto’g‘ri pozitivlarga olib keladi. Keyinchalik, “sandbox” va “virtual mashina” texnologiyalari virusning dinamik harakatlarini aniqlay oladi, bu esa noma’lum zararli kodni aniqlash qobiliyatini sezilarli darajada yaxshilagan holda statik aniqlashdan dinamik tahlilga qadar katta muvaffaqiyat deb hisoblanishi mumkin.

Xavfsizlik va aloqa tarmoqlari mashinali o’rganishning an’anaviy usullari bilan yuzaga kelgan kamchiliklarni yanada bartaraf etish uchun tarmoq paketlarini tahlil qilish uchun Teran o’rganish texnologiyasi amalga oshiriladi, bu esa kirishni aniqlashning asosiy g‘oyasini qora ro’yxatdan oq modelga o’zgartiradi.

Anomaliya hujumlarini aniqlash tizimi uchun integratsiya usuli bilan tizim chaqiruvini modellashtirish yondashuvini loyihalash mumkin. Tizim qo’ng‘iroqlarini modellashtirish tarmoqdagi har bir qo’ng‘iroq va munosabatlarning semantikasini olishga yordam beradi.

Zararli dasturlarni aniqlash. Zararli dastur kompyuter, server yoki kompyuter tarmog‘ining ishlashi va zaifligini kamaytirish uchun mo’ljallangan. Haddan tashqari holatlarda zararli dastur butun tizimni yo’q qilishga olib keladi. Zararli dastur dastlab maqsadli kompyuterga joylashtirilishi kerak. Keyinchalik, u kod, skript, faol tarkib va boshqa dasturlarni avtomatik ravishda bajarishi mumkin. Ta’kidlanishicha, bunday dasturiy ta’minot yoki kodlar kompyuter viruslari, qurtlar, troyanlar, josuslik dasturlari, reklamalar, reklama dasturlari va zararli kodlar ko’rinishida tasniflanishi mumkin. Hujumni aniqlashning hozirgi Teran o’rganish usullarini hisobga olgan holda toifalarga bo’lishdan so’ng, biz ularni taxminan uchta toifaga ajratamiz:

- nazoratsiz (masalan, avtokoder (AE),
- Teran bilish tarmog‘i (DBN)

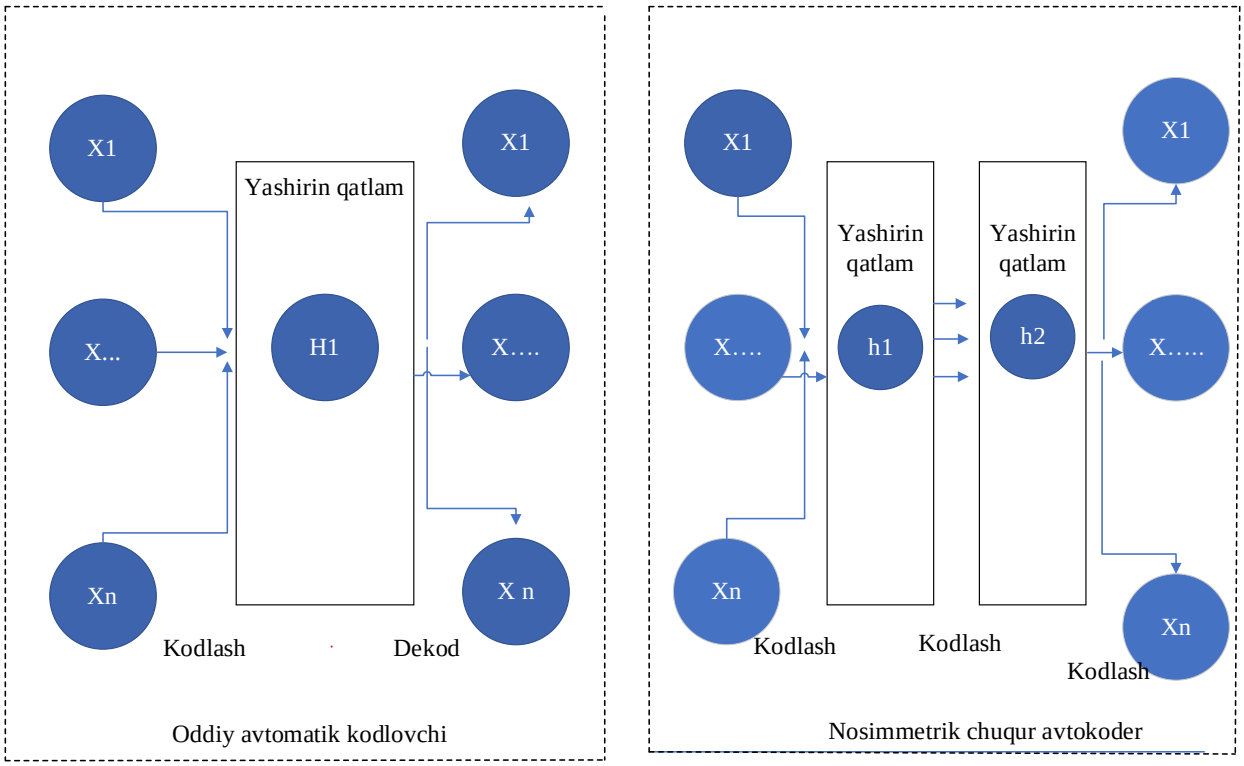
- generativ raqib tarmog‘i (GAN)),

Hujumni aniqlash uchun Teran o’rganish usullari. Turli kiberxavfsizlik ilovalari uchun AE tuzilmasi bilan xususiyatlarni namoyish qilishni o’rganishni taklif qiladi, bu ikki o’quv bosqichidan, ya’ni oldindan tayyorlash va nozik sozlashdan iborat.

Oldingi bosqich- nozik sozlash bosqichi uchun tegishli boshlang‘ich nuqtani izlash uchun mo’ljallangan. Tayyorgarlik bosqichida parametrlarni aniqlagandan so’ng, nozik sozlash bosqichi kiritilgan ma’lumotlar uchun xususiyat tavsifini taklif qiladi.

Taklif qilingan xususiyatlarni o’rganish sxemasi xususiyat o’lchamlarini sezilarli darajada kamaytirishi mumkin, shuning uchun saqlash talablarini sezilarli darajada kamaytiradi.

Ularning taklif qilingan usuli variantli hujumlarning tabiatini tushunish orqali yaxshi ishlashi mumkinligiga ishoniladi, bunda ular o’zlarining usullari yangi vaziyatlarda o’quv majmuasini qo’lda yangilamasdan, kurashish mumkinligini ko’rsatish uchun tajribalar ishlab chiqishadi. “Intrusion” hujumlarini aniqlash vaqtida moslashuvchan tizimni yaratish uchun Javaid qurish sababli siyrak AE va softmaxregressiya qatlamidan va o’quv jarayonida o’z-o’zini o’rgatish (STL) dan foydalaniladi. Xususan, ular taklif qilgan STL ikki bosqichga bo’linishi mumkin, bunda siyrak AE birinchi navbatda nazoratsiz xususiyatlarni o’rganish uchun ishlatiladi va softmax-regressiya xususiyatni ajratib olgandan keyin tasniflash uchun ishlatiladi. Aslida, STL-dan foydalanish noma’lum hujumlarga duch keladigan qurilgan tarmoqning o’rganish qobiliyatini sezilarli darajada yaxshilashi mumkin, bu yerda yangi toifadagi hujumlar noldan mashq qilish, muammosiz ish vaqtida asta-sekin tahlil qilinishi mumkin. AE ni sayoz o’rganish bilan birlashtirib, tahlil qilish uchun hisoblash xarajatlarini muvaffaqiyatli kamaytiradi.



2-rasm. Shone va boshqalarning tarmoq tuzilishi. [17], bu nosimmetrik bir nechta yashirin qatlamlar bilan yaratilgan AE ning yangi tuzilishi.

Xususan, NDAE odatdagi AE bilan solishtirganda qo'shimcha kodlash bosqichiga ega, bu murakkablikni kamaytirishi va modelning aniqligini oshirishi mumkin. Bunday tuzilma 2-rasmda keltirilgan. Bu yerda biz uning ierarxik xususiyati ekstraktorini kuzatishimiz mumkin. Taklif etilgan NDAE oxirida ular NDAElardan o'rganilgan xususiyatlarni namoyish qilish yordamida g'ayritabiy vaziyatlarni tanib olish uchun tasodifiy o'rmon tuzilishini qo'llaydilar. O'zlarining modellarini baholash uchun mualliflar o'zlarining kodlarini GPU-ga kiritdilar va KDDCup 99 va NSL-KDD bilan baholanib, boshqalar bilan solishtirganda istiqbolli natijalarga erishdilar.

Xulosa

Machine Translated by Google Xitoy Grant 2018YFC0407901, Asosiy ko'pchilik tomonidan tasdiqlangan yaxshi ishlashni ta'minlaydi hujumni aniqlash uchun tasniflagichlar hisoblanadi. Ushbu ma'lumotlarga kirish uchun so'rovlar bo'lishi kerak tasvir va naqshni aniqlashda biz, qanday o'tkazish kerak yordamida hujumni aniqlash usullari samaradorligini oshirishga yordam beradi. Hozirda Teran o'rganish ochiq va qiziqarli savol bo'lib qolmoqda.

SUN’IY INTELLEKT TEXNOLOGIYALARI YORDAMIDA VIDEO TASVIRLARDAN FOYDALANIB JINOYATLARNI ANIQLASH VA OLDINI OLISH TIZIMLARINI ISHLAB CHIQISH

Azimov Bunyod Raximjonovich
t.f.f.d., PhD TATU Sun’iy intellekt kafedrasi dotsenti, +998902684801
Nurmurodov Javoxir Nurmurod o‘g‘li
t.f.f.d., PhD TATU Sun’iy intellekt kafedrasi dostsenti, +998942947886
Boytemirov Asror Maxmado‘stovich
TATU Sun’iy intellekt kafedrasi tayanch doktoranti +998912104199

Annotatsiya. *Ushbu tadqiqot vizual ma’lumotlardan foydalangan holda shahar muhitida shubhali faoliyatni aniqlashda kompyuter ko‘rish modellarining samaradorligini aniqlashga qaratilgan. Shuningdek, u jinoyatlarning oldini olish strategiyalarini xabardor qilish va yaxshilash uchun ushbu aniqlashlardan qanday foydalanish mumkinligini o‘rganishga qaratilgan. Biz kuzatuv tasvirlarini tahlil qilish uchun potentsial jinoiy faoliyatni ko‘rsatadigan xatti-harakatlar modellarini aniqlashga e'tibor qaratish uchun Konvolyutsion Neyron Tarmoq (CNN) modelidan foydalandik. Model real vaqt rejimida aniqlash imkoniyatlariga e'tibor qaratgan holda shahar joylarining turli ma’lumotlar to‘plamida o‘qitildi va sinovdan o‘tkazildi.*

Аннотация. *Целью данного исследования является определение эффективности моделей компьютерного зрения при обнаружении подозрительной активности в городской среде с использованием визуальных данных. Целью исследования также является изучение того, как эти результаты могут быть использованы для информирования и улучшения стратегий предотвращения преступности. Мы использовали модель сверточной нейронной сети (CNN) для анализа изображений наблюдения, чтобы сосредоточиться на выявлении моделей поведения, указывающих на потенциальную преступную деятельность. Модель была обучена и протестирована на различных наборах данных городских территорий с упором на возможности обнаружения в реальном времени.*

Abstract*. This study aims to determine the effectiveness of computer vision models in detecting suspicious activity in urban environments using visual data. It also aims to explore how these findings can be used to inform and improve crime prevention strategies. We used a Convolutional Neural Network (CNN) model to analyze surveillance images to focus on identifying patterns of behavior that indicate potential criminal activity. The model was trained and tested on different datasets of urban areas, focusing on real-time detection capabilities.*

Kirish. Bilamizki butun dunyoda shaharlar infrastruktura va aholi sonini ko‘pligi bilan ajralib turadi. Shu asnoda shahar muhiti jinoiy faoliyat uchun imkoniyatlar bilan to‘la bo‘lib, ular ko‘pincha kuzatuv tizimlari orqali kuzatiladi va jinoyatlar aniqlanadi. Jinoyatni aniqlashning an’anaviy usullari asosan videoyozuvlarni qo‘lda kuzatishga tayanadi, bu

jarayon nafaqat koʻp vaqt talab etadi, balki inson xatosi va kechikishlariga ham sabab boʻladi. Kechikishlar oʻz navbatida shubhali harakatlarni erta aniqlash va jinoyatning oldini olish imkoniyatini pasaytiradi. Ushbu tadqiqotda aynan yuqoridagi kamchiliklarni bartaraf etish maqsadida potentsial jinoiy faoliyatni aniqlash uchun vizual ma'lumotlarni tahlil qila oladigan kompyuter koʻrish modelini ishlab chiqish va baholash koʻrib chiqiladi. Ishlab chiqilgan model real vaqtda shubhali xatti-harakatlarni aniqlash va tasniflash orqali huquqni muhofaza qilish organlarining oʻz vaqtida ogohlantirishga qaratiladi. Ushbu yondashuv nafaqat jinoyatlarni aniqlash samaradorligini oshirishga, balki ilgʻor texnologik yechimlar orqali jamoat xavfsizligini ta'minlashga katta hissa qoʻshadi.

Assosiy qism.

Bilamizki tasvirlarni tanib olish uchun bugungi kunda keng qoʻllanilayotgan sun'iy intellekt modellari mavjud. Biz tadqiqot ishimizda aniqlik yuqori boʻlgan konvolyutsion neyron tarmogʻini (CNN) tanlab oldik.

CNN modeli xususiyatlarni ajratib olish uchun bir nechta konvolyutsion qatlamlardan, oʻlchamlarni kamaytirish uchun birlashtiruvchi qatlamlardan va tasniflash uchun toʻliq bogʻlangan qatlamlardan iborat[1]:

- **Konvolyutsion qatlamlar:** tasvirlardagi fazoviy ierarxiya va naqshlarni olish uchun.
- **Pooling qatlamlari:** fazoviy oʻlchamlarni kamaytirish va dominant xususiyatlarni ta'kidlash uchun.
- **Toʻliq bogʻlangan qatlamlar:** olingan xususiyatlar asosida yuqori darajadagi fikrlash va tasnifni amalga oshirish uchun.

Konvolyutsion neyron tarmogʻi (CNN) modeli kuzatuv videolaridagi shubhali harakatlarni aniqlashda mustahkam ishlashni namoyish etdi, masalan:

- **Bevositalik:** nozik joylarda aniq sabablarsiz qolgan shaxslarning aniqlangan holatlari, bu koʻpincha potentsial jinoiy niyatdan dalolat beradi.
- **Ruxsatsiz kirish:** noqonuniy faoliyatning boshlanishi boʻlishi mumkin boʻlgan cheklangan yoki nazorat qilinadigan zonalarga kirayotgan odamlar aniqlandi.

Model real vaqt rejimida video kuzatuv tizimiga integratsiya qilingan boʻlib, u jonli muhitda samarali ishlashni namoyish etdi:

[1]Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25, 1097-1105.

- **Real vaqt tahlili:** CNN modeli video tasmalarini real vaqt rejimida qayta ishladi va har bir kadrni doimiy ravishda tahlil qilib, shubhali harakatlar sodir bo‘lganligini aniqladi.
- **Hodisa haqida xabar berish:** Model tomonidan aniqlangan shubhali harakatlar huquq-tartibot idoralari tomonidan tekshirilishi uchun belgilandi va belgilandi. Bu qobiliyat potentsial tahdidlarni tezkor baholash va ularga javob berish imkonini berdi, kuzatuv operatsiyalari samaradorligini sezilarli darajada oshirdi[2]. Aniqlash, real vaqt rejimida qayta ishlash va samarali vizualizatsiya vositalarining kombinatsiyasi CNN modelining amaliy tushunchalarni taqdim etish va o‘z vaqtida aralashuvni osonlashtirish orqali jinoyatlarning oldini olish strategiyasini yaxshilash salohiyatini namoyish etdi. Ushbu batafsil natijalar bo‘limi huquqni muhofaza qilish faoliyatini qo‘llab-quvvatlashda qo‘llaniladigan modelning ishlashi, amaliy qo‘llanilishi va vizualizatsiya usullarining to‘liq ko‘rinishini taqdim etadi[3].

Konvolyutsion neyron tarmog‘i (CNN) modelining ishlashi bir nechta asosiy ko‘rsatkichlar yordamida baholandi. Matematik formulalar va natijalar quyidagicha:

Accuracy (Aniqlik): Aniqlik barcha misollar orasida to‘g‘ri tasniflangan misollarning (haqiqiy ijobiy va haqiqiy salbiy) ulushini o‘lchaydi. U quyidagicha hisoblab chiqiladi:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (1)$$

bu yerda TP haqiqiy ijobiylar soni, TN haqiqiy negativlar soni, FP noto‘g‘ri musbatlar soni va FN noto‘g‘ri salbiylar soni. CNN modeli 92% aniqlikka erishdi.

Precision (Aniqlik): Aniqlik ijobiy deb tasniflangan barcha misollar orasidagi haqiqiy musbatlar nisbatini bildiradi. U tomonidan beriladi:

$$Precision = \frac{TP}{TP + FP} \qquad (2)$$

model 0,87 aniqlikka erishdi, ya’ni belgilangan harakatlarning 87 foizi shubhali deb to‘g‘ri aniqlangan.

Recall (Eslab qolish): Recall barcha haqiqiy ijobiy holatlar orasida haqiqiy ijobiylarning ulushini o‘lchaydi. U quyidagicha hisoblanadi:

2 Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), *580-587.*

3 Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 779-788.

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

modelni chaqirib olish **0,91 ni** tashkil etdi, bu haqiqiy shubhali faoliyatning 91% aniqlanganligini koʻrsatadi.

F1-score (F1-ball): F1 balli Precision va Recall garmonik oʻrtacha koʻrsatkichi boʻlib, ikkalasini ham muvozanatlashtiradigan yagona koʻrsatkichni ta'minlaydi. U quyidagicha hisoblanadi:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

model shubhali harakatlarni aniqlashda muvozanatli ishlashni aks ettiruvchi **0,89** F1 balliga erishdi[4].

CNN arxitekturasi kuzatuv tasvirlarini samarali qayta ishlash va tasniflash uchun ishlab chiqilgan. Arxitektura tafsilotlari quyidagicha:

Kirish qatlami: kirish qatlami model arxitekturasi bilan mosligini ta'minlab, 224x224 piksel oʻlchamini oʻzgartirgan kadrlarni qabul qildi.

Konvolyutsion qatlamlar:

1-qatlam: yadro oʻlchami 3x3 boʻlgan 32 filtr, undan keyin ReLU faollashtirish funksiyasi.

2-qatlam: yadro hajmi 3x3 boʻlgan 64 ta filtr, undan keyin ReLU faollashtirish funksiyasi.

3-qatlam: yadro hajmi 3x3 boʻlgan 128 ta filtr, undan keyin ReLU faollashtirish funksiyasi.

Birlashtirish qatlamlari: Fazoviy oʻlchamlarni kamaytirish va muhim xususiyatlarni olish uchun har bir konvolyutsion qatlamdan keyin maksimal birlashtiruvchi qatlamlar (2x2) amalga oshiriladi.

Toʻliq bogʻlangan qatlamlar:

1-qatlam: ReLU faollashtirilgan 512 birlik.

2-qatlam: ReLU faollashtirilgan 256 birlik.

Chiqish qatlami: Softmax faollashtirish funktsiyasi shubhali va shubhali boʻlmagan toifalarga tasniflaydi.

Tartibga solish: Toʻliq bogʻlangan qatlamlarda haddan tashqari moslashishni oldini olish va modelni umumlashtirishni yaxshilash uchun tushirish (0,5) qoʻllanildi[5].

Optimizator: Modelni oʻrgatish uchun Adam optimallashtiruvchi 0,001 oʻrganish tezligi bilan foydalanilgan.

4 LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

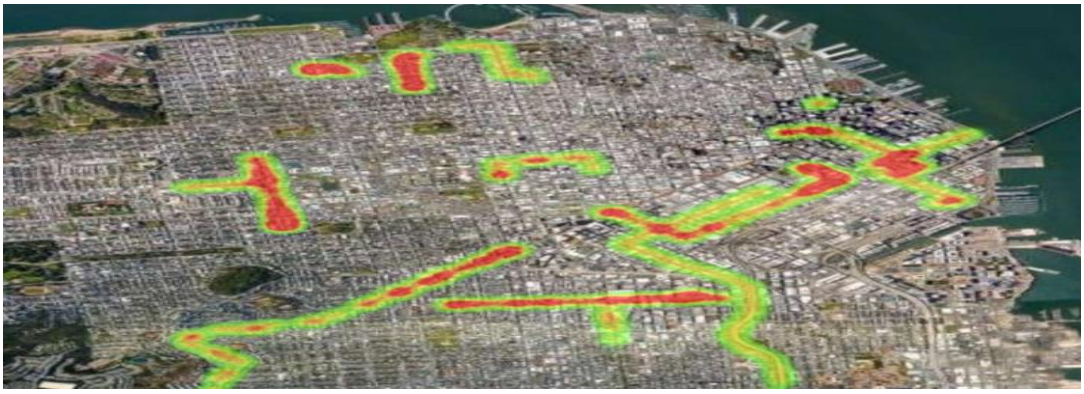
5 Ronneberger, O., Fischer, P., & Brox, T. (2015). U-Net: Convolutional Networks for Biomedical Image Segmentation. Proceedings of the International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI), 234-241.

Vizualizatsiya natijalari. Model natijalarini talqin qilish va ulardan samarali foydalanish uchun vizualizatsiya usullari qo‘llanilgan:

Chegara qutilari: Aniqlangan shubhali harakatlar tegishli ob'yektlar yoki shaxslar atrofida cheklovchi qutilar bilan belgilangan. Bu huquqni muhofaza qilish organlari xodimlariga ehtimoliy tahdidlarni vizual tarzda tasdiqlash va baholash imkonini beradi[6].

1 - rasm. Kuzatuv kamerasi tasvirlarida aniqlangan shubhali harakatlarni ko‘rsatadigan chegaralovchi qutilarga misol

Issiqlik xaritalari: Aniqlangan shubhali harakatlarning fazoviy taqsimotini ko‘rsatish uchun issiqlik xaritalari yaratilgan. Issiq ranglar shubhali xatti-harakatlarning yuqori ehtimolini ko‘rsatib, yuqori xavfli hududlarni aniqlashga yordam beradi.



2 - rasm. Shubhali harakatlar ko‘proq bo‘lgan hududlarni ko‘rsatuvchi issiqlik xaritasi

Kadrlar tahlil jadvallari: Videokadrlar vaqt o‘tishi bilan shubhali harakatlarni ko‘rsatish uchun yaratilgan. Ushbu tahlil naqshlarni tushunishga va resurslarni taqsimlashni rejalashtirishga yordam beradi.

[6] Zeiler, M. D., & Fergus, R. (2014). Visualizing and Understanding Convolutional Networks. European Conference on Computer Vision (ECCV), 818-833.

3 - rasm. Vaqt o‘tishi bilan aniqlangan shubhali harakatlarni ko‘rsatadigan tahliliy kadrlar jadvali.

Ushbu vizualizatsiya amaliyotga taalluqli tushunchalarni taqdim etdi va huquqni muhofaza qilish organlari tomonidan tezkor qarorlar qabul qilishga yordam beradi, jinoyatchilikning oldini olish strategiyasining umumiy samaradorligini oshirdi[7].

Ushbu tadqiqot natijalari kuzatuv kameralaridagi shubhali harakatlarni aniqlashda konvolyutsion neyron tarmoqlari (CNN) samaradorligini ko‘rsatadi. 92% aniqlik bilan CNN modeli kompyuterni ko‘rish texnikasi real vaqtda jinoyatlarning oldini olish uchun kuchli vosita bo‘lishi mumkinligini ko‘rsatdi. Yuqori aniqlik (0,87) va eslab qolish (0,91) modelning noto‘g‘ri pozitivlarni minimallashtirish va haqiqiy tahdidlarni aniq aniqlash qobiliyatini yanada ta’kidlab, uni avtomatlashtirilgan kuzatuv tizimlarida ishonchli komponentga aylantiradi[8].

Ushbu natijalar shuni ko‘rsatadiki, kompyuter ko‘rish modellari turli xil va keng qamrovli ma’lumotlar to‘plamida o‘qitilganda, potentsial jinoiy xatti-harakatlarni aniqlashni yuqori darajada oshirishi va shu bilan xavfsizroq jamoat muhitiga hissa qo‘shishi mumkin. Video tasmalarini real vaqt rejimida kuzatish va tahlil qilish imkoniyati hodisalarga zudlik bilan javob berish imkonini beradi, bu jinoyatlar avj olishidan oldin ularning oldini olishda muhim ahamiyatga ega hisoblanadi[9].

Xulosa. Ushbu tadqiqot kompyuterni ko‘rish texnikasi, xususan, konvolyutsion neyron tarmoqlari (CNN) shahar muhitida shubhali harakatlarni aniqlashda juda samarali ekanligi haqida ishonchli dalillarni taqdim etadi. Model yuqori darajadagi aniqlikka erishdi (92%) va noto‘g‘ri pozitivlarni minimallashtirish va potentsial tahdidlarni aniq aniqlash qobiliyatini namoyish etdi. Ushbu topilmalar CNN ning jamoat xavfsizligini kuchaytiruvchi proaktiv yondashuvni taklif qiluvchi

7 Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 511-518.
8Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 16, 321-357.
9 Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

zamonaviy jinoyatlarning oldini olish strategiyalarida muhim tarkibiy qism bo‘lib xizmat qilish potentsialini ta’kidlaydi. Uzluksiz monitoring uchun inson operatorlariga bo‘lgan ishonchni kamaytirish orqali tizim huquqni muhofaza qilish organlariga o‘z resurslarini tasdiqlangan tahdidlarga yo‘naltirish, javob berish vaqtlarini yaxshilash va jinoyatlar sodir bo‘lishidan oldin oldini olish imkonini beradi. Ushbu integratsiya jamoat joylarini nazorat qilish usulini yaxshilashi mumkin, bu esa shaharlarni aholi va mehmonlar uchun xavfsizroq qilish imkonini beradi.

PROPOSAL OF SMART HOME SECURITY SYSTEM USING RASPBERRY PI 4

Mamirov Hudoyberdi Xomidjonovich
TATU Sun’iy intellekt kafedrasi tayanch doktoranti +998772625477
Boytemirov Asror Maxmado’stovich
TATU Sun’iy intellekt kafedrasi tayanch doktoranti +998912104199
Qobilov Sirojiddin Sherqulovich
TATU Sun’iy intellekt kafedrasi assistenti +998975324636

Abstract: *IoT (Internet of Things) technology, the core technology of the 4th industrial revolution, is currently being applied to various fields. Among them, the most basic application is the security system. The security system automatically detects a moving object or person approaching a restricted area, and if the object orperson moves, it can immediately take a picture and store it. By taking a picture and storing it, you can recognize what the moving object is and who it is if it is a person. You can open the door by checking who it is, and you can also find out what time someone came. In this paper, we propose a smart home security system based on Raspberry Pi 4. The proposed smart home security system uses a Raspberry Pi 4, a relatively easy-to-handle main processor, and a human body sensor (PIR sensor) to configure smart home security to determine intrusion. In addition, a web camera was connected to the Raspberry Pi 4 to record the intruder'svideo. As a result of verifying the efficiency by actually implementing the smart home security system proposed in this paper, it was possible for individuals to configure it more easily than the existing home security system. All sensors used inthis study were inexpensive and easily available on the market. The computer was configured using Raspberry Pi 4 so that Uzbekistan could have a lot of interest in Raspberry Pi. The PIR sensor detects if there is an object moving within the measuring range, and the detected data is transmitted back to the camera system tooperate camera and take a picture. The captured images are immediately displayedon the monitor and stored in the database. The computer program was written in Python language, and it was found that the implementation worked well*[1].

[1] Ye-Jin Jang, Young-Tae Chun, "Technology trend of Smart-home Security System", Korean Security Science Review, no.30, pp.119-138, 2012

Keywords: *IoT, Raspberry pi 4, camera, PIR sensor, smart home, security*

1. Introduction

Recently, the world is undergoing technological development in many fields under the influence of the 4th industrial revolution. The characteristics of the 4th Industrial Revolution technology are changing to make people's lives more effective and convenient, and for this purpose, the Internet of Things connected as one basedon the Internet forms the core. Also, in the 4th industry, cloud computing that can be connected to one computer around the world, artificial intelligence with self-determination, and virtual reality suitable for simulation are key technologies. Amongthese core technologies, IoT and artificial intelligence (AI) fields are particularly interested in many countries around the world, so universities and global companies are mainly researching them. These research results are also developing day by day. In addition, artificial intelligence and the Internet of Things are organically cooperating with each other to create new synergies. IoT technology, represented by smart cities, smart factories, smart farms, smart buildings, and security systems, is of great interest in cities and local governments in each country.

In particular, Korea's competitiveness in the field of IoT-based method systems, smart cities, smart factories, smart farms, and smart buildings has reachedthe world's highest level. There are many research presentations on the current system and many prototype presentations. [1] to [16]. The theoretical background is sufficient, and based on this technical background, each company makes prototypes and announces and sells them. However, Uzbekistan still imports and uses foreign technology because the competitiveness of IoT is still weak. In order to activate technology in the field of IoT in Uzbekistan, first, each university should pay attention to fostering experts in the field of IoT and produce them, and the discharged manpower should work professionally in this field. In addition, it is important for the government to spread awareness and R&D in the field of IoT.

This study aims to implement a basic Smart Home Security system as a basic step study to activate Uzbek's IoT technology. In order to induce interest in the IoT of students and related persons, a basic and easy system was created using the most general-purpose sensor and camera. A PIR sensor is used to detect motionin a designated area, and the detected data is transmitted to a computer, which activates another image sensor, the camera, to take pictures of moving objects. It isdisplayed directly on the monitor system and stored in the computer's database. If necessary, you can take a video and archive it. These digital technologies require skills to understand and use sensors. In order to operate the camera, you need to

understand the basics of the camera and have the skills to connect the camera to a computer. The program that directly controls these technologies was written as a Python program, and the necessary software libraries were written by directly downloading them from the outside. Raspberry Pi's RPi.GPIO, time, and opencv libraries were installed and used on the Raspberry Pi 4 computer.

As a result, this study implemented a basic IoT system for the security system, and measured and analyzed moving people or objects, which are the most basic data in the Smart Home Security System. A commonly used PIR sensor was used as the sensor, and a logitech webcam 270 model, a universal web camera, was usedas the camera. All of them are universally used and inexpensive, so students can easily purchase and use them. Although this study is still insufficient to induce interest in the new IoT field in Uzbekistan, it showed a lot of interest from students and professors by developing the most basic IoT system[2].

2. Smart Home security system (theoretical background)

2.1 Internet of Things (IoT)

The Internet of Things (IoT) is all network technology of things (Things) embedded with sensors, software, and other technologies for the purpose of connecting all computers and things through the Internet, transmitting data with other devices and systems, and improving efficiency. It is a wide range of technologies, including Such things range from ordinary household electronics to sophisticated industrial tools. Currently, more than 7 billion IoT devices are connected to the network worldwide, but experts predict that more than 20 billion things will be connected to the Internet by 2025. Most of these connections are connected to the servers of IoT specialist companies. There is, and it is expected that more servers will be connected in the future. Currently, many companies, led by Amazon, a representative IoT company, operate cloud computers and are connected to things around the world through the Internet. Cloud computer companies specializing in IoT are expected to appear in Uzbekistan in the future, and I think that Uzbekistan will show a lot of interest in IoT soon.

In the future living environment, the safety of people living in offices or homes becomes important. If an unauthorized person appears in a specific area, a big problem can occur, and when this situation occurs, information to effectively deal with it is very necessary. In addition, if a large computer is used to create such a system, efficiency may be a

[2] Han-Gook Kim, "Analysis of Entry Strategy and Market Trend of Home Security", Korea Entertainment Industry Association, pp.223-226, 2014.11.

problem, and the size of the system will become very large. For this system, the size can be configured very small by implementing the system using Raspberry Pi 4, which is exclusively used in the Internet of Things. In Uzbekistan, there are not many papers related to the Security System of the Internet of Things yet, and there is little interest.

2.2 Basic configuration of Smart Home Security System

The basic configuration of the Smart Home Security System requires a system that measures environmental data in a specific area. The changing information of a specific area is very important environmental data. A sensor is required to measure and analyze it, and a transmission system to transmit data is also required. In special cases, you need a camera to take pictures, and the programthat drives it is also important. This study can be divided into a sensor part that monitors a specific area, a camera that takes pictures, and a computer part that controls them all. A PIR sensor was used for the sensor, a logitech webcam 270 model was used for the camera, and a Raspberry Pi 4 was used for the computer to implement the system. Based on the Smart Home Security System and the basic theory of each sensor, a basic Smart Home Security System was produced, and thistechnology was studied at a university in Uzbekistan and was intended to be applied where necessary within the university.

3. Proposed Smart Home Security system function and operation algorithm

3.1 Implemented system block diagram

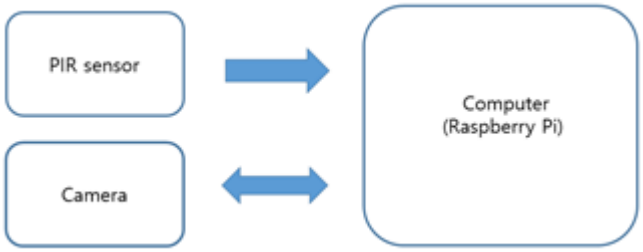


Figure 1. System block diagram

The block diagram of the implemented system is shown in Figure 1. The implemented system is largely divided into three divisions. It can be divided into PIR sensor part, camera part, and computer Raspberry Pi part. The computer part can create a database part inside and store the images taken from the camera in the database. A PIR sensor is connected to the Raspberry Pi 4, so when a person enters the limited range, the PIR sensor detects the person and informs the Raspberry Pi 4 that a person has entered the restricted area. The Raspberry Pi 4 sends a separate warning message to the monitor and activates another image sensor connected to the Raspberry Pi 4. Since the camera is used as an image

sensor, the camera is operated to take pictures of moving objects. The captured data is stored in a database. Since the stored data uses the saved time as a name, it is possible to check when a person was there.

3.2 Sensors and computers

3.2.1 PIR sensor

Figure 2. PIR sensor

Figure 2 is a picture of the PIR sensor. The PIR sensor weighs about 7g and is small, and the size is about 3.2cm x 2.4cm x 2.8cm. The range of operating voltage is about DC 4.5V ~ 20V, and the sensing distance is about 3 ~ 7m, which can be adjusted by volume within the sensor. The delay time can also be adjusted from 5 to 200 seconds. Since the most important working environment temperatureis around -20 ~ +80 ℃ everything operates normally within the normal range. These sensors are small in size, inexpensive, use low power, and are easy to use and connect[3].

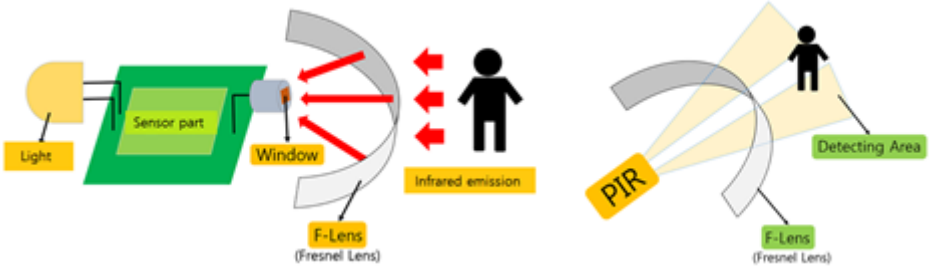


Figure 3. PIR sensor operating principle

Figure 3 shows the operating principle of the PIR sensor. When a person emitting infrared rays comes within the detection distance, the sensor passes theinfrared rays of the person through the condensing lens, F-Lenz (Fresnel Lenz), and reaches the window located on the sensor surface. The window passes only infrared rays of a certain frequency band. The infrared signal passing through the window is converted into

[3] Woo-Sik Lee, Nam-Gi Kim, "Omnidirectional Distance Estimation using ultrasonic in Wireless Sensor Networks", The Journal of The Institute of Webcasting, Internet Television and Telecommunication vol.9, no.5, pp.85-91, 2009.

voltage through the sensor unit and amplified by the amplifier built into the sensor unit itself.

3.2.2 Camera

Figure 4. Camera

Figure 4 is the camera used in this study. The model name is Logitech webcam 270. This camera is a web camera and can be used by connecting to the USB connector of Raspberry Pi 4 in general, so it can be used very conveniently. It has a resolution of 1280 x 720 pixels, uses Logitech RightLight technology, and is available with Logitech Vid HD software. In this study, programming was done using the opencv library, which is a commonly used library.

3.2.3 Computer (Raspberry Pi 4)

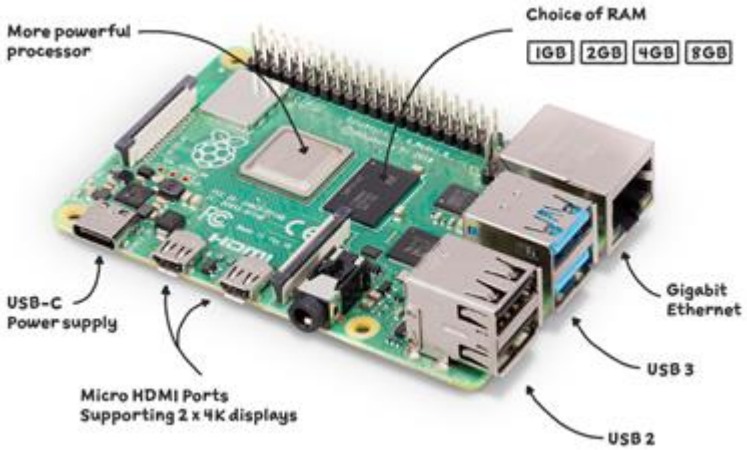


Figure 5. Computer (Raspberry Pi 4)

Figure 5 is Raspberry Pi 4 used in this study. The Raspberry Pi 4 is a single board, capable of interfacing with a screen, keyboard and mouse. The computer used in this study has 8 MB of RAM. The operating system uses the Raspberry Pi OS, and the computer language mainly used in this computer is the Python language. There are two Micro HDMI ports that can connect a monitor to the outside, two USB 2.0 ports for general use, and two high-speed USB 3.0 ports. In addition, there is a jack that outputs

an audio signal to the outside, a connector that can connect a dedicated display device, and a camera port that can connect a dedicated Raspberry Pi camera. Since Bluetooth and Wi-Fi are built-in, it is possible to transmit data through wireless communication with the outside without connecting a separate device. The operating system used can be downloaded and installed from the Raspberry Pi website, and the Micro SD card used at this time can be used farther than 16GB. When installing the operating system, if you use theRaspberry PI Imager provided on the website, you can easily install the operating system on the Micro SD card[4].

3.2.4 Raspberry pi GPIO pins

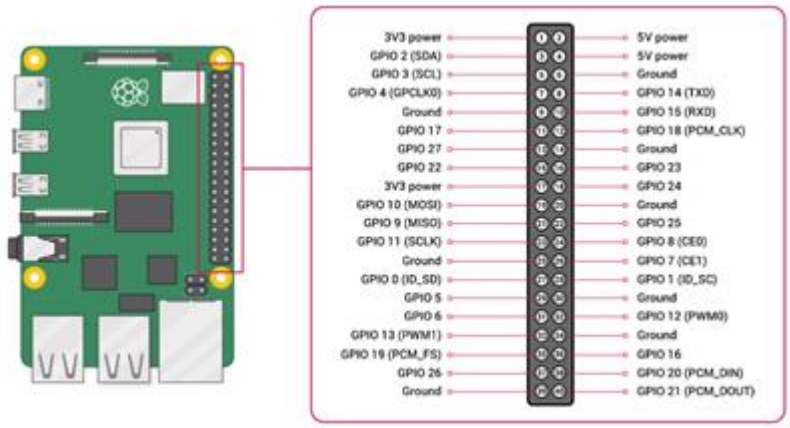


Figure 6. Raspberry Pi 4 GPIO and 40 Pins

Figure 6 shows the PGIO and 40 pins of Raspberry Pi 4. Since it has 40 pins, it can send or receive data to the outside. A number is attached to each pin, and the user can connect them to the outside. It contains power, ground, and pins with special functions. In Raspberry Pi 4, all pins use +3.3V, so you should always be careful when connecting to other computers or connecting external circuits. In this study, the PIR sensor was connected to GPIO pin 7. Python and C languages are mainly used to control externally connected circuits, but in this study, the Python language was used for programming. The editor used the “Thonny” editor built into the Raspberry Pi OS.

4. Proposed Smart Home Security System Diagram and Implementation

[4] Kim Howon, "IoT technology and security", Information Security Journal, vol.22, no.1, 2012

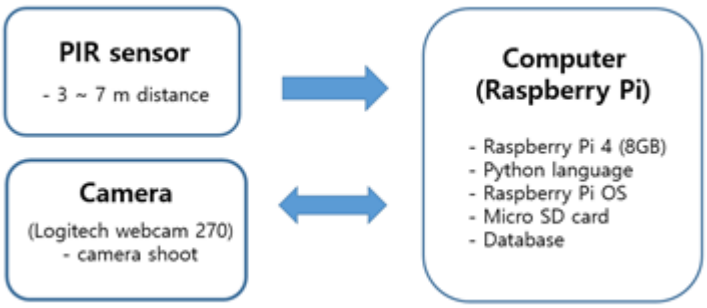


Figure 7. The configuration diagram of the Smart Home Security System

Figure 7 shows the configuration of the proposed system. The PIR sensor can measure a range between 3 and 7m, and the camera takes a picture when aperson enters within the limited range. At this time, a warning message indicating an emergency is displayed on the monitor. Overall control for them is done by Raspberry Pi 4, and the main program is written in Python language. The captured image data is stored in the database set in the Raspberry Pi 4.

As a result of completing and implementing this system, the following results were confirmed.

1) Confirmation of basic Smart Home Security System configurability using Raspberry Pi

2) Check the possibility of measuring motion within a limited distance using a PIR sensor

3) Install OpenCV library to use camera and check operation

4) Automatically check camera shooting and saving[5]

[5] Wi Yukyeong, Kwak Jin, "Analysis of Smart TV Trends and Security Vulnerabilities to Use in the Smartwork", Korea Multimedia Society, 2012

Figure 8. Shooting and warning message when a person enters the limited range

Figure 8 shows the case where a person appears in a limited range, that is, in case of an emergency, the camera shoots and displays the “Motion detected” warning on the monitor. Depending on the camera installation location, you can take pictures from different angles, and if you use multiple cameras, you can take pictures from multiple angles.

5. CONCLUSION

The system proposed in this study used commonly and easily available parts. Also, a Raspberry Pi 4 computer was used to promote interest in Raspberry Pi in Uzbekistan. For those who are new to the Internet of Things, it is composed using the most common and low-cost parts, so anyone interested in the Internet of Thingsor the Smart Home Security System can implement it without spending a large amount of money. This study is a basic study to propose and arouse interest in the Smart Home Security system among the basic systems of the Internet of Things in developing country, so it can be implemented relatively cheaply. However, in order to implement a more precise and delicate system, more precise sensors and more diverse warning devices should be added. A more precise sensor can identify abnormal situations more quickly, and a better camera can take higher-resolution photos. In this study, two sensors were used, but I am sure that it will become a more effective Smart Home Security system if a system is created using more sensors in the future and connected with communication.

РАҚАМЛИ ДАЛИЛ. ЭКСТРЕМИЗМ БИЛАН БОҒЛИҚ ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШДАГИ РАҚАМЛИ ДАЛИЛЛАРНИНГ ЎРНИ

Атаниязов Жасурбек Курбанбаевич
Ўзбекистон Республикаси Жамоат хавфсизлиги университети “Жиноий-ҳуқуқий фанлар” кафедраси доценти, юридик фанлар бўйича фалсафа доктори (PhD),
Содиков Муҳамадбобур Алишер ўғли
Ўзбекистон Республикаси Жамоат хавфсизлиги университети мустақил изланувчиси,.

Аннотация. *Мақола ижтимоий тармоқлардаги профил/аккаунт фойдаланувчилари шахсига оид бошқа рақамли маълумотларни тўплаш, улардан фойдаланиш ҳамда экстремизм билан боғлиқ жиноятларни аниқлаш,*

тергов қилишда тезкор-қидирув тадбирлари натижаларидан фойдаланиш масалаларига бағишланган бўлиб, унда рақамли маълумотлардан далил сифатида фойдаланиш билан боғлиқ муаммолар ва хорижий давлатлар тажрибаси кўриб чиқилган.

Таянч сўзлар: *ижтимоий тармоқ, компьютер маълумотлари, электрон далил, рақамли далил, тезкор-қидирув фаолияти, суд қарори, интернет, ижтимоий тармоқ.*

Аннотация. *Статья посвящена вопросам сбора и использования иной цифровой информации о личности пользователей профилей/аккаунтов в социальных сетях и использования результатов оперативно-розыскной деятельности при выявлении и расследовании преступлений, связанных с экстремизмом, в которых раскрываются проблемы, связанные с использованием цифровых данных в качестве доказательств и опыт зарубежных стран.*

Ключевые слова: *социальная сеть, компьютерные данные, электронные доказательства, цифровые доказательства, следственная деятельность, решение суда, Интернет, социальная сеть.*

Annotation. *The article is devoted to the issues of collecting and using other digital information about the identity of users of profiles/accounts on social networks and using the results of operational search activities in identifying and investigating crimes related to extremism, which reveal problems associated with the use of digital data as evidence and experience foreign countries.*

Keywords: *social network, computer data, electronic evidence, digital evidence, investigative activity, court decision, Internet, social network.*

Интернет ва замонавий ахборот тизимларини яратилиши билан бир қаторда, турли вирусли дастурларнинг тарқалиши, ҳимоя паролларни бузиш, қонунга зид бўлган ахборотларни тарқатиш, хакерлик ҳужумлари, давлат ва корхона-ташкилотларнинг расмий веб-сайтларига ноқонуний кириш, муаллифлик ҳуқуқини бузилиши, фирибгарлик ва банк карталарини ноқонуний эгаллаш ҳамда пул маблағларини талон-торож қилиш каби ахборот технологияларидан фойдаланиб содир этиладиган жиноятлар – кибержиноятчилик тушунчасини пайдо бўлишига олиб келди.

Ўзбекистон Республикасининг янги таҳрирдаги Конституциясининг 33-моддаси 3-бандига кўра, эндиликда, “Давлат Интернет жаҳон ахборот тармоғидан фойдаланишни таъминлаш учун шарт-шароитлар яратади”, деб кўрсатилган.

Интернет ва ижтимоий тармоқларни назорат қилиш ва бошқаришнинг мураккаблиги экстремистик мазмундаги материалларни ушбу тармоқда эркин тарқалиш имконини бермоқда.

Диний экстремизм ва терроризм масаласи дунёдаги энг глобал муаммога айланиб бормоқда. Ўз тарафдорларини кенгайтириш мақсадида, тарғиботларда оммавий ахборот воситалари, замонавий

техналогиялар, интернет каби глобал тармоқлардан максимал фойдаланишмоқда.

Экстремизм билан боғлиқ жиноят содир этган шахсларни айбини исботлаш тезкор-қидирув фаолияти ва дастлабки тергов жараёнида гумонланувчининг интернет ва ижтимоий тармоқлардаги саҳифаларини кўздан кечириш ҳаракати орқали амалга оширилмоқда.

Кўздан кечириш ҳаракати давомида гумонланувчининг ижтимоий тармоқдаги саҳифасидан олинган қонунга зид ҳарактердаги маълумотлар мазмуни бўйича судга оид экспертиза тайинланиб, экспертлар олдига ҳал этиш учун саволлар берилади. Терговчилар томонидан эксперт хулосаси таянган ҳолда жиноят содир этган шахсга нисбатан айблаш ёки реабилиция қилиш масаласи кўриб чиқилмоқда.

Интернет ва ижтимоий тармоқ маълумотларини кўлга киритиш, улардан далил сифатида фойдаланиш ҳанузгача амалиётга жорий этилгани йўқ.

Таъкидлаш жоизки, амалдаги жиноят-процессуал қонунчиликда **рақамли далил** тушунчаси киритилмаган ҳамда ушбу **далилларни олиш, сақлаш ва исботлашда улардан фойдаланиш** тартиби ва шартлари ёритилмаганлиги, умумий бир бир сўз билан “Рақамли далил”нинг ҳуқуқий мақоми белгиланмаганлиги ҳозирги кунда ушбу турдаги далиллар билан ишлашда бир қатор муаммоларни келтириб чиқармоқда.

Рақамли далил тушунчасининг таг маъносига назар ташласак, ушбу тушунчалар учун ягона таърифлар ва ечимлар борасида бир қанча қарашлар мавжудлиги кузатилмоқда. Лекин, далилларнинг янги турларини “Электрон далил” ёхуд “Рақамли далил” деб эътироф этишда олимлар гуруҳи томонидан турлича ёндашилмоқда.

Компьютер ва интернетдаги маълумотлардан жиноятларга қарши курашишда фойдаланиш, жумладан экстремизм билан боғлиқ жиноятлар мисолида кўрадиган бўлсак, сўнгги вақтларда аниқланган жиноятларнинг содир этиш усули сифатида интернет жаҳон ахборот тармоғи эканлигини кўришимиз мумкин.

Бу борада, хорижий давлатлар жумладан АҚШ, Туркия, Россия ва бошқа суд-тергов ҳуқуқи ривожланган давлатлар тажрибалари ўрганилганида, ижтимоий тармоқлардан профил ва унинг фойдаланувчисига оид маълумотларни олиш ва жиноят-процессуал

қонунчилик асосида ундан далил сифатида фойдаланиш амалиёти йўлга қўйилган.

Мисол тариқасида оладиган бўлсак, юқорида таъкидланганидек, юртимиз аҳолиси орасида кенг фойдаланиб келинаётган “Мета Platforms” корпорациясига тегишли “Facebook” ва “Instagram” ижтимоий тармоқларидаги профил фойдаланувчиси саҳифасида қонунга зид бўлган контентларни жойлаштириши натижасида ҳуқуқбузарлик содир этилганида, “Мета Platforms” ўзида мавжуд маълумотларни асослантилган **суд қарори** асосида ҳуқуқ-тартибот идораларига тақдим этади ва ушбу маълумотлардан рақамли далил сифатида фойдаланиб келинмоқда.

Бу бўйича “Facebook” ва “Instagram” платформаларида ҳуқуқ-тартибот идоралари учун тегишли тавсиялар ва кўрсатмалар бўлими мавжуд бўлиб, унда ҳамкорлик масалаларида тегишли давлатнинг расмий ҳуқуқ-тартибот идоралари томонидан суд қарори келтирилиши назарда тутилган [1].

“Мета Platforms” томонидан ҳуқуқ-тартибот идораларининг сўрови бўйича профил ва унинг фойдаланувчиси тўғрисида шахсга доир маълумотлар тақдим этилиши мумкин.

Ушбу маълумотлар улкан серверлар сақланишини инобатга олиб, улар доимий равишда сақланиб турмайди. Маълум муддат ўтганидан сўнг, эски маълумот ўрнига янгиси келиб тушганидан сўнг олдинги маълумотлар ўчириб юборилади. Бу эса, жиноий қилмишни исбот қилишда, ушбу маълумотларни олиш ва далил сифатида эътироф этиш масалаларини қонунчиликда мустаҳкамланишни тақозо этмоқда.

Россия Федерациясининг 1995 йилда қабул қилинган 144-ФЗ-сонли Федерал қонуни *(Тезкор-қидирув фаолияти тўғрисида)*га 2016 йил 6 июлда 374-ФЗ-сонли Федерал қонун билан киритилган ўзгартириш ва қўшимчаларда 15-тезкор қидирув-тадбири сифатида **“Компьютер маълумотларини олиш”** тезкор-қидирув тадбири киритилган бўлиб, шахс ва фуқароларнинг дахлсизлигига бўлган конституциявий ҳуқуқларини чекловчи тезкор-қидирув фаолиятини *(шу жумладан, компьютер маълумотларини олиш)* етарли асослар мавжуд бўлганда **суд қарори** асосида ўтказилиши кўрсатиб ўтилган [2].

Хулоса ўрнида шуни айтиш жоизки, “рақамли далил” тушунчасини амалиётга жорий этиш орқали жиноятларни, жумладан экстремизм билан боғлиқ жиноятларни аниқлаш ва тергов қилишда компьютер серверида сақланаётган рақамли

далилларни қўлга киритиш, ундан исботлашда фойдаланиш бўйича тезкор-қидирув ва жиноят-процессуал қонунчиликни такомиллаштириш муҳим аҳамиятга эга ҳисобланади.

КИБЕРЖИНОЯТЛАРГА ҚАРШИ КУРАШИШДА ПРОКУРОР-КРИМИНАЛИСТЛАРНИНГ ЎРНИ

Ражабов Бекзод Халимович
Ҳуқуқни муҳофаза қилиш академияси
катта ўқитувчиси
ТДЮУ мустақил изланувчиси

Аннотация: *Мақолада замон ва макон танламайдиган кибержиноятларни тергов қилишда, уларни фош этишда прокурор - криминалистлар институтининг ўрни, бу борада мамлакатимизда амалга оширилаётган ислоҳотлар ва жорий ҳолат таҳлил қилинган.*

Шунингдек, Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш Академиясида янги ташкил этилган Рақамли криминалистика илмий тадқиқот институти фаолиятини тартибга солувчи норматив – ҳуқуқий ҳужжатларда прокурор-криминалистнинг ҳуқуқий мақомига доир айрим муаммолар таҳлил қилинган.

Прокурор-криминалистлар фаолиятини тўғри йўлга қўйиш мақсадида, унинг ҳуқуқий мақомини такомиллаштиришга доир айрим таклифлар берилган.

Калит сўзлар: *кибержиноятлар, ахборот технологиялари воситасида содир этиладиган жиноятлар, экспертиза, эксперт, эксперт-криминалист, прокурор-криминалист.*

Аннотация: *В статье анализируется роль института прокуроров-криминалистов в расследовании киберпреступлений, которые не выбирают время и пространство, реформы и текущая ситуация в нашей стране в связи с этим.*

Также в нормативных правовых документах, регламентирующих деятельность вновь созданного научно–исследовательского института цифровой криминологии при Академии правоохранительных органов Республики Узбекистан, были проанализированы некоторые проблемы, связанные с правовым статусом прокурора- криминалиста.

Для того чтобы должным образом наладить деятельность прокуратуры-криминалиста, были внесены некоторые предложения по улучшению ее правового статуса.

Ключовые слова: *киберпреступления, преступления совершаемые с использованием информационных технологий, экспертиза, эксперт, эксперт-криминалист, прокурор-криминалист.*

Abstract: *this article analyzes the reforms and the current situation in the development of the institute of forensic-prosecutors.*

Also, in the regulatory legal acts, an analysis of some problems related to the legal status of the forensic-prosecutor was carried out and subsequently some proposals and considerations were put forward regarding the correct implementation of the activities of forensic-prosecutors and improving their legal status.

Key word: *cybercrimes, crimes committed using information technologies, examination, expert, forensic expert, forensic prosecutor*.

Жиноятлар содир этилиши борасидаги халқаро экспертлар таҳлилига кўра, ер юзида тахминан ҳар бир соатда 200 мингга яқин жиноятлар содир этилади”[1].

Кибержиноятлар XXI асрнинг энг муҳим жиноятларидан бири бўлиб, ушбу жиноятларни тергов қилиш самарадорлиги эса, атиги 0,05%ни ташкил қилмоқда[2].

Ушбу кўрсаткичлар таҳлили тергов соҳасини фан ва технологияларнинг янги замонавий ютуқлари билан қуроллантириб бориш лозимлигини талаб этмоқда.

Мамлакатимиз суд-тергов фаолиятини яхшилаш, тергов сифатини ошириш, суд-тергов фаолиятида шахснинг ҳуқуқ ва эркинликларини ҳимоя қилиш кафолатларини янада кучайтиришга қаратилган бир қатор ислоҳотлар амалга ошириб келинмоқда.

Жумладан, 2020 йил 10 августдаги “Суд-тергов фаолиятида шахснинг ҳуқуқ ва эркинликларини ҳимоя қилиш кафолатларини янада кучайтириш чора-тадбирлари тўғрисида”ги 6041-сонли Фармонида, суд-тергов фаолиятини янада такомиллаштиришнинг асосий йўналиши сифатида процессуал ҳаракатларнинг сифатини ошириш, жиноят процессида далилларни тўплаш ва мустаҳкамлаш, уларга баҳо бериш тизимини илғор хорижий тажрибада кенг қўлланиладиган исботлаш стандартларини инобатга олган ҳолда қайта кўриб чиқиш белгиланган[3].

Шунингдек, Фармон билан прокуратура органларининг белгиланган штат бирлиги доирасида, Ўзбекистон Республикаси Бош прокуратураси, Қорақалпоғистон Республикаси, вилоят ва Тошкент шаҳар прокуратуралари тизимида прокурор-криминалист лавозимини жорий этиш ва Давлат бюджети параметрларида прокуратура органлари учун ажратилган маблағлар доирасида ва бюджетдан ташқари маблағлари ҳисобидан прокурор-

[1] https://www.newsru.com/crime.

[2] Борба с киберпреступностью — что происходит с законом, когда закон не может быт приведен в исполнение? артислес/борба-с-киберпреступностью-что-происходит-с-законом-когда-закон-не-может-быт-приведен-в-исполнени.

[3] Ўзбекистон Республикаси Президентининг 2020 йил 10 августдаги “Суд-тергов фаолиятида шахснинг ҳуқуқ ва эркинликларини ҳимоя қилиш кафолатларини янада кучайтириш чора-тадбирлари тўғрисида”ги 6041-сонли Фармони//https://lex.uz/docs/4939467

криминалистларни замонавий махсус жиҳозлар билан таъминлаш чораларини кўриш назарда тутилган.

Ўзбекистон Республикаси Президентининг 2023 йил 11 сентябрдаги “Ўзбекистон - 2030” Стратегияси тўғрисида”ги ПФ-158-сонли Фармони билан тасдиқланган “Ўзбекистон-2030” Стратегиясининг 87-мақсадида, ҳуқуқни муҳофаза қилувчи органларнинг фаолиятини инсон манфаатлари, қадр-қиммати, ҳуқуқларини ҳимоя қилишга йўналтириш назарда тутилган.

2030 йилгача “Далилларни тўплаш ва мустаҳкамлаш фаолиятини замонавий технологиялар ва сўнгги илмий ютуқларни жорий қилиш орқали тўлиқ рақамлаштириш” 87-мақсадни амалга оширишнинг самарадорлик кўрсаткичи сифатида белгиланди.

Ушбу юксак мақсадларга эришиш ҳамда мамлакатимизда тергов сифатини оширишга қаратилган янги механизмларни жорий қилиш, жиноят ишлари бўйича судга қадар бўлган босқичда ечимини кутаётган процессуал муаммоларни ўрганиш ва қонунчиликдаги мавжуд муаммоларни ҳал қилиш, тергов органлари фаолиятида ўзига хос ўринга эга бўлган прокуратура органлари тизимида фаолият юритаётган прокурор - криминалистларнинг тергов сифатини оширишдаги ролини янада кучайтириш орқали мазкур мақсадларга эришиш мумкин.

Сўнги йилларда ахборот технологиялари соҳасида кўплаб жиноятлар содир этилаётганлиги, кибермаконда содир этилаётган жиноятларни фош этиш, тергов қилиш амалиёти прокурор – криминалистларни рақамли далиллар билан ишлаш кўникмаларини шакллантириб уларни мунтазам равишда ошириб боришни тақозо қилмоқда.

Ўзбекистон Республикаси Президентининг 2024 йил 21 июндаги “Рақамли криминалистика соҳасида илмий тадқиқот фаолиятини ташкил этиш чора-тадбирлари тўғрисида”ги ПҚ-229-сонли Қарори қабул қилиниши прокурор–криминалистлар институтининг тарихий ривожланишида янги босқични бошлаб берди.

Мазкур қарор асосида, Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси Рақамли криминалистика илмий-услубий маркази негизида, Рақамли криминалистика илмий - тадқиқот институти ташкил этилиб, “Ихтисослаштирилган рақамли тадқиқот маркази”, “Рақамли терговга кўмаклашиш бўлими”, “Услубий ёрдам кўрсатиш бўлими” ва “Рақамли криминалистика лабораторияси” фаолияти йўлга қўйилди.

Институт таркибидаги марказ, бўлим, лабораторияда фаолият юритадиган янги прокурор-криминалистлар лавозимини жорий қилинди.

Уларнинг ваколатлари доирасига, рақамли криминалистика ва кибержиноятчиликка қарши курашиш соҳасига оид норматив-ҳуқуқий ҳужжатлар, Бош прокуратура ҳайъати қарорлари, Бош прокурорнинг буйруқ, фармойиш ва кўрсатмалари, Академия бошлиғининг буйруқлари талабларини сўзсиз ижро этиш, рақамли криминалистика ва кибержиноятчиликка қарши курашиш соҳасига доир ўқув-услубий мажмуа ишлаб чиқиш, рақамли криминалистика ва кибержиноятчиликка қарши курашиш соҳасига доир ўқув-амалий машғулотларни сифатли ўтказилишини таъминлаш, рақамли криминалистика ва кибержиноятчиликка қарши курашиш соҳасига доир ўқув-услубий, илмий-амалий қўлланмалари, монографиялар ва диссертацияларга тақризлар бериш, фуқароларни қабул қилиш, жисмоний ва юридик шахсларнинг мурожаатларини кўриб чиқиш ва қонунчиликни тарғиб қилишда иштирок этиш, рақамли криминалистика ва кибержиноятчиликка қарши курашиш фаолиятини такомиллаштириш жараёнига оид ҳисобот лойиҳаларини тайёрлаш, рақамли криминалистика соҳасида тадқиқотлар ўтказиш ва экспертиза хулосаларини тайёрлаш, тергов ҳаракатларида иштирок этиб, рақамли далилларни аниқлаш, олиб қўйиш, сақлаш ва тадқиқ қилиш бўйича тергов органларига амалий ёрдам кўрсатиш, рақамли далилларни йиғиш, таҳлил қилиш ва визуаллаштириш учун махсус дастурий воситаларни яратиш ва мавжудларини такомиллаштириш, рақамли далилларнинг яхлитлигини таъминлаш ва уларни сақлаш учун махсус воситаларни ишлаб чиқиш ва бошқа вазифаларни бажариш юклатилди[4].

Энди, прокурор-криминалистлар ананавий криминалистикага оид махсус билимларни пухта эгаллашидан ташқари, ахборот технологиялари, кибермаконда содир этиладиган жиноятларни фош этишга доир махсус билимларни эгаллашлари талаб этилади.

Кибержиноятларни, ахборот технологиялари воситалари билан содир этилаётган жиноятларни фош этишда, уларни аниқлашда, тергов ва тезкор-қидирув тадбирларини ташкиллаштиришда, экспертизалар тайинлаш ва ўтказишда прокурор-криминалистлар алоҳида ўринга эга бўлмоқда.

[4] Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш Академияси бошлиғининг 01.08.2024 йилдаги 59-Т-сонли буйруғи билан тасдиқланган “Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академиясининг Рақамли криминалистика илмий-тадқиқот институти тўғрисида”ги НИЗОМнинг 23-банди.

Ҳозирги кунда прокурор-криминалистлар фаолиятини тартибга солувчи норматив - ҳуқуқий ҳужжатларни таҳлил қиладиган бўлсак, уларнинг фаолияти Ўзбекистон Республикаси Бош прокурорининг 2021 йил 12 июлдаги 243-сонли буйруғи билан тасдиқланган «Ўзбекистон Республикаси Бош прокуратурасининг Прокуратура органлари тергов тармоқлари фаолияти устидан назорат бошқармаси тўғрисида»ги Низом[5] ва “Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш Академияси бошлиғининг 2024 йил 1 августдаги 59-Т-сонли буйруғи билан тасдиқланган “Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академиясининг Рақамли криминалистика илмий-тадқиқот институти тўғрисида”ги Низом билан тартибга солинган.

Бироқ, ушбу ҳужжатларни бир-бирига мос равишда мувофиқлаштириш, Институтда фаолият кўрсатаётган прокурор-криминалист билан Бош прокуратуранинг Прокуратура органлари тергов тармоқлари фаолияти устидан назорат тармоғида (қуйи турувчи прокуратураларда) фаолият кўрсатаётган прокурор-криминалистларнинг фаолияти бўйича айрим мунозарали ҳолатни юзага келтирмоқда.

Бош прокурорнинг 243-сонли буйруғининг 15-хат бошида, бошқарма катта прокурор-криминалистига — тергов амалиётига илғор криминалистика–техника воситаларини, замонавий ахборот технологияларини, шунингдек, илмий ва экспертлик тадқиқотлари натижалари ҳамда хорижий тажрибани жорий қилиш юзасидан таклифлар тайёрлаши, терговда криминалистик техника воситаларидан, тергов ўтказишнинг илғор услублари ва илм-фан ютуқларидан самарали фойдаланилишини таъминлаши, мазкур соҳада мавжуд тизимли муаммоларни аниқлаш, бунга имкон берган шарт-шароитларни бартараф этиш чораларини кўриши, раҳбарият кўрсатмасига кўра оғир ва ўта оғир жиноятлар бўйича тезкор-тергов гуруҳлари таркибида иштирок этиши, жиноятларни фош этишга қаратилган кечиктириб бўлмас тезкор-тергов тадбирларини ўтказиши, жумладан ҳодиса жойини кўздан кечириш ҳамда далилларни аниқлаш ва олишда бевосита қатнашиши, прокуратура органларида мавжуд криминалистик-техника воситаларини ҳисобини юритиши, уларнинг бутлиги ва созлигини, шунингдек, улардан самарали фойдаланишни назорат қилиши, хизматда фойдаланиш учун зарур бўлган замонавий криминалистик техника

[5] Ўзбекистон Республикаси Бош прокурорнинг 2021 йил 12 июлдаги «Ўзбекистон Республикаси Бош прокуратурасининг Прокуратура органлари тергов тармоқлари фаолияти устидан назорат бошқармаси тўғрисидаги Низомни тасдиқлаш ҳақида»ги 243-сонли буйруғи.

воситаларига эҳтиёжини ўрганиб, тегишли таклифлар киритиши, қуйи прокуратуралар прокурор-криминалистларнинг фаолиятини мувофиқлаштириб бориши, уларга амалий ёрдам кўрсатиб, назорат қилиб боришни таъминлаш вазифалари юклатилган.

Фикримизча, Академияда янги ташкил этилган Институт прокурор - криминалистлари ваколатлари билан прокруатура органлари тергов тармоқлари фаолияти устидан назорат тармоғи прокурор-криминалистлари ваколатларини бир-бирига мос тарзда мувофиқлаштириш, прокурор-криминалистга хос бўлмаган айрим ваколатларни чиқариш мақсадга мувофиқ.

Жумладан, прокурор-криминалистлар экспертиза ўтказиш ваколатига эга бўлиши унинг ҳуқуқий мақоми нуқтаи назардан тўғри келмайди. Чунки, экспертизани шахсан эксперт мақомини олган, экспертлик вазифани амалга ошириш учун махсус малака ва рухсатномага эга бўлган муайян соҳа мутахассиси экспертиза ўтказиши мумкин.

Прокурор-криминалистга экспертиза ваколатини бериш фикримизча ноўрин бўлади, деб ҳисоблаймиз. Чунки, прокурор-криминалист ҳам терговда иштирок этиб, ҳам экспертизани ўзи ўтказиши ишнинг келгусида холисона олиб борилишига тўсқинлик қилишига, келгусида ўтказилган экспертиза тадқиқоти натижасида олинган далиллар бўйича суд томонидан ҳуқуқий баҳо берилишида айрим муаммолар келтириб чиқариши мумкин.

Келгусида, Рақамли криминалистика илмий-тадқиқот институтида фаолият юритадиган прокурор-криминалистлар экспертиза ўтказиш ҳуқуқини марказнинг бошқа ходимларига ёки прокурор-криминалист экспертиза ўтказиш ваколатига эга бўлган штатида фаолият кўрсатаётган ходимнинг лавозимни эксперт-криминалистга ўзгартириш ва прокурор-криминалист ваколатидан экспертиза ўтказиш ваколатини чиқариш таклиф қилинади.

Келгусида, бундай номувофиқликларни турли талқинларни олдини олиш мақсадида, прокурор-криминалистнинг процессуал ва криминалистик фаолияти бўйича уларнинг ҳуқуқий мақомини аниқ тартибга солишни назарда тутувчи нормаларни Ўзбекистон Республикаси “Прокуратура тўғрисида”ги Қонунига, амалдаги Жиноят-процессуал кодексида қатъий белгилаш таклиф қилинади.

Шу билан бирга, прокурор-крминалистларнинг фаолиятини тартибга солувчи алоҳида Бош прокурорнинг янги буйруғини қабул қилишни лозим бўлади.

Прокурор–криминалистлар институтининг ривожланиш тенденцияларини амалга ошириш ва замонавий ҳолатини янги босқичга янада кўтариш учун мамлакатимиз томонидан қабул қилиниши кўзда тутилган янги Жиноят-процессуал кодексида унинг ҳуқуқий мақомини белгилаш, жиноят ишларини сифатли тергов қилинишини таъминлашда уни жиноят процессининг мустақил иштирокчиси сифатида қонунан мустаҳкамлашни лозим деб ҳисоблаймиз.

Ҳозирги кунда Ўзбекистон Республикаси Бош прокуратурасининг прокуратура органлари тергов тармоқлари фаолияти устидан назорат бошқармасининг асосий фаолияти йўналишларидан бири бўлган криминалистик фаолият бўйича алоҳида штат ташкил қилиниши лозим бўлсада, 2020 йилда 28 сентябрдан бошқармадаги катта прокурор лавозими бошқарма катта прокурор-криминалистига ўзгартирилиб, ушбу штатга яна қўшимча иш ҳажми юклатилган.

Оқибатда прокурор-криминалистга юклатилган муҳим вазифалар ижросида муаммолар кузатилаётганлиги маълум бўлган.

Мазкур муаммоларни бартараф қилиш мақсадида, Бош прокуратурада прокурор-криминалистлардан иборат гуруҳ фаолияти юритиши учун ихтисослаштирилган “Криминалистика маркази”ни ташкил қилиш таклиф этилади.

Марказда замонавий криминалистика лабораторияси, терговнинг илғор техника ва технологияларидан иборат бўлган илмий-техник воситалар, терговчи, прокурор-криминалистлар жиноятларни фош этишда фойдаланиши учун янги замонавий техник жиҳозлари бўлган чемоданлар, рақамли далиллар қатнашган жиноят ишларининг фош этилиш ва терговига оид компьютер техника воситалар билан тўлиқ ҳажмда жиҳозлаш таклиф қилинади.

Сифатли терговни ташкил этиш орқали фуқароларнинг ҳуқуқ ва эркинликлари таъминланади, жиноят ҳақиқатининг адолатли таъминланишига хизмат қилади.

АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДА КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ ВА ҚЎЛЛАШ

Камалов Мадрасилла Эркинович
ИИВ Академияси рақамли технологиялар
ва ахборот хавфсизлиги кафедраси катта ўқитувчиси.

Аннотация: *ахборот технологиялари соҳасида киберхавфсизликни ривожлантириш ва қўллашни ўрганишнинг долзарблиги ахборот тизимлари кундалик ҳаётимизнинг ажралмас қисми бўлиши ва замонавий дунёда муҳимлигини ортишидир. Ушбу мақоланинг мақсади ахборот технологиялари соҳасида киберхавфсизликни ишлаб чиқиш ва қўллашни батафсил таҳлил қилишдир. Киберхавфсизликнинг асосий жиҳатлари, масалан, зарарли дастурлардан ҳимоя қилиш, тармоқ хавфсизлигига таҳдидлар, аутентификация ва маълумотларни шифрлаш, шунингдек, ахборот технологиялари хавфсизлигининг ташкилий жиҳатлари кўриб чиқилган.*

Таянч сўзлар: *киберхавфсизлик, ахборот кибержиноятлари, Internet, ахборот тизимлари, технологиялар, замонавий дунё.*

Аннотация: *актуальность изучения развития и применения кибербезопасности в сфере информационных технологий особенно важна в современном мире, где информационные системы являются неотъемлемой частью нашей повседневной жизни. Целью данной статьи является подробный анализ развития и методов применения кибербезопасности в сфере информационных технологий. Рассмотрены основные аспекты кибербезопасности, такие как защита от вредоносного программного обеспечения, угрозы безопасности сети, аутентификация и шифрование данных, а также организационные аспекты безопасности информационных технологий.*

Ключевые слова: *кибербезопасность, информационные киберпреступления, Интернет, информационные системы, современный мир, технологии.*

Бугунги кунда глобал ахборот майдонида кибер макон билан боғлиқ янгидан-янги таҳдидлар юзага келмоқда. Шу боис виртуал оламдаги ҳужумлардан ҳимояланиш масаласи дунё ҳамжамиятини жиддий ташвишга солмоқда. Рақамли экотизимга таянадиган бугунги технологик ривожланган даврда киберхавфсизлик бўйича мустаҳкам чора-тадбирларни таъминлаш зарурати муҳим аҳамиятга эга. Кибертаҳдидлар табиатан турлича бўлиб, ўзаро боғланган тизимларимиздаги заифликлардан фойдаланишга доимо интилаётган зарарли шахслар сони ортиб бормоқда.

Компьютерлар сонининг кўпайиши ва Интернетнинг ривожланиши билан хавфсизликни бузиш билан боғлиқ янги таҳдидлар пайдо бўлмоқда. Кибержиноятчилар муҳим

маълумотларга рухсатсиз кириш учун тизимлар ва тармоқлардаги заиф томонлардан фаол фойдаланган ва фойдаланишда давом этмоқдалар.

Бу жисмоний шахслар учун ҳам, ташкилотлар ва давлатлар учун ҳам жиддий оқибатларга олиб келиши мумкин. Шунинг учун киберхавфсизликни ўрганиш ва қўллаш устувор вазифадир. Бу сизга маълумотларнинг оқиши ва рухсатсиз ишлатилишини олдини олиш, шунингдек тизимлар ва тармоқларни зарарли дастурлардан ва хакерлик ҳужумларидан ҳимоя қилиш имконини беради [2].

Ахборот технологиялари (АТ) соҳасида киберхавфсизликнинг муҳимлигини англаб етиш компаниялар ва ташкилотлар орасида тобора кўпайиб бу масалага катта эътибор берилмоқда. Ахборот ресурсларининг ишончли ҳимоясини таъминлаш учун киберхавфсизлик бўйича мутахассисларни ёлланган ҳолда махсус бўлимлар, бошқармалар очилмоқда. Бундан ташқари, киберхавфсизликни ўрганиш таҳдидлардан ҳимоя қилиш учун янги усул ва технологияларни ишлаб чиқишга ёрдам беради. Кибержиноятчилар ўз усулларини доимий равишда такомиллаштириб борадилар, шунинг учун доимо олдинда бўлиш ва янги таҳдидларга мослашиш муҳимдир. Шундай қилиб, ахборот технологиялари соҳасида киберхавфсизликни ривожлантириш ва қўллашни ўрганишнинг долзарблиги аниқ. Бу бизнинг рақамли ҳаётимизни ҳимоя қилишга ва фойдаланувчилар, ташкилотлар ва давлатларнинг хавфсизлигини таъминлашга ёрдам беради [3].

Ахборот технологиялари соҳасида киберхавфсизликни ишлаб чиқиш ва қўллаш бизнинг давримизнинг энг долзарб вазифаларидан биридир. Интернет ва рақамли технологиялардан фойдаланишнинг кўпайиши туфайли киберхавфсизлик соҳасидаги таҳдидлар кенг тарқалиб янада жиддийлашмоқда. Киберхавфсизликни ривожлантиришнинг асосий мақсадларидан бири ахборот тизимларини ҳар хил турдаги киберҳужумлардан ва хакерлардан ҳимоя қилишни таъминлашдир [5]. Ахборот хавфсизлиги ахборот-коммуникация технологиялари ривожланишининг ажралмас қисми бўлиб ва турли ахборот технологияларининг тизимлари ва веб-хизматларнинг ишончи ва барқарорлигига таъсир қилувчи асосий омиллардан бири эгалигини тушуниш муҳимдир.

Ахборот технологиялари соҳасидаги киберхавфсизлик нафақат техник ҳимоя воситаларини, балки ташкилий чора-тадбирлар, ҳуқуқий нормалар ва таълим дастурларини ҳам ўз ичига олган комплекс ёндашувга асосланади. Бироқ, асосий компонент киберҳужумларни аниқлаш ва олдини олиш учун инновацион

технологиялар ва усулларни ишлаб чиқишдир. Киберхавфсизлик бўйича мутахассислар маълумотларни шифрлашнинг янги алгоритмлари, бошқариш ва мониторинг тизимлари, шунингдек аутентификация ва фойдаланувчини идентификация қилиш усулларини яратиш устида ишламоқдалар. Шунингдек, улар фойдаланувчиларнинг хатти-ҳаракатларидаги заифликларни бартараф этиш ва махфий маълумотларнинг тарқалишини олдини олиш учун ижтимоий муҳандислик ва фишингга қарши янги тизимларни ишлаб чиқмоқдалар.

Киберхавфсизлик ландшафти доимо янги таҳдид ва муаммоларга мослашиб, ривожланиб боради. Корхоналар, жисмоний шахслар ва ташкилотлар учун ўзларининг киберхавфсизлик амалиётларида хабардор ва фаол бўлишлари жуда муҳимдир. Киберхавфсизлик соҳасидаги муҳим жиҳатларни ўрганиб чиқиб, биз хавф-хатарларга самарали қарши тура оламиз ва рақамли ҳимоямизни мустаҳкамлай оламиз.

Бироқ, киберхавфсизликнинг ривожланиши кибержиноят-чилик ривожланишидан ажралган ҳолда ривожлана олмайди. Кибержиноятчилар ўзларининг ҳужум усулларини доимий равишда такомиллаштириб борадилар ва шунинг учун ахборот хавфсизлигини доимий равишда янгилаб туриш ва такомиллаштириш зарур. Бу мутахассислар янги таҳдидларга тезда жавоб бериш ва уларнинг пайдо бўлишининг олдини олишнинг ягона йўли. Шундай қилиб, ахборот технологиялари соҳасида киберхавфсизликни ишлаб чиқиш ва қўллаш ахборот хавфсизлиги ва АТ инфратузилмасининг ишончли ишлашини таъминлаш учун зарур шартдир. Бу турли тузилмалар, жумладан, давлат идоралари, компаниялар, таълим муассасалари ва умуман жамиятнинг ҳамкорлигини талаб қилади. Фақат биргаликда ишончли ва хавфсиз ахборот маконини яратишимиз мумкин.

Инновацион технологиялар ва киберхавфсизликни қўллаш усуллари замонавий ахборот технологиялари соҳасида муҳим рол ўйнайди. Онлайн жиноятчилик ва хакерлик ҳужумлари кенг тарқалган дунёда ахборот хавфсизлигини таъминлаш ҳар қандай ташкилот ёки шахс учун заруратдир. Киберхавфсизликни таъминлаш учун ишлатиладиган инновацион технологиялардан бири бу сунъий интеллект (СИ) технологияси. Ва у ҳужумларни аниқлаш ва олдини олиш, шунингдек, шубҳали фаолиятни аниқлаш учун катта ҳажмдаги маълумотларни таҳлил қилиш учун ишлатилиши мумкин. Бу ташкилотларга таҳдидларга тезда жавоб

бериш ва мумкин бўлган даражада зарарли оқибатларни минималлаштириш имконини беради.

Яна бир инновацион техника-бу блокчейндан фойдаланиш. Блокчейн-бу маълумотларнинг хавфсизлиги ва ўзгармаслигини таъминлайдиган марказлаштирилмаган маълумотларни сақлаш тизими. Бу блокчейнни ахборот технологияларида ахборот хавфсизлиги учун идеал воситага айлантиради. Блоскчейн рақамли идентификаторларни сақлаш ва текшириш, шунингдек молиявий операцияларни амалга оширишда ёки махфий маълумотларни узатишда хавфсизликни таъминлаш учун ишлатилиши мумкин. Машинани ўрганиш (англ. machine learning, ML) технологиялари ҳам инновацион киберхавфсизлик техникасининг муҳим қисмидир. Машинани ўрганиш компьютер тизимларини маълумотлардаги нақшларни таниб олиш ва таҳлил қилишга ўргатади, бу эса таҳдид ва тажовузкорларни самарали аниқлаш имконини беради. Масалан, машинани ўрганиш тизимлари веб-трафикни автоматик равишда таҳлил қилиши ва хакерлик уринишлари ёки фишинг ҳужумлари каби шубҳали ҳаракатларни аниқлаши мумкин [2].

Ахборот технологиялари соҳасида киберхавфсизликни қўллашнинг инновацион технологиялари ва усуллари маълумотлар ва тармоқларни зарарли фаолиятдан ҳимоя қилишда муҳим рол ўйнайди. Сунъий интеллект, блокчейн ва машинани ўрганиш технологияларидан фойдаланиб, биз ахборот хавфсизлигини таъминлашимиз ва кибертаҳдидларга қарши самарали курашишимиз мумкин.

КРИПТОАКТИВЛАРНИ ТИЖОРАТДА ПОРА ЭВАЗИГА ОҒДИРИБ ОЛИШ ЖИНОЯТИНИНГ ПРЕДМЕТИ СИФАТИДА ТАН ОЛИШ МУАММОЛАРИ

Облакулов Давлат Олтинбоевич
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси ўқитувчиси, мустақил изланувчи

Бизга маълумки, жиноятнинг предмети жиноят таркибининг факультатив белгиси бўлиб, у жиноят таркибида муҳим аҳамиятга эга ҳисобланади.

Профессор Н.И.Коржанский жиноят предмети бу –маълум бир моддий объект бўлиб, унда ижтимоий муносабатларнинг айрим жиҳатлари, хусусиятлари (жиноят объекти) намоён бўлади, унинг

таъсири орқали ушбу ижтимоий муносабатлар соҳасига ижтимоий хавфли зарар етказиладидеган таърифни берган[1].

Профессор А.В.Наумов эса, жиноят содир этиш воситаси сифатида жиноятчи томонидан жиноят содир этиш учун фойдаланадиган нарсаларни тушунишни таклиф қилади[2].

Шуни айтиш мумкинки, юқорида қайд қилинган таърифлар жиноят ҳуқуқи назариясида энг кенг тарқалган.

М.Усмоналиев жиноятнинг предмети - у туфайли ёки унинг муносабати билан жиноят содир қилинадиган объектив ҳаётда мавжуд бўлган моддий маънодаги нарсалардир[3] деб такидлайди.

Юқоридагиларга кўра, жиноят пердмети- моддий тусдаги нарса, жисм бўлиб, жиноят содир этаётган шахснинг жиноий қилмиши натижасида унга бевосита таъсир кўрсатилади. Шу билан бирга, жиноятнинг объекти билан предмети бир хил тушунча эмас, яъни жиноят предмети жиноят объекти каби ижтимоий муносабат ҳисобланмайди.

Жиноят ҳуқуқида пора предмети деганда одатда мансабдор шахс нима эвазига оғдирилаётгани ёки у хизмат юзасидан пора берувчи манфаатларини кўзлаб қандайдир хатти-ҳаракат содир этгани ёки содир этмаслиги учун қандай ҳақ олаётгани тушунилади[4].

Тижоратда пора эвазига оғдириб олиш жиноятининг предмети-нодавлат тижорат ва бошқа нодавлат ташкилот мансабдор шахсига турли усул ва йўллар билан бериладиган мулкий қийматга эга бўлган буюмлар, жумладан пул бўлиши мумкин.

Тижоратда пора эвазига оғдириб олиш предмети ҳақида гап кетганда бу борада қонун чиқарувчи ЖКнинг 192[9]- моддаси диспозитциясида бевосита кўрсатган моддий қимматлик ёки мулкий манфаатдорликнитушуниш мумкин.Демак, мазкур жиноят предмети мулкий манфаат хусусиятига ёки муайян қийматга эга бўлиши талаб этилади.

Бунда иккинчи томон (нодавлат тижорат ёки нодавлат ташкилот мансабдор шахси) ундан қандайдир мулкий ёки бошқача мулкий характердаги манфаат кўриши лозим. Агар нодавлат тижорат ташкилотининг ёки бошқа нодавлат ташкилотининг мансабдор шахсига бирор моддий қимматликлар берилмаса ёки

---

[1]Коржанский Н. И. Объект и предмет уголовно-правовой охраны. М., 1980.

[2] Наумов А. В. Российское уголовное право. Общая часть. М., 1997.

[3] М.Усмоналиев Жиноят ҳуқуқи (Умумий қисм) Дарслик. Т.: “Янги аср авлоди” 2005. Б.160.

[4] Зуфаров Р.А. Порахўрлик учун жиноий жавобгарлик. // Масъул муҳаррир: ю.ф.д.профессор М.Х.Рустамбоев. - Т/.ТДЮИ., 2004.Б.29

мулкий манфаатдор этилмаса ёки ушбу ташкилотлар мансабдор шахси шундай моддий ёхуд мулкий манфаатдор бўлмаса ушбу қилмишни Жиноят Кодексининг 192[9]-моддаси билан квалификация қилиб бўлмайди.

Қайд қилиш керакки, ЖКнинг 192[9]-моддасида кўрсатилган тижоратда пора эвазига оғдириб олиш жиноятининг предмети ЖКнинг 210-моддаси пора олиш ва ЖКнинг 211-моддаси пора бериш, шунингдек, ЖКнинг 213,214-моддалари ҳамда 192[10]-моддасида назарда тутилган жиноятларнинг предмети билан бир хил бўлиб, бунда пора предмети сифатида моддий қимматлик сифатида пул, қимматбаҳо қоғозлар, кўчар ва кўчмас мулк ҳуқуқини ўтказиш, моддий бойликлар, шунингдек, пора оладиганга қайтармаслик шарти билан, лекин мулкий моҳиятга молик бўлган (масалан, таъмирлаш, қурилиш, қайта тиклаш ишларини бажариш ва бошқалар) хизматлар пора предмети бўлиши назарда тутилган.

Шунга кўра, ЖКнинг 192[9]-моддаси диспозициясидан келиб чиқиб, жиноят предметига моддий бойликлар, мулкий фойда, мулкий тусга эга фойдани киритиш мумкин. Бунда:

а) ***моддий бойликларга*** (пул, қимматли қоғозлар, акциялар, облигациялар бошқа мулк, шу жумладан валюта қимматликлари, қимматбаҳо металлар, нодир тошлар, кўчар ва кўчмас мулклар (ЎзРес ФКнинг 83-моддасига асосан мол-мулк фуқаролик ҳуқуқлари объекти сифатида кўчмас мулкка ва кўчар мулкка бўлинади деб белгиланган) уй ҳайвонлари, жумладан от, чорва моллари, хусусан, қорамол, қўй, эчки ва ҳ.к.)

в) ***мулкий фойда*****:** бунда нодавлат тижорат ва бошқа нодавлат ташкилот мансабдор шахсига текин тарзда ва (ёки) очиқчасига ўта пасайтирилган нархда амалга ошириладиган турли хил хизматлар ва (ёки) моддий наф келтириш тушунилади (масалан, кам фоизли кредит бериш, қарзидан воз кечиш, бошқа шахслар олдидаги мажбуриятларни бажариш)

с) ***мулкий тусга эга фойда:*** масалан, йўл чипталар олиб бериш, шу жумладан санаторий ёки туристик йўлланмаси (бепул ёки арзон нархларда), автомашинага текин бензин, газ (метан, пропан) қуйиб бериш, автотранспорт воситасини текинга таъмирлаб бериш, автотранспорт воситаларини вақтинча фойдаланиш учун бериш, қурилиш, таъмирлаш, қайта тиклаш, реставрациява бошқа ишларини бажариш тушунилади.

Мулкий характердаги хизмат ҳар қандай ҳаракат ёки маълум бир пул қийматига эга бўлган, шунингдек, одатдагидек пуллик ва

шахсий бўлмаган ҳар қандай фаолиятни амалга ошириш бўлиши мумкин. Шу билан бирга, мазкур хизмат натижасида баъзан мансабдор шахс моддий натижага эга бўлмаслиги мумкин. Масалан юридик ёки тиббий хизмат ёхуд бошқа консалтинг хизмат аммо шунга қарамай, у пора олганлар учун маълум бир харажат ва тўлов аҳамиятга эга ва шунинг учун у порахўрлик передмети сифатида қаралади.

Пора предмети мулкий ҳуқуқлар бўлган ҳолларда, бундай ноқонуний ҳақ олган мансабдор шахс бошқа бировнинг мол-мулкига ўз мулки сифатида эгалик қилиш ёки тасарруф этиш, қарздордан мулкий мажбуриятларни ўз фойдасига бажаришни талаб қилиш, ҳужжатиз қимматли қоғозлардан ёки рақамли ҳуқуқлардан фойдаланишдан даромад олиш ва ҳ.к. тушуниш мумкин.

Бу борада Л.П.Тумаркина яхши фикрни илгари суради, унга кўра, мулкий характердаги хизматни умумий тушунчасидан ушбу хизмат нархига ўтказиш керак деб ҳисоблайди. Тақдим этилаётган хизмат мулкий хусусиятга эга ва шунга мос равишда ушбу хизмат учун тўлов унинг нархи миқдорини белгилайди. Хизмат нархи ҳар доим нархнинг универсал эквиваленти, яъни пул орқали аниқланади[5].

Биз ҳам олимани фикрига қўшилган ҳолда шуни айтишимиз мумкинки, тижоратда пора эвазига оғдириб олишда мулкий характердаги хизматни пул кўринишида баҳоланиши жиноятни квалификациясига ҳам таъсир қилади.

Хусусан, дейлик пора эвазига уйни таъмирдан чиқарди, биз бу борада мутахссис хулосасаси асосида таъмирлаб бериш хизматини нархини аниқласак, бу кўп миқдор ва жуда кўп миқдор билан квалификация қилиш учун асос бўлади. Бу борада Ўзбекистон Республикаси Олий суди Пленумининг 1999 йил 24 сентябрдаги 19-сонли “Порахўрлик ишлари бўйича суд амалиёти тўғрисида”ги қарорида жиноятни тавсифлаш пора миқдорига боғлиқлигини эътиборга олган ҳолда, ҳар қандай пора предметининг қиймати товарларнинг нархи, хизматларнинг ҳақи ёки тарифи асосида, улар бўлмаганда экспертлар хулосаси асосида аниқланади деб кўрсатилганлиги фикримизни тасдиқлайди.

Агар тижорат пора эвазига оғдириб олиш жинояти предмети муомаладан чиқарилган ёки муомалада чекланган мулк бўлса, у ҳолда ушбу ҳаракат ЖК махсус қисмининг тегишли моддалари

[5] Л.П.Тумаркина Уголовная ответственностьзакоммерческий подкупдиссертации на соискание ученой степеникандидата юридических наукМосква2007

бўйича қўшимча равишда жиноятлар мажмуи бўйича квалификация қилиниши керак. Масалан, ўқотар қурол, гиёҳвандлик воситалари ёки психотроп моддалар кўринишидаги порахўрликни ноқонуний ўтказиш ёки олиш ҳолатларида, шунингдек, ЖК 247, 273-моддаларида назарда тутилган жиноят содир этилади.

Жиноят ҳуқуқ назариясида умуман пора предмети ҳақида фикрлар мунозарали бўлсада, бироқ мамлакатимиз Жиноят Кодексида моддий қимматликлар ёки мулкий манфаатдорлик пора предмети бўлиши мумкинлиги белгиланган.

Бироқ, адбиётларда иккита мансабдор шахс ўртасида ўзаро ёрдам кўрсатиш шаклидаги хизматлар ҳам пора предмети бўлиши мумкинлиги ҳақида фикрлар ҳам бор. Шунингдек, интеллектуал мулк ҳам пора предмети бўлиши мумкин деган фикрлар учрайди. Масалан, профессорлар Р.А.Зуфаров, Б.Д.Ахрароввa У.М.Мирзаевлар“интелектуал мулк порахўрлик жиноятларининг предмети бўлиши мумкин, деган фикрга қўшилиш мумкин, чунки бундай мулк ўз эгасига моддий манфаат келтириши мумкин.Пора сифатида интеллектуал мулкни қабул қилаётган мансабдор шахс, кейинчалик бундай интеллектуал мулкдан моддий манфаатдор бўлишини мақсад қилган ҳолларда бу мулк жиноятнинг предмети бўлиши мумкин”,- деб қайд қилади[6].

Юқоридақайд қилган Олий суднинг Пленум Қарорига асосан назаримизда интеллектуал мулкни баҳолаш қиймати мавжуд, шу сабабли, Р.А.Зуфаров, Б.Д.Ахраров, У.М.Мирзаевларнинг фикрлари асосли кўринади. Шунга кўра, биз ҳам интелектуал мулкни пора предмети деб қараш фикрига қўшиламиз.

Умуман олганда жиноят ҳуқуқида порахўрлик ва тижоратда пора эвазига оғдириб олиш жиноятининг предмети ҳақида баҳсли фикрлар мавжуд. Масалан, В.Е.Зварыгин, А.С.Кондаковлар ушбу жиноят предметига ҳар қандай бошқа мулк (саноат товарлари, озиқ-овқат, кўчмас мулк), шунингдек моддий хизматлар (дам олиш, ҳордиқ чиқариш, маиший эҳтиёжларни қондириш учун тўлов) киритади[7].

И.Кузнецова[8] тижоратда пора эвазига оғдириб олишжиноятининг предметисифатида пул, қимматли қоғозлар,

---

[6]Р.А.Зуфаров, Б.Д.Ахраров, У.М.Мирзаев Коррупция. Қонун. Жавобгарлик. Монография. Масъул муҳаррир: ю.ф.д., профессор М.Х.Рустамбоев. - Т.:ТДЮИ.-2011.-272 б., Б.123.

[7] В.Е.Зварыгин, А.С.КондаковУголовно-правовые проблемы привлечения к ответственности за преступления коррупционной направленностина примере коммерческого подкупа//Экономика и Право 2021. Т. 31, вып. 4 С.647-653

[8] И.А.Кузнецова Ответственность за коммерческий подкуп Авторефератдиссертации на соискание ученой степеникандидата юридических наук Москва-2003

бошқа мулк ва мулкий характердаги хизматларни тан олади.Бундай ёндашувни профессор А.И.Рарога[9] билдирган.

Умуман олганда аксарият жиноят ҳуқуқий адабиётларда[10]ҳам тижоратда пора эвазига оғдириб олиш жиноятининг предмети сифатида пул, қимматли қоғозлар, бошқа мулк ва мулкий характердаги хизматларни тан олади.

Демак, қайд қилинган ишлардамазкур жиноятнинг предмети сифатида фақат мулкий ва мулкий характердаги хизматлар назарда тутилмоқда. Номоддий наф эса передмет доирасига киртилмаган.

Бироқ, олимлар орасида моддий ёки ҳарқандай наф ёки афзалликни тижоратда пора эвазига оғдириб олиш жиноятининг передмети бўлиши мумкин деб ҳисоблайдиганлари мавжуд. Масалан П.В.Никонов[11] тижоратда пора эвазига оғдириб олиш жиноятини пора предмети сифатида мулкий ва номулкий имтиёзлар (афзаллик)ни тан олишни таклиф қилади.

П.В.Никонов мазкур таклифни илгари суришда коррупцияга қарши халқаро стандартлар ва хорижий давлатларнинг тажрибаси инобатга олган.

Л.П.Тумаркина кўриб чиқилаётган жиноятнинг предмети номоддий мулк эҳтиёжларини қондиришга қаратилган ҳаракатлар ёки муайян фаолиятни амалга ошириш деб тушуниладиган мулкий бўлмаган имтиёзлар сифатида ҳам тан олиниши мумкин деб ҳисоблайди[12].

Е.Н.Карабанова порахўрлик предметига ҳар қандай ноқонуний афзалликларни, шу жумладан, номоддий афзалликларни, уларнинг

---

[9] Уголовное право России. Части Общая и Особенная: учебник / под ред.А. И. Рарога. — 10-е изд., перераб. и доп. — Москва: Проспект, 2018. —944 с. С.633-634.;

[10] Преступления в сфера экономика: учебник для академического бакалавриата/ под ред.Н.Г.Иванов.- М.: Издательство Юрайт, 2018,-168с.- Серия: Бакалавр. Академический курс. С.155-156.; Уголовное право. Особенная часть: учебник для прикладного бакалавриата/В.Б.Боровиков, А.А.Смердов; под ред. В.Б.Боровикова. 3-е. изд., перераб. и.доп. М: ИздательствоЮрайт 2016.-364 с.С.143-145; Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков [и др.]; под ред. А. В. Бриллиантова. — 2-е изд. — Москва: Проспект, 2017.Т. 2 -704 с; *Квалификация*деяния. Тактика и методика расследования коррупционных преступлений. Настольная книга следователя: учеб, пособие для студентов вузов, обучающихся по направлению «Юриспруденция» и специальности «Правоохранительная деятельность» / [Д.И. Аминов и др.]; под ред. Н.Д. Эриашвили. — 2-е изд., перераб. и доп. — М.: Юнити-Дана, 2019. - 319 с.С.98.

[11]П.В.Никонов Теоретические основы уголовно-правового противодействия преступлениям, связанным с дачей и получением взятки и иными видами незаконного вознаграждения Диссертация на соискание ученой степени доктора юридических наук Москва – 2024 568 с.

[12] Тумаркина Л.П. Уголовная ответственностьзакоммерческий подкупдиссертации на соискание ученой степеникандидата юридических наукМосква2007

баҳоланадиган бозор қийматига эга ёки йўқлигидан қатъий назар киритиш керак деган ғояни илгари сурган[13].

Бу борада профессор Р.А.Зуфаровнинг фикрлари қизиқиш уйғотади, унинг фикрига кўра,пора берувчи фоҳишанинг жинсий (олим томониданбошқа сўз ишлатилган) хизматларига ҳақ тўласа, пора олувчи эса бу хизматлардан фойдаланса, буларни пора предмети деб эътироф этиш лозим. Биз биламизки, бундай фикр олимлар ва амалиётчилар ўртасида тўлиқ қўллаб-қувватланмайди, лекин ҳуқуқий адабиётларда ушбу назариянинг ҳам ўз тарафдорлари бор деб, профессор Р.А.Зуфаровўзининг фикрини В.М.Хомичнинг мансабдор шахсга аён бўлган ҳолда унга кўрсатилган жинсий хизматлари иктисодий жихатдан фойдали дейишга асослар етарли деган фикри билан асослайди[14].Аммо назаримизда профессор Р.А.Зуфаровнинг фикри баҳсли кўринади, чунки, биринчидан мамлакатимизда қонунан бунақа турдаги хизматнинг ўзи йўқ (бундан кейин бўлмаслигини истаймиз албатта), иккинчидан бизнингчабу ерда олим барибир мулкий характердаги тўловни, юқорида санатория ёки саёҳатга бепул чипта олиб бериш каби хизматни назарда тутмоқда холос.

Лекин агар тасаввур қиладиган бўлсак, пора берувчи аёл нодавлат тижорат ва бошқа нодавлат ташкилот мансабдор шахсига порани ўрнига жинсий хизмат таклиф қилса, пора олувчи эса бу хизматлардан фойдаланса, буларни пора предмети деб эътироф этиб бўладими йуқми мана буниҳақиқий баҳсли, айни пайтда мунозарали масала деса бўлади.

Агарда хизмат бўйича тобе бўлган аёлни у манфаатдор бўлган хизмат юзасидан ҳаракатларни бажариш ёки бажармаслик хавфи остида жинсий алоқа қилишга мажбурлаш Жиноят Кодекси 121-моддасига биноан аёлни жинсий алоқа қилишга мажбур этиш учун жавобгарликка асос ҳисобланади.

1884 йилда немис олими А.Фейербах "Порахўрлик тўғрисида"ги асарида пора предмети (шунингдек, тижоратда пора эвазига оғдириб олиш) "умуман шаҳвонийликни қондириш ва ўзи учун хизмат қиладиган ҳар қандай нарса бўлиши мумкин, деб

---

[13] Карабанова Е.Н. Пробелы российского законодательства, регламентирующего уголовную ответственность за коррупцию // Пробелы в российском законодательстве. 2015. № 5. С. 109-111

[14] Зуфаров Р.А. Порахурлик учун жиноий жавобгарлик. // Масьул муҳаррир М.Х. Рустамбоевюридик фанлари доктори, профессор. - Т/.ТДЮИ., 2004. 221 - б.// Р.А.Зуфаров Порахўрликка қарши курашнинг жиноят-ҳуқуқий ва криминологик жиҳатлари: назария ва амалиёт ю.ф.д илмий даражасини олиш учун ёзилган диссертацияси Т.:2005

таъкидлаган, бунда буюртма ваъдаси, пора бериш, хизмат учун тўлов шаклида унинг танасининг сўровчи бир хизмат" деган[15].

Жинсий хизматларни пора предмети сифатида тан олиш масаласи жиноят ҳуқуқи назариясида узоқ вақтдан бери кўтарилган. Айтганча, мутахассислар "жинсий хизматлар" ни пора предмети сифатида тан олиш имкониятини муҳокама қилмоқдалар. Бу борада В.В.Качалов[16] ҳамда юқорида қайд қилиб ўтганимиздек профессорР.А.Зуфаров[17]нинг (жинсий жиноятлар бўйича Ф.Тохиров ишларини кўриш мумкин[18]) ишларида батафсилроқ кўришимиз мумкин, аммо мамлакатимиз қонунчилигида номоддий ҳақ (жумладанжинсий алоқа қилиш) умуман порахўрлик жиноятининг, шунингдек, тижоратда пора эвазига оғдириб олишнинг передмети бўлмайди.

Шунингдек, пора предмети сифатида хусусан ижобий тавсиянома, тақриз, тавсиянома бериш, нашрда чоп эттириш, телевидения орқали намойиш этиш ва бошқалар бўлмайди.

Бу борада С.Д.Красноусов тижоратда пора эвазига оғдириб олишнинг предмети сифатида номоддий имтиёзлар ва афзалликларни тақдим этиш, масалан, лавозимга тайинлаш, диссертацияларни ҳимоя қилиш, чиройли серияли автомобил рақамларини беришни тан олади[19] .

Назаримизда реклама, диссертация учун ижобий тақризни, мақола ёки монография ёзиш, илмий асарларга ҳаммуаллифликка қўшилишни ҳам тижорат пора предмети сифатида қараш мақсадга мувофиқ ҳисобланади.

Шунингдек, қайд қилиш лозимки, инста блогерлар томонидан ижтимоий тармоқда маҳсулотларни реклама қилиб беришни ҳам пора предмети сифатида қараш мумкин. Чунки, у ҳам мулкий хизматнинг бир тури ҳисобланади.

Кейинги вақтларда олимлар орасида баҳс-мунозараларга сабаб бўлаётган криптоактивларни пора пердмети сифатида киритилиши долзарб масалалардан бири бўлиб тирибди, бу борада миллий

---

[15] Приградов-Кудрин А. Нематериальная выгода и взяточничество // Право и жизнь. 1925. Кн. 7-8. С. 95.//Л.П.Тумаркина Уголовная ответственностьзакоммерческий подкупдиссертации на соискание ученой степеникандидата юридических наукМосква2007 С.52

[16] Качалов В. В. Сексуальные услуги как предмет взятки // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 4-2. С. 118—124.

[17] Р.А.Зуфаров Порахўрлик учун жиноий жавобгарлик. Монография. Масъул муҳаррир: ю.ф.д., профессор М.Х.Рустамбоев. - Т.:ТДЮИ.- 2004. 221б., / Р.А.Зуфаров Порахўрликка қарши курашнинг жиноят-ҳуқуқий ва криминологик жиҳатлари: назария ва амалиёт ю.ф.д илмий даражасини олиш учун ёзилган Дисс. Т.:2005

[18] Тохиров Ф. Жинсий жиноятлар ва уларни квалификация қилиш асослари. Монография. – Т.: ТДЮИ, 2006.

[19] Красноусов С. Д. Коммерческий подкуп какформа коррупции в частном секторе. М., 2014.С. 24

олимларимиздан Е.В.Коленко ўзининг тадқиқотида рақамли мулк ҳуқуқи ёки бошқа моддий манфаатлар (фойдалар) сифатида криптоактивлар пора предмети эканлигини аниқ тушунтириб берган[20]. Тадқиқотчи, криптоактивларни рақамли мулк ҳуқуқи ёки бошқа моддий неъматлар (фойдаларни) сифатида пора олиш ва бериш предмети деб эътироф этиш тўғрисидаги позицияни асослайди. Биз ҳам Е.В.Коленконинг илгари сурган фикрларига қўшиламиз, чунки бу ҳам пора бериш усулини олдини олишда долзарб масала ҳисобланади.

Шунга яқин фикрни профессор А.В.Куликов, О.А.Шелег[21], П.В.Никонов[22], М.М.Долгиева[23]каби олимлар ҳам билдириб, улар назарий жиҳатдан крипто-активларни порапредмети бўлиши мумкин деган хулосага келадилар.

Ўзбекистон Республикаси Президентининг 03.07.2018 йилдаги “Ўзбекистон Республикасида рақамли иқтисодиётни ва крипто-активлар айланмаси соҳасини ривожлантириш чора-тадбирлари тўғрисида”ги ПҚ-3832-сонли Қарорига кўра, а)крипто-актив мулкий ҳуқуқ ҳисобланиб, маълумотларнинг тақсимланган реестридаги рақамли ёзувлар йиғиндиси бўлган қиймати ва эгасига эга; б)крипто-активлар айланмаси соҳасидаги фаолият турлари қуйидагилардан иборат: майнинг; крипто-активлар айланмаси соҳасидаги хизматлар провайдерлар фаолияти; в)майнинг бу ҳисоблаш операцияларини бажариш орқали маълумотларнинг тақсимланган реестрини юритиш, блокларнинг яхлитлигини яратиш ва тасдиқлаш фаолиятидир[24].Шунга асосан бизнинг назаримиздабуни предмет сифатида баҳолаш мумкин.Бундан ташқари, крипто-актив баҳолаш қийматига эга.

Шундай қилиб, биз юқорида мамлакатимиз жиноят қонунида тижоратда пора эвазига оғдириб олиш жиноятининг предмети моддий ҳақ, шу билан бирга мулкий тусдаги турли хил хизматлар бўлиши мумкинлиги белгиланганлигини кўриб чиқдик. Бироқ, коррупцияга қарши халқаро стандартларда, жумладан, БМТнинг

---

[20] Батафсилроқ қаранг: Е.В.Коленко “Пора олиш учун жавобгарлик: ЎзбекистонРеспубликаси жиноят қонунчилигини халқаростандартларни ҳисобга олган ҳолдатакомиллаштириш истиқболлари” мавзусида юридик фанлар бўйича фалсафа фанлари доктори илмий даражасини олиш учун ёзилган диссертация Автореф. Т.:2023 Б.36

[21] А.В.Куликов, О.А.Шелег К вопросу расширения субъектного состава и предмета коммерческого подкупа (ст.204 УК РФ)//Криминалистъ. 2024. № 1 (46). С. 56—62 • Criminalist. 2024;1(46):56-62

[22] П.В.Никонов Теоретические основы уголовно-правового противодействия преступлениям, связанным с дачей и получением взятки и иными видами незаконного вознаграждения Диссертация на соискание ученой степени доктора юридических наук Москва – 2024 568 с.

[23] М.М.Долгиева Теоретические основания уголовной политики в сфере оборота криптовалюты Диссертация на соискание ученой степени доктора юридических наук Москва 2023

[24] https://lex.uz/docs/3806053 Кириш санаси 31.08.2024 йил

Коррупцияга қарши Конвенциясида, шунингдек, Шарқий Европа ва Марказий Осиё учун коррупцияга қарши бўйича Истанбул ҳаракат режаси 5-босқич мониторинг сўровномаларига кўра, “ноқонуний афзалликлар” термини остида номоддий неъматлар[25] ҳам пора предмети сифатида қаралиши лозимлиги белгиланган.

Ўзбекистон Республикасининг ФКга кўра, номоддий неъматлар жумласига: 1)интеллектуал фаолият натижалари; 2)хизмат ва тижорат сири; 3)шахсий номулкий ҳуқуқлар ва бошқа номоддий неъматлар; 4)шаън, қадр-қиммат ва ишчанлик обрўсини ҳимоя қилиш киритилган. Бу борада назаримизда тадқиқ қилаётган жиноятнинг предмети сифатида интеллектуал фаолият натижалари ҳамда тижорат сирини предмет сифатида қабул қилса бўлади, шахсий номулкий ҳуқуқлар ва бошқа номоддий неъматлар; шаън, қадр-қиммат ва ишчанлик обрўсини ҳимоя қилиш шахснинг бевосита ўзи билан боғлиқ бўлганлиги ҳамда уни шахсдан айри ҳолда мавжуд бўлмаслигини инобатга олиб, жиноят предмети сифатида қараш бизнинг фикримизча унчалик тўғри эмас.

Бу борада Ф.З.Джалилов ўзининг тадқиқотида интеллектуал фаолият натижалари, хизмат ва тижорат сири ҳам жиноят предмети сифатида қаралиши лозимлиги асослаган. Шунингдек, у жиноят предмети нафақат мулк ҳуқуқи асосида, балки фойдаланиш ва эгалик қилиш ҳуқуқи асосида ҳам берилиши мумкинлигини билдирган[26].

Юқоридаги фикрларни умумлаштириган ҳолда БМТнинг Коррупцияга қарши Конвенцияси талабларидан келиб, қолаверса, олимлар томонидан илгари сурилган фикрларни[27]таҳлил қилган

---

[25] Ўзбекистон Республикасининг Фуқаролик Кодекси 81-моддасига кўра, фуқаролик ҳуқуқларининг объектларига ашёлар, шу жумладан пул ва қимматли қоғозлар, бошқа буюмлар, мол-мулк, шу жумладан мулкий ҳуқуқлар, ишлар ва хизматлар, ихтиролар, саноат намуналари, фан, адабиёт, санъат асарлари ва интеллектуал фаолиятнинг бошқа натижалари, шунингдек шахсий номулкий ҳуқуқлар ва бошқа моддий ҳамда номоддий бойликлар киради.

[26] Батафсилроқ қаранг: Ф.З.Джалилов “Давлат органи, давлат иштирокидаги ташкилотёки фуқаролар ўзини ўзи бошқариш органихизматчисининг мулкий манфаатдорлиги биланбоғлиқ жиноий жавобгарлик” мавзусида ю.ф.ф.д (PhD) илмий даражасини олиш учун ёзилган дисс. Автореф. Т.:2023 Б.8.

[27] И.А.Кузнецова Ответственность за коммерческий подкуп Автореф.Дисс. на соискание ученой степеник.ю.н. Москва-2003, Э.С.Шимшилова Преступления коррупционной направленности, совершаемые в коммерческих организациях уголовно-правовое и сравнительно правовое исследование 12.00.08. Автореф.к.ю.н М.2019, Д.А.Кононов Злоупотребление полномочиями и коммерческийподкуп: уголовно-правовая характеристикаДисс. на соискание ученой степеник.ю.н. Москва – 2016;П.В.Никонов Теоретические основы уголовно-правового противодействия преступлениям, связанным с дачей и получением взятки и иными видами незаконного вознаграждения Диссертация на соискание ученой степени доктора юридических наук Москва – 2024 568 с.; Ф.З.Джалилов “Давлат органи, давлат иштирокидаги ташкилотёки фуқаролар ўзини ўзи бошқариш органихизматчисининг мулкий манфаатдорлиги биланбоғлиқ жиноий жавобгарлик” мавзусида ю.ф.ф.д (PhD) илмий даражасини олиш учун ёзилган дисс. Автореф. Т.:2023 Б.8;Е.В.Коленко “Пора олиш учун жавобгарлик: ЎзбекистонРеспубликаси жиноят қонунчилигини

ҳолда, ЖК 192[9]-моддаси бўйича қонунни қўллаш амалиётини яхшилаш мақсадида қуйидаги ўзгартиришларни киритиш таклиф қиламиз:

Биринчидан, ЖК 192[9]-моддаси биринчи қисм диспозициясида “моддий қимматликлар бериш ёки уни мулкий манфаатдор этиш” деган сўзларни “ноқонуний афзалликларни, яъни моддий ёки номоддий ҳақ ёки мулкий тусдаги иш, хизмат ёки бошқа имтиёзлар ёхуд бошқача нафни ваъда қилиш, таклиф қилиш ёки тақдим этиш” деган сўзлар билан алмаштириш;

Иккинчидан, ЖК 192[9]-моддаси иккинчи қисм диспозициясида “моддий қимматликлар олиши ёки мулкий манфаатдор бўлиши” деган сўзларни “ноқонуний афзалликларни, яъни моддий ёки номоддий ҳақ ёки мулкий тусдаги иш, хизмат ёки бошқа имтиёзлар ёхуд бошқача нафни талаб қилиш ёки қабул қилиб олиш” деган сўзлар билан алмаштириш;

Бу эса мазкур жиноятни номоддий наф орқали содир этилишини олдини олишда хизмат қилади. Қолаверса ушбу ўзгартиришлар орқали Жиноят Кодекси 192[9]–моддаси Коррупцияга қарши кураш тўғрисидаги БМТ Конвенциясига мувофиқлаштирилган бўлади.

ГИЁҲВАНДЛИК ВОСИТАЛАРИ ВА ПСИХОТРОП МОДДАЛАР БИЛАН ҚОНУНГА ХИЛОФ РАВИШДА МУОМАЛА ҚИЛИШ ЖИНОЯТЛАРИНИНГ ЎЗИГА ХОС ХУСУСИЯТЛАРИ

Мирзаходжаев Даврон Атхамович
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси криминалистика ва суд экспертизалари кафедраси катта ўқитувчиси.
mirzaxodjayevdavron@gmail.com

Аннотация *Мақолада гиёҳвандлик воситалари ва психотроп моддалар билан қонунга хилоф равишда муомала қилиш жиноятларининг ўзига хос хусусиятлари ва уларнинг ноқонуний айланмалари тўғрисида илмий асосланган маълумотлар келтирилган.*

Калит сўзлар: *гиёҳвандлик, психотроп моддалар, ҳуқуқий онг, ҳуқуқ, жиноят, ёшлар.*

халқаростандартларни ҳисобга олган ҳолдатакомиллаштириш истиқболлари” мавзусида ю.ф.ф.д (PhD) илмий даражасини олиш учун ёзилган дисс. Автореф. Т.:2023 Б.36

Аннотация *В статье представлены научно обоснованные данные об особенностях преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, а также о незаконных каналах их распространения.*

Ключевые слова: *наркомания, психотропные вещества, правовое сознание, право, преступление, молодежь.*

Annotation: *The article presents evidence-based data on the distinct features of criminal offenses involving the illicit trafficking and circulation of drugs and psychotropic substances*

Keywords: *Drug addiction, psychotropic substances, legal consciousness, law, crime, youth*

Мамлакат ўз келажагини ёшларнинг жисмоний ва маънавий жиҳатдан баркамол бўлиб вояга етишида кўриши табиий ҳолдир. Давлат тараққиётининг ривожи ёш авлоднинг таълим, тарбия даражаси билан бевосита боғлиқдир. Бунга эришиш учун аввало, жамият аъзоларининг, шу жумладан, ёшларнинг сиёсий, ижтимоий, маънавий ва ҳуқуқий савияси юқори даражада бўлиши талаб этилади. Республикасмизда ёшларнинг баркамол ва комил инсон бўлиб, улғайишига давлат сиёсати даражасида эътибор қаратилмоқда. Бу борада Президентимиз Ш.М.Мирзиёев “Бугунги мураккаб замонда ёшларни жисмоний ва маънавий баркамол инсонлар этиб тарбиялаш биз учун ғоят муҳим вазифа бўлиб қолмоқда”-деб таъкидлаб ўтди.

Бугунги кунда ёшларимизнинг ҳуқуқ ва манфаатларини ҳимоя қилиш, уларга зарур шарт-шароитлар ва имкониятларни яратиб бериш борасида мустаҳкам ҳуқуқий база яратилган.

Парламент томонидан ёшларга оид 40 дан зиёд қонун ҳужжатлари қабул қилинган бўлиб, 30 дан ортиқ халқаро ҳуқуқий ҳужжатлар ратификация қилинган.

Шунингдек давлат раҳбари томонидан ижтимоий, маънавий-маърифий соҳалардаги саъй-ҳаракатларни тизимли асосда йўлга қўйиш бўйича 5 та муҳим ташаббуснинг илгари сурилиши Ўзбекистон тарихида ёшлар таълим-тарбияси бўйича яна бир янги босқични бошлаб берди.

Биринчи ташаббус – ёшларнинг мусиқа, рассомлик, адабиёт, театр ва санъатнинг бошқа турларига қизиқишларини оширишга, истеъдодини юзага чиқаришга хизмат қилади.

Иккинчи ташаббус – ёшларни жисмоний чиниқтириш, уларнинг спорт соҳасида қобилиятини намоён қилишлари учун зарур шароитлар яратишга йўналтирилган.

Учинчи ташаббус – аҳоли ва ёшлар ўртасида компьютер технологиялари ва интернетдан самарали фойдаланишни ташкил этишга қаратилган.

Тўртинчи ташаббус – ёшлар маънавиятини юксалтириш, улар ўртасида китобхонликни кенг тарғиб қилиш бўйича тизимли ишларни ташкил этишга йўналтирилган.

Бешинчи ташаббус – хотин-қизларни иш билан таъминлаш масалаларини назарда тутади.

Бугунги кунда мамлакат аҳолисининг 40 фоизини 18 ёшгача бўлган болалар, 64 фоизини 30 ёшгача бўлган ёшлар ташкил этган Ўзбекистон учун баркамол авлодни тарбиялаш, уларга эртанги кунимизнинг ҳал қилувчи кучи сифатида ишонч билдириш, шунингдек уларнинг ҳаётда, жамиятда тинчлик ва осойишталикни, жамоат тартибини сақлаш, ҳар қандай кўринишдаги ҳуқуқбузарликларга қарши курашда фаол иштирок этишини таъминлаш қанчалик долзарб эканлиги барчамизга маълум.

Республикамизда ёшлар учун кенг имкониятлар яратиб берилаётганига қарамасдан, улар орасида носоғлом муҳит таъсирига тушиб қолаётган ёшларимиз ҳам учраб турмоқда. Айниқса ёшлар орасида кенг авж олиб бораётган гиёҳванд ва психотроп моддаларни истеъмол қилиш, унинг таъсирига тушиб қолиш ҳолатлари жуда аянчли ҳолатдир.

БМТ Бош Ассамблеясининг 1987 йил 7 декабрда қабул қилган резолюциясига биноан ҳар йили 26 июнда Халқаро гиёҳвандлик ва бангифурушликка қарши кураш куни (International Day against Drug Abuse and Illicit Trafficking) нишонланади. Таҳлилчиларнинг фикрича, гиёҳванд моддаларнинг кенг тарқалиши бир қатор ижтимоий муаммоларга сабаб бўлади. Яъни, демографик фожеаларни келтириб чиқаради, ижтимоий-иқтисодий ҳаётда жиноятчилик кўзга ташланади. БМТ Бош Ассамблеясининг тан олишича, кўрилаётган чора-тадбирларга қарамай, жаҳонда гиёҳванд моддалар ноқонуний савдоси муаммолигича қолмоқда. Бу муаммо ҳамон жиддий таҳдид сифатида кўрилади.

Статистик маълумотларга кўра дунёда 500 миллиондан ортиқ одам гиёҳвандлик дардига йўлиққан. Унинг аксарият қисмини 30 ёшгача бўлганлар ташкил этмоқда. Бунинг оқибатида ҳар йили 200 мингдан ортиқ киши ҳаётдан кўз юмади. Шу билан бирга, жаҳонда содир этилаётган жиноятларнинг 57 фоизи гиёҳвандлар ҳиссасига тўғри келади. Шу боисдан, гиёҳвандликка қарши қурашни кучайтириш мақсадида, БМТ томонидан “Наркотик моддалар

тўғрисида”ги, “Психотроп моддалар” ҳамда “Гиёҳвандлик воситалари ва психотроп моддаларнинг ноқонуний айланишига қарши қураш тўғрисида”ги конвенциялар қабул қилинган.

Маълумотларга кўра, бир йилда 211 мингта ўлим айнан гиёҳвандлик оқибатида келиб чиқади. Европада гиёҳвандлик оқибатида ҳалок бўлаётганларнинг ўртача ёши 35 ёшни ташкил қилади.

Гиёҳванд моддаларни истеъмол қилиш билан боғлиқ хасталикларга учраганлар сони дунё бўйича 29 миллион кишидан ортиб кетган. Гиёҳванд моддалар истеъмоли сўзсиз аҳоли соғлиғи ва жамоат хавфсизлигига тахдид сифатида кўрилади. Бир қатор мамлакатларда бу иллат жамиятнинг барқарор ривожланишига халақит бераётганидан асло кўз юмиб бўлмайди.

Жумладан, гиёҳвандларни даволаш учун катта миқдорда маблағлар сарфланади. Бу маблағлар давлат бюджетидан ажратилади. Мутахассисларнинг ҳисоб-китобларига қараганда, бугунги кунда ҳар олти гиёҳванднинг биттаси даволаниш имкониятига эга экан. Уларни даволаш учун ажратиладиган сарф-харажатлар ўз йўлига, аммо уларнинг жамият ҳаётига таҳдид солишларини ҳам асло ёддан чиқариш керак эмас. Шу сабабли ҳам гиёҳвандлар соғлиқни сақлаш тизимидан ташқари ижтимоий ҳаётга ҳам муаммо яратувчи сифатида тан олинади.

Гиёҳвандликка қарши кураш доирасида гиёҳванд моддаларни ноқонуний савдосига чек қўйиш ҳам асосий вазифалардан ҳисобланади. Трансмиллий гиёҳванд моддалар савдосига қарши курашда халқаро хуқуқни муҳофаза қилиш ташкилотлари, жумладан, Интерпол, Жаҳон Божхона ташкилоти каби ташкилотлар ҳамкорликда фаолият юритишмоқда. Экспертларнинг фикрича, гиёҳванд моддалар ноқонуний савдо айланмаси бир йилда 300 миллиард доллардан 800 миллиард долларни ташкил қилади.

Гиёҳванд моддалар савдоси ва уюшган жиноятчилик Осиё, Африка, Лотин Америкаси мамлакатларининг иқтисодий, сиёсий барқарорлигига катта хавф солмоқда. Гиёҳвандлик замонавий ҳаётнинг энг хавфли кўринишларидан бири ҳисобланади. Ҳар куни гиёҳвандлик деб аталмиш қўрқинчли қармоққа минглаб одамлар тушиб қолмоқда.

Ўзбекистон Республикаси гиёҳванд моддаларнинг ноқонуний айланишига қарши кураш бўйича халқаро ҳамжамият олдидаги ўз мажбуриятларини тўлақонли бажаришга алоҳида эътибор қаратмоқда. Ўз ортидан бошқа қора иллатларни ҳам етаклаб

юрадиган гиёҳвандлик балосига қарши курашишда юртимизда мустаҳкам ҳуқуқий асослар ишлаб чиқилган.

Мамлакатимиз 1995 йил февраль ойида Бирлашган Миллатлар Ташкилотининг 1961 йилдаги “Наркотик моддалар тўғрисида”ги Ягона Конвенцияси, 1971 йилдаги “Психотроп моддалар тўғрисида”ги ҳамда 1988 йилдаги “Гиёҳвандлик воситалар ва психотроп моддаларнинг ноқонуний айланишига қарши кураш тўғрисида”ги Конвенцияларига аъзо бўлган.

Бундан ташқари, 1999 йилда Ўзбекистон Республикасининг “Гиёҳвандлик воситалари ва психотроп моддалар тўғрисида”ги Қонуни қабул қилинган бўлиб, мазкур қонунга мувофиқ гиёҳвандлик воситалари ва психотроп моддалар билан қонунга зид равишда муомалада бўлишнинг ҳар қандай кўринишларига қарши жиноий жавобгарлик белгиланган.

Мамлакатимизда гиёҳванд моддалар савдоси ва истеъмолига қарши кескин чоралар кўрилаётган бўлса-да, бугун гиёҳвандлик воситаларининг ноқонуний айланиши энг хатарли ва долзарб муаммолардан бири бўлиб қолмоқда. Гиёҳфурушлар янги усул ва найрангларни қўллаб, заҳри қотилни сотиш ҳаракатларини давом эттиришмоқда, яъни Интернет тармоғи орқали наркотик воситалар, психотроп моддалар ёки уларнинг аналогларини тарқатиш ноқонуний олди-сотдиси билан шуғулланмоқдалар. Бугунги кунда ёшлар орасида турли хил таблетка, пастилка, сақич ва бошқа кўринишидаги наркотик моддаларни 150-300 сўмга таклиф қилиш ҳолатлари тез-тез учраб турибди.

Афсуски, ҳозирги кунда ёшлар орасида таркибида гиёҳвандлик воситалари бўлган (“Трамадол”, “Налбуфин”, ва ҳ.к.) психафаол “Лирика”, “Регапен”, “Галара” ва ҳ.к.) дори воситаларини истеъмол қилиш ҳолатларининг учраб туриши ҳамда ёшларимизнинг руҳан ва жисмонан соғлом бўлиб етишишлари, замонавий билим ва касбга эга бўлишлари учун барча шарт-шароитлар яратилиб берилган бўлишига қарамай, наркотик моддалар билан боғлиқ жиноятларни содир қилишлари ва гиёҳвандлик йўлига кириб кетаётганлиги ачинарли ҳолдир.

Ўзбекистонда бугунги кунда ёшлар ўртасида анъанавий гиёҳвандлик моддаларидан воз кечиб, айниқса, психотроп ва кучли таъсир этувчи моддаларни истеъмол қилиш ҳолатлари кўпаймоқда. Ҳозирги ёшларда трамадол ва янги пайдо бўлган тропикамид ва бошқа дорилари истеъмоли ҳам кучаймоқда. Улар таъсирида эса ёшлар томонидан оғир турдаги жиноятлар содир этилмоқда, ушбу

турдаги моддаларини ва бошқа турдаги моддаларини ижтимоий тармоқдан фойдаланиб, тарқатиб келмоқда. Айрим турдаги наркотик воситалар турли хил чой ва шифобахш ўтлар сифатида ниқобланиб сотилмоқда. Бундан ташқари, интернет орқали наркотик воситалари учун нақд тўловсиз бевосита учрашмасдан тўловларни амалга ошириш имконияти мавжуд.

Ҳозирги кунда ер юзидаги наркобизнесда айланаётган пул маблағи дунё аҳолисининг озиқ-овқат, кийим-кечак, турар-жой, таълим тизими ва тиббий хизматга сарфланаётган харажатларидан анча кўплиги билан фарқланиши ҳеч кимга сир эмас. Энг ачинарлиси, гиёҳвандлик оғир жиноятларнинг содир этилишига, оилалар ва миллат генофондининг бузилишига сабаб бўлмоқда.

Хулоса ўрнида шуни таъкидлаш керакки, дунёқараши эндигина шаклланиб бораётган, бор куч-ғайратини фақат билим олишга, изланишга, ҳунар ўрганишга сарфлаши керак бўлган бир пайтда, ўсмирларни алдов йўли билан гиёҳвандлик қурбонига айлантираётган кимсалар озми? Қанчадан-қанча оилаларнинг ёстиғини қуритаётган гиёҳвандликка қарши ҳар бир инсон ўзи курашмоғи, ташқи таъсирлардан ҳимояланмоғи лозим. Вояга етаётган фарзандларимиз ўтмиши қадим, тупроғи олтин, осмони мусаффо Ўзбекистоннинг келажак ворисларидир. Уларни мана шундай соғлом муҳитда, эзгу тушунчаларни юракларига жойлаб вояга етказайликки, ҳеч қанақа ташқи салбий хуружлар ва қора иллатлар ўпқони уларни ўзига жалб қила олмасин.

ДИНИЙ ЭКСТРЕМИСТИК ТАШКИЛОТЛАР ТОМОНИДАН КИБЕРМАКОНДА СОДИР ЭТИЛАЁТГАН ЖИНОЯТЛАРНИ ТЕРГОВ ҚИЛИШНИНГ АЙРИМ ЖИҲАТЛАРИ

Каримов Ифтихор Ибрагимович
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси
Криминалистика ва суд экспертизалари
кафедраси катта ўқтувчиси
E-mail: karimov.i.i@proacademy.uz

Аннотация: *Мақолада диний экстремистик ташкилотлар томонидан кибермаконда яъни Интернет жаҳон ахборот тармоғи ва ижтимоий тармоқлар орқали экстремистик ғоялар акс эттирилган материалларни тарғиб қилиш, тарқатиш орқали ўз сафларига шахсларни жалб этиш ҳолатлари ортиб бораётгани, мазкур ҳолатларни терговга қадар текширув ва тергов вақтида олиш, исботлаш билан боғлиқ долзарб масалалари кўриб чиқилган. Мазкур турдаги*

жиноятларга қарши курашувчи ходимларни ахборот технологиялари соҳасидаги зарурий билимларини ошириш ва зурурий компьютер техник воситалар билан таъминлаш муҳим ҳисобланади.

Таянч сўзлар: *диний экстремизм, терроризм, кибермакон, Интернет, Ижтимоий тармоқлар, терговга қадар текширув, тергов.*

Аннотация: *В статье рассматривается актуальная проблема роста случаев вербовки людей в экстремистские организации посредством пропаганды и распространения экстремистских материалов в киберпространстве, в частности, в социальных сетях. Анализируются вопросы, связанные с обнаружением, фиксацией и доказыванием таких фактов в ходе досудебной проверки и судебного расследования. Отмечается важность повышения уровня знаний сотрудников, занимающихся противодействием такого рода преступлениям, в области информационных технологий, а также обеспечения их необходимыми техническими средствами.*

Ключевые слова: *религиозный экстремизм, терроризм, киберпространство, Интернет, социальные сети, досудебная проверка, судебное расследование.*

Annotation: *The article examines the growing trend of religious extremist organizations using the cyberspace, particularly social media platforms, to propagate extremist materials and recruit individuals. It delves into the pressing issues related to the detection, investigation, and proof of such activities during pre-trial investigations and trials. The article highlights the critical need to enhance the knowledge of law enforcement officers combating these crimes in the field of information technology and to equip them with the necessary computer tools.*

Keywords: *religious extremism, terrorism, cyberspace, Internet, social media, pre-trial investigation, investigation.*

Бугунги глобаллашув шароитида ахборот инсоният ҳаётининг ажралмас қисмига айланган. Шу сабабли ҳалқаро экстремистик ташкилотлар ўз сафларига шахсларни ёллашда интернет жаҳон тармоғидан кенг фойдаланиб келмоқдалар.

Маълумотларга кўра, Ўзбекистон аҳолисининг интернет хизматидан фойдаланувчилари сони 31 миллиондан ортиб, улардан 29,5 миллиони мобил интернетдан фойдаланади[99]. Бу албатта, мамлакатимизда ахборот-коммуникация технологиялари жадаллик билан ривожланаётганидан, фуқароларимизнинг ахборот олиш, сақлаш, тарқатиш каби конституцион ҳуқуқларини амалга оширишда сифатли алоқа тизимларидан фойдаланиш имкониятлари ривожланаётганлигидан далолат беради.

Бу эса Интернет бутун жаҳон ахборот тармоғида аҳолини экстремистик оқимлар таъсирига тушиб қолишларини олдини олиш

[99] Ш. Шерматов. Ўзбекистонда интернетдан фойдаланувчилар сони 31 миллиондан ошди. https://www.gazeta.uz/uz/2022/12/15/internet-users. (Электрон манбага мурожаат қилинган вақт: 19.11.2023)

зарурлигини, ёшларнинг ахборотдан фойдаланиши учун соғлом муҳит яратиш лозимлигини кўрсатмоқда. Ўзбекистон Республикаси Президенти Ш.М.Мирзиёев ёшларимизнинг қалби ва онгида мафкуравий иммунитетни кучайтириш билан боғлиқ вазифаларга тўхталиб: “Бу вазифаларни амалга оширишда биз асрлар мобайнида шаклланган миллий анъаналаримизга, аждодларимизнинг бой меросига таянамиз[100]”, – деб таъкидлаган эди.

Бугунги кунда, экстремизм хусусиятига эга бўлган ишлар бўйича қўзғатилган жиноят ишлари таҳлили мазкур турдаги жиноятларнинг 90 фоизи интернет ижтимоий тармоқлари орқали содир этилаётганлигини кўрсатмоқда.

Таҳлилларга кўра, ҳозирги кунда дунёда диний экстремистик ташкилотлар тарғиботи асосан интернет ижтимоий тармоқлари, хусусан Telegram (48 фоиз), Youtube (14 фоиз), Facebook (13 фоиз), Odnoklassniki (13 фоиз), Instagram (11 фоиз), WhatsApp (1 фоиз) каби ижтимоий тармоқлар, мессенжерлар ва видеохостинглар орқали фаол олиб борилмоқда. Бу ҳаракатлар миллий, диний адоватни қўзғатишга, шахсларни ўз жонига қасд қилишга ундашга қаратилган бўлиб, бунинг оқибатлари ўта хавфли ва ташвишлидир.

Ҳозирда интернет глобал тармоғида 40 мингдан ортиқ шахсларни ёлловчи экстремистик сайтлар мавжуд бўлиб[101], БМТ Бош котибининг сиёсий масалалар бўйича ўринбосари Жеффри Фелтманнинг сўзларига кўра, “Twitter” ижтимоий тармоғида ИШИД (Ироқ Шом Ислом давлати) ғоялари ва фаолиятини қўллаб-қувватловчи 50 минг атрофида аккаунт мавжуд, уларнинг ҳар бири ўртача мингта “ҳамфикр” ва “издош”га эга[102]. Шу билан бирга ижтимоий тармоқлар орқали ИШИДнинг “Ал-Фурқон” ва “Ал-Ҳаёт” медиа марказлари асосан араб, инглиз, немис, француз, рус, ҳинд, урду, бенгал, турк, курд ва бошқа яна бир қатор тилларда тарғибот-ташвиқот хуружларини амалга ошириб келмоқда[103].

Бу ҳолат мазкур турдаги жиноятлар юзасидан терговга қадар текширув ўтказиш ва тергов қилишда муайян қийинчиликларни

---

[100] Ш. Мирзиёев. Қонун устуворлиги ва инсон манфаатларини таъминлаш — юрт тараққиёти ва халқ фаровонлигининг гарови. Ўзбекистон Республикаси Конституцияси қабул қилинганининг 24 йиллигига бағишланган тантанали маросимдаги маъруза. https://www.gazeta.uz/uz/2016/12/07/speech. (Электрон манбага мурожаат қилинган вақт: 24.10.2022 yil)

[101] В Интернете около 40 экстремистских сайтов URL https://www.pravda.ru/news/society/82120-internet_ekstremistskikh_saitov_40_miroshnikov. (Электрон манбага мурожаат қилинган вақт: 19.07.2023)

[102] А.Федоров. О некоторих аспектах информатсионной политики игил в сотсиалних сетях. https://cyberleninka.ru/article/n/onekotoryh-aspektah-informatsionnoy-politiki-igil1-vsotsialnyh-setyah. (Электрон манбага мурожаат қилинган вақт: 03.02.2024)

[103] Т.М.Албо. Пропагандистская деятелност ИГИЛ и методи борби с ней. https://cyberleninka.ru/article/n/propagandistskaya-deyatelnost-igil-i-metody-borby-s-ney. (Электрон манбага мурожаат қилинган вақт: 03.11.2023)

вужудга келтирмоқда.

Диний экстремистик ташкилотлар ҳалқаро террористик ташкилотлар сафига жангариларни тайёрлаб берувчи плацдарм эканлигини инобатга олсак, аҳвол нақадар ташвишли эканлигини англашимиз мумкин.

Қайд этиш жоизки, сўнгги 15-20 йил давомида дунё мамлакатлари аҳолиси, шу жумладан, ўзбекистонлик ёшлар ҳаётида мобил алоқа урф тусини олган бўлса, ҳозирги даврга келиб мобил ускуналардаги WhatsApp, ICQ, MSN Messenger ва Telegram орқали матнли мулоқот оммавийлик касб этиб бормоқда[104].

Маълумот учун, ҳозирда дунё аҳолисининг қарийб ярми – яъни 3 млрд.га яқин киши турли ижтимоий тармоқлардан фойдаланмоқда. Шундан, энг катта қисми – 2 млрд. одам “Facebook” ижтимоий тармоғидан фойдаланмоқда. Ўзбекистонда “Facebook” тармоғидан фойдаланувчилар 1 миллионга яқинлашиб қолган. Улар ўртача 25-34 ёшда бўлиб, 65,5 фоизини эркаклар, 34,5 фоизини хотин-қизлар ташкил этади. Дунёда 1 млрд.лик аудиторияга эга Instagram Ўзбекистонда 1.586.500 нафар фойдаланувчига эга. 200 млн. обуначисига эга бўлган Telegram ижтимоий тармоғидан Ўзбекистонда 18 млн.лик обуначига хизмат кўрсатмоқда[105].

Мазкур ижтимоий тармоқлар орқали диний экстремистик ташкилотлар бир неча сония ичида катта хажмдаги материалларни етказиб бериш имкониятига эгалигидан ўз тарафдорларига экстремистик материалларни тарқатишда самарали фойдаланмоқдалар. Улар асосан “такфир”, “ҳижрат”, “жиҳод”, “халифалик” ва “шаҳид” каби Ислом динига оид тушунчаларни мазмунини бузган ҳолда илгари суриб, ўз мақсадига эришишни кўзлашмоқда. Жумладан, ИШИД ўз ғояларининг кенг тарқалишини таъминлаш мақсадида Facebookда “Caliphatebook” саҳифасини очган бўлиб[106], ҳозирда ундан радикал ғоялар тарафдорларини шакллантиришда фойдаланмоқда.

Шу каби сайт ва аккаунтлар тармоқда тўсатдан пайдо бўлиб, маълум вақт ўтгач йўқолади, мазмунини ўзгартирмаган ҳолда тез-тез номланиши ва доменини ўзгартириб туриши натижасида ушбу сайтларни блоклаш имконсиз бўлиб қолмоқда.

---

[104] А.Рахмонов. Вайронкор ғояларнинг салбий оқибатлари ва уларнинг олдини олиш зарурати. https://telegra.ph/33-mavzu-08-14. (Электрон манбага мурожаат қилинган вақт: 03.02.2024)

[105] Г.Ғаффарова. Ижтимоий тармоқларнинг ёшлар маънавиятига таъсири. Academic research in educational sciences. Scientific Journal Impact Factor (SJIF) 2021: 5.723 https://cyberleninka.ru/article/n/izhtimoiy-tarmolarning-yoshlar-manaviyatiga-tasiri. (Электрон манбага мурожаат қилинган вақт: 19.09.2022)

[106] "Исламское государство" запустило собственную сотсиалную сет. URL https://www.interfax.ru/world/428849. (Электрон манбага мурожаат қилинган вақт: 11.02.2023)

Шунингдек, диний экстремистик гуруҳлар ҳуқуқ тартибот идоралари эътиборига тушмаслик мақсадида интернетдаги спорт мавзусидаги контентлар, веб-конференциялар, порнографик саҳифалар ва онлайн ўйин дастурларида ўз маълумотларини яширмоқдалар. Бўлажак экстремистик ҳаракатларга оид тафсилотлар ёки тарғиботлар бутун интернет бўйлаб ёйилган кўринишда сақланмоқда. Яширин кодларни билган экстремистлар уларни бир жойга жамлаб танишиш имконига эга бўлмоқдалар.

Экспертлар фикрича, жангарилар томонидан тарқатилаётган видеолавҳалар юқори савияда, профессионал тарзда тайёрланиб, Интернетдаги имкониятлар боис бундай сифатли видеолавҳалар жангарилар фаолиятини тарғиб қилиш учун қўл келмоқда. Ҳар сафар жангарилар томонидан янги видеолавҳа ва фотосуратлар чиқарилганида, улар аввалгисидан мазмун ва сифат жиҳатдан фарқ қилиб, жангарилар ўзлари тайёрлаган маҳсулот халқаро жамоатчиликка қандай таъсир этганини кузатиб, таҳлил қилиш орқали сифатни янада яхшилаб бормоқдалар.

Маълумки, вояга етмаган шахслар ёшлигидан компьютер ўйингоҳларида Counter-Strike, GTA, PUBG ва бошқа жангари ўйинларини ўйнашлари оқибатида уларда жангларни реал ҳаётда бажаришга қизиқиш пайдо бўлади. Мутахассисларнинг фикрига кўра, экстремистик ташкилотларнинг дала қўмондонлари айнан ушбу омилдан устомонлик билан фойдаланмоқдалар. Яъни улар томонидан тайёрланган махсус видеоматериаллардаги реал вақт режимидаги жангари саҳналар ёшларда ҳам ушбу жанговор ҳаракатларда иштирок этиш ҳиссини кучайтиради. Террорчи ёлловчилар ёшларни онлайн компьютер ўйинларининг чатида суҳбатга жалб қилиб террористик ҳужумларни ўйин тарзида амалга ошириш клонларини яратмоқда. Россия ФХХ директори Александр Бортников 2021 йилнинг июнь ойида бўлиб ўтган, халқаро хавфсизлик бўйича IX Москва конференциясининг очилишида: “ёшлар алоҳида “хавф гуруҳи”да, уларнинг психологик ишловга олиниши ижтимоий тармоқларда ва машҳур компьютер ўйинларининг ўйин чатларида амалга оширилмоқда. Бундан ташқари, террорчи гуруҳлар аллақачон ёшларга таъсир ўтказишга имкон берадиган ушбу ўйинларнинг ўз клонларини яратиш даражасига етишган. Яъни террористик ва экстремистик ташкилотларнинг потенциал тарафдорлари нафақат овозли чат

орқали, балки фойдаланувчини ўйин орқали теракт содир этишга ўргатишмоқда”деб айтиб ўтган эди[107].

Мисол учун, бундай шахслардан бири интернет ижтимоий тармоқларида фаол тарғибот тадбирларини олиб бораётган “Тавҳид ва Жиҳод” террористик гуруҳини ғоявий раҳнамоси Мухтаров Сирожиддин (таҳаллуси “Абу Салоҳ Оший”) ҳисобланади. Россия Мудофаа вазирлиги томонидан унинг вафот этганлиги тўғрисида хабарлар тарқалган бўлса-да С.Мухтаровнинг Сурия давлатида амалга ошираётган қўпорувчилик ҳаракатларини бевосита интернет ижтимоий тармоқлари орқали намойиш этган видеоматериаллари таъсирида кўплаб шахслар ушбу гуруҳлар сафига келиб қўшилмоқда[108].

Мазкур ҳолатлар ҲМҚО ходимларидан компьютер ўйингоҳларида Counter-Strike, GTA, PUBG ва бошқа жангари ўйинлар йўналишида ҳам ўзига хос назорат олиб бориш лозимлигини кўрсатмоқда.

Бугунги кунда ҳуқуқни муҳофаза қилувчи органларда Интернетдаги тақиқланган веб-сайтларини блоклашнинг техник имконияти мавжуд, бироқ ижтимоий тармоқлардаги аккаунтларни блоклашнинг имконияти йўқлиги, унда материалларни тарқатишнинг тез, қулай ва ҳуқуқ тартибот органлари томонидан мониторинг қилиш имкониятининг чекланганлиги экстремистик ташкилотлар учун қулай имкониятни вужудга келтириб, ушбу йўналишда тарғибот тадбирларига кўпроқ куч-восита сарфламоқдалар.

Ўзбекистон Республикаси Президентининг 04.09.2019 йилдаги “Диний-маърифий соҳа фаолиятини такомиллаштириш бўйича қўшимча чора-тадбирлар тўғрисида”ги ПҚ-4436-сонли қарорининг 8-бандида Олий суд ўзининг расмий веб-сайтлари ва бошқа оммавий ахборот воситалари орқали суд томонидан экстремистик ёки террористик деб топилган ҳамда Ўзбекистон Республикаси ҳудудида фаолияти тақиқланган ташкилотлар, веб-сайтлар, ижтимоий тармоқлар ва мобил мессенжерлар рўйхатини эълон қилиб, унинг доимий равишда янгилаб борилишини таъминлаши алоҳида қайд этилган.

Мазкур вазифалар ижросини таъминлаш мақсадида Олий суд томонидан мамлакатимиз ҳудудига олиб кириш, тайёрлаш, тарқатиш ва намойиш этиш тақиқланган манба ва контентлар (материаллар) рўйхати Олий суднинг расмий веб-сайтидаги “Очиқ

---

[107] Бортников заявил, что террористи создают клони компютерних игр с имитатсией терактов // ТАСС. 2021. 23 июня. URL : https://tass.ru/obschestvo/11723253 (Электрон манбага мурожаат қилинган вақт: 23.06.2021).

[108] В Минобороны сообщили об уничтожении лидера террористов в Сирии. Подробнее на РБК: https://www.rbc.ru/rbcfreenews/631bb4429a7947c68e37dc50?from=copy. (Электрон манбага мурожаат қилинган вақт: 04.09.2023)

маълумотлар” рукнида мунтазам равишда янгиланиб, эълон қилиб борилмоқда.

Мазкур қарор асосида, 2019-2024 йилларда Ўзбекистон Республикаси Олий судининг 80 дан зиёд ҳал қилув қарорлари асосида “Facebook”, “Odnoklassniki”, “Instagram” ва “TikTok” ижтимоий тармоқлари, “Telegram” мобил мессенжери, “YouTube” видеохостинги ва бошқа 1000 дан ортиқ манбаа ва улардаги материаллар экстремистик ва террористик ғояларини тарғиб этишга йўналтирилган деб топилиб, уларни Ўзбекистон Республикаси ҳудудида фаолияти расман тақиқланган.

Бироқ, ҳуқуқни қўллаш амалиётида веб-сайтларни блоклаш учун зарурий шарт-шароитлар яратилган бўлсада, ижтимоий тармоқлардаги аккаунтлар фаолиятини чеклашнинг техник имкониятини мавжуд эмаслиги айрим тушунмовчиликларни келтириб чиқармоқда. Шу сабабли, Ўзбекистон Республикаси Адлия вазирлиги ва Олий суди томонидан расмий веб-сайтлар ҳамда бошқа оммавий ахборот воситалари орқали суд томонидан тақиқланган веб-сайтлар, ижтимоий тармоқлар ва мобил мессенжерларнинг рўйхатини эълон қилиб бориш амалиёти кенг жамоатчилик учун огоҳлантириш эмас, аксинча салбий маънодаги тарғибот вазифасини бажариб қолмоқда. Натижада, айнан мазкур аккаунтлар ва улардаги ахборот манбалари минглаб ёшларнинг эътибор марказида бўлиб, келгусида мазкур ташкилотларнинг таъсир доирасига тушиб қолишларига олиб келмоқда.

Бинобарин, Вазирлар Маҳкамасининг 2022-йил 14-апрелдаги “Диний мазмундаги материалларни тайёрлаш, олиб кириш ва тарқатиш ҳамда диншунослик экспертизасини ўтказиш тартиби тўғрисидаги низомни тасдиқлаш ҳақида”ги 180-сонли Қарорига кўра, ҳар қандай диний мазмундаги материаллар диншунослик экспертизасидан ўтказилиши ва экспертизанинг ижобий хулосаси уларнинг Ўзбекистон Республикаси ҳудудида тайёрланиши, олиб кирилиши ва тарқатилиши учун асос бўлиб хизмат қилади. Бироқ, ушбу кўзда тутилган профил ва каналларни блоклашнинг техник имконияти йўқлиги сабабли, ҳозирги кунга қадар уларнинг айримлари ўз фаолиятларини давом эттирмоқда.

Хулоса сифатида шуни айтиш мумкинки, интернет ижтимоий тармоқларининг ёпиқлиги, мониторинг қилиш имкониятининг чекланганлиги, шунингдек, уларда исталган ҳажмдаги материалларни бир неча сонияда керакли манзилга етказиш мумкинлиги диний экстремистик ташкилотларга экстремистик материалларни асосан кибермаконда, интернет ижтимоий тармоқлари орқали

тарқатишларига имкон бермоқда. Мазкур жиноятлар юзасидан ҳуқуқни муҳофаза қилувчи органлар томонидан терговга қадар текширув ва тергов ҳаракатларини ўтказишда зарурий билимларнинг етишмаслиги ва техник имкониятнинг чекланганлиги ушбу турдаги жиноятларни тергов қилишда бир қатор муаммоларни вужудга келтирмоқда. Бу борада мазкур турдаги жиноятларга қарши курашувчи ходимларни ахборот технологиялари соҳасидаги зарурий билимларини ошириш ва зурурий компьютер техник воситалар билан таъминлаш муҳим ҳисобланади.

ГУВОҲНИНГ ЁКИ ЖАБРЛАНУВЧИНИНГ БИЛА ТУРИБ ЁЛҒОН КЎРСАТУВ БЕРИШИНИ БАРТАРАФ ЭТИШДА СУНЪИЙ ИДРОК ИМКОНИЯТЛАРИДАН ФОЙДАЛАНИШ МАСАЛАЛАРИ

Абдуллаев Акмалжон Йўлчибоевич,
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси
Дастлабки тергов ва суриштирув кафедраси ўқитувчиси
ORCID ID 0009-0002-4302-2341

Аннотация: *Мазкур мақолада сунъий идрок имкониятларидан фойдаланиб гувоҳнинг ёки жабрланувчининг била туриб ёлғон кўрсатув беришини ўз вақтида фош этиш ва уларни зарарсизлантиришнинг ўзига хос хусусиятлари муҳокама қилинади. Шунингдек, сунъий идрок имкониятлардан фойдаланиш бўйича айрим хорижий мамлакатларнинг илғор тажрибалари фикр юритилади.*

Калит сўзлар: *гувоҳ, жабрланувчи, ёлғон, кўрсатув, сўроқ қилиш, сунъий идрок.*

Аннотация. *В данной статье обсуждаются особенности своевременного выявления и нейтрализации заведомо ложных показаний свидетеля или потерпевшего с использованием возможностей искусственного интеллекта. Также рассматривается передовой опыт некоторых зарубежных стран в применении технологий искусственного интеллекта.*

Ключевые слова: *свидетель, потерпевший, ложь, показания, допрос, искусственный интеллект.*

Annotation. *This article discusses the features of timely detection and neutralization of knowingly false testimony by witnesses or victims using artificial intelligence capabilities. The advanced experience of some foreign countries in the application of artificial intelligence technologies is also considered.*

Key words: *witness, victim, lie, testimony, interrogation, artificial intelligence.*

Барчамизга маълумки, бугунги кунда ахборот-технологияларидан фойдаланиш бутун дунёда долзарб аҳамиятга эга масалага айланиб, замонавий технологиялардан фойдаланиш инсон

меҳнатини енгиллаштириб, вақт, маблағ, куч ва воситаларни тежашга имкон бермоқда. Ҳозирда ҳаётимизни уларсиз тасаввур қилиш қийин, чунки кундан-кунга ахборот-технологиялари ҳаётимизнинг ҳар бир жабҳасига кириб бормоқда. Сунъий идрокнинг яратилиши эса фан-технология соҳасида кескин бурилиш ясади. Айни вақтда кўплаб дунё мамлакатларида ҳуқуқни муҳофаза қилиш идоралари томонидан жиноятчиликка қарши курашиш соҳасида сунъий идрок имкониятларидан фойдаланиб келинмоқда. Энг кўп тарқалган усуллардан бири — улардан жамоат хавфсизлигини таъминлаш мақсадида фойдаланишдир. Мисол учун Хитой, Сингапур ва бир қатор бошқа мамлакатларда кузатув камераларига юзни аниқлаш тизими интеграция қилиш орқали жиноят содир этиб яшириниб юрган жиноятчиларни ушлашда кенг фойдаланилмоқда. Кореяда жиноят содир этилишидан олдин уларни башорат қиладиган нейрон тармоқ ишлаб чиқилди. Dejaview жиноятларни 82,8% аниқлик билан башорат қилади, бу инсон хатти-ҳаракатларини таҳлил қилиш, куннинг вақтини, жойлашувини ва ўтмишдаги воқеаларни таҳлил қилиш ҳисобига амалга оширилади. Бундан ташқари, модель ўтмишда жиноят содир этган жиноятчиларни ҳам яхши аниқлай олади[109].

Сир эмаски, ахборотлашган жамиятда фуқароларнинг ҳуқуқ ва эркинликларини самарали ҳимоя қилишда ахборот технологиялари ва сунъий идрокдан фойдаланмаслик имконсиз. Бу жиноятдан жабр кўрган шахслар ва жиноят иш юритишда манфаатдор бўлмаган иштирокчилар учун қулай рақамли муҳит яратиб, тергов жараёнларининг самарадорлигини оширади ва тергов органларига фуқароларнинг ишончини мустаҳкамлайди.

Сунъий идрокдан жиноят-процессуал фаолиятда фойдаланиш кенг тарқалган бўлиб, бугунги кунда АҚШда фаол қўлланилмоқда. Бунда алгоритмларга нафақат ёрдамчи вазифалар, балки юридик аҳамиятга эга қарорлар қабул қилиш топширилади. Алгоритмлар жиноятчи томонидан қайта жиноят содир этилиши эҳтимолини аниқлаш учун қўлланилади. Сунъий идрокнинг хулосалари асосида судья қўшимча жазо тайинлайди, озодликдан маҳрум қилиш билан боғлиқ бўлган қамоқ чорасини белгилайди ёки қўлга олинган шахснинг гаров эвазига озод қилиниш эҳтимолини аниқлайди. Дастур жиноят ишидан олиш мумкин бўлган барча статистик омилларни ҳисобга олади ва айбланувчи суддан қочиб кетиши ёки жамият учун хавф туғдириш эҳтимоли қанчалик юқори эканлигини аниқлашга ёрдам беради.

[109] https://aniq.uz/yangiliklar/(Электрон манбага мурожаат қилинган сана: 01.10.2024 й)

Алгоритм 49 та жиноятга хос хусусиятларни (масалан, қурол билан боғлиқ бўлган ҳолатлар) ва 15 та айбланувчига тегишли хусусиятларни (масалан, жинси, ёши, олдинги ҳибсга олиниш ҳолатлари) кўриб чиқади. Компьютер алгоритмининг қўлланилиши қарор қабул қилишда объективликни сезиларли даражада оширади ва инсоннинг бир томонлама қарашларини чиқариб ташлайди, деб ҳисобланади[110]. Шунга қарамай, ўтказилган тадқиқотлар алгоритм ишлаб чиқиш жараёнида уни ишлаб чиқувчининг қадрият йўналиши таъсир қилиши мумкинлигини кўрсатади, масалан, қора танли айбланувчиларни қайта жиноят содир этишга кўпроқ мойил деб аниқлаш мумкин[111].

Шу муносабат билан, компьютерга якуний қарор қабул қилиш ҳуқуқини бериш нафақат дискриминацияга, балки алгоритмлар орқали дарҳол сиёсий вазифаларни ҳал қилишга уринишларга ҳам олиб келиши мумкин (қамоқдаги шахслар сонини камайтириш ёки ошириш, қайта жиноят содир этилишини камайтириш ва ҳоказо). Шу боис, 2018 йил 4 декабрда Европа Кенгаши CEPEJ суд тизимлари ва уларнинг атроф-муҳитларида сунъий идрокдан фойдаланиш бўйича Европанинг этик Хартиясини қабул қилди. Ушбу ҳужжатда адолатли қарор қабул қилишда алгоритмлардан фойдаланиш бўйича масъулият ошганлиги ва сунъий идрокга якуний қарор қабул қилиш ҳуқуқини бериш мумкин эмаслиги кўрсатилган[112].

Сунъий идрокдан фойдаланишнинг аҳлоқий муаммоларидан ташқари, жиноят-процессуал қонунчилигини кескин ўзгартириш зарурати тўсқинлик қилади, буни эса қисқа муддатда амалга ошириб бўлмайди. Шунга қарамай, ишни судга қадар юритиш босқичида ишларнинг сифати ва самарадорлигини мавжуд тизимни бутунлай ўзгартирмасдан сунъий идрокни ёрдамчи вазифаларни бажариш вазифасини юклаш орқали қўллаш орқали ҳам сезиларли даражада ошириш мумкин, Бу йўналиш энг истиқболли ва амалга ошириш учун ҳақиқий имкониятга эга деб ҳисобланади. Биринчи навбатда фуқароларни ҳуқуқни муҳофаза қилиш органларига шикоят бериш имкониятини махсус электрон хизмат орқали онлайн тақдим этишни кўриб чиқиш лозим. Бу борада Қозоғистон Республикасининг ижобий

[110] Jung J., Concannon C., Shroff R., Goel Sh., Goldstein D. Simple Rules for Complex Decisions // Working paper, Stanford University. 2017. 2 Apr. URL: https://arxiv.org/pdf/1702.04690.pdf /(Электрон манбага мурожаат қилинган сана: 01.10.2024 й)

[111] Kirsten M. Ethical Implications and Accountability of Algorithms // Journal of Business Ethics. 2018. Vol. 160. P. 835–850. DOI: 10.1007/s10551-018-3921-3/(Электрон манбага мурожаат қилинган сана: 01.10.2024 й)

[112] Европейская этическая хартия CEPEJ об использовании искусственного интеллекта (ИИ) в судебных системах и их среде от 4 декабря 2018. URL: https://rm.coe.int//(Электрон манбага мурожаат қилинган сана: 01.10.2024 й)

тажрибасидан фойдаланиш мақсадга мувофиқ бўлади. У ерда Qamqor (qamqor.gov.kz) порталида ҳуқуқий хизматлар ташкил қилинган бўлиб, жиноят ҳақида ариза топшириш хизмати 5 босқичдан иборат — авторизация, жиноий таъқиб органини танлаш, шахсий маълумотларни киритиш, шикояти мазмунини акс эттириш ва ариза ҳолати тўғрисида билдиришнома олиш[113] .

Ариза берувчининг авторизацияси электрон рақамли портал ёки мобил телефон рақами орқали амалга оширилади. Ҳозирги пайтда биометрик маълумотлар орқали идентификацияни қўшиш мумкин деб ҳисоблаймиз, бундай технология банк секторида кенг тарқалган. Қозоғистоннинг ишни судга қадар иш юритиш босқичида ишларни ҳам қоғозли, ҳам электрон форматда олиб бориш бўйича тажрибаси ҳам амалий қизиқиш уйғотади. Форматни танлаш иш бўйича иш олиб борувчи шахс томонидан амалга оширилади. Электрон форматда жиноий иш юритишни давом эттириш мумкин бўлмаган тақдирда, қоғозли форматга ўтиш амалга оширилади. Бу ғоя осонликча амалга оширилиши мумкин ва сезиларли моддий харажатларни талаб қилмайди, чунки кўпчилик ҳуқуқни муҳофаза қилиш органларида ҳозирда хизмат ёзишмалари учун қўлланилаётган электрон ҳужжат айланиши тизими мавжуд. Бундан ташқари, коррупциянинг олдини олиш учун жиноий ишлар терговчилар ўртасида тақсимланиши чоғида мутахассислик ва судьяларнинг юкламасига асосланган ҳолда ишлар тақсимланиши учун тасодифий танлов тизимларини қўллаш мақсадга мувофиқ. Бундай тизимлар аллақачон судларда ишларни тақсимлаш учун, шунингдек, ҳимоячи танлаш учун муваффақиятли қўлланилмоқда. Жабрланувчилар билан ўзаро алоқа қилишда чат-ботлардан фойдаланиш мумкин, улар сўров бўлган тақдирда қабул қилинган қарорлар тўғрисида хабар беради, тез-тез учрайдиган ҳолатларда ҳаракатлар тартибини тушунтиради, шунингдек, ҳуқуқ ва мажбуриятларни аниқлайди. Бу жабрланувчини олиб борилаётган тергов ишларидан хабардор қилишга, шунингдек, моддий ва вақтинчалик харажатларсиз ўз ҳуқуқларини тўлиқ амалга оширишга ёрдам беради.

Сунъий интеллектдан фойдаланиш тергов ҳаракатларининг сифатига таъсир кўрсатиши мумкин. Айниқса сўроқ жараёнида қўшимча ва виртуал реалликдан фойдаланиш мумкин, бу эса кўрсатувлар сифатини сезиларли даражада оширади. Бундан ташқари, ўтказилган тадқиқотлар шуни кўрсатадики, виртуал

[113] Qamqor. URL: https://egov.kz/cms/ru///(Электрон манбага мурожаат қилинган сана: 07.10.2024 й)

персонаждан ўзаро кўрсатувларни олиш иштирокчиларнинг кескинлигини пасайтиради ва холислик ҳиссини оширади[114].

Маълумки, гувоҳ ва жабрланувчининг кўрсатувлари ишни қонуний, асосланган ва адолатли ҳал қилишдаги асосий далил манбаларидан бири ҳисобланади. Бироқ ҳозирги вақтда нафақат Республикамизда,балки бутун дунёда гувоҳ ёки жабрланувчининг кўрсатувларини ҳақиқат ёки ёлғон эканлигини баҳолаш энг мушкул масала бўлиб қолмоқда. Аксарият давлатлар томонидан фойдаланилиб келинаётган полиграф ва бошқа техника воситалар ҳам муайян шахсни кўрсатуви ёлғон эканлигини аниқ баҳолаб бера олмайди. Шунинг учун ҳам кўп давлатларда полиграф натижалари яққол далил сифатида фойдаланилмайди.

Тадқиқотимиз давомида гувоҳнинг ёки жабрланувчининг била туриб ёлғон кўрсатув беришини аниқлаш 98% ҳолатда имконсиз эканлиги, бироқ уни ўз вақтида фош этиш ва зарарсизлантириш мумкинлиги ҳақида хулосага келдик. Бу масалада терговчига энг қўл келадиган восита сунъий идрок ҳисобланади. Чунки сунъий идрок ёлғонга ишора қилувчи новербал белгиларни, жумладан, қўллар, бармоқлар, оёқлар ва тўпиқларнинг маълум ҳаракатларини аниқ белгилай олади. Юқори ва паст даражали визуал функциялардан фойдаланувчи техник кўриш тизими ёлғонни одамларга нисбатан анча яхшироқ башорат қилади[115].

Сўроқ қилишда сунъий идрок имкониятидан фойдаланишимиз сўроқ пайтида олинган маълумотларни тўлиқроқ ва объектив бирлаштиришга ёрдам беради ҳамда сўроқнинг самарадорлигига таъсир қилади. Чунки терговчи сўроқ қилинаётган шахснинг кўрсатувларини унинг интонацияси ва нутқ хусусиятлари бўйича таҳлил қила олмайди. Сўроқда сунъий идрокдан фойдаланиш, гувоҳ ва жабрланувчининг кўрсатувларига объектив баҳо беришга имкон беради. Шу билан бирга, сўроқ қилинувчини кўрсатувларни турли объектив ва субъектив сабабларга кўра ўзгартириш мақсадини тийиб туришга хизмат қилади.

Гувоҳ ёки жабрланувчи сунъий идрок ҳиссиётларни намоён қилсагина, унга ишониши мумкин. Бундай ҳолда, сунъий интеллект

---

[114] Pollina D. A., Barretta A. The effectiveness of a national security screening interview conducted by a computer-generated agent // Computers in Human Behavior. 2014. Vol. 39. P. 39–50. //(Электрон манбага мурожаат қилинган сана: 09.10.2024 й)

[115] Ulatowska M. Indicators of deception in different lie scenarios // Roczniki Psychologiczne / Annals Of Psychology. 2013. Vol. XVI, No. 1. P. 127–146.

нафақат керакли маълумотларни олиши, балки маънавий ёрдам ҳам бериши мумкин [116].

Терговчи гувоҳ ёки жабрланувчини сўроқ қилишда сунъий идрокдан фойдаланиш орқали қуйидагиларни аниқлаши мумкин:

- сўроқ қилинган шахс ҳаққоний ёки ёлғон кўрсатма бераётганлигини аниқлаш мумкин. Бунда сунъий идрокнинг дастурий таъминотида сўроқ қилинувчи шахснинг шахсиятига оид белгилари ва ҳаракатлари белгиланган бўлиб, улар ёрдамида буни аниқлаш мумкин. Буларга юз мимикалари, мушакларининг ҳаракатлари, тана аъзоларининг, юзнинг ва овознинг турли қисмларидаги қўрқув белгилари ва ҳ.к. киради;

- кўрсатувларнинг ёлғонлигини, бунинг учун дастур гапни таҳлил қилади, яъни муаллиф томонидан қандай гаплар тузилгани ва уларнинг таҳririни, қандай сўзлар ёки терминлар танланганини ва ҳ.к.

Бизнинг назаримизда, гувоҳ ёки жабрланувчини сўроқ қилишда сунъий идрок имкониятларидан фойдаланиш жиноятларни тез ва тўла тергов қилишнинг мутлақо янги сифат даражасига олиб чиқиш имконини беради. Кўрсатувлардаги ёлғонни ўз вақтида фош этиш ва уларни зарасизлантириш орқали ҳақиқатни аниқлашга хизмат қилиб, шу билан бир қаторда айбсиз одамни жиноий жавобгарликка тортишни ёки ҳақиқий айбдорни жиноий жавобгарликдан озод қилишни олдини олади.

ЗАРАРЛИ ДАСТУРЛАР ЁРДАМИДА СОДИР ЭТИЛАЁТГАН КИБЕРЖИНОЯТЛАР

Ахроров Бахром Джаббарович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети профессори, юридик фанлар доктори (DSc)
Муродов Акобир Рахмонжон ўғли
Ўзбекистон Республикаси Жамоат хавфсизлиги университети мустақил изланувчиси,

Аннотация*. Мазкур мақолада зарарли дастурлар тушунчаси, улар ёрдамида содир этилаётган жиноятларнинг турлари, амалга ошириш усуллари ва зарарли дастурлар ёрдамида содир этилган ҳуқуқбузарликларнинг оқибатлари ҳамда улардан ҳимояланиш усуллари тўғрисида*

[116] Villalobos J. G., Davis D. Interrogation and the Minority Suspect: Pathways to True and False Confession // In: Miller M., Bornstein B. (eds) Advances in Psychology and Law. 2016. Vol. 1. P. 1–41. URL: https://doi.org/10.1007/978-3-319-29406-3_1 //(Электрон манбага мурожаат қилинган сана: 12.10.2024 й)

Калит сўзлар*: компьютер вируси, morris worm, экотизим, ransomware, аутентификация маълумотлари, "Monero" криптовалютаси*

Аннотация. *В данной статье речь идет о понятиях вредоносных программ, видах преступлений, совершаемых с их помощью, способах реализации и последствиях правонарушений, совершенных с помощью вредоносных программ, а также способах защиты от них.*

Ключевые слова: *компьютерный вирус, червь Морриса, экосистема, программы-вымогатели, учетные данные, криптовалюта Monero.*

***Annotatio*n:** *This article is about the concept of malicious programs, types of crimes committed with their help, methods of implementation and consequences of offenses committed with the help of malicious programs, as well as ways to protect against them.*

Keywords: *computer virus, morris worm, ecosystem, ransomware, credentials, Monero cryptocurrency*

Бугунги ривожланиб бораётган ахборот технологиялари инсон ҳаётини енгиллаштириш ва вақтини тежаш билан бир қаторда кўплаб муаммоларни ҳам келтириб чиқармоқда. Ўзларининг ғаразли мақсадларини амалга оширишда ахборот технологиялари имкониятларидан кенг фойдаланаётган фирибгарлар бугунги киберхавфсизлик соҳасига хавф туғдирмоқда. Фирибгарлар томонидан фойдаланилаётган зарарли дастурлар (вируслар)нинг эволюцияси ва уларнинг тарқалиши бутун дунё бўйлаб маьлумотларнинг махфийлиги, ишончлилиги ва энг муҳими ҳимояланганлик каби талабларнинг бузилишига олиб келмоқда.

Рақамли дунёда вирус атамаси кенг тарқалган бўлиб, зарарли дастурларнинг деярли барча турлари учун қўлланилади. Компьютер вируси атамасининг пайдо бўлишига 1983 йилда хавфсизлик семинарида Фред Коен ўзи яратган дастур орқали кўплаб компьютерларни зарарлаганлиги сабаб бўлган. Яратилган дастур оддий вирус каби бир компьютердан иккинчи компьютерга ўтганлиги ва тез тарқалганлиги боис "компьютер вируси" деб номланган.

Зарарли дастурларнинг эволюцияси катта даврни ўз ичига олмасада, шу қисқа вақт давомида уларнинг кўплаб турлари яратилди. Замонавий зарарли дастурларнинг илк кўринишларидан бири Карнел университети аспиранти Роберт Морис томонидан ишлаб чиқилиб, 1988 йил 2 ноябрь куни Интернет тармоғига жойлаштирилган[1]. Унинг номи "Morris worm" *(Моррис чувалчанги)* бўлиб, у Интернет орқали тарқаладиган биринчи тармоқ чувалчанг

[1] https://uz.wikipedia.org/wiki/Kompyuter_virusi

вирусларидан бири ҳисобланади. “Morris worm” вирусининг тарқалиши натижасида Интернет фойдаланувчиларига 96,5 миллион доллар миқдорида зарар етказилган. Дастлаб зарарли дастурлар қизиқиш ва тажриба ўтказиш мақсадида фойдаланилган бўлса, бугунги кунга келиб улар маълумотларни ўғирлаш, жосуслик, геосиёсий манипуляция ва бошқа ғаразли мақсадларни амалга ошириш учун яратилаётган мураккаб экотизимга айланди.

Зарарли дастурлар ёрдамида содир этилаётган кибержиноятлар сонининг ортишига даркнетда сотиладиган ҳар хил турдаги арзон вирусли дастурлар мавжудлиги ҳам ёрдам бермоқда. Зарарли дастурларни сотиб олиш, лойиҳалаш ва тарқатиш учун малакали дастурчи бўлиш ёки махсус техник билимга эга бўлиш шарт эмас. Зарарли дастурлар тўпламлари ёрдамида кучли зарарли дастурларни осонгина яратиш ва уни ташкилот ичида тарқатиш мумкин.

Кенг тарқалган зарарли дастурлардан бири “Ransomware” бўлиб, улар фойдаланувчи компьютеридаги файлларга киришни чеклаб қўяди. Ушбу файлларни қайтариб олиш учун шифрни очиш калити зарур. Калит киберҳужум ташкилотчиси юборган ҳисоб-рақамга белгиланган миқдордаги пуллар ўтказилгандан сўнг тақдим этилади, аммо ҳар сафар ҳам тўлов амалга оширилгандан сўнг жабрланувчиларга уларнинг маълумотлари қайтариб берилмайди.

Статистик маълумотларга кўра, 2023 йилда “Ransomware” зарарли дастурларидан зарар кўрганлар сони 2022 йилдагига қараганда 70% га ўсган. Сўнги 3 йил ичида амалга оширилган киберҳужумлар сони таҳлил қилинганда 2021 йилда 304 миллион, 2022 йилда 236.1 миллион маротаба амалга оширилганлигини кўришимиз мумкин.[2] Бундай кўнгилсиз ҳодисаларнинг олдини олиш мақсадида “Google” ҳар ҳафтада зарарли дастурларни ўз ичига олган 50 та веб сайтни аниқлаб блоклаш чораларини кўради.

Зарарли дастурларнинг кенг кўламли хавф туғдиришининг яна бир сабаби уларнинг тарқалиш йўллари бўлиб, улар турли йўллар билан тарқалади. Мисол учун, электрон почта хабарлари, зарарланган веб-сайтлар ва бошқалар. Зарарли дастурларнинг кенг тарқатишнинг энг содда ва самарали йўли электрон почта хабарлари ҳисобланади. Зарарли кодлар ПДФ ёки бошқа ҳужжатлар кўринишда бўлиб, фойдаланувчилар файлларни очишлари билан зарарли файллар қурилма хотирасига ўрнашиб олиб қурилманинг нормал ишлашишига таъсир қилиши, маълумотларни ўчириб

[2] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

юбориши ёки учинчи шахсларга шахсий маълумотларни қўлга киритиши учун имкон яратиб бериши мумкин.

Зарарли дастурларнинг таъсири кенг кўламли бўлиб нафақат мамлакатнинг ижтимоий, иқтисодий ва сиёсий соҳаларига балки оддий Интернет фойдаланувчиларига ҳам катта хавф туғдириши мумкин. Зарарли дастурларнинг энг сезиларли таъсиридан бири унинг иқтисодий нархидир. Зарарли дастурлар орқали амалга ошириладиган киберҳужумлар катта молиявий йўқотишларга олиб келиши билан бир қаторда маълумотларнинг ўғирланиши, интеллектуал мулк ҳуқуқларининг бузилиши ва тизимни тиклаш билан боғлиқ катта сарф-харажатлар каби кўнгилсиз оқибатларга олиб келади. 2023 йилда маълумотларнинг ўғирланиши оқибатида 4,45 миллион доллар миқдорида зарар кўрилган. “Ransomware” зарарли дастурлари орқали етказилган зарар миқдори эса 5,13 миллион долларни ташкил этади, бу 2022 йилга нисбатан 13 фоизга юқори.

Кибер таҳдидлар ландшафтининг ўзгариши 2023 йилда тўлов дастурлари ва бошқа кўплаб соҳаларда катта таҳдидларнинг пайдо бўлишига олиб келди. Хакерлар катта саноат индустриялари тизимига бузиб кириш ва маълумотларни қўлга киритиш учун оммавий киберҳужумларнинг янги, шунингдек ўзига хос бўлган турларини яратишмоқда. Хусусан, кибер жиноятчилар аутентификация маълумотларини қўлга киритишни жуда яхши кўрадилар, чунки аутентификация маълумотлари улар ўйлаган ғаразли мақсадларини амалга ошириш ва ҳар қандай тизимга киришнинг ишончли, самарали ҳамда энг муҳими хавфсиз усулидир.

Хакерлар аутентификация маълумотларини одатда зарарли веб-сайтлар, ботнетлар ёки фишинг электрон почта хабарларини тарқатиш орқали қўлга киритишлари мумкин. Бунда фойдаланувчи зарарли ҳаволага кириши натижасида қурилмадаги карта маълумотлари, ҳимоя пароллари, шахсий ёзишмалар ва шунга ўхшаш бошқа шахсий маълумотларидан ҳаттоки қурилманинг “cookie” файлларидан ҳам нусха кўчириб олишлари мумкин. Бундан ташқари, доимий равишда бир хил ҳимоя паролларидан фойдаланадиган Интернет фойдаланувчиларинг хакерлардан жабрланиш эҳтимоли бир неча баробарга ошиб кетади. “SpyCloud” тадқиқотлари шуни кўрсатадики, 2022 йилда маълумотлари икки ёки ундан кўп маротаба бузилган Интернет фойдаланувчиларининг 72 % ўз ҳимоя паролларини илова ва дастурларда қайта

фойдаланган[3]. Бу эса ҳар тўрт кишидан деярли уч нафари хакерлар томонидан ўғирланган ҳимоя паролларидан яна қайта фойдаланганлигини билдиради.

Зарарли дастурий таъминотларнинг доимий равишда янгиланиб бораётганлиги киберхавфсизлик воситалари ва стратегияларининг ҳам муттасил ривожланишини талаб қилади. Зарарли дастурларнинг тарқалиши турли соҳалардаги ташкилотларда кибер таҳдидларга қарши ҳимояни кучайтириш учун зарарли дастурларни таҳлил қилиш, тескари муҳандислик ва киберҳужумларга жавоб бериш бўйича юқори малакага эга мутахассисларга бўлган талабни ошириб боради.

Зарарли дастурлардан ҳимояланишнинг оддий ва самарали йўли бу антивирус дастурларини ўрнатиш ва улардан фойдаланиш. Аммо ҳар доим ҳам антивируслар қурилмани тўла ҳимоя қила олмайдилар. Мисол учун, “Доктор Веб” компанияси мутахассислари ўрнатилиши вақтида компьютердаги антивирус дастурини ўчириб ташловчи вирусни аниқланганликларини маълум қилишди. “Linux.BtcMine.174” деб номланувчи ушбу троян вируси компьютерга тушганда “Linux.BackDoor.Gates.9” деб номланувчи ва ДДоС-ҳужумларида иштирок эта олувчи бошқа вирусни ўрнатади. Сўнгра вирус компьютерда бошқа рақобатчи вирус-майнерларни излаб, уларни ёпади. Кейин эса антивирус дастурларини қидириб, уларни ўчириб ташлайди. Шундан кейин “Monero” криптовалютасини майнинг қилиш жараёнини ишга туширади.[4] Вирусли дастур ўзини-ўзи тўғри ишлаётганини мунтазам текшириб туради ва муаммо ҳолатида уни қайта юклайди ҳамда доимий янгиланмаларни ўрнатиб туради. Мутахассислар янги вирусдан ҳимояланиш учун антивирус тизимларини тез-тез янгилаб туришни тавсия қилишади.

Зарарли дастурларнинг киберхавфсизлик соҳасига таъсири иқтисодий, ижтимоий, ҳатто сиёсий жараёнларни қамраб олиши жиддий муаммоларни келтириб чиқарсада, у инновацияларни рағбатлантиради, ҳамкорликни ривожлантиради ва ўзаро боғланган рақамли дунёмизда киберхавфсизликнинг муҳим аҳамиятини оширади. Кибертаҳдидлар ривожланишда давом этар экан, киберхавфсизлик саноатида пайдо бўлаётган таҳдидлардан самарали ҳимоя қилиш ва уларнинг таъсирини камайтириш учун ҳар томонлама замон талабларига мос бўлиши лозим.

[3] https://spycloud.com/resource/2023-annual-identity-exposure-report/
[4] https://bitnovosti.io/2018/11/22/doktor-veb-obnaruzhil-virus-dlya-skrytogo-majninga-monero/

KIBERMAKONDA POTENSIAL TAHDIDLARNI ANIQLASHDA KIBERRAZVEDKA AMALIYOTINING USUL VA VOSITALARI

G‘aniyev Abduxalil Abdujaliovich
PhD, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti dotsenti, Toshkent shahar, +998998356730
Tojimatov Dostonbek Xomidjon o’g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali katta o’qituvchisi, Farg‘ona shahar,
+998902322743

Annotatsiya: *Kiberrazvedka amaliyoti bu kibermakonda axborot aktivlari bo’ladigan har qanday tahdid yoki xavflarni aniqlash, identifikatsiyalash, turlarga ajratish, reaksiya strategiyasini tuzishga qaratilgan keng qamrovli ma’lumotlarni yig‘ish jarayoni hisoblanadi. Shu sababli ushbu maqolada potensial tahdidlarni aniqlashda kiberrazvedka amaliyotining maqola kibertahdidlarni oldini olishda kiberrazvedka amaliyotini hozirgi kundagi dolzarbligi, kiberrazvedka olib borishning usul va vositalarini tavsiflash va tushuntirishga qaratilgan. Maqolada kibermudofa samarodorligini oshirish, turli kibertahdid qarshi tizimli imunitet reaksiyasini rivoshlantirish bo’yicha keltirilgan usul va vositalarni takomillashtirish bo’yicha taklif va yondashuvlar berib o’tilgan.*

Kalit so’zlar: *kiberrazvedka, kibertahdid, avtomatlashtirish, kiberhujum, integratsiya, tarmoq monitoring, sun’iy intelekt, mashinali o’qitish, tahdid zanjiri proaktiv jarayon, maltego, shodan, darktrase, splunk, axborot aktivi*.

Аннотация: *Практика киберразведки представляет собой комплексный процесс сбора данных, направленный на выявление, идентификацию, классификацию и создание стратегии реагирования на любые угрозы или риски для информационных активов в киберпространстве. Поэтому цель данной статьи – описать и объяснить современную актуальность практики киберразведки в предотвращении киберугроз, методы и средства проведения киберразведки. В статье представлены предложения и подходы по совершенствованию методов и средств повышения эффективности киберзащиты, развития системного иммунного ответа против различных киберугроз.*

Ключевые слова: *киберразведка, киберугроза, автоматизация, кибератака, интеграция, сетевой мониторинг, искусственный интеллект, машинное обучение, упреждающий процесс цепочки угроз, Maltego, Shodan, Darktrace, Splunk, информационный актив.*

Abstract: *The practice of cyber intelligence is a comprehensive data collection process aimed at identifying, identifying, classifying, and creating a response strategy for any threats or risks to information assets in cyberspace. Therefore, this article aims to describe and explain the current relevance of cyber intelligence practice in the*

prevention of cyber threats, the methods and means of conducting cyber intelligence. The article provides proposals and approaches for improving the methods and tools for increasing the effectiveness of cyber defense, developing systemic immune response against various cyber threats.

Keywords: *cyber intelligence, cyber threat, automation, cyber attack, integration, network monitoring, artificial intelligence, machine learning, threat chain proactive process, maltego, shodan, darktrace, splunk, information asset.*

Hozirgi kunda butun dunyoda raqamlashtirirish jarayoni jadal rivojlanib bormoqda. Raqamlashtirish jarayoni deyarli barcha sohalarni (davlat boshqaruvi, mudofaa, iqtisodiyot, ishlab chiqarish, oziq-ovqat, sanoat, xizmat ko'rsatish va boshqa) qamrab olmoqda. Bu o'z navbatida katta ma'lumotlarga asoslangan virtual olam, ya'ni kibermakonni kengayib borishiga xizmat qilmoqda. Kibermakon[1] qanchalar kengaygani sari unda uchraydigan, axborot aktivlarini o'g'irlashga, yo'q qilishga, o'zgartirishga qaratilgan kibertahdidlar[2], kiberxujumlar, internet firibgarliklari ham ko'payib bormoqda. Bu kiberxavfsizlik[3] sohasi mutaxasislarini axborotlarni himoyalashga qaratilgan chora tadbirlari va amaliy harakatlarini izchil rivojlantirib borish zaruriyatini keltirib chiqarmoqda.

Kiberxavfsizlikni ta'minlash uchun kibermudofaa strategiyasini ishlab chiqish muhim omil hisoblanadi. Kibermudofaa strategiyasi uchun esa kibertahdidlar va ularni ish prinsiplarini tushunish haqidagi ishonchli ma'lumotlar kerak bo'ladi. Bunday ma'lumotlar kiberrazvedka amaliyoti orqali qo'lga kiritiladi.

Kiberrazvedka soha tashkilotlari kiberxavfsizligiga bo'ladigan tahdidlar haqida ma'lumot to'plash, tahlil qilish va almashishni o'z ichiga oladi. Bu tashkilotlarga potentsial kibertahdidlarni tushunish, sodir etilishi mumkin bo'lgan hujumlarni bashorat qilish va himoya choralarini tayyorlashga yordam beradi.

Hozirgi kunda kiberrazvedka amaliyoti tahdidlar ko'lamiga qarab uchta:

- *strategik;*
- *operativ;*
- *taktik;*

[1] O'zbekiston Respublikasining "Kiberxavfsizli to'g'risidagi" O'RQ-764-son qonuni., kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit;

[2] O'zbekiston Respublikasining "Kiberxavfsizli to'g'risidagi" O'RQ-764-son qonuni., kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

[3] O'zbekiston Respublikasining "Kiberxavfsizli to'g'risidagi" O'RQ-764-son qonuni., kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

yo’nalishlarda olib boriladi va xar bir tur bo’yicha erishiladigan natijalar 1-rasmda keltirilgan savollarga yechimlarni o’z ichiga olishni taqazo etadi.

1-rasm. Kiberrazvedka amaliyoti turlari.

Strategik kiberrazvedka tahdidlar haqida umumiy ma’lumot beradi. Amaliyotdan olingan hisobotlardagi topilmalar asosida yuqori darajadagi tashkiliy strategiyani ishlab chiqishga hizmat qiladi. Ideal holda, strategik kiberrazvedka tashkilotning tahdidlar landshafti bilan bog‘liq zaifliklar va xavflar, profilaktik harakatlar, tahdid qiluvchilar, ularning maqsadlari va potentsial hujumlarning jiddiyligi kabi tushunchalarni beradi. Tahdidlarni amalga oshirishda “kim va nima uchun?” degan savolga javob beradi[4].

Operativ kiberrazvedka hujumlar haqidagi bilimlarga e'tibor qaratadi. U hujumning tabiati, motivi, vaqti va qanday hamda qayerdan amalga oshirilishi kabi omillar haqida batafsil ma’lumot beradi. Ideal holda, ma’lumotlar xakerlar chat xonalaridan yoki ularni onlayn muhokama qilish orqali infiltratsiya orqali yig‘iladi.

Taktik kiberrazvedka yaqin kelajakda sodir etilishi mumkun bo’lgan tahdidlarni aniqlash va ularni amaga oshirish usullari, texnikasi, hamda tartiblarini tushunish uchun olib boriladi. Taktik kiberrazvedkada asosan aniqlanga tahdidlar keng tarqalgan tahdid bazalariga solishtirilib, unga qarshi ishlab chiqilgan chorlar haqida hisobotlarni tayyorlaydi[5].

Kiberrazvedkani amalga oshirishning turli usullar mavjud va ular odatda quyidagi toifalarga bo’linadi:

[4] Constance S. Uthoff., Cyber Intelligence: Actors, Policies, and Practices., Copyright © 2022, Chiristopher Ahlberg., The Threat Intelegence Handbook”., Second edition., CyberEdge Group, LLC-2019, Tojimatov, D. (2023, October). Kiberrazvedkani amalga oshirishda sun’iy intelekt texnologiyalarini o’rni. In Conference on Digital Innovation:" Modern Problems and Solutions,

[5] Constance S. Uthoff., Cyber Intelligence: Actors, Policies, and Practices., Copyright © 2022, 13-bet

1. Ma’lumotlar yig‘ish toifasi.

- Open Source Intelligence (OSINT): Ijtimoiy tarmoqlar, forumlar, bloglar va yangiliklar maqolalari kabi hammaga ochiq manbalardan ma’lumot to’plash.
- Yopiq manba razvedkasi: obunaga asoslangan xizmatlar, xususiy ma’lumotlar bazalari va xususiy manbalardan ma’lumotlarni to’plash.
- Texnik razvedka: zararli dastur namunalaridan ma’lumotlarni to’plash, murosa ko’rsatkichlari (IoCs) va tarmoq trafigini tahlil qilish.
- Inson razvedkasi (HUMINT): Insayder hisobotlari, intervyular va boshqa tashkilotlar bilan hamkorlik kabi inson manbalaridan olingan ma’lumotlar.

2. Ma’lumotlarni qayta ishlash va tahlil qilish toifasi.

- Mashinali o’qitish va sun’iy intelekt: Katta hajmdagi ma’lumotlarni qayta ishlash, naqshlarni aniqlash va potentsial tahdidlarni bashorat qilish uchun algoritmlardan foydalanish.
- Tahdid korrelyatsiyasi: potentsial tahdidlarni aniqlash uchun turli ma’lumotlar nuqtalari o’rtasidagi munosabatlarni tahlil qilish.
- Xulq-atvor tahlili: tahdidni ko’rsatishi mumkin bo’lgan anomaliyalarni aniqlash uchun foydalanuvchilar va tizimlarning xatti-harakatlarini kuzatish va tahlil qilish.
- Kontekstli tahlil: Tashkilotning o’ziga xos muhiti va tahdid landshaftini hisobga olgan holda tahdid ma’lumotlarining dolzarbligini baholash.

3. Tahdid atributi toifasi.

- Barmoq izlari: hujumlar yoki tajovuzkorlarning o’ziga xos xususiyatlarini aniqlash, ularni muayyan tahdid ishtirokchilariga bog‘lash.
- Hujum zanjiri tahlili: hujumchining usullari va motivlarini tushunish uchun hujumdagi voqealar ketma-ketligini o’rganish.
- Geosiyosiy kontekstualizatsiya: geosiyosiy voqealar va motivlarning kengroq kontekstida kibertahdidlarni tahlil qilish.

4. Tarqatish va almashish toifasi

- Tahdid razvedkasi platformalari (TIPs): Tahdid ma’lumotlarini tashkil qilish, saqlash va boshqa tashkilotlar bilan almashish uchun vositalar va platformalar.
- Axborot almashish va tahlil markazlari (ISACs): a’zolar o’rtasida kibertahdid ma’lumotlarini almashishni osonlashtiradigan sohaga oid tashkilotlar.

- Huquqni muhofaza qilish va xavfsizlik oraganlari bilan hamkorlik: razvedka ma’lumotlarini almashish va jamoaviy choralar ko’rish uchun tashqi agentliklar bilan yaqindan hamkorlik qilish.

5. Faoliyatli razvedka toifasi.

- Voqealarga javob berishni rejalashtirish: Hodisalarga javob berish rejalarini xabardor qilish va takomillashtirish uchun CTI-dan foydalanish.
- Proaktiv mudofaa: potentsial hujumlarning oldini olish uchun bashoratli razvedkaga asoslangan xavfsizlik choralarini qo’llash.
- Tahdid ovlash: Tashkilot muhitidagi tahdidlarni voqea sodir bo’lishidan oldin faol ravishda izlash.

6. Baholash va fikr-mulohazalar toifasi.

- Doimiy takomillashtirish: Kiberrazvedka usullarining samaradorligini muntazam ravishda baholash va ularni yangi axborot va texnologiyalar asosida yangilash.
- Hodisadan keyingi tahlil: O’tmishdagi voqealardan olingan saboqlardan tahdidlar bo’yicha razvedka amaliyotini takomillashtirish uchun foydalanish.
- Ushbu usullar birgalikda kibertahdidlarni aniqlash, tushunish va yumshatish uchun kompleks yondashuvni tashkil qiladi.
- Kiberrazvedka nafaqat sodir etilgan kiberjinoyatlar, balki kelajakda sodir etilishi mumkun bo’lgan potensial kibertahdidlarni aniqlash va ularni oldini olishga ham xizmat qiladi.

Yuqorida keltirilgan usullardan foydalanib potensial tahdidlarni aniqlashning keng qo’llaniladigan turli vositalari mavjud bo’lib bularga quyidagilarni misol qilib keltirish mumkun.

1. Open Source Intelligence (OSINT) vositalari

- **Maltego:** aloqalar va aloqalarni xaritalash uchun hammaga ochiq ma’lumotlarni yig‘ish va tahlil qilish uchun platforma.
- **Shodan:** Internetga ulangan qurilmalarni topish uchun qidiruv tizimi, ochiq yoki zaif tizimlarni aniqlash uchun foydalaniladi.
- **Recon-ng:** Ochiq manbalardan ma’lumot yig‘ish jarayonini avtomatlashtiradigan veb-razvedka tizimi.

2. Tahdid razvedka platformalari (TIPs)

- **Threat Connect:** Tashkilotlar bo’ylab tahdidlar haqidagi ma’lumotlarni yig‘ish, tahlil qilish va almashish uchun platforma.
- **Anomali ThreatStream:** Haqiqiy vaqtda tahdid haqida ma’lumot beruvchi va tahdidlarni aniqlash va javob berish jarayonini avtomatlashtiradigan platforma.

- **Recorded Future:** Haqiqiy vaqtda tahdid haqida ma'lumot berish uchun mashinani o'rganish va tabiiy tilni qayta ishlashdan foydalanadigan platforma.

3. Tarmoq trafigini tahlil qilish vositalari

- **Wireshark:** real vaqt rejimida tarmoq trafigini ushlaydigan va ular bilan o'zaro ta'sir qiluvchi tarmoq protokoli analizatori.
- **Bro (Zeek):** Tarmoq trafigini tahlil qilish va xavfsizlik hodisalarini aniqlash uchun kuchli platformani ta'minlovchi tarmoq monitoringi tizimi.
- **NetFlow:** Monitoring va tahlil qilish uchun IP-trafik ma'lumotlarini to'playdigan Cisco routerlaridagi xususiyat.
- Zararli dasturlarni tahlil qilish vositalari
- **IDA Pro:** Zararli dasturlarni va teskari muhandislikni tahlil qilish uchun ishlatiladigan kuchli qismlarga ajratuvchi va tuzatuvchi.
- **Cuckoo Sandbox:** Shubhali fayllarni ularning xatti-harakatlarini kuzatish uchun izolyatsiya qilingan muhitda bajaradigan avtomatlashtirilgan zararli dasturlarni tahlil qilish tizimi.
- **YARA:** Ikkilik fayllardagi naqshlar asosida zararli dasturlarni aniqlash va tasniflash uchun vosita.

4. Xulq-atvorni tahlil qilish vositalari

- **Splunk:** Veb uslubidagi interfeys orqali mashina tomonidan yaratilgan katta ma'lumotlarni qidirish, kuzatish va tahlil qilish uchun platforma.
- **Darktrace:** tarmoq trafigining xulq-atvori tahlili asosida tahdidlarni aniqlash, ularga javob berish va tekshirish uchun AIdan foydalanadigan vosita.
- **Elastik xavfsizlik:** xatti-harakatlar tahlilidan foydalangan holda real vaqtda tahdidlarni aniqlash, oldini olish va javob berishni ta'minlaydigan yechim.

5 . Hamkorlik va almashish vositalari

- MISP (Zararli dasturiy ta'minot ma'lumotlarini almashish platformasi): tashkilotlar o'rtasida tahdidlar haqida ma'lumot almashishni osonlashtiradigan ochiq manba platformasi.
- STIX/TAXII: Tashkilotlar o'rtasida avtomatlashtirilgan almashinuvni ta'minlovchi kibertahdid ma'lumotlarini taqdim etish va almashish standartlari.

6. Voqealarga javob berish vositalari

- **TheHive:** Turli xil tahdidlarni razvedka manbalari va tahlil vositalari bilan integratsiyalashgan ochiq manbali xavfsizlik hodisalariga javob berish platformasi.

- **Cortex:** Kuzatiladigan narsalarni (IP manzillar, domenlar, fayllar) tahlil qilish va ularni tahdid razvedkasi ma’lumotlari bilan ulash uchun ishlatiladigan ochiq manbali vosita.
- **SOAR:** Hodisalarga javob berish jarayonlarini soddalashtirish va avtomatlashtirishga yordam beradigan xavfsizlikni boshqarish, avtomatlashtirish va javob berish (SOAR) platformasi.

Yuqorida keltirlgan usullar va vositalar samarali kiberrazvedka operatsiyalari uchun zarur bo’lib, tashkilotlarga potentsial tahdidlardan oldinda turishga va hodisalarga tezkor javob berishga yordam beradi. Lekin kibertahdidlar potensial bo’lganligi sababli bunday usul va vositalardan foydalanish doim ham samarali hisoblanmaydi. Chunki tahdidlarni qachon va qaysi qatlamda hamda qanday darajada sodir etilishini bashorat qilish ko’p omillarga bog‘liq. Bu o’z navbatida vaqt masalasini o’rtaga chiqaradi. Qaysidir usul va vositani qo’llagan holda razvedka qilinayotgan vaqtda amaliyotdan tashqari bo’lgan kutilmagan tahdid sodir etilishi mumkun. Barcha usul va vositalardan esa bir vaqtni o’zida foydalanishning texnik imkoniyati kam va turli xatoliklar yuzaga kelish ehtimolligi yuqori hisoblanadi[6].

Shu sababli barcha jixatlarni hisobga olgan holda potensial tahdidlarni samarali aniqlashda kiberrazvedka usul va vositalarni takomillashtirish bo’yicha quyidagi strategiyalar va yondashuvlarni taklif qilamiz.

1. Ma’lumotlar to’plashni jarayonini takomillashtirish.

Turli xil ma’lumotlar manbalarini integratsiyalash: kengroq manbalardan olingan ma’lumotlarni, shu jumladan qorong’u veb monitoringi, tahdidlar haqida razvedka tasmasi, ijtimoiy media va ichki jurnallarni birlashtirish. Ushbu ko’p manbali yondashuv potentsial tahdidlarning yanada kengroq ko’rinishini ta’minlaydi.

Avtomatlashtirilgan OSINT to’plami: Ochiq manba ma’lumotlarini doimiy ravishda to’playdigan va yangilaydigan, yangi tahdidlarni aniqlash uchun ketadigan vaqtni qisqartiradigan avtomatlashtirilgan vositalarni joriy qilish.

IoT va oxirgi nuqta monitoringi: Internet of Things (IoT) qurilmalari va so’nggi nuqtalarini o’z ichiga olish uchun monitoring imkoniyatlarini kengaytirish, chunki bular ko’pincha kiberhujumlar uchun maqsadli kirish nuqtalari hisoblanadi.

2. Kengaytirilgan tahlil va mashinali o’qitishni takomillashtirish.

[6] Yevropa ittifoqi kiberxavfsizlik agentigining “Threat Landscape Report” hisoboti., 2023/19/10, Chiristopher Ahlberg., The Threat Intelegence Handbook”., Second edition., CyberEdge Group, LLC-2019

Xulq atvor tahlili qo’llash. Bu tarmoqlar, tizimlar va foydalanuvchi faoliyatidagi normal xatti-harakatlardan og‘ishlarni aniqlay oladigan mashinani o’rganish modellarini joriy qilish. Anomaliyalarni aniqlashda aniqlikni oshirish uchun ushbu modellar katta ma’lumotlar to’plamlarida o’qitilishi kerak.

Sun’iy intellekt yordamida tahdidlarni aniqlash. Bu katta hajmdagi ma’lumotlarni tezda tahlil qilish, inson tahlilchilariga ko’rinmasligi mumkin bo’lgan murosa ko’rsatkichlarini (IoC) aniqlash uchun sun’iy intellektdan (AI) foydalanish.

Real vaqt rejimida ma’lumotlarni qayta ishlash: Xotirada hisoblash va parallel ishlov berish usullaridan foydalangan holda ma’lumotlarni qayta ishlash tezligini oshirish, bu tahdidlarni bir zumda aniqlash imkonini beradi.

3. Tahdidlar nisbati va korrelyatsiyasini aniqlashni takomillashtish.

Platformalar o’rtasidagi korrelyatsiya: Ko’p vektorli hujumlarni erta aniqlash uchun turli platformalar va muhitlar (masalan, bulut, mahalliy, mobil) ma’lumotlarini o’zaro bog‘lashi mumkin bo’lgan vositalarni qo’llang.

Kengaytirilgan barmoq izlari texnikasi: Noyob hujum imzolarini aniqlashning yanada murakkab usullarini ishlab chiqish, bu esa ma’lum bo’lgan tahdid ishtirokchilariga tezroq bog‘lanish imkonini beradi.

Tahdid ishtirokchilari profilini yaratish: tahdid ishtirokchilarining batafsil profillarini yaratish uchun katta ma’lumotlar tahlilidan foydalanish, bu ularning keyingi harakatlarini bashorat qilishga va tahdidlarni avvalroq aniqlashga yordam beradi.

4. Tahdid zanjirining proaktiv jarayonida tahdidlarni ovlash

Avtomatlashtirilgan tahdidlarni ovlash: tarmoq ichidagi potentsial tahdidlarni doimiy ravishda qidirish uchun sun’iy intellekt va avtomatlashtirishdan foydalaning va tahdidlarni qo’lda ovlash harakatlariga bog‘liqlikni kamaytiring.

Gipotezaga asoslangan ov usulini qo’llash. Bu tahdidlarni ovlashga tizimli yondashuvni rag‘batlantiring, bunda potentsial tahdidlar haqidagi maxsus farazlar ma’lumotlar tahlili va mashinani o’rganish yordamida sinovdan o’tkaziladi.

Qizil va ko’k jamoalar hamkorligi: hujumlarni simulyatsiya qilish va aniqlash imkoniyatlarini yaxshilash uchun qizil (hujum) va ko’k (mudofaa) jamoalari o’rtasidagi hamkorlikni kuchaytirish. Bu uzluksiz qayta aloqa halqasi vositalar va strategiyalarni takomillashtirishga yordam beradi.

5. Hamkorlik va axborot almashishni takomillashtirish.

Haqiqiy vaqtda razvedka ma’lumotlarini almashish: avtomatlashtirilgan, xavfsiz ma’lumotlar almashinuvini qo’llab-quvvatlaydigan platformalardan foydalangan holda, sanoatdagi tengdoshlar va tegishli manfaatdor tomonlar bilan tahdidlar haqidagi ma’lumotlarni almashish tezligi va samaradorligini oshiring.

Tahdid ma’lumotlarini standartlashtirish: ma’lumotlarning turli xil vositalar va platformalarga osongina integratsiyalashuvini ta’minlash uchun tahdidlar haqidagi ma’lumotlarni almashish uchun standartlashtirilgan formatlarni (masalan, STIX/TAXII) qabul qilish va ulardan foydalanishni targ‘ib qilish. Ko’p manbali tahdidlarni aniqlash: Bir nechta tashkilotlar umumiy razvedkaga hissa qo’shadigan va undan foyda ko’radigan hamkorlikda tahdidlarni aniqlash harakatlarida ishtirok etish.

6. Integratsiya va avtomatlashtirishni takomillashtirish.

Xavfsizlikni tartibga solish, avtomatlashtirish va javob berish (SOAR): SOAR platformalarini muntazam tahdidlarni aniqlash va ularga javob berish vazifalarini avtomatlashtirish, xavfsizlik tahlilchilariga yanada murakkabroq masalalarga e’tibor qaratish imkonini beradi.

Yagona tahdidlarni boshqarish (UTM): Har tomonlama tahdidlarni aniqlash va javob berish imkoniyatlarini ta’minlash uchun bir nechta xavfsizlik funktsiyalarini (masalan, xavfsizlik devori, hujumni aniqlash, antivirus) yagona platformaga birlashtirish. Bulutli mahalliy xavfsizlik vositalari: bulutga asoslangan aktivlar mahalliy tizimlar kabi samarali nazorat qilinishini ta’minlab, dinamik, kengaytiriladigan muhitda ishlashga mo’ljallangan bulutli mahalliy xavfsizlik vositalaridan foydalanish.

7. Uzluksiz o’rganish va takomillashtirish

Moslashuvchan mashinani o’rganish modellari: Vaqt o’tishi bilan moslashadigan va o’rganadigan, yangi va rivojlanayotgan tahdidlarni aniqlash qobiliyatini yaxshilaydigan mashinani o’rganish modellaridan foydalanish.

Tahdidlarni simulyatsiya qilish va o’qitish: Doimiy ravishda tahdid simulyatsiyasini o’tkazing (masalan, qizil jamoalar, penetratsion testlar) va xavfsizlik guruhlarini aniqlash va javob berish ko’nikmalarini yaxshilash uchun doimiy treninglar o’tkazish.

Teskari aloqa davrlari: Aniqlangan tahdidlar va hodisalarning natijalari tahlil qilinadigan va aniqlash usullari va vositalarini takomillashtirish uchun foydalaniladigan uzluksiz teskari aloqa davrlarini o’rnatish.

8. Foydalanuvchi va shaxs xatti-harakatlari tahlili (UEBA)

Kontekstdan xabardorlik: noto’g‘ri pozitivlarni kamaytirish va aniqlashning aniqligini oshirish uchun foydalanuvchi rollari, tarixiy xatti-

harakatlar va atrof-muhit omillari kabi kontekstual ma’lumotlarni o’z ichiga olish uchun UEBA vositalarini yaxshilash.

Kengaytirilgan anomaliyalarni aniqlash: Oddiy xatti-harakatlardan yomon va zararli og‘ishlarni ajrata oladigan yanada murakkab anomaliyalarni aniqlash algoritmlarini joriy qilish.

9. Bashoratli tahlil usullarini qo’llash.

Tahdidlarni bashorat qilish: tarixiy ma’lumotlar, paydo bo’lgan tendentsiyalar va tahdid aktyorining ma’lum xatti-harakati asosida potentsial tahdidlarni taxmin qilish uchun bashoratli tahlillardan foydalanish. Bu tashkilotlarga himoyani oldindan tayyorlash imkonini beradi.

Xatarlarni baholash: Turli faoliyatlar, aktivlar yoki foydalanuvchilarga xavf darajasini belgilaydigan, ustuvor monitoring va yuqori xavfli vaziyatlarga tezroq javob berishga imkon beruvchi xavflarni baholash tizimlarini joriy qilish.

10. Hodisalarga tezkor javob berish integratsiyasini takomillashtirish.

Avtomatlashtirilgan hodisaga javob berish: Ba’zi tahdid mezonlari bajarilganda oldindan belgilangan javob harakatlarini avtomatik ravishda boshlash uchun hodisalarga javob berish tizimlari bilan erta aniqlash vositalarini birlashtirish.

Stsenariyga asoslangan qo’llanmalar: javoblarning o’z vaqtida va mos bo’lishini ta’minlash uchun erta aniqlangan tahdidlarning muayyan turlari tomonidan qo’zg‘atiladigan hodisalarga javob berish qo’llanmalarini ishlab chiqish va muntazam yangilash.

Ushbu taklif etilayotgan sohalarga e'tibor qaratish orqali tashkilotlar o’zlarining erta aniqlash imkoniyatlarini sezilarli darajada yaxshilashlari mumkin, bu ularga kibertahdidlarni jiddiy zarar yetkazishidan oldin aniqlash va yumshatish imkonini beradi.

Xulosa

Maqolani yozish davomida soha bo’yicha ko’plab adabiyotlar o’rganilib tahlil qilinib potensial kibertahdidlarni aniqlashdan kiberrazvedka amaliyotini olib borishning usullari bajarilish bosqichlari va toifalari bo’yicha ajratilib tasniflab berildi. Kiberrazvedka usullarini qo’llashda keng tarqalgan vositalar turlari tahlil qilinib, ularni tegishliligi bo’yicha ajratilib tasniflab chiqildi. Kiberrazvedkani samarali amalga oshirish va mavjud muammolarni hal qilish maqsadida mavjud usul va vositalarni takomillashtirish bo’yicha olib borilgan tahlillar asosida yondashuvlar taklif etildi.

KIBER XAVFSIZLIKNING ICHKI ISHLAR ORGANLARI TIZIMIDA TUTGAN O'RNI VA KIBER JINOYATLARNI OLDINI OLISH

Iminov Abdurasul Abdulatipovich
Ichki ishlar vazirligi Akademiyasi
raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig'i.
Kamolov Madrasilla Erkinovich
Ichki ishlar vazirligi Akademiyasi raqamli texnologiyalar
va axborot xavfsizligi kafedrasi katta o'qituvchisi.
Mamatjonov Jahongir Tursunali o'g'li
Ichki ishlar vazirligi Akademiyasi 2-o'quv kursi kursanti

Annotatsiya: *Ushbu maqolada kiberxafsizlikning Ichki ishlar organlarida tutgan o'rni va kiber jinoyatlarni oldini olishga qaratilgan ma'lumotlar berilgan. Internet tarmoqlaridan foydalanib sodir etiladigan huquqbuzarliklarning barvaqt oldini olish masalasi, qonunchilikda belgilab berilgan huquqbuzarliklar profilaktikasining barcha turlari va ularning chora-tadbirlaridan samarali foydalanish, Ichki ishlar organlarini kiberxavsizlikni ta'minlash va kiberjinoyatlarni sodir etilishini profiliktikasi, ularni oldini olish, O'zbekistonda kiberjinoyatchilikning oldini olish tizimini yaratish to'g'risidagi masalalar ko'rib chiqilgan.*

Kalit so'zlar*: kiberxavfsizlik, kibertahdidlar, raqamli ekotizim, chegarasiz jinoyat, kiberjinoyatlar, kiber-terrorizm, kiberharakat, ichki ishlar organlarida kiberxavsizlik, noqonuniy bank-moliya operasiyalari, plastik kartalarga xujum, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o'yinlar.*

Аннотация: *В данной рассмотрены вопросы обеспечения кибербезопасности и представлена информация о роли обеспечения кибербезопасности в органах внутренних дел, предотвращении киберпреступлений, а также рассмотрены вопросы раннего предупреждения преступлений, совершаемых с использованием сетей Интернет, эффективного использования предусмотренных законом всех видов профилактики преступности и их мер обеспечения кибербезопасности органов внутренних дел и создания системы предотвращения киберпреступлений в Узбекистане.*

Ключевые слова: *кибербезопасность, киберугрозы, цифровая экосистема, преступность без границ, киберпреступления, технологии, изобретения, интернет, кибервойна, кибертерроризм, кибербезопасность в органах внутренних дел, незаконные банковские и финансовые операции, пластиковые карты, распространение вредоносных вирусов, азартные игры, онлайн-игры.*

Annotation*: This article considered the issues of cybersecurity and provided information on the role of cybersecurity in law enforcement agencies, the prevention of cybercrime, as well as considered the issues of early prevention of crimes committed using the Internet, the effective use of all types of crime prevention provided by law and their measures to ensure cybersecurity of law enforcement agencies and the prevention of cybercrime, the creation of cybercrime prevention systems in Uzbekistan.*

Keywords: *cybersecurity, cyberthreats, digital ecosystem, crime without borders, cybercrimes, technologies, inventions, Internet, cyberwar, cyberterrorism, cybersecurity in internal affairs agencies, illegal banking and financial transactions, plastic cards, spread of malicious viruses, gambling, online games.*

Bugungi kunda global axborot maydonida kiber makon bilan bog'liq yangidan-yangi tahdidlar yuzaga kelmoqda. Shu bois virtual olamdagi hujumlardan himoyalanish masalasi dunyo hamjamiyatini jiddiy tashvishga solmoqda. Raqamli ekotizimga tayanadigan bugungi texnologik rivojlangan davrda kiberxavfsizlik bo'yicha mustahkam chora-tadbirlarni ta'minlash zarurati muhim ahamiyatga ega. Kibertahdidlar tabiatan turlicha bo'lib, o'zaro bog'langan tizimlarimizdagi zaifliklardan foydalanishga doimo intilayotgan zararli shaxslar soni ortib bormoqda.

Kiberxavfsizlik landshafti doimo yangi tahdid va muammolarga moslashib, rivojlanib boradi. Korxonalar, jismoniy shaxslar va tashkilotlar uchun o'zlarining kiberxavfsizlik amaliyotlarida xabardor va faol bo'lishlari juda muhimdir. Kiberxavfsizlik sohasidagi muhim jihatlarni o'rganib chiqib, biz xavf-xatarlarga samarali qarshi tura olamiz va raqamli himoyamizni mustahkamlay olamiz.

Mamlakatimizda fuqarolarimizni uzog'ini yaqin qilishga, yashash sharoitlarini zamonaviy shaklda o'zgartirishga qaratilgan sog'lom Internet-muhitiga ega axborotlashgan jamiyatni rivojlantirishga alohida e'tibor qaratilgan. Internet tarmoqlaridan foydalanib sodir etiladigan huquqbuzarliklarning barvaqt oldini olish masalasida qonunchilikda belgilab berilgan huquqbuzarliklar profilaktikasining barcha turlari va ularning chora-tadbirlaridan samarali foydalanish lozim. Ichki ishlar organlarini kiberxavsizlikni ta'minlash va kiberjinoyatlarni sodir etilishini profiliktikasi, ularni oldini olish borasida O'zbekiston Respubikasining "Huquqbuzarliklar profilaktikasi to'g'risida"gi Qonuni bilan profilaktikasining turlari belgilab berilgan. Shuningdek, O'zbekiston Respublikasi Qonuni 15.04.2022-yildagi O'RQ-764-son "Kiberxavfsizlik to'g'risida"gi qonunida kibermakonda shaxs, jamiyat va davlat manfaatlarini ta'minlash, kiberjinoyatni sodir etgan shaxslarga nisbatan qo'llaniladigan jazolar haqida gap boradi.

O'zbekistonda 2023-yilda sodir etilgan kiberjinoyatning 70 foizi bank kartalari bilan bog'liq firibgarlik va o'g'rilik jinoyatlaridir. Tahlillarga ko`ra, dunyo bo`ylab har yili 500 milliondan ortiq kiber hujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kiber makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo`shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Lyuksemburg kabi rivojlangan

davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda.

O’zbekistonda ham so’nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko`payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga etgan. Xususan, noqonuniy bank-moliya operasiyalari orqali o’zgalarning plastik kartadagi mablag‘larini o’zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o’yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko’payib bormoqda. Achinarlisi, axborot texnologiyalari yordamida huquqbuzarlik va jinoyatga qo’l urgan shaxslar orasida yoshlar ko’pchilikni tashkil etmoqda. Respublikamizda virtual olamdagi qonunbuzilishlarning aksariyati 16-23 yosh oralig‘idagi o’smir-yoshlar tomonidan sodir qilinmoqda. Bundan ko’rinib turibdiki, kiberxavfsizlikni ta’minlash masalasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda.

Hozirda juda mashhur bo’lgan bank hisob raqamingizdan, virtual kartalaringizdan sizni har xil aldov yo’li bilan onlayn muloqot tarzida pul undurishi yoki sizni chuv tushurishi mumkin. Bu jarayonlar ustidan ko’plab arizalar tegishli tartibda Ichki ishlar organlariga kelib tushgan. Bu jarayon juda oson tarzda amalga oshiriladi va siz kiberjinoyat qurboni bo’lasiz. O’zingizni har qanday holatda telefon raqamingiz yoki akkauntingizga begona shaxslar, kompaniyalar tomonidan kelgan kodlarni aytmang. Hushyor bo’ling zamon shiddat bilan rivojlangani bois internetga kirishlar ortmoqda. Axborot texnologiyalari aholiga, jamiyatga, davlatga foyda keltiradi va qulaylik yaratadigan dasturlar, platformalar, ilovalar bor. Lekin bular xavfsizlik tomondan ham, har tomonlama sinab keyin ommaga joriy qilgani maqul.

Kiberjinoyatlarning umumiy profilaktikasining ob’ekti keng jamoatchilikdir va bunda alohida shaxslar tanlab olinmaydi. Masalan, mahalla aholisi, mehnat jamoalari (korxona, muassasa, tashkilotlar xodimlari), voyaga etmaganlar jamoasi (maktab, kollej va akademik liseylar), yoshlar jamoasi va boshqalar. Bunda huquqbuzarliklar profilaktikasi barchaga bir xil ravishda yetkazib beriladi va ta’sir doirasi kengroqligi bilan ajralib turadi. Huquqbuzarliklarning umumiy profilaktik faoliyati jamiyatga zid g‘ayriijtimoiy hodisa va jarayonlarning, turli voqea, hodisa va holatlarni aniqlash va ularni bartaraf etish, ta’sir etish, kuchsizlantirish va oldini olishga qaratilgan keng qamrovli ijtimoiy-huquqiy vositalar orqali amalga oshiriladigan faoliyatdir. Aholi orasida huquqiy targ‘ibot ishlarini olib borish huquqbuzarliklarning oldini olishda muhim ahamiyat kasb etadi. Bunda vakolatli organlar tomonidan mehnat, voyaga yetmaganlar kabi jamoalar o‘rtasida Internet tarmoqlaridan

foydalanib sodir etiladigan huquqbuzarliklarning oldini olish borasida tushuntirishlar, xususan, ma'ruzalar o‘qish, davra suhbatlari uyushtirish, targ‘ibot bukletlari tayyorlash tarqatish katta samara beradi. Ushbu targ‘ibot tadbirlarida fuqarolarda Internet tarmoqlari orqali sodir etildigan huquqbuzarliklarning salbiy oqibatlari, kelib chiqish sabablari va bu borada shaxslarning xushyorligini oshirish borasida turli vazifalar amalga oshirilishi muhim ahamiyat kasb etadi.

O’zbekistonda kiberjinoyatchilikning oldini olish tizimi yaratiladi. Bu haqda Shavkat Mirziyoyevning “Yangi O’zbekistonning 2022-2026-yillarga mo’ljallangan taraqqiyot strategiyasi to’g‘risida”gi farmoni loyihasida belgilab qo’yilgan. Qayd etilishicha, 2023-2026-yillar uchun O’zbekistonning kiberxavfsizlik strategiyasi ishlab chiqiladi. Bunda “uz” domen zonasi internet-makonining kiberxavfsizligini ta’minlashning asosiy yo’nalishlari belgilanadi. Elektron hukumat, energetika, raqamli iqtisodiyot tizimlari va muhim axborot infratuzilmasiga taalluqli boshqa yo’nalishlarni himoya qilish bo’yicha kompleks vazifalar tuzib chiqiladi. Shuningdek, kiberjinoyatchilik uchun jinoiy javobgarlikni qayta ko’rib chiqish rejalashtirilgan. Axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimi takomillashtiriladi. Bu orqali kiberxavfsizlik yagona tarmog‘ining texnik infratuzilmasi kengaytiriladi. “Kibernetikada innovatsiyalar IT-parki” faoliyatini yanada jadallashtirish rejalashtirilgan.

IT-parkning hududlardagi raqamli texnologiyalar o’quv markazlari negizida yoshlarni kiberxavfsizlik asoslari bo’yicha o’qitilishini ta’minlash hamda har yili talaba va o’quvchilar orasida kiberhujumlar aniqlash bo’yicha respublika miqyosida konkurslar o’tkazish nazarda tutilgan. Kiberxavfsizlik kelajagi.Kiberxavfsizlik bo’yicha karyerangizni va kelajagingizni rivojlantirishni istaysizmi, lekin uning hayotimizdagi ko’lami va kelajakdagi ahamiyati haqida tasavvurga ega emasmisiz? Unda ushbu maqola aynan siz uchun. Kiberxavfsizlikni bugun va kelajak kasblaridan bo’ladi deb aytishimiz mumkin. Business Insider India ma’lumotlariga ko’ra, birgina Hindistonda 2025-yilga kelib kiberxavfsizlik bo’yicha 3,5 million bo’sh ish o’rinlari bo’ladi. Ko’pchilik kiberxavfsizlikning kelajagi bilan qiziqadi. Kiberxavfsizlik hali ham IT ning nisbatan yoshroq sohasi bo’lib, so’nggi yillarda IT xavfsizligi bo’yicha alohida kasb sifatida sezilarli darajada rivojlandi. Ushbu maqolada biz axborot xavfsizligi, xususan, kiberxavfsizlik sohasidagi joriy o’zgarishlarni ko’rib chiqamiz va kiberxavfsizlikning kelajagi qanday ekanligini taxmin qilishga harakat qilamiz.

Kiberxavfsizlik innovatsiyalari ushbu sohada muhim yutuqlarni keltirib chiqardi. Biz raqamli imkoniyatlarga ega kelajak sari intilayotganimiz sababli, kiberxavfsizlik bo’yicha mutaxassislar

tasavvurga ega bo'lishlari va yangi g'oyalarni hayotga tatbiq etishlari muhim. Kiberxavfsizlik kelajagidagi ish o'rinlari va imkoniyatlar Kelajakda kiberxavfsizlik bo'yicha ish imkoniyatlari juda ajoyibdir. Bu haqida o'ylab ko'rsangiz, kiberxavfsizlik bo'yicha bandlikning o'rtachadan yuqori o'sishi juda mantiqiy bo'ladi. Texnologiya har bir insonning kundalik hayotiga tobora ko'proq kirib borar ekan, kiberxavfsizlik bo'yicha professional mutaxassislarga talab ortib boradi. Kiberxavfsizlik maoshlari ham yuqori va kundan-kunga ortib bormoqda. Kelajakda kiberxavfsizlik bo'yicha ish bilan ta'minlash bo'yicha hisob-kitoblar ko'proq imkoniyatlarni ko'rsatsa-da, haqiqat shuki, hozir bu sohada ishlash uchun yetarli malakali mutaxassislar yo'q. Malakali kadrlar tanqisligi tufayli kiberxavfsizlik bo'yicha kasbni tanlaganlar ko'plab imkoniyatlar, yaxshi daromad va ajoyib imtiyozlarni kutishlari mumkin, chunki kiberxavfsizlikning kelajagi porloq.

INFORMATION SECURITY RISK ASSESSMENT OF E-RESOURCES UNDER PHYSICAL THREATS

KOMIL FIKRATOVICH KERIMOV
D.Sc., associate professor, head of the Department of System and Application Programming
ZARINA ILDAROVNA AZIZOVA
PhD-student of the Department of Information Security, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, 108 Amir Temur Avenue, Yunusabad paradise, 100084, Tashkent.

Abstract: *The article presents a methodology for assessing the information security risk of electronic resources from physical threats, which is based on the principles of recognizing the signs of information characteristics of protection and vulnerability of assets. The distinctive feature of the proposed methodology is the application of automatic identification of physical threats based on the attributes of protection and vulnerabilities on the basis of the proposed mechanism of formation of the attributes of protection against physical threats.*

Key words: *computer network, vulnerability, risk, information security, artifacts, testing.*

Anotatsiya: *Maqolada fizik tahdidlardan elektron resurslarning axborot xavfsizligi risklarni baholash metodologiyasi keltirilgan bo'lib, u axborot xavfsizligi xususiyatlarining belgilarini va aktivlarning zaifligini tan olish tamoyillariga asoslangan. Taklif etilayotgan metodologiyaning o'ziga xos xususiyati fizik tahdidlardan xavfsizlik belgilarini yaratish uchun tavsiya etilgan mexanizm asosida*

xavfsizlik va zaiflik belgilariga asoslangan fizik tahdidlarni avtomatik aniqlashdan foydalanishdir.

Kalit so'zlar: *kompyuter tarmog'i, zaiflik, risk, axborot xavfsizligi, artefaktlar, testlash.*

Аннотация: *В статье представлена методика оценки риска информационной безопасности электронных ресурсов от физических угроз, которая основана на принципах распознавания признаков информационных характеристик защиты и уязвимости активов. Отличительной особенностью предлагаемой методики является применение автоматической идентификации физических угроз на основе признаков защищенности и уязвимости на основе предложенного механизма формирования признаков защищенности от физических угроз.*

Ключевые слова: *компьютерная сеть, уязвимость, риск, информационная безопасность, артефакты, тестирование.*

Introduction

The information security risk assessment process is aimed at identifying and assessing the level of criticality of possible threats and vulnerabilities that directly impact organizational assets. This process facilitates the most cost-effective and impactful selection of countermeasures to protect information and physical assets.

Protection of electronic resources information from physical threats, such as physical unauthorized access [1] to organizational premises, offices and server rooms, equipment, paper documents, storage devices, storage media, theft or damage to computer equipment and storage media, paper documents, is no less relevant than protection from information attacks.

The analysis of scientific works of researchers dealing with this problem has shown that a significant part of the applied methods of risk assessment from threats of unauthorized access to the organization's assets are aimed at qualitative assessment of the threat under study. The risk arises when there is insufficient information about the consequences when making a decision, or in its absence in general [2].

There are many risk assessment techniques, such as CRAMM, CORAS, MSAT, OCTAVE and others. Despite the many positive aspects (risk categorization, consideration of risk characterization indicators at both technical and organizational levels, etc.) of these methodologies, the key disadvantage is the lack of risk mitigation countermeasures provided as a result of risk assessment (except for the MSAT methodology), as well as the lack of a category of physical security threat types.

Let's take a closer look at the specific risk assessment methodologies. CRAMM risk assessment methodology is a tool with the

help of which it is possible to justify the necessity of proposed costs for certain countermeasures to protect the information system of the organizational structure. In the case of assessing the information security risks of the physical assets of the organization, the application of this methodology becomes inappropriate. The application of this methodology is focused on three main stages: identification and assessment of assets, identification of threats and vulnerabilities for risk calculation, and selection of optimal countermeasures. The process of asset identification and assessment is of key importance, as the acceptable level of security is determined depending on the value of an asset in the organization and the choice of countermeasures directly depends on the level of criticality of risk for important assets.

The most difficult part of the process of assessing information assets is interviewing the subjects-owners of the assets to determine the level of importance of the asset, which may require additional clarifying information, considered as informing. After that, the possible situations of risk occurrence are analyzed, often fatal situations are considered as critical, the occurrence of which is minimized. This leads to the loss of objectivity of consideration of the most frequently occurring situations of information security risk and is a negative indicator of the universality of this methodology. In addition, it becomes impossible to consider system and technical vulnerabilities when assessing security threats, which also affects the universality of this methodology and becomes a disadvantage, as well as the need to recruit qualified specialists to apply the methodology.

The *OCTAVE risk assessment methodology* is a tool for security planning and strategic risk-based information security risk assessment [3]. With its help, organizational structures can determine the current state of asset security, as well as develop a security strategy based on the knowledge of the organization's employees and all business processes, taking into account the identified risks for important assets. A significant advantage of this methodology is its focus on organizational risks and, as a result, the strategic planning of countermeasures for the assets of each individual organization. The disadvantage of this methodology is that it does not focus on the application of individual security technologies, but rather takes into account general security practices.

Our proposed risk assessment methodology presents an approach to assessing information security risks of electronic resources that involves several steps and uses various artifacts and attributes of protection and vulnerability. It includes several steps and requires the application of information about various artifacts, security and vulnerability attributes

and a database for expert risk assessment. The presented methodology for assessing information security risks of electronic resources has its own peculiarities and can also be useful for a specific organizational structure or project.

Proposed methodology for information security risk assessment

In the context of the proposed methodology for assessing the information security risks of electronic resources it is necessary to:

- form the space of protection and vulnerability attributes of the project;
- build a table of project artifacts, protection and vulnerability attributes;
- develop a database;
- build a scheme of automatic detection of physical threats based on protection and vulnerability attributes;
- prepare data for expert assessment of information security risks of electronic resources.

The analysis of the subject area will allow to define the attributes of objects (Fig. 1), which will be further represented in the form of artifacts. The main purpose of attributes is observation, recording, notification and transfer of information in case of various incidents [9-11] related to information security of the organization.

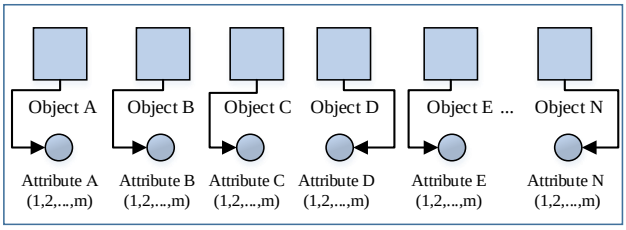


Fig. 1: Simplified diagram of the organization's computer network

The interaction scheme is represented by the following objects and attributes: objects (A, B, C, D, N) and attributes: A (1, 2, 3, 4..., m).

Attributes can be considered as artifacts of the e-resource risk management process, as in the example below, and express the technical and functional state of the object elements.

Formation of the space of signs of protection from physical threats. The feature space is formed from the following information about the technical and functional state of the protection elements of the project objects:

- the elements of protection are technically serviceable, i.e. the elements of protection receive and transmit information;

- the elements of protection are technically defective or do not fulfill their functions of information transmission;
- the state of protection elements to fulfill their functions is transmitted through communication channels to the video surveillance operator;
- the elements of protection are controlled via communication channels by the video surveillance operator.

The first state of the protection element is defined as a defense attribute and the second state is defined as a vulnerability attribute.

Formation of project artifacts to the signs of protection and vulnerability. Project artifacts with corresponding protection and vulnerability attributes are presented in Table 1. Construction of the table is necessary to solve the problem of artifact identification by the code value of the protection or vulnerability attribute.

Database for information security risk assessment. The database includes the following data sets:

1 artifacts of security feature codes;
2 artifacts of vulnerability codes;
3 electronic images of faces of employees of the organization;
4 electronic images of faces of third-party visitors of the organization;
5 codes of electronic passes of the organization's employees with personal data;
6 temporary array of indications about the operating state of the protection elements;
7 temporary array of artifacts with corresponding codes of protection and vulnerability signs.

Formation of physical threat risk assessment stages. Physical threat risk assessment is carried out as follows:

1) Take readings on the operating state of the protection elements (array 5);
2) Arrays 2, 3 and 5 are used to form an array of artifacts with corresponding codes of protection and vulnerability features (array 6);
3) Using arrays 3, 4, 5 and 6, the presence of a threat to the project objects is determined;
4) Perform an information security risk assessment;
5) The decision on information security risk mitigation should be made.

Conclusion

As a result of the conducted research, a methodology for assessing the risk of information security from physical threats to objects was

developed. The developed methodology was based on recognizing the signs of protection and vulnerability of information characteristics of electronic resources. The principles underlying the methodology, namely, the development of a feature space, the construction of elements of protection and vulnerability of a system of tables linking elements of protection and vulnerability with physical threats, make it possible to develop methods for assessing risks and managing information security risks, for example, in the event of threats of unauthorized access to an organization's information.

METHODOLOGY OF INFORMATION SECURITY RISK ASSESSMENT OF ELECTRONIC RESOURCES DERIVED FROM ATTRIBUTES OF PROTECTION OBJECTS UNDER PHYSICAL THREATS

KOMIL FIKRATOVICH KERIMOV
D.Sc., associate professor, head of the Department of System and Application Programming
ZARINA ILDAROVNA AZIZOVA
PhD-student of the Department of Information Security, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, 108 Amir Temur Avenue, Yunusabad paradise, 100084, Tashkent.

Abstract: *The proposed methodology is based on the identification of physical threats based on key protection attributes and vulnerability attributes by forming the space of physical threat protection attributes. The methodology includes five main stages, including the definition and formation in a single database of initial data of protection artifacts and vulnerabilities, identification of threats by the formed signs and subsequent expert assessment of information security risks. Data for expert assessment of information security risks of electronic resources are also developed.*

Key words: *computer network, vulnerability, risk, information security, artifacts, testing.*

Annotatsiya: *Taklif etilayotgan metodologiya asosiy himoya atributlari va zaiflik atributlari bo'yicha jismoniy tahdidlarni fizik tahdidlarga qarshi himoya atributlari makonini shakllantirish orqali aniqlashga asoslangan. Metodologiya beshta asosiy bosqichni o'z ichiga oladi, jumladan, dastlabki ma'lumotlarning yagona ma'lumotlar bazasida xavfsizlik artefaktlari va zaifliklarini aniqlash va shakllantirish, yaratilgan belgilar asosida tahdidlarni aniqlash va axborot xavfsizligi xavflarini keyingi ekspert baholash. Elektron resurslarning axborot xavfsizligi risklarini ekspert baholash uchun ma'lumotlar ham ishlab chiqilgan.*

Kalit so'zlar: *kompyuter tarmog'i, zaiflik, risk, axborot xavfsizligi, artefaktlar, testlash.*

Аннотация: *Предлагаемая методология основана на идентификации физических угроз по ключевым атрибутам защиты и атрибутам уязвимости путем формирования пространства атрибутов защиты от физических угроз. Методика включает пять основных этапов, в том числе определение и формирование в единой базе данных исходных данных артефактов защиты и уязвимостей, идентификацию угроз по сформированным признакам и последующую экспертную оценку рисков информационной безопасности. Также разработаны данные для экспертной оценки рисков информационной безопасности электронных ресурсов.*

Ключевые слова: *компьютерная сеть, уязвимость, риск, информационная безопасность, артефакты, тестирование.*

A review of research in the field of Information Security Risk Assessment

The issues of information security risk assessment are devoted to the studies of many scientists around the world. Among such works, attention should be paid to the work [1] in which the authors consider the life cycle of the risk assessment procedure in 7 stages, such as the characterization of physical features of the object, identification of undesirable events, determination of the consequences of incidents, etc., while not taking into account the relationship between negative events and objects, as well as possible changing indicators used as parameters to determine the causal relationship in the assessment of information security risks.

Information security risk in the general sense is a certain probability of occurrence of an adverse event leading to some damage or loss in relation to the assets of the organization [2]. Information security risk of electronic resources on the Internet remains high if they are not adequately protected from unauthorized access.

In turn, the authors [3] proposed a combined approach to risk assessment taking into account behavioral characteristics, parameters of negative impact of events on the infrastructure and consequences of possible risks. This approach showed positive results, but it was used by the authors only for risk assessment in cloud computing systems, and did not provide separate scenarios of the outcome of events in their categorization.

The paper [4] presents a three-level architecture of cyber-physical systems and the results of risk assessment at each level of the proposed architecture. The peculiarity of the method proposed by the authors is the application of the failure tree method together with the graphical method of modeling the cyber-physical system, including such stages as asset identification, threat and vulnerability identification, simulation and

scenario modeling. The use of the Failure Tree Method did not allow the authors to determine a specific amount of risk, despite the convenience of using modeling to reduce costs.

For information security of electronic resources of the organization, it is necessary to carry out a number of design works [5], including:

– selection of a building with the necessary number of rooms for staff work, on the placement of physical protection means;

– determination of physical means of information protection from physical threats;

– optimal placement of physical protection means [6];

– development of a system of surveillance and notification of various events and incidents related to physical threats.

In the process of information security risk assessment can be used indicators of each series of project work, depending on the degree of criticality of the occurred information security incident and the importance of the asset, both physical and information. For this purpose, it is important to take into account the indicators of security attributes, as well as indicators of asset vulnerability for the organizational structure, which often becomes difficult because the risk assessment is performed after the occurrence of an information security incident.

In this paper, we propose a methodology for assessing the security risks of electronic resources, taking into account possible physical threats. The developed methodology allows us to determine the degree of influence of possible information security risk on organizational assets by forming a space of attributes and attributes necessary for further automation of the process of information security incident detection and transfer of information related to the information security of the organization.

Information Security Risk Assessment from Unauthorized Access

For the threat under consideration, we obtain the following artifacts of the risk management process:

1. Suppose that, as a result of scanning the protection elements, an array of 5 is obtained, presented in the column "State of the protection element" of Table 1.

2. Array 5 results in array 6, represented by the column "Artifacts with protection and vulnerability feature codes" in Table 1.

3. Identification of threats to the project objects.

In order to conduct an information security risk assessment from unauthorized access, it is necessary to conduct an analysis of possible

threats to objects. The following variables can be used for risk assessment [7]:

- Ut (t=1,...,n) - the maximum level of threat to the object. Ut is determined by the number of rows of the table of results of the analysis of possible threats.
- Pg = (1,2,...,m) - the value of the threat sign for the object. Pg takes the value 1, if the sign of threat takes place, otherwise 0.
- Lj (j=1) - the maximum threat level for the project, by the total number of possible threats to the project. L1= 5 by the number of objects.
- M - the maximum level of information security risk. The value of M is determined by the sum of the maximum threat levels of projects, (in this paper one project is studied, therefore, M =L1).

Figure 1 shows the scheme of physical protection of the organization's electronic resources.

The scheme shows the following objects and attributes:

1. Objects: O1 - organization building; O2 - organization manager's office; O3 - organization computer room; O4 - equipment room (for storage devices, storage media); O5 - server room; O6 - video surveillance operator's room.

2. Attributes: A1 - video surveillance cameras; A2 - entrance and exit doors; A3 - duty officer's watch; A4 - windows of premises; A5 - safes; A6 - switching communication channels.

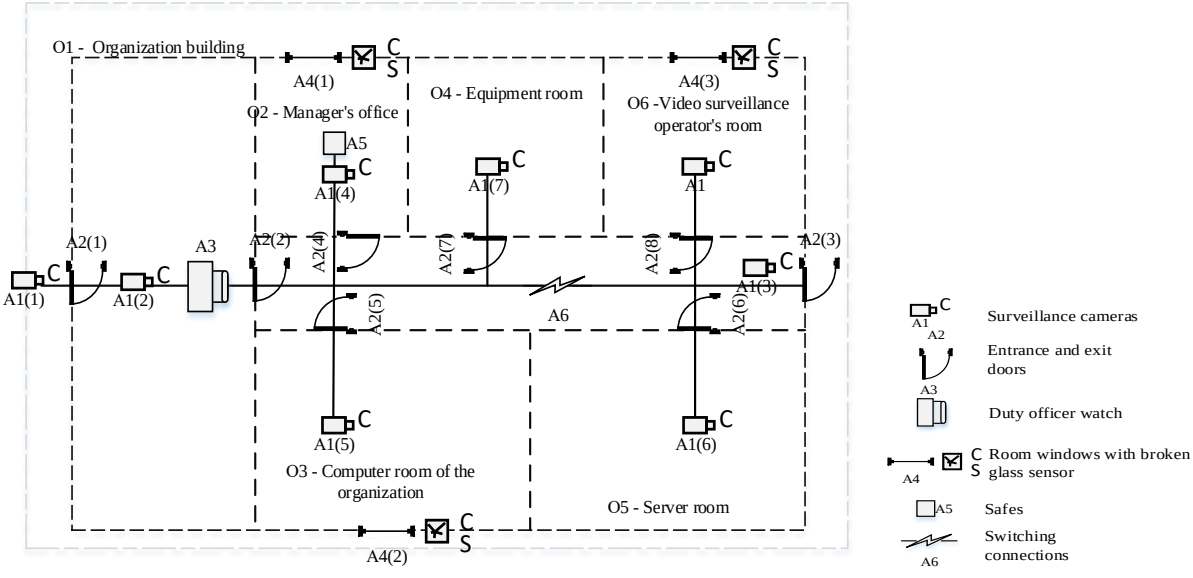


Fig. 1: Simplified scheme of the project to protect electronic resources from physical threats

These object attributes are created in the process of analyzing the subject area to solve the problems of information protection of electronic resources.

Table 1: Project artifacts with corresponding attributes and states of protection elements

Project artifact designation	*Project artifacts*	*Protection feature code*	*Vulnerability code*	*Protection element state*	*Artifacts with protection and vulnerability feature codes*
A1(1)	Surveillance camera in front of the entrance to the organization's building	x1	y1	operates (transmits information)	x1
A2(1)	Entrance doors to the organization's building	x2	y2	functional (protected by a code lock)	x2
A1(2)	Surveillance camera at the duty officer's watch	x3	y3	operates (transmits information)	x3
A2(2)	Doors to the common hallway	x4	y4	functional (protected by a code lock)	x4
A1(3)	Surveillance camera of the emergency exit from the organization's building	x5	y5	disabled	y5
A2(3)	Emergency exit doors from the organization's building	x6	y6	functional (protected by a code lock)	x6

Project artifact designation	*Project artifacts*	*Protection feature code*	*Vulnerability code*	*Protection element state*	*Artifacts with protection and vulnerability feature codes*
A2(4)	Entrance doors to the manager's office	x7	y7	functional (protected by a code lock)	x7
A1(4)	Surveillance camera in the manager's office	x8	y8	functional (protected by a code lock)	x8
(A5)	The safe in the manager's office	x9	y9	functional (protected by a code lock)	x9
A4(1)	Window in the manager's office	x10	y10	notification sensors in working condition	x10
A2(5)	Entrance doors to the organization's computer room	x11	y11	functional (protected by a code lock)	x11
A1(5)	Surveillance camera in the organization's computer room	x12	y12	functions (transmits information)	x12
A4(2)	Window in the organization's computer room	x13	y13	notification sensors in working condition	x13
A2(6)	Server room entrance doors	x14	y14	functional (protected by a code lock)	x14

Project artifact designation	*Project artifacts*	*Protection feature code*	*Vulnerability code*	*Protection element state*	*Artifacts with protection and vulnerability feature codes*
A1(6)	Surveillance camera in the server room	x15	y15	operates (transmits information)	x15
A2(7)	Equipment room entrance doors	x16	y16	functional (protected by a code lock)	x16
A1(7)	Surveillance camera in the equipment room	x17	y17	disabled	y17
A2(8)	Entrance doors to the video surveillance operator's room	x18	y18	functional (protected by a code lock)	x18
A4(3)	Window in the video surveillance operator's room	x19	y19	notification sensors in working condition	x19
(A6)	System of operator communication channels with video surveillance cameras	x20	y20	communication system is functioning	x20

According to the scanning results, we can see that the indications of the working state of the threat protection elements for the objects of the manager's office, computer room, server room and video surveillance operator's room are the same. Therefore, the results of the analysis of possible access threats for the listed rooms of the organization can be summarized in a single table 2.

Table 2: Results of analysis of possible access threats

№	*Video camera reading matches the data in the database*	*The code of the electronic ID card matches the code in the database*	*Facility threat sign*	*Note*
1	yes	no	yes	Unauthorized entry on one's own pass into a categorized room
2	yes	no	no	No access to the premises
3	yes	yes	yes	Threat of entry using another person's ID card
4	no	yes	yes	Threat of entry using another person's ID card
5	no	yes	yes	Threat of entry using another person's ID card
6	no	no	no	No access to the premises

The table of results of the analysis of possible threats to access to the premises for storage devices, storage media will differ from Table 2 in that the first column "Video camera readings match database data" will not be filled with readings matching the video camera data with the database data of electronic resources.

Next, we introduce the concept of object threat characteristic Dt (t=1,...,5) and use the expression:

$$Dt = \begin{cases} 0, & \sum_1^6 Pg \\ \frac{\sum_1^6 Pg}{Ut}, & 0 < \sum_1^6 Pg \le Ut \end{cases}, \text{ where,}$$

$Ut = 6$, ($t = 1, \dots, 6$), according to the table of results of the analysis of threats to objects; $D1 = 2/3$, $\sum Pg = 4$, for the manager's office; $D2 = 2/3$, $\sum Pg = 4$, for the computer room; $D3 = 2/3$, $\sum Pg = 4$, room for storage devices, data carriers; $D4 = 2/3$, $\sum Pg = 4$, for the server room; $D5 = 2/3$, $\sum Pg = 4$, for the server room.

The threat characteristic Xj to the project with index j is determined from the following expression:

$$Xj = \begin{cases} \sum_1^5 Dq, & 0 < \sum_1^5 Dq < Lj \\ 0, & \sum_1^5 Dq = 0 \end{cases}.$$

Threats to information security are determined only for one project, so the index of the threat to the project has the value $j = 1$. According to

the calculated data of threat characteristics Dt ($t = 1, \dots, 5$ and the condition $\sum Dq = \frac{10}{3} < Lj = 5$, $X1 = \sum Dq = \frac{10}{3}$ determined.

We define the characteristics of information security risks from the following expression: $V = \begin{cases} \sum_1^m Xk, & 0 < \sum_1^m Xk < M \\ 0, & \sum_1^m Xk = 0 \end{cases}$, since $V = L1 = 5$, then according to the formula for the risk characterization of the project V and condition $0 < \sum Xk = 10/3 < M = 5$, it follows $V = \sum Xk = 10/3$. In percent the risk of the project will be equal to $R = (V/M) \times 100 =$ 66,7%. Naturally, at such a significant level of risk it is necessary to take measures to reduce it.

Information security risk mitigation solutions

Reduction of information risks associated with physical access, as a rule, carried out by introducing physical risk control in the activities of the organizational structure as an addition to the risk management of the organization as a whole. Thus, in organizational structures, separate security profiles formed for employees in the work environment [8], and security roles in working with information systems should be provided. It should also take into account the need to implement information technologies for physical security, which will allow:

– implement data collection from various disparate devices and systems available in the organizational structure;

– simplify the process of analyzing and comparing data, event results and notifications when identifying real-time situations;

– minimize the response time of the operator to an identified emergency situation;

– define standard operating procedures and instructions based on the information security policy of the organizational structure;

– track necessary information and steps for compliance reporting, training, and follow-up investigation when an out-of-scope situation occurs;

– monitor operator interaction with the system, by tracking manual changes to security inputs;

– calculate the required response time to information security events.

Our proposed methodology for assessing the information security risks of electronic resources was applied under possible scenarios of physical security breaches of organizational assets. The stages of risk assessment were reduced to a minimum, and all necessary parameters and characteristics of the investigated objects were taken into account,

which allowed reducing the time for the implementation of the risk assessment process without affecting the quality of the assessment.

Conclusion

The article proposes a methodology for assessing information security risks from physical threats to objects. The developed methodology was based on recognizing the signs of protection and vulnerability of information characteristics of infrastructure objects and electronic resources. The principles underlying the methodology, namely, the development of the feature space, the construction of protection elements and vulnerabilities of the system (presented in the form of a table linking protection elements and vulnerabilities to physical threats), make it possible to develop new methods of risk assessment and information security risk management, for example, at threats of unauthorized access to information of organizational structures. This methodology can be applied in modeling different scenarios of security breaches in organizations, depending on the target assets and objects of assessment for optimal asset protection.

DETECTING AND COMBATING CORRUPTION AT THE STATE LEVEL USING DIGITAL TECHNOLOGIES

Khasanov Mukhriddin Oroqboy ugli
Doctoral student of Law Enforcement Academy

Abstract: *This article examines some foreign experience, defining that combating corruption and forming conceptual approaches through information technologies helps to identify and combat corruption in our country.*

Keywords: *Corruption, anti-corruption, media, technology, convention, level of corruption.*

Multilateral documents on preventing and combating corruption in the world, and in particular, ***the Inter-American Convention*** against Corruption , adopted ***by the Organization of American States on March 29, 1996 , adopted by the Council of the European Union on May 26, 1997,*** to officials of the European Community or ***Convention*** on Combating Corruption of Officials of the Member States of the European Union, ***Convention*** on Combating Bribery of Foreign Officials in International Commercial Practices adopted ***by the Organization for Economic Co-operation and Development on November 21, 1997***, adopted by the Committee of Ministers of the Council of Europe on

January 27, 1999 the Convention on Criminal Liability for Corruption, ***the Convention*** on Civil Liability for Corruption, adopted ***by the Committee of Ministers of the Council of Europe on November 4, 1999,*** and the Prevention of Corruption, adopted ***by the Heads of State and Government of the African Union on July 12, 2003*** Having regard to ***the African Union Convention*** on Combating

The Convention against Corruption was approved on October 31 of this year [1], approving the fact that the United Nations Convention against Transnational Organized Crime entered into force on September 29, 2003

Despite this, the fact that the scale of corruption-related crimes is increasing year by year indicates that it is **extremely important to improve the organizational and legal foundations of departmental systems in this area.** As recognized in the Occupational Fraud 2024 study of the Association of Certified Fraud Examiners (ACFE) , only[2]in 2022-2023, **138 of the world's 3.1 trillion from the state budget as a result of 1921 major** corruption crimes . more than **100,000 dollars** have been appropriated. The Republic of Uzbekistan also joined the United Nations Convention Against Corruption (New York, October 31, 2003) on July 7, 2008, approved by the Law No.-158.

On January 3, 2017, the adoption of the Law **of the Republic of Uzbekistan "On Combating Corruption"** defined the main directions of the state policy on combating corruption, the bodies authorized to combat corruption, their duties, the participation of citizens, mass media, and non-governmental non-profit organizations in this activity [3].

the Action Strategy [4]for the five priority directions of the development of the Republic of Uzbekistan in 2017-2021 It was a historical document aimed at rooting out corruption.

It defined specific measures aimed at eliminating corruption in all spheres and the causes that create conditions for its rooting.

The President of the Republic of Uzbekistan Sh.M. Mirziyoev in his address to the Oliy Majlis of the Republic of Uzbekistan on January 24, 2020, "The evil of corruption in our society is hindering our development in its various forms. If we do not prevent this evil scourge, it will be impossible to create a real business and investment environment, and in general, not a single sector of society will develop [5]. "

1https://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml

2Occupational Fraud 2024: A Report to the Nations// https://www.acfe.com

[3] https://lex.uz/docs/3088008
[4] https://lex.uz/acts/3107036
[5] https://president.uz/ru

In this regard, it is necessary to improve anti-corruption systems not only at the state level, but also in all agencies. Based on this, it is an urgent issue to take appropriate measures in the labor authorities.

It should be noted that the Ministry of Poverty Alleviation and Employment of the Republic of Uzbekistan is a state administration body that carries out a single policy in the field of population employment, labor migration and labor relations [6]. Labor bodies systematically work to provide employment to different segments of the population, ensure labor rights, and ensure the rights and interests of workers in migration processes.

To date, labor bodies are operating in more than **170 countries of the world.**

The decision of the Republic of Uzbekistan "On Employment of the Population" of October 20, 2020, **"labor bodies"** - the Ministry of Employment and Labor Relations of the Republic of Uzbekistan (currently - the Ministry of Poverty Reduction and Employment), as well as the Ministry of Employment and Labor Relations of the Republic of Karakalpakstan, regions and It has been determined that the main employment offices of Tashkent city, districts (cities) are the centers of public employment assistance [7].

According to the information provided by the Anti-Corruption Agency of the Republic of Uzbekistan in the report No. 03-07/4260 dated September 5, 2023, in 2022, **183 corruption crimes were committed** by [8] 176 **employees of the Ministry of Poverty Alleviation and Employment in the fields of employment and labor relations in the territory of the republic** .

When analyzed by the type of crimes, **79** or **43.1 percent of the crimes are covered by Article 167** of the Criminal Code (Empropriety or embezzlement), **43** or **23.4** percent by Article **209** (Professional fraud), **26** or **14 2** percent under Article **168** (Fraud), **20** or **10.9** percent under Article **211** (Bribery), **9** or **4.9** percent under Article **205** (Abuse of Power or Authority), **5** or **2.7** percent Article **210** (Bribery) and **1** or **0.5** percent were crimes provided for in Article **212** (Intermediary in receiving and giving bribes) [9].

[6] Legislation information national base , 04/30/2021, No. 09/21/258/0400, 06/24/2021, No. 09/21/391/0590, 10/26/2021, No. 09/21/656/0996; 02/22/2022, No. 09/22/80/0154, 03/02/2022, No. 07/22/149/0186, 04/19/2022, No. 09/22/195/0319

[7] https://lex.uz/docs/5055690

[8] Taken from the report No. 03-07/4260 dated September 5, 2023 of the Anti-Corruption Agency of the Republic of Uzbekistan

[9] Information provided by the Ministry of Internal Affairs of the Republic of Uzbekistan / Submission No. 03-07/4260 dated September 5, 2023 of the Anti-Corruption Agency of the Republic of Uzbekistan

56 cases related to corruption committed in the field of employment and labor relations were considered by the courts.

If we analyze the crimes committed by regions, **14 cases (7.8%) were committed** in Namangan region, **13 cases (7.2%)** in Andijan region, **6 cases (3.3%)** in the Republic of Karakalpakstan, **5 cases (2.8 percent)** Kashkadarya region, **4 (2.2 percent)** Tashkent and Fergana regions, **3 (1.6 percent)** Bukhara and Syrdarya regions, **2 (1.1 percent)** Tashkent city and **1 each (0.5 percent)** corresponded to Jizzakh and Samarkand regions [10].

For this reason, the Russian scientist Popov E.V. and Semyachkov K.A. as stated "In order to reduce threats to the economic security while the country is developing, digital technologies are the priority task of the modern state [11]. "

Corruption is a serious obstacle to socio-economic development. This is largely due to the fact that corruption is a sensitive topic, often measured by indirect or direct methods, and often relies on the subjective assessments of experts.

As noted by Spanish researchers López-Iturriaga and Sanz, when analyzing the level of corruption in 52 administrative regions of Spain, despite the integrity of the state, it was determined that economic and political freedom is high.

El Mundo , based on popular material, related to corruption crimes against officials since 2000, and used an artificial neural network ***"SOMs" to analyze such publications*** and distinguish between corrupt administrative areas and non-corrupt administrative areas. -book pointers (per 100,000 inhabitants).[12]

The following factors influence the level of corruption in the analysis: level of taxation, public debt per capita, economic growth, population growth, dynamics of registered companies, rising housing prices, unemployment, party support.

in Indonesia that collects news on corruption offenses and provides a Google API geographic map view of the number and extent of corruption violations. This study used 7 Indonesian news sites (liputan6.com, tribunnews.com, merdeka.com, kompas.com, detik.com and tempo.co), in which 2 thousand (0.2%) of the 900 thousand news are related to corruption.[13]

---

[10] Information provided by the Supreme Court of the Republic of Uzbekistan / Submission No. 03-07/4260 dated September 5, 2023 of the Anti-Corruption Agency of the Republic of Uzbekistan

[11] https://cyberleninka.ru/article/n/institutsionalnaya-model-razvitiya-umnyh-gorodov

[12] https://ideas.repec.org/a/spr/soinre/v140y2018i3d10.1007_s11205-017-1802-2.html

[13] https://www.researchgate.net/scientific-contributions/Noerlina-2125212307

You can see a diagram of corruption factors in Indonesia through the "Indonesia Corruption Map".

Based on the above experience:

– Artificial intelligence to detect corruption is not objective, but subjective information news sites. In these cases, confirmed facts and sentences are reported that may be more relevant, but in general, the resulting map shows the manifestation of corruption to a large extent depending on the political situation in different geographical areas of the studied countries (the combination of political forces and the level of influence of certain parties, the executive authority for anti-corruption activities) , as well as the level of activity of news website journalists and the general level of freedom of expression in the compared regions. In addition, the reflection of what is happening in the news may show reformatting and does not always reflect the function of civilian control. Media coverage is associated with the possibility of deliberate distortion of information on anti-corruption issues.

– The subject of corrupt manifestations in different, stratified mood and feeling cultural environments. For example, one country may have a low prevalence of corruption, but awareness of corruption may increase due to public interest in fighting corruption .

PROSPECTS FOR THE USE OF MODERN DIGITAL TECHNOLOGIES IN THE FRAMEWORK OF ANTI-CORRUPTION MONITORING

Yumatov Bogdan Olegovich
A postgraduate student of Law Enforcement Academy

Abstract*: This article notes that humanity is on the verge of the fourth industrial revolution, which leads to many global changes in almost all spheres of life. Modern digital technologies are entering deeper into the reality around us. The author examines in the article which modern technologies could become effective and useful tools in the framework of anti-corruption monitoring.*

Keywords: *anti-corruption monitoring, modern technologies, digital technologies.*

Аннотация*: В данной статье отмечается, что человечество находится на пороге четвертой промышленной революции, что приводит к множеству глобальных изменений почти во всех сферах жизнедеятельности. Современные цифровые технологии проникают все глубже в окружающую нас действительность. Автор в статье рассматривает, какие современные технологии могли бы стать эффективными и полезными инструментами в рамках антикоррупционного мониторинга.*

Ключевые слова: *антикоррупционный мониторинг, современные технологии, цифровые технологии.*

Annotatsiya*: Ushbu maqolada ta'kidlanishicha, insoniyat to'rtinchi sanoat inqilobi arafasida, bu hayotning deyarli barcha sohalarida ko'plab global o'zgarishlarga olib keladi. Zamonaviy raqamli texnologiyalar atrofimizdagi voqelikka tobora chuqurroq kirib bormoqda. Maqolada muallif korrupsiyaga qarshi monitoring doirasida qanday zamonaviy texnologiyalar samarali va foydali vositalarga aylanishi mumkinligini ko'rib chiqadi.*

Kalit so'zlar: *korrupsiyaga qarshi monitoring, zamonaviy texnologiyalar, raqamli texnologiyalar.*

Today, it is obvious that digitalization continues to become an integral part of many processes in human life. Modern technologies are entering deeper and deeper into the reality around us, changing not only the format of interaction and relationships between people, but also the people themselves. Humanity is not only witnessing, but also participating in the fourth industrial revolution currently taking place, which represents a new approach to production based on the ubiquitous introduction of information technology, artificial intelligence and automation of most production processes.

This concept was formulated by the German economist Klaus Schwab[1]. The author noted: "Of the many diverse and fascinating tasks facing modern society, the most important and impressive is the awareness and formation of a new technological revolution, which provides for at least the transformation of humanity. We are at the origins of a revolution that will fundamentally change our lives, our work and our communication. In terms of scale, the scope and complexity of this phenomenon, which I consider the Fourth Industrial Revolution, has no analogues in all previous human experience.[2]"

This stage of the development of human civilization is characterized by the introduction, use and development of technologies and areas such as:

- Artificial intelligence;
- Machine learning;
- Neural networks;
- Robotics, robotization and automation;
- Cloud computing;
- Big Data;
- Blockchain;
- Additive manufacturing (3D printing);
- Cybersecurity;

[1] https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab/ - Schwab, K. (2016) The Fourth Industrial Revolution. World Economic Forum.

[2] https://hes.mephi.ru/?page_id=21597 - The Fourth Industrial Revolution

- Genetic engineering;
- Augmented and virtual reality, etc.

All this should contribute to accelerated productivity growth, improving the quality of products and services, increasing competition and competitiveness, reducing the number of mistakes made due to human factors and to many other advantages.

Speaking about the gradual spread of modern digital technologies, it is necessary to draw attention to the Government AI Readiness Index[3], or rather to the dynamics of the position of the Republic of Uzbekistan in this Index (see **Table No. 1**).

Year	Overall score	Global position
2019	1,412	158 / 194
2020	37,17	95 / 172
2021	40,13	93 / 160
2022	44,51	79 / 181
2023	43,79	87 / 193

Table No. 1

The position of the Republic of Uzbekistan in the Government AI Readiness Index

Modern technologies have proven themselves to be extremely effective and useful tools in areas related to crime prevention, and the anti-corruption sphere is no exception. The subjects of corruption offenses eventually adapt to all methods of countering corruption, which leads to the formation of more complex corruption connections and schemes that the previous anti-corruption mechanisms cannot effectively resist, which means that the appropriate introduction of modern digital technologies is not just one of the fashionable trends, but the necessity for the reality around us.

Modern digital technologies not only increase the effectiveness of anti-corruption monitoring, but also contribute to ensuring the principles of efficiency, accountability, openness and transparency in the activities of government bodies related to combating corruption[4].

According to the fact that monitoring activities in most cases involve the collection, processing and analysis of a huge amount of data (a complete and comprehensive study of such a large amount of information

[3] https://oxfordinsights.com/ai-readiness/ai-readiness-index/ - Government AI Readiness Index

[4] https://www.undp.org/publications/new-technologies-sustainable-development-perspectives-integrity-trust-and-anti-corruption - New Technologies for Sustainable Development: Perspectives on Integrity, Trust and Anti-Corruption

is hardly possible, relying solely on human resources, in addition, the human factor can cause distortion of collected information) concerning corruption manifestations, it is necessary to agree with the approaches according to the authors[5], digitalization in this context not only facilitates and accelerates the work with information, but it also allows to form the most objective conclusions and statistical data, which are subsequently used in the formation and implementation of anti-corruption policy. It is also necessary to agree with the author's position, according to which increasing the effectiveness of the use of digital technologies in the study of corruption relations can determine the effectiveness of anti-corruption policy[6].

Touching upon the prospects for the use of modern digital technologies in the framework of anti-corruption monitoring, it should be mentioned that **anti-corruption monitoring** is the activity of authorized subjects of anti-corruption policy to collect, summarize, analyze, evaluate and interpret information related to the real state of corruption, the level of its spread in the country, certain forms of its manifestation, the causes of corruption (corruption-related factors and corruption risks), the results of the implementation of anti-corruption policy, anti-corruption strategies, programs and plans, which is implemented on the basis of an established unified methodology[7].

Taking into account the fact that the system-forming objects (directions) for anti-corruption monitoring are corruption, corruption-related factors and corruption risks, as well as the results of the implementation of anti-corruption policy, we believe that modern technologies can be applied both separately and comprehensively in each direction.

The most difficult obstacles to more effective implementation of anti-corruption monitoring are the huge amount of necessary data (which in fact already represents *Big Data*) and limited human resources. *Artificial intelligence* can be used to solve this problem, since this tool will not only speed up the processing of large amounts of information, but also

---

[5] Gans-Morse, Jordan and Borges, Mariana and Makarin, Alexey and Mannah Blankson, Theresa and Nickow, Andre and Zhang, Dong, Reducing Bureaucratic Corruption: Interdisciplinary Perspectives on What Works. World Development, 2018 (vol. 105, p. 171-188); Brown, Nerissa C. and Smith, Jared D. and White, Roger M. and Zutter, Chad J., Political Corruption and Firm Value in the U.S.: Do Rents and Monitoring Matter? (April 27, 2019). Journal of Business Ethics, 2021 (vol. 168, no. 2, p. 335-351)

[6] Сосновская Л.Р., Цифровизация способов проведения антикоррупционного мониторинга // Уголовная политика в условиях цифровой трансформации / Казань: «Отечество», - 2023. - С. 144.

[7] Yumatov B.O., Prerequisites for the implementation of the anti-corruption monitoring system in the anti-corruption policy of the Republic of Uzbekistan, Ҳуқуқни муҳофаза қилиш соҳасида юридик таълим ва фан: замонавий тенденциялар ва истиқболлари" мавзусида халқаро илмий-амалий конференция материаллари тўплами. II-жилд. - Т.: "Lesson press". - 2024. - С. 359.

direct human resources to study the most significant data for anti-corruption monitoring. *AI* is already finding its application in practice, for example, as part of the investigation of the Rolls-Royce case, a team of seven investigators of Serious Fraud Office of the United Kingdom used ACE capabilities to analyze about 30 million documents (600,000 per day), mainly to sort them into "important" and "unimportant"[8], such an approach allowed them to select the most relevant data for the investigation in just a couple of months.

Neural networks are another promising technology. This tool can contribute to the early detection of corruption-related factors and corruption risks, suspicious patterns in the framework of anti-corruption monitoring. A group of Spanish researchers has developed a model based on neural networks, the essence of this model is to calculate the probability of corruption violations in the regions of the country and determine the conditions that contributed to their commission. Also, the results of using this tool can be used by authorities to implement preventive measures and reduce corruption risks in various fields, as well as to make the necessary management decisions[9]. To ensure the development of these tools, *machine learning* will certainly be required.

Blockchain technology in the framework of anti-corruption monitoring can also be extremely useful, since this system is transparent and accountable. The information contained in this system can be verified, which, in turn, makes it difficult for falsification and any unfair modification or deletion of data by unscrupulous persons, since any such actions will lead to a violation of the integrity of the entire volume of information.

Summarizing the above, it should be noted that despite the obvious advantages of using modern digital technologies in the field of anti-corruption in general, as well as in the framework of anti-corruption monitoring in particular, these tools can also be used by unscrupulous persons, which certainly requires appropriate preventive measures, as well as measures to bring violators to punishment. In this context, it will be necessary to develop and subsequently adopt the necessary regulatory legal acts that would regulate various aspects of the use of these technologies.

[8] clck.ru/3DfXUK - UK authorities used artificial intelligence in corruption investigation

[9] Félix J. López-Iturriaga & Iván Pastor Sanz, 2018. "Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces," Social Indicators Research: An International and Interdisciplinary Journal for Quality-of-Life Measurement, Springer, vol. 140 (3), p. 975-998.

CYBERSECURITY THREATS AND SOLUTIONS

Aliyev Avazbek Ulugbek ugli
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Teacher of the Department of Digital Technologies and Information Security

Annotasiya*: Kibertahdidlar rivojlanishda davom etar ekan, ularga qarshi kurashish strategiyalarimiz ham shunday bo'lishi kerak. Texnologiya, xodimlarni o'qitish va proaktiv rejalashtirishni o'z ichiga olgan ko'p qirrali yondashuv nozik ma'lumotlarni himoya qilish va raqamli operatsiyalarga ishonchni saqlash uchun zarurdir.*

Kalit so'zlar: *Zararli dastur, Fishing hujumlari, (DoS) hujumlari, Insider tahdidlar, Ko'p faktorli autentifikatsiya.*

Аннотация: *Поскольку киберугрозы продолжают развиваться, должны развиваться и наши стратегии борьбы с ними. Многогранный подход, включающий технологии, обучение сотрудников и упреждающее планирование, имеет важное значение для защиты конфиденциальных данных и поддержания доверия к цифровым операциям.*

Ключевые слова: *вредоносное ПО, фишинговые атаки, (DoS) атаки, внутренние угрозы, многофакторная аутентификация.*

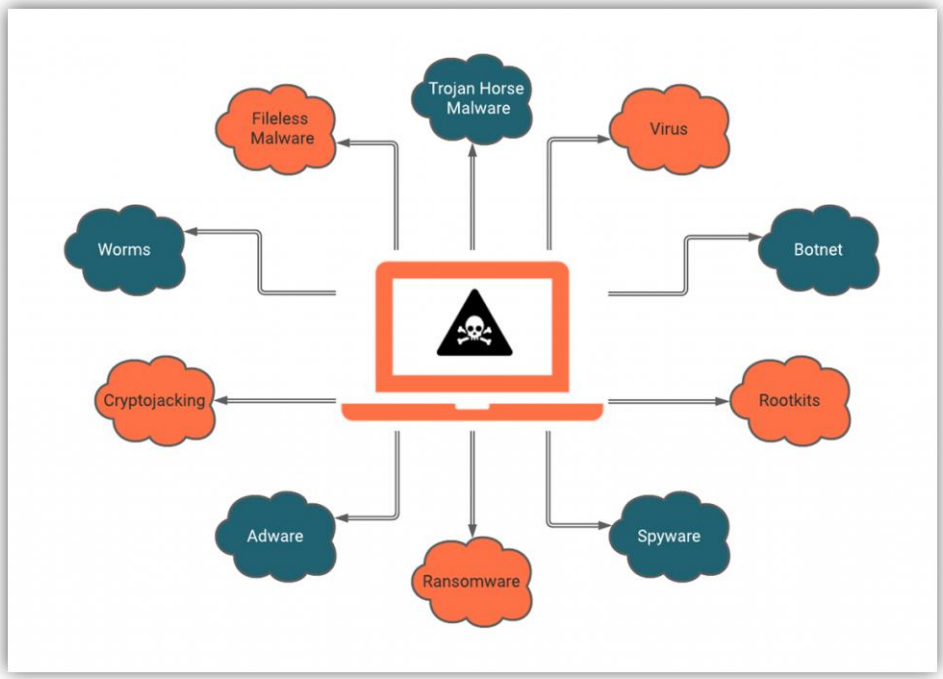
Annotation: *As cyber threats continue to evolve, so too must our strategies for combating them. A multi-faceted approach that includes technology, employee education, and proactive planning is essential for protecting sensitive data and maintaining trust in digital operations.*

Key words: *Malware, Phishing Attacks, (DoS) Attacks, Insider Threats, Multi-Factor Authentication.*

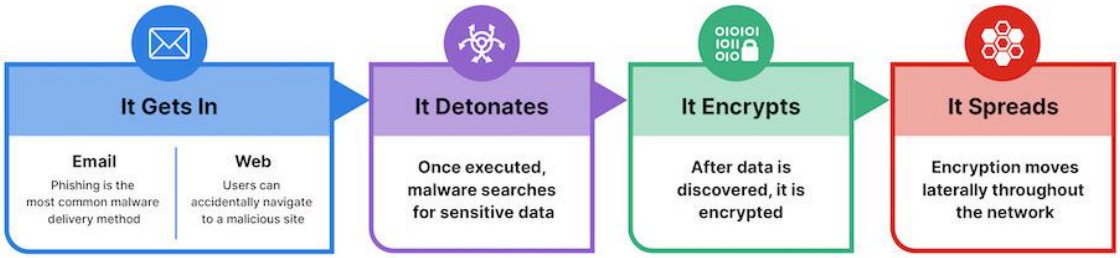
In our increasingly digital world, cybersecurity threats are a constant concern for individuals, businesses, and governments alike. As technology evolves, so do the methods employed by cybercriminals. Understanding these threats and implementing effective solutions is crucial for safeguarding sensitive information and maintaining trust in digital systems. Cybersecurity refers to any technologies, practices and policies for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect computer systems, applications, devices, data, financial assets and people against ransomware and other malware, phishing scams, data theft and other cyberthreats. Although many aspects of computer security involve digital security, such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering. IT security is not a perfect subset of information security, therefore does not completely align into the security convergence schema.

Common Cybersecurity Threats

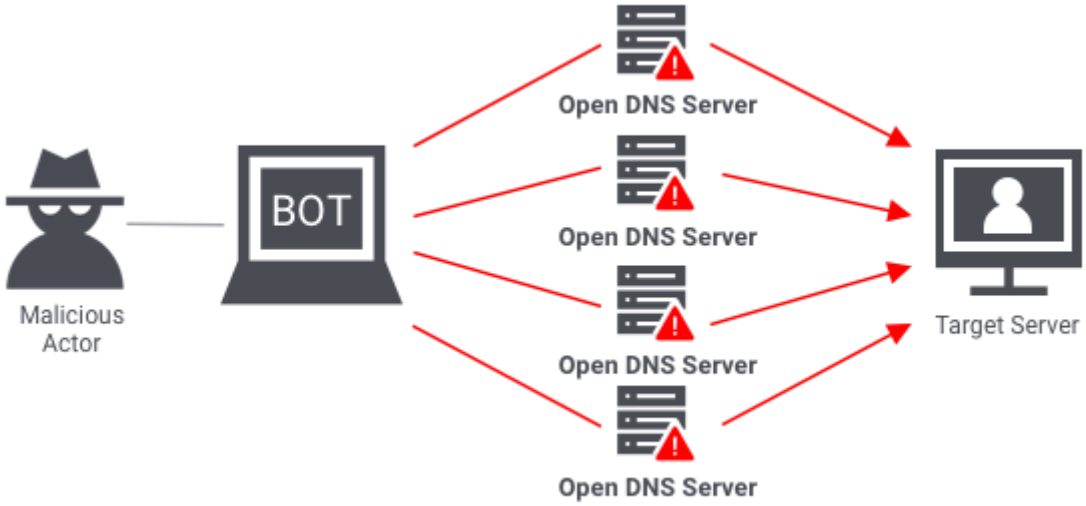
1. **Malware**: Malicious software, including viruses, worms, and ransomware, can infiltrate systems to steal data, disrupt operations, or demand ransom. Ransomware, in particular, has surged in recent years, locking users out of their data until a payment is made.



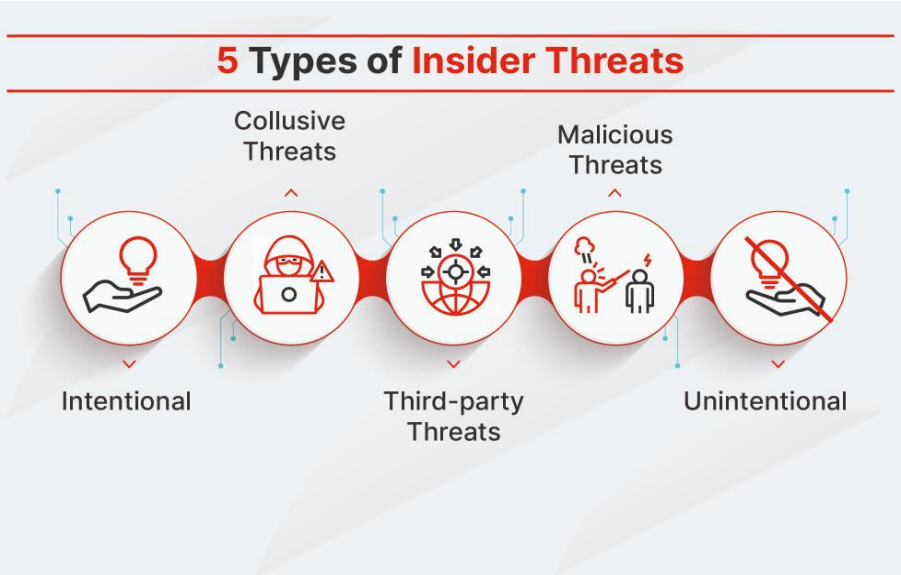
2. **Phishing Attacks**: These attacks involve deceptive emails or messages that trick individuals into revealing personal information or downloading malware. Phishing has become increasingly sophisticated, often mimicking legitimate organizations.



3. **Denial of Service (DoS) Attacks**: Cybercriminals may flood a network with traffic to overwhelm systems and disrupt services. Distributed Denial of Service (DDoS) attacks use multiple compromised systems to launch an even larger assault.

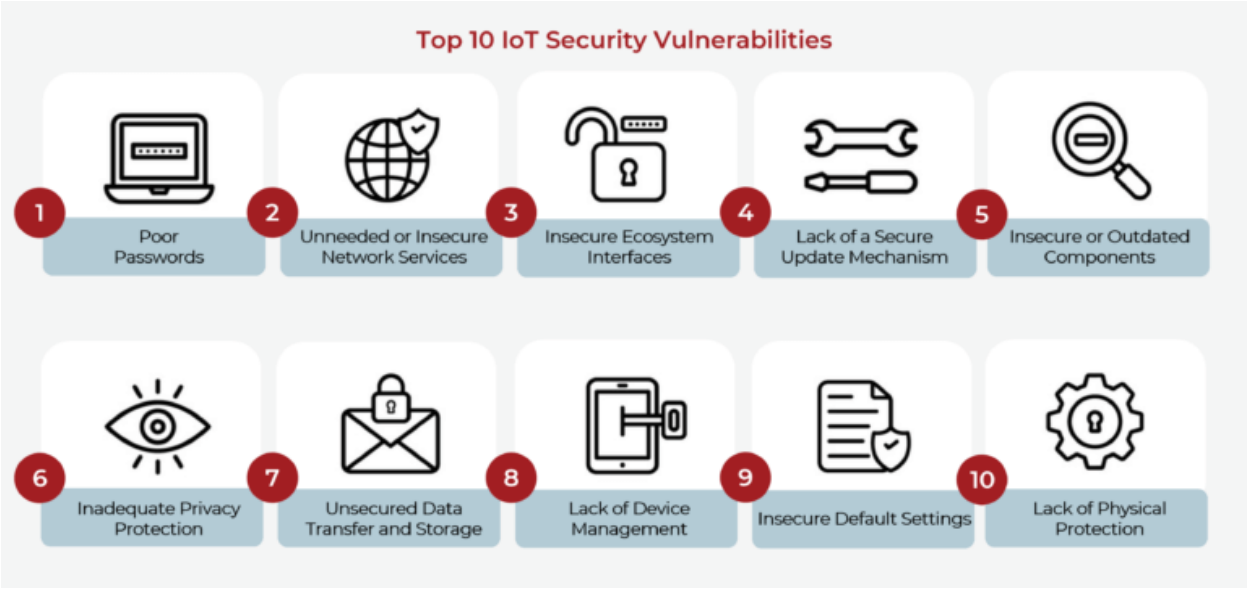


4. **Insider Threats**: Employees or contractors with access to sensitive information can intentionally or unintentionally compromise security. This could involve data theft or inadvertently sharing credentials.



5. **Advanced Persistent Threats (APTs)**: APTs involve prolonged and targeted cyberattacks where attackers gain access to a network and remain undetected for long periods, often with the goal of stealing sensitive information.

6. **Internet of Things (IoT) Vulnerabilities**: As more devices become connected to the internet, the potential entry points for cyberattacks increase. Many IoT devices lack adequate security measures, making them easy targets.



Solutions to Cybersecurity Threats

1. **Robust Security Software**: Employing comprehensive antivirus and anti-malware solutions can help detect and mitigate threats. Regular updates ensure protection against the latest threats.

2. **Employee Training and Awareness**: Educating employees about cybersecurity best practices, including recognizing phishing attempts and proper data handling, is essential in reducing human error.

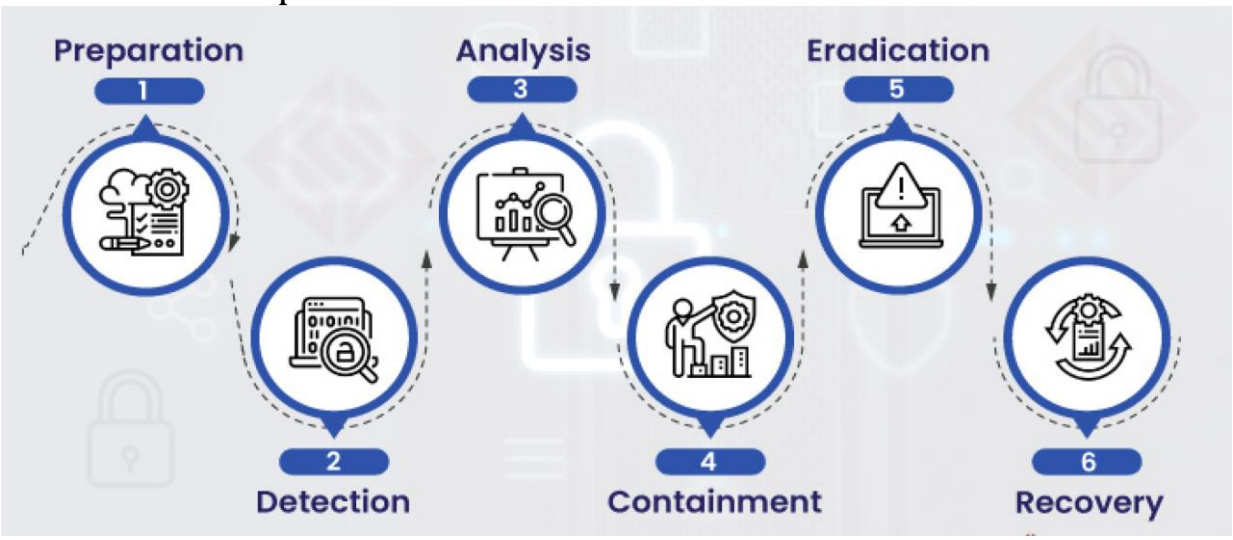
3. **Multi-Factor Authentication (MFA)**: Implementing MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access to accounts.

4. **Regular Software Updates**: Keeping operating systems, applications, and devices updated is critical. Many updates include security patches that protect against known vulnerabilities.

5. **Network Security Measures**: Utilizing firewalls, intrusion detection systems, and virtual private networks (VPNs) can help secure networks and monitor for unusual activity.

6. **Data Encryption**: Encrypting sensitive data both at rest and in transit protects it from unauthorized access. Even if data is intercepted, encryption makes it unreadable without the proper keys.

7. **Incident Response Planning**: Organizations should develop and regularly update an incident response plan to address potential breaches. This includes identifying critical data, defining roles, and establishing communication protocols.



8. **Regular Backups**: Maintaining regular backups of important data ensures that in the event of a ransomware attack or data loss, recovery is possible without capitulating to cybercriminals.

9. **Vulnerability Assessments**: Conducting regular assessments and penetration testing can help identify weaknesses in a system before they are exploited by attackers.

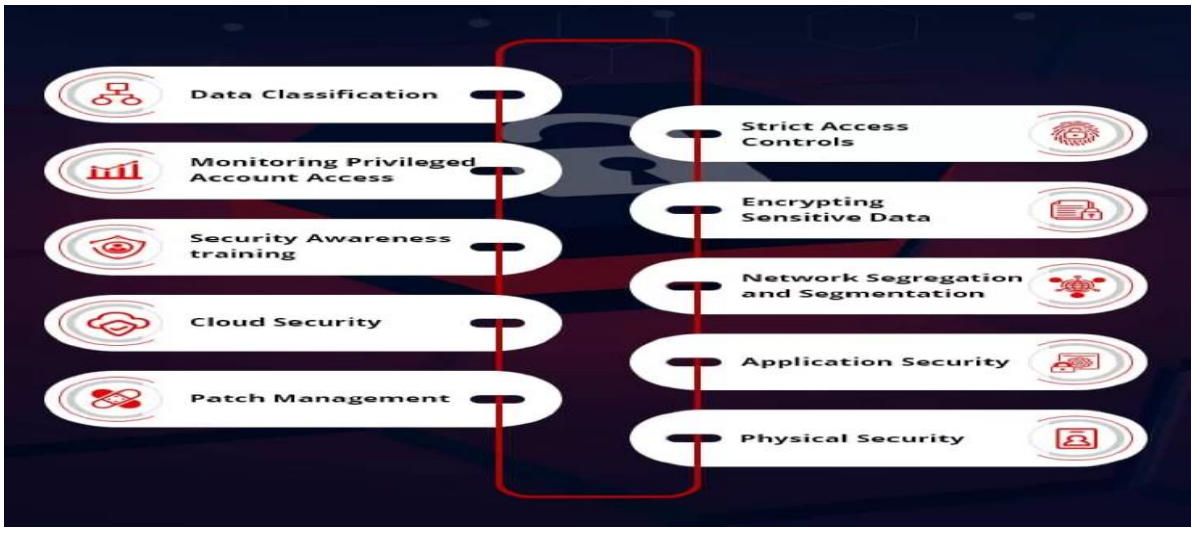
Conclusion

As cyber threats continue to evolve, so too must our strategies for combating them. A multi-faceted approach that includes technology, employee education, and proactive planning is essential for protecting sensitive data and maintaining trust in digital operations. By understanding the landscape of cybersecurity threats and implementing robust solutions, individuals and organizations can significantly reduce their risk and ensure a safer online environment.

KIBERTERRORIZM VA UNGA QARSHI KURASHISHDAGI MUAMMOLAR VA YECHIMLAR

Maxamadov Rustam Xabibullaevich,
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi o'qituvchisi, mustaqil izlanuvchi;

Djamatov Mustafa Xatamovich,
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o'qituvchisi.



Annotatsiya: *Ushbu maqolada hozirgi kunda yuzaga kelayotgan eng xavfli tahdidlardan biri bo'lgan – kiberterrorizm va unga qarshi kurashish bo'yicha va shu bo'yicha xalqaro tajribalar haqida ma'lumotlar keltirilgan. Shuningdek, kiberterrorizmga qarshi kurashish bo'yicha bir nechta taklif va tavsiyalar keltirilgan.*

Kalit so'zlar: *Kiber, kiberterrorizm, tahlil, terror, kompyuter, jinoyat, internet,*

mantiqiy bomba, virus.

Аннотация: *В данной статье представлена информация об одной из самых опасных угроз, возникающих сегодня – кибертерроризме и международном опыте борьбы с ним. Также представлены несколько предложений и рекомендаций по борьбе с кибертерроризмом.*

Ключевые слова: *Кибер, кибертерроризм, анализ, террор, компьютер, преступление, интернет, логическая бомба, вирус.*

XXI asrda axborot-kommunikatsiya texnologiyalarining tobora rivojlanib va kengayib borishi ushbu sohada turli ko'rinishdagi kiberjinoyatlar, shu jumladan terroristik yo'nalishdagi jinoyatlar paydo bo'lishiga sabab bo'lmoqda.

Hozirgi kunda yuzaga kelayotgan xavf-xatar va tahdidlar, avvalo, xalqaro terrorizm, diniy ekstremizm, noqonuniy migratsiya, odam savdosi, yoshlar o'rtasida xalqimizga yot g'oyalar tarqalishining tobora kuchayib borayotganligi ichki ishlar organlari oldiga o'z vaqtida ularning oldini olish va ularga barham berish bo'yicha yangi vazifalarni qo'ymoqda.

Kiberterrorizmning o'sishiga oid tahlillar shuni ko'rsatmoqdaki, uning butun insoniyatga nisbatan solayotgan tahdidi kun sayin ko'payib bormoqda. Sababi oddiy. Bugun dunyoda kompyuter kirib bormagan xonadon qolmayapti, tezkor internet tarmog'i iste'molini yaratish uchun davlatlar o'rtasida raqobat eng so'nggi cho'qqiga chiqmoqda.

Kompyuter ichiga "yorib" kirish, tarmoq ichidagi yoki tizimdagi ma'lumotlarni o'g'irlash va o'zlashtirib olish, kredit kartalardan fuqarolarning shaxsiy mablag'larini o'zlashtirish, yirik tashkilotlar yoki jismoniy shaxslar shaxsiy kompyuterlariga xavfli viruslar yuborib, elektron usulda mablag' talab qilish holatlarini kiberterrorizmning ishlash mexanizmining dastlabki bosqichlari sifatida ko'rsatishimiz mumkin.

Birinchidan, ushbu jinoyatning ishlash mexanizmi xalqaro tahlilchilar tomonidan to'liq va asosli o'rganib chiqilmaganligi;

Ikkinchidan, virtual dunyo ichidagi terrorchini aniqlash va uni xavfsizlantirish mushkul, o'z-o'zidan biz yashab turgan borliqdan farqli ravishda kiberterrorning izlari deyarli ko'rinmaydi. Afsuski, "elektron dunyo" turli siyosiy kuchlar uchun o'zlarining terroristik, ekstremistik tashviqotlar va g'oyalari, o'z qarashlarini ommaga targ'ib qilish, har xil jinoiy to'dalar faoliyatlarini amalga oshirish yo'lida asosiy qurol sifatida foydalanishmoqda. Yirik salbiy kuchlarning internet tarmog'ida o'zlarining mafkuraviy maydonlarini yaratib, internetda keng qamrovli axboriy terror – "kiber jihod" olib borayotgani, global va mintaqaviy xavfsizlikka nisbatan yangi tahdidlar, muammolar paydo qilayotganlari dunyo mamlakatlari oldida axborot xavfsizligini ta'minlash muammolarini keltirib chiqarmoqda.

Jahonning yirik davlatlari singari O’zbekistonga ham internet shiddatli qadamlar bilan kirib kelmoqda va kundalik hayotimizda o’z o’rniga ega bo’lmoqda. Hozirgi kunda hududimizda internet foydalanuvchilari soni yigirma milliondan oshib ketdi. Bugun terrorizm terrorchilar yashirinib yurgan yoki bosh qarorgohlari joylashgan muayyan davlat hududi bilan chegaralanib qolayotgani yo’q. Ular allaqachon kiber olamga ko’chib ulgurganlar. Terrorchi tashkilotlar o’z saflarini kengaytirish hamda maqsadlariga erishishda texnika va internetning so’nggi imkoniyatlaridan ustamonlik bilan foydalanmoqdalar.

Milliy qonunchilikda terrorizm qarshi kurashish bilan bog‘liq munosabatlar O’zbekiston Respublikasining 2000-yil 15-dekabrdagi “Terrorizmga qarshi kurash to’g‘risida”gi PQ-167-II-son Qonunida tartibga solingan bo’lib, bunda terrorizm (155-modda), tayyorlanayotgan yoki sodir etilgan terrorchilik harakatlari to’g‘risidagi ma’lumotlar va faktlarni xabar qilmaslik (155^1-modda), terrorchilik faoliyatini amalga oshirish maqsadida o’quvdan o’tish, chiqish yoki harakatlanish (155^2-modda) va terrorizmni moliyalashtirish (155^3-modda) kabi xatti-harakatlar uchun jinoiy javobgarlik O’zbekiston Respublikasi Jinoyat kodeksida belgilangan. Mutaxasisslar fikriga ko’ra, yuqori texnologiyalardan foydalangan holda uyushtirilgan kiberterrorizmning oqibatlari – yadro, kimyoviy yoki bakteriologik xujumlardan xavfliroq bo‘lishi mumkin.

Kompyuter terrorchilarining bugungi kundagi arsenali - turli xil viruslar, zararli dasturlar, “mantiqiy bombalar”, ya’ni dasturga oldindan o’rnatilgan va kerakli vaqtda ishga tushuriladigan buyruqlardan tashkil topgan. Biroq, hozircha zamonaviy terrorchilar Internetdan asosan yangi qurol sifatida emas balkim targ‘ibot va axborotni uzatish vositasi sifatida foydalanishmoqda.

Oddiy terrorichidan farqli ularoq kiberterrorchi o’z maqsadlariga erishish uchun zamonaviy axborot texnologiyalari, kompyuter tizimlari va tarmoqlari, kompyuter tizimlariga ruxsatsiz kirish va jabrlanuvchining axborot resurslariga masofadan hujum qilish uchun mo’ljallangan maxsus dasturlardan foydalanadi. Bu maqsadlarda ular, avvalambor tarmoqda axborotni olib tashlash, o’zgartirish yoki yo’q qilishni amalga oshiradigan kompyuter viruslari, shu jumladan yuqorida aytib o’tilgan "mantiqiy bombalari", "troyan" dasturlari, zararli dasturlar va boshqa turdagi axborot qurollaridan foydalanishadi.

Kiberterrorizm bank, transport va energetika tizimiga ega bo’lgan mamlakat uchun jiddiy xavf to’g‘diradi, ayniqsa, hukumat, davlat va iqtisodning xususiy sektori axborot tarmoqlari va yuqori texnologiyalarga tayangan bo’lsa.

Milliy qonunchiligimizda kiberterrorizm tushunchasi va uning usullari deyarli yoritilmagan bo'lib, bu holat kiberterrorizmga qarshi kurashish va uni oldini olishda asosiy muammolardan biri hisoblanadi. Milliy yuridik fanda ham "kiberterrorizm" tushunchasini ta'rifiga oid yagona nuqtai nazar ishlab chiqilmagan.

Ta'kidlash joizki, kiberterrorizm termini birinchi marotaba tahminan 1980-yillarda AQShdagi Xavfsizlik va razvedka instituti (Institute for Security and Intelligence) katta ilmiy xodimi Barri Kollin tomonidan ishlatilgan.

Ayrim olimlar kiberterrorizm tushunchasini o'zining siyosiy, iqtisodiy va ijtimoiy masalalarini yechishda ustunlikka erishish maqsadida odamlarning hayotiga suiqasd qilish, moddiy ob'ektlarga nisbatan destruktiv va boshqa bir qator harakatlar amalga oshirish, ob'ektiv ma'lumotlarni o'zgartish yoxud buzish orqali jamiyatda qurquv va vaxima uyg'otishga qaratilgan qonunga xilof harakatlarning majmui sifatida ta'riflashsa, boshqalari esa kompyuter tomonidan ishlov berilayotgan ma'lumotlarga, kompyuter tizimi yoki tarmog'iga qasddan hujum qilishni, agarda bunday harakatlar jamoat tartibini saqlash, aholini qo'rqitish va harbiy mojaroni provokatsion usulda keltirib chiqarishni maqsad qilish - deb ta'riflashadi.

AQSh FBQ Milliy infratuzilmalarni himoya qilish markazi direktori Ronald Dik 2002-yil hukumat tashkilotining saytida e'lon qilgan axborotida "kompyuter texnologiyasiga qaramlik zamonaviy dunyoning "Axilles nuqtasi" *("zaif nuqtasi" muallif izohi)*" sifatida atab, kiberterrorizmni o'z maqsadlariga erishish va davlat infratuzilmalarini yo'q qilishda, kompyuter va tarmoqlardan foydalanuvchi terrorizmning yangi ko'rinishi deb ta'riflagan.

Kiberterrorizm tushunchasi, uni sodir etishning asosiy usullari, shuningdek ahamiyati va maqsadlarini ko'rib chiqib, mazkur yo'nalishdagi mavjud muammolarni hal qilish uchun quyidagilarni taklif etamiz:

1. Ommaviy axborot vositalarida va ijtimoiy tarmoqlarda kanallar yaratib, reklama roliklari va turli podkastlar joylashtirib, targ'ibot ishlarini faol olib borish.

2. Huquqni muhofaza qilish organlari xodimlari uchun malaka oshirish kurslarini tashkil yetish va o'tkazish. Misol uchun, O'zbekiston Respublikasi IIV Akademiyasi tinglovchi-kursantlariga mazkur yo'nalishda kerakli bo'lgan bilim va ko'nikmalar berish.

3. Huquqni muhofaza qilish organlari tuzilmasida kiberterrorizmga qarshi kurashga ixtisoslashgan bo'linmalarni tashkil etish maqsadga muvofiq hisoblanadi. (Masalan, O'zbekiston Respublikasi Ichki ishlar vazirligining "Kiberxavfsizlik markazi"da).

4. Transchegaraviy terroristik kiberhujumlarning oldini olishda asoslangan ilmiy yondashuvlar olib borish va ushbu sohada ilmiy-uslubiy ta’minotini ishlab chiqish, shu orqali barcha mamlakatlarga integratsiya bo‘ladigan yagona platformani ishlab chiqish hamda xorijiy tajribani doimiy o‘rganib borish va amalda foydalanish.

Xulosa qilib aytganda, XXI asrda yuqori texnologiyalar yordamida sodir etilgan kiberterrorizm harakatlari global axborot inqirozini keltirib chiqarishi, mamlakatlarning infratuzilmasiga jiddiy ziyon keltirishi, turli mamlakatlarni bir-biriga qarama-qarshi qo‘yish va shu orqali dunyo ayrim mintaqalariga to’g‘ridan-to’g‘ri xavf tug‘dirishi mumkin. O’zbekiston Respublikasining jinoyat-huquqida bu kabi kibertahdidlarga munosib javob berishi lozim. Shuning uchun, kiberterrorizmga qarshi kurashish sohasida jinoyat-huquqiy siyosatni takomillashtirish ustuvor yo’nalishlaridan biriga aylantirish hamda ushbu sohada o‘qitib, yetuk mutaxassislar va kadrlar bo‘lib yetishishi uchun shart-sharoitlar yaratib berish maqsadga muvofiqdir.

THE IMPORTANCE OF MODERN TECHNOLOGIES IN ENSURING THE RIGHTS AND LEGAL INTERESTS OF JUVENILE VICTIMS IN CRIMINAL PROCEEDINGS

Zoirova Irodabegim Faizi kizi,
Doctoral student of the Law Enforcement
Academy of the Republic of Uzbekistan
irodabegim0206@icloud.com, +998970050012

Annotation: *This article explores the foundations of using videoconferencing systems as a form of applying modern technologies in criminal proceedings. It analyzes the significance of this practice in ensuring the rights and legal interests of juvenile victims during criminal court processes. Additionally, the article examines legal issues related to the implementation of this practice.*

Keywords: *video conferencing, open space, victims, children, publicity, special rooms, investigative actions.*

Аннотация: *Ушбу мақолада жиноят процесси жараёнларида замонавий технологияларни қўллаш шакли сифатида видеоконфернцалоқа тизимининг қўлланиши асослари ёритилган бўлиб, унга кўра жиноий суд процесси жараёнларида вояга етмаган жабрланувчиларнинг ҳуқуқ ва қонуний манфаатларини таъминлашдаги аҳамияти ҳамда мазкур амалиётни қўллашга оид ҳуқуқий муаммолар таҳлил қилинаган.*

Калит сўзлар: *видеоконференцалоқа, очиқ майдон, жабрланувчилар, болалар, ошкоралик, махсус хоналар, тергов ҳаракатлари.*

Аннотация: *В данной статье рассматриваются основы использования систем видеоконференцсвязи как формы применения современных технологий в уголовном судопроизводстве. Анализируется значение данной практики в обеспечении прав и законных интересов несовершеннолетних потерпевших в*

ходе судебных процессов по уголовным делам. Кроме того, в статье рассматриваются правовые вопросы, связанные с внедрением данной практики.

Ключевые слова: *видеоконференция, открытое пространство, потерпевшие, дети, публичность, специальные помещения, следственные действия.*

In the modern era, electronic justice is rapidly developing, and its application is demonstrating positive results. Technologies that seemed novel in the recent past have proven their viability and necessity, becoming an integral part of court proceedings. In this matter, the use of videoconferencing systems is of particular importance.

To examine the essence of videoconferencing, we need to determine what this technology actually is. Videoconferencing is a computer technology that allows long-distance subjects to view and hear each other, sharing information in Real-time. The essence of this technology lies in the fact that the image on the monitor or television replaces the direct participation of the person in the court hearing the case[1].

From a technical standpoint, video conferencing is a telecommunications technology involving the interactive participation of two or more remote subscribers, between whom audio and video data is exchanged in real time.[2]

The term "videoconferencing" also refers to any transmission or reception of images, sounds, and information exchange between computers using videoconferencing technology.

Several scientists have conducted research on topics related to the application of new technologies in the criminal justice system. According to the interpretation of foreign scholars on this topic[3], the "white board" in the videoconference system is a special application that opens a window and can enter text and graphic images (for example, signature) visible to each participant.

It should be noted that in order to ensure the safety of victims and witnesses, existing cryptographic protection tools allow for the confidentiality of video conferencing sessions from other users of the electrical network (computer network).

In particular, it is necessary to analyze the regulatory framework governing the use of similar technologies in ensuring the rights and legal interests of juvenile victims in criminal proceedings. According to Article 91^1 of the Criminal Procedure Code of the Republic of Uzbekistan, investigative actions involving witnesses, victims, suspects, and defendants (such as interrogation, identification of persons and objects, and confrontation) can be conducted through video conferencing using technical means. This can be done by summoning these individuals to the

law enforcement agency or court of the region, district, or city where they are currently located or reside. In the process of videoconferencing, participants in the investigative action directly monitor the process and results of the investigative action through direct broadcasting.

At the same time, Article 91^2 provides grounds for conducting investigative actions in videoconferencing mode, and in accordance with the second paragraph of this article, the need to ensure the safety of participants in the criminal process is also a basis. Also, interrogation, identification of persons or objects or confrontation in the videoconference mode shall be carried out in compliance with the requirements of Articles 96 - 108, 112 - 131 of this Code.

In the matter of realizing the legal interests of child victims at the stage of trial, according to Serbian scholars, minors are placed under special protection when they participate in the criminal proceedings as victims[4]. This special case primarily relates to the rules for hearing and questioning a victim who is a minor and requires careful treatment. Indeed, courtrooms are usually an unfamiliar and anxious environment for children. For the effective participation of juvenile victims, special procedural protection measures must be applied, taking into account their special needs.

When conducting a comparative legal analysis related to ensuring the rights and legal interests of juvenile victims at the stage of judicial proceedings, we should first focus on the essence of international standards.

In 1985, based on the general content of provisions 11 and 20 of the UN Minimum Standard Rules for the Administration of Juvenile Justice ("Beijing Rules") and the Guidelines on Juvenile Justice in Cases Related to Children Victims and Witnesses of Crime, it was established that, in the best interests of the child, information should be obtained from them by means other than the personal participation of children in court. For example, it is stated that it is advisable to use video recording or audio recording or camera listening at the pre-trial stage.

Children who are juvenile victims or witnesses of a crime should be interrogated outside the eyes of the defendant, using screens or closed-circuit television, and protected from direct negotiation by the defendant.

In this regard, according to A. Sharofutdinov, "In the legislation, the process of conducting procedural actions and their results can be recorded using video recording tools, and in some cases it is mandatory, but their procedural order is not fully covered, which leads to different interpretations of legal requirements in judicial and investigative practice. This is also evidenced by the analysis of the articles of the Criminal Procedure Code related to the use of video recording tools in the conduct

of procedural actions"[5]. That is, there are no clear rules regarding the use of the aforementioned methods in court proceedings involving juvenile victims. S. Aripov also expressed his opinion on this situation, stating that "if there is an opportunity to use modern information technology tools as auxiliary methods for confirming the conduct of investigative actions, the process and results of their conduct in criminal procedural legislation, why not use this opportunity and think about ways to reduce the turmoil of citizens through it!"[6]. Indeed, in order to ensure the legal interests of juvenile victims, it is advisable to use new modern methods.

If we analyze the legislation of foreign countries on similar rights, in Poland, the Ministry of Justice, with the support of non-governmental non-profit organizations, has established appropriate interrogation rooms for children, consisting of qualified, professional employees, to interview victims and witnesses[7]. This category of interrogation room ensures that it is conducted in a separate room with a double mirror or live broadcast of the interrogation. The room is equipped with a camera, microphone and other technical equipment to make the child feel comfortable and comfortable, as well as to assist the criminal justice system.

Under South African Criminal Law[8], children who are victims or witnesses can be present in courtroom and testify through mediators in order to prevent them from being subjected to excessive psychological stress or suffering.

In addition, children testifying on cases of sexual violence will give testimony in a separate room via video to avoid direct confrontation with the accused.

In accordance with Article 19 of the Criminal Procedure Code of the Republic of Uzbekistan, open consideration of criminal cases in courts may be carried out at the initiative of the court or at the request of the participants in the criminal process using audio and video recording, as well as in the mode of video conferencing. However, cases of crimes committed by persons under the age of eighteen, as well as other cases in order not to disclose information about the private life of citizens or information that degrades their honor and dignity, and in cases where it is necessary to ensure the safety of the victim, witness or other persons participating in the case, as well as members of their families or close relatives, are allowed to be considered in a closed court session by a court ruling. For similar reasons, the use of a videoconferencing system is not allowed in a closed court session, and audio and video recording of such a session is not carried out.

The controversial aspect of the issue is that in cases where the victim participating in the case is a minor, problems arise with the legal use of such technical methods.

For example, when cases involving a minor victim of crimes against sexual freedom are conducted in a closed format, videoconferencing cannot be used. To ensure the legal interests of juvenile victims, it is advisable to accept the testimony of the juvenile victim in a separate room in a videoconferencing mode to protect them from the eyes of the person who committed the crime. In this matter, In this regard, according to O. Allanazarov, in investigative units in areas where specially equipped interrogation rooms are not organized, the identification of the investigative action with the participation of minors can be carried out by turning the place of the identifier into a dark state and strengthening the light level of the identifiable location[9]. Of course, it is advisable to conduct similar practical experiments with a focus on regulatory norms.

According to our analysis, in order to ensure the testimony of juvenile victims in court, it is advisable to establish norms regarding the place where juvenile victims participate in video conferencing processes established by the Criminal Procedure Code of the Republic of Uzbekistan, as well as the technical methods used in accordance with their rights and interests. In our opinion, it is necessary to clarify the rules on the principle of transparency established in the Criminal Procedure Code in this matter.

KIBERJINOYAT VA ULARGA QARSHI KURASHISHNING O‘ZIGA XOS XUSUSIYATLARI

Iminov Abdurasul Abdulatipovich,
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i.
Maxamadov Rustam Xabibullaevich,
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi o’qituvchisi, mustaqil izlanuvchi;

Annotatsiya: *Maqolada bugungi kunda kibermakonda sodir etilayotgan jinoyatlar, ularning o’ziga xos xususiyatlari, kiberjinoyatlarni oldini olishning asosiy yo’nalishlari, kiberxavfsizlikni ta’minlash bo‘yicha taklif va tavsiyalar keltirilgan.*

Kalit so‘zlar: *Kiberjinoyat, jinoyat, internet, plastik karta, virus, kompyuter, URL, axborot texnologiyalari, sayt, DDoS, axborot, zararli dastur, ma’lumot, tarmoq.*

Аннотация: *В статье представлены преступления, совершаемые в современном киберпространстве, их специфика, основные направления предупреждения киберпреступности, предложения и рекомендации по обеспечению кибербезопасности.*

Ключевые слова: *киберпреступность, преступность, интернет, пластиковая карта, вирус, компьютер, URL, информационные технологии, сайт, DDoS, вредоносное ПО, информация, сеть.*

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi va kishilik jamiyatining barcha sohalarida internetdan keng foydalanish kundalik faoliyatning bir qismini tashkil etib, xizmat ko'rsatish, ilm-fan, ta'lim, elektron tijorat, shuningdek zamonaviy insonning fikrlash tarziga o'zining ijobiy ta'siri bilan kirib keldi. Hayot sifatini yaxshilash bilan bog'liq bo'lgan ushbu o'zgarishlar bilan bir qatorda, jinoyatchilikning yangi shakllarini rivojlantirishga qulay sharoitlar paydo bo'lganligini ta'kidlash lozim. Mazkur jinoyatlar o'z navbatida "Axborot texnologiyalari sohasidagi jinoyatlar" (kiberjinoyatlar) deb nomlanadi.

Kiberjinoyat - bu firibgarlik, o'g'irlik, tovlamachilik va boshqa noqonuniy harakatlarni amalga oshirish uchun dasturiy ta'minot va onlayn platformalardan foydalanish, kompyuterlar, tarmoqlar yoki internetdan hackerlik, fishing, identifikatorni o'g'irlash va kiber ta'qib qilish kabi noqonuniy xatti-harakatlarni amalga oshirishni o'z ichiga olgan jinoiy faoliyat jinoiy huquqbuzarlik hisoblanadi.

Axborot texnologiyalarining keng miqyosda rivojlanishi bir vaqtning o'zida ko'p turdagi jinoyatlarning sodir etilishiga imkon yaratdi, o'z navbatida ushbu turdagi jinoyatlarni aniqlash va ularni oldini olishda yuqori bilim va kasbiy tayyorgarlikni talab qilmoqda. Shunday qilib, "axborot texnologiyalari sohasidagi jinoyat" kompyuterlar va ma'lumotlarni qayta ishlash tizimlaridan foydalangan holda sodir etiladigan jinoiy harakat bo'lib, buning uchun qonunchilikda jinoiy javobgarlik nazarda tutilgan. Shu bois, fuqarolar o'rtasida axborot texnologiyalari sohasidagi jinoyatlar to'g'risida ma'lumotlarni tarqatish va targ'ibot-tashviqot ishlarini olib borish zarur. Kiberjinoyatlar va odatiy jinoyatlarning asosiy farqi shundaki, ular real hayotda emas balki virtual olamda sodir etiladi.

Kiberjinoyat shakllari ko'p qirrali bo'lib, Axborot texnologiyalari va internetning doimiy rivojlanishi bilan tobora ortib bormoqda. Shuningdek, ushbu jinoyatlarni aniqlash va fosh etishda bir qator qiyinchiliklar mavjud bo'lib, ulardan biri fuqarolarning o'ziga nisbatan sodir etilgan huquqbuzarligi to'g'risida huquqni muhofaza qiluvchi organlarga xabar berishni istamasliklari va kiberjinoyatlarga duch kelganda huquqiy bilimlari yetarli emasligi bilan bog'liqligini taqozo etmoqda.

Axborot texnologiyalari sohasidagi jinoyatlarning ayrim turlarini quyidagilar bo'lishi mumkin:

– virusli dasturiy ta’minotni tarqatish;
– foydalanuvchining maxfiy ma’lumotlarini o’g‘irlash;
– boshqa odamlarning intellektual faoliyat mahsulotlarini o’g‘irlash;
– ijtimoiy tarmoqlarda boshqalarning akkauntlarini buzish;
– yolg‘on ma’lumot tarqatish, tuhmat qilish;
– millatlararo nizo yoki dinlararo adovatni qo’zg‘atish.
– bank plastik kartalari (karta rekvizitlari) bilan noqonuniy operatsiyalarni amalga oshirish;
– qimmatli qog‘ozlar bozoridagi internet-firibgarlik bilan shug‘ullanish;
– internetdagi moliyaviy piramidalar yaratish;
– mobil aloqa bilan bog‘liq jinoyatlarni amalga oshirish;
– elektron boshqa jinoyatlar.

Yuqoridagi misollarni inobatga olgan holda, internet foydalanuvchilari uchun ularga nisbatan sodir etilishi mumkin bo’lgan kiberjinoyatlarni oldini olish bo’yicha ba’zi tavsiyalarni berish mumkin:

– Internetdan foydalanilganda, zararli faoliyatga qarshi kurashish uchun mo’ljallangan maxsus dasturiy ta’minotga ega qurilmalardan foydalanish, ularni o’z vaqtida yangilab turish;
– xavfsizlikka javob beradigan yangilanishlar o’rnatilgan, boshqa dasturiy ta’minotning joriy versiyalariga ega bo’lgan operatsion tizimdan foydalanish;
– saytlardan foydalanganda ularning tashqi ko’rinishiga, veb-manziliga e’tibor berish (ehtimol Siz uning soxta nusxasiga kirgandirsiz!);
– shaxsiy ma’lumotlarni faqat xavfsiz protokollardan foydalanadigan veb-saytlarga kiritish (odatda brauzerda bunday sayt manzili yonida yashil fonda blokirovka belgisi ko’rsatiladi);
– turli xil saytlarda bir xil login va parollardan foydalanmaslik;
– juda yengil yoki osongina taxmin qilinadigan parollardan foydalanmaslik (tug‘ilgan sana, telefon raqamlari va hokazo);
– imkon qadar, foydalanuvchi nomi va parolni kiritishdan tashqari, vaqtinchalik kodni kiritishni talab etuvchi, ikki martalik autentifikatsiyadan foydalanish, odatda SMS-xabar yoki “PUSH” xabarnomasi shaklida mobil telefoningizga yuboriladi;
– kutilmagan yoki g‘ayrioddiy tasodifiy kelgan elektron pochta xabarlaridan ehtiyot bo’lish, hatto jo’natuvchini bilsangiz ham, hech qachon ichidagi qo’shimchalarni ochmaslik yoki bunday elektron pochta manzilidagi havolalardan foydalanmaslik;

– hisob ma’lumotlarini talab qiladigan elektron pochta xabarlaridan ehtiyot bo’lish (moliya muassasalari deyarli hech qachon elektron pochta orqali moliyaviy ma’lumotni so’ramaydilar), hech qachon himoyalanmagan internet kanallari orqali moliyaviy ma’lumotlarni yubormaslik;

– do’stlaringizdan moliyaviy operatsiyalarni amalga oshirish yoki moliyaviy ma’lumotlarni uzatishni rag‘batlantiruvchi xabarlarni olganingizda, ushbu ma’lumotni boshqa aloqa kanallari (shaxsiy uchrashuv, telefon qo’ng‘irog‘i, ovozli xabar yo’llash imkoniga ega messenjer) yordamida tekshirish yoki o’ta og‘ir holatlarda javoblarini uchinchi shaxslar bilishi mumkin bo’lmagan nazorat savollarini berish orqali suhbatdoshingizning shaxsiga aniqlik kiritish;

– Internet orqali to’lovlarni amalga oshirishda, imkon qalar, “Visa” va “Mastercard” xalqaro to’lov tizimlari uchun “3D Secure” kabi to’lovlarning qo’shimcha xavfsizligini ta’minlash texnologiyalaridan foydalanish;

– o’zlarini bank xodimi deb tanishtirgan va bank kartangiz ma’lumotlarini berishingizni so’ragan notanish odamlar bilan hech qachon telefonda gaplashmaclik;

– bank karta ma’lumotlarini xavfsiz joyda saqlash, ularni hech kimga aytmaslik, xabar bermaslik yoki SMS orqali yubormaslik va hokazo;

–qayd etish yozuvlarining saqlanib qolishi uchun do’stlaringiz va yaqinlaringiz doirasini cheklash. Shaxsiy ma’lumotlaringizni hech qachon yangi onlayn do’stlar bilan baham ko’rmaslik. Tug‘ilgan sana, elektron pochta manzillari yoki parol sifatida ishlatilishi mumkin bo’lgan uy hayvonlari ismlari haqidagi ma’lumotlarni ommalashtirishdan saqlanish. Ushbu ma’lumotlarning barchasi professional hacker uchun juda foydali bo’lishi mumkin;

– “Diqqat! Sizning akkauntingiz buzib tashlandi. Akkauntingizni tasdiqlash uchun qo’ng‘iroq qilishingiz kerak. Bizga xabar yuboring, biz sizni qayta chaqiramiz” kabi xabarlardan ehtiyot bo’lish;

– “Clickjacking” qurboniga aylanmang. Bu shunday turdagi kiberhujumki, birinchi qarashda ular zararsiz kontentga o’xshab ko’rinadigan giperhavolalarni o’zida saqlaydi. Biroq giperhavolani bosish zararli dastur uchun yo’l ochadi, bu sizning kompyuteringizga tajovuz qilishi yoki sizning shaxsiy ma’lumotlaringizni chetga uzatishi mumkin;

– elektron pochta manzillarida va veb-saytda, agar siz ular bilan ish olib boradigan obro’li moliyaviy muassasalarning nomlarini o’z ichiga olgan bo’lsa ham URL manzillarini diqqat bilan ko’rib chiqing. Eng keng tarqalgan hiyla - bu qonuniy veb-sayt nomi va soxta narsalarning

kombinatsiyasi. Ushbu manzillar ko’pincha qonuniy ko’rinishda hackerlik faoliyati bilan bog‘liqligini yashiradigan nusxa ko’chiradigan saytlarga olib keladi. Ba’zida URL qonuniy bo’lishi mumkin, ammo havolani bosganingizda, u Sizni boshqa saytga olib boradi.

Kiberjinoyatchilik va kiberhujumlarga qarshi kurashishning 100% aqlga sig‘maydigan usuli yo’qligini allaqachon bilishingiz mumkin, ammo shunga qaramay, kompyuterlaringizni himoya qilish uchun shuncha ehtiyot choralarini ko’rishingiz kerak. Amalga oshiriladigan asosiy ishlar - bu nafaqat xavfsizlikni ta'minlaydigan dasturiy ta'minotdan foydalanish, bu nafaqat virusni qidiradi, balki turli xil zararli dasturlarni qidiradi, shu jumladan to’lov dasturini ham o’z ichiga oladi va uni kompyuterga kiritishni to’xtatadi. Asosan ushbu zararli kodlar sizning kompyuterlaringizga taniqli bo’lmagan veb-saytlarga, “Drive-by” tomonidan yuklab olingan fayllarga, “Mal Advertising” deb nomlanuvchi zararli reklamalarni ko’rsatadigan buzilgan veb-saytlarga tashrif buyurish yoki yuklab olish orqali kiritiladi.[1]

Antivirus bilan birga siz yaxshi xavfsizlik devoridan foydalanishingiz kerak. Windows 10/8/7 da o’rnatilgan xavfsizlik devori yaxshi bo’lsa ham, siz odatiy Windows xavfsizlik devoridan kuchliroq bo’lgan uchunchi tomon xavfsizlik devorlaridan foydalanishingiz mumkin. Agar u korporativ kompyuter tarmog‘i bo’lsa, foydalanuvchi kompyuterlarining hech birida Plug and Play qo’llab-quvvatlanmasligiga ishonch hosil qiling. Ya’ni, xodimlar flesh-disklarni yoki o’zlarining internet-kalitlarini USB ga ulay olmasliklari kerak. Shuningdek, kompaniyaning Axborot texnologiyalari bo’limi barcha tarmoq trafigini kuzatib borishi kerak. Yaxshi tarmoq trafigi analizatoridan foydalanish har qanday terminalda (xodimlar kompyuterida) kelib chiqadigan g‘alati xatti-harakatlarga tezkorlik bilan yordam beradi. DDoS hujumlaridan himoya qilish uchun veb-sayt oddiygina bitta serverga joylashtirilish o’rniga, turli xil serverlarga ta’sirini kamaytiradi. Bulutli xizmat yordamida Windowsni doimo yangilab turish eng yaxshi usul bo’ladi. Bu DdoS ning muvaffaqiyatli bo’lish imkoniyatini sezilarli darajada kamaytiradi (hech bo’lmaganda uzoq vaqt davomida). Sucuri kabi yaxshi xavfsizlik devoridan foydalaning va veb-saytingizni himoya qilish va himoya qilish uchun ba'zi bir asosiy choralarni ko‘ring.

Yuqoridagilardan kelib chiqib, xulosa o’rnida shuni ta’kidlash joizki, axborot texnologiyalari sohasidagi jinoyatlardan himoyalanishning eng yaxshi usuli-zamonaviy tahdidlardan xabardor bo’lishdir va o‘z vaqtida uning oqibatlarini bartaraf qilish chora-tadbirlarini qo‘llash lozim.

[1] http//www.uzbekcoders.uz /kiberhujumlar va ularni oldini olish

Shuningdek, kiber hujumlarga qarshi kurashishda viruslar, zararli dasturlar, ijtimoiy muhandislik va ma'lumotlarni uzatilish va qabul qilishiga javob beruvchi tarmoq protokollari, kompyuter tizimiga yoki uning ma'lumotlariga ruxsatsiz kirish huquqini olish yoki olishga harakat qilishlarni oldini olish, xizmat hujumlarini buzish yoki rad etish (DDoS), veb-saytni buzish yoki sayt xavfsizligini nazorat qilish, xodimlar tomonidan kompyuterlardan yoki ilovalardan noto‘g‘ri foydalanish, shifrlash usullari va algoritmlari bo‘yicha bilimlarni bilishi zarur va shart.

DIGITAL CONSTRUCTION – AS A FACTOR IN SUCCESSFUL ANTI-CORRUPTION ACTIVITIES

Abdurakhmatova Kamola Murodjon kizi
Doctoral student of Law Enforcement Academy
Electronic address: magic_star@bk.ru

Annotation: *In this article, the importance of introducing digital technologies in the field of construction, the organizational and legal reforms being carried out in our republic in this regard, and the need to automate construction control processes in the future are justified.*

Keywords: *Construction industry, digitization, fight against corruption, digital technologies*

Аннотация: *Ушбу мақолада рақамли технологияларни қурилиш соҳасига жорий этишнинг аҳамияти, бу борада республикамизда олиб борилаётган ташкилий - ҳуқуқий ислоҳотлар, келгусида қурилишни назорат қилиш жараёнларини автоматлаштириш зарурияти асослантирилилган.*

Калит сўзлар: *Қурилиш саноати, рақамлаштириш, коррупцияга қарши кураш, рақамли технологиялар*

Аннотация: *В данной статье обоснована важность внедрения цифровых технологий в сфере строительства, организационно-правовые реформы, проводимые в нашей республике в связи с этим, а также необходимость автоматизации процессов контроля строительства в будущем.*

Ключевые слова: *Строительная отрасль, цифровизация, борьба с коррупцией, цифровые технологии*

As we know, the construction industry has long been at the forefront of shaping the world around us, building tall skyscrapers, building solid infrastructure, and creating the places that serve as the foundation for modern life. However, traditional construction workflows often hinder the achievement of high efficiency, productivity and profitability.

The advent of digital technology ushered in a transformational era that is also encouraging the construction industry to rethink its activities and adopt innovative solutions.

The construction industry has struggled for a long time with many problems arising from inefficient and outdated processes. Manual planning, dispatch, and time tracking procedures proved laborious, error-free, and time-consuming, leading to costly delays and operational inefficiencies.

Among the developing countries, the scope of construction works in the territories of our Republic is increasing year by year.

In particular, the total volume of construction works in the republic in 2020 is 88 trillion. soums, 108 trillion soums in 2021, 131 trillion soums in 2022, 139 trillion soums in 2023 and 32 trillion soums in the 1st quarter of 2024, amounted to soums (118% increase compared to the 1st quarter of 2023)[1].

President Sh.Mirziyoev, in his holiday greetings to the employees of the construction sector of our country, noted that today our country has literally become a huge construction site, among other aspects, the construction industry is developing rapidly, new technologies and innovations, the most modern architectural solutions are actively entering the field.

In recent years, within the framework of the "Obod qishloq" and "Obod mahalla" programs, more than 1,500 villages and neighborhoods have been involved in the construction and improvement of road and transport infrastructure, engineering and communication networks, and social facilities.

It was emphasized that issues of increasing public control, improving quality and efficiency at all stages of construction processes through the wide introduction of modern information and communication technologies are in the center of constant attention.

Today, a new era has begun in the construction industry of our country. First of all, the legal and material-technical base of the industry has been strengthened, new construction organizations operating on the basis of advanced technologies and approaches are emerging in all regions of our republic, the building materials industry is developing at a high pace, and a system of training qualified mature personnel has been established[2].

Decree of the President of the Republic of Uzbekistan dated 27.11.2020 No. PF-6119 "On approval of the strategy of modernization, rapid and innovative development of the construction network of the Republic of Uzbekistan for 2021 - 2025"[3] on digitalization of urban

[1] https://mc.uz/uploads/mcuz_15107733652129.pdf

[2] https://president.uz/uz/lists/view/6552

[3] National database of legislative information, 29.08.2023, No. 06/23/151/0661

planning activities, introduction of modern information and communication technologies to the network Republic of Uzbekistan modernization of the construction network was defined as the main direction of rapid and innovative development.

Also, by 2025, the creation of four additional electronic platforms within the framework of the "Transparent Construction" national information system, as well as their integration with interdepartmental information systems and databases, was noted as one of the target indicators for the implementation of this strategy.

It should also be said that the work of the Ministry of Construction and Housing and Communal Economy in the field of digitization has been improved. In particular, 15 electronic information systems were developed and implemented in the field.

In particular, electronic information systems such as "Transparent Construction", "Rating", "Tender", "Construction Quality Control", "Aware Citizen" and "My House" are widely used by legal entities and individuals.

It is worth noting that globalization has a significant impact on the construction industry, like all other industries. In today's time when many important construction and infrastructure projects are being implemented, improving the legal system and processes to control bribery and corruption shows its relevance.

Most scholars point out that the construction industry is one of the most labor-intensive and least digitized and automated industries worldwide, facing low productivity, labor shortages, and safety issues[4].

And they believe that a potential solution to these problems is the study of technological advances[5].

In particular, in this regard, the German scientist Nathan Melenbrink and others noted that the goal of creating a fully automated construction site is to solve the above-mentioned problems, to allow the robot system to perform tasks autonomously in various conditions at the construction site[6].

[4] G. Ofori, Research on construction industry development at the crossroads, Construction Management and Economics 11 (3) (1993) 175–185, https://doi. org/10.1080/01446199300000017.

[5] A. Zhu, P. Pauwels, B. De Vries, Smart component-oriented method of construction robot coordination for prefabricated housing, Automation in Construction 129 (2021), 103778, https://doi.org/10.1016/j. autcon.2021.103778

[6] N. Melenbrink, J. Werfel, A. Menges, On-site autonomous construction robots: towards unsupervised building, Automation in Construction 119 (2020), 103312, https://doi.org/10.1016/j.autcon.2020.103312.

In fact, the increasing use of information and communication technologies (ICT) in the construction industry enables the automatic acquisition and enrichment of data from construction-related entities.

At the same time, digital construction management, enterprise resource planning and supply chain management systems can provide a large amount of information about activities, labor, equipment and materials, including related entities.

Based on the above, we can say that digital technologies in construction for managing and controlling the construction process in our country are not sufficiently developed. This can allow various law violations and corruption cases.

For example, information provided on paper by a construction company may not correspond to the actual situation. This poses an additional risk to the quality of construction.

Another common violation is construction with deviations from the design and design-build documents.

Unauthorized construction endangers the safety of these facilities and their compliance with construction norms and standards.

That being said, digital technologies in construction help with transparency.

The advantages of digitization in the construction industry are:

- This allows you to identify conflicts, quickly eliminate errors, defects and threats to the security of the project.
- This ensures full compliance with construction standards at construction sites and increases the reliability of projects.
- It serves to constantly monitor the progress of work and control the quality of construction works.
- Effective communication between all participants in the construction process creates the basis for rapid interaction and information sharing.

In construction, digital technologies serve as a tool that unites all participants of construction, including customers, contractors, technical control, control inspection in the field of construction and housing and communal economy, emergency situations, the state sanitary-epidemiological control center and other control bodies.

To sum up, digital technologies in construction are an integral part of the construction of the future, and in order to carry out effective state control over construction and prevent cases of corruption in the field, it is appropriate to implement the following organizational and legal measures.

Transparency and digitization are recognized as the best preventive measures to prevent corruption in every field.

For this reason, it is very important to ensure transparency in the field of construction control, digitalization of control measures.

In practice, maintenance of internal control logs by technical supervisors and the practice of conducting control in paper form is still preserved. This makes it difficult to monitor the construction regularly and remotely.

In some cases, there is no guarantee that the customer and the technologist colluding and deviating from the project or not complying at all will not occur in state construction facilities.

The solution to this problem is to establish a system for recording all control activities electronically (together with photos and video recordings through special tablets - for example, each stage of construction, digging, priming, etc.), automating work quality control processes and for all project participants.

We believe that it is necessary to create a special Unified Information Portal, which allows creating a single information space, and integrate it with the law enforcement agencies (prosecutors) charged with the task of controlling the construction industry.

KIBERBULLING - YOSHLAR ONGIGA TA'SIR

Abduraximov Amriddin Abduraximovich
IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o'qituvchisi, katta leytenant e-mail: amr.herezen28@gmail.com tel:+998944282802

Annotatsiya: *Ushbu maqolada shiddat bilan o'sib borayotgan jamiyatning ijtimoiy-iqtisodiy muammosi sifatida kiberbulling onlayn o'yin zo'ravonlik, virtual hujum uchun umumiy faktlar keltirilgan. Muammoning butunjamiyatga tarqalishi, asosan o'smir yoshlar o'rtasida o'zini o'zi tasdiqlashning universal usuli bo'lib travmatik holatlar bilan izohlanadi. Virtual hujum, sotsializatsiya muammolarini keltirib chiqaradigan, halokatli o'smirlar shaxsiyatidagi o'zgarishlar va ularning agressiv xulq-atvoriga tasirini aks etadi. Kiberbullingga doir statistik ma'lumotlar diagrammalarda namoyon qilingan.*

Kalit so'zlar: *kiberbulling; kibermobing; virtual aloqa; elektron pochta; ijtimoiy-iqtisodiy muammo; travmatik holatlar.*

Аннотация: *В данной статье представлены общие факты о кибербуллинг, насилии в онлайн-играх, виртуальных атаках как социально-экономической проблеме быстро растущего общества. Распространение проблемы на все общество объясняется травмирующими ситуациями, которые являются универсальным методом самоутверждения среди молодежи.*

Виртуальная агрессия отражает изменения личности деструктивных подростков, вызывающие проблемы социализации и их влияние на агрессивное поведение. Статистика кибербуллинга представлена в виде диаграмм.

Ключевые слова: *кибербуллинг; кибермоббинг; виртуальное общение; электронная почта; социально-экономическая проблема; травмирующие ситуации.*

Abstract: *This article presents general facts about cyberbullying, online game violence, virtual attack as a socio-economic problem of a rapidly growing society. The spread of the problem to the whole society is explained by traumatic situations, which are a universal method of self-affirmation among young people. Virtual aggression reflects the changes in the personality of destructive adolescents that cause socialization problems and their impact on aggressive behavior. Statistics on cyberbullying are presented in charts.*

Keywords: *cyberbullying; cyber mobbing; virtual communication; Email; socio-economic problem; traumatic situations.*

Bugungi Global o'zgaruvchan vaziyatda misol tariqasida kiberbulling va shu kabi hujum turlari ommalashib bormoqda. Kiberbulling ko'p hollarda insonlar o'limga sabab bo'lib, kibermakonda onlayn o'yin zo'ravonlik deb ataladigan kibermobbing muammosi sonining ko'payishi orqali, o'zaro aloqada platformalardan foydalangan holda odamlarni birlashtiradi go'yoki ularning ijtimoiy, madaniy va geografik kelib chiqishini taqdim etish o'zlarini qiziqtirgan mavzular bo'yicha fikrlar, vayronkor g'oyalar hamda onlayn tahdidlar bilan miyasini zaharlab bundan qo'pol matnlardan, tvitlardan, postlardan yoki xabarlar bilan ommaga oshkor etishadi. Shu kabi qulay imkoniyatdan boshqa birovni xafa qilish yoki sharmanda qilish uchun mo'ljallangan shaxsiy ma'lumotlar, rasmlar yoki videolarni joylashtirib o'zining g'arazli maqsadlari tomon harakatlanishadi.

Kiberbulling o'zi nima?

Rossiyalik mutaxassislar ijtimoiylashuv jarayoni tobora kuchayib borayotganiga e'tibor berishmoqda [1]. Ma'lumotga tariqasida g'araz niyatli guruhlar bo'linib Internetda tanishish, turli ijtimoiy rollar va me'yorlarni o'zlashtirishga urinishadi. Biroq, virtualga bog'lanish dunyo shaxslararo muloqotning o'ziga xos xususiyatlarini o'zgartirmoqda. Virtual aloqa haqiqiy o'zaro ta'sirdan anonimlik, bilvositalik, nazoratsizlik, axloqiy va ijtimoiy chegaralarini pasaytirish, bu Internetda tovlamachilik holatlariga olib kelishi mumkin.

Bulling (inglizcha bullying - masxara, ta'qib, qo'rqitish) ichida haqiqiy muloqot turli yosh guruhlarida, masalan: ta'lim dargohida yoki sport to'garaklarida sodir bo'ladi, lekin ko'pincha o'smirlar orasida kuzatiladi. Masalan: V. K. Jeleznikovning hikoyasida tasvirlangan. R. Bikov shu nomdagi "Daxshatli" filmida aks ettirilgan. Onlayn zo'ravonlik,

kiberbulling deb ataladi. Kiberbulling – qaysidir bir texnologiyadan boshqa odamni bezovta qilish, tahdid qilish, sharmanda qilish yoki nishonga olish uchun foydalaniladi. [2] Bu jabrlanuvchining hissiy sohasining yomonlashuviga intiladi yoki uning ijtimoiy munosabatlarini buzilishiga sabab bo'ladi. Virtual psixologik hujumning og'ir oqibatlari depressiya, o'z joniga qasd qilish va boshqalar mavjud bo'lib, bu qiyinchiliklarni keltirib chiqaradigan doimiy shaxsiy o'zgarishlarga olib keladi.

Kiberbullying belgilari turlicha, ammo quyidagilarni o'z ichiga olishi mumkin:

Global tarmoqda yoki smartfonlardan foydalanish paytida yoki undan keyin hissiy jihatdan tez xafa bo'lish;

O'zining raqamli hayotini juda yashirin yoki himoya qilish o'z xonasida odatdagidan ko'proq vaqt o'tkazish;

Oila a'zolari, do'stlari va o'zini faoliyatidan voz kechish yoki ularga qiziqish yo'qligi;

Turli tashkilotlarda yoki guruh yig'ilishlaridan qochish g'azab bilan "harakat qilish";

kayfiyat, xatti-harakatlar, uyqu yoki ishtahaning o'zgarishi;

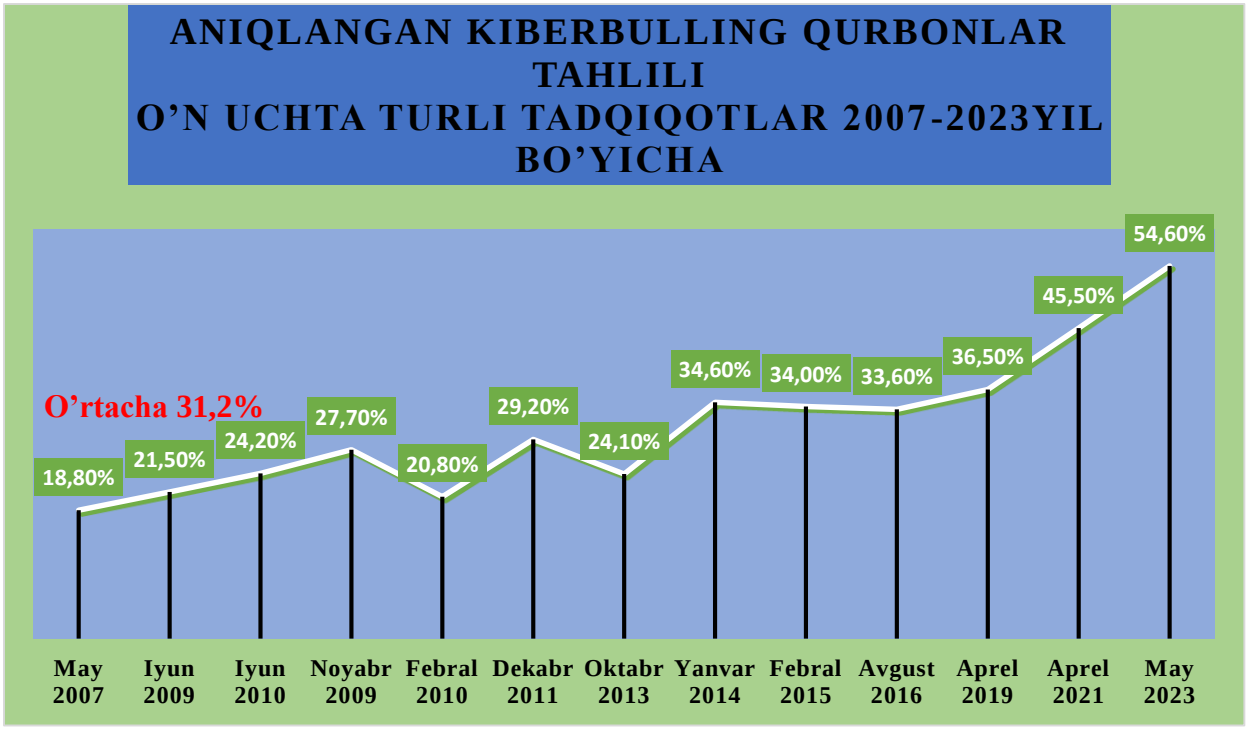
to'satdan kompyuter yoki qurilmadan foydalanishni to'xtatish istagi xabar, matn yoki elektron pochta xabarini olayotganda asabiylashish;

kompyuter yoki telefon faoliyati haqida munozaralardan qochish.

Kiber-mobbing -axborot-kommunikatsiya texnologiyalaridan foydalanish bilan tavsiflangan mobbing shakllaridan biri (masalan, Internet-ijtimoiy tarmoqlarga muvofiqlashtirilmagan suratlarni yuklash yoki kimnidir masxara qilish uchun shaxsiy ma'lumotlarni almashish). Mobbingning zaruriy shartlaridan biri bu doimiy harakat yoki faoliyat bo'lib, u odatda tajovuzkor va jabrlanuvchi o'rtasidagi kuch nomutanosibligi bilan tavsiflanadi. Quvvatning bu nomutanosibligi jismoniy (masalan, bo'y yoki kuch) yoki ijtimoiy (masalan, tengdoshlar orasida mashhurlik) bo'lishi mumkin, ammo kibermobbing bunday old shartlarni talab qilmaydi. Axborot-

kommunikatsiya texnologiyalaridan foydalanish qobiliyati (ba'zi tadqiqotchilar ham ularni afzallik deb bilishadi) har kimga boshqalarga zarar yetkazish imkoniyatini beradi. Onlayn muloqot juda qisqa vaqt ichida kontentni qayta ishlab chiqarish va tarqatish qobiliyati, kontentning nisbiy abadiyligi yoki doimiyligi (kontentni o'chirishning iloji yo'q), nashr etilgan kontentni nazorat qila olmaslik va uning doimiy mavjudligi bilan tavsiflanadi. Internetda joylashtirilgan kontentni o'chirib bo'lmasligi yoki ma'lum vaqtdan keyin qayta paydo bo'lishi kibermobbingning o'ziga xos xususiyatlaridan biridir. Aynan mana shu omil jabrlanuvchilar uchun ayniqsa og'riqli bo'lib, ular ta'lim muassasasini, ish joyini o'zgartirganda yoki boshqa davlatga ko'chib o'tganda yana masxara qilishlariga to'g'ri keladi va shu bilan to'liq kuchsizlik hissi paydo bo'ladi.

1-rasm. Dunyoda kiberbulling qurbonlar tahlili



Yuqoridagi jadvalda ko'rsatilganidek, biz ushbu hodisani o'rgangan yillar davomida kiberbulling qurboni bo'lish darajasi o'zgarib turardi. O'rtacha, bizning so'nggi 2023-yilda kiberbullingni 13 ta tadqiqotimizning bir qismi bo'lgan talabalarning taxminan 31% zi o'zlarining hayotlari davomida kiberbulling qurboni bo'lganliklarini aytishdi. Biz o'tkazgan tadqiqot ishlarida kiberbulling jinoyatlarining ko'rsatkichlari ham turlicha bo'lgan. O'rtacha, so'nggi 12 ta tadqiqotimizning bir qismi bo'lgan talabalarning taxminan 16 % zi o'zlarining hayotlari davomida boshqalarni kiberbulling qurboni bo'lganini tan olishgan.

2-rasm Kiberbullingga jarayoni

Xulosa qilib aytadigan bo'lsak, kiber zo'ravonlik odamlar uchun juda zararli oqibatlarga olib keladi. Bu maktab hayotini buzadi balki Oliy o'quv yurti tinglovchilarga ham katta hissiy zarar keltiradi va halokatli

oqibatlarga olib kelishi mumkin. Texnologiya talabalar va o'smirlar uchun yangi imkoniyatlarni taqdim etgan bo'lsa-da, har bir kishi undan mas'uliyat bilan foydalanishni o'rganishi muhimdir. Texnologiyadan mas'uliyat bilan foydalanishni ta'minlash uchun modellar ham ishlab chiqilishi kerak. Maktab rahbariyati maktablarda kiber jinoyatlarni aniqlash, oldini olish va ularga javob berish usullarini qo'yishi kerak. Ota-onalar ham o'z farzandlarini himoya qilish mas'uliyatini o'z zimmalariga olishlari kerak. Xalqimizda shunday naql bor: "Bir bolaga yetti mahalla Ota-ona". Boshqa tomondan, o'smirlar kiber jinoyatlar va bezorilikning oldini olish uchun birinchi zarur choralarni ko'rishlari shart.

CYBERSECURITY CHALLENGES IN REAL-TIME NAVIGATION SYSTEMS FOR AUTONOMOUS VEHICLES

Nurilla Mahamatov Ergashovich
Doctor of technical sciences, professor, Turin polytechnic university in Tashkent, head of the department, Tashkent region,
n.mahamatov@polito.uz
+998 97 749 70 15

Javokhir Rahimov Rustam o'g'li
Turin polytechnic university in Tashkent,
PhD student, Tashkent region,
j.rakhimov@polito.uz
+998 99 887 84 07

ABSTRACT: *Autonomous vehicles (AVs) represent a significant breakthrough in transportation technology, offering opportunities to enhance safety and efficiency. However, the integration of real-time navigation systems introduces critical cybersecurity challenges that must be addressed to ensure the reliability and safety of*

these systems. This paper explores the primary cybersecurity threats faced by real-time navigation systems in autonomous vehicles, examines their impact on vehicle safety and performance, and discusses potential solutions and best practices to mitigate these risks.

Keywords: *Cybersecurity, Autonomous Vehicles (AVs), Real-Time Navigation Systems, GPS Spoofing, V2X Communication.*

АННОТАЦИЯ: *Автономные транспортные средства (АТС) представляют собой значительный прорыв в транспортной технологии, предлагая возможности для повышения безопасности и эффективности. Однако интеграция систем навигации в реальном времени вводит критические кибербезопасностные вызовы, которые необходимо учитывать для обеспечения надежности и безопасности этих систем. В данном тезисе рассматриваются основные кибербезопасностные угрозы, с которыми сталкиваются системы навигации в реальном времени в автономных транспортных средствах, анализируется их влияние на безопасность и производительность транспортных средств, а также обсуждаются потенциальные решения и лучшие практики для снижения этих рисков.*

Ключевые слова: *кибербезопасность, автономные транспортные средства (АТС), системы навигации в реальном времени, подделка GPS-сигналов, связь V2X.*

ANNOTATSIYA: *Avtonom transport vositalari (ATVlar) transport texnologiyasida muhim yutuq bo'lib, xavfsizlik va samaradorlikni oshirish imkoniyatlarini taqdim etadi. Biroq, real vaqt rejimidagi navigatsiya tizimlarining integratsiyasi ushbu tizimlarning ishonchliligi va xavfsizligini ta'minlash uchun hal qilinishi lozim bo'lgan kiberxavfsizlikka oid jiddiy muammolarni keltirib chiqaradi. Ushbu tezisda avtonom transport vositalaridagi real vaqt rejimidagi navigatsiya tizimlari duch keladigan asosiy kiberxavfsizlik tahdidlari, ularning transport vositalari xavfsizligi va samaradorligiga ta'siri tahlil qilinadi hamda ushbu xavflarni kamaytirish uchun mumkin bo'lgan yechimlar va eng yaxshi amaliyotlar muhokama qilinadi.*

Kalit so'zlar: *kiberxavfsizlik, avtonom transport vositalari (AV), real vaqt rejimida navigatsiya tizimlari, GPS soxta signallari, V2X aloqa.*

Introduction

The rapid development of autonomous vehicles (AVs) has brought about transformative changes in transportation, with real-time navigation systems playing a central role in their operation. These systems rely on a combination of sensors, communication networks, and complex algorithms to make real-time decisions regarding vehicle movement. However, the increasing sophistication of cyber threats poses significant risks to the security and reliability of these systems. This paper aims to identify and analyze the cybersecurity challenges associated with real-time navigation systems in autonomous vehicles and propose strategies for addressing these challenges.

Real-Time Navigation Systems in Autonomous Vehicles

Real-time navigation systems in AVs encompass various technologies, including Global Navigation Satellite Systems (GNSS),

Inertial Measurement Units (IMUs), radar, lidar, and vehicle-to-everything (V2X) communication networks. These components work together to provide accurate positioning, map updates, and situational awareness. The effectiveness of these systems is crucial for the safe operation of AVs, as they enable real-time decision-making and adaptive responses to dynamic driving conditions.

Cybersecurity Threats to Real-Time Navigation Systems

1. GPS Spoofing and Jamming

Global Navigation Satellite Systems (GNSS), such as GPS, are fundamental to real-time navigation in AVs. However, they are vulnerable to spoofing and jamming attacks. Spoofing involves transmitting false GNSS signals to mislead the vehicle's navigation system, while jamming disrupts the signal reception, leading to potential loss of positioning accuracy [1]. These attacks can result in navigation errors, incorrect route decisions, and compromised vehicle safety.

2. Data Interception and Manipulation

Real-time navigation systems rely on the exchange of data between various components, including sensors and communication networks. Data interception and manipulation attacks can occur when malicious actors gain unauthorized access to these data streams. This can lead to the introduction of false information, such as incorrect road conditions or obstacle data, potentially causing accidents or unsafe driving behavior [2].

3. Vehicle-to-Everything (V2X) Communication Vulnerabilities

V2X communication is essential for enabling AVs to interact with their environment, including other vehicles, infrastructure, and pedestrians. However, V2X networks are susceptible to various cyber threats, including eavesdropping, spoofing, and denial-of-service (DoS) attacks. Compromising V2X communication can disrupt the exchange of critical information, affecting the vehicle's ability to respond to dynamic traffic conditions and hazards [3].

4. Sensor Fusion Attacks

Real-time navigation systems use sensor fusion techniques to integrate data from multiple sensors, such as lidar, radar, and cameras, to create a comprehensive understanding of the vehicle's environment. Sensor fusion attacks involve manipulating or falsifying sensor data to deceive the navigation system. These attacks can lead to incorrect hazard detection, navigation errors, and unsafe vehicle behavior [4].

Impact of Cybersecurity Threats on Vehicle Safety

Cybersecurity threats to real-time navigation systems can have severe consequences for vehicle safety and performance. Compromised navigation accuracy can result in dangerous driving decisions, such as

incorrect lane changes or failure to detect obstacles. Data manipulation can lead to erroneous situational awareness, increasing the risk of accidents. Additionally, vulnerabilities in V2X communication can disrupt coordination with other road users, exacerbating traffic congestion and safety hazards.

Mitigation Strategies

1. Robust Authentication and Encryption

To address cybersecurity threats, it is essential to implement robust authentication and encryption mechanisms for data transmission and communication. Encryption ensures that data exchanged between the vehicle's components and external networks is protected from unauthorized access and tampering. Additionally, authentication mechanisms can verify the integrity and authenticity of data sources [5].

2. Redundancy and Fail-Safe Mechanisms

Implementing redundancy and fail-safe mechanisms can enhance the resilience of real-time navigation systems. For instance, backup navigation systems and sensors can be used to cross-check and validate data, reducing the impact of potential attacks. Fail-safe mechanisms can ensure that the vehicle remains in a safe state in the event of a system compromise [6].

3. Continuous Monitoring and Threat Detection

Real-time monitoring and threat detection systems are crucial for identifying and responding to cybersecurity threats. Implementing intrusion detection systems (IDS) and anomaly detection algorithms can help detect suspicious activities and potential attacks. Continuous monitoring enables timely responses to mitigate the impact of cyber threats [7].

4. Collaboration and Standards Development

Collaboration between industry stakeholders, researchers, and policymakers is essential for developing cybersecurity standards and best practices for autonomous vehicles. Establishing industry-wide standards can help ensure consistent security measures and promote the adoption of best practices across the sector [8].

Conclusion

The integration of real-time navigation systems in autonomous vehicles introduces significant cybersecurity challenges that must be addressed to ensure the safety and reliability of these systems. Cyber threats, including GPS spoofing, data interception, V2X communication vulnerabilities, and sensor fusion attacks, pose serious risks to vehicle safety and performance. Implementing robust authentication and encryption, redundancy and fail-safe mechanisms, continuous

monitoring, and collaborative standards development are critical for mitigating these risks. As autonomous vehicle technology continues to evolve, addressing cybersecurity challenges will be essential for achieving safe and secure transportation systems.

KIBERJINOYATCHILIKNI RIVOJLANISHIDA DARKNETNING O'RNI

Risqaliyev Jaxongir Dadajon-o'g'li
Ichki ishlar vazirligi Malaka oshirish instituti, Toshkent shahri

Annotatsiya: *Internetning bir qismi, maxsus dasturlar orqaligina kirish mumkin bo'lgan darknetdan kiberjinoyatchilar qurol-yarog', giyohvand moddalar va odam savdosi kabi noqonuniy faoliyat uchun foydalanib kelishmoqda. Tor tarmog'i hamda kriptovalyutalarning yaratilishi jinoyatchilarga noqonuniy faoliyatlarni anonim tarzda amalga oshirishlariga imkon berdi. Buning natijasida esa darknetdan foydalanish ko'payib bormoqda.*

Kalit so'zlar: *internet, darknet, kiberjinoyatchilik, Tor brauzer.*

Abstract: *The darknet, a part of the Internet accessible only through special software, is being used by cybercriminals for illegal activities such as arms, drug, and human trafficking. The Tor network and the creation of cryptocurrencies have allowed criminals to conduct illegal activities anonymously. As a result, the use of the darknet is increasing.*

Keywords: *internet, dark web, cybercrime, Tor browser.*

Аннотация: *Даркнет, часть Интернета, доступная только через специальное программное обеспечение, используется киберпреступниками для незаконной деятельности, такой как торговля оружием, наркотиками и людьми. Сеть Tor и создание криптовалют позволили преступникам анонимно вести незаконную деятельность. В результате использование даркнета увеличивается.*

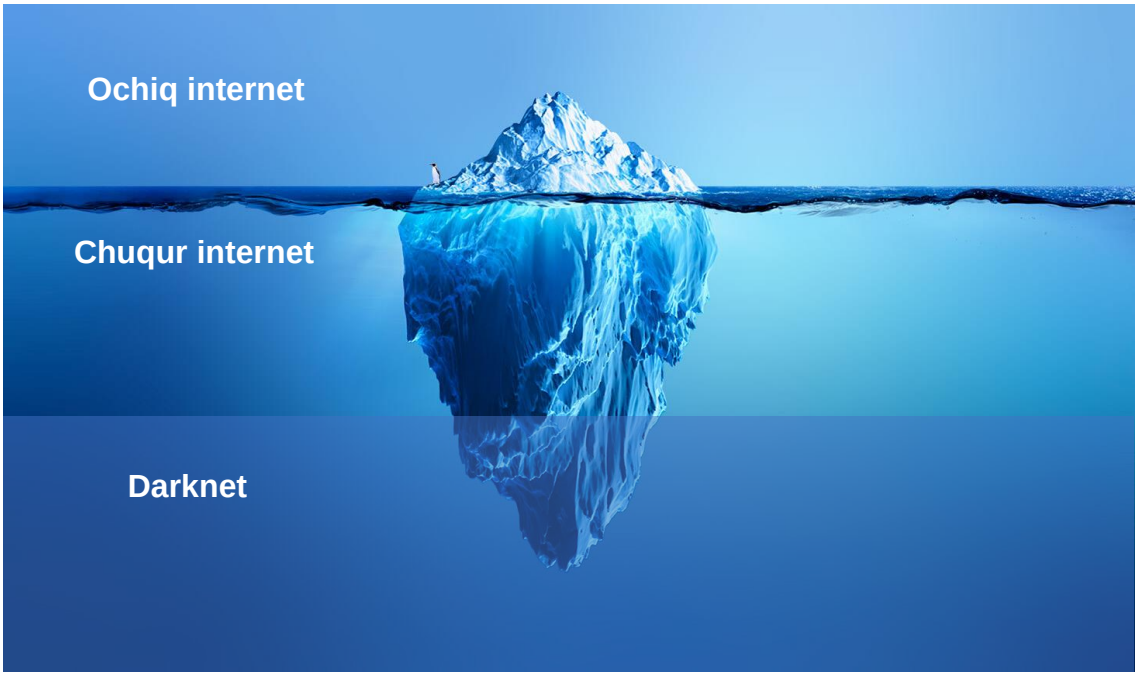
Ключевые слова*: интернет, даркнет, киберпреступность, браузер Tor.*

Foydalanuvchi so'rov orqali Google, Yandex yoki Bing internet qidiruv tizimlaridan oladigan ma'lumotlar ochiq internetdagi ma'lumotlardir. Internetning shunday tarkibiy qismlari borki, u yerdagi ma'lumotlar yuqoridagi qidiruv tizimlariga ko'rinmaydi.

Mutaxassislar odatda internetni quyidagi 3 ta qatlamga, ya'ni ochiq internet (surface web), chuqur internet (deep web), yopiq internet yoki darknet (dark web) bo'lishadi (1-rasm).

Ochiq internet – bu barcha uchun ochiq bo'lgan internetdir. Agar butun internetni aysberk deb tassavur qilinsa, ochiq internetni aysberkni uchi deb qarash mumkin. Google Chrome, Microsoft Edge yoki Mozilla

Firefox kabi an’anaviy brauzerlar orqali kirish mumkin bo’lgan barcha ommaviy veb-saytlar ochiq internetda joylashadi. Bunday saytlarni mashhur qidiruv tizimlarida osongina topish mumkin, chunki qidiruv tizimlari internetni ko’rinadigan havolalar orqali indekslanadi. Statistik ma’lumotlarga qaraganda ochiq internet jami internetning 5 %idan kamrog‘ini tashkil qiladi[1].



1-rasm. Internet qatlamlari

Chuqur internet (deep web) – ochiq internet ostidagi, kuchli himoyalangan sayt yoki ma’lumotlar bazalaridan tashkil topgan internet hisoblanadi. Bunday saytlarga kirish uchun oddiy brauzerlarni ishlatsa bo’ladi, ammo bunday saytlar internet qidiruv tizimlari tomonidan aniqlanmaydi. Bu saytlarni chuqur internetga joylashtirilishining sababi xakerlarning hujumidan himoya qilishdir[2]. Odatda chuqur internetdagi axborot tizimlari xavfsizlik devori (firewall) ortiga yashiriladi. Chuqur internetda bank, soliq, moliya, elektron pochta, tibbiyot xujjatlari yoki ijtimoiy tarmoq xabarlari bo’ladi.

Darknet (dark web) – bu oddiy brauzerlar orqali kirib bo’lmaydigan, internetning yashirin, shifrlangan qismidir. Darknet dastlab AQShda harbiy aloqa uchun ishlab chiqilgan bo’lsa-da, hozirda odamlar noqonuniy yoki anonim faoliyatlarni amalga oshirishda foydalanib kelishmoqda. Darknet foydalanuvchining haqiqiy IP-manzilini

[1] https://www.kaspersky.com/resource-center/threats/deep-web
[2] https://texnokun.uz/?p=3842

anonimlashtiradigan murakkab tizimlardan foydalanadi, bu esa qurilma qaysi veb-saytlarga tashrif buyurganligini aniqlashni juda qiyinlashtiradi[3].

Darknetda quyidagi faoliyatlar keng tarqalgan:

1. Noqonuniy bozorlar: Giyohvand moddalar, qurollar, o'g'irlangan ma'lumotlar, qalbaki hujjatlar kabi noqonuniy mahsulotlar va xizmatlar;

2. Anonim xizmatlar: Anonim elektron pochta, shifrlangan chatlar va VPN (virtual private network) xizmatlari;

3. Forumlar va hamjamiyatlar: foydalanuvchilarni anonim ravishda muloqot qilishi, ba'zida esa noqonuniy harakatlar yoki xakerlik bo'yicha maslahatlar;

4. Xakerlik xizmatlari: Xakerlik xizmatlari, zararli dasturiy mahsulotlar.

Satoshi Nakamoto ismli odam tomonidan 2009-yilda birinchi kriptovalyuta, ya'ni Bitcoinni taqdim etilishi internetda noqonuniy operatsiyalarni amalga oshirishda inqilob yasadi[4]. Chunki, bitkoinlardagi anonimlik, transchegaraviy operatsiyalarning qulayligi va hisob-kitoblarning yakuniyligi jinoyatchilar uchun saytda o'zlarining noqonuniy faoliyatini amalga oshirishda mukammal vositaga aylandi.

Darknetga Tor (The Onion Router) brauzer yoki I2P (Invisible Internet Project) kabi anonimlashtiruvchi dasturlar orqali kiriladi. Darknet saytlarini yuqori darajadagi *"onion"* domeni bilan ajratib olish mumkin.

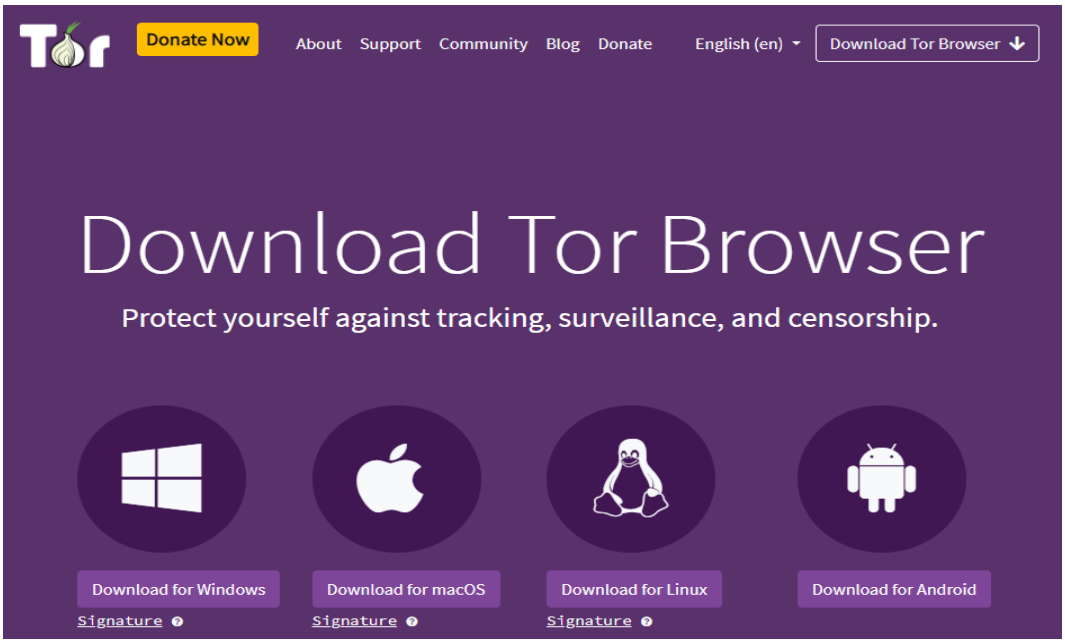
Masalan,

- https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/
- http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/

[3] https://www.ceopeducation.co.uk/parents/articles/what-is-the-dark-web/

[4] https://www.soscanhelp.com/blog/history-of-the-dark-web

Tor brauzerini *https://www.torproject.org/download/* saytiga kirib, bepul yuklab olish mumkin (2-rasm).



2-rasm. Tor brauzerini yuklab olish sayti interfeysi

Tor tarmog‘i orqali veb-trafikni shifrlash va qayta yo’naltirish uchun “onion” marshrutlashdan foydalanadi. Ma’lumotlar bir nechta shifrlash qatlamlarida himoyalangandan so’ng, veb-trafik onion routerlari deb ataladigan bir qator tarmoq tugunlari orqali uzatiladi. Har bir marshrutizator (yoki tugun) ma’lumotlar to’liq shifrlangan yakuniy manzilga yetguncha shifrlash qatlamini yo’q qiladi[5].

So’rov yuborilganda, so’rovdagi paketlar (ma’lumotlar bloklari) alohida shifrlanadi. Keyin Tor ko’p qatlamli shifrlangan ma’lumotlarni Tor sxemasini tashkil etuvchi xalqaro proksi-serverlarning 3 ta qatlami bo’ylab uzatadi, ular har biri bitta qatlam shifrini ochadi. Tarmoq tugunlarining 3 ta qatlamini quyidagicha:

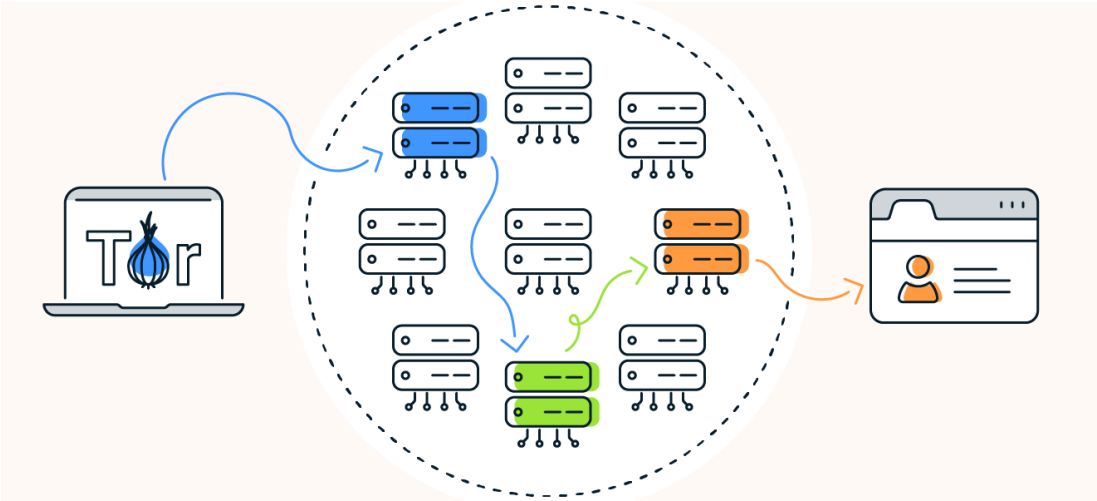
1. Kirish/qo’riqlash tugunlari: Birinchidan, Tor brauzeri hammaga ma’lum bo’lgan kirish tuguniga tasodifiy ulanadi. Kirish tugunlari ma’lumotlarni Tor sxemasiga kiritadi, bu ma’lumotlarni uzatadigan o’rta tugun manzilini ochish uchun shifrlashning birinchi qatlamini parolini hal qiladi.

2. O’rta tugun: Ushbu tugun kirish tugunidan so’rovni oladi. U so’rov kelgan kirish tugunining IP-manzilini biladi, lekin asl so’rov egasining shifrlangan IP-manzilini bilmaydi. O’rta tugun keyingi paketning shifrini ochib, sxemadagi keyingi tugunni ko’rsatadi, ammo so’rovning mazmuni va yakuniy manzili shifrlaydi.

[5] https://www.avast.com/c-tor-dark-web-browser

3. Chiqish tugunlari: Chiqish tugunlari so’rovni qabul qiladi va oxirgi manzilni ko’rsatib, oxirgi paketning shifrini ochadi. Shifrlashning oxirgi qatlami o’chirilgach, shifrlangan ma’lumotlar Tor tarmog‘idan chiqib va oxirgi server manzilga yetib boradi (3-rasm).

Tor brauzer IP-ni yashiradi va foydalanuvchining internetdagi



3-rasm. Tor brauzeri trafikni shifrlash va shifrini ochish uchun kirish tugunlari (ko’k), o’rta tugun (yashil) va chiqish tugunlari (to’q sariq) orqali veb-trafikni yuboradi

faoliyatini kuzatishni qiyinlashtiradi. Joylashuv va identifikatorni yashirish uchun tarmoq tugunlari orqali ma’lumotlarni uzatishdan tashqari, Torning onion marshruti maxfiylikni yanada mustahkam himoya qilish uchun ko‘p qatlamli shifrlashdan foydalanadi. Qisqacha qilib aytganda, darknet internetning yashirin qismi bo’lib, anonimlik va ba’zi hollarda noqonuniy faoliyatlar uchun foydalaniladi. Shu bilan birga, u huquqiy maqsadlarda ham ishlatilishi mumkin, lekin foydalanishda ehtiyotkor bo’lish talab etiladi

KIBERMAKONDA INTELLEKTUAL MULK HUQUQLARINI HIMOYA QILISH

Haydarov Elshod Dilshod o’g‘li
Texnika fanlari bo’yicha falsafa doktori(PhD), Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot xavfsizligi kafedrasi mudiri

Anotatsiya: *ushbu maqolada intelektual mulk tushunchasi, intelektual mulkka bo’lgan huquq, respublikamiz qonunchilik bazasidagi intelektual mulk bilan bog‘liq normalar, kompyuter dasturlari uchun mualliflik huquqi normalari va uni ta’minlash yo’llari, mualliflik huquqini ro’yxatdan o’tkazish tartibi va butunjahon dasturiy ta’minot mualliflik huquqi konvensiyasi va uning asosiy qoidalari tasnifi keltirilgan.*

Kalit so'zlar: *intelektual mulk, O'zbekiston Respublikasi Fuqarolik kodeksi, mualliflik huquqi, kompyuterr dasturi, shaxsiy nomulkiy huquq, ismga bo'lgan huquq, nashr qilish huquqi, milliy rejim.*

Аннотация: *в данной статье рассмотрены понятие интеллектуальной собственности, право интеллектуальной собственности, нормы, связанные с интеллектуальной собственностью в законодательной базе нашей республики, нормы авторского права на программы для ЭВМ и способы его обеспечения, порядок регистрации авторских прав. классификацию Всемирной конвенции об авторском праве на программное обеспечение и ее основные положения.*

Ключевые слова: *интеллектуальная собственность, Гражданский кодекс Республики Узбекистан, авторское право, программа для ЭВМ, право личной собственности, право на имя, право публикации, национальный режим.*

Abstract: *this article examines the concept of intellectual property, intellectual property rights, norms related to intellectual property in the legislative framework of our republic, copyright rules for computer programs and methods of ensuring it, the procedure for registering copyrights. classification of the Universal Copyright Convention on Software and its main provisions.*

Key words: *intellectual property, Civil Code of the Republic of Uzbekistan, copyright, computer program, personal property rights, right to a name, right to publication, national treatment.*

Intellektual mulk huquqiqi insonning ijodiy faoliyati natijalariga bo'lgan huquqdir. Intellektual mulk - ijodiy aqliy faoliyat mahsuli. Ixtirochilik va mualliflik obyekti huquqi majmuiga kiruvchi, fan, adabiyot, san'at va ishlab chiqarish sohasida ijodiy faoliyatning boshqa turlari, adabiy, badiiy, ilmiy asarlar, ijrochi aktyorlik san'ati, jumladan ovoz yozish, radio, televideniye asarlari, kashfiyotlar, ixtirolar, ratsionalizatorlik takliflari, sanoat namunalari, kompyuterlar uchun dasturlar, ma'lumotlar bazasi, nou-xauning ekspert tizimlari, tovar belgilari, firma atamalari va boshqa aqliy mulk obyektlariga kiradi.

O'zbekiston Respublikasi Fuqarolik Kodeksida (164-modda) mulk huquqi deganda shaxsning o'ziga qarashli mol-mulkka o'z xohishi bilan va o'z manfaatlarini ko'zlab egalik qilish, undan foydalanish va uni tasarruf etish, shuningdek o'zining mulk huquqini, kim tomonidan bo'lmasin, har qanday buzishni bartaraf etishni talab qilish huquqidan iboratdir. Mulk huquqi muddatsiz ekanligi belgilab qo'yilgan.

Mulk huquqi shakllaridan biri bu Intellektual mulk obyektlari hisoblanib fuqarolar bunga egalik qilishi mumkin (O'zbekiston Respublikasi Fuqarolik kodeksining 169-moddasi). Bularga quyidagilar kiradi:

1) intellektual faoliyat natijalari:

- fan, adabiyot va san'at asarlari;

- eshittirish yoki kabel orqali eshittirish tashkilotlarining chiqishlari, fonogrammalari, eshittirishlari;
- elektron kompyuterlar va ma’lumotlar bazalari uchun dasturlar (keyingi o’rinlarda kompyuterlar deb yuritiladi);
- ixtirolar, foydali modellar, sanoat namunalari;
- naslchilik yutuqlar;
- oshkor etilmagan ma’lumotlar, shu jumladan tijorat sirlari (nou-xau);

2) fuqarolik bitimlari, tovarlar, ishlar va xizmatlar ishtirokchilarini individuallashtirish vositalari:
- markali ismlar;
- tovar belgilar (belgilar xizmat);
- ismlar joylar kelib chiqishi tovarlar;

3) ushbu Kodeksda yoki boshqa qonunlarda nazarda tutilgan hollarda intellektual faoliyatning boshqa natijalari va fuqarolik muomalasi ishtirokchilarini, tovarlar, ishlar va xizmatlarni individuallashtirish vositalari. (O’zbekiston Respublikasi Fuqarolik kodeksining 1031-moddasi):

Tarixiy jihatdan intellektual mulk ikkita asosiy toifani o’z ichiga olgan. Bu mualliflik huquqi va sanoat mulki.

Mualliflik huquqi milliy va xalqaro miqyosda maxsus qonunlar bilan himoyalangan. O’zbekiston Respublikasida zamonaviy mualliflik huquqi qonunchiligi mavjud.

O‘zbekiston Respublikasining mualliflik huquqi to‘g‘risidagi qonun hujjatlari O‘zbekiston Respublikasi Konstitutsiyasi, O‘zbekiston Respublikasining Fuqarolik kodeksi, “Mualliflik huquqi va turdosh huquqlar to‘g‘risida”gi qonun, Prezident farmon va farmonlari hamda boshqa hujjatlar qoidalaridan iborat.

Quyida dasturiy ta’minot ishlab chiqaruvchilari uchun kompyuter dasturlariga nisbatan qo’llaniladigan mualliflik huquqi to’g‘risidagi qonun hujjatlarining eng muhim qoidalarini keltirib o’tilgan.

Mualliflik huquqi qonunining asosiy qoidalari. Kompyuter dasturlari O’zbekiston Respublikasining “Mualliflik huquqi va turdosh huquqlar to’g‘risida”gi qonuni bilan mualliflik huquqi obyektlari sifatida tasniflanadi. Qonunda kompyuter dasturi deganda “kompyuter yordamida ma’lum natijani olish uchun moddiy tashuvchida qayd etilgan, shuningdek, elektron hujjatlarga ilova qilinadigan buyruqlar va ma’lumotlarning tartiblangan to’plami” tushuniladi. “Kompyuter dasturlari adabiy asarlar sifatida himoyalanadi va bunday himoya har qanday tilda va har qanday shaklda, shu jumladan dastlabki matn va

obyekt kodida ifodalanishi mumkin bo'lgan amaliy dasturlar va operatsion tizimlarni o'z ichiga olgan barcha turdagi dasturlarga taalluqlidir".

Kompyuter dasturiga mualliflik huquqi uning yaratilganligi sababli yuzaga keladi va "mualliflik huquqining paydo bo'lishi va amalga oshirilishi uchun hech qanday rasmiyatchilik talab etilmaydi".

Bu yerda ishlab chiquvchilar kompyuter dasturida mualliflik huquqini tan olish va amalga oshirish uchun qonun dasturlarni majburiy ro'yxatdan o'tkazishni talab qilmasligiga e'tibor berishlari kerak.

Kompyuter dasturining muallifi - uni ijodiy ishi yaratgan shaxs.

Mualliflik huquqi, ism huquqi va muallifning obro'sini himoya qilish huquqi cheksiz himoya qilinadi. Mulk huquqi muallifning butun hayoti davomida va vafotidan keyin 50 yil davomida amal qiladi. Anonim asarga yoki taxallus ostidagi asarga nisbatan himoya qilish muddati asar birinchi marta qonuniy nashr etilgan kundan boshlab 50 yilni tashkil etadi.

Dastur ishlab chiquvchilari shuni bilishlari kerakki, berilgan himoya kompyuter dasturi asosidagi g'oyalar va tamoyillarga taalluqli emas. Xususan, ushbu himoya dasturning ishlash usullariga taalluqli emas. Binobarin, algoritmga kiritilgan g'oya emas, balki faqat ushbu algoritmni operatorlar ketma-ketligi va ushbu operatorlar bo'yicha harakatlar ko'rinishidagi o'ziga xos amalga oshirish qonun bilan himoyalangan.

Shunday qilib, ishlab chiquvchi, birinchi navbatda, ushbu o'ziga xos shaklni - dasturning manba matnini va/yoki obyekt kodini himoya qilishi kerak.

Qonunda huquqlarni boshqarish to'g'risidagi axborot tushunchasi aniqlanganini alohida ta'kidlash lozim. "Huquqlar to'g'risidagi ma'lumotlar – muallifni, asarni... yoki asardan foydalanish shartlari haqidagi ma'lumotni, shuningdek, ushbu ma'lumotlardan birortasi hujjatga ilova qilinganida bunday ma'lumotlar taqdim etilgan har qanday raqamlar yoki kodlar haqidagi ma'lumotlardir. asarning nusxasi...". Mualliflik huquqi egasining ruxsatisiz har qanday elektron huquqlarni boshqarish ma'lumotlarini yo'q qilish yoki o'zgartirish mualliflik huquqining buzilishi hisoblanadi.

O'zlarining mutlaq mulkiy huquqlari to'g'risida xabardor qilish uchun ularning egasi asarning har bir nusxasiga joylashtirilgan va uchta elementdan iborat bo'lishi kerak bo'lgan mualliflik huquqini himoya qilish belgisidan foydalanishga haqlidir:

1. Lotin harfi "C" doira ichida: ©;
2. Mutlaq mulk huquqi egasining nomi;
3. Asarning birinchi nashr etilgan yili [11-modda].

Mualliflik huquqining o’ziga xos xususiyati uning qat’iy hududiy xususiyatidir, ya’ni, dasturga bo’lgan huquq doirasi ushbu huquq paydo bo’lgan davlat hududi bilan belgilanadi va ushbu davlat chegaralari bilan cheklanadi. Boshqa davlatda xalqaro shartnoma bo’lmaganda bu huquq tan olinmaydi. Kompyuter dasturlari boshqa davlatlarda himoyalanishi uchun bu davlatlar yo o‘zaro mualliflik huquqlarini tan olish va himoya qilish to‘g‘risida shartnomalar tuzishlari yoki xalqaro mualliflik huquqi hujjatlarining ishtirokchilari bo‘lishlari zarur.

O’zbekiston Respublikasining xalqaro shartnomalariga muvofiq asarga O’zbekiston Respublikasi hududida himoya berilganda, asarga mualliflik huquqining egasi uning hududida harakat yoki hodisa sodir bo’lgan davlatning qonun hujjatlari bilan belgilanadi.

Kompyuter dasturlari uchun mualliflik huquqi. Kompyuter dasturlari mualliflarining huquqlari shaxsiy nomulkiy va mulkiy huquqlarga bo’linadi. Shuni ta’kidlash kerakki, shaxsiy nomulkiy huquqlar uning mulkiy huquqlaridan qat'i nazar, muallifga tegishlidir.

Dastur muallifiga tegishli shaxsiy nomulkiy huquqlarga quyidagilar kiradi:

1. Mualliflik huquqi – ya’ni asar muallifi deb tan olinish huquqi.

“Mualliflik huquqi va turdosh huquqlar to’g‘risida”gi Qonunning 9-moddasida aksini tasdiqlovchi dalillar bo’lmasa, asarning asl nusxasida yoki nusxasida muallif sifatida ko’rsatilgan shaxs asar muallifi hisoblanadi (mualliflik huquqi prezumpsiyasi). Va agar ma’lum bir kompyuter dasturiga nisbatan shaxsning muallifligi haqida shubha tug‘ilsa, bu shubhalar faqat sud tomonidan hal qilinishi mumkin.

2. Ismga bo’lgan huquq - ya’ni “asardan muallifning haqiqiy ismi, taxallusi ostida yoki nomini ko’rsatmasdan, ya’ni anonim ravishda foydalanish yoki undan foydalanishga ruxsat berish huquqi”.

E’tibor bering, agar kompyuter dasturida muallifning ismi ko’rsatilmagan bo’lsa, dasturiy mahsulotda nomi ko’rsatilgan tashkilot, agar buning aksini tasdiqlovchi dalillar bo’lmasa, muallifning vakili hisoblanadi va shu maqomda muallifning huquqlarini himoya qilish, shuningdek ularning amalga oshirilishini ta’minlash mumkin.

3. Obro’-e’tiborni himoya qilish huquqi - ya’ni “asarni, shu jumladan uning nomini ham muallifning sha’ni va qadr-qimmatiga putur yetkazishi mumkin bo’lgan har qanday buzish yoki boshqa hujumlardan himoya qilish huquqi”.

Kompyuter dasturlariga nisbatan ushbu huquq ushbu asarlar uchun muallifga ma’lum bo’lmagan holda, ularning funksional xususiyatlari va xususiyatlariga ta’sir ko’rsatishi mumkin bo’lgan bunday o’zgartirishlar

va tushuntirishlarni kiritish eng katta ahamiyatga ega ekanligini ko'rsatadi. Dastur muallifining sha'ni va qadr-qimmatiga zarar yetkazish boshqa shaxslarning ruxsatsiz aralashuvi natijasida yuzaga kelishi mumkin.

4. Nashr qilish huquqi - ya'ni asarni istalgan shaklda nashr etish yoki nashr etishga ruxsat berish huquqi.

Kompyuter dasturi muallifining mulkiy huquqlari bir qator harakatlarni amalga oshirish yoki amalga oshirishga ruxsat berishning mutlaq huquqiga qisqartiriladi:

a) Qayta ishlab chiqarish, ya'ni asarning bir yoki bir nechta nusxasini istalgan moddiy shaklda tayyorlash, shu jumladan elektron tashuvchida raqamli shaklda doimiy yoki vaqtincha saqlash;

b) Yoyish - original yoki nusxalari sotish yoki mulkni boshqa o'tkazish yo'li bilan ishlaydi;

c) Ijara asarlarning asl nusxasi yoki nusxalariga egalik huquqidan qat'i nazar, kompyuter dasturlarining asl nusxalari yoki nusxalari. E'tibor bering, ushbu huquq kompyuter dasturlariga taalluqli emas, agar dasturning o'zi ijaraning asosiy elementi bo'lmasa,

d) Tarjima boshqa tilda ishlaydi,

e) O'zgartirish yoki boshqa ishlov berish dasturlar va boshqalar.

Kompyuter dasturiga mualliflik huquqini ro'yxatdan o'tkazish uni mualliflik huquqi obyekti sifatida ro'yxatdan o'tkazish uchun ariza berish orqali amalga oshiriladi.

Kompyuter dasturiga mualliflik huquqini ro'yxatdan o'tkazish uchun hujjatlar:

- Vakolatnoma;
- Kompyuter dasturining dastlabki matni (manba matnining bo'laklari) uni identifikatsiya qilish uchun zarur bo'lgan darajada. Ariza beruvchi kompyuter dasturining dastlabki matnining qaysi qismlarini saqlash uchun topshirishni mustaqil ravishda hal qiladi va taqdim etilgan manba matn qismlaridan, uning fikricha, qamrab olinmasligi kerak bo'lgan joylarni olib tashlashga haqli;
- Kompyuter dasturidan foydalanish bo'yicha qo'llanma (ko'rsatmalar);
- EHM dasturi yaratilgan fakt va sanani ko'rsatishi mumkin bo'lgan hujjatlar;
- Muallifning (agar ariza muallifning merosxo'ri tomonidan taqdim etilgan bo'lsa) kompyuter dasturiga bo'lgan mulk huquqi meros bo'yicha o'tkazilganligini tasdiqlovchi hujjat.

Butunjahon dasturiy ta’minot mualliflik huquqi konvensiyasi va uning asosiy qoidalari. Bir asrdan ortiq tarixga ega Bern konvensiyasidan farqli ravishda Jahon konvensiyasi ancha kechroq, 1952-yil 6-sentyabrda imzolangan. Ushbu xalqaro shartnomani imzolashdan asosiy maqsad Qo’shma Shtatlar va G‘arbiy yarim sharning boshqa bir qator mamlakatlarini mualliflik huquqini himoya qilish bo’yicha global hamjamiyatga jalb qilish edi. Yuqorida ta’kidlab o’tilganidek, AQSh mualliflik huquqi qonuni barcha rasmiyatchiliklari bilan (ro’yxatga olish talabi, mualliflik huquqi xabarnoma va boshqalar) Bern konvensiyasi tamoyillariga mos kelmas edi. Shunday qilib, Umumjahon konventsiya o’ziga xos kelishuv bitimi bo’lib chiqdi, unga ko’ra Qo’shma Shtatlar ko’plab davlatlar bilan xalqaro mualliflik huquqi munosabatlariga kirdi (ularning aksariyati hali ham Bern klubi a’zolari bo’lib qoldi), shu bilan birga ushbu shartnoma ishtirokchilaridan shartnoma tuzish shart emas edi. 1973-yilda Sovet Ittifoqi Jahon konvensiyasiga qo’shildi.

So’nggi o’n yil ichida Jahon konvensiyasi Bern konventsiyasi soyasiga yanada uzoqlashdi, uning maqomi ushbu xalqaro shartnoma ishtirokchilari doirasining sezilarli darajada kengayishi tufayli sezilarli darajada oshdi. Bern klubining yangi a’zolari qatoriga AQSH (1989-yilda), Xitoy (1992-yilda) va nihoyat, Rossiya Federatsiyasi (1995-yilda) kabi davlatlar kirdi. Shu bilan birga, Jahon konvensiyasi mualliflik huquqi sohasidagi eng muhim xalqaro shartnomalar ro’yxatida o’zining “ikkinchi” mavqeini qat’iy saqlab qolgan holda, mustaqil ahamiyatga ega bo’lishda davom etmoqda. Xususan, Jahon konvensiyasi 2005-yil 19-apreldan boshlab O’zbekiston hududida chop etilgan, Jahon konvensiyasi ishtirokchisi bo’lgan xorijiy davlatlarda chop etilgan asarlarni xalqaro himoya qiladi. Jahon konvensiyasiga AQSHdan tashqari dunyoning deyarli barcha rivojlangan davlatlari a’zo.

Ikkala konvensiya ham ruhan, ham mazmunan bir-biriga juda yaqin. Bern konvensiyasida bo’lgani kabi, xorijlik mualliflarga nisbatan kamsitmaslik tamoyili ham Umumjahon konvensiyasining markaziy elementi hisoblanadi. Umuman olganda, Bern konvensiyasi mualliflar uchun qulayroqdir, chunki ushbu konvensiya xorijiy mualliflarning asarlariga nisbatan har qanday rasmiyatchiliklarni kiritishni butunlay rad etadi. Umumjahon Konvensiya mualliflik huquqi to’g‘risidagi bildirishnomadan foydalanish, hatto boshqa turli rasmiyatchiliklar mavjud bo’lgan mamlakatlarda ham (masalan, Qo’shma Shtatlarda ro’yxatdan o’tish) mualliflik huquqi uchun zarur va shu bilan birga yetarli shart ekanligini ta’minlaydi.

Shunday qilib, hozirgi vaqtda kompyuter dasturlari mualliflari huquqlarini himoya qilish uchun yetarli huquqiy baza yaratilgan.

Umumjahon mualliflik huquqi konvensiyasining asosiy qoidalari. Konvensiyaning muqaddimasi, ya'ni uning kirish qismi ushbu xalqaro shartnomani tuzish maqsadlarini belgilash uchun mo'ljallangan uchta asosiy qoidani ifodalaydi. Birinchidan, unda ishtirokchi davlatlarning barcha mamlakatlarda adabiy, ilmiy va san'at asarlariga mualliflik huquqi himoyasini ta'minlash istagi bildirilgan. Ikkinchidan, konvensiyada ko'zda tutilgan mualliflik huquqini himoya qilish rejimi shaxs huquqlariga hurmatni ta'minlashga, adabiyot, fan va san'at rivojiga ko'maklashishga qodir ekanligi qayd etilgan. Uchinchidan, mualliflik huquqining bunday universal rejimi ma'naviy asarlarning tarqalishini osonlashtirishi va xalqaro tushunishni yaxshilashga yordam berishi ta'kidlangan.

Konvensiyaning asosiy qoidalarini va unga asoslangan tamoyillarnining ayrimlari quyida keltirilgan.

Milliy rejim. Konvensiyaning asosiy prinsipi milliy rejim deb ataladigan tamoyildir. Milliy rejim prinsipi (yoki assimilyatsiya qilish prinsipi) tufayli xalqaro huquq xorijiy fuqarolar, tashkilotlar va firmalarga mahalliy fuqarolar, tashkilotlar va firmalarga qanday rejim taqdim etilgan bo'lsa, shunday holatni mustahkamlaydi. Biz ko'rib chiqayotgan konvensiyada milliy muomala tamoyili San'atda mustahkamlangan. Xorijda nashr etilgan asar Konvensiyaga a'zo bo'lgan har bir mamlakatda o'z fuqarolarining o'z hududida birinchi marta nashr etilgan asarlariga ushbu davlat tomonidan taqdim etilgan himoyadan foydalanadi.

Milliy rejim prinsipi tufayli, konvensiyada aniq ko'rsatilgan qoidalar bundan mustasno va bunday qoidalar kam bo'lsa, himoyalangan asarga nisbatan munosabat milliy qonunchilik bilan belgilanadi. Bu shuni anglatadiki, tegishli xorijiy mualliflarga mahalliy mualliflar bilan bir xil shaxsiy va mulkiy huquqlar beriladi.

Xulosa sifatida shuni ta'kidlash mumkinki, hozirgi kunda respublikamizda va jahonda nualliflik huquqlarini himoyalash bo'yicha ko'plab normativ-huquqqiy hujjatlar yaratilgan, ushbu hujjatlar fuqarolarning intelektual mulklari himoyasini mustahkamlashda xizmat ko'rsatadi. Bu huquqlarning buzilishi qonuniy javobgarlikka tortilishiga sabab bo'ladi.

STRENGTHENING ACADEMIC PRIORITY STANDARDS AS AN INSTRUMENT TO AGAINST CORRUPTION IN THE FIELD OF SCIENTIFIC AND EDUCATION

ISMAILOV BAHODIR ISLAMOVICH
Doctor of Science, professor, Head of the department Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan

RASULOVA GULBAHOR ABIDJANOVNA
Basic doctoral student of Law Enforcement
Academy of the Republic of Uzbekistan

The rapid development of science and the increasing prestige of scientific activity in modern society are largely due to its focus on acquiring scientific knowledge that significantly influences the solution of practical tasks in various fields of activity.

The pronounced pragmatism and utilitarianism of most scientific research, its constantly increasing prestige, and connection with scientists' career prospects and material considerations have inevitably led to an exacerbation of the problem of academic integrity and an increase in violations of basic ethical principles in education and scientific research.

In recent years, the topic of academic integrity has become one of the main subjects in discussions about higher education and science, regardless of the level at which or by whom such discussions are conducted. Politicians and scientists, public activists and students are just a partial list of those who raise this issue to some extent[1].

Unfortunately, experts believe that plagiarism, fraud, and corruption in the education system and scientific environment have reached unprecedented levels worldwide[2].

This threatens the quality of education, the prospects for scientific development, and the professionalism of graduates.

For example, if we consider only the prevalence of plagiarism (in its various forms) among students, researchers, and postgraduate students, it depends on the methodology used to study this issue. Many researchers employ the so-called self-reporting methodology, i.e., internal university control of scientific works for plagiarism.

[1] Мельник Р. О борьбе за академическую добропорядочность// https://ru.osvita.ua/vnz/74950/

[2] Smaldino P, McElreach R. The natural selection of bad science. Royal society open sci. 2016; Sept 21. DOI: 10.1098/rsos.160384., Muller R. Postdoctoral life scientists and supervision work in contemporary university: A case study of changes in cultural norms of science. Minerva. 2014;52(3):329-349., Park R. Fraud in science 11 Social research: An international quarterly. Baltimore, 2008;75(4):1135-1150.

Using this methodology, researchers obtained completely different data on the prevalence of plagiarism in scientific works of students from the USA, Australia, and several Western European countries. According to the results of McCabe et al.'s research, 19% of the diploma papers of students at a technological university contained plagiarism[3].

D.Pecorari, in his observation, clearly demonstrated that 76% of American university graduates for whom English is not their native language incorrectly borrow up to 70% of the source text when writing their final essay, i.e., they quote authors of various works without providing references to them[4].

It is no coincidence that UNESCO's Roadmap for the Development of Higher Education until 2030 lists honesty and ethics as one of its key principles[5]. According to this principle, universities should pay great attention to ethical values in order to promote the development of integrity, tolerance, and solidarity in society[6].

The Singapore Statement "On Research Integrity" from the World Conference on Research Integrity (Singapore, July 22-24, 2010) emphasizes that "The value and benefits of research entirely depend on how responsibly it is conducted. While differences in the organization and conduct of research, determined by national and disciplinary contexts, are possible and encountered in practice, certain principles and professional obligations are fundamental to research integrity, regardless of where it is conducted[7]".

As can be seen, issues of ensuring academic integrity are indicated as the most important components of modern, high-quality, and competitive higher education.

Despite different approaches to terminology (terms used include academic integrity, conscientiousness, honesty, etc.), the common understanding is that academic integrity encompasses a set of moral values such as honesty, fairness, trust, respect, and responsibility, as well as ideals that all participants in the scientific and educational process must uphold.

From a legal perspective, experts and specialists believe that academic integrity includes a set of principles and values that guide

[3] McCabe D. L., Feghali T., Abdallah H. 2008. Academic Dishonesty in the Middle East: Individual and Contextual Factors. Research in Higher Education. 49 (5): 451–467.

[4] D. Pecorari, Academic writing and plagiarism: a linguistic analysis September 2010Australian Review of Applied Linguistics 33(2):23.1-23.4

[5]https://cdn.eventscase.com/www.whec2022.org/uploads/users/699058/uploads/69c2df623079c3845e236c56ba2d7a8aa21b3d75489e28c7910226f24f7989aec7aae05a23f31fae4587aeb4be088f99dccd.6282b2a95281d.pdf

[6] Приняты на Всемирной конференции ЮНЕСКО по высшему образованию 2022 года, которая проходила 18–20 мая в Барселоне (Испания).

[7] https://repository.globethics.net/handle/20.500.12424/209905

students, teachers, and educational institutions in the process of learning and scientific activity. It includes adherence to honesty, ethical behavior, and respect for intellectual property[8].

The issues of ensuring academic integrity and overcoming corrupt practices that harm it, among which plagiarism is probably the most widespread, fall within the competence of law and relevant legal procedures. Given this, the legal regulation of processes to promote academic integrity is of paramount importance and significance.

Experts believe that the most common types of violations of academic integrity are actions that undermine the principles of honesty and intellectual integrity in the academic sphere. These include:

Plagiarism - one of the most common violations, which involves presenting someone else's work or idea as one's own without proper attribution or acknowledgment of authorship.

Collusion - implies unauthorized cooperation or joint work by individuals on assignments meant to be completed independently. Improper use of artificial intelligence language services such as ChatGPT, Copilot, etc. for writing academic papers, manifested in unauthorized automated writing of scientific works, compilation of texts, etc.

Favoritism - manifested in the form of informal support for individual employees or teachers based on acquaintance, kinship, patronage, etc.

Cheating - a widespread violation that occurs when unauthorized resources are used, as well as when external assistance is provided to students during exams.

Fabrication - refers to the falsification or invention of data, sources, or information, distorting the truth and misleading others.

Informal relations in the scientific and educational spheres - manifested in cliquishness, localism, cronyism, and nepotism.

Forced co-authorship - manifests itself in the form of including co-authors or co-performers in publications or research “recommended by leadership”, coercing subordinates to write scientific or research papers, etc.

Providing positive expert assessments, conclusions, and recommendations for compensation - manifested in ignoring principles

[8] Segerstrale U. The mark border land between scientific intuition and fraud. J. appl. Philosophy. N.Y., 1990;5(1):11-20.

of fairness, falsifying research data, and granting exclusive rights and powers[9].

Bribery in scientific research manifests itself in the form of graft when obtaining research grants, acts of implementing scientific results in practice, etc.

Fraud in examinations or final assessments manifests itself in the form of leaking exam questions, test tasks, substitution of test assignments, alteration of attestation commission protocols, etc.

Extortion manifests itself in the form of giving positive grades in exams, competitions, nominations, defenses of scientific works, reports on grant implementation, etc[10].

Commercialization of scientific activity includes writing scientific works for payment, giving gifts to scientific supervisors, experts, reviewers, opponents, etc.

These various types of academic integrity violations undermine the principles of fairness, authenticity, and personal responsibility, which are fundamental to the pursuit of knowledge and intellectual growth.

Experts point out the following benefits of ensuring academic integrity:

it fosters a culture of trust, fairness, and respect among students and teachers;

encourages critical thinking, creative approach and originality in the educational work;

minimizes the risks of corruption and informal relations between officials and employees of educational and scientific institutions;

contributes to personal growth, moral development and moral thinking;

promotes the creation of a favorable learning environment that contributes to cooperation and knowledge exchange;

strengthens the trust and reputation of individuals and institutions;

prepares students for making ethical decisions in their future professional careers, etc.

---

[9] Kisamore J., Stone T., Jawahar I. 2007. Academic Integrity: The Relationship between Individual and Situational Factors on Misconduct Contemplations. Journal of Business Ethics. 75: 381–394., Kuntz J. R., Butler C. 2014. Exploring Individual and Contextual Antecedents of Attitudes Toward the Acceptability of Cheating and Plagiarism. Ethics & Behavior. 24 (6): 478–494., Magnus J. et al. 2002. Tolerance of Cheating: an Analysis a Countries. Journal of Economic Education. 33 (2): 125–135, Marsden H., Carroll M., Neill J. T. 2005. Who Cheats at University? A Self-Report Study of Dishonest Academic Behaviours in a Sample of Australian University Students. Australian Journal of Psychology. 57 (1): 1–10.

[10] Аббадия Д. Столпы академической честности: Определение, преимущества и стратегии//https://mindthegraph.com/blog/ru/academic-integrity/ academicintegrity.org [Internet]. International Center for Academic Integrity, Fundamental Values Project [cited 2017 Jul 9]. Available from: http://www.academicintegrity.org/icai/resources-2.php.

Experts and specialists indicate as problems of achieving academic honesty:

strengthening the requirements for academic performance and competition among students;

the availability of online resources that can contribute to plagiarism and write-off;

cultural differences and different understandings of academic ethics;

limited awareness and understanding of policies and expectations regarding academic integrity;

the need for constant monitoring and updating of policies and preventive measures;

different views on academic honesty and others[11].

Accordingly, to minimize these problems at the international and national levels, the legal framework in this area began to be formed.

The issue of ensuring academic integrity in OECD countries emerged in the 1990s. Ukraine was a pioneer in this field among the post-Soviet countries. The term "academic integrity" appeared in the legislation of Ukraine on education and higher education on September 5, 2017, as a result of the adoption of the new edition of the Law of Ukraine "On Education" and amendments to the Law of Ukraine "On Higher Education"[12].

The National Agency for Quality Assurance of Higher Education of Ukraine was defined as the central body authorized at the state level to combat violations of academic integrity, to cancel the decisions of the dissertation councils on the award of academic degrees.

In accordance with the Resolution of the Cabinet of Ministers of Ukraine dated April 15, 2015 No. 244 (with subsequent amendments and additions), the National Agency is authorized to apply such measures of academic responsibility as:

refusal to grant a scientific degree or a scientific title;

deprivation of the awarded scientific (educational-creative) degree or the awarded scientific title;

refusal to grant or deprive a pedagogical title, qualification category;

deprivation of the right to participate in the work of lawful bodies or to hold lawful positions[13].

[11] Josien L., Broderick B. 2013. Cheating in Higher Education: the Case of Multi-Methods Cheaters. Academy of Educational Leadership Journal. 17 (3): 93–105.

[12] https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF#Text

[13] https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF#Text

The sanctions (punishments) introduced by the Law of Ukraine "On Education" that can be applied to violators of academic integrity marked the "birth" of a new type of legal responsibility - academic responsibility. This, in turn, means that during its implementation, all requirements and standards that accompany the application of other types of legal responsibility, primarily criminal, administrative, or disciplinary, must be observed.

In foreign practice, strategies for promoting academic honesty involve a number of measures, among which the most important are:

development of academic integrity codes;

involvement of the academic community, students, researchers, and parents;

demonstration of appropriate academic conduct and ethical norms;

conducting anti-corruption training and trainings on compliance with academic integrity codes;

training in proper citation, referencing, collaboration, and use of external sources;

providing detailed instructions on assignments, exams, and projects to avoid ambiguity and ensure students understand the parameters of academic integrity;

developing a culture of respect and trust among students and teachers;

maintaining open and inclusive communication channels between students and teachers;

creating mentoring programs or peer support networks to facilitate positive interaction and mutual support;

implementing online proctoring or plagiarism detection software to prevent and identify cases of cheating or plagiarism;

promoting group discussions and debates that foster critical thinking and the study of ethical issues, etc[14].

Disciplinary sanctions for violating academic integrity depend on the educational institution's policy and may include:

Reprimands: official warnings to faculty about inappropriate conduct.

[14] Mayhew M. J. et al. 2009. Using Structural Equation Modeling to Validate the Theory of Planned Behavior as a Model for Predicting Student Cheating. Review of Higher Education. 32 (4): 441–468., McCabe D. L., Butterfield K. D., Trevino L. K. 2006. Academic Dishonesty in Graduate Business Programs: Prevalence, Causes, and Proposed Action. Academy of Management Learning & Education. 5 (3):294–305., Ogilvie J., Stewart A. 2010. The Integration of Rational Choice and Self-Efficacy Theories: A Situational Analysis of Student Misconduct. The Australian and New Zealand Journal of Criminology. 43 (1):
130–155.

Oral or written warnings: issued for minor violations or first-time offenses.

Academic penalties: may include lowering grades, reassigning work, or failing a course.

Disciplinary probation: placing a student on probation for a certain period, during which any further violation may result in more serious consequences.

Suspension: temporary removal of a student from academic classes and courses for a specified period.

Expulsion: permanent removal of a student from the educational institution due to repeated or serious violations.

On June 6, 2024, the Verkhovna Rada adopted the draft **Law No. 10392 "On Academic Integrity"** in the first reading[15].

The developers note that the adoption of the Law will be a historic step, as it has no analogues in any European country. The law will provide an opportunity to raise the level of culture to a higher standard, corresponding to European norms, in all educational and scientific institutions, to affirm the values of academic integrity both in the academic environment and in society as a whole[16].

The Law "On Academic Integrity" is designed to:

ensure legal certainty regarding the content of academic integrity, revealing it through specific basic values defined by the global academic community: honesty, trust, respect, fairness, responsibility, perseverance, and decisiveness;

determine the basic principles and fundamental rules of academic integrity that all participants in the educational process at all levels of education, all scientists in the implementation of scientific activities, as well as applicants must adhere to;

outline the main ways to ensure academic integrity;

determine the content and main types of violations of academic integrity, the content and main issues of academic responsibility, including the main types of sanctions for such violations;

regulate the main procedures for responding to the violation of academic integrity, determining the features of responding to the violation of academic integrity by the education recipient, the features of attracting the heads of educational institutions, scientific institutions to academic

[15] https://jurliga.ligazakon.net/ru/news/228295_akademicheskaya-dobroporyadochnost-zakonoproekt-proshel-pervoe-chtenie,

[16] https://ips.ligazakon.net/document/JI10516I?utm_source=jurliga.ligazakon.net&utm_medium=news&utm_content=jl03&_ga=2.23941308.785533876.1728713498-898253240.1728713498#_gl=1*bxq8ur*_gcl_au*NjQ5NDA2MDMwLjE3Mjg3MTM0OTg.

responsibility and the features and consequences of deprivation of the awarded academic degree, higher education degree or the awarded academic title;

envisage amendments to other laws in the concluding and transitional provisions of the draft Law for the systematic and balanced introduction of academic integrity at all levels of education, in scientific activity, etc[17].;

clearly define the issue of protecting academic integrity and the issue of protecting copyright and related rights (they have different objects of protection and these are different public relations);

terminate the practice of writing educational and scientific works on demand, including with appropriate advertising, etc.

Ukrainian experts believe that the formation of a culture of academic integrity in educational institutions should lead to:

1) increasing students' confidence in learning outcomes;

2) Improve the quality of education received (educators should learn to write themselves, respecting copyright and the work of others, and provide their own learning outcomes for evaluation, not the learning outcomes and intellectual work of classmates/groupmates);

3) Increasing the quality and honesty of scientific research (those who are able to write and write scientific works should write them under their own name, and those who are not able and do not write should engage in another socially useful work);

4) Improving the integrity of citizens (graduates of schools and universities) in public life: in public service, in courts, law enforcement agencies, in business, etc.

Based on this, we believe that the adoption of a similar law in the Republic of Uzbekistan is highly demanded, as strengthening academic integrity standards is an important tool for combating corruption in the scientific and educational sphere.

In conclusion, it should be noted that combating academic malpractice should become one of the priority areas of state policy in the field of science and education. However, in such a struggle, the rights, freedoms and legitimate interests of scientists should be put first, for some reason (including the envy of colleagues) various non-formal illegal relations may be “involved”. It is clear that both scientists and the state need transparent, clear and understandable procedures in this area, because without this, scientists will lose faith in the state, and the state, as a result, will lose its scientific potential.

[17] Политика академической честности: опыт университетов США// https://kpi.ua/ru/code-info

ОСОБЕННОСТИ ПРЕСТУПЛЕННИЙ, СОВЕРШЕННЫХ В КИБЕРПРОСТРАНСТВЕ

Сабырбаева Айнура Бахыт кызы
Доцент кафедры уголовно-процессуального права Академии МВД, д.ф.ю.н. (PhD), доцент
a_sabyrbaeva@inbox.ru
+99877-007-75-67

Аннотация: *в статье рассматривается понятие преступлений, совершенных в киберпространстве, а также описаны специфическое характеристики данных видов киберпреступлений. В ходе изучения судебно-следственной практики были выявлены некоторые присущие им особенности, на которые необходимо обратить внимание при противодействии киберпреступности.*

Ключевые слова: *киберпреступность, киберпространство, латентность, дроп, дроповод, информационное технологии.*

Annotation: *the article discusses the concept of crimes committed in cyberspace, and describes the specific characteristics of these types of cybercrimes. During the study of judicial and investigative practice, some inherent features were identified that need to be paid attention to when countering cybercrime.*

Keywords: *cybercrime, cyberspace, latency, drop, drop guide, information technology.*

Аннотация: *мақолада кибермаконда содир этилган жиноятлар тушунчаси кўриб чиқилган, шунингдек, ушбу турдаги кибержиноятларнинг ўзига хос хусусиятлари тавсифланган. Суд-тергов амалиётини ўрганиш жараёнида кибержиноятчиликка қарши курашда эътибор қаратиш лозим бўлган айрим ўзига хос хусусиятлар аниқланган.*

Калит сўзлар: *кибержиноят, кибермакон, латент жиноят, дроп, дроповод, ахборот технологиялари.*

XXI век не зря именуется веком цифровых технологий, искусственного интеллекта, ведь современный человек уже не может обойтись без современных технологий (телефоны, Интернет, социальные сети и так далее). И даже маленький ребенок с детства познает этот мир сквозь призму телефона. Киберпространство, являясь одним из ответвлений информационно-коммуникационных технологий, на протяжении всего нескольких десятков лет стало частью жизни каждого человека и предоставило массу возможностей как для рядового обывателя, так и для стран в целом, в том числе и в вооружении армий. Можно увидеть, к примеру использование дистанционно управляемых самолетов, дронов в любую точку мира для сбора разведывательных данных и даже

нападения. Однако, помимо положительных аспектов, которые дает нам цифровизация общества, она также несет в себе опасности, как например преступления в киберпространстве либо его использование в противоправных целях.

Примечательно, что появление словосочетания «кибернетическое пространство» связано далеко не с наукой, впервые этот термин употребил в 1982 г. Уильям Гибсон в своем научно-фантастическом произведении[178]. Под киберпространством У. Гибсоном понималась виртуальная среда, существующая внутри компьютерных сетей, с которой может взаимодействовать человек[179].

Как отметил международный эксперт по гармонизации законодательства в сфере киберпреступности Штайн Шольберг, «киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых правовых мер на международном уровне»[180]. Британский журнал «The Economist» пишет о кибепространстве как о «пятой потенциальной зоне ведения войны после суши, моря, воздуха и космоса»[181].

Как справедливо отметил Лебедев В.Н. «Компьютерные технологии внедряются для изменения и повышения эффективности творческих и рабочих процессов во всех аспектах жизни, и мир преступности больше не является исключением»[182].

Умение преступников подстраиваться под современные условия (будь то технологии, законы или лазейки в них) поражает. Так, буквально в начале тысячелетия такие понятия как искусственный интеллект, цифровая валюта были за гранью фантастики. Однако, распространение Интернета, внедрение в банковские системы возможность осуществления онлайн транзакций, находясь в любой точке мира, привлекли внимание целого пласта преступников, которые уже получили название «киберпреступники».

---

[178] *Henthorne T. William Gibson:* A Literary Companion. Jefferson: McFarland & Company, 2011. 176 p

[179] *Киселев А.С., Горбунова К.А.* Особенности криминалистической характеристики преступлений в сфере компьютерной информации // Актуальные проблемы государства и права. 2023. Т. 7. № 3. С. 370-378. https://doi.org/10.20310/2587-9340-2023-7-3-370-378

[180] *Schjolberg Stein.* A Cyberspace Treaty — A United Nations Convention or Protocol on Cyber-Security and Cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19April 2010.

[181] Cyberwar: War in the Fifth Domain»-Economist, Июль 25, 2010. URL: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain (дата обращения: 07.12.2022).

[182] *Лебедь В.Н.* Управление процессами обеспечения кибербезопасности как фактор международной стабильности / В. Н. Лебедь, Б. И. Терещенко, К. А. Восканян // Коммуникология: электронный научный журнал. — 2017. — Т. 2. — № 4. — С. 30–37.

Киберпреступники – это интеллектуалы сведущие не только в IT-технологиях, но и умеющие анализировать, выстравить целые схемы для обхода системы и вывода средств, которые путем изучения и исследования информационных систем, технологий, сети, ищут в них уязвимости или недостатки. В этих целях в своей деятельности они пользуются разными средствами, ресурсами (как денежными, так и человеческими) для достижения поставленной цели. Киберпреступники подстраиваются под изменение условий финансового рынка либо ситуацией в стране в целом и, следуя за развитием финансовых технологий, вооружается современными механизмами, алгоритмами и обеспечением.

Но что же такое киберпреступление?

Само официальное понятие, а также основные признаки киберпреступления были сформулированы лишь в 1974 г. на Конференции Американской ассоциации адвокатов[183]. Хотя дискуссии о киберпреступности длятся уже не один год. Более десяти лет назад исследователи стали задаваться вопросом, что нового в киберпреступности, не является ли это просто старым явлением, использующим новые инструменты. Большинство исследователей представляют киберпреступность как уникальное явление[184].

Киберпреступления на сегодняшний день представляют огромную угрозу для мира и стабильности в стране. Взять, к примеру, небезызвестный сценарий поражения иранской атомной станции вирусом STUXNET в 2010 г., чудом не приведший к катастрофическим последствиям, планировался и для терактов в Европе в 2016 г.[185] Опасность киберпреступности трудно переоценить, не только рядовые граждане, но и целые государства подвержены реальным «виртуальным» угрозам.

К «киберпреступлению» относится любое преступление, совершенное с применением различных способов и средств создания, обработки, передачи компьютерной информации[186].

Трудно согласиться с Глотиной И.М. о том, что «киберпреступность является подкатегорией компьютерной

---

[183] *Айков Д., Сейгер К., Фонсторх У.* Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М.: Мир, 1999. 351 с.

[184] *Попов, М.В.* Кибербезопасность как элемент национальной безопасности России / М. В. Попов, Л. Н. Мамаева // Вестник Саратовского государственного социально-экономического университета. — 2019. — № 5 (79). — С. 80–82.

[185] Координатор ЕС считает, что АЭС Бельгии могут угрожать кибератаки // РИА новости. 26.03.2016. URL: http://ria.ru/world/20160326/1397664506.html.

[186] *Глотина И.М.* Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. – 2014. – №8. – 12 с.

преступности», хотя далее она сама же отмечает, что «термин подразумевает преступления, совершенные с использованием компьютеров, сети Интернет или иной компьютерной сети как компонента преступления», потому что если в компьютерном преступлении используется только компьютер, то в киберпреступлениях помимо него, также могут быть использованы сети, иные технологии, гаджеты и т.д. Такого же мнения Бутусова Л.И.[187]

По мнению ряда ученых[188] «**киберпреступность** – это преступление *с использованием* компьютеров, отличительной особенностью является то, что компьютеры играют *вспомогательную* роль, в то время как **компьютерная преступность** – это преступление, целью которого является сам компьютер, являющийся прямым результатом компьютерных технологий (к примеру, хакерство)».

Бреннер С.В. (Brenner, S.W.)[189] считает, что «киберпреступность в первую очередь охватывает компьютерные преступления, хакерство, интернет-мошенничество, кибертерроризм и кибершпионаж». Этого же мнения придерживаются Чои К.С. (Choi, K. S.)[190], Холт Т.Ж. (Holt, T.J.), Буррусс Г.В. (Burruss, G.W.), Босслер А. (Bossler, A.)[191], Синчул Бэк (Sinchul Back)[192].

По мнению экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети[193].

По мнению Сериевой М.М. ««киберпреступность» – это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей.

---

[187] *Бутусова Л.И.* К вопросу о киберпреступности в международном праве. Вестник экономической безопасности. №2. 2016. С. 48

[188] *Albanese, J.S.* (2011). Transnational crime and the 21st century: Criminal enterprise, corruption, and opportunity. New York, NY: Oxford University Press; *Brenner, S. W.* (2010). Cybercrime: criminal threats from cyberspace. Santa Barbara, CA: ABC-CLIO; *Choi, K.S.* (2015). Cybercriminology and digital investigation (p. 340). El Paso, TX:LFB Scholarly Publishing; Computer misuse act 1990 (2018, July 5). In Legislation.gov.uk. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/contents; *Holt, T. J., Burruss, G. W., & Bossler, A. (2015).* Policing cybercrime and cyberterror. Durham, NC: Carolina Academic Press.

[189] *Brenner, S W.* (2010). Cybercrime: criminal threats from cyberspace. Santa Barbara, CA: ABC-CLIO

[190] *Choi, K.S.* (2015). Cybercriminology and digital investigation (p. 340). El Paso, TX: LFB Scholarly Publishing

[191] *Holt, T.J., Burruss, G.W., & Bossler, A.* (2015). *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press.

[192] *Back, Sinchul,* "The Cybercrime Triangle" (2019). FIU Electronic Theses and Dissertations. 4450. https://digitalcommons.fu.edu/etd/4450

[193] *Валько Д.В.* Киберпреступность в России и мире: сравнительный анализ // Управление в современных системах. – 2016. – №3(10). – С.29. https://cyberleninka.ru/ article/n/ kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka/viewer

В то же время термин «компьютерная преступность» относится только преступлениям, совершаемым против компьютеров или компьютерных данных»[194].

Важно учесть, что несмотря на то, что в 2001 году была принята Конвенция ЕС «О компьютерных преступлениях»[195], в которую входят: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием данных; правонарушения, связанные с нарушением авторского права и смежных прав. Однако, распределение на данную категорию и уже тем более наименование их компьютерными преступлениями, по нашему мнению, не совсем корректно. К примеру, статья 8 касается мошенничества с использованием компьютерных технологий, в то время как оно давно перешагнуло порог использования только компьютерных технологий, даже фишинговые или вишинговые атаки осуществляются на данный момент и с использованием обычного мобильного устройства.

Как справедливо отметила Яковлева А.В. «преступные деяния в компьютерной информационной отрасли всегда совершаются с применением компьютерного оборудования, к которому относится, помимо непосредственно компьютеров, различные технологии, в том числе инновационные, и различные типы программного обеспечения»[196].

В зарубежных правовых системах часто отсутствует строгое нормативное определение термина «киберпреступность», поскольку он охватывает широкий спектр правонарушений в киберпространстве. Как правило, понятие киберпреступности формулируется через описание конкретных видов противоправной деятельности в рамках уголовного законодательства.

К примеру, основным документом в Сингапуре, регламентирующим уголовную ответственность за киберпреступления, является Акт о злоупотреблениях в компьютерных сетях и кибербезопасности, однако и в нем не предусмотрено определение понятия «киберпреступность», также, как и в нашем законодательстве. «В Будапештской конвенции

---

[194] *Сериева М.М.* Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – 104-106 с.

[195] Конвенция о компьютерных преступлениях. СЕД 185. Будапешт, 23 ноября 2001 года.

[196] *Яковлева А.В.* Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. Т. 11. № 4. С. 70-81.

определения киберпреступности тоже нет, есть перечисление видов киберпреступлений. По тому же пути идет и итальянский законодатель»[197].

Исходя из этого, можно сформулировать определение киберпреступности как *«совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения, информационно-коммуникационных технологий, сетей и технических средств с целью получения финансовой или иной выгоды».*

Стоит отметить, что при изучении судебно-следственной практики по расследованию киберпреступлений, были выявлены некоторые присущие им специфические особенности:

- отсутствие идеальных следов преступления, характерное для традиционных видов преступлений ввиду бесконтактного выуживания необходимой информации и вследствие денежных средств, находясь в значительном отдалении от жертвы преступления (в некоторых случаях находясь на территории другой страны), что делает фактически трудно достижимым установление личности всех участников преступления. Как отметили Мордвинов К.В., Удавихина У.А. «киберпреступления имеют специфические характеристики, которые усложняют процесс их обнаружения»[198];

– передача денежных средств совершается бесконтактным путем, то есть посредством систем онлайн-банкинга (Click, Payme) либо электронных систем платежа (UzCard, Humo), электронных денег (WebMoney, QiWi, Яндекс. Деньги) либо через крипто-валютные биржи (Binance);

- киберпреступники, применяя новые технологии, используют главным образом невнимательность, неосведомленность и доверчивость пользователей виртуального пространства. Пользователи информационных систем «без достаточных к тому оснований верят в отсутствие кибератак, используя информационное пространство с незнанием ограничений и угроз безопасности системы»[199];

---

[197] *Соколов А.Ю., Солдаткина О.Л.* Правовая политика зарубежных стран в сфере противодействия преступлениям, совершаемым с использованием информационных технологий. Саратов, РФ, Государство и право. №9. 2023. С. 190. http://gospravo-journal.ru/s102694520027662-9-1/

[198] *Мордвинов К.В., Удавихина У.А.* Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1. С. 83–88. © http://gospravo-journal.ru/s102694520027662-9-1/

[199] Forensic Investigation Processes for Cyber Crime and Cyber Space / K.K. Sindhu, R. Kombade, R. Gadge, B.B. Meshram// Proceedings of International Conference on Internet Computing and Information Communications. 2012.Vol. 16. P. 193-206.

- простота в эксплуатации инструментов для совершения киберпреступлений в связи с огромным количеством «инструкций», таких как: как написать вирусы, взломать сервер, создать фишинговое письмо и так далее, при этом каких-либо специальных познаний и опыта работы совершенно не нужно;

- повышенная анонимность совершенного киберпреступления и низкая раскрываемость. Так, согласно статистике в Узбекистане в 2023 году около 90% киберпреступлений осталось нераскрытым. «По статистике, из общего числа поданных заявлений лишь 3 % доходят до возбуждения уголовных дел. Ответственность за свои действия несут лишь 5—7 преступников, а значит, доля привлеченных к ответственности не составляет и 0,1 % всех имевших место киберпреступлений. Это порождает чувство полной безнаказанности у киберпреступников»[200] ;

- возможность нанесения огромного ущерба без больших материальных затрат. Так по уголовному делу №260003/2019-15PG, размер ущерба составил 438.217 долларов США;

- транснациональность преступления так как в большинстве случаев преступники находятся на территории других государств, что делает труднодостижимым сбор доказательств для изобличения преступников;

- особая подготовленность преступников, организованный характер действий, преступники делятся на подгруппы, которые выполняют строго отведенные роли (колл-центры, кодеры, скаммеры и т.д.). «Современный киберпреступник уже не пират-одиночка, а звено в серьезном криминальном бизнес-процессе»[201];

- интеллектуальный характер преступной деятельности, что означает использование умственных навыков вместо грубой физической силы. Хотя встречаются случаи формирования «силовых» групп, состоящих из *спортиков.* Киберпреступники «тщательнее планируют свою деятельность, дополняя ее специализированными техническими возможностями, поэтому в результате таких действий затрагиваются интересы большего числа жертв»[202]*;*

---

[200] Аналитический отчет Norton report 2013 [Электронный ресурс]. — URL: http://www.symantec.com/ about/news/ resources/ press_kits/detail.jsp?pkid=norton-report-2013 (дата обращения: 03.05.2014).
[201] *Унучек Р.С., Чебышев В.В.* Мобильные угрозы // Вопросы кибербезопасности. 2014. № 3(4). С.57
[202] *Глотина И.М., Шевчук И.С.* Киберпреступность – проблема без границ // Экономика АПК Предуралья. 2019. № 1. С. 32

- киберпреступление совершается в автоматизированном режиме (in automated mode) и атака может происходить в одно и то же время в нескольких местах по принципу все, везде и сразу;

- трудность раскрытия киберпреступлений «традиционными» средствами, в частности когда дело касается отмывания денежных средств через дропов посредством крипто-валютных бирж, найти самих организаторов почти нереально. Как отметили некоторые ученые «злоумышленник при совершении хищений использует мобильные устройства, сим-карты, банковские карты, личные кабинеты, электронные кошельки, иные технические средства и предметы, которые оформлены на несуществующих либо третьих лиц, не причастных к совершению преступления (полученные в результате утраты, продажи, передачи сим-карт, банковских карт, личной информации третьим лицам и т. п.)»[203];

- очень высокий уровень латентности. В некоторых случаях, особенно касательно внедрения вредоносных программ, потерпевшие не знают, что на них была произведена кибератака и их устройства могут быть использованы для кибершпионажа, перенаправления IP-адреса и сокрытия следов. Но, в большинстве случаев латентность может быть в двух видах: скрытая (отсутствие обращения жертвы ввиду нежелания, малого ущерба и т.д.) и скрываемая («укрытие» преступления путем отказа в регистрации преступления из-за статистики, квалификация деяния как непреступного с вынесением постановления об отказе в возбуждении уголовного дела и т.д.), что приводит к тому, что киберпреступники, чувствуя свое превосходство и безнаказанность совершают все более опасные преступные деяния. «По оценкам специалистов, от 85 до 97% компьютерных преступлений остаются не обнаруженными или о них не сообщается по различным причинам в правоохранительные органы»[204].

Противодействие киберпреступности предполагает координацию всех сил и средств, совершенствование как уголовного, так и уголовно-процессуального законодательства, повышение квалификации сотрудников, оснащение всех подразделений современным оборудованием. Без комплексного подхода невозможно говорить о возможности даже уменьшения киберпреступлений.

---

[203] *Макаров, Роман А., Александр А. Кузнецов.* 2020. «Следственная профилактика хищений с банковских карт, совершаемых дистанционно с использованием средств сотовой связи». Алтайский юридический вестник 4 (32): 144–150.

[204] *Амелин Р.В.* Компьютерная безопасность.URL: https:// docviewer. yandex.ru/view/757079236

ЯРАТИЛАЁТГАН ИМКОНИЯТЛАР ЭНГ АВВАЛО ФУҚАРОЛАРНИНГ ҲУҚУҚ ВА ЭРКИНЛИКЛАРИНИ МУҲОФАЗА ҚИЛИШГА ХИЗМАТ ҚИЛМОҒИ ЛОЗИМ

Мавлонов Авазбек
Ўзбекистон Республикаси
Ҳуқуқни муҳофаза қилиш академияси
мустақил изланувчиси
avtoritet-353@mail.ru

Аннотация:*Мақолада муаллиф томонидан тезкор-қидирув фаолиятида шахснинг ҳуқуқи ва эркинликларини қонун билан кафолатланганлиги ҳамда бу борада олиб борилаётган қонун ижодкорлиги, амалиётга татбиқ этилган янги ўзгаришлар ҳамда бу борада амалга оширилиши зарур бўлган чора-тадбирлар, тезкор-қидирув тадбирлари доирасида ахборот-коммуникация технологиялари орқали кибермаконда олиб бориладиган мониторинг ва уларнинг натижаларидан фойдаланиш ҳамда бу борада қонун устиворилигига амал қилиш ва адолатни таъминлаш масалалари батафсил ўрганилади, тезкор-қидирув фаолияти билан боғлиқ бўлган ҳуқуқий муносабатларни тартибга солувчи норматив ҳужжатлар таҳлил қилинади.*

Шунингдек, «Тезкор-қидирув фаолияти тўғрисида»ги Қонунга киритилган қўшимчаларга мувофиқ тезкор-қидирув тадбирларини ахборот-коммуникация технологияларини қўллаган ҳолда, шу жумладан кибермаконда ва унинг имкониятларидан фойдаланган ҳолда ўтказиш жараёнида ваколатли давлат органлари томонидан шахсларнинг ҳуқуқ ва эркинликларини муҳофаза қилиниши таъминлаш, бунинг учун кўрилиши лозим бўлган чора-тадбирлар хусусида фикр ва мулоҳаза юритилади.

Бундан ташқари, тезкор-қидирув фаолиятига ахборот-коммуниказия технологияларини қўллаш жараёнида ваколатли органлар ходимлари томонидан алоҳида аҳамият қаратилиши лозим бўлган омиллар юзасидан таклифлар берилади.

Якунда амалдаги қонунчилик нормаларига киритилаётган ўзгартириш ва қўшимчалар энг аввало инсон ҳуқуқлари ва манфаатларига хизмат қилиш лозимлиги юзасида ҳулоса билдирилади.

Калит сўзлар. *Тезкор-қидирув тадбирлари, ахборот-коммуникация технологиялари, киберхавфсизлик, кибермакон, виртуал-муҳит, веб-ресурс, ижтимоий тармоқлар, шахснинг ҳуқуқ ва эркинликлари, қонунийлик, адолат*

Мақсадимиз – адолат ва қонун устуворлигини таъминлаш орқали халқимизни рози қилиш.
Ш.Мирзиёев

Сўнги йилларда мамлакатимизда фуқароларнинг ҳуқуқлари, эркинликлари ҳамда қонуний манфаатларини ҳимоя қилиш

борасида яхлит ва мукаммал ҳуқуқий тизим яратиш бўйича кўп ишлар қилинди ва бу борадаги ишлар ҳануз давом эттирилмоқда.

Қайд этиш лозимки, жамиятда ахборот ахборот-коммуникация технологияларининг ўрни тобора мустаҳкамланиб, улар қамраб олаётган соҳалар соат сайин кенгайиб бормоқда. Бунинг натижасида жамият ва давлатда юз бераётган ижобий ўзгаришларни санаб саноғига етиш имконсиз.

Сир эмаски, бу жараёнлар шахс, жамият ва давлат хавфсизлигини таъминлаш бўйича ваколатли ташкилотлар зиммасига қўшимча маъсулият ва жавобгарлик юклайди. Қонун ижодкорлиги соҳасида ҳам ўта ҳассос ва зийрак бўлишни талаб этади.

Ўзбекистон Республикаси Олий мажлиси томонидан 2024 йил 13 мартда қабул қилинган Қонун билан «Тезкор-қидирув фаолияти тўғрисида»ги Ўзбекистон Республикаси Қонунига ахборот технологиялари соҳасидаги жиноятчиликка қарши курашишнинг ҳуқуқий асосларини мустаҳкамлашни, тезкор-қидирув тадбирлари ахборот-коммуникация технологияларини қўллаган ҳолда, шу жумладан кибермаконда ва унинг имкониятларидан фойдаланган ҳолда ўтказилиши мумкин эканлигини белгилашни назарда тутувчи қўшимча ва ўзгартиришлар киритилганлиги юқоридаги фикримизга яққол мисол бўла олади.

Мазкур қонунга мувофиқ Ўзбекистон Республикаси «Тезкор-қидирув фаолияти тўғрисида»ги Қонуннинг 14-моддаси «тезкор-қидирув тадбирлари ахборот-коммуникация технологиялари қўлланилган ҳолда, шу жумладан кибермаконда ва (ёки) унинг имкониятларидан фойдаланилган ҳолда ўтказилиши мумкин» жумлалари билан тўлдирилди.

Ўзбекистон Республикасининг 2022 йил 14 апрелда қабул қилинган «Киберхавфсизлик тўғрисида»ги Қонунининг 3-моддасида кибермакон — ахборот технологиялари ёрдамида яратилган виртуал муҳит эканлиги кўрсатиб ўтилган.

Таъкидлаш жоизки, ҳозирда аксарият инсонлар ўзларини ижтимоий тармоқлардан айро ҳолда тасаввур эта олмайдилар. Кун сайин бу жараён тобора кучайиб бормоқда. «Киберхавфсизлик тўғрисида»ги Қонуннинг 3-моддасидаги тушинтиришдан келиб чиқадиган бўлсак, ижтимоий тармоқларни ҳам кибермаконнинг ажралмас бир қисми сифатида айта оламиз.

«Тезкор-қидирув фаолияти тўғрисида»ги Қонунга киритилган қўшимчага мувофиқ эндиликда тезкор-қидирув фаолиятини амалга

оширувчи давлат органлари тезкор ишловда бўлган шахслар тўғрисида ижтимоий тармоқларда ва виртуал муҳитнинг бошқа ресурсларида, яъни кибермаконда сақланаётган ёки учинчи шахслар томонидан тарқатилган маълумотларни ҳам алоҳида тезкор-қидирув тадбирлари натижасида олинган маълумотлар сифатида тезкор қидирув ишига қўшиши мумкин бўлди.

Бундан англашиладики, бу турдаги маълумотлар тезкор-қидирув тадбирларини натижалари бўйича ўтказиладиган суриштирув ва дастлабки тергов жараёнларида ҳуқуқий жиҳатдан баҳоланиши шарт. Жорий этилган янги тартиб, тезкор-қидирув фаолиятини амалга оширувчи давлат органларига тезкор-ишловда бўлган шахслар тўғрисида маълумотлар тўплашда бир қатор қулайликлар тақдим этсада, шахснинг ҳуқуқ ва эркинликларини ҳамда қонуний манфаатларини ҳимоя қилиш масаласида бир қатор нозик масалаларни муҳокама майдонига олиб киради.

Жумладан, кибермаконда олиб бориладиган мониторинглар давомида шахснинг мамлакатимиз ҳудудида тарқатилиши таъқиқланган маълумотлар жойлаштирилган ижтимоий тармоқлардаги гуруҳлар ва каналларга аъзо эканлиги аниқланди.

Бу ҳолат тезкор-қидирув фаолиятини амалга оширувчи давлат органлари томонидан ушбу шахснинг бузғунчи ғоялар таъсирига тушган шахс сифатида тавсифланиши учун етарли асос деб қаралмаслиги лозим.

Шунингдек, оператив ишловда бўлган шахс тўғрисида кибермакондаги барча маълумотларни ҳам тезкор-қидирув ишига жамлашга яроқли бўлган маълумот сифатида қабул қилиб бўлмаслигига жиддий аҳамият бериш зарур.

Бундан ташқари, ахборот-коммуникация технологиялари орқали, шу жумладан кибермаконда ва унинг имкониятларидан фойдаланилган ҳолда ўтказиладиган тезкор тадбирлар натижасида тўпланган маълумотлар шахсларнинг айнанлиги, яъни олинган маълумотлар айнан тезкор ишловда бўлган шахсга тааллуқли эканлиги ёки айнан ўша шахс ҳақида эканлиги, нуқтаи назаридан синчковлик билан таҳлил қилиниши шарт. Яъни, тезкор тадбир давомида тезкор ходим ўрганишда бўлган ресурсларни таҳлил қилиш давомида профил ва аккаунтлар бир шахсга доир биографик маълумотлардан фойдланган ҳолда бошқа бир шахс ёки гуруҳ томонидан очилмаганлигига ишонч ҳосил қилиш лозим.

Яна шуни алоҳида таъкидлаш лозимки, кўп ҳолларда фуқаро-лар ўзлари томонидан ахборот-коммуникация технологиялари

орқали тарқатилаётган маълумотларнинг мазмун ва моҳиятини англаб етмайдилар. Ҳорижий тилларда жозибали оҳангда куйланган қўшиқ ёки жимжимадор шаклларга эга бўлган каллиграфик ёзувларни асл мазмунидан мутлақо бехабар бўлган ҳолда ўзларнинг танишларига, қариндошларига, ҳамкасбларига шунчаки юбориш ёки кибермакондаги ўзларининг саҳифаларига жойлаштириш орқали ҳам тезкор-қидирув тадбирлари объектига айланиб қолмоқдалар.

Энг ачинарлиси, тезкор-қидирув фаолияти давомида аниқланган фуқаролар томонидан содир этиладиган юқоридаги каби хатти-ҳаракатлар айрим ҳолларда Ўзбекистон Республикаси Жиноят Кодексининг 156, 159, 244^1, 244^3-моддалари билан квалификация қилишга асос сифатида баҳоланмоқда.

Қайд этиш лозимки, Ўзбекистон Республикаси Конституциясининг 13-моддасида Ўзбекистон Республикасида демократия умуминсоний принципларга асосланади, уларга кўра инсон, унинг ҳаёти, эркинлиги, шаъни, қадр-қиммати ва бошқа ажралмас ҳуқуқлари олий қадрият ҳисобланиши белгилганган.

Шунингдек, Қомусимизнинг 20-моддасида давлат органлари томонидан инсонга нисбатан қўлланиладиган ҳуқуқий таъсир чоралари мутаносиблик принципига асосланиши ва қонунларда назарда тутилган мақсадларга эришиш учун етарли бўлиши кераклиги, инсон билан давлат органларининг ўзаро муносабатларида юзага келадиган қонунчиликдаги барча зиддиятлар ва ноаниқликлар инсон фойдасига талқин этилиши мустаҳкамланган.

Шундай экан, тезкор-қидирув тадбирлари ахборот-коммуникация технологияларини қўллаган ҳолда ташкил этилганида энг аввало Қомусимизда белгиланган инсон ҳуқуқларига оид юқорида қайд этилган нормалар талабларига оғишмасдан риоя этилиши лозим**.**

Бунинг учун тезкор-қидирув тадбирлари давомида ахборот технологияларини қўллаган ҳолда кибермаконда олиб бориладиган мониторинглар давомида эътиборга тушган шахсларга нисбатан ҳар қандай турдаги жавобгарлик масаласи кўтарилишидан аввал ушбу шахсларнинг ахборот технологиялари сохасидаги билим ва кўникмалари ўрганилиши, турли ҳил ижтимоий тармоқлардан ҳамда бошқа веб-ресурслардан фойдалана олиш имкониятлари мутахассислар иштирокида ҳолисона баҳоланиши лозим.

Шунингдек, тезкор-қидирув фаолиятини амалга оширишга ваколатли бўлган давлат ташкилотлари ахборот-коммуникация соҳасидаги ўзларнинг техник имкониятларидан қатъий равишда қонун доирасида ҳамда шахсларнинг ҳуқуқ ва эркинликларини бузмаган ҳолда фойдаланишлари алоҳида назоратга олиниши зарур.

Ҳулоса ўрнида шуни айтиш жоизки, мамлакатимизда криминоген вазиятни яхшилаш, жиноятчиликка қарши курашиш ва уларнинг олдини олиш, шунингдек, латент жиноятлар сонини камайтириш мақсадида амалга оширилаётган барча ислоҳотлар, тезкор-қидирув фаолиятини амалга оширувчи давлат органларига берилаётган ҳуқуқлар ва яратилаётган ҳар қандай шарт-шароит ҳамда имкониятлар энг аввало инсон ҳуқуқ ва эркинликларига хизмат қилиш зарур.

ИННОВАЦИОН ТЕХНОЛОГИЯЛАР ЁРДАМИДА СУД-ЭКСПЕРТЛИК ФАОЛИЯТИНИ ТАКОМИЛЛАШТИРИШ

Абдувахоб Зулфуқоров
Ички ишлар вазирлиги Академияси Криминалистик экспертизалар кафедраси доценти юридик фанлар бўйича фалсафа доктори (PhD), доцент

Аннотация:*Мақолада суд экспертлик фаолиятида иновацион технологияларни қўллашга оид муаммоли масалалар кўриб чиқилган. “Технология” атамасининг мазмун-моҳиятидан келиб чиқиб, “суд экспертиза технологияси” атамасига таъриф берилган. Суд-экспертлик фаолиятининг ахборот таъминотига оид муаммоларини кўриб чиқиб ва давлат суд экспертиза муассасаларининг ижобий тажрибалари, шунингдек, экспертлик амалиёти ва суд экспертизаси асосларини ўқитиш жараёнларини янгича ёндашувлар асосида суд-экспертлик фаолиятини такомиллаштириш йўналишлари таклиф қилинган.*

Калит сўзлар: *услуб, услубиёт, ахборот таъминоти, суд-экспертлик фаолияти, инновацион технологиялар, суд экспертиза технологияси, тадқиқот услублари, суд экспертизасининг ахборот таъминоти, суд экспертиза мутахассисликлари бўйича ўқитиш, суд экспертизасининг назарий ва ҳуқуқий асослари.*

Аннотация: *Рассмотрены проблемные вопросы применения инновационных технологий в судебно-экспертной деятельности. Исходя из содержания термина “технология”, дается определение термину “технология судебной экспертизы”. Рассмотрены проблемы информационного обеспечения судебно-экспертной деятельности и предложены направления совершенствования судебно-экспертной деятельности на основе положительного опыта государственных судебно-экспертных учреждений, а*

также новых подходов к процессам обучения основам экспертной практики и судебной экспертизы.

Ключевые слова: *метод, методика, информационное обеспечение, судебно-экспертная деятельность, инновационные технологии, технология судебной экспертизы, методы исследования, информационное обеспечение судебной экспертизы, обучение по специальностям судебной экспертизы, теоретико-правовые основы судебной экспертизы*

Abstract: *Problematic issues of application of innovative technologies in forensic activity are considered. Based on the content of the term "technology", the definition of the term "technology of forensic examination" is given. Problems of information support of forensic activity are considered and directions of improvement of forensic activity on the basis of positive experience of state forensic institutions, and also new approaches to processes of training in the basics of forensic practice and forensic examination are offered.*

Key words: *method, methodology, information support, forensic activity, innovative technologies, forensic technology, research methods, information support of forensic examination, training in forensic specialities, theoretical and legal foundations of forensic examination.*

Илм-фан ва техниканинг замонавий ютуқлари мамлакатимизнинг суд экспертиза институтида мустаҳкам ўрин эгаллайди. Инновацион технологиялардан фойдаланиш туфайли нафақат суд экспертизасининг турли йўналишлари, балки умуман суд-экспертлик фаолияти ҳам такомиллаштирилмоқда.

Маълумки, технология деганда (юнонча techne – маҳорат, санъат + logos – таълимот) – 1) ишлаб чиқаришнинг бирор соҳасида хомашё, материал, яримфабрикат ва ш.к.ларга ишлов бериш ёки қайта ишлаш, уларнинг ҳолати, хоссалари ва шаклини ўзгартиришда қўлланиладиган усуллар, методлар мажмуи; 2) хомашё ва материалларга тегишли ишлаб чиқариш қуроллари ёрдамида ишлов бериш усул ва йўллари ҳақидаги фан тушунилади[1].

Бундан келиб чиқадики, суд экспертиза технологияси – бу махсус билимларга асосланган, белгиланган кетма-кетликдаги операциялар, ҳаракатлар тўплами. Ушбу операция ва ҳаракатлар суд экспертига ҳал қилиш учун берилган вазифаларни бажаришда ашёвий далиллар – тадқиқот объектларини тадқиқ қилишда амалга оширилади.

Суд экспертизасида инновацион технологиялар – бу белгиланган вазифаларни юқори сифатли даражада амалга оширишга

[1] Ўзбек тилининг изоҳли луғати. Т – ҳарф. / Таҳрир ҳайъати: Э.Бегматов, А.Мадвалиев, Н.Маҳкамов, Т.Мирзаев (раҳбар), Н.Тўхлиев, Э.Умаров, Д.Худойберганова, А.Ҳожиев. А.Мадвалиев таҳр.ост. – Т.: “Ўзбекистон миллий энциклопедияси” Давлат илмий нашриёти. 2013 й. – 81-б.

ёрдам берадиган янги усул ва воситалардан фойдаланишдир.

Маълумки, янги техник воситалар, услублар ва тадқиқот услубиётининг ишлаб чиқилиши ёки мавжудларининг такомиллаштирилиши ҳисобига мамлакатимизда суд экспертизаси жадал ва доимий равишда ривожланиб бормоқда. Бу каби ёндашув кўп сабабларга боғлиқ. Бу жиноятчиликнинг ўсиши, жиноят содир этишнинг янги усуллари, янги тадқиқот объектларининг пайдо бўлиши кабиларда намоён бўлади. Жиноят содир этишнинг янги шакллари қанчалик ғайриодатий бўлса, эксперт тадқиқотлари ҳам шунчалик мураккаб бўлади.

Шунинг учун экспертизаларнинг тадқиқот услубларига қўйиладиган асосий талабларга – услубларнинг илмий асосланганлиги (тўғри натижалар олиш нуқтаи назаридан услубларнинг ишончлилиги); услубларнинг рухсат этилганлиги (услубнинг қонунийлиги ва этика қоидаларига риоя этилиши, эксперт учун хавфсизлиги) ва янги услубларни ишлаб чиқишда амал қилиниши лозим бўлган бошқа бир қатор талабларга риоя қилиш керак. Шу муносабат билан суд-экспертлик фаолиятини такомиллаштириш мақсадларига эришишга амалий экспертлик фаолиятига янги усул ва услубларни жорий этиш жараёнларини таҳлил қилиш ҳам ўз ҳиссасини қўшади.

Суд-экспертлик фаолиятининг ахборот таъминотига оид муаммоларни кўриб чиқишда унинг ўзига хос хусусиятларини ҳисобга олган ҳолда, бу жараён назарий, услубий ва ташкилий асосларни, янги усуллар, услублар ва техник воситаларни ишлаб чиқиш, инновацион технологияларни ривожлантириш орқали доимий равишда такомиллаштирилиши керак.

Суд экспертизасининг ахборот таъминоти суд экспертизалари вазифаларини ҳал қилиш учун зарур бўлган тизимлаштирилган илмий-техник маълумотларни танлаш, тайёрлаш ва беришнинг илмий ташкил этилган ва узлуксиз жараёни бўлиши керак.

Экспертлик амалиётини такомиллаштириш йўналишларидан бири экспертизалар ўтказиш жараёнларини автоматлаштиришдир. Бу жараён экспертизаларни ўтказиш давомида керакли маълумотларни олиш, қайта ишлаш, узатиш ва улардан фойдаланиш жараёнларида суд экспертини бевосита иштирок этишдан қисман ёки тўлиқ озод қиладиган техник воситалар, математик усуллар ва фаолият дастурларидан фойдаланишдан иборат. Шу сабабли ахборотни қидириш, йиғиш, қайта ишлаш, сақлаш, таҳлил қилиш ва тақдим қилиш самарадорлигини

оширишга ёрдам берадиган автоматлаштирилган ахборот тизимларини суд-экспертлик фаолиятига жорий этиш ва фаолият юритишга зарурат мавжуд. Бу каби автоматлаштирилган тизимларнинг фаолияти вазифаси минимал даражада вақт, куч ва меҳнат сарфлаган ҳолда максимал натижага эришишдан иборат бўлган техник воситалардан фойдаланиш орқали суд-экспертлик фаолиятини ахборот билан таъминлаш самарадорлигини оширишга ёрдам беради.

Суд-экспертлик фаолиятини такомиллаштириш йўналишларидан яна бири суд экспертлари томонидан амалий иш фаолиятида йўл қўйиладиган хатоларнинг олдини олишдан иборат. Шу боисдан турли хил хатоларни аниқлаш, шу жумладан суд экспертизаларини ўтказишдаги янги усуллардан фойдаланиш ёки улардан фойдаланишни қўйилган саволларнинг ижобий ҳал этилишига олиб келмаган даражада эътиборсиз қолдириш ҳолатларини аниқлаш мақсадида суд экспертизасининг турли соҳалари бўйича экспертлик амалиётини даврий равишда умумлаштириш ва таҳлил қилиш зарур бўлади. Бунда комплекс экспертизалар, олинган натижаларни баҳолаш ва уларни расмийлаштиришнинг тўғрилигига алоҳида эътибор бериш лозим.

Инновацион технологиялар кўплаб таркибий қисмлардан иборат бўлиб, улар орасида ахборот дастурлари муҳим ўрин тутади. Ушбу ёндашув мураккаб тадқиқот услублари қўлланиладиган экспертизаларнинг, суд экспертизаларининг янги турлари ва синфларини илмий таъминотининг аҳамиятини оширади, бу эса уларни бажариш учун юқори малакали мутахассислар ва тадқиқотчиларни талаб қилади. Шу муносабат билан экспертизаларнинг илмий даражасини ошириш, илмий кадрлар (илмий даража ва илмий унвонга эга мутахассислар) ва суд экспертларини тайёрлаш масалалари ҳам муҳим аҳамиятга касб этади.

Ўзига хос касбий фаолият бўлган суд экспертизасининг моҳиятидан келиб чиқиб, суд экспертларини ўқитиш ўзига хос хусусиятларга эга бўлади.

Суд экспертиза мутахассисликлари бўйича ўқитиш самарадорлиги ўқитувчининг касбий маҳорати ва тажрибасига боғлиқ бўлади. У нафақат янги эксперт усулларини, янги ўқув ва илмий адабиётларни, суд-экспертлик фаолиятини амалга ошириш билан боғлиқ барча соҳаларни қамраб олган замонавий процессуал қонунчиликни билиши, балки амалиётчи ходимлар – экспертизаларни ўтказувчи суд экспертлари ҳамда экспертизаларни тайинловчи шахслар (органлар) билан доимий ҳамкорлик қилиши

керак.

Суд-экспертлик фаолиятида касбий маҳорат ва малака даражасини ошириш бир неча йўналишларни қамраб олади.

Муҳим аҳамиятга эга бўлган ушбу йўналишларда бири, суд экспертизасининг янги тадқиқот услублари ва услубиёти, янги техник-криминалистик воситалар базаси билан таниш, аниқ ўтказилаётган экспертизаларни ўрганиш имконини берадиган ўқитувчиларнинг суд экспертиза муассасасида амалиёт ўташи ҳисобланади. Бу каби стажировкаларда махсус атамаларни, эксперт хулосаларининг якуний жавоблари шакли ва уларнинг қанчалик асосли ва ишончли эканлигини, ушбу якуний хулосаларни тасдиқловчи фотосуратларни ҳамда суд экспертлари билан аниқ бир турдаги суд экспертизаларини ўтказишда мавжуд бўладиган бошқа кўплаб ижобий ва салбий жиҳатларни муҳокама қилиш фойдалидир.

Ушбу ёндашув ўқитувчига суд экспертларини ўқитиш жараёнида, амалиётчи суд экспертига – суд экспертизаларини ўтказиш жараёнида ягона тактикани ишлаб чиқишга имкон беради. Шубҳасиз, стажировка жараёнидаги норасмий самимий мулоқот ҳар икки томонга ҳам ижобий таъсир кўрсатади ва фойда келтиради. Шунинг учун ўқитувчининг экспертлик амалиёти билан билан танишиши ва амалий фаолиятни ўрганиши чуқур ва мазмунли бўлиши керак.

Суд экспертизасининг турли йўналишлари бўйича мутахассисларни ўқитиш самарадорлигини ошириш учун ҳуқуқни муҳофаза қилиш органлари, бошқа турдош муассасалар ва халқаро ташкилотлар билан ўзаро ҳамкорлик ҳам муҳим аҳамият касб этади.

Республикамизнинг барча давлат суд экспертиза муассасаларида ушбу йўналишда ижобий тажриба мавжуд. Жумладан, Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Х.Сулаймонова номидаги Республика суд экспертизаси маркази “лабораторияларини халқаро стандартларга мослаштириш мақсадида, 2020 йилда БМТнинг гиёҳвандлик ва жиноятчиликка қарши курашиш бўйича Марказий Осиёдаги минтақавий ваколатхонаси кўмагида “Тадқиқот ва калибровка лабораториялари ваколатига қўйиладиган умумий талаблар” ISO/IEC 17025 халқаро стандартига мувофиқ аккредитация қилиниб, мувофиқлик сертификатига эга бўлди. Мазкур аккредитация марказга тадқиқотларни халқаро стандартлар даражасида бажариш имконини беради, бу эса олинган натижаларнинг барча томонлар ва

иштирокчилар томонидан тан олинишини таъминлайди. Яъни ISO 17025 стандарт талаблари бўйича халқаро аккредитациядан ўтиш лабораториялар томонидан берилган тадқиқот натижаларининг (хулосаларнинг) халқаро миқёсда шубҳасиз тан олинишини, фуқароларнинг бузилган ҳуқуқ ва манфаатлари ишончли ҳимоя қилинишига ва одил судлов таъминланишига хизмат қилади”[2].

Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Х.Сулаймонова номидаги Республика суд экспертизаси маркази бугунги кунда нафақат экспертиза тадқиқотларини ўтказиш билан, балки амалиётга янги экспертиза турларини жорий қилиш, давлат ва нодавлат суд экспертларини қайта тайёрлаш, ҳуқуқий билимларини ошириш ҳамда судлар ва ҳуқуқни муҳофаза қилувчи органларга махсус билимларни қўллаш йўли билан кўмаклашиш бўйича ҳам фаолият кўрсатиб келмоқда. “Марказда суд экспертизасини ривожлантиришнинг замонавий босқичида биринчи навбатда экспертиза тадқиқотлари сифатига алоҳида эътибор қаратилмоқда. Кўплаб хорижий давлатлардаги аксарият экспертиза лабораторияларида сифатни таъминлаш ва назорат қилиш мақсадида ISO/IEC 17025 халқаро стандартига мувофиқ сифат менежменти тизимлари жорий этилгани каби Марказда бу борада тегишли ишлар амалга оширилмоқда. Жумладан, “Синов ва калибрлаш лабораториялари компетентлигига умумий талаблар” деб номланган, лабораториялар томонидан ишлаб чиқилган усуллар, стандарт ва ностандарт усуллар бўйича ўтказиладиган текширувлар ва калибровкаларга бўлган умумий талаблар ўрнатилган. Бундан ташқари, БМТнинг наркотиклар ва жиноятчилик бошқармасининг Марказий Осиёдаги минтақавий ваколатхонаси кўмагида Марказнинг 2 та лабораторияси, жумладан Одам ДНКси суд биологик экспертизаси ва Материаллар, ашёлар ва буюмлар криминалистик экспертизаси лабораториялари ўтган йили халқаро аккредитациядан ўтди. Ҳозирги пайтда Марказнинг яна 2 та лабораторияси, жумладан Ҳужжатлар криминалистик экспертизаси ва Суд-фонография экспертизаси лабораторияларини халқаро аккредитациядан ўтказиш бўйича тайёргарлик ишлари олиб борилмоқда”[3].

Х.Сулаймонова номидаги Республика суд экспертизаси марказида Халқаро ҳамкорлик соҳасида ҳам бир қатор ижобий

[2] А.Халилов. Суд экспертизасида янги одимлар / “Ўзбекистон суд экспертизаси” ҳуқуқий, ижтимоий, илмий-амалий журнали, 2021 й., (1) №1. – 2-5-б.

[3] У.Х.Узаков. Республика суд экспертизаси маркази: бугунги кун ва истиқболи. / “Ўзбекистон суд экспертизаси” ҳуқуқий, ижтимоий, илмий-амалий журнали. 2021. (1) №1. – С.102-105.

ишлар амалга оширилиб, бир қатор хорижий суд экспертиза муассасалари билан ҳамкорлик ўрнатилиб, меморандумлар имзоланган. Жумладан, “Суд-экспертиза соҳасида халқаро ҳамкорликни кенгайтириш Марказнинг муваффақиятли ривожланишининг муҳим кафолати ҳисобланади. Чунончи, халқаро тажриба соҳа ривожланишининг интеграцион хусусиятга эгалигини кўрсатмоқда. Бу борада ҳозирги вақтда Европа суд экспертиза муассасалари тармоғи (ENFSI) ёки Осиё суд-экспертиза тармоғи (AFSN) каби бир қатор минтақавий халқаро суд-экспертиза жамиятлари, жаҳон миқёсида Суд-экспертиза халқаро ассоциацияси (IAFS) фаолият кўрсатмоқда. Шунингдек, дунё миқёсида катта нуфузга эга бўлган Суд-экспертиза фанлари Америка академияси (AAFS) номини алоҳида эътироф этиш лозим. Марказ Корея Республикаси, Япония, Малайзия, Сингапур, Хитой, Қозоғистон каби давлатларни ўзида жамлаган нуфузли Осиё суд-экспертиза тармоғига аъзо бўлиш, Европа суд экспертиза муассасалари тармоғи билан ҳамкорлик ўрнатиш йўлида дадил қадамлар ташламоқда”[4].

Ҳуқуқни муҳофаза қилиш органлари ходимлари суд экспертларини учун ташкил қилинаётган ўқув жараёнларида, тегишли семинар ва амалий машғулотларда қатнашадилар, ташкил этилаётган илмий-амалий анжуманлар, давра суҳбатлари, илмий-амалий семинарларга таклиф қилинадилар. Бу жараёнларда суд экспертизаларини тайинлаш ва ўтказишнинг процессуал жиҳатлари, тадқиқотлар ўтказиш учун зарур бўлган материаллар, шу жумладан таққослаш учун намуналар билан таъминлаш билан боғлиқ муаммоли масалаларни муҳокама қиладилар. Бундай учрашувлар суд экспертларини ўқитиш ҳамда алоҳида ўқув тергов ҳаракатларини (турли изларни аниқлаш ва уларни белгиланган тартибда олиш мақсадида ҳодиса содир бўлган жойни кўздан кечириш, ҳодиса содир бўлган жойда эксперт экспериментини ўтказиш ва ҳоказо) ўтказиш самарадорлигини оширишга ёрдам беради.

Таълим билимларни ўзлаштириш, кўникма ва малакаларни эгаллаш бўйича ўқитувчи томонидан бошқариладиган жараёни

[4] Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Х.Сулаймонова номидаги Республика суд-экспертиза марказининг Суд-экспертлик илмий-тадқиқот институти тўғрисида низом. / Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2021-йил 22-ноябрдаги “Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Х. Сулаймонова номидаги Республика суд-экспертиза марказининг Суд-экспертлик илмий-тадқиқот институти фаолиятини ташкил этиш чора-тадбирлари тўғрисида”ги 704-сон қарори.// Қонунчилик маълумотлари миллий базаси, 22.11.2021-й., 09/21/704/1079-сон; 14.07.2022-й., 09/22/385/0643-сон.

эканлигини ҳисобга олган ҳолда таъкидлаш жоизки, суд-экспертлик фаолиятида касбий маҳорат ва малака даражасини оширишга нисбатан яна бир ёндашув тайёр шаклланган билимларни дарсликлар, ўқув қўлланмалари ҳамда турли дидактик воситалар ва техникалар ёрдамида беришдан иборатдир. Билим олиш ва тегишли маълумотларни, айниқса янги адабиётларни самарали идрок қилиш жараёнини оқилона бошқариш, нафақат билимлар ва адабиётларни ўрганиш учун тавсия этиш, балки ҳар бир манба учун кенгайтирилган изоҳларни тайёрлаш мақсадга мувофиқ бўлади. Бу тингловчи ва талабаларга адабий манбалар мазмунини тўғри идрок этиш имконини беради.

Суд экспертларини ўқитишда ўқитувчилик маҳоратини оширишга ҳисса қўшадиган яна бир йўналишни қайд этиш лозим – бу криминалистика ва суд экспертизаси фанлари бўйича маърузалар ўқийдиган ўқитувчиларнинг ўзаро ҳамкорлигидир. Суд экспертизаси бўйича фанлар мустақил ўқув фани сифатида криминалистика фанидан анча кейинроқ ва фақат бир нечта олий тиаълим муассасаларида бошланганлиги сабабли айрим мавзулар ҳали-ҳануз “Криминалистика” фани доирасида, хусусан, унинг “Криминалистик техника” бўлими ўқитилмоқда. Худди шу мавзулар анчагина чуқурроқ тарзда “Суд экспертизаси” фани доирасида ўрганилиши лозим. Масалан, ҳодиса содир бўлган жойни кўздан кечириш ва уни терговчи томонидан ўтказиш тактикаси ва мутахассиснинг (экспертнинг) худди шу тергов ҳаракатида иштирок этишига оид мавзулар. Ушбу процессуал субъектларнинг ўзаро ҳамкорлиги бир-бирларини тўлиқ тушуниш асосида амалга оширилиши керак, уларнинг ҳаракатлари аниқ мувофиқлаштирилиши керак. Шунинг учун ўқитувчилар мавзуга оид маълум бир материални тингловчи ва талабаларга тақдим этиш бўйича умумий фикр ва қарашларга эга бўлишлари керак.

Ўқув жараёнининг ҳар томонлама бўлишини таъминлаш учун ўқитувчи янги эксперт усулларини, нафақат ўқув, балки илмий адабиётларни ҳам билиши, янги педагогик технологияларни ишлаб чиқишда шахсан иштирок этиши ва уларни (масалан, интерактив доскалар, мултимедиа воситаларини ва ҳоказо) ўқув жараёнларига татбиқ қилиши керак.

Суд экспертизасининг назарий ва ҳуқуқий асосларини самарали ўқитиш ва ўргатиш учун суд экспертизаларининг турлари ҳамда мутахассисликларнинг йўналишлари бўйича махсус дарсликлар, услубий ва ўқув қўлланмаларини тайёрлаш ишларини тизимли давом эттириш керак.

Бундай ўқув ва илмий нашрларни тайёрлашнинг самарали шакли бу ўқитувчи ва давлат суд экспертиза муассасаси етакчи мутахассисининг биргаликдаги ноширлик фаолияти ҳисобланади. Муайян ўқув ёки илмий асарни ёзишда бундай биргаликдаги фаолият бир-бирини муваффақиятли тўлдиради ва шубҳасиз эксперт мутахассислигининг ривожланишига ижобий таъсир кўрсатади.

Ўзбекистон Республикаси Президентининг 2021 йил 5 июлдаги “Ўзбекистон Республикасида суд-экспертлик тизимини такомиллаштириш чора-тадбирлари тўғрисида”ги 6256-сонли Фармони асосида қабул қилинган Ҳукуматимизнинг қарорларига кўра, мамлакатимиз тарихида илк маротаба Х.Сулаймонова номидаги Республика суд экспертизаси марказининг Суд-экспертлик илмий-тадқиқот институти фаолияти ташкил этилган. Қуйидагилар институтнинг асосий вазифалари ҳисобланади:

суд экспертизаси соҳасида илмий-тадқиқот ишларини амалга ошириш; давлат суд экспертиза муассасалари ва нодавлат суд экспертиза ташкилотларига илмий-услубий кўмак бериш; суд-экспертлик вазифаларини ҳал қилишнинг илмий асосларини такомиллаштириш ва ягона илмий-методик ёндашувларни ишлаб чиқиш; суд, ҳуқуқни муҳофаза қилувчи органлар, таълим муассасалари ва илмий ташкилотларга услубий ёрдам кўрсатиш; суд-экспертлик фаолиятига фан ва техника ютуқларини жорий этиш бўйича чораларни кўриш; суд экспертизаси соҳасидаги тизимли муаммоларни комплекс ўрганиш ва уларни ҳал этишга доир илмий асосланган таклифлар ва таъсирчан механизмларни ишлаб чиқиш; ҳуқуқни муҳофаза қилувчи органлар ва судларнинг малакали суд экспертиза хулосаларига бўлган эҳтиёжларини доимий равишда ўрганиш орқали суд экспертизасининг янги турлари ҳамда услубиётларини ишлаб чиқиш ва босқичма-босқич амалиётга татбиқ этиш бўйича таклифлар киритиш; суд экспертизаси соҳасига ривожланган ахборот технологиялари ва инновацияларни кенг жорий қилиш бўйича таклифлар ишлаб чиқиш”[5].

[5] Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Х.Сулаймонова номидаги Республика суд-экспертиза марказининг Суд-экспертлик илмий-тадқиқот институти тўғрисида низом. / Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2021 йил 22 ноябрдаги “Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Х.Сулаймонова номидаги Республика суд-экспертиза марказининг Суд-экспертлик илмий-тадқиқот институти фаолиятини ташкил этиш чора-тадбирлари тўғрисида”ги 704-сон қарори.// Қонунчилик маълумотлари миллий базаси, 22.11.2021 й., 09/21/704/1079-сон; 14.07.2022 й., 09/22/385/0643-сон.

Ушбу йўналиш учун муҳим ҳисобланган “Суд экспертизалари ҳисоби тизими” ва “Электрон таълим платформаси” жорий этилиб, аҳолига суд-экспертлик соҳасига доир маълумотларни тезкор етказиш мақсадида “sud ekspert.uz” ахборот портали, экспертиза учун тақдим этилган ашёвий далилларни идентификациялаш дастури фаолиятга татбиқ этилган. Бундан ташқари, ҳуқуқни муҳофаза қилувчи органлар, судлар ва суд экспертиза муассасаларининг ўзаро ҳужжат айланишини ва унинг хавфсизлигини таъминлаш учун тегишли вазирлик ва идоралар билан ҳамкорлигида “E-ekspertiza” электрон ахборот тизими фаолиятимизга татбиқ этилган.

Юқорида таъкидланган амалиётчи суд экспертлари, ҳуқуқни муҳофаза қилувчи органлар вакиллари ҳамда ўқитувчиларнинг ўзаро ҳамкорлигининг устувор йўналишларига қуйидагилар киради:

турли хил тўпламлар, ахборот фондларини мунтазам равишда тўлдириб бориш ва фаолиятда фойдаланиш; суд экспертиза муассасаларининг амалий фаолияти учун криминалистик техниканинг янги (шу жумладан қўшма) ишланмаларини яратиш ва жорий этиш; суд экспертизаларини ўтказишнинг янги усулларини яратиш бўйича қўшма илмий-тадқиқот ишларини ташкил этиш; суд экспертиза муассасалари мутахассисларининг ўзаро амалиёти (стажировкаси) ва семинарларини тизимли ташкил этиш ва ўтказиш; суд-экспертлик фаолиятининг ўзаро ахборот ва услубий таъминотини амалга ошириш ва бошқалар.

Суд экспертизасининг тадқиқот объектларини тавсифлаш, излар ва шикастланишларни ўлчаш, умуман аниқ бир турдаги суд экспертизаларини ўтказишнинг ягона услубиётини ҳамда эксперт хулосасининг ягона тузилишини ишлаб чиқиш учун янги ёндашувлар талаб этилади. Шунингдек, ҳар хил турдаги объектлар (масалан, поябзал, инсон сочлари, тупроқ, бўёқ ва бошқалар) ҳақида маълумотларни ўз ичига олган “Автоматлаштирилган ахборот-қидирув тизимлари (AAQT)”ни яратиш тавсия этилади.

Юқорида таъкидланганлар инновацион технологияларни жорий этиш нафақат суд экспертизалари сифатини оширишга, самарадорлигига ва умуман суд-экспертлик фаолиятини такомиллаштиришга ёрдам беришини, балки жиноятларни очиш ва тергов қилишга ҳам ижобий таъсир кўрсатишини тасдиқлайди.

КИБЕРЖИНОЯТЛАРГА ҚАРШИ КУРАШИШНИНГ ҲУҚУҚИЙ АСОСЛАРИ ТАҲЛИЛИ

Бобомуродов Фарход Боймуротович
Тошкент шаҳар Ички ишлар бош бошқармаси Ягона тезкор бошқарув марказининг масъул ходими, подполковник, ю.ф.ф.д.(PhD),
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси мустақил изланувчиси
farxodbobomurodov663@gmail.com 90-977-19-09

Бугунги кунда кибержиноятларнинг ижтимоий хавфлилиги кун сайин ортиб бормоқда. Ушбу жиноятларга самарали қарши курашишда ваколатли давлат органлари фаолиятини тартибга солувчи норматив-ҳуқуқий асосларни мустаҳамлаш талаб этилиб, норматив-ҳуқуқий ҳужжатларни шартли равишда икки гуруҳга бўлиб ўрганамиз. Булар: миллий норматив-ҳуқуқий ҳужжатлар ва ва халқаро ҳужжатлар.

Норматив-ҳуқуқий ҳужжатлар. Кибержиноятларга қарши курашишда жами 13 та миллий норматив-ҳуқуқий ҳужжатлар (шундан 1 та Конституция, 3 та кодекслаштирилган қонунлар, 2 та жорий қонунлар, 2 та Президент Фармони, 3 та Президент қарорлари, 1 та ДХХни буйруғи ва 1 та Марказий банк қарори)нинг моҳияти таҳлил қилинганида биринчидан, жисмоний ва юридик шахсларнинг мулкий дахлсизлигини таъминланиши Конституция даражасида тартибга солинганлиги; иккинчидан, мазкур масала ниҳоятда долзарблиги ва жиддий бўлганлиги боис, унга самарали қарши курашиш учун кодекслаштирилган ва жорий қонунларнинг мазмунида жавобгарлик ва қоидалар белгиланганлиги, бироқ мазкур миллий қонунларда айрим ҳуқуқий бўшлиқлар (мисол учун жабрланувчига етказилаётган реал зарар миқдоридан келиб чиққиб жавобгарликка тортиш масаласини ҳал этиш) ҳали ҳамон мавжудлиги; учинчидан, кибержиноятларни исботлаш жараёнида электрон (рақамли) далилларни йиғишда бевосита Марказий банк ва унинг ҳудудий бўлинмалари билан ваколатли давлат органлари ҳамкорлик қилиш қонуности ҳужжатлар билан тартибга солингани ўрганишлар жараёнида маълум бўлди.

Қуйида кибержиноятларга қарши курашишда энг асосий ҳисобланган қонун мазмун-моҳиятини кўриб чиқамиз. Жумладан, Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги Қонунида: “телекоммуникация тармоқлари, алоқа каналлардаги тезкор-қидирув тадбирлари тизими киберхавфсизлигини таъминлаш; киберхавфсизлик ҳодисалари юзасидан тезкор-

қидирув тадбирларини, терговга қадар текширувни амалга ошириш; киберхавфсизлик соҳасидаги ваколатли давлат органи фуқаролардан маълумотни, бошқа зарур ҳужжатларни сўраши ва олиши”[1] белгиланганлиги, кибермаконда содир этилаётган жиноятларга қарши курашишда ҳуқуқий асос бўлади.

Ҳозирда Республикамизда содир этилаётган жиноятларнинг қариийб 30 фоизини кибермаконда содир этилаётган жиноятлар ташкил этмоқда. ТҚФни амалга оширувчи ИИОлари ходими кибермаконда содир этилаётган жиноятларнинг олдини олиш ва фош этишда сўров, маълумотлар тўплаш, махсус ТҚТларини ўтказишда фуқароларнинг мурожаат қилиш билан боғлиқ сиёсий ҳуқуқларини бузмаслиги, қонун доирасида уларга моддий, маънавий зарар етказган айбдор шахсларни топишлари талаб этилади. Ахборот технологиялардан фойдаланиб содир этилган жиноятларни олдини олиш ва фош этишда тезкор бўлинмаларнинг фаолиятини аппарат дастурий таъминлаш ишлари бугун қониқарсиз аҳволда. Буни, кибермаконда содир этилаётган ўзгалар мулкини талон-торож қилиш билан боғлиқ жиноятларнинг аксарият фош этилмаётганлиги билан изоҳлашимиз мумкин.

Масалан, 2020-2022 йилларда бундай жиноятлар қарийб 25 баробар ошган бўлиб, ҳозирги кунда фуқароларнинг катта миқдордаги пуллари онлайн тарзда ўғирланмоқда[2]. Эмпирик ҳужжатларни мазмунидан шу аёнки, ҳозирда кибермаконда содир этиладиган жиноятларнинг 48,5 фоизи фош этилмасдан қолмоқда. Бунинг асосий сабаби, жиноятни фош этиш билан боғлиқ излов тадбирлари етарли ташкил этилмаяпти. Идоравий назорат тўғри ташкил этилмаслиги боис, оғир ва ўта оғир турдаги фош этилмаган жиноятлар бўйича махсус иш йиғма жилдлари белгиланган талаблар асосида юритилмасдан, жиноятларни фош этиш чоралари кўрилмасдан келинмоқда[3]. ИИОлари тезкор бўлинмалари ходимлари кибермаконда содир этилаётган жиноятларга қарши курашишда сўров, маълумотлар тўплаш тезкор-қидирув тадбирлари ўтказилиши ушбу жиноятни фош этиш кўрсаткичини оширади.

Сўров ТҚТ ошкора ва ноошкора усулларда ТҚФнинг вазифасини ҳал этиш учун зарур бўлган маълумотларни тўплаш

[1] Ўзбекитон Республикасининг 2022 йил 15 апрелдаги ЎРҚ-764-сон “Киберхавфсизлик тўғрисида”ги Қонуни // http: www.lex.uz. (Электрон манбага мурожаат қилинган вақт: 10.10.2024).

[2] https://www.xabar.uz/huquq/ Бош прокурор мамлакатимиз аҳолисига мурожаат билан чиқди (Электрон манбага мурожаат қилинган вақт: 11.10.2024).

[3] Тошкент шаҳар прокуратурасининг 2023 йил 20 ноябрдаги 16/к-23-сонли “Қонун бузилиши, унинг келиб чиқиш сабаблари ва бунга имконият яратиб бераётган шарт-шароитларни бартараф этиш тўғрисида”ги тақдимномаси.

мақсадида гумонланувчи, айбланувчи, жабрланувчи, гувоҳ ва бошқа шахсларга нисбатан ИИОларида терговга қадар текширувни амалга оширувчи органлар ходимлари томонидан ИИВнинг 2024 йил 26 февралдаги 101-сон “Айрим процессуал ҳаракатлар ёки бошқа тадбирларни ички ишлар органларининг маъмурий биноларида амалга ошириш тартиби тўғрисида” йўриқномасига биноан сўровхоналарда ўтказилади. Вояга етмаган шахс билан сўров ўтказилганида қонуний вакили, педагок ёки психолог иштирок этиши зарур.

Маълумотлар тўплаш ТҚТ ошкора ва ноошкора усулларда ТҚФнинг вазифаларини ҳал этишда ахборот тизимларини ўрганиш, сўровномалар юбориш орқали жисмоний ва юридик шахслар, фактлар, ҳолатлар ҳақида аҳамиятга эга бўлган ахборотни олиш, бошқа ТҚТларига оид маълумотларни умумлаштириш ва таҳлил қилиш мақсадида ўтказилади. Ушбу тадбир тезкор-қидирув қонунчилигида назарда тутилган қонунийлик тамойилига риоя қилган ҳолда амалга оширилиши лозим[4]. Тадбир расмий сўровнома асосида олиниши талаб этилганида ТҚФни амалга оширувчи орган раҳбари имзоси билан тасдиқланган расмий хат билан мурожаат қилиши шарт, оғзаки мурожаат билан маълумот олиниб, терговга қадар текширув материалларни шу маълумотга таяниб қарор қабул қилиши, инсон ҳуқуқ ва эркинликларини бузилишига сабаб бўлади. Мансаб ваколатидан фойдаланиб, маълумотлар расмий сўровнома тақдим этмасдан олиниши маълумот бераётган шахснинг ҳуқуқлари бузилган деб топилади. Амалиётда банк сирига оид маълумотлар тўплаш тадбири вилоятларда терговга қадар текширув вақтида, Тошкент шаҳрида эса, жиноят иши қўзғатилгандан кейин қарор асосида амалга оширилмоқда.

Бу ҳолат ТҚФни идоравий контроль ва прокурор томонидан назорат қилинишида яъни, ушбу тадбирни ўтказишда қонун нормасини ўзи билганича қўллаши кибержиноятларнинг ошиб кетишига, оқибатида эса фуқароларнинг мулкий дахлсизлик ҳуқуқи бузилишига олиб келмоқда. Мазкур тадбирни амалга оширишда кўмаклашувчи фуқарони имкониятидан фойланилганда шахсий хавфсизлигини таъминлаш чораларини таъминлаш керак. ТҚФни амалга оширувчи субъектлар мазкур тадбирни ўтказишга таъсир кўрсатувчи ташкилий муаммоларни ҳал этишда биринчидан, расмий сўровномалар асосида шахс ҳақида маълумотномалар

[4] *Рясов А.В., Мещерин А.И.* О проведении оперативно-розыскного мероприятия «Наведение справок» // Закон и право. 2020. №1. URL: https://cyberleninka.ru/article/n/o-provedenii-operativno-rozysknogo-meropriyatiya-navedenie-spravok (дата обращения: 12.10.2024).

тўплаш; иккинчидан, ТҚФни амалга оширувчи орган раҳбарининг имзоси билан тасдиқланган расмий сўровнома асосида зарур мутахассисларни жалб этиш; учинчидан; ушбу тадбирга ТҚФга ошкора ва ноошкора шаклда кўмаклашувчи фуқаролар жалб этилганида уларнинг ижтимоий ва ҳуқуқий ҳимоясини таъминлаш чоралари кўрилиши, ТҚФда инсон ҳуқуқлари ва эркинликларини таъминлашга имкон беради.

Халқаро ҳужжатлар. Дунёда тинчликни, хавфсизликни таъминлашда давлатларнинг ва барча миллатларнинг ўзаро хамкорлигини ривожлантириш мақсадида 1945 йилда Бирлашган Миллатлар Ташкилоти ташкил этилди. Ушбу халқаро нуфузли ташкилот томондан бугунги кунга қадар универсал, минтақавий, шунингдек жиноятчиликка қарши курашишда ҳамкорлик ва бошқа соҳаларда икки томонлама, кўп томонланма характердаги инсон ҳуқуқлари (ижтимоий-иқтисодий, сиёсий, маданий ва бошқ.)ни таъминлашга оид юздан ортиқ халқаро ҳужжатлар қабул қилинди.

Кибержиноятлар бўйича исботлашни амалга оширишда Ўзбекистон Республикаси ҳукумати билан бошқа давлатлар ўртасида халқаро ҳужжатлар қабул қилинган.

Жумладан, Ўзбекистон Республикаси Ҳукумати билан Бирлашган Араб Амирликлари Ҳукумати ўртасида “Уюшган жиноятчилик, терроризм ва жиноятчиликнинг бошқа хавфли турларига қарши кураш соҳасида ҳамкорлик тўғрисида”ги битимда ҳамкорлик соҳаси сифатида “кибер жиноятлар”(2-м.)[5]; Ўзбекистон Республикаси билан Тожикистон Республикаси ўртасида “Хавфсизлик ва жиноятчиликка қарши курашиш соҳасида ҳамкорлик тўғрисида”ги битимда: “томонлар хавфсизликни таъминлаш ва жиноятчиликка қарши курашиш мақсадида ахборот технологияларидан фойдаланишга оид жиноятлар ва кибержиноятчиликнинг олдини олиш ва уларга қарши курашиш, шунингдек, Томонларнинг миллий манфаатларига қарши ахборот тарқатадиган интернет-сайтлар фаолиятини аниқлаш ва тақиқлаш”(1-м)[6]; Ўзбекистон Республикаси Ҳукумати билан Беларус Республикаси Ҳукумати ўртасида “Жиноятчиликка қарши кураш

[5] Ўзбекистон Республикаси Ҳукумати билан Бирлашган Араб Амирликлари Ҳукумати ўртасида уюшган жиноятчилик, терроризм ва жиноятчиликнинг бошқа хавфли турларига қарши кураш соҳасида ҳамкорлик тўғрисида битим 2008 йил 17 март, Абу Даби (Ўзбекистон Республикаси учун 2012 йил 23 мартдан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 13.10.2024).

[6] Ўзбекистон Республикаси билан Тожикистон Республикаси ўртасида хавфсизлик ва жиноятчиликка қарши курашиш соҳасида ҳамкорлик тўғрисида битим 2018 йил 9 март, Душанбе (Ўзбекистон Республикаси учун 2018 йил 6 июндан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 14.10.2024).

соҳасида ҳамкорлик тўғриси”даги битимда: “ахборот технологиялари, шу жумладан, компьютер-ахбороти соҳасида жиноятлар (1-м)[7]; Ўзбекистон Республикаси Ҳукумати билан Туркманистон Ҳукумати ўртасида “Жиноятчиликка қарши курашда ҳамкорлик қилиш тўғрисида”ги битимда ҳамкорлик йўналишлари сифатида: ахборот технологиялари соҳасида хавфсизликни таъминлаш” (2-м)[8]; Шанхай ташкилотига аъзо бўлган давлатлар Ҳукуматлари орасида “Жиноятчиликка қарши кураш тўғрисида”ги шартномада: “ҳамкорлик соҳаси сифатида ахборот технологиялари соҳасида жиноятлар”(2-м)[9]; Ўзбекистон Республикаси Ички ишлар вазирлиги билан Қозоғистон Республикаси Ички ишлар вазирлиги ўртасида ҳамкорлик ҳақида битимда: “ахборот технологиялари соҳасида ҳамкорликни йўналиши”(2-м)[10]; Ўзбекистон Республикаси Ҳукумати билан Кипр Республикаси Ҳукумати ўртасида “Жиноятчиликка қарши курашда ҳамкорлик қилиш тўғрисида”ги битимда: “ҳамкорлик соҳалари сифатида ахборот технологиялари соҳасидаги жиноятлар”(2-м.)[11]; Ахборот технологиялари соҳасидаги жиноятларга қарши курашишда Мустақил Давлатлар Ҳамдўстлиги иштирокчи давлатларининг ҳамкорлик тўғрисидаги битимда: “ахборот технологиялари соҳасидаги жиноятларга қарши самарали курашни таъминлашда ахборот технологиялари соҳасидаги жиноятларга қарши курашишда томонларнинг ўзаро келишилган ҳаракатлари муҳим зарурат эканлигига ишонч ҳосил қилган ҳолда, ахборот технологиялари соҳасидаги жиноятларга қарши курашишда томонларнинг ҳуқуқни муҳофаза қилиш органларининг ҳамкорлиги учун ҳуқуқий асос яратилганлиги”(2-м.)[12]; Ўзбекистон

[7] Ўзбекистон Республикаси Ҳукумати билан Беларусь Республикаси Ҳукумати ўртасида жиноятчиликка қарши кураш соҳасида ҳамкорлик тўғрисида битим 2008 йил 19 июнь, Минск (2008 йил 24 декабрдан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 15.10.2024).

[8] Ўзбекистон Республикаси Ҳукумати билан Туркманистон Ҳукумати ўртасида жиноятчиликка қарши курашда ҳамкорлик қилиш тўғрисида битим 2009 йил 25 февраль, Тошкент (Ўзбекистон Республикаси учун 2009 йил 20 ноябрдан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 16.10.2024).

[9] Шанхай ташкилотига аъзо бўлган давлатлар Ҳукуматлари ўртасида жиноятчиликка қарши курашишда ҳамкорлик тўғрисида шартнома 2010 йил 11 июнь (2012 йил 11 январдан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 17.10.2024).

[10] Ўзбекистон Республикаси Ички ишлар вазирлиги билан Қозоғистон Республикаси Ички ишлар вазирлиги ўртасида ҳамкорлик тўғрисида битим 2013 йил 14 июнь, Тошкент (2013 йил 14 июндан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 18.10.2024).

[11] Ўзбекистон Республикаси Ҳукумати билан Кипр Республикаси Ҳукумати ўртасида жиноятчиликка қарши курашда ҳамкорлик қилиш тўғрисида битим 2012 йил 5 апрель, Тошкент (2015 йил 27 февралда кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 19.10.2024).

[12] Ахборот технологиялари соҳасидаги жиноятларга қарши курашда Мустақил давлатлар ҳамдўстлиги иштирокчи давлатларининг ҳамкорлик тўғрисидаги битим Душанбе, 2018 йил 28 сентябрь (Ўзбекистон Республикасида 2020 йил 12 мартдан кучга киради) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 20.10.2024).

Республикаси билан Испания қироллиги ўртасида “Жиноятчиликка қарши курашда ҳамкорлик қилиш тўғрисида”ги битимда: “ахборот технологиялари соҳасидаги жиноятлар ҳамкорликнинг йўналишларидан бири экани”(2-м.)[13] баён этилган бўлиб, ушбу қоидаларнинг ҳуқуқий тартибга солинганлиги мазкур йўналишда халқаро ҳамкорлик қилиш учун ҳуқуқий асос бўлиб хизмат қилади.

Таҳлил қилинган 9 та халқаро ҳужжатларнинг мазмунида асосан “*ахборот технологиялари соҳасидаги жиноятлар*”қоидаси ҳамкорликнинг йўналишларидан бири сифатида белгиланиб, бизнинг фикримизча, “*ахборот технологиялари соҳасидаги кибержиноятлар*” қоидаси билан ушбу халқаро ҳужжатлар мазмунига ўзгартириш киритилиши тўғри деб ҳисоблаймиз.

Фуқароларнинг ҳуқуқлари ва эркинликларини таъминлашда ИИОлари тезкор бўлинмалари томонидан кибермаконда содир этилаётган жиноятларга қарши курашда тезкор-қидирув тадбирларни ўтказишнинг самарадорлигини оширишда қуйидагилар таклиф этилади:

биринчидан, ТҚФни амалга оширувчи органлар, Олий суд, Марказий банк ўртасида қўшма қарор ишлаб чиқилиб, банк пластик карталарини зудликда блоклаш ва ўғирланган электрон пулларни дарҳол музлатилиши ва Республикамиз ҳудудидан чиқиб кетмаслик чораларини кўриш лозим;

иккинчидан, ҳозирги кунда Республикамиз ҳудудида кибержиноятларга қарши курашиш масаласи энг долзарб муаммоларидан бири бўлганлиги боис, жисмоний ва юридик шахснинг мулкий дахлсизлик ҳуқуқи бузилишини олдини олиш лозим. Ушбу турдаги ҳуқуқбузарликлар 2019 йилда 122 та; 2020 йилда 723 та; 2021 йилда 2553 та; 2022 йилда 5277 тани ташкил этиб, тўрт йил ичида мурожаатлар сони 43 баробарга ошган. 2023 йилнинг 9 ойида 8734 та мурожаатлар келиб тушган бўлиб, фуқароларга етказилган моддий зарарнинг миқдори уч йилда 372 миллиард 800 млн. сўмни ташкил этган. Киберҳужумлар асосан қўшни давлатларнинг ҳудудида истиқомат қилаётган шахсларни хакерлик билан шуғулланиши натижасида юзага келиб, уларнинг фаолиятига тўлиқ чек қўйишда халқаро ҳамкорлик ишини амалга ошириш. Ахборот технологиялари соҳасидаги жиноятларга қарши

[13] Ўзбекистон Республикаси билан Испания Қироллиги ўртасида жиноятчиликка қарши курашда ҳамкорлик қилиш тўғрисида битим 2013 йил 5 ноябрь, Мадрид (Ўзбекистон Республикаси учун 2022 йил 10 февралдан кучга кирган) // URL: http:// www.lex.uz (Электрон манбага мурожаат қилинган вақт: 21.10.2024).

курашишнинг самарадорлигини оширишда Ўзбекистон Республикаси Ҳукумати билан ривожланаётган хусусан, Жанубий Корея, Япония, Хитой, Германия, Болгария, Австрия, Қувайт, Миср, Саудия Арабистони, Кипр ва Испания давлатлари билан *“Ахборот технологиялари соҳасидаги жиноятларга қарши курашишда ҳамкорлик тўғрисида*” битимларни қабул қилиш ва ҳамкорликда мақсадли ва манзилли чора-тадбирларни белгилаш лозим;

учинчидан, ТҚФни рақамлаштириш орқали тезкор бўлинмаларнинг кундалик иш фаолиятини онсон ва қулай бўлишига катта эътибор қаратиш, масалан барча журналларни, тезкор карточкаларни электрон шаклда юритиш ва ўзаро ёзишмаларни махсус ёпиқ локал тармоқлар асосида юборилишини йўлга қўйиш. ИИВнинг соҳавий хизматлари ҳамда бошқа давлат органлари билан логин ва парол асосида электрон почта орқали ёзишмаларни амалга ошириш керак. Статистик маълумотларнинг таҳлилига кўра, сўнгги 5 йилда Республикамиз ҳудудида кибермаконда содир этилаётган жиноятларнинг салмоғи жуда ошиб бораётганлиги туфайли, тезкорлик билан фуқароларнинг банк пластик карталарининг ҳисобидан пул ечиб олинишини зудликда тўхтатилиши учун банк муассасалари билан электрон шаклда ёзишмаларни амалга ошириш лозим, ҳозирда ушбу ҳаракатлар жиноят иши қўзғатилгандан кейин ўтказилаётганлиги тезкор ҳаракатланишга салбий таъсир кўрсатмоқда, оқибатда жабрланган фуқароларга етказилган мулкий зарар қопланмасдан қолишига олиб келмоқда.

Бундай салбий ҳолатларнинг олдини олиш учун банк сирига оид маълумотлар тўплаш ТҚТни электрон шаклда терговга қадар текширув вақтидан бошлаб яъни, ИИОларига ариза ва хабар келиб тушган заҳоти амалга оширишни таъминлашда ИИО тезкор бўлинмаларининг қуйи тизими (шаҳар ва туманлар)да “Е ИИО ТҚФ” махсус дастурини яратиш ва шу платформа асосида банк, прокуратура ва суд органларининг ходимлари билан логин, парол асосида электрон ёзишмаларни йўлга қўйилиши, ТҚФда инсон ҳуқуқларини таъминлашда ҳар томонлама фойдали амалиёт бўлади. ТҚФда инсон ҳуқуқлари ва эркинликларини таъминлашда ИИОлари тезкор хизматида ахборот таҳлил фаолияти самарали ташкил этилиши зарур.

Бунинг учун соҳада таҳлил иши билан шуғуланадиган тезкор ходим сунъий интелект технологияларининг имкониятларидан

унумли фойдаланишлари[14] (масалан, жиноятларнинг содир этиш вақти, шароити, жойи, усуллари, шахси ҳақида маълумотларнинг базаларини яратиш), шу орқали, ТҚФ соҳада айниқса, кибержиноятларга қарши курашишда, жамоат жойларида, хусусий, давлат объектларида, ўтган йилларда содир этилиб фош этилмасдан қолаётган мулкий турдаги жиноятларни фош этишда тўғри қарорлар қабул қилиниб, ТҚФнинг вазифалари ижобий ҳал этилишига эришилади.

Хулоса қилиб айтганда, фуқароларнинг ҳуқуқлари ва эркинликларини таъминлашда ИИОлари тезкор бўлинмалари томонидан кибермаконда содир этилаётган жиноятларга самарали қарши курашишда ушбу бўлинмаларнинг моддий базасини такомиллаштириш, ҳамкорликни тўғри ташкил этиш лозим.

СУД ИШЛАРИНИ ЮРИТИШДА СУНЪИЙ ИНТЕЛЛЕКТДАН ФОЙДАЛАНИШНИНГ ТУШУНЧАСИ, АҲАМИЯТИ, ЗАРУРАТИ ВА РЕТРОСПЕКТИВ ТАҲЛИЛИ

Уринбоева Мухлиса Маъруфовна
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси мустақил изланувчиси

Абдуфаттоев Йўлдошали Фарходжон Ўғли
Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси магистратураси тингловчиси

Аннотация: *Мақолада суд ишларини юритишда сунъий интеллектдан фойдаланишнинг тушунчаси, аҳамияти, зарурати ва ретроспектив таҳлили кўриб чиқилган. Мақолада шунингдек сунъий интеллектни суд ишларини юритишда қўллаш заруриятининг асосий омиллари аниқланиб, муайян хулосалар илгари сурилган.*

Калит сўзлар: *суд ҳокимияти, суд тизими, суд ишларини юритиш, сунъий интеллект, ҳуқуқий асос, халқаро ҳужжатлар, хорижий тажриба, такомиллаштириш.*

Аннотация: *В статье рассматриваются понятие, значение, необходимость и ретроспективный анализ использования искусственного интеллекта при ведении судебного разбирательства. Также в статье обозначены основные факторы необходимости использования искусственного интеллекта в судебном разбирательстве и сделаны определенные выводы.*

[14] *Акимов А.Б.* Жамоат хавфсизлигини таъминлашда техника воситаларини қўллашнинг ўзига хос жиҳатлари // Academic research in educational sciences. 2022. №1. URL: https://cyberleninka.ru/article/n/zhamoat-havfsizligini-taminlashda-tehnika-vositalarini-llashning-ziga-hos-zhi-atlari (дата обращения: 22.04.2024).

Ключевые слова: *судебная власть, судебная система, судебная система, судебное разбирательство, искусственный интеллект, правовая основа, международные документы, зарубежный опыт, совершенствование.*

Abstract: *The article examines the concept, importance, necessity and retrospective analysis of the use of artificial intelligence in conducting court proceedings. The article also identifies the main factors of the need to use artificial intelligence in court proceedings and puts forward certain conclusions.*

Keywords: *judiciary, judicial system, court proceedings, artificial intelligence, legal basis, international documents, foreign experience, improvement.*

XXI асрда инсоният турмуш тарзининг ўзгариб бориш жараёнлари сунъий интеллект (artificial intelligence – AI) нинг реалликка айланиб, ҳаётимизга кириб келиши билан ўзининг энг юқори чўққисига чиқди. Турли технологиялар инсонларнинг меҳнатини енгиллиштириш баробарида, уларнинг қўлидан ишини олди. Дастлаб ёзишмалардаги имловий хато ва камчиликларни текширадиган ақлли ахборот технологиялари ҳаётимизга кириб келди. Бугунги кунда аэропортларда юзни таниш орқали юртимизга кириб келаётган саёҳатчиларни текшириш имкони яратилди. Технологиялар хатто борадиган манзилимизга қандай қилиб тез етиб олиш, борадиган манзилимиздаги мавжуд тўсиқлар ва тирбандликлар бўйича сўралмаган маслаҳатларни беради. Планшет ва мобил телефонимиз орқали саволларимизга самимий жавоблар оламиз, қўполлашсак бизни қўполлашмасликка чақиради.

Ўзбекистон Миллий ахборот агентлиги замон билан ҳамнафас бўлган ҳолда сунъий интеллект асосида “Собира Холдорова” номли махсус робот-мухбир яратди. Мазкур мухбир тўққиз тилда (ўзбек, инглиз, рус, француз, араб, хитой, немис, испан, қозоқ) расмий ахборотлар ва тезкор янгиликларни етказиб туриши, синов тарзида ишга туширилган сунъий интеллект видео репортажлар тайёрлаш кўламини босқичма-босқич кенгайтириб бориши ҳақида маълумотлар берилган.[15] Дарҳақиқат, мутахассислар ҳам сунъий интеллект медиа соҳасига шиддат билан кириб келганлигини таъкидламоқда.[16]

Сунъий интеллект — бу компьютер тизимларига ёки машиналарга одамлар каби “ақлли” вазифаларни бажариш қобилиятини бериш учун ишлатилган технологиялар ва усуллар мажмуасидир. Буларга кўпинча тушуниш, ўрганиш, хулоса чиқариш,

[15] Сунъий интеллект ёрдамида яратилган ЎзА мухбири иш бошлади // https://uza.uz/uz/posts/suniy-intellekt-yordamida-yaratilgan-oza-muxbiri-ish-boshladi_626944

[16] Сунъий интеллект қанчалик хавфли ёки фойдали? // https://kun.uz/kr/news/2024/01/09/suniy-intellekt-qanchalik-xavfli-yoki-foydali

ва қарорлар қабул қилиш киради. Сунъий интеллектнинг асосий мақсади инсон ақлига хос бўлган вазифаларни автоматлаштириш ва уларни компьютер ёки роботлар ёрдамида бажаришдан иборатдир.

Бирлашган Миллатлар Ташкилоти Бош Ассамблеяси 2024 йил 21 март куни “Барқарор ривожланиш учун хавфсиз, ҳимояланган ва ишончли сунъий интеллект тизимларининг имкониятларидан фойдаланиш” номли А/78/Л.49-сонли резолюцияни қабул қилди.[17]

БМТ Бош Ассамблеясининг сунъий интеллект бўйича юқоридаги резолюциясида ҳеч ким сунъий интеллектдан тинчликка таҳдид солиш ёки инсон ҳуқуқларини поймол этиш учун фойдаланишга ҳақли эмаслиги алоҳида уқтирилган. Сунъий интеллектни тартибга солиш ва инновациялар – бир-бирини инкор қилмаслиги, аксинча, ўзаро уйғун ҳамда чамбарчас боғлиқ тушунчалар эканлиги таъкидланган.

Сунъий интеллектни танқид қилувчиларнинг фикрича эса, тармоққа уланган сунъий интеллект инсон автономияси, ваколатлари ва имкониятларига таҳдид солади.[18] Технологиялар тараққиёти интернетдаги шусиз ҳам оғир вазият янада ёмонлашишига, яъни одамлар осонгина ишонадиган ғирт ёлғон ахборот ҳажмининг ҳаддан ортиқ кўпайишига олиб келади. Бунинг оқибатида жамоатчиликнинг янгиликлар ва ахборотга бўлган ишончига узил-кесил путур етади.

Бироқ шундай бўлса-да, сунъий интеллект муайян вазифаларни бажаришда инсон хатти-ҳаракатига тақлид қилишга қодир бўлган тизим ёки технология бўлиб, олинган маълумотлардан фойдаланиб аста-секин мукаммаллашиб боради. Умуман олганда сунъий интеллект формат ҳам, функция ҳам эмас, балки бу жараён бўлиб, маълумотларни йиғиш, таҳлил қилиш кабиларни ўз ичига олади.[19]

Ўзбекистонда сунъий интеллект технологияларини жадал жорий этиш ва уларни мамлакатимизда кенг қўллаш, рақамли маълумотлардан фойдаланиш имкониятини ва уларнинг юқори сифатини таъминлаш борасида қатор ишлар амалга оширилмоқда Бинобарин, Ўзбекистон Республикаси Президентининг 2021 йил 17 февралдаги “Сунъий интеллект технологияларини жадал жорий этиш учун шарт-шароитлар яратиш чора-тадбирлари тўғрисида”ги Қарорида “Сунъий интеллектни ривожлантириш стратегияси”ни

---

[17] https://www.undocs.org/Home/Mobile?FinalSymbol=A%2F78%2FL.49&Language=E& DeviceType=Desktop&LangRequested=False

[18] Artificial Intelligence and the Future of Humans // https://www.pewresearch.org /internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/

[19] Абдуқундузова Н. Сунъий интеллект – технологик ривожланиш асоси // https://yuz.uz /news/suniy-intellekt--texnologik-rivojlanish-asosi

ишлаб чиқиш ва 2021 йил ноябрда Норматив-ҳуқуқий ҳужжат лойиҳасини Вазирлар Маҳкамасига киритиш назарда тутилган.[20]

Дарҳақиқат, бу борада хорижий давлатлар тажрибаси таҳили шуни кўрсатадики, масалан, Ирландиянинг Accenture компанияси томонидан олиб борилган таҳлиллар G20 рўйхатдаги давлатларда (АҚШ, Буюк Британия, Германия, Франция, Япония ва Корея Республикаси каби) 2035 йилга қадар сунъий интеллектнинг ўсиш суръати 2 маротабага ортиши таъкидланмоқда.[21] Бу албатта, ушбу давлатлар учун сунъий интеллект иқтисодий ривожланиш ва давлат бошқарувини такомиллаштиришдаги асосий воситаларидан бири эканлигини эътироф этади.

2017 йил март ойида Европа давлатларининг йирик тижорат компания раҳбарлари орасида ўтказилган сўровномада уларнинг қарийб 70 фоизи ўз фаолиятларида сунъий интеллектни кенг қўллаётганликлари ёки сунъий интеллектни қўллаш имкониятларини баҳолаётганликларини эътироф этишган.

Маълумки, бугунги кунга қадар жаҳон саҳнасида сунъий интеллектни ривожлантириш бўйича 7 та халқаро даражадаги ҳамкорлик келишувлари ва 50 дан ортиқ миллий стратегиялар қабул қилинган.[22]

2017 йилга нисбатан сунъий интеллектни ривожлантириш стратегияларини эълон қилган мамлакатлар сони 2020 йил бошига келиб 8 маротаба ортди. 2017 йил Канада, Сингапур, Бирлашган Араб Амирликлари, Финландия, Япония ва Хитой давлатларида сунъий интеллект стратегиялари ишлаб чиқилди. 2019 йилда бу рўйхатдан Италия, Тунис, Буюк Британия, АҚШ, Швеция, Мексика, Европа иттифоқи, Кения, Дания, Франция, Австралия, Корея Республикаси, Ҳиндистон ва Германия каби кўплаб бошқа давлатлар ҳам ўрин эгаллади.

Европа давлатларида сунъий интеллектни ривожлантириш стратегиялари бор бўлишига қарамай, мавжуд куч ва имкониятларни бирлаштириш ва жаҳон ҳамжамиятида юқори натижаларни қўлга киритиш мақсадида 2018 йил 10 апрель санасида 25 та Европа давлатлари Сунъий интеллектни ривожлан-тиришдаги ҳамкорлик Декларациясини имзолади.[23] Унда Европанинг сунъий интеллект

[20] Ўзбекистон Республикаси Президентининг 2021 йил 17 февралдаги “Сунъий интеллект технологияларини жадал жорий этиш учун шарт-шароитлар яратиш чора-тадбирлари тўғрисида”ги Қарори // https://president.uz/uz/lists/view/4195

[21] AI research how AI boosts industry profits and innovation

[22] HolonIQ and source government strategy and policy papers

[23] https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

технологияларидаги салоҳиятини ошириш, сунъий интеллектни ўзлаштириш, ижтимоий-иқтисодий глобал чақирувларга ҳамкорликда сунъий интеллект технологиялари асосида қарши курашиш ва сунъий интеллект доирасида ҳуқуқий ва ахлоқий асосларни ишлаб чиқиш ва сунъий интеллект ютуқларини давлат бошқарувига йўналтириш асосий мақсад қилинган.

Сунъий интеллектнинг инсоният равнақи учун хизматини ошириш ва ривожлантириш мақсадида 2018 йил май ойида 10 та давлат иштирокида Шимолий Болтиқ ҳудудида Сунъий интеллект декларацияси имзоланди.[24] Декларацияда сунъий интеллект истиқболларидан бизнес ва давлат бошқарувида фойдаланиш имкониятларини кенгайтириш мақсадида билим, кўникма ва маҳоратни ошириш; ҳудудларда бизнес ва давлат хизматлари учун намунавий хизматларни ташкил этиш мақсадида сунъий интеллектда қўлланиладиган маълумотлар очиқлигини таъминлаш; сунъий интеллектнинг қўлланилиш соҳалар ва меъёрларини белгиловчи ахлоқий ва шаффоф кўрсатмалар, стандартлар ва низомларни ишлаб чиқиш; сунъий интеллектда фойдаланиладиган барча инфратузилмаларнинг жумладан, зарурий ускуна ва қурилмалар, дастурий таъминотлар ҳамда маълумотларнинг ишончлилиги, хавфсизлиги ва даҳлсизлигини таъминлаш белгиланган.

2019 йил июль ойида Японияда G20 давлатларнинг бўлиб ўтган учрашувида “G20 Сунъий Интеллект тамойиллари” сунъий интеллектдан фойдаланишнинг тамойиллари бўйича келишув имзоланди.[25] Келишув сунъий интеллектдан фойдаланишда адолат ва шаффофлик тамойилларига таянилиши шунингдек, қонун устуворлиги, шахсий қадриятлар, тенглик ва халқаро меҳнат ҳуқуқларини ҳурмат қилишга чақиради.

Германия Федератив Республикаси сунъий интеллектни ривожлантириш эртанги кун имконият ва муваффақият эшикларининг “олтин калити” эканлигига алоҳида урғу берган ва ҳозирги кунга қадар сунъий интеллект соҳасидаги 15 та сиёсий ташаббусларни кетма-кет амалга ошириб келмоқда.[26]

2019 йил июнь ойида Америка Қўшма Штатлари (АҚШ) Миллий сунъий интеллект илмий тадқиқот ва ривожлантириш стратегик

[24] https://www.norden.org/en/declaration/ai-nordic-baltic-region
[25] https://www.g20-insights.org/related_literature/g20-japan-ai-principles/
[26] OECD.AI (2020), powered by EC/OECD (2020), STIP Compass database, accessed on 21/02/2020, http://oecd.ai.

режасини маъқуллади.[27] АҚШда бугунги кунга қадар сунъий интеллект соҳасини ривожлантиришга қаратилган жами 36 та сиёсий ташаббуслар рўйхатга олинди.

Қозоғистон Республикаси ҳозирга қадар сунъий интеллект соҳасини ривожлантиришда ўзининг миллий стратегиясига эга бўлмаса-да, бироқ Марказий Осиё давлатлари ичида Сунъий интеллект соҳасини ривожлан-тиришда дунё ҳамжамияти томонидан алоҳида эътироф этилаётган давлатдир.

2019 йилдан Назарбаев Университети томонидан дунёнинг етакчи сунъий интеллект технологиялари ечимларини ишлаб чиқувчиларини жалб этиш мақсадида, Сунъий интеллект илмий тадқиқот ва ривожлантиришни қўллаб-қувватлаш жамғармаси жорий этилди.[28] Жамғарманинг асосий мақсади Қозоғистонда таълим, илмий тадқиқот, маданият, техника, инновация, бошқарув соҳалари ва бошқа манфаатли соҳаларда сунъий интеллектни ривожлантиришдан иборат.

Сунъий интеллект замонавий ҳуқуқий тизимда ўта муҳим ва кўп қиррали роль ўйнайди. Унинг таъсири ва имкониятлари турли жабҳаларда ўз аксини топади, бу эса ҳуқуқий соҳадаги амалиёт ва тадқиқотларда янги имкониятлар ва чегараларни очиб беради.

Сунъий интеллект унга кўмаклашувчи дастурлар орқали ҳуқуқий ҳужжатларни тезкор ва самарали равишда таҳлил қилиш имкониятини яратади. Масалан, ҳужжатларнинг автоматик индексацияси ва тегишли қарорлар ёки қонунлар билан боғлиқ муҳокамаларни топиш осонлашди. Бу норматив-ҳуқуқий ҳужжатларни тайёрлаш жараёнини сезиларли даражада тезлаштиради ва хато эҳтимолини камайтиради.

Айрим юрисдикцияларда сунъий интеллект алгоритмлари айрим турдаги ҳуқуқий масалаларда қарор қабул қилиш жараёнига киритилган. Масалан, шартнома шартларини автоматик баҳолаш ёки кредит беришда қарз олувчининг қарзга қайтариш имкониятларини таҳлил қилиш шулар жумласидандир.

Ҳозирги кунда суд ва ҳуқуқни муҳофаза қилиш фаолиятида сунъий интеллект имкониятларидан фойдаланиш масаласи ҳар кунгидан кўра долзарб бўлиб келмоқда. Сунъий интеллект имкониятларидан суд ишларини юритиш жараёнларини автоматлаштиришда, шу жумладан, айрим турдаги ишларнинг

---

[27] https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Deve-lopment-Strategic-Plan-2019-Update-June-2019.pdf

[28] https://nu.edu.kz/ru/zakupki/kf-fond-podderzhki-issledovanij-razrabotok-v-sfere-iskusstven-nogo-intellekta

дастлабки таҳлилини ўтказишда фойдаланилиши мумкин. Бу судьяларга ва прокурорларга ишлар бўйича маълумотларни тизимлаштириш ва тезкор баҳолашга ёрдам беради.

DailyMail берган ҳабарга кўра, 2019 йилнинг февраль ойида Буюк Британияда бўлган суд тинглови тарихга киради, чунки унда илк бор судланувчига сунъий интеллект, яъни робот маслаҳат бериб турди. DoNotPay компанияси яратган дунёда биринчи робот-адвокат судланувчининг смартфонида ишлайди ва мажлис чоғида мижозига ўзини ҳимоя қилиши учун нима дейиши кераклигини айтиб туради.[29]

Лекин шу билан бирга судда ишларни кўриш жараёнида сунъий интеллектни қўллаш ва унинг хавф-хатарларини ўрганиш долзарб ҳисобланади.

Шу ўринда юридик адабиётларда судларда ишларни кўриш жараёнида сунъий интеллектни қўллаш борасида турли фикрлар ва баҳс-мунозаларлар илгари суриб келинмоқда. Масалан, 2019 йилда Tashkent Law Spring халқаро юридик форумида маъруза қилган Россия Федерацияси Адвокатлар палатаси президенти Юрий Пилипенко юридик хизматлар бозори инсон билан робот ўртасида тақсимланаётгани, қатор ҳуқуқий процесслар аллақачон юристлар иштирокисиз кечаётгани ҳақида фикр юритар экан, шундай деган эди: “Никоҳ бекор қилингани ҳақидаги ҳужжатни олиш учун интернетда бир нечта “дарча”да бланка тўлдириш кифоя қиляпти. Аҳоли билан ишлайдиган кўплаб йирик корпорациялар яқин йилларда аксарият юристларини бўшатиб юборади. Масалан, банклар ипотека кредитларию шартномалар тўлдириш билан шуғулланаётган мутахассислардан воз кечиши аниқ бўлиб қолди. Биз ишимизни роботларга бериб, бекор қолмаслигимиз керак. Акс ҳолда цивилизация сифатида ҳалокатга учраймиз”.[30]

Бироқ бошқа бир манбаларда суд ишларини юритишда сунъий интеллектни жорий этиш муҳим аҳамият касб этиши, сунъий интеллект суд қарорларини чиқаришда учрайдиган хатолар сонини камайтириш орқали суд қарорларининг асослилигини янги даражага олиб чиқишга ва суд иш юкламасини енгиллаштиришга хизмат қилиши ҳақида фикрлар илгари сурилади.[31] Бошқа бир

[29] Robot lawyer takes its first court case: Hearing next month will see the defendant get advice from artificial intelligence using a smartphone app // https://www.dailymail.co.uk/sciencetech /article-11599805/Robot-lawyer-takes-case-Hearing-month-defendant-advice-AI.html

[30] Юристларнинг ўрнини роботлар эгалламоқда. Бу биз учун ҳалокатлидир // https://advokatnews.uz/xabar/1513.html

[31] Хабибуллаев Д.Ю. Фуқаролик суд ишларини юритишни рақамлаштириш истиқболлари: миллий амалиёт ва хорижий тажриба таҳлили // Ўзбекистон Республикаси Олий суди расмий сайти. https://old.sud.uz/0811-3/

мутахассисларнинг фикрича, ахборот технологиялари ва сунъий интеллект ҳозирда суд ва ҳуқуқни муҳофаза қилувчи органларда ҳам кенг фойдаланилаётган инновацияларда ҳисобланади. Ушбу технологиялар суд ва бошқа органларнинг самарали, қонуний ва масъулиятли фаолият юритишида, уларнинг коррупцияга қарши курашда кучли қуроли сифатида фойдалана олишида муҳим рол ўйнамоқда. Уларнинг фикрича, сунъий интеллект суд ишларини кузатиш, ҳужжатларни бошқариш ва режалаштириш жараёнларини яхшилайди, манипуляция ва порахўрлик имкониятларини минималлаштиради. Сунъий интеллектга асосланган алгоритмлар судяларга далилларни баҳолашда, адолатли ва холис қарор қабул қилишни таъминлашда ҳам ёрдам бера олади.[32]

Хатто, айрим мутахассислар халқаро тажрибада сунъий интеллект қонун ижодкорлиги жараёнида ҳам фаол фойдаланиб келинаётганлигини эътироф этадилар.[33] Масалан, Нидерландия Вакиллар палатаси Speech2Write тизимини жорий қилди, бу эса Парламентнинг Ҳисобот идорасига овозни матнга айлантириш ва йиғилишларнинг ёзма баённомаларини автоматик таҳрирлаш имкониятини беради.[34] Худди шундай, 2020 йилнинг кузидан Эстония парламенти Таллин технология университети технологик ишланмалари асосида Эстониянинг Finestmedia IT компанияси томонидан яратилган HANS сунъий интеллект тизимидан ҳам фойдаланмоқда. Ялпи мажлислар стенограммаларини тайёрлаш учун нутқ ва маърузачини аниқлаш тизими қўлланилади.[35]

АҚШ Конгрессида қонун лойиҳалари, тузатишлар ва амалдаги қонунлар ўртасидаги фарқларни аниқлаш жараёнини автоматлаштириш учун сунъий интеллект технологияларидан фойдаланилади. Ушбу восита қонун лойиҳаларидаги ҳаволаларни шарҳлаши, тегишли қоидаларни чиқариши ва тузатишлар бўйича кўрсатмаларга амал қилиши мумкин.[36]

---

[32] Қодиров М.И. Ахборот технологиялари ва сунъий интеллектнинг коррупцияга қарши курашдаги ютуқлари: хорижий давлатлар илғор тажрибалари таҳлили // https://universalpublishings.com/index.php/jusr/article/download/1084/2072/1049

[33] Ҳотамов Ҳ.С. Сенат фаолияти самарадорлигини оширишда рақамли технологиялар ва инновацион ёндашувлардан фойдаланиш истиқболлари// Юрист ахборотномаси | Вестник юриста | Lawyer herald. 2023. №5. Б. 18-19.

[34] Васильева Т. А. Внедрение информационных технологий в парламентскую деятельность // Вестник Университета имени ОЕ Кутафина. – 2022. – №. 9 (97). Б.93-101

[35] Estonian parliament uses speech recognition technology to create verbatim records // e-Estonia. 24 September 2020. // URL: https://e-estonia.com/estonian-parliament-usesspeech-recognition-technology-to-create-verbatim-records.

[36] Artificial Intelligence: Innovationin Parliament // Innovation tracker. 2020. Is. 4. InterParliamentary Union. // URL: https://www.ipu.org/innovation-tracker/story/artificialintelligence-innovation-in-parliaments.

Юқоридагилардан келиб чиққан ҳолда ҳамда бошқа таҳлилларимиз сунъий интеллектни суд ишларини юритишда қўллаш заруриятининг қуйидаги асосий омиллари мавжудлиги ҳақида хулоса қилиш мумкин:

Биринчидан, самарадорликни ошириш имконияти яратилади. Сунъий интеллект жуда катта ҳажмдаги маълумотларни тез фурсатда таҳлил қилиб чиқади. Бу эса суд ишларини ўз вақтида, тезкорлик билан кўриб чиқиш ва ҳужжатларни тайёрлаш жараёнларини жадаллаштиради. Ҳуқуқий ҳужжатлар ва иш материлларини тез фурсатда топиш ва таҳлил қилиш имконияти орқали суд ишларини кўриш муддатлари қисқаради.

Иккинчидан, адолатни таъминлашга кўмаклашилади. Сунъий интеллект-нинг имкониятлари инсон омили таъсирини камайтиришга ёрдам беради. Бунинг натижасида, суд қарорлари кўпроқ объектив ва ҳаққоний бўлиши таъминланади.

Учинчидан, суднинг иш юритишида мавжуд бўлган маълумотлар ва иш материалларининг аниқлиги таъминланади. Маълумки, суд ишларини юритишда тўғри ва янгиланган маълумотлардан фойдаланиш муҳим аҳамият касб этади. Сунъий интеллект алгоритмлари инсонга хос бўлган хатоларни камайтириши мумкин, бу эса суд қарорларини қабул қилишда аниқликни оширади.

Тўртинчидан, суд харажатларини камайтиришга имкон беради. Сунъий интеллектдан фойдаланиш орқали суд жараёнларини иқтисодий жиҳатдан тежамкор бўлишига эришилади. Суд ишларини юритишдаги автоматлаштириш жараёнлари инсон ресурсларига бўлган эҳтиёжни қисқартириши мумкин, бу эса суд тизими харажатларини сезиларли даражада камайтиради.

Бешинчидан, хавфсизлик ва махфийликни таъминлашга хизмат қилади. Сунъий интеллект маълумотларни шифрлаш ва ҳимоя қилиш тизимларини такомиллаштириш орқали суд ишлари билан боғлиқ маълумотларнинг махфийлигини таъминлашга ёрдам беради.

Шундай экан, хулоса қилиб айтиш мумкинки, суд ишларини юритишда сунъий интеллектни қўллаш судлар фаолиятида умумий самарадорликни ошириш, адолатни таъминлаш ва инсон омили таъсирини камайтириш учун муҳим қадам ҳисобланади.

XORIJIY MAMLAKATLARDA MAYNING VA KRIPTO AKTIVLARDAN FOYDALANISHNING HUQUQIY TARTIBI

Abduraxmanov Muzaffar Mamurovich,
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi magistraturasi tinglovchisi

Mayning tushunchasi va huquqiy tabiatini aniqlash butunlay boshqacha yondashuvlarga asoslangan bo'lishi mumkin, bu bugungi kunda turli mamlakatlar qonunchiligida kuzatiladi. Jahon amaliyotidagi bunday yondashuvlarni tahlil qilish mayningni huquqiy tartibga solishning huquqiy tabiatining turli jihatlariga qarab turli darajalarda shakllangan bir nechta qonunchilik modellarini aniqlash imkonini beradi.

Mayningning huquqiy tabiatining birinchi jihati uning ruxsat etilgan yoki taqiqlangan faoliyat mezoni bo'yicha malakalanishidir. Ushbu mezondan kelib chiqib, qonunchilik modellarining uchta guruhini ajratish mumkin. Birinchi guruh Kanada, AQSh, Avstraliya, Yaponiya, Shveytsariya, shuningdek, Yevropa Ittifoqi kabi mamlakatlar uchun xos bo'lgan ruxsat beruvchi mayning modelidir. Bu guruhga MDHga a’zo bir qancha davlatlarni ham kiritish mumkin, masalan, Belarus Respublikasi va Qozog‘iston Respublikasi. Biroq, bunday mamlakatlar ushbu faoliyat uchun ruxsat olish zarurati masalasida bir xil emas. Qozog'iston Respublikasining 2023-yil 6-fevraldagi QRQ-193-sonli "Qozog'iston Respublikasida raqamli aktivlar to'g'risida" gi Qonunining 9-moddasiga ko'ra mayning litsenziyani talab qiladi, uch yil muddatga chiqariladi va egalik huquqi ostida raqamli mayning ma'lumotlarini qayta ishlash markazi mavjudligiga qarab ikki xil bo'ladi. Belarus Respublikasi Prezidentining 2017-yil 21-dekabrdagi 8-sonli “Raqamli iqtisodiyotni rivojlantirish to‘g‘risida”gi qaroriga ko‘ra, mayning uchun maxsus ruxsat olish shart emas, shuningdek, hokimiyatning boshqa ruxsati yoki ro'yxatdan o'tish talab qilinadi. O‘zbekiston Respublikasida mayning faoliyati litsenziyalanmaydi, biroq bunday faoliyat agentlik tomonidan internet tarmog‘i orqali ro‘yxatdan o‘tkazilishi kerak.

Amerika Qo'shma Shtatlarida mayning va kriptovalyutalarni huquqiy tartibga solish rivojlanish bosqichida. Federal darajada kriptovalyutalarning muomalasi holati va qoidalarini belgilovchi yagona to'liq qonun hali mavjud emas. Biroq, kriptovalyuta tovar sifatida tan olingan, ya'ni u Qimmatli qog'ozlar va birja komissiyasi (SEC) va boshqa federal idoralar tomonidan soliqqa tortilishi va tartibga solinishi kerak.

Bank siri to'g'risidagi qonun (BSA): Kriptovalyuta birjalari va kriptovalyuta savdosi bilan shug'ullanadigan boshqa kompaniyalar

Moliyaviy jinoyatlarga qarshi kurash tarmog'ida (FinCEN) ro'yxatdan o'tishlari va KYC/AML talablariga rioya qilishlari shart.

Soliq kodeksi – Kriptovalyuta operatsiyalaridan olingan daromad oddiy daromad sifatida soliqqa tortiladi. Kriptovalyuta mayninggi ham soliqqa tortiladigan hodisa hisoblanadi.

Tovar birjasi to'g'risidagi qonun – Tovar fyucherslari savdo komissiyasi (CFTC) kriptovalyuta fyuchers shartnomalarini tartibga solishi mumkin.

Hozirda 40 dan ortiq shtat kriptovalyuta va mayningni tartibga soluvchi o'z qonunlarini qabul qildi. Ushbu qonunlar quyidagi masalalarni qamrab olishi mumkin:

- Kriptovalyuta birjalarini litsenziyalash
- Iste'molchilar huquqlarini himoya qilish
- Soliq solish
- Pul yuvishga qarshi kurash

Kriptovalyuta mayninggi: Federal darajada kriptovalyuta mayninggi taqiqlanmagan. Biroq, ba'zi shtatlar yuqori energiya iste'moli va atrof-muhitga salbiy ta'siri tufayli mayningni cheklab qo'ygan. Masalan, Nyu-York shtati qayta tiklanmaydigan energiya manbalaridan foydalangan holda kriptovalyuta mayninggi uchun yangi ruxsatnomalar berishga ikki yillik moratoriy kiritdi. AQSh federal hukumati kelgusi yillarda kriptovalyutalar va mayningni tartibga soluvchi yanada kengroq qonunchilikni joriy qilishi kutilmoqda. Shuni ta'kidlash kerakki, kriptovalyutani tartibga solish dinamik rivojlanayotgan sohadir va qonunchilik tez-tez o'zgarishi mumkin.

Amerika Qo'shma Shtatlari kriptovalyuta bozorini qonunchilik bilan tartibga solish bo'yicha ham yetakchi davlatlar qatoriga kiradi. Avvalo shuni ta'kidlash kerakki, raqamli valyutaga umumiy (federal) qonunchilik va shtat qonunchiligi mavjud bo'lgan, ba'zan boshqa subyektlardan sezilarli darajada farq qiladigan AQSh huquqiy tizimining o'ziga xos xususiyatlari tufayli yagona huquqiy maqom berilmaydi. Buning oqibati kriptovalyutaning naqd pulning analogi va egalarining mulki sifatida tan olinishi, boshqa hollarda bu moliyaviy vositalar sifatida tan olinishi mumkin. AQShda raqamli valyutadan foydalanish ko'lamini belgilovchi huquqiy maydonni yaratishga eng katta turtki – Silk Road anonim savdo platformasi bo'lib, huquq-tartibot idoralari tomonidan masalaning markazlashtirilmaganligi va kriptovalyuta muomalasining barcha

bosqichlarida anonimlikning yuqori darajasi tufayli shubhali tranzaktsiyalarni aniqlash qiyinligi ko‘rsatilgan[246].

Federal darajada kriptovalyuta aylanmasini huquqiy tartibga solish “Virtual valyuta biznesini yagona tartibga solish to'g'risida”gi qonun bilan ifodalanadi. Bu maslahat xarakteriga ega va davlatlar uchun huquqiy tartibga solish uchun qo'llanma bo'lib xizmat qiladi, u quyidagi masalalarga taalluqlidir: kriptovalyuta muomalasi bilan shug'ullanadigan kompaniyalarni litsenziyalash; mijozlarni himoya qilish; kiberxavfsizlikni ta'minlash; pul yuvishga qarshi kurash va boshqalar. Moliyaviy jinoyatlarga qarshi kurash tarmog'i (FinCEN) ham mavjud [8]. Bu jinoiy daromadlarni legallashtirishga oid qonun hujjatlari talablariga rioya etilishini nazorat qiluvchi organlar to'plami bo'lib, uning bir qismi Bank siri to'g'risidagi qonun (1970) - AQSh moliya institutlarining davlat organlariga pul yuvish holatlarini aniqlash va bostirishda yordam berish majburiyatini o'rnatishdan iborat. Bank siri to'g'risidagi qonun – BSA 1970-yilda kriptovalyutalarning paydo bo'lishi bilan qabul qilinganligini hisobga olsak, uning normalari to'liq huquqiy tartibga solishni ta'minlay olmadi, buning natijasida FinCEN tomonidan BSA normalarini raqamli valyutalarga qo'llash imkoniyatini aniqlaydigan maxsus qo'llanma nashr etildi[247].

Ushbu xususiyatlar doirasida sud jarayoni 2013 yilda bo'lib o'tgan The US vs Faiella[248] jinoiy ishini ta'kidlash kerak. Ish syujetiga ko‘ra, ayblanuvchi Robert Faiella va Charli Shrem naqd va fiat pullarni bitkoinlarga almashtirib, ikkinchisini Silk Road foydalanuvchilarining hisob raqamlariga o‘tkazgan. Himoyachining ta'kidlashicha, Bitcoin pul emas, shuning uchun ayblanuvchilarning harakatlarini pul yuvish sifatida tan olish mumkin emas. Biroq, sud Bitcoin maqomini belgilashda Merriam Webster lug'atida pulning umumiy ta'rifiga tayandi, unda pul buxgalteriya birligi sifatida ishlasa va tovarlar va xizmatlar uchun to'lash uchun mo'ljallangan bo'lsa, har qanday narsa sifatida ifodalanishi mumkinligi ta'kidlangan.

Shunisi e'tiborga loyiqki, AQShda v. Petrix[249], bu yerda ayblanuvchi mohiyatan xuddi shu harakatlarda, ya'ni pul mablag'larini o'tkazishda

[246]https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf Виртуальная валюта Биткойн: уникальные возможности его использования представляют различные проблемы для сдерживания незаконной деятельности [Электронный ресурс]: Отчет ФБР о криптовалютах от 24.04.2012 г

[247]Кто и как регулирует криптовалюты в США. // Сетевой журнал «IHODL» [сайт]. https://ru.ihodl.com/analytics/2018-12-18/kto-i-kak-

[248]Материалы дела The US v. Faiella // Law of cryptocurrency [сайт]. URL https://www.lawofcryptocurrency

[249]Материалы дела № 15-CR-227A The US v. Petrix // Электронная библиотека судебных решений США «LEAGLE» [сайт]. URL: https://www.leagle.com/decision/infdco20161202c43

vositachilik harakatlarida (fiat pul - Bitcoin) ayblangan, ammo bu holatda sud ayblanuvchi tarafini oldi va Bitcoinni pul vositasi sifatida tan olmadi.

SEC (AQSh Qimmatli qog'ozlar va birja komissiyasi) v. Trendon T Shavers[250]. Sud jarayonida, Bitcoin Saving and Trust platformasi asoschisi, sudlanuvchi Trendon T. Shevers tez qaytarilishi va yuqori foiz stavkalari bahonasida bitkoinlarga investitsiyalarni jalb qilgani ma’lum bo‘ldi.

Keyin u o'z sarmoyasini firibgarlik yo'li bilan qaytarib olish uchun Ponzi sxemasidan foydalangan. Sud jarayoni doirasida sudlanuvchi bitkoinlar AQSh qonunlari bilan tartibga solinadigan narsa emasligini ham aytdi. Biroq, sud bunday investitsiyalar, ular amalga oshirilgan shakldan qat'i nazar, qimmatli qog'ozlar sifatida tan olinishi kerak degan xulosaga keldi.

AQSh Ichki daromad xizmati 2014 yilda nizom e'lon qildi, unga ko'ra Bitcoin mulk sifatida belgilanadi va konvertatsiya qilinadigan raqamli valyutani sotish yoki almashtirish, shuningdek, tovarlar va xizmatlar uchun to'lash uchun foydalanish soliq oqibatlariga olib kelishini ko'rsatadi. Bo’yin tovlagan taqdirda, aybdor amaldagi qonun hujjatlariga muvofiq javobgarlikka tortiladi. Soliq miqdorini aniqlash uchun kriptovalyutaning sotish vaqtidagi AQSh dollaridagi qiymati hisobga olinadi[251].

Shunday qilib, Qo'shma Shtatlarda kriptovalyutalarning huquqiy maydoni bir sub'ekt hududidan boshqasiga sezilarli darajada farq qiladi. Federal qonunchilik mavjud bo'lmaganda, kriptovalyutalarning aylanishini juda batafsil tartibga solish AQSh darajasida amalga oshiriladi. Jinoiy ishlarda bunday tartibga solishni qo'llash masalalariga kelsak, bu yerda biz kriptovalyutaning huquqiy maqomining aniq ta'rifi bilan u amaldagi jinoyat qonunchiligiga osongina mos kelishini tasdiqlaymiz. Bu holda, asosan, virtual valyutaning iqtisodiy xususiyatlari hisobga olinadi, axborot xususiyatlari esa ikkinchi ahamiyatga tushadi.

Kriptovalyuta muomalasi doirasini belgilovchi qonunchilikni ishlab chiqqan birinchi mamlakatlardan biri **Yaponiya** hisoblanadi. 2014-yilgacha ushbu yo'nalishda qonunchilik bazasini yaratish uchun aniq shartlar yo'q edi, ammo 2013-yilda Tokiyoda joylashgan Mt.Gox ochiq savdo platformasining qulashi va uning ochiq joylarida taxminan 47% "sof" Bitcoin operatsiyalarining amalga oshirilishi Yaponiya hukumatini kriptovalyutalar bilan savdo qiluvchi kompaniyalar va fuqarolar xavfsizligini ta'minlash maqsadida kriptovalyutalar uchun huquqiy

[250]Материалы дела №23090 SEC v. Trendon T. Shavers [Электронный ресурс]: URL: https://www.sec.gov/litigation/litreleases/2014/lr23090.htm

[251] Кто и как регулирует криптовалюты в США. // Сетевой журнал «IHODL» [сайт]. URL https://ru.ihodl.com/analytics/2018-12-18/kto-i-kak-

bazani ishlab chiqish bo'yicha ishlarni boshlashga undadi. Ushbu sa'y-harakatlarning natijasi qonunlar to'plamini yaratish bo'ldi, unga ko'ra Bitcoin birjalari faoliyati Moliyaviy xizmatlar agentligi (FSA) orqali litsenziyalanishi kerak. Birjani ro'yxatdan o'tkazishning asosiy shartlari 10 million iyen (taxminan 88 ming AQSh dollari) miqdoridagi kapitalning mavjudligi, shuningdek, har yili moliyaviy hisobotlarni taqdim etish va muntazam audit o'tkazish majburiyatidir. Shu bilan birga, kriptovalyuta bilan operatsiyalar 8% soliqqa tortiladi. Bitcoin, boshqa virtual valyutalar singari, qonuniy ravishda valyuta hisoblanmaydigan to'lov vositasi maqomini oldi, boshqacha aytganda, ular aktivlarga tenglashtirildi.

2017-yilda raqamli valyutalarning holati o‘zgardi va 1-apreldan Yaponiyada raqamli valyuta qonuniy to‘lov vositasi sifatida tan olindi, bu esa ular bilan bo‘lgan operatsiyalar bo‘yicha 8 foizlik soliq tugatilishini anglatardi. Biroq keyinchalik ushbu valyutalar bilan operatsiyalarni amalga oshiruvchi treyderlar uchun 15 foizdan 55 foizgacha soliq belgilandi[252].

Shu bilan birga, fuqarolarning xavfsizlik darajasini oshirishga qaratilgan kriptovalyuta birjalari uchun qo'shimcha shart-sharoitlarni nazarda tutuvchi qonun e'lon qilindi, xususan, bular kiberxavfsizlik darajasini oshirish, birja aktivlari va mijozlarning aktivlarini ajratish, shuningdek, shaxsiy identifikatsiya tizimini tashkil etish kabilardan iborat edi. Shuningdek, yangi talablar kompaniyalarning pul yuvishga qarshi global tizimga o‘tishini, shu jumladan anonim kriptovalyutalardan foydalanishdan butunlay voz kechishni ham o‘z ichiga oldi[253]. 2020-yil aprel oyida Yaponiyada yangi qoidalar kuchga kiradi, ular kriptovalyutalar holatiga va kriptobirjalarning ishlash tartibiga ham ta'sir qiladi. Xususan, raqamli valyutalarni kriptoaktivlar sifatida tan olish rejalashtirilmoqda[254] . Kriptovalyutani tartibga solish siyosatining kuchaytirilishi mamlakat iqtisodiyotini ta'minlash bilan bog’liq. Chunki kriptovalyutani tartibga soluvchi qonun qabul qilinishidan oldin ham ko’pgina operatsiyalar amalga oshirilgan. Qonun qabul qilingach, davlat aktivlarining bir qismi raqamli formatga ega bo’ldi. Birjalar xavfsizligi doimiy tashvishlarga sabab bo’lgan. 2018-yil boshida Yaponiyadagi eng yirik kriptobirjalardan biri *Coincheck* xakerlar hujumiga uchradi, natijada hujumchilar jami 500 million dollarlik kriptovalyutani o'g'irlab ketishdi.

[252] Япония признала криптовалюты законным платежным средством. // Российская газета [сайт]. URL: https://rg.ru/2017/04/01/iaponiia-priznala-

[253] Восток - дело тонкое: криптовалюты в Японии. // Сетевой журнал CoinSpot [сайт]. URL: https://coinspot.io/law/asia-and-africa/vostok-delo-tonkoe-

[254] Япония приняла новое законодательство в области регулирования криптовалют. // Сетевой журнал ForkLog [сайт]. URL: https://forklog.com/yaponiya-prinyala-novoe-zakonodatelstvo-v-oblasti-

Ikkinchidan, kriptovalyutalar muomalasiga qo‘shimcha cheklovlar Yaponiyada pul yuvish holatlari ko‘payganligi sababli o‘rnatilmoqda. Shunday qilib, Yaponiya Milliy politsiya agentligi ma'lumotlariga ko'ra, 2018-yilda mamlakatda kriptovalyutalar orqali pul yuvishning 7 mingga yaqin holati qayd etilgan, bu o'tgan yilga nisbatan o'n baravar ko'pdir[255].

Jinoiy harakatlarni jinoiy-huquqiy baholashga kelsak, u Yaponiyaning amaldagi Jinoyat kodeksi bilan to'liq qamrab olingan va kriptovalyutaga nisbatan kodeksga maxsus o'zgartirishlar kiritilmagan. Bunday xatti-harakatlar 2017-yildan boshlab, kriptovalyutalarning davlat hududida qabul qilingan huquqiy holatiga asoslanadi, ular qonuniy to'lov vositasi sifatida tan olingan va tegishli ravishda soliqdan ozod qilingan; jinoyat huquqi siyosati ularni boshqa ishonchli pul bilan teng asosda ko'rib chiqadi[256]. Shu munosabat bilan, ikki tomonlama xususiyatga ega bo'lgan kriptovalyutalar, shu jumladan pulning xususiyatlari va kompyuter ma'lumotlari xususiyatlari, yapon amaliyotida faqat kriptovalyutaning qiymat xususiyatlari nuqtai nazaridan ko'rib chiqiladi. Ularda kriptovalyuta bilan bog'liq jinoyatlar mulkka qarshi jinoyatlar deb tasniflanadi.

Estoniya kriptovalyuta bozori uchun haqiqiy “jannat”dir. Yevropaning kichik mamlakati o'z hududida kriptovalyuta aylanishiga nisbatan qulaylik nuqtai nazaridan darhol yetakchi o'rinni egallamadi. Dastlab Estoniya Markaziy banki raqamli valyutalarni moliyaviy piramidalarga tenglashtirib, odamlarni ulardan foydalanishdan tiyilishga chaqirdi. Estoniyada kriptovalyuta bozorining rivojlanishiga turtki bo'lgan birinchi qadam Yevropa sudining 2015-yil 22-oktyabrdagi qarori bo'lib, uning ma'nosi bitkoinlarni ishonchli valyutalarga almashtirish bo'yicha operatsiyalarni Yevropa Ittifoqi mamlakatlari uchun QQSdan ozod qilishdir. Bu qaror Devid Xedkvist va Shvetsiya soliq politsiyasi[257] o‘rtasidagi huquqiy nizoni ko‘rib chiqish natijasida qabul qilingan.

Ish materiallaridan ma'lum bo'lishicha, Xedkvist Internetda boshqa valyutalar uchun Bitcoin’ni almashtirish punktini tashkil etishga qaror qilgan va shuning uchun Soliq qonuni komissiyasiga murojaat qilgan, u yerda ular unga ushbu operatsiyalar QQSga tortilmasligini tushuntirgan. Shvetsiya soliq politsiyasi bunga rozi bo'lmadi va Oliy ma'muriy sudga murojaat qildi. Ikkinchisi tushuntirish talab qildi, u yerda kriptovalyuta almashinuvi operatsiyalari nihoyat soliqdan ozod qilindi, chunki Yevropa

[255] В Японии в 10 раз участились случаи отмывания денег при помощи криптовалют. // Сетевой журнал ForkLog [сайт] https://forklog.com/v-yaponii-v-

[256] Шарапов Р.Д., Минин Р.В., Капаева Е.О. Криптовалюта: уголовно-правовой аспект // Юридическая наука и правоохранительная практика 2 (44) 2018 г С. 45

[257] Дело Хэдквист против Шведской налоговой полиции https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=EN

Ittifoqi qoidalariga ko'ra, valyuta ayirboshlash operatsiyalari, banknotlar va tangalar uchun soliq undirish taqiqlanadi. Xuddi shu sud kriptovalyutani tovarlar yoki xizmatlar sifatida emas, balki to'lov vositasi sifatida tasniflaganligi sababli, ushbu qoida u bilan tuzilgan bitimlarga nisbatan qo'llaniladi.

Estoniyada kriptovalyutalarni yaratish yo‘lidagi navbatdagi qadam jinoiy daromadlarni legallashtirish va terrorizmni moliyalashtirishga qarshi kurashish to‘g‘risidagi qonunning qabul qilinishi bo‘ldi. 2017-yil 27-noyabrda kuchga kirgan mazkur aktga ko‘ra, raqamli valyuta bilan bog‘liq faoliyatni amalga oshirish Estoniya moliyaviy razvedka boshqarmasidan ikki turdagi litsenziyadan birini olish orqali mumkin: 1) virtual qiymatlarni naqd (fiat) mablag'larga almashtirish bo'yicha xizmatlar ko'rsatuvchi provayder; 2) Virtual qiymat hamyon xizmati provayderi.

Ushbu faoliyat, Estoniya sud amaliyotiga muvofiq, tadbirkorlik faoliyatidan boshqa narsa emas - ya'ni muqobil to'lov usullari xizmatlarini ko'rsatish. Bundan kelib chiqadiki, ikkinchisini amalga oshiruvchi shaxslar litsenziya olishlari va jinoiy faoliyatdan olingan daromadlarni legallashtirishga va terrorizmni moliyalashtirishga qarshi kurashish to'g'risidagi qonun talablariga rioya qilishlari shart[258]. Aks holda, ushbu talablarni buzgan holda tadbirkorlik faoliyatini amalga oshirish, moddaga muvofiq jinoiy javobgarlikka sabab bo'ladi. Estoniya Respublikasi Jinoyat kodeksining 148[259], noqonuniy tadbirkorlik, shuningdek, boshqa moddalar, shu jumladan noqonuniy ravishda olingan daromadlarni legallashtirish bilan bog'liq moddalar.

Shunday qilib, mamlakatda kripto-biznesni rivojlantirish uchun qulay shart-sharoitlarga qaramay, soliqqa tortishning yo'qligi va yuridik shaxsni ro'yxatdan o'tkazishning juda oddiy tartibi ko'rsatilgan qonunchilikka rioya qilish talablari juda qattiq. Bundan tashqari, yaqinda Moliyaviy nazorat organi boshqaruvi raisi Kilav Kesslerning kriptovalyutalardan noqonuniy maqsadlarda foydalanish bo'yicha muhokamalar doirasida hukumatlararo moliyaviy harakatlar bo'yicha ishchi guruhi (FATF) yig'ilishida e'lon qilingan bayonotidan kelib chiqib,), tokenlar bilan bog‘liq bo‘lgan yoki boshqa yo‘l bilan bog‘langan shaxslar faoliyati ustidan nazoratni kuchaytirish taklif qilinmoqda. Boshlang'ich

[258] Ефимова Н. А. К вопросу о регулировании первичного размещения монет (ICO) и криптовалюты в зарубежных странах: опыт Эстонии // Журнал зарубежного законодательства и сравнительного правоведенья № 5. 2018. С. 66 Уголовный Кодекс Эстонской Республики // Российский правовой портал: библиотека Пашкова https://constitutions.ru/?p=446

[259] Недолго музыка играла: криптовалютчиков в Эстонии хотят задавить пошлинами. // Новостное агентство «Sputnik» [сайт]. URL: https://ee.sputniknews.ru/economy/20190725/17324838/kriptovaljuta-estonia-

chora sifatida ularga "bir martalik" firmalarni bozordan chiqarib tashlash uchun davlat boji miqdorini oshirish taklif qilindi[260]. Bunday bayonotlar, birinchi navbatda, kriptovalyutadan jinoiy maqsadlarda foydalanish bilan bog'liq.

Xitoy kriptovalyutalarni huquqiy tartibga solish masalalarida boshqa pozitsiyani egalladi. Dastlab, Bitcoinning shakllanishi davrida Xitoy qonunchiligi dunyodagi eng ilg'or qonunlardan biri edi. Tokenlar davlat hududida huquqiy nuqtai nazardan tovar sifatida qaralgan. Raqamli valyutalar savdosi amalga oshirilgan birjalar va veb-saytlar Telekommunikatsiyalar byurosida ro'yxatdan o'tishlari va vaqti-vaqti bilan o'z faoliyati to'g'risida hisobotlarni taqdim etishlari kerak edi. Kriptovalyuta bilan operatsiyalar oddiy tovarlar bilan bir xil qoidalarga muvofiq soliqqa tortildi.

Keyin, 2013 yilda Xitoy Xalq banki "Bitcoin moliyaviy xavflarning oldini olish to'g'risida xabarnoma"ni nashr etadi[261]. Ushbu hujjatga ko'ra, banklarga kriptovalyutalardan foydalangan holda tranzaktsiyalarni amalga oshirish tokenlar aylanishi xavfsizligi bilan bog'liq muammolar tufayli taqiqlangan. 2016 yilda Xitoy kriptovalyuta va blokcheyn texnologiyalarini ajratdi.

2017 yildan beri Xitoy barcha kriptovalyutalarni taqiqlab qo'ydi, bu esa birjalarning savdo operatsiyalarini to'xtatishiga sabab bo'ldi. Mamlakatda raqamli valyutalar almashtirilgan P2P bozorlari asta-sekin yopiladi va shundan so'ng offshor kripto almashinuvchilari ham bloklandi. 2018 yil iyul oyida Xitoy Xalq banki raqamli valyutalar ustidan yakuniy qarorni e’lon qildi. Kriptovalyutalar orqali pul yuvishga qarshi kurashda siyosat kuchaytirilmoqda.

2019-yilda Xitoy hukumati o‘zining kriptovalyutasini yaqinda ishga tushirilishini e’lon qildi, u davlat tomonidan to‘liq ta’minlanadi va uning qat’iy nazorati ostida bo‘ldi.

Shunday qilib, kriptovalyuta sohasini huquqiy tartibga solish bo'yicha mamlakatlarni uchta guruhga bo'lishimiz mumkin. Birinchi guruh mamlakatlari bu masalani hal qilish choralarini ko'rmaydi va kuzatuvchi pozitsiyasini egallaydi, shu bilan birga fuqarolarni tokenlardan foydalanish xavfi haqida xabardor qiladi: BAA, Rossiya, Shveysariya va boshqalar.

Ikkinchi guruh mamlakatlari o‘z hududida kriptovalyuta muomalasini butunlay taqiqlab qo‘ydi: Xitoy, Bangladesh, Boliviya,

[260] Уведомление о предотвращении рисков, связанных с биткойнами Китайской комиссией по регулированию ценных бумаг. http://www.csrc.gov.cn/pub/newsite/flb/flfg/bmgf/zh/gfXwjfxq/201401/t201401

[261] FATF разработает стандарты для борьбы с отмыванием денег через криптовалюты. // Электронное периодическое издание «Ведомости». https://www.vedomosti.ru/finance/news/2018/09/06/780121

Ekvador va boshqalar. Uchinchi guruh mamlakatlari kripto aktivlarning huquqiy maqomi va foydalanish tartibini belgilab, o'z hududida raqamli valyutalarning muomalasini qonuniylashtirdilar. Ular quyidagilarni amalga oshirdilar: anonimlikni istisno qilish – foydalanuvchilarni aniqlash, birja platformalarini ro'yxatdan o'tkazish (foydalanuvchi huquqlarini himoya qilish kafolatlari bilan), ular tomonidan organga hisobotlarni taqdim etish, kriptovalyuta faoliyatini nazorat qilish, aylanma ishtirokchilaridan soliq undirish, shuningdek huquqbuzarlarga nisbatan jarimalar belgilash vakolatiga ega. Bundan tashqari, ushbu chora-tadbirlar, qoida tariqasida, amaldagi jinoyat qonunchiligiga mos keladi va huquqiy maqomiga qarab, jinoyatlar tasniflanadi. Umumiy elementlar asosan noqonuniy yo'l bilan olingan daromadlarni yuvish, noqonuniy biznes yoki noqonuniy bank faoliyatidan iborat.

Shuningdek, kriptovalyuta, bir hodisa sifatida, ikki tabiatga – ham iqtisodiy ham axborot xarakteriga ega ekanligini qayd etiladi. Bir tomondan, u ma'lum moddiy qiymatga ega bo'lib, to'lov vositasi vazifasini bajaradi, ikkinchi tomondan, u axborot olamining hodisasi bo'lib, axborot xususiyatlariga ega (masalan, kriptovalyutaning o'zi ma'lum matematik kod). Raqamli valyutalar muomalasi uchun qonunchilik bazasini yaratgan mamlakatlarda, birinchi navbatda, iqtisodiy komponent hisobga olinadi. Kuzatuvchi maqomidagi davlatlarda, huquqiy maqom o'rnatilmagan. Jinoiy himoya choralarini belgilash bevosita ushbu fuqarolik-huquqiy maqomning belgilanishiga bog'liq.

2018-yil sentabrida FATF (Finance Action Task Force on Money Leading) 2019-yilning yozigacha kriptovalyutalarni huquqiy tartibga solish boʻyicha xalqaro standartlarni ishlab chiqishi haqida xabar berilgan edi[262]. Ushbu standartlar universal bo'lishi va oxir-oqibat raqamli valyutalar uchun huquqiy asosga ega bo'lmagan mamlakatlar qolmaydi, deb taxmin qilingan, ammo bu standartlar hali ishlab chiqilmagan. Bundan kelib chiqadiki, bugungi kunda kriptovalyuta muomalasi masalalari har qachongidan ham dolzarbdir, chunki ular amaliyotda tez-tez uchrab turadi, biroq qonunchilik bazasi yoʻqligi sababli sud va sudgacha boʻlgan jarayonda huquqni muhofaza qilish masalalari yuzaga keladi.

[262] Официальный сайт Центрального банка РФ httpwww.cbr.ru/press/pr/?file=27012014_1825052.html

РАҚАМЛИ ДАЛИЛЛАРНИНГ АХБОРОТ-КОММУНИКАЦИЯ СОҲАСИДАГИ ЗАМОНАВИЙ ЖИНОЯТЛАРНИ ТЕРГОВ ҚИЛИШ ВА ФОШ ЭТИШДАГИ ЎРНИ

Кудратов Бунёд Бахтиёрович
Ҳуқуқни муҳофаза қилиш академияси
Рақамли криминалистика илмий-тадқиқот интитути
Рақамли терговга кўмаклашиш бўлими бошлиғи

Аннотация: *мақолада ахборот-коммуникация технологиялари соҳасида содир этилган жиноятларни тергов қилишда рақамли далилларнинг аҳамияти таҳлил қилинган. Рақамли далиллар — қурилмалардан олинган ва жиноятларни исботлаш, жиноятчиларни аниқлаш ёки айбсизликни тасдиқлаш учун қўлланиладиган маълумотлардир. Тергов жараёнида тизим логлари, тармоқ трафиги, электрон почта ва файл тизимларидан олинган маълумотлар муҳим аҳамиятга эга. Муаллиф рақамли далиллар билан ишлашдаги ҳуқуқий ва техник муаммоларни кўриб чиқиб, сунъий интеллект ва блокчейн технологияларининг аҳамиятини таъкидлаган.*

Калит сўзлар: *рақамли далил, тармоқ трафиги, электрон почта, тизим логи.*

Ахборот технологияларининг жадал ривожланиши ва кенг тарқалиши билан бирга, бу соҳада содир этиладиган жиноятлар сони ҳам ортиб бормоқда.

Бундай жиноятларни самарали тергов қилиш ва фош этиш учун рақамли далиллардан фойдаланиш муҳим аҳамият касб этади.

Хусусан, ахборот технологиялари соҳасидаги жиноятлар ўзига хос хусусиятларга эга бўлиб, улар асосан виртуал муҳитда содир этилади, трансчегаравий хусусиятга эга, тез ўзгарувчан ва юқори даражадаги анонимлик билан ажралиб туради. Бу хусусиятлар уларни аниқлашва исботлашни мураккаблаштиради.

Рақамли далиллар - бу рақамли қурилмаларда сақланадиган, қайта ишланадиган ёки узатиладиган ва суд жараёнида фойдаланиш мумкин бўлган ҳар қандай маълумотлар. Бу маълумотлар жиноят содир этилганлигини исботлаш, айбдорни аниқлаш ёки айбсизликни тасдиқлаш учун ишлатилиши мумкин. Рақамли далиллар кенг қамровли бўлиб, улар компьютерлар, смартфонлар, тармоқ қурилмалари, булутли хизматлар ва бошқа рақамли технологиялардан олиниши мумкин.

Рақамли далиллар бу турдаги жиноятларни тергов қилиш ва фош этишда муҳим рол ўйнайди. Улар жиноят изларини сақлаш, жиноятчининг шахсини аниқлаш, жиноят механизмини тушуниш

ҳамда жиноят вақти ва жойини аниқлашда ёрдам беради. Рақамли далилларнинг асосий турларига тизим логлари, тармоқ трафиги, электрон почта ва мессенжер хабарлари, файл тизими маълумотлари киради.

Тизим логлари фойдаланувчиларнинг тизимга кириш ва чиқиш вақтлари, бажарилган амаллар, хатто хабарлар ва тизим конфигурациясидаги ўзгаришлар ҳақида маълумот беради. Бу маълумотлар жиноятчининг ҳаракатларини кузатиш ва жиноят вақтини аниқлашда муҳим рол ўйнайди.

Тармоқ трафиги эса IP-манзиллар, порт рақамлари, протоколлар ва маълумотлар пакетларини ўз ичига олади. Бу маълумотлар жиноятчининг жойлашувини аниқлаш ва унинг бошқа шахслар билан алоқаларини ўрнатишда ёрдам беради.

Электрон почта ва мессенджер хабарлари хабарлар мазмуни, жўнатувчи ва қабул қилувчи манзиллари, жўнатиш вақти ва санаси, иловаларни ўз ичига олади. Бу маълумотлар жиноятчиларнинг ўзаро алоқаларини ва жиноят режаларини аниқлашда муҳим аҳамиятга эга. Файл тизими маълумотлари эса файлларнинг мазмуни, файл метамаълумотлари ва ўчирилган файлларни ўз ичига олади. Бу маълумотлар жиноят далилларини топиш ва жиноятчининг ҳаракатларини реконструкция қилишда ёрдам беради.

Рақамли далилларни тўплаш ва таҳлил қилиш жараёни бир неча босқичдан иборат.

Биринчи босқичда далиллар аниқланади ва сақланади. Бунда потенциал далил бўлиши мумкин бўлган рақамли қурилмалар аниқланади, хавфсиз олиб қўйилади ва далилларнинг бутунлигини таъминлаш учун чоралар кўрилади.

Иккинчи босқичда далиллар тўпланади. Бу жараёнда рақамли қурилмаларнинг нусхалари яратилади, тармоқ трафиги қайд этиладива булутли хизматлардан маълумотлар олинади.

Учинчи босқичда далиллар таҳлил қилинади. Таҳлил жараёни маълумотларни қидириш ва фильтрлаш, шифрланган маълумотларни очиш, ўчирилган файлларни тиклаш, хронологик таҳлил ўтказиш ва маълумотлар ўртасидаги боғлиқликларни аниқлашни ўз ичига олади. Сўнгги босқичда эса таҳлил натижалари асосида ҳисобот тайёрланади. Бу ҳисобот топилган далилларнинг батафсил тавсифи, таҳлил усуллари ва қўлланилган воситаларнинг тавсифи, хулосалар ва тавсияларни ўз ичига олади.

Рақамли далиллар билан ишлашда бир қатор муаммолар юзага келади. Техник муаммолар орасида шифрлаш технологиялари,

маълумотларнинг катта ҳажми ва тез ўзгарувчан технологиялар билан боғлиқ қийинчиликлар мавжуд. Ҳуқуқий муаммолар эса далилларнинг мақбуллиги масаласи, шахсий ҳаёт дахлсизлиги ҳуқуқи ва трансчегаравий ҳуқуқий масалаларни ўз ичига олади. Бундан ташқари, малакали мутахассисларнинг етишмаслиги ва махсус жиҳозлар ҳамда дастурий таъминотнинг қимматлиги каби ресурс билан боғлиқ муаммолар ҳам мавжуд.

Келажакда рақамли далиллар билан ишлаш самарадорлигини ошириш учун бир қатор истиқболли йўналишлар мавжуд. Булар орасида сунъий интеллект ва машинавий ўқитиш технологияларининг қўлланилиши алоҳида ўрин тутади. Бу технологиялар катта ҳажмдаги маълумотларни тезроқ ва самаралироқ таҳлил қилиш, аномалияларни автоматик равишда аниқлаш ва мураккаб алоқаларни топиш имконини беради.

Блокчейн технологиясининг қўлланилиши ҳам истиқболли йўналишлардан бири ҳисобланади. Бу технология далилларнинг бутунлигини таъминлаш, далилларнинг келиб чиқиш манбасини кузатиш имконияти ва рақамли далилларнинг ишончлилигини ошириш каби афзалликларга эга.

Булутли ҳисоблаш технологияларининг ривожланиши эса катта ҳажмдаги маълумотларни сақлаш ва қайта ишлаш, масофадан туриб далилларни таҳлил қилиш ҳамда халқаро ҳамкорликни осонлаштириш имконини беради.

Хулоса ўрнида шуни айтиш мумкинки, рақамли далиллар замонавий жиноятларни тергов қилиш ва фош этишда муҳим рол ўйнайди. Улар турли хил манбалардан олиниши мумкин ва кенг қамровли маълумотларни ўз ичига олади. Рақамли далиллар билан ишлаш махсус билим ва кўникмаларни, шунингдек махсус дастурий ва аппарат воситаларидан фойдаланишни талаб қилади. Бундан ташқари, рақамли далилларни тўплаш ва таҳлил қилиш жараёнида ҳуқуқий ва этик меъёрларга қатъий риоя қилиш зарур. Рақамли технологияларнинг ривожланиши билан бирга, рақамли далилларнинг аҳамияти ва уларни тўплаш ҳамда таҳлил қилиш усуллари ҳам доимий равишда такомиллашиб бормоқда.

АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНИБ СОДИР ЭТИЛГАН ФИРИБГАРЛИКНИ ФОШ ЭТИШНИНГ АЙРИМ ЖИҲАТЛАРИ

Каримов Ваҳобжон
Ўзбекистон Республикаси Ҳуқуқни
муҳофаза қилиш академияси
профессори, ю.ф.д.
Таштемиров Анвар Алиқулович,
Ўзбекистон Республикаси ИИВ Академияси,
Маъмурий ҳуқуқ кафедраси доценти.
E-mail: *anvartoshtemirov05031979@gmail.com*

Аннотация: *Мақолада ахборот технологияларидан фойдаланиб содир этилган фирибгарликни фош этиш билан боғлиқ масалалар назарий, ҳуқуқий томонидан таҳлил қилиниб, жиноят процесси, криминалистика ва тезкор-қидирув соҳасидаги мутахассислар фикрларига асосланиб ушбу жиноятларни фош этиш борасида тегишли тавсиялар берилган.*

Калит сўзлар. *Ахборот технологиялари орқали содир этилган фирибгарлик, кибержиноят, киберфирибгарлик, ижтимоий тармоқ, ахборот макони, банк пластик картаси, электрон манзил.*

Аннотация: *В статье анализируются вопросы, связанные с выявлением мошенничества, совершенного с использованием информационных технологий с теоретической, правовой точки зрения, и на основе мнений специалистов в области уголовного процесса, криминалистики и оперативного расследования даются соответствующие рекомендации по выявлению этих преступлений.*

Ключевые слова. *Мошенничество, совершенное с использованием информационных технологий, киберпреступление, кибермошенничество, социальная сеть, информационное пространство, банковская пластиковая карта, электронный адрес.*

Annotation: *the article analyzes issues related to the detection of fraud committed using information technology from a theoretical, legal point of view, and based on the opinions of experts in the field of criminal procedure, forensics and operational investigation, appropriate recommendations are given for identifying these crimes.*

Keywords. *Fraud committed with the use of information technology, cybercrime, cyberfraud, social network, information space, bank plastic card, electronic address.*

Республикамизда қонун устуворлигини таъминлаш, суд-ҳуқуқ тизимини ислоҳ қилиш, шахсларнинг ҳуқуқ ва эркинликлари бузилишининг олдини олиш, қонунни бузган шахсни жавобгарликка тортиш, жиноий тажовузлар натижасида фуқаролар ва юридик шахсларга етказилган мулкий зарарларни қоплаш бўйича кенг қамровли ислоҳотлар изчил амалга оширилмоқда. Хусусан, 2022-2026

йилларга мўлжалланган Ўзбекистон Республикасини ривожлантиришнинг еттита устувор йўналиши бўйича Тараққиёт стратегиясида “ахборот технологияларидан фойдаланган ҳолда содир этилаётган янги турдаги жиноятлар, шу жумладан кибержиноятларни фош этиш бўйича тезкор-қидирув фаолиятини ислоҳ қилиш, қўшимча куч ва воситаларни жалб қилиш ҳамда ушбу жиноятларга қарши курашиш жараёнларида фуқароларнинг қадр-қиммати ва эркинлигини ҳимоя қилишнинг самарадорлигини янада ошириш”[1] каби долзарб вазифалар ижросини таъминлашда ахборот технологияларидан фойдаланиб содир этилган фирибгарликка қарши курашиш фаолиятини тартибга солувчи қонунчилик нормалари ва уларни амалга ошириш билан боғлиқ ҳуқуқни қўллаш амалиётини чуқур ва танқидий ўрганиб чиқиш долзарб масалалардан биридир.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарлик ёки интернет фирибгарлиги деб ном олган жиноятлар кўлами кенгайиб бормоқда. Уларга қарши курашишда бугунги кунда кадрлар салоҳияти, уларнинг билим ва кўникмалари даражасига алоҳида эътибор қаратилмоқда. Шу ўринда жиноят ҳуқуқи назариясида киберфирибгарлик тушунчаси тўғрисида турли хил ёндашувлар мавжуд. Хусусан, В.К.Барчуковнинг фикрича, киберфирибгарлик комьпютер фирибгарлиги бўлиб, у ички маълумотлардан фойдаланган ҳолда фирибгарлик ва ишончни суиистеъмол қилиш орқали ўзганинг мулкига тажовуз қилишдир[2]. Д.А.Зикованинг фикрича, киберфирибгарлик жинояти компьютер технологиялари ёрдамида фирибгарлик, ишончни суиистеъмол қилиш орқали ўзга шахснинг пул маблағларини ўзлаштириш, унинг мулкига зарар келтириш ва ушбу мулкка эга бўлиш ҳисобланади[3]. М.А.Ефремова эса, «киберфирибгарлик» тушунчасини «компьютер маълумоти орқали фирибгарлик қилиш» тушунчаси билан бир хил эканлигини ва уларнинг синоним сўзлар ҳисобланишини таъкидлайди[4].

Юқоридаги олимларнинг фикрларига қўшилган ҳолда, таъкидлаш жоизки, хақиқатан ҳам киберфирибгарлик ахборот технологиялари ёрдамида амалга оширилади ва ўзга шахснинг мулкига, уларнинг ишончига кириш ёки ишончини суиистеъмол қилиш йўли билан эга бўлишга қаратилади. Бироқ, миллий қонунчилигимизда ахборот технологиялари тизими билан боғлиқ тушунчалар ва унинг амалга оширилиш механизми тўлиқ белгилаб берилмаган, фақатгина компьютер тизими билан боғлик айрим қоидалар мавжуд эканлиги билан ифодаланади. Шунингдек, мазкур

тушунча тор доирада, яъни ахборот технологиялари ва коммуникациялари негизида кўрсатиб ўтилган.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни фош этиш методикасини такомиллаштириш бўйича услубий тавсияларни ишлаб чиқишнинг объектив хусусияти билишнинг ўзига хос объекти (аниқроғи объектлари) ҳисобланади. Бир томондан – қонун чиқарувчи томонидан ўзганинг мулкини талон-торож қилиш ёки ўзганинг мулкига бўлган ҳуқуқини сотиб олиш деб белгилаган фирибгарлик, бошқа томондан – ушбу жиноий фаолият ахборот технологиялар орқали маълумотларни киритиш, ўчириш, блокировка қилиш, ўзгартириш ёки бошқа турдаги аралашув орқали амалга ошириладиган виртуал ҳаракатдир. Ахборот технологиялари орқали амалга ошириладиган маълумотларни ахборот ва телекоммуникация тармоқларида сақлаш, қайта ишлаш ёки узатиш каби фаолиятларда номоён бўладиган ва шу орқали жиноятга оид аниқ далилий маълумотлар шаклида акс эттирилган жараёндир. Айнан шу шаклда тадқиқот объекти ушбу турдаги жиноятлар тўғрисида криминалистик аҳамиятга эга бўлган маълумотларни шакллантиришда ҳал қилувчи аҳамиятга эга. Бу хусусиятларга қуйидагиларни киритиш мумкин:

биринчидан, ахборот технологияларидан фойдаланиб содир этиладиган фирибгарликлар бошқа турдаги фирибгарликлардан содир этилиш усули билан кескин фарқ қилади. Жабрланувчилар фирибгарлар билан муайян вақт (3-4 кун, 10-20 кун) давомида, баъзи вақтларда узоқроқ муддат (3 ой ва ундан кўп вақт) давомида ўзаро виртуал муносабатда бўладилар. Шунинг учун ҳам жабрланувчилар жиноят содир этилгандан кейин фирибгарнинг муомиласи, гапириш оҳанги, мулоқотга киришиш усули, айрим ҳолларда ташқи кўриниш белгилари тўғрисида тўлароқ маълумот беришлари мумкин;

иккинчидан, ахборот технологиялари орқали фирибгарлик содир этувчи жиноятчилар ўзиларининг IT соҳасида чуқур билимга эгалиги, бугунги кундаги замонавий технологиялар имкониятидан фойдаланиш кўникмасининг юқорилиги, ақл-фаросати, дунёқараши, фикрлаш доираси ва хулқ-атвори билан бошқа турдаги жиноятларни содир этувчи (ўғри, талончи, безори) шахслардан кескин фарқ қилади. Улар жиноятни содир этишда ўзларининг билими ва маҳорати, айёрлиги ва чапдастлиги каби қобилиятларини ишлатиб одамларни ўзига жалб этадилар, уларда ўзларига нисбатан ишонч ва қизиқиш уйғотадилар;

учинчидан, ахборот технологияларидан фойдаланиб содир этилган фирибгарлик баъзи вақтларда фуқароларнинг ўз ноўрин

истаклари натижасида содир этилади. Жабрланувчилар фирибгарга нисбатан ўта ишонч ва очиқ кўнгиллик билдирадилар ва шу орқали ўзларининг алданиб қолганлигини сезмай қоладилар[5].

Юқорида таъкидлаб ўтилганидек, нафақат ахборот технологияларидан фойдаланиб содир этиладиган фирибгарликларда балки, бошқа турдаги жиноятларда ҳам жиноятчининг шахси асосий роль ўйнайди. Бу борада биз кўриб чиқаётган соҳадаги фирибгарлар эса ўз "соҳаси" нинг билимдони сифатида анча кенг имкониятларга эга шахслар ҳисобланади. Одатда, ахборот технологияларидан фойдаланиб содир этиладиган фирибгарликлар аосан гуруҳ таркибида амалга оширилади. Шундай экан, гуруҳдаги ҳар бир иштирокчига унинг имкониятидан келиб чиқиб, тегишли вазифалар белгиланади. Бунда энг катта "иш" ни ижтимоий тармоқ орқали (телефон, Telegram, Instagram, Whats App ва ҳ.к.) жабрланувчи билан мулоқотга киришувчи амалга оширади, шу боис фирибгарликка хос индивидуал хусусиятлар айнан гуруҳнинг ушбу иштирокчиларида намоён бўлишини кузатиш мумкин. Бошқалар эса вазифалар тақсимотини амалга ошириб уни назорат қилиб турувчи раҳбарлик, маълумотлар алмашинувини таъминловчи воситачилик, ахборот технологиялари орқали маълумотларга ишлов бериш вазифасини амалга оширувчи техник мутахассислик каби фаолият турлари билан шуғулланишлари белгиланади.

Шу ўринда, ахборот технологияларидан фойдаланиб содир этиладиган фирибгарлик жиноятларида жиноятчи ва жабрланувчи бир бирини кўриши шарт эмаслиги, яъни билвосита мулоқотга киришиш орқали ҳам жиноятчилар ўз мақсадларини осонгина эришаётганлиги бугунги кундаги ушбу соҳадаги энг катта муаммолардан бирига айланиб бормоқда. Бундай турдаги жиноятларнинг мураккабликларидан яна бири, нафақат жиноятчи ва жабрланувчи, балки гуруҳ иштирокчилари ҳам кўпгина ҳолларда ўзаро бир бирини кўрмасдан, билмасдан, танимасдан фақатгина гуруҳ етакчисининг кўрсатмалари орқали ижтимоий тармоқларда мулоқотга киришиши натижасида уларнинг шахсини аниқлашга бўлган уринишларни имконсиз даражага тушириб қўймоқда. Албатта, бу жараёнда мулоқотни таъминлаб берувчи ижтимоий тармоқларнинг ўрни ва аҳамияти қанчалик катта эканлигини ҳис этиш мумкин.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарлик жиноятларининг жамият учун хавфи сўнги вақтларда янада ортиб бормоқда. Чунки, ижтимоий тармоқлар дастлаб одамлар орасида асосан мулоқот қилиш, маълумот алмашиш воситаси

сифатида хизмат қилган бўлса, ҳозирда оддий бир инсоннинг оилавий ёки кундалик харажатлари учун амалга оширадиган тўлов воситаси бўлиш билан бирга халқаро даражадаги мисли кўрилмаган миқдордаги молиявий муносабатларни амалга оширишнинг асосий воситаси бўлиб хизмат қилмоқда.

Ҳар қандай ҳолатда ҳам фирибгарларнинг айёрлиги, уддабуронлиги бевосита фирибгарлик жиноятини фош этишни қийинлаштиради. Шу боис тезкор суриштирувни амалга оширувчи ходимлар фирибгарларга оид ўзига хос таърифномаларни билишлари лозим. Бунда муайян гумонланаётган шахс ва жабрланувчи тўғрисидаги маълумотларни атрофлича ўрганиш талаб қилинади[6].

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликнинг криминалистик тавсифи элементлари қуйидагилардан иборат: жиноят содир қилиш тўғрисидаги дастлабки ахборотлар; фирибгар шахси; жиноятнинг содир этилишидаги шарт-шароитлар; фирибгарликнинг содир этилиш йўли, уни яшириш усуллари ва ўзига хос оқибатлари; жиноятнинг содир этилишига имкон берган сабаб ва шарт-шароитлар.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликдан жабрланган шахслар ёки уларнинг қариндошлари берган аризаларда, айрим ҳолларда эса давлат, жамоат, корхона ва муассасалардан келиб тушган мурожаатларда жиноят содир этган шахс тўғрисида етарлича маълумотлар қайд этилмайди. Шу билан бирга, жиноят ҳодисаси, унинг содир этилиш механизми, эпизодлари ва бошқа иш учун муҳим ҳолатлар тўғрисида етарлича маълумотлар бўлмайди.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликлар бўйича дастлабки маълумотларнинг таснифини аниқлаш терговчига жиноят ишини қўзғатиш ёки қўзғатишини рад қилиш тўғрисидаги масалани ҳал этишга, содир бўлган воқеанинг таърифи, жиноятни содир қилиш йўли ва уни яшириш усуллари, жиноятчининг шахси тўғрисидаги асосли гумонларни ишлаб чиқишга ёрдам беради ва натижада содир этилган жиноятни фош этиш бўйича вазифаларни тўғри баҳолаш, унинг йўналишини белгилаш ва фирибгарни қидириш ҳамда у томонидан қонуний ўзлаштирилган мулкни топишда ўзига хос аҳамиятга эга ҳисобланади.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликнинг содир этилиши кўпроқ объектив омиллар билан белгиланади[7]. Уларга тажовуз қилинаётган предмет хусусияти, унинг вақти, жойи ва жиноят содир этишнинг бошқа объектив шарт-

шароитларини киритиш мумкин. Ахборот технологиялари кенг қўлланилаётган ҳамда молиявий хизматлар истеъмолчилари билан ўзаро муносабатларда масофавий хизмат кўрсатиш каналлари кенгайиб бораётган ҳозирги шароитда ишонувчан ҳамда молиявий саводхонлик даражаси етарли бўлмаган фуқароларга нисбатан фирибгарлик ҳаракатлари кузатилмоқда. Бу каби фирибгарлик ҳолатлари банк картаси эгасининг хабарисиз унинг карта ҳисобварағидан пул маблағини ечиб олиш, пароль ва ПИН-кодларни ўғирлаш ва бошқа ноқонуний фаолият турлари билан боғлиқ[8].

Ахборот технологияларидан фойдаланиб содир этилган фирибгарлик ўйлаш учун вақт қолдирмай, турли гаплар билан чалғитиб, карта маълумотларингизни айёрлик билан қўлга киритади ёки ёлғонларига ишонтириб, пул маблағларини уларга ўз хоҳишингиз билан ўтказиб беришга ундайди. Шу сабабли, ахборот технологияларидан фойдаланиб содир этилган фирибгарларнинг турли баҳоналар билан банк картадаги маълумотларини (карта рақами, ПИН-код, шунингдек, СМС-код ва бошқа шахсий маълумотлар) билиб олишга уринишларига жавоб бермаслик керак.

Агарда шахсга ўзини банк, ҳуқуқни муҳофаза қилиш идораси ёки бирон савдо ташкилоти ходими деб таништирган нотаниш фуқаролардан қўнғироқ бўлганда, уларнинг сўзларига ёки кўрсатмаларига амал қилишга шошилиш керак эмас ва шахсий маълумотларини ошкор қилмаслик керак. Ҳар қандай шароитда ҳам банк карта тўғрисидаги маълумотларни (карта рақами, ПИН-код, банк картасининг олд қисми расмлари) ҳамда ўз шахсий маълумотларини бегона фуқароларга ошкор қилиш ва юбориш мумкин эмас.

Жиноятни содир қилиш йўлини аниқлаш учун жиноятчининг тегишли малакалари даражасини белгилаш, яъни жиноятни содир этишда қўлланилган усул, тажовуз қилинаётган мулк ва унинг эгасини аниқлаш катта аҳамиятга эгадир. Жумладан, бугунги кунда ахборот технологияларидан фойдаланиб содир этилган фирибгарлик ўзгалар мулкини талон-тарож қилишнинг нисбатан кўп тарқалган тури бўлиб ҳисобланади. Ҳозирги кунда фирибгарликнинг умумий динамикаси, унинг кўринишлари кўпайиб бораётганлиги ҳам мавзунинг долзарблигидан далолат беради. Ундан ташқари, ҳаёт кечириш учун зарур маблағларни одамларни алдаш йўли билан топаётган шахс фақат жиноятчи сифатида хавфли бўлмай, унинг қилмиши туфайли давлатга, фуқароларга моддий зарар етказилиши билан бир қаторда, фирибгарлик оқибатлари аҳолига, айниқса ёшлар тарбиясига салбий таъсир кўрсатмоқда. Бундай ўсиш динамикаси

фирибгарликка қарши курашишнинг замонавий усулларини жорий этишни тақозо қилади.

Айни пайтда мамлакатимиз бутун дунёда авж олган жиддий иқтисодий рақобат шароитида иқтисодиётни барқарорлаштириш ва ривожлантириш йўлидан бормоқда. Замонавий ахборот-телекоммуникация тизимлари ва молия-банк секторини такомиллаштиришсиз иқтисодиётни ривожлантириш мумкин эмас, бу эса, ўз навбатида, янги технологияларни ишлаб чиқиш ва банк хизматларининг жозибадорлиги, самарадорлиги ва ишончлилигини ошириш воситаларини излашни тақозо этади[9]. Шубҳасиз, бундай воситалардан бири банк пластик картаси бўлиб, у ўзига хос, кўп функцияли банк маҳсулотидир. Замонавий тараққиёт билан бирга ахборот технологияларидан фойдаланиб содир этилган фирибгарлик ҳам тобора замонавийлашиб, энг сўнгги ахборот-коммуникацион технологиялар (АКТ) воситаларини қўллаган ҳолда содир этилмоқда.

Дунёда ижтимоий-иқтисодий муносабатлар ҳамда рақамли иқтисодиёт ривожланиши, хусусан, мулкий характердаги битимларни онлайн интернет платформалари орқали расмийлаштиришини оммалашиши билан мулкий ҳуқуқлар дахлсизлигини таъминлашга оид қонун ҳужжатларини такомиллаштириш асосий вазифалардан бири бўлиб қолмоқда. Дунё иқтисодий тизимидаги жадал ўзгаришлар замирида фирибгарлик содир этиш анча осонлашди ва у дунёда латентлиги юқори бўлган жиноятлардан бирига айланди. Жумладан, PwC халқаро илмий тадқиқот маркази томонидан 2024 йилда ўтказилган тадқиқотларга кўра сўнгги 2 йил ичида дунёнинг етакчи компаниялари иқтисодий жиноятчилик натижасида кўрган зарарининг 47 фоизи фирибгарликка тўғри келиши, жорий йилда эса ушбу компанияларга 42 млрд доллар миқдоридаги зарар етказилганлиги сўнгги 20 йилдаги энг юқори кўрсаткич сифатида қайд этилган[10].

Банк карталари, турли хил молиявий “пирамидалар” ва бошқа янгича шаклдаги фирибгарлик жиноятлари унинг умумий жиноятчиликдаги салмоғини тобора ошириб бормоқда. Мисол учун, молиявий пирамида тузишда айбдор оғзаки ёки ёзма битим тузиб, ушбу битим шартларига амал қилади, битим шартлари бўйича белгиланган фоизлар ўз вақтида тўлаб борилади, битимда назарда тутилган вақт келганида пуллар тўлиқ қайтарилади.

Бу билан айбдор кўпроқ фуқароларни ўзининг жиноий “молиявий пирамида” сига жалб қилади. Бунда айбдор янгидан пул киритаётган фуқароларнинг пуллари эвазига муқаддам олинган мажбуриятларини бажариб боради.

Айбдор қабул қилиб олган пуллари учун банклар ва бошқа кредит ташкилотларига нисбатан юқори фоиз тўлаб, пулларни қайтарилишидаги қатъий интизоми эвазига ўзининг “мижозлари” ни сонини кўпайишига эришади.

Бунда фуқаролар томонидан ушбу “моливий пирамида”га кириталётган пуллар ҳеч нима билан кафолатланмаган бўлиб, пул тушуми тўхтаб қолса, моддий қимматликлар киритган барча фуқаролар ўзларини моддий қимматликларини тиклай олмайдилар, яъни мазкур фаолиятнинг охири кўплаб фуқароларни касодга учратиш билан тугайди.

Шунингдек, хизмат кўрсатиш, электрон савдо соҳаларида шу жумладан, интернет орқали авиачипталар, маиший техника ва бошқа маҳсулотларни сотиб олиш жараёнида интернет фирибгарликни содир этиш ҳолатлари кўплаб кузатилмоқда.

Фирибгарлар томонидан АКТ воситаларининг замонавий турларидан фойдаланиб жиноят содир этилган ҳолатларда қилмишни квалификация қилишда фирибгар томонидан қўлланилган замонавий воситаларни “компьютер техникаси воситаси” сифатида малакалашда вужудга келаётган муаммоларни бартараф этиш учун айнан норманинг шу қисмини қайта таҳрирдан ўтказиш лозим. Фуқароларнинг фирибгарлар таъсирига тушиб қолиш ҳолатлари йилдан йилга кўпаймоқда. Айрим шахсларнинг фирибгарликни касб этиб олиши, кўплаб инсонларни алданиб қолишга сабаб бўлмоқда.

Фирибгарликка қарши курашда энг аввало, уни олдини олиш ва барвақт аниқлаш масалалари долзарб масалалардан бири саналади. Ўзбекистон Республикаси Марказий банки томонидан тақдим этилган маълумотларга кўра, 2024 йилнинг 9 ойи мобайнида банк пластик карта эгаларига етказилган моддий зарар миқдори 2022 йилда 6 млрд., 2023 йилда 80 млрд., 2024 йилнинг 9 ойи давомида 286,8 млрд. сўм миқдорни ташкил этган, шундан ундирилган пул маблағлари миқдори 2022 йилда 2 млрд., 2023 йилда 9 млрд., 2024 йилнинг 9 ойи давомида 12 млрд. сўм миқдорни кўрсатмоқда. Биргина сўнгги 9 ойдаги қайтарилган маблағлар миқдори ўзлаштирилган маблағга нисбатан атиги 4,2 %ни ташкил этганлиги ҳам ачинарли ҳолатдир.

Аҳолининг ҳуқуқий билимларини оширишга доир вазифаларнинг умумий тусда белгиланганлиги ҳамда уларни амалга оширишнинг аниқ таъсирчан механизми мавжуд эмаслиги, жамиятда ҳуқуқий маданиятни юксалтириш борасидаги ишларнинг самарасиз олиб борилаётганлигини кўрсатади.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликнинг содир бўлиш жараёнида жабрланувчиларнинг ўзлари кўпинча ўз ҳаракатлари билан жиноят содир этилишига сабабчи бўлиб қоладилар. Фирибгарликнинг келиб чиқишига кўпинча айрим фуқароларнинг бахиллик, очкўзлик, пулга ҳирс қўйиш, тез бойиб кетишга ва бунинг учун ноқонуний равишда маълум имтиёзларни ёки қимматбаҳо нарсаларни ўзлаштиришга ҳаракат қилишлари сабаб бўлади. Бундай «жабрланувчилар» фирибгарлик тўғрисида ички ишлар органларига хабар бера олмайдилар, фирибгарлар ҳам ушбу ҳолатни ҳисобга оладилар ва бу уларга қўл келади. Жабрланувчининг шахсини ўрганишда ва жиноят содир бўлишида, унинг роли қандай эканлигини ёдда тутиш керак, чунки у томонидан ҳам жиноят содир этиш ёки унга суиқасд қилиш имконияти бор.

Шундай қилиб, ахборот технологияларидан фойдаланиб содир этилган фирибгарликни фош этишда исботланиши лозим бўлган ҳолатлар мавжуд бўлиб, уларга жиноятни содир этиш усули, жиноят содир этилишида жабрланувчининг роли, фирибгарлик жиноятининг содир этилишига имконият яратган шароитлар киради.

ПРОКУРОРНИНГ НАЗОРАТ ВАКОЛАТЛАРИНИ ЎЗГАРИШИ БИЛАН БОҒЛИҚ БАЪЗИ МУЛОҲАЗАЛАР (жиноят процесси мисолида)

Иброхимов Бахтиёр Тойиржонович,
Ўзбекистон Республикаси ҳуқуқни муҳофаза қилиш академияси мустақил изланувчиси

Ўзбекистон истиқлолга эришгандан сўнг прокурор назоратини ҳуқуқий тартибга солиш даврида сезиларли ўзгаришларга дуч кела бошлади, хусусан судга қадар иш юритиш босқичида қамоққа олиш тарзидаги эҳтиёт чорасининг судлар томонидан қўлланилиши билан боғлиқ жараёнлар.[1]

Терговга қадар текширув, тезкор-қидирув фаолияти, суриштирув ва дастлабки тергов устидан суд назорати тасдиқланиши билан прокурор назорати таъқиб органларининг процессуал ҳаракатларининг қонунийлиги ва асослилигини таъминлашнинг ягона воситаси бўлмай қолди. Маълумки, ислоҳотлар, биринчи

[1] "Судга қадар иш юритиш босқичида қамоққа олиш тарзидаги эҳтиёт чорасининг судлар томонидан қўлланилиши тўғрисида"ги Ўзбекистон Республикаси Олий суди Пленумининг Қарори, 14.11.2007 йилдаги 16-сон.

навбатда, прокурорнинг жиноят ишини қўзғатиш босқичида, суриштирув ва дастлабки тергов давридаги ўрни ва ролига таъсир кўрсатди. Бироқ, процессуал мажбурлов чораларини қўллашда прокурорнинг ваколатлари доирасидаги ўзгаришлар, прокурор жиноят иши юритувида иштирок этиши энг муҳим процессуал кафолат сифатида ўз аҳамиятини йўқотмади. Бугунги кунда, прокурор жиноят процессида асосий иштирокчиларидан бири бўлиб қолмоқда. Шу билан бирга, прокурор назорати фаолиятининг мазмун-моҳияти масалалари ҳамон илмий доирада диққат марказидадир.

Албатта, бу ислоҳотлар, норматив-ҳуқуқий ҳужжатларга ҳам ўз таъсирини кўрсатди. Бинобарин, Ўзбекистон Республикаси Конституцияси 27-моддаси учинчи қисмида "Шахсга нисбатан ҳибсга олишга, қамоққа олишга ва қамоқда сақлашга фақат суднинг қарорига кўра йўл қўйилади. Шахс суднинг қарорисиз қирқ саккиз соатдан ортиқ муддат ушлаб турилиши мумкин эмаслиги белгиланиб қўйилган".[2]

Ўзбекистон Республикасининг Жиноят-процессуал кодекси (кейинги ўринларда ЖПК) 29-моддасига биноан, эҳтиёт чораларини қўллаш ёхуд қамоқда сақлаш ёки уй қамоғи муддатини узайтириш масалалари билан боғлиқ илтимосномаларни суд томонидан кўриб чиқилади.[3]

Шунингдек, "Прокуратура тўғрисида"ги Қонуннинг 28-моддасида суриштирувчи, терговчи тақдимномасига биноан, эҳтиёт чораси сифатида қамоқда сақлаш ёки уй қамоғи ва айбланувчининг тиббий муассасада бўлиши муддатини узайтириш тўғрисида судга илтимоснома киритади.[4]

Бу тенденциялар, албатта қонун чиқарувчи томонидан қабул қилинган прокурорнинг ваколатларини чекловчи нормаларнинг ҳаммаси ҳам муайян объектив воқелик билан асосланган ва такомиллаштирилган.

Чунончи, Ўзбекистон Республикасининг Жиноят-процессуал кодексининг умумий қоидаларига мувофиқ, жиноят ишларини юритиш халқаро ҳуқуқнинг умум эътироф этган нормаларига ҳамда Ўзбекистон Республикасининг бошқа давлатлар билан тузилган шартнома ва битимларига асосланганлиги мустаҳкамлаб қўйилган.[5]

---

[2] Ўзбекистон Республикасининг Конституцияси. – Т.: Ўзбекистон, 2023.
[3] Ўзбекистон Республикасининг Жиноят-процессуал кодекси. – Т.: Ўзбекистон, 2023.
[4] Ўзбекистон Республикасининг "Прокуратура тўғрисида"ги Қонуни. Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 2001 й., 9-10-сон, 168-модда.
[5] Ўзбекистон Республикасининг Жиноят-процессуал кодекси. – Т.: Ўзбекистон, 2023.

Демак, жиноят процессининг дастлабки босқичида эҳтиёт чорасини қўллаш билан боғлиқ масалалар яъни суд фаолиятининг ҳуқуқий асоси Ўзбекистон Республикаси ҳуқуқ тизимида амалга оширилган халқаро-ҳуқуқий ҳужжатларни ҳам ўз ичига олади.

Мисол учун, “Фуқаровий ва сиёсий ҳуқуқлар тўғрисида”ги Халқаро Пактнинг 9-моддаси 3-бандида, жиноий айблов бўйича ҳибсга олинган ёки ушлаб турилган ҳар бир шахс зудлик билан судья ёки қонун бўйича суд ҳокимиятини амалга ошириш ҳуқуқи бўлган бошқа мансабдор шахс ҳузурига келтирилади ва оқилона муддатда суд муҳокамаси ўтказилиши ёки озод қилиб юборилиши ҳуқуқига эга. Суд муҳокамасини кутаётган шахсларнинг қамоқда сақланиши умумий қоида бўлмаслиги керак, бироқ озод қилиш судга келиш кафолатлари берилишига, суд муҳокамасига унинг ҳар қандай босқичига келишга ва, зарур ҳолларда, ҳукм ижро этилиши учун келишга боғлиқ қилиб қўйилиши мумкин.[6]

Эҳтиёт чоралари шахснинг процессуал чеклашнинг энг қатъий шаклидир. Эҳтиёт чораси - жиноят содир этишда гумонланаётган шахсга нисбатан келгусида жиноятни давом эттиришини олидини олиш ва жиноят процессида иштирок этишини таъминлаш мақсадида қўлланиладиган мажбурлов чораларининг бир тури ҳисобланади.

Баъзилар эҳтиёт чорасини қўллашни прокурор санкция асосида амалга ошириш зарурлиги тўғрисида фикр билдирсалар, айримлар олимлар эҳтиёт чораси суд рухсати орқали амалга ошириш жиноят процессини демократлаштириш воситаси деб билишади.[7]

Бизнинг фикримизча, миллий ҳуқуқ тизимимизга халқаро-ҳуқуқ нормаларни имплементация қилиниши, яъни судга қадар иш юритиш босқичида қамоққа олиш тарзидаги эҳтиёт чорасининг судларга ўтказилиши жиноят процессида шахс ҳуқуқ ва эркинликлари ҳамда қонуний манфаатларини таъминлайдиган қўшимча процессуал воситалар ва механизмлар сифатида қараш лозим. Ушбу ваколатларни судларга берилиши, прокурор ваколатларини чекланишига олиб келадими деган савол ўринлидир. Ахир, бу масалалар прокурорнинг асосий функцияси билан боғлиққу деган фикр бизни ўйлантириб қўяди. Келинг шу мунозарали саволни атрофлича таҳлил қилиб чиқамиз.

---

[6] Ўзбекистон Республикаси мазкур Халқаро пактга Ўзбекистон Республикаси Олий Мажлисининг 1995 йил 31 августдаги 127-I-сонли “1966 йил 16 декабрдаги фуқаровий ва сиёсий ҳуқуқлар тўғрисидаги халқаро пактга қўшилиш ҳақида”ги қарорига асосан қўшилган.

[7] Шодиев Ғ.М. Фуқароларнинг ҳуқуқ ва эркинликларини чекловчи тергов ҳаракатлари устидан суд назорати: Юрид. фан. номз. ... дисс. автореф. – Т., 2010. – 5 б. Пакирдинов М.А. Санкция прокурора в досудебном производстве. // Вестник КазНУ. Серия юридическая. - № 1.- 2004.

Агар Ўзбекистон Республикаси Конституцияси 55-моддаси иккинчи қисмига назар ташлайдиган бўлсак, “Ҳар кимга мансабдор шахсларининг қонунга хилоф қарорлари, ҳаракатлари ва ҳаракатсизлиги устидан судга шикоят қилиш ҳуқуқи берилган”. Яъни бузилган ўз ҳуқуқлари ва эркинликларини суд орқали ҳимоя қилиш мумкин.[8]

Шунингдек, ЖПКнинг 27-моддасига кўра, жиноят процесси иштирокчилари ва бошқа шахслар, шунингдек жиноят ишини юритишдан манфаатдор бўлган юридик шахсларнинг вакиллари белгилаб қўйилган тартибда ва муддатда терговга қадар текширув, тезкор-қидирув фаолиятини амалга оширувчи мансабдор шахслар, суриштирувчи, терговчи, прокурор, судья ва суднинг процессуал ҳаракати ёки қарори устидан шикоят беришга ҳақлилиги белгилаб қўйилган.[9]

Ёхуд, ЖПКининг 338-моддасига кўра, суднинг ажрими устидан эса юқори судга шикоят қилиниши.[10] Демак, судгача бўлган иш юритишда мансабдор шахсларининг қонунга хилоф ҳаракатлари (ҳаракатсизлиги) ва қабул қилган қарорлари устидан судга шикоят қилиш ва назорат қилиш кенг тарқалган ижобий қаралади.

Бизнингча, айрим прокурор ваколатларини (санкция) судга берилиши кўпроқ фуқароларнинг қонуний манфаатларини ҳисобга олганлиги нуқтаи назардан тўғридир. Негаки, прокурор кўпроқ жиноятларни очиш ва айблов вазифасини бажариш учун жавобгардир. Агар амалиётга назар ташлайдиган бўлсак, кўпроқ прокурор фаолияти қонуннинг аниқ ва қатъий бажарилишини таъминлашга қаратилган қонун қўриқчиси сифатида эмас, балки жиноят иши юритилишида айблов (тараф) натижаларидан манфаатдор бўлган шахс сифатида иштирок этади. ЖПК ва “Прокуратура тўғрисида”ги Қонунларда прокурорнинг асосий вазифаси жиноят содир этган шахсни аниқлаш ва унга нисбатан қонунда назарда тутилган жазо қўлланилишини таъминлаш ҳисобланади (ЖПК 15-модда). ЖПК 33-моддасига кўра, прокурор суриштирув ва дастлабки тергов босқичларида қонуннинг бузилишини аниқлаш ва бартараф этиш учун қонунда назарда тутилган чора-тадбирларни ўз вақтида кўриши шарт ҳисобланади. Шундай қилиб, прокурорнинг асосий функцияси таъқиб қилиш ва айблов билан боғлиқ. Бундан ташқари, “Судлар тўғрисида”ги

[8] Ўзбекистон Республикаси Конституцияси. – Т.: Ўзбекистон, 2023.
[9] Ўзбекистон Республикасининг Жиноят-процессуал кодекси. – Т.: Ўзбекистон, 2023.
[10] Ўзбекистон Республикасининг Жиноят-процессуал кодекси. – Т.: Ўзбекистон, 2023.

Қонуннинг 4-моддасига мувофиқ, суднинг асосий вазифалари фуқароларнинг Ўзбекистон Республикаси Конституцияси ва қонунлари, инсон ҳуқуқлари халқаро шартномаларида кафолатланга ҳуқуқлари, эркинликлари, юридик шахсларни ҳуқуқлари ва қонуний манфаатларини ҳимоя қилишдан иборатдир.[11] Суд ўз ваколатини амалга оширда доимо беғараз ва холис тараф этади. Демак, суд прокурорга қараганда кўпроқ фуқароларни ҳуқуқ ва эркинликларини ҳимоя қилиш қаратилган.

Аммо, суд назорати прокурор назоратини ўрнини алмаштира олмайди. Ва, буни тасдиқлаш учун бир қанча сабабларни келтириш мумкин: **биринчидан,** *жиноят иши бўйича суриштирув ва терговнинг боришини прокурор назорат қилади яъни судгача бўлган процессда прокурор назорати жиноят иши қўзғатилган пайтдан эътиборан ва тугалланган жиноят иши судга юборилгунга қадар ёки жиноят ишини тугатиш тўғрисида қарор қабул қилингунга қадар амалга оширилади, бу эса ҳуқуқбузарликларни ўз вақтида аниқлаш ва уларга чек қўйишга ёрдам беради*; **иккинчидан,** *прокурорга жиноий иш бўйича барча керакли маълумотлар ўз вақтида келиб тушади ва тезкорлик (таъсир чора-тадбирларни кўриш) билан ҳаракат қилиши мумкин, бунда суднинг вазифалари иккинчи ўринни эгаллайди*; **учинчидан,** *жиноят иши юритаётган мансабдор шахслар томонидан берилган маълумотлар прокурорга давом этаётган суриштирув ва тергов ҳақида тўлиқ тасаввур эга бўлади, бу эса тўғри қарор қабул қилишга ёрдам беради. Суд эса муайян жиноят ишининг моҳиятини тўлиқ тушунмаган ҳолда, эҳтиёт чораси сифатида қамоққа олишни асоссиз равишда рад этиши ёки аксинча, рухсат бериши мумкин. Буларнинг барчаси, шубҳасиз, судгача бўлган иш юритишда назоратининг сифатига, хусусан, қамоққа олиш тарзидаги эҳтиёт чорасини қўллашга таъсир қилади*; **тўртинчидан,** *суд назорати суд фаолиятининг ўзига хос хусусиятидан келиб чиққан ҳолда, фақат вақти-вақти билан амалга оширилиши мумкин, мисол учун жиноий таъқиб қилувчи органларнинг хатти-ҳаракатлари ва қарорлари устидан шикоятни кўриб чиқишда ёки айрим процессуал ҳаракатларга рухсат беришда* (масалан, ҳибсга олиш).

Юқоридагилардан келиб чиқиб, қамоққа олишга санкция бериш ҳуқуқи судларга ўтказилишининг ижобий ва салбий томонларни таҳлил қиламиз: 1) биз юқоридаги параграфларда таъкидлаганимиздек, қамоққа олиш санкция бериш ҳуқуқи судларга ўтказилиши судга қадар иш юритишда судда тарафларда

[11] "Судлар тўғрисида"ги ЎзР Қонуни, 28.07.2021 йилдаги ЎРҚ-703-сон.

тортишувчанлик принципи юзага келади яъни тарафларда тенг имкониятлар юзага келади (фикр билдириш, далилларни тақдим этиш). Бундай ҳолда таъқиб томонда, суднинг розилигини олиш учун асосли ва етарли тақдим этиш учун кўпроқ ҳаракат қилишга тўғри келади, суд эса, холис ва беғараз иштирокчи сифатида тарафларни тинглайди ва қарор қабул қилади; 2) қамоққа олиш сакция судларга берилиши салбий оқибатларга олиб келиши мумкин, негаки судгача бўлган даврда эҳтиёт чорасини кўллаган судья, келгусида худди шу ишни кўриб чиқиши мумкин, бу туман миқиёсида кўп учрайдиган ҳолат, агар судга бўлган даврда судья нотўғри мажбурлов чораларини қўллаганлигини аниқласа ёки хато йўл қўйганини билса, унда суд муҳокамасида судьяда холислик ва беғаразлик масалаларига шубҳа уйғотади, бундай ҳолатда хато йўл қўйганини билса, ҳар қандай судья судланувчини айбдор деб ҳукм чиқаришга ҳаракат қилади. Айниқса, суд тизимида корпоративлик мавжуд (дўстона муносабат, курсдош, устоз ва шогирд анъаналари, симпатия, боғлиқлик, коррупция ва бу ҳолат жиноят процесс иштирокчилар ўртасида шубҳа туғдирмаслик лозим) ва бу салбий таъсирини олдини олади. Қамоққа олиш эҳтиёт чораси қўлланилиши шахснинг айби тўғрисидаги хулосани олдиндан белгиламайди (Конституция 28-модда), жиноят ишини юритаётган мансабдор шахс (суриштирувчи, терговчи) фақат далилларни тўплайди ва тақдим этади ва бу амалий жиҳатдан судьянинг ҳукм чиқаришдаги холислигига таъсир қилмаслиги керак. Шу мақсадда, агар миллий жиноят процессуал қонунчилигимизга тергов судьяси институтини жорий қилинсагина, бундай ҳолатни истисно қилиш мумкин. Ва, бу суд тизимига салбий таъсир ўтказмайди; 3) прокурор таъқиб орган бўлган учун суриштирувчини, терговчинига (эҳтиёт чорасини қўллаш тўғрисидаги илтимосномани) қўллаб-қувватлаши мумкин.

Келинг, шу процессуал ҳаракатлар механизмини таҳлил қилиб чиқамиз. Бу процессуал ҳаракат ЖПК 243-моддасида батафсил ёритилган. Айтиш мумкинки, дастлаб суриштирувчи, терговчи шахсга нисбатан қамоққа олиш тўғрисидаги эҳтиёт чорасини қўллаш учун тегишли қарор қабул қилади. Бунда, суриштирувчи, терговчи шахсга нисбатан қамоққа олиш тўғрисидаги эҳтиёт чорасини қўллашда прокурорни четлаб ўтиши мумкинми деган савол туғилади, яъни суриштирув ва дастлабки тергов ҳаракатини ўтказишга рухсат сўраб мустақил равишда судга мурожаат қилишга ҳақлими, албатта хақли эмас, негаки суриштирувчи ва терговчи фақат прокурорнинг розилиги билан судга тегишли илтимоснома билан мурожаат қилиш мумкин. Бошқа қилиб айтганда, суриштирувчи ва терговчи

томонидан берилган илтимоснома фақат прокурорнинг ижобий қарори билан судга юборилиши мумкин. Суд (судья) қамоққа олиш тўғрисидаги илтимоснома олгандан якка тартибда тегишли материалларни ўрганиб ва тарафларни иштирокида кўриб чиққандан сўнгина у ёки бу қарорни қабул қилади.

Юқоридагилар шуни англатадики, шахснинг конституциявий ҳуқуқ ва эркинликларини чекловчи суриштирув, дастлабки тергов ҳаракатини амалга ошириш тўғрисидаги қарорни қабул қилишда учта субъект – (суриштирувчи) терговчи, прокурор ва суд иштирок этаётганлигини англатади, уларнинг ҳар бири бу жараёнда ўзига хос рол ўйнайди.[12]

Мисол учун, (суриштирувчи) терговчи – дастлабки тергов ҳаракатларида жиноят ишини қўзғатишга фактик асослар мавжудлигини, далилларни тўплаш ва текшириш нуқтаи назардан ҳаракат қилади (ЖПК 43, 46[1]-боб).

Прокурор – суриштирувчи ва терговчи томонидан қабул қилинган қарорнинг қонунийлиги ва асослилигини (тўғри баҳоланганлигини текширади) текшириш (қўшимча далилларни сўраши мумкин) мажбуриятидан ҳаракат қилади (ЖПК 243-моддаси тўртинчи қисми).

Суд – суриштирувчи, терговчи томонидан жиноятга оид тўпланган фактик далилар ва прокурор суриштирувчи, терговчи томонидан қабул қилинган қарорнинг қонунийлиги ва асослигини текширгандан сўнг, холис ва беғараз тараф сифатида қамоққа олиш ёки уй қамоғи тарзидаги эҳтиёт чорасини қўллаш ҳақидаги ёки уни қўллашни рад қилиш тўғрисидаги ажримини қабул қилади (ЖПК 243-моддаси бешинчи ва олтинчи қисмлари).

Шундай қилиб, қуйидаги асосий хулосаларга келишимиз мумкин:

1. Қамоққа олиш тўғрисидаги эҳтиёт чораси қўллашни прокурор ваколатларига ўтказилиши дастлаб Ўзбекистон Республикаси Конституцияси ва халқаро умумэътироф этилган нормаларига зид келади, деб хулоса қилишимиз мумкин, чунки Ўзбекистон Республикаси Конституцияси ва халқаро ҳуқуқнинг умумэътироф этилган принцип ва нормалар Ўзбекистон Республикаси ҳудудида энг юқори юридик кучга эга бўлган ҳужжат ҳисобланади ва давлатимизнинг асосий қонунидир.

[12] Ўзбекистон Республикасининг Жиноят-процессуал кодекси. – Т.: Ўзбекистон, 2023.

2. Шахсларларнинг конституциявий ҳуқуқ ва эркинликларини чекловчи қарорлар ва ҳаракатлар суднинг ҳуқуқий табиатига хос эмас, чунки қамоққа олишга санкциялар судга айблов характерини беради ҳамда ваколат бериш орқали судьяга илгари тергов жараёнида ўзи қабул қилинган қарорга қарши чиқиш ноқулай ҳолатга мажбур қилади ва бу одил судловни амалга оширишда холислик ва беғаразлик принципининг бузилишига олиб келади. Бундан ташқари, судгача бўлган босқичларида прокурорга қараганда судья доимий ва тезкор назоратни таъминлай олмайди. Бу ўз навбатида, суд назорати дастлабки тергов жараёнида қарорлар қабул қилиш самарадорлигини пасайишига олиб келади.

3. Суд назорати прокурор назоратини алмаштирмади, балки шахс ҳуқуқ ва эркинликларининг процессуал кафолатлари тизимини, шу жумладан, ушбу ҳуқуқ ва эркинликларни чекловчи суриштирув ва тергов ҳаракатлари бўйича қарорлар қабул қилишда манфаатларини ҳимоя қилади. Кўринишидан, бундай суриштирув ва тергов ҳаракатларини ўтказиш тўғрисида қарор қабул қилишнинг амалдаги тартиби прокурорнинг ушбу қарордан четлаштирилмаганлигини (прокурорнинг розилиги олинади) таъкидлаш учун барча асослар беради.

АХБОРОТ ТЕХНОЛОГИЯЛАРИ ОРҚАЛИ СОДИР ЭТИЛГАН ФИРИБГАРЛИК ЖИНОЯТЛАРИНИ ФОШ ЭТИШДА ҲАМКОРЛИК МАСАЛАЛАРИ

Анвар Алиқулович Таштемиров
Ўзбекистон Республикаси ИИВ Академияси,
Маъмурий ҳуқуқ кафедраси доценти.
E-mail: *anvartoshtemirov05031979@gmail.com*

Аннотация*:Ушбу мақолада ахборот технологияларидан фойдаланиб содир этилган фирибгарликни фош этишда тезкор хизмат ходимларининг соҳавий хизматлар билан хамкорлик масалалари, ўзига хос жиҳатлари, мавжуд муаммолар ёритилиши билан бирга, ҳамкорлик доирасида етакчи мутахассисларнинг фикр ва мулоҳазаларига асосланиб ушбу жиноятларни фош этиш бўйича тегишли хулосалар берилган.*

Калит сўзлар: *Ахборот технологиялари орқали содир этилган фирибгарлик, кибержиноят, киберфирибгарлик, ижтимоий тармоқ, ахборот макони, банк пластик картаси, электрон манзил, аккаунт.*

Аннотация: *В данной статье рассматриваются вопросы взаимодействия сотрудников оперативной службы с профильными службами в*

раскрытии мошенничества, совершённого с использованием информационных технологий, их особенности и существующие проблемы. Кроме того, на основе мнений и размышлений ведущих специалистов в рамках сотрудничества даны соответствующие выводы по раскрытию данных преступлений.

Ключевые слова: *Мошенничество, совершенное с использованием информационных технологий, киберпреступление, кибермошенничество, социальная сеть, информационное пространство, банковская пластиковая карта, электронный адрес, аккаунт.*

Annotation*: This article examines the issues of cooperation between operational service officers and specialized services in uncovering fraud committed using information technologies, their specific features, and existing problems. Additionally, based on the opinions and reflections of leading specialists within the framework of cooperation, relevant conclusions on solving these crimes are provided.*

Keywords: *Fraud committed with the use of information technology, cybercrime, cyberfraud, social network, information space, bank plastic card, electronic address, account.*

Бугунги кунда, Республикамизда аҳолини сифатли ва хавфсиз телекоммуникация ва интернет хизматлари билан таъминлаш борасида бир қатор ишлар амалга ошириб келинмоқда. Айниқса, бу борада соғлом интернет-муҳитига эга ахборотлашган жамиятни ривожлантириш, миллий сайтларни кўпайтиришга алоҳида эътибор берилган. Шу билан бир қаторда, шахсларни интернет хуружларидан ҳимоя қилиш, ахборот олиш ва тарқатиш маданиятини тарғиб қилиш, тармоқ хавфсизлигини таъминлаш юзасидан кўплаб чора-тадбирлар амалга оширилмоқда. Оммавий ахборот воситалари орқали мунтазам равишда интернет тармоқларидан фойдаланиш қоидалари, веб-макондаги хавф ва фирибгарликларга қарши курашиш усуллари тушунтирилмоқда.

Ўзбекистон Республикаси ИИВ Киберхавфсизлик Маркази ходимлари иштирокида АОКАда ўтказилган матбуот анжуманида, бугунги кунда Ўзбекистонда 25 млн. нафардан ортиқ интернет фойдаланувчилари мавжуд. Ўтказилган таҳлил натижалари бугунги кунда мамлакатда кибержиноятчиликнинг ўсиш тенденцияси кузатилаётганлиги, сўнгги 3 йилда кибержиноятлар сони бир неча бараварга ошиб кетган ҳақида маълумотлар берилди. Матбуот анжуманида қайд этилишича, кибержиноятчиликнинг қуйидаги турлари кўп содир этилаётганлиги маълум қилинган, булар:

– фирибгарлар пластик карта фойдаланувчиларига келган СМС-хабарномадаги кодларни тўловни амалга ошириш, ютуқни бериш каби баҳоналар орқали эгаллаб, ундаги маблағларни ўзлаштириши;

– шахсий маълумотларни эгаллаш ва уларни ошкор қилиш билан қўрқитиб товламачилик қилиши (кибертовламачилик);

– ижтимоий тармоқда зўрлик ишлатиш билан қўрқитиши, ҳақорат, суицид ҳолатлари (кибербуллинг) ва бошқалар[1].

Бугунги кунда таҳлиллар шуни кўрсатмоқдаки, мамлакатимизда интернет тармоқларидан фойдаланиб асосан “ўғирлик”, “фирибгарлик”, “туҳмат”, “ҳақорат”, “товламачилик” каби ҳуқуқбузарликларнинг содир этилиши кузатилмоқда. Айрим ривожланган мамлакатларда эса, “Ўзини ўзи ўлдириш даражасига етказиш”, “Ўзини ўзи ўлдиришга ундаш”, “Хат-ёзишмалар, телефонда сўзлашув, телеграф хабарлари ёки бошқа хабарларнинг сир сақланиши тартибини бузиш”, “Урушни тарғиб қилиш”, “Фарзандликка олиш сирини ошкор қилиш”, “Порнографик маҳсулотни тайёрлаш, олиб кириш, тарқатиш, реклама қилиш, намойиш этиш”, “Зўравонликни ёки шафқатсизликни тарғиб қилувчи маҳсулотни тайёрлаш, олиб кириш, тарқатиш, реклама қилиш, намойиш этиш” ва бошқа шунга ўхшаш жиноятларнинг ҳам ижтимоий тармоғи орқали содир этилаётганлиги аниқланган.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни фош этишда ИИОлари соҳавий хизматларининг ўзаро ҳамкорлик фаолияти ушбу йўналишдаги вазифалар самарадорлигида муҳим аҳамиятга эга жиҳатлардан бири ҳисобланади. Айниқса, тезкор хизмат вакилларининг тергов органлари билан ахборот алмашув, биргаликда тезкор қидирув чора-тадбирларини амалга ошириш, маълумотлар тўплаш ва уларни таҳлил этиш борасидаги ўзаро ҳамкорлик фаолиятини ушбу турдаги жиноятларни қисқа фурсатларда фош этиш тизимининг муҳим таркибий қисми дейиш мумкин.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда тезкор хизмат вакили, терговчининг терговга қадар текширувни амалга оширувчи органлари билан криминалистик ҳамкорлиги тактикасининг зарурлиги бир қатор объектив омиллар билан боғлиқ бўлиб, улар қуйидагиларда ўз ифодасини топган:

1) ҳамкорлик қилувчи субъектлар фаолиятининг криминалистик тактикасининг қоидаларига амал қилиш аҳамиятга эгалиги;

2) ҳамкорлик тактикасини қўллаётган субъектлари фаолиятининг воситалари, усуллари ва ҳуқуқий базаси ўзаро фарқ қилиши;

3) ички ишлар органларининг суриштирувчи ва терговчиларининг терговга қадар текширувни амалага оширувчи органлар билан ҳамкорлик қилиши зарурлиги.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни очишга қаратилган тергов-тезкор гуруҳи таркибида тезкор ходимнинг вазифалари сифатида қуйидагиларни таъкидлаш мумкин, яъни ушбу турдаги жиноятлар содир этилишнинг дастлабки босқичида ўтказилган тезкор-қидирув тадбирлар натижасида жиноят фош этилмаса, кейинги босқичида ўтказиладиган тезкор-қидирув тадбирлари амалга оширилади. Кейинги босқичда ўтказиладиган тезкор-қидирув тадбирлари терговчи томонидан жиноят иши қўзғатилгандан сўнг тегишли йиғмажилдлар доирасида амалга оширади.

Ҳар бир фош этилмаган ахборот технологияларидан фойдаланиб содир этилган фирибгарликни очиш учун тергов-тезкор гуруҳини тузиш бўйича буйруқ чиқарилади. Гуруҳга барча соҳавий хизматлардан жумладан тезкор йўналишдан ҳам алоҳида тезкор вакил жалб этилади. Тергов-тезкор гуруҳи аъзолари раҳбарият олдида жиноятни фош этиш юзасидан қилинган ишлар бўйича доимий равишда ҳисобот бериб боради. Гуруҳ таркибида тезкор ходимнинг асосий вазифаси “Тезкор-қидирув фаолияти тўғрисида”ги қонуннинг 4-моддасига асосан жиноятчи шахсни аниқлаш ҳамда унинг жиноий фаолиятини фош этишдан иборат бўлади[2].

Тезкор ходим жиноятни фош этиш бўйича тегишли йиғма жилдни юритади ва йиғма жилд бўйича тезкор-қидирув тадбирлар режасини ишлаб чиқади. Режада жиноятни фош этиш бўйича жиноят содир этилиш усули ҳамда дастлабки босқичда ўтказилган тезкор-қидирув тадбирлар натижасида олинган маълумотлар асосида тегишли тусмоллар илгари сурилади. Тусмолларни текшириш юзасидан тегишли тезкор-қидирув тадбирлар, уларни ўтказувчи шахслар ҳамда ўтказиш вақти белгилаб берилади. Соҳавий хизматлар билан ҳамкорлик масалаларига алоҳида эътибор қаратилади.

Ички ишлар органлар суриштирувчи ва терговчиларнинг иш натижалари ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда уларнинг терговга қадар текширувни амалга оширувчи органлари билан криминалистик ҳамкорлиги тактикаси, ушбу жиноятларни тез ва тўла очишга, жиноят ишларини ҳар томонлама, тўла ва холисона тергов қилишга, дастлабки тергов сифатини яхшилашга, жиноят содир этган ҳар бир

шахсни адолатли жазога тортишга, жиноят учун жазонинг муқаррарлигини таъминлашга, дастлабки тергов даврида қонунийликка қатъий риоя қилиниши таъминлаш ва риоя этишга шунингдек ҳамкорлик фаолиятининг изчил йўлга қўйилганлигига боғлиқ ҳисобланади.

Ҳамкорликни ташкил этишда янги усул ва услубларнинг қўлланилиши, самарали олиб борилиши, ҳамкорлик интизомини яхшилайди ва ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда ҳамкорлик тактикаси орқали муваффақиятли бажарилишига замин яратади.

Бизнинг фикримизча ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлиги тактикаси икки босқичда амалга оширилади.

Биринчи босқичда: суриштирув, терговни режалаштириш (жиноят ҳақидаги хабарни қўлга киритгандан сўнг); суд-ахборот технология ёки суд-компьютер экспертизани тайинлаш, ҳодиса содир бўлган жойни кўздан кечириш; бошқа кечиктириб бўлмайдиган тергов ҳаракатларини ўтказиш; жиноятни содир этган шахсни аниқлаш ва ушлаш.

Икинчи босқичда: далилларни тергов харакатлар орқали йиғишни давом эттириш; гумон қилинувчи, айбланувчи тариқасида ишга жалб қилиш ва ишни якунлаш.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлиги тактикаси ҳам ушбу соҳа олимлари томонидан ҳамкорликнинг давомийлигига кўра 2 та катта гуруҳга бўлинади, булар:

1) терговга қадар текширув материалларига кўра жиноят ишини қўзғатиш давридаги ҳамкорлик;

2) жиноят иши терговчининг иш юритувига ўтганидан ва жиноят иши қўзғатилгандан кейинги даврдаги ҳамкорлик[3].

Бу турдаги жиноятлар бўйича ҳамкорлик дастлабки босқичда объектив равишда навбатчилик қисмининг ҳамкорлиги билан ҳам қўшилиб кетади яъни жиноят ҳақидаги хабар навбатчилик қисмга келиб тушгач, дарҳол у суриштирувчи, терговчи ва терговга қадар текширувни амалга оширувчи органларга маълумот етказади. Бу ҳолатда навбатчилик қисми ташкилий-таъминловчи рол ўйнайди.

Шунингдек, ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлиги тактикасининг давомийлигига ва ташкил этилишига кўра қуйидаги шакллари мавжуд:

– кундалик (жорий ёки доимий);

– вақти-вақти билан амалга ошириладиган (оралиқ);

– узоқ муддатга мўлжалланган (бирон-бир иш ёки фаолият жараёнида ташкил этиладиган);

– доимий (мунтазам равишда олиб бориладиган);

– фавқулодда ташкил этиладиган.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлик тактикасининг асосий йўналишларидан бири – бу тергов ва тезкор-қидирув тусмолларини ҳамда жиноятни иссиқ изидан очиш бўйича келишилган режани ишлаб чиқиш ҳисобланади.

Бу турдаги жиноятлар билан боғлиқ ҳамкорлигининг асосий йўналишларидан яна бири – бу жиноят тўғрисидаги хабарларга ўз вақтида эътибор қаратиш, тергов-тезкор гуруҳларининг ҳодиса жойига зудлик билан чиқиш, ҳодиса жойини сифатли кўздан кечиришни ва имкони борича кўпроқ далиллар йиғишни таъминлашдан иборат.

И.М.Нурбеков томонидан жиноятларини тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлиги тактикаси жиҳатларини жиноятларни қўзғатиш ва тергов қилиш жиҳатларига оид масалалар ўрганилган[4].

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлигини ташкил этиш ўзининг айрим жиҳатлари эга бўлиб, улар қуйидагилардан иборат: тергов қилиш босқичларида уларнинг ўртасида мажбуриятларнинг тақсимланиши; тергов ва процессуал харакатларни режалаштириш; суриштирув ва дастлабки терговнинг турли босқичларида ҳамкорлик шаклларини қўллаш[5].

Т.А.Паутова томонидан жиноятларини тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлиги тактикаси нуқтаи назаридан ўрганилган ва ҳамкорликнинг қуйидаги босқичлари кўрсатиб берилган: жиноят иши қўзғатишдан бошлаб то жиноят содир этган шахс аниқлангунга қадар бўлган босқич; жиноят содир этган шахсни айбланувчи тариқасида ишга жалб этилган давргача бўлган босқич; айбланувчини биринчи марта сўроқ қилишдан бошлаб то дастлабки терговнинг тугатилишига қадар бўлган босқич[6].

Юқорида кўрсатилган ҳолатлар дастлабки терговга қадар текширув муҳимлигини белгилайди. Бунда Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлик тактикаси талабларини ҳисобга олган ҳолда юзага келиши керак, булар жумласига:

1) қонунийликка риоя қилиш;

2) текширувнинг тўлиқлиги;

3) ҳужумкорлик таъминлаш;

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликни тергов қилишда суриштирувчи, терговчининг терговга қадар текширувни амалага оширувчи органлари билан криминалистик ҳамкорлиги тактикаси жиноят-процессуал қонунга нисбатан таянган субординациявий фаолият бўлиб, терговга қадар текширувни амалга оширувчи органлари томонидан суриштирувчи, терговчининг топшириқларини бажаришга қаратилган ва тегишли мақсадлар, вазифалар ва кучлар, чораларни ўтказишнинг вақти ва шакли бўйича келишилган ҳамда содир этилган ёки содир этилаётган жиноятни очишга, жиноят содир этган шахсни жавобгарликка тортиб, жабрланувчи ва фуқаровий даъвогарга нисбатан келтирилган зарарни бартараф этишга қаратилган фаолият тушунилади.

Ушбу турдаги жиноятларга қарши курашиш, уларнинг содир этилишининг олдини олиш, содир этилган жиноятларни ўз вақтида фош этиш, шунингдек фуқароларнинг бузилган ҳуқуқларини ҳимоя қилиш ҳамда етказилган моддий зарарнинг қопланишини таъминлаш мақсадида, қуйидагилар таклиф этилади, булар:

Доимий равишда, банк пластик карталари билан боғлиқ пул ўғирлиш ва фирибгарлик ҳолатлари юзасидан келиб тушган ҳар бир мурожаатларни текширув натижаси бўйича унинг қонунийлиги ва

жазо муқаррарлигини таъминлаш мақсадида, Ўзбекистон Республикаси ИИВ тизимида республика миқёсида банк пластик карталари билан боғлиқ содир этилаётган пул ўғирлаш ва фирибгарлик ҳолатлари, интернет ижтимоий тармоқлари орқали жиноят содир этиб келаётган ҳамда ушбу турдаги жиноятларни содир этишга мойил шахслар рўйхатининг ягона базасини шакллантириш, ушбу шахслар тўғрисида маълумотларнинг вилоятлараро алмашинувини ва тезкор ишлар олиб борилишини йўлга қўйиш;

- Ҳозирги кундаги ахборот – коммуникация технологиялари соҳаси бўйича мутахасислар тайёрлаб бераётган олий ва ўрта-махсус таълим ўқув юртлари талабалари ва уларнинг битирувчилари томонидан мазкур турдаги жиноятларни содир этилишини олдини олиш мақсадида уларни ҳуқуқий онгини шакллантириш, талабалар онгида интернет тармоқлари орқали жиноят содир этилиши қонунчилик билан тақиқланганлиги ва тегишли жавобгарликни келтириб чиқариши юзасидан илмий асосланган ягона мафкуравий йўналиш ишлаб чиқиш;

- Барча таълим муассасаларида Интернет тармоғи ахборот ресурсларидан унумли фойдаланишларини кўникмасини ташкил этиш учун “Хавфсиз Интернет”, “Интернет маданияти” мавзуларида ўқув машғулотлари ташкил этиш;

- Фуқароларда ахборот технологияларидан фойдаланиб содир этилган фирибгарликнинг жабрланувчисига айланиб қолмаслик юзасидан профилактик-огоҳлантирув тадбирларини олиб боришда блогер ва ижтимоий тармоқларда кенг аудиториясига эга бўлган шахслардан кенг фойдаланиш;

- Жиноятлар профилактикасини бевосита амалга оширувчи органлар ва муассасаларнинг айрим турдаги жиноятлар профилактикасига, бу турдаги жиноятларнинг содир этилиши сабабларини ва уларга имкон бераётган шарт-шароитларни бартараф этишга, айрим тоифадаги шахсларни аниқлаш ва уларга профилактик таъсир кўрсатишга қаратилган “Хавфсиз Интернет” махсус тадбирларини ишлаб чиқиш ҳамда амалиётга жорий этиш.

- Аҳоли орасида ҳуқуқий тарғибот ишларини олиб бориш жиноятларнинг олдини олишда муҳим аҳамият касб этади. Бунда ваколатли органлар томонидан меҳнат, вояга етмаганлар каби жамоалар ўртасида ахборот технологияларидан фойдаланиб содир этилган фирибгарликнинг олдини олиш борасида тушунтиришлар, хусусан, маърузалар ўқиш, давра суҳбатлари уюштириш, тарғибот

буклетлари тайёрлаш тарқатиш катта самара беради. Ушбу тарғибот тадбирларида фуқароларда интернет тармоқлари орқали содир этилдиган жиноятларнинг салбий оқибатлари, келиб чиқиш сабаблари ва бу борада шахсларнинг хушёрлигини ошириш борасида турли вазифалар амалга оширилиши муҳим аҳамият касб этади.

Хулоса ўрнида шуни айтиш лозимки, жиноятлар профилактикасини амалга ошириш нафақат давлат органларининг, балки шу жамиятнинг аъзоси ҳисобланган ҳар бир инсоннинг вазифасидир. Энг аввало, ўзимиз, оила аъзоларимиз ва жамият олдидаги масъулиятни доимо ҳис қилиб яшаш, атрофдаги ҳодисаларга бепарволик билан муносабатда бўлмаслик, тинч ва осуда ҳаётимизнинг қадрига етиб яшаш барчамизнинг кундалик ҳаёт тарзимизга айланиши зарур.

ГИЁҲВАНДЛИК ВОСИТАЛАРИНИ КОНТАКТСИЗ УСУЛДА ЎТКАЗИШНИ АНИҚЛАШ ВА ФОШ ЭТИШ БЎЙИЧА ЎТКАЗИЛАДИГАН ТЕЗКОР-ҚИДИРУВ ТАДБИРЛАРИ ХУСУСИЯТЛАРИ

Очилов Илёс Абдураимович
Ўзбекистон Республикаси ИИВ
академияси мустақил изланувчиси

Аннотация. *Мақолада гиёҳвандлик воситаларини қонунга хилоф равишда контактсиз усулда ўтказиш билан боғлиқ жиноий фаолиятни ҳужжатлаштиришнинг асосий йўналишлари кўриб чиқилган.*

Калит сўзлар: *тезкор-қидирув фаолияти, гиёҳвандлик воситалари, контактсиз ўтказиш, Интернет тармоғи, ҳужжатлаштириш.*

Аннотация. *В статье рассмотрены основные направления документирования преступной деятельности по незаконному сбыту наркотических средств бесконтактным способом.*

Ключевые слова: *оперативно-розыскная деятельность, наркотические средства, бесконтактный сбыт, сеть Интернет, документирование.*

Summary. *The article describes the main directions for documenting criminal activity on illegal sale of drugs by contactless means, provides recommendations for conducting operational investigative action. The author concludes that each stage of documenting the contactless method of illegal sale and purchase of drugs has its own specific goals that determine the organization and tactics of operational investigative measures.*

Key words: *operatively-investigative activity, narcotic drugs, contactless sales, Internet, documentation.*

Кўриб чиқилаётган мавзунинг долзарблиги шундан иборатки, сўнгги йилларда аҳоли ўртасида гиёҳвандлик муаммоси деярли глобал офатга айланиб, давлатнинг миллий хавфсизлигига таҳдид солмоқда. Жиноятчилик таҳлили шуни кўрсатадики, 2023 йилда Жиноят кодексининг XIX бобида қайд этилган жиноятлар, яъни, гиёҳвандлик воситалари, психотроп моддалар ёки уларнинг аналоглари, кучли таъсир этувчи моддаларнинг қонунга хилоф равишда муомаласи билан боғлиқ 8461 та жиноят содир этилган бўлиб, бу кўрсаткич 2022 йилга (7312 та) таққослаганда 11,6 фоизга ошган[1]. Таҳлилларга кўра охирги йилларда гиёҳвандлик воситаларини ўтказиш (ЖКнинг 173-моддаси) билан боғлиқ жиноятлар сонининг ошиб бориши кузатилмоқда. 2023 йилда содир этилган бу турдаги жиноятларнинг 28 фоизи (3012 та) гиёҳвандлик воситаларини қонунга хилоф равишда ўтказиш билан боғлиқ ҳолда содир этилган.

Гиёҳвандлик воситаларини қонунга хилоф равишда ўтказиш билан боғлиқ жиноятларни аниқлаш ва фош этишнинг мураккаблиги шундаки, улар ноаниқлик шароитида, ҳар икки томоннинг розилиги билан содир этилади. Бунда жабрланувчи томоннинг мавжуд эмаслиги, мазкур жиноятнинг латент қилмишлар қаторига киришини билдиради. Шу боис, ушбу жиноятларни аниқлаш ва очишнинг самарали усуллари сифатида назорат остида олиш ва бошқа тезкор-қидирув тадбирларини (кейинги ўринларда – ТҚТ деб юритилади) ўтказишни келтириш мумкин.

Гиёҳвандлик воситаларини ноқонуний ўтказишни фош этиш мақсадида назорат остида олиш ТҚТнинг ўтказишни ташкил этиш ва тактикаси ҳамда унинг натижадорлиги бир қатор омилларга боғлиқ бўлиб, улар орасида гиёҳвандлик воситаларини жиноятчилар томонидан контактсиз усулда ўтказиш амалиёти кенг тарқалган. Ушбу усулдан фойдаланган ҳолда гиёҳвандлик воситаларининг, айниқса синтетик гиёҳвандлик воситаларини ноқонуний ўтказишда кейинги пайтларда жиноятчилар Интернет ва ахборот-телекоммуникация воситаларидан фойдаланиш амалиёти ошиб бормоқда.

Бугунги кунда вояга етмаганларни жалб қилган ҳолда ҳамда телекоммуникация тармоқларидан ва Интернет жаҳон ахборот тармоғидан фойдаланиш орқали гиёҳвандлик воситаларининг, улар

[1] Ўзбекистон Республикаси ИИВнинг Ҳуқуқий статистика ва тезкор-ҳисоб маълумотлар маркази маълумотлари.

аналогларининг ва психотроп моддаларнинг қонунга хилоф муомаласи ортиб бораётганлиги муносабати билан ушбу ҳуқуқбузарликлар учун жавобгарлик чораларини кучайтириш мақсадида Ўзбекистон Республикаси Жиноят кодексининг 273-моддаси учинчи қисми “телекоммуникация тармоқларидан, шунингдек Интернет жаҳон ахборот тармоғидан фойдаланиб содир этилган бўлса” деган мазмундаги “д” банди билан тўлдирилди[2]. Ушбу Қонун билан гиёҳвандлик воситаларини, уларнинг аналогларини ёки психотроп моддаларни телекоммуникация тармоқларидан ва Интернет жаҳон ахборот тармоғидан фойдаланиш орқали қонунга хилоф равишда муомалага киритганлик учун жавобгарлик чоралари кучайтирилди.

Гиёҳвандлик воситаларини ноқонуний ўтказиш билан боғлиқ фаолият ташкилотчилари интернетдан фойдаланиб, бугунги кунда нафақат гиёҳванд воситалар сотувчиси ва уларни истеъмол қилувчилари ўртасидаги бевосита алоқадан, балки уюшган гуруҳнинг барча иштирокчиларининг ўзаро учрашувларидан ҳам қочишади. Бу омил, бир томондан, харидорга дори воситаларини харид қилиш тартибини имкон қадар соддалаштиришга, иккинчи томондан, гиёҳванд воситалар сотувчисининг хавфсизлик даражасини оширишга имкон беради. Яъни, бундай воситаларни тарқатишнинг бу усули контактсиз (алоқасиз) деб аталади.

Таъкидлаш жоизки, кейинги йилларда гиёҳвандлик воситаларини телекоммуникация тармоқларидан, шунингдек Интернет жаҳон ахборот тармоғидан фойдаланиб ноқонуний ўтказиш хавфи кучайганлигини ҳам қайд етиш лозим бўлиб, бу усулни қўллаш орқали чексиз кенг доирадаги одамларга, шу жумладан, вояга етмаганларга салбий таъсир кўрсатиш имконияти янада ортади.

Гиёҳвандлик воситаларини “назорат остида олиш” ТҚТни ўтказиш орқали сотишнинг контактсиз усулини ҳужжатлаштиришда, ушбу тадбирни ўтказишнинг умумий қоидаларига риоя қилинади. Уни амалга оширишнинг ўзига хослиги шундаки, сотиб олинган гиёҳвандлик воситалари учун тўловни амалга оширишда нақд пулсиз тўлов тизими қўлланилади, харидор ва сотувчи ўртасида тўғридан-тўғри алоқа мавжуд бўлмайди.

[2] Ўзбекистон Республикасининг 2024 йил 5 октябрдаги “Ўзбекистон Республикасининг Жиноят, Жиноят-процессуал кодексларига ҳамда Ўзбекистон Республикасининг маъмурий жавобгарлик тўғрисидаги кодексига гиёҳвандлик воситаларининг, улар аналогларининг ёки психотроп моддаларнинг, шунингдек кучли таъсир қилувчи ва заҳарли моддаларнинг қонунга хилоф муомаласига қарши курашишга қаратилган ўзгартириш ва қўшимчалар киритиш ҳақида”ги ЎРҚ-971-сон Қонуни 1-моддаси.

Гиёҳвандлик воситаларини контактсиз сотиш усулини ҳужжатлаштириш учун “назорат остида олиш” ТҚТни ўтказишнинг дастлабки босқичида фақат дори мавжудлиги ва уни сотиш фактини тасдиқлаш мумкин, аммо уни ўтказишни ташкил этишда иштирок этган шахслар доирасини аниқлашнинг имкони бўлмайди. Шу сабабли, ушбу босқичда гиёҳванд воситаларни сотиш билан шуғулланадиган шахсларни, улар ишлатадиган телекоммуникация қурилмаларини, уюшган гуруҳ аъзоларининг жойлашган манзилларини аниқлашга қаратилган комплекс ТҚТни амалга ошириш зарур.

Ҳозирги кунда, гиёҳвандлик воситаларини контактсиз усулда сотаётган шахсларни аниқлаш мақсадида Ўзбекистон Республикаси ИИВ Жиноят қидирув департаменти таркибида кибержиноятчиликка қарши курашиш маркази фаолият олиб бораётган бўлиб, Марказ ходимлари томонидан бу каби жиноятларни аниқлаш мақсадида Интернет орқали мониторинг ишлари олиб борилмоқда. Турли хил қидирув дастурларига (масалан, Yandex, Rambler, Google ва бошқалар) сўровлар юбориш орқали Интернетда гиёҳванд воситаларни таклиф қилувчи шахсларнинг сайтлари ва алоқа маълумотлари (код номлари, мобил телефон рақамлари) аниқланади. Шундан сўнг, гиёҳванд воситалар савдоси билан шуғулланувчи шахсларнинг идентификация маълумотларини, улар фойдаланадиган техник воситаларни, шу жумладан гиёҳванд воситаларни сотиш ва сотиб олиш учун яратилган веб-сайтларларни аниқлашга қаратилган кейинги ТҚТни ўтказиш учун тармоқ ресурсида кўрсатилган шахс билан алоқа ўрнатилади. Жиноий ҳаракатларни ҳужжатлаштириш мақсадида дори воситаларини харид қилиш учун маблағлар киритилиши лозим бўлган электрон ҳисоб (электрон ҳамён) ҳақидаги маълумотларни олиш ва уларни ўрганиш чоралари кўрилади.

Амалиёт тажрибасидан маълумки, жиноятчилар кўпинча рўйхатдан ўтиш учун фақат мобиль телефон рақамини кўрсатиш орқали амалга ошириладиган банкдаги ҳисоб рақами (ҳамён)дан фойдаланадилар. Шу билан бирга, уяли алоқа операторларининг виждонсиз вакиллари томонидан СИМ-карталарни тегишли рўйхатдан ўтказмасдан сотиш ҳолатларини ҳисобга олиш керак. Электрон ҳамённи виртуал рўйхатдан ўтказмасдан, гиёҳванд воситалар савдоси билан шуғулланувчи шахслар, ўз шахси ҳақидаги маълумотларни яширишга, шунингдек, кўрсатилган ҳисоб рақамларига пул маблағларини аноним тарзда ўтказишга муваффақ бўлишади. Бу ҳолат гиёҳванд воситалар савдосига алоқадор

шахсларни аниқлаш ва жавобгарликка тортиш жараёнини анча мураккаблаштиради. Пул ўтказмалари ҳақидаги маълумотларни ўрганиш ва кейинчалик уларнинг эгасини аниқлаш учун банкга сўров юборишдан иборат бўлган “маълумотлар тўплаш” ТҚТни ўтказиш керак бўлади[3]. Банкдан олинган маълумотларнинг батафсил таҳлилини ўтказгандан сўнг, қуйидаги тадбирларни режалаштириш ва амалга ошириш лозим:

- жиноятчилар томонидан қўлланиладиган телефон рақамлари аниқланганидан сўнг, улар ёрдамида қуйидаги ТҚТ, жумладан, телефонлар ва бошқа телекоммуникация қурилмалари орқали олиб бориладиган сўзлашувларни эшитиб туриш, улар орқали узатиладиган ахборотни олиш; абонентлар ёки абонент қурилмалари ўртасидаги боғланишлар тўғрисида ахборот олиш, IMEI-телефонларни аниқлаш, уларни активлаштириш; гиёҳвандлик воситалари учун маблағлар ўтказиладиган банк карталари рақамларини аниқлаш тадбирлари ўтказилади. Ушбу босқичда гиёҳвандлик воситаларини сотиш билан шуғулланган шахсларни аниқлаш ва уларнинг фаолиятига раҳбарлик қилаётган тезкор ходим, жиноий фаолиятини ҳужжатлаштириш самарадорлигини ошириш учун ТҚТни режалаштириш ва ўтказиш бўйича ваколатли давлат органи бўлинмалари билан яқин ҳамкорликни йўлга қўйиши зарур.

- кейинги босқичда гиёҳванд воситалар савдоси билан шуғулланувчи шахсларнинг жиноий фаолиятини ҳужжатлаштириш жараёнида банк карточкалари, ҳисоб рақамлари, уларнинг эгалари аниқланиб, гиёҳвандлик воситалари учун тўлов сифатида олинган маблағлар ҳаракати назорат қилинади;

- ҳужжатлаштиришнинг кейинги йўналиши жиноий гуруҳнинг сони, тузилиши ва аниқланган иштирокчилар тўғрисида илгари олинган маълумотларни таҳлил қилишдир. Жиноий фаолиятга алоқадор шахслар аниқлангандан ва ҳужжатлаштирилгандан сўнг, “назорат остида олиш” ТҚТни ўтказиш режалаштирилади.

Гиёҳвандлик воситаларини контактсиз ўтказиш ҳолатини аниқлашга қаратилган “назорат остида олиш” ТҚТни ўтказишда қуйидаги бир қатор талабларга риоя этилиши зарур:

– телекоммуникация тармоқларида (веб-сайт, форумларда) гиёҳвандлик воситасининг номи ва нархи кўрсатилганлигига оид аниқ таклифлар аниқланганидан сўнг, “назорат остида олиш” ТҚТни

[3] Қаранг: Каримов В. Ўзбекистон Республикасининг “Тезкор-қидирув фаолияти тўғрисида”ги қонунига илмий-амалий шарҳ: Масъул муҳаррирлар Э.Т. Юлдашев, Е.В. Коленко. – Тошкент, 2021. – Б. 120-122.

ўтказиш жараёнида зудлик билан харидорнинг (тезкор ходимнинг) ҳаракатларини ҳужжатлаштириш, яъни. таклиф этилаётган гиёҳвандлик воситасини сотиб олишга харидорнинг розилиги ҳақида сотувчига юборилган хабар электрон ташувчида скриншот ёрдамида ёзиб олиш чоралари кўрилади.

– сотувчидан ижобий жавоб олинганидан сўнг, тўлов терминали орқали пул маблағларини ўтказиш факти қайд этилади ва ушбу терминал жойлашган жой кўрсатилган ҳолда пул маблағларини киритиш тўғрисидаги квитанция олинади ва илова қилинади;

– сотувчидан маълум жойда гиёҳвандлик воситасининг яшириб қўйилганлиги тўғрисида хабар олингандан сўнг, унинг аниқ манзили (сақлаш жойи) “назорат остида олиш” ТҚТ далолатномасида батафсил қайд этилади;

– тадбир давомида харидор ва сотувчи ўртасидаги барча ёзишмалар электрон алоқа воситасида (компьютер, смартфон, ноутбук) сақланиши керак;

- харидор ва сотувчи ўртасида алоқа ўрнатилган компьютернинг хавфсизлиги таъминланади (жиноят ишини тергов қилиш доирасида исботлаш жараёнида фойдаланиш учун).

Кейинчалик, “назорат остида олиш” ТҚТни муваффақиятли ўтказиш учун ваколатли давлат органи, тезкор-қидирув бўлинмалари кучлари ва воситаларидан комплекс фойдаланиш ва ўтказилган гиёҳвандлик воситалари учун тўлов сифатида олинган молиявий маблағлар ҳаракатини кузатиш билан бир вақтда амалга ошириш зарур. Кузатув жараёнида гиёҳвандлик воситаларини ўтказишни ҳужжатлаштириш билан боғлиқ барча ҳаракатлар хронологик тартибда қайд этилади. Гиёҳвандлик воситаларни сотувчиларнинг ноқонуний фаолиятини қайд қилиш учун махсус техник воситалар қўлланилади.

Ўтказилган ТҚТнинг натижалари, жиноят ишини қўзғатиш ва улардан исботлаш жараёнида далил сифатида фойдаланиш масаласи ҳал қилинади. Ушбу материаллар тезкор-қидирув фаолиятини амалга оширувчи орган раҳбарининг қарори асосида, "Тезкор-қидирув фаолияти тўғрисида" қонуни талаблари[4] ва тезкор-қидирув фаолияти натижаларини суриштирув органига, терговчига ёки прокурорга тақдим этиш тартиби тўғрисидаги Йўриқномага[5] биноан юборилади.

[4] Ўзбекистон Республикасининг «Тезкор-қидирув фаолияти тўғрисида»ги Қонуни 19-моддаси.

[5] Ўзбекистон Республикаси Бош прокуратураси, Президент давлат хавфсизлик хизмати, Давлат хавфсизлик хизмати, Ички ишлар вазирлиги, Мудофаа вазирлиги, Давлат божхона қўмитаси ва

Мазкур вазифаларни ҳал этиш мақсадида Ўзбекистон Республикасининг “Тезкор-қидирув фаолияти тўғрисида”ги Қонуни 14-моддасига ахборот технологиялари соҳасидаги жиноятчиликка қарши курашишнинг ҳуқуқий асосларини мустаҳкамлашни, ТҚТни ахборот-коммуникация технологияларини қўллаган ҳолда кибермаконда ўтказилиши белгилашни назарда тутувчи ўзгартиришларни киритилиши[6], бу соҳадаги жиноятларни аниқлаш ва фош этиш самарадорлигини оширади.

Кейинчалик терговчи ТҚТ материаллари асосида жиноят ишини қўзғатиш тўғрисида қарор қабул қилади. Амалиёт шуни кўрсатадики, контактсиз тарзда гиёҳванд воситаларни сотиш фактлари бўйича қўзғатилган жиноят ишлари бўйича тергов ҳаракатларини ўтказиш муайян ўзига хос хусусиятларга эга. Жиноий фаолиятга оид далилларни олиш учун қуйидагиларга қаратилган тергов ҳаракатларини ўтказиш зарур:

- олиб қўйиш ва тинтув тергов ҳаракатини ўтказиш чоғида ушланган шахслардан барча телекоммуникация воситаларини (мобил телефонлар, смартфонлар, планшетлар, ноутбуклар, компьютерлар, СИМ-карталар, флеш-карталар, қаттиқ дисклар ва бошқа ахборот сақлаш ташувчилари), шунингдек, Интернет хизматлари кўрсатишга доир шартномалар, пароллар, мобил телефонлар учун ПИН-кодлар, мобил алоқа ва Интернет хизматлари учун тўлов квитанцияларини олиб қўйиш чоралари кўрилади;

– олиб қўйиш ва тинтув жараёнида ушланган шахслардан банк карталари, банк ҳисобварақларини очиш тўғрисидаги ҳужжатларни аниқлаш ва олиб қўйиш;

– банк муассасаларидан банк карталари ҳисобварақлари орқали пул маблағларининг айланиши тўғрисидаги маълумотларни ўз ичига олган ҳужжатларни олиб қўйиш[7];

- ТҚТни ўтказувчи тезкор бўлинмалар ходимларидан гиёҳванд воситалар сотувчиси билан ёзишма ва алоқалар олиб борилган телефонлар, компьютерларни олиб қўйиш (амалиётда тезкор ходимлар томонидан ТҚТни ўтказиш жараёнида қўлланилган барча техник воситалари, электрон ташувчиларда қайд этилган

Электрон технологияларини ривожлантириш марказининг 2021 йил 31 августдаги қарорининг 4-боби.

[6] Ўзбекистон Республикасининг 2024 йил 13 мартдаги “Ўзбекистон Республикасининг айрим қонун ҳужжатларига жиноятчиликка қарши курашиш курашиш бўйича фаолиятнинг ҳуқуқий асосларини такомиллаштиришга қаратилган қўшимча ва ўзгартишлар киритиш тўғрисида”ги ЎРҚ-920-сон Қонуни.

[7] Қаранг: Каримов В. Ўзбекистон Республикасининг “Тезкор-қидирув фаолияти тўғрисида”ги Қонунига илмий-амалий шарҳ: Масъул муҳаррирлар Э.Т. Юлдашев, Е.В. Коленко. – Тошкент, 2021. – Б. 121.

ёзишмаларнинг скриншотлари қонунда белгиланган тартибда терговчига исботлаш жараёнида фойдаланиш учун топширилади);

– гиёҳвандлик воситаларининг қадоқланган ўрамларда (“яширин жойда”) топилган намуналарини, кейинчалик ушланган шахсларнинг биологик намуналари билан таққослаш учун олиб қўйиш;

– ушланган шахслар фойдаланаётган абонент рақамларининг кирувчи ва чиқувчи боғланишлари тўғрисидаги маълумотларни мобил операторлардан олиш ва ўрганиш.

Гиёҳвандлик воситалари, психотроп моддалар ёки уларнинг аналогларини қонунга хилоф равишда юқорида кўрсатилган воситалар ва тармоқлардан фойдаланган ҳолда ўтказишда айбдор деб топиш учун шахс ушбу жиноятнинг объектив томонини ташкил этувчи воситалар ва тармоқлардан фойдаланиш билан боғлиқ хатти-ҳаракатларни содир этганлигини аниқлаш зарур. Гиёҳвандлик воситаларини ўтказиш билан боғлиқ сўзлашувларда телефон алоқасидан фойдаланишнинг ўзи малакавий белги сифатида тан олинмайди.

Яхши режалаштирилган ва олдиндан тайёргарлик кўрилган “назорат остида олиш” ТҚТ натижалари гиёҳвандлик воситаларини қонунга хилоф равишда ўтказиш бўйича жиноят иши қўзғатилиши учун асос бўлиши мумкин. Ҳозирги кунда “назорат остида олиш” ТҚТни гиёҳвандлик воситаларини ўтказиш учун шахснинг гиёҳвандлик воситаларни сотишга алоқадорлигидан дарак берувчи аниқ ва объектив маълумотлар олинганидан кейин тезкор ишлов жараёнида амалга оширилиши мақсадга мувофиқ.

Юқоридаги таҳлиллардан келиб чиқиб қуйидаги хулосалар чиқаришимиз мумкин: шахсда гиёҳвандлик воситаларни ноқонуний ўтказишга тайёргарлик кўрилаётганлиги ва қасднинг мавжудлигидан дарак берувчи аниқ маълумотлар бўлмаган ҳолларда тезкор маълумотларни текшириш мақсадида “назорат остида олиш” ТҚТни ўтказишни тақиқлаш тўғрисида ТҚТни ташкил этиш ва тактикасини тартибга солувчи идоравий-меъёрий ҳужжатларга ўзгартиришлар киритиш, зарур деб ҳисоблаймиз.

Мобил операторларнинг СИМ-карталарни амалдаги қонунчиликка риоя этилмаган ҳолда тегишли рўйхатдан ўтказмасдан сотганликлари учун мобил операторларнинг жавобгарлигини кучайтириш зарурдир. Эслатиб ўтамиз, Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2020 йил 31 декабрдаги қарори билан мамлакатда мобил қурилмаларни ИМЕИ-кодларини

рўйхатга олиш тизими жорий этилди. Тизим оператори сифатида “Ўзбекистон телекоммуникациялари тармоқларини бошқариш республика маркази” белгиланди[8]. Бундан кўзланган мақсад, мобил қурилмаларни ИМЕИ-кодларини рўйхатга олиш тизимини жорий этиш орқали электрон ҳамёнлардан фойдаланиш ва электрон пул маблағларини аноним ўтказиш учун уяли алоқа тармоғи абонентларини аноним рўйхатга олишни бекор қилиш ҳисобланади. Шунингдек, фойдаланувчининг шахсий маълумотларини тасдиқламасдан, абонент рақамларини ижарага бериш хизматларини таклиф қилувчи сайтларни блокировка қилиш масаласига ҳам эътибор қаратиш лозим деб ҳисоблаймиз.

Электрон пул маблағларини ўтказиш фақат молиявий ташкилот томонидан, уяли алоқа операторидан маълумотларни сўраш орқали, пул жўнатувчи шахс олдиндан аниқлангандан кейин амалга оширилиши керак. Ушбу ҳаракатлар банкда ҳам, алоқа операторида ҳам мавжуд бўлган жисмоний шахс ҳақидаги маълумотларни (тўлиқ исм, паспорт серияси ва рақами, телефон рақами) тасдиқлаш имконини беради. Бундай ўзаро алоқа учун абонент маълумотларини текшириш учун ахборот тизимини яратиш керак бўлади.

Шу муносабат билан, таъкидлаш жоизки, бугунги кунда юқоридаги каби ахборот технологияларидан фойдаланиб содир этиладиган жиноятларга қарши курашиш самарадорлигини ошириш мақсадида бундай қилмишларни фош этишда қўлланиладиган махсус техник воситаларни амалиётга кенг жорий этиш зарурияти мавжуд. Шу боис, бу борада ўтказиладиган тезкор-қидирув тадбирларида қўлланиладиган техник воситаларни республика ҳудудига олиб киришда телекоммуникациялар операторларига солиқ ва божхона имтиёзлари бериш, яъни уларни солиқ солишдан ва божхона божини тўлашдан озод қилиш бўйича амалдаги солиқ ва божхона қонунчилигига тегишли ўзгартишлар киритишга оид чора-тадбирлар белгилаш мақсадга мувофиқ деб ҳисоблаймиз. Қонунчиликка таклиф этилаётган бундай имтиёзлар, шубҳасиз, тезкор-қидирув тадбирларида қўлланиладиган техник воситаларни республика ҳудудига олиб киришшда фойдаланиш тартибини ҳамда тезкор-қидирув тадбирлари самарадорлигини оширишга ҳизмат қилади.

[8] Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2020 йил 31 декабрдаги “Ўзбекистон Республикасида мобил қурилмаларни ҳисобга олиш тизимини тартибга солиш чора-тадбирлари тўғрисида”ги № 828-сон қарори.

Ушбу чора-тадбирлар гиёҳвандлик воситаларининг муомалага киритилиши билан боғлиқ бўлган молиявий активларнинг контактсиз амалга оширилган ҳаракати устидан самарали назоратни амалга ошириш, гиёҳвандлик воситаларни сотиб олувчилардан воситачиларга пул ўтказмаларини кузатиш, жиноий гуруҳлар аъзолари томонидан пул маблағларини вақтинча сақлаш учун фойдаланиладиган банк ҳисобварақлари реквизитларини белгилаш, гиёҳвандлик бизнесидан олинган маблағларнинг ўтишнинг бутун занжирини аниқлаш имконини беради.

ОБЛАЧНЫЕ ДАННЫЕ: ОСНОВЫ ИССЛЕДОВАНИЯ

Кахрамонов Азизбек Собирович
Преподаватель кафедры Криминалистики и судебных экспертиз Правоохранительной академии Республики Узбекистан
E-mail: azekmr@gmail.com

Аннотация. *В статье раскрыты основные стадии производства исследования облачных данных и включает в себя краткую обзорную информацию о ключевых аспектах данной области, включая рекомендации и требования при производстве экспертизы облачных данных.*

Ключевые слова: *Облачные технологии, облачное хранилище, экспертиза, компьютерно-техническая экспертиза, метаданные, цифровые доказательства.*

Annotatsiya: *maqolada bulutli ma'lumotlar tadqiqoti o'tkazishning asosiy bosqichlari yoritib berilgan va ushbu sohaning asosiy jihatlari, shu jumladan bulut ma'lumotlari ekspertizasi bo'yicha ekspertga qo'yiladigan tavsiyalar va talablar haqida qisqacha ma'lumot berilgan.*

Kalit so'zlar: *bulutli texnologiyalar, bulutda saqlamoq, ekspertiza, kompyuter-texnik ekspertiza, metama'lumotlar, raqamli dalillar.*

Abstract: *the article reveals the main stages of cloud data forensics production and includes a brief overview of the key aspects of the field, including recommendations and requirements for the cloud data forensics examiner.*

Keywords: *cloud technology, cloud storage, forensics, computer forensics, metadata, digital evidence.*

Облачные технологии стали неотъемлемой частью современного бизнеса и повседневной жизни. Компании и частные лица все больше переносят свои данные и приложения в облако для повышения доступности, масштабируемости и удобства использования [1].

Однако, с этим ростом популярности облачных решений, возникают новые вызовы в области безопасности и производства экспертизы цифровых устройств.

Экспертиза облачных данных — это процесс анализа и исследования информации, которая хранится в облачных хранилищах, с целью выявления и документирования цифровых доказательств, имеющие значения для расследования и раскрытия преступления. Облачные данные могут быть критически важными в расследованиях различных преступлений, включая компьютерные атаки, киберпреступления, финансовые махинации и другие.

Процесс экспертизы облачных данных включает в себя следующие этапы исследования:

Определение целей и необходимых данных: сначала необходимо определить цели экспертизы и какие конкретные данные потребуются. Это может включать в себя поиск файлов в виде текстовых сообщений, фото видео аудио файлов, электронной почты и других типов информации.

Сбор облачных данных: под сбором облачных данных понимается процесс сбора информации и цифровых данных, хранящихся в облачных системах хранения информации. Эксперты сначала должны определить, какие облачные службы использовались, чтобы хранить информацию. Это может быть Google Drive, Dropbox, Microsoft OneDrive и другие. Затем идёт процесс получения и извлечения данных с доступом к соответствующим учетным записям. Это может включать в себя загрузку файлов, доступ к базам данных или извлечение конкретной информации при необходимости.

Контакт с облачными провайдерами: Эксперты, при необходимости, могут связаться с провайдерами облачных услуг и запросить доступ к данным. Провайдеры могут предоставить копии данных или доступ к учетной записи.

Анализ метаданных: это изучение и интерпретация метаданных, связанных с цифровыми файлами, документами или информацией. Метаданные, по сути, являются информацией о цифровых данных и позволяют получить ценные сведения о различных аспектах описываемого ими содержимого. Метаданные могут включать в себя такие сведения, как дата создания, авторство, тип файла, история версий и т.д. Метаданные, такие как даты и времена доступа, заголовки электронных сообщений, IP-адреса и др., могут предоставить важные сведения о том, как и когда данные были использованы или изменены.

Извлечение и анализ контента: Эксперты могут извлекать и анализировать содержимое облачных файлов, текстовых сообщений, электронной почты и других видов информации, чтобы найти доказательства или свидетельства преступлений.

Восстановление удаленных данных: это процесс восстановления информации или файлов, которые были ранее удалены с устройства хранения данных или системы. Если какие-либо данные были удалены или скрыты, эксперты с применением специальных технических средств могут попытаться восстановить их, чтобы выявить данные, имеющие значения для следствия или суда.

Аутентификация и целостность данных: Аутентификация и целостность - два фундаментальных аспекта обеспечения безопасности и надежности цифровых данных. Они играют решающую роль в защите данных от несанкционированного доступа и фальсификации.

Под целостностью понимается уверенность в том, что цифровые данные не были изменены или подделаны несанкционированным образом в процессе хранения, передачи или обработки. Обеспечение целостности данных необходимо для поддержания достоверности и точности данных. Одним из методом обеспечения целостности данных является Хеш-функция. Хеш-функции генерируют из данных строки символов фиксированной длины (хэши). Даже небольшое изменение в данных приведет к значительному изменению хэша [2].

Подготовка экспертных заключений: Подготовка экспертного заключения — это тщательный и зачастую трудоёмкий процесс. Он требует четкого и систематического подхода, а также объективности, точности и профессионализма. Экспертные заключения являются важнейшим инструментом, помогающим судам и следственным органам, разобраться в сложных технических или узкоспециальных вопросах [3].

Эксперты по экспертизе облачных данных играют важную роль в исследовании и анализе цифровых доказательств в различных сферах, включая правоохранительную деятельность, кибербезопасность и корпоративное расследование. Для успешного проведения исследования в области облачных данных, необходимо соответствовать определенным требованиям и обладать определенными навыками и квалификацией: Образование (наличие степени бакалавра в областях, таких как информатика, вычислительная техника, кибербезопасность, цифровая

криминалистика или информационные технологии). Наличие сертификата, подтверждающее компетентность к производству данного вида экспертизы. Техническая квалификация – умение пользоваться инструментами и программным обеспечением цифровой криминалистики. А также имеет важное значение наличие аналитических навыков, навыки решения проблем, этическое и профессиональное поведение и опыт в данной сфере [4].

Выполнение этих требований и постоянное совершенствование своих навыков и знаний является необходимым условием для того, чтобы стать квалифицированным экспертом в области цифровой криминалистики. Кроме того, эксперты должны обеспечивать соблюдение всех законодательных требований и правил при сборе, анализе и исследовании данных. В настоящее время эта область становится все более важной, поскольку облачные хранилища становятся широко используемыми и все больше информации переходит в облачные хранилища.

ЖИНОЯТ ПРОЦЕССИДА РЕАБИЛИТАЦИЯ ЭТИШ СОҲАСИДА ПРОЦЕССУАЛ ВА ПРОКУРОР НАЗОРАТИ (қиёсий таҳлил)

Шодиев Ғулом Махаммatович
Ҳуқуқни муҳофаза қилиш академияси
марказ катта прокурори ю.ф.н., доцент

ЖПКга кўра ҳозирги вақтда жиноят ишини судга қадар юритиш жараёнида, шу жумладан шахсни реабилитация этиш асосларига кўра жиноят ишини тугатиш устидан назорат бўйича яхлит тизим йўқлигини таъкидлаш ўринли.

Ҳозирги кунда жиноят ишини судга қадар иш юритишни амалга оширувчи органлар фаолияти, уларнинг қонунларга риоя этилиши устидан назоратни амалга оширувчи прокурор назорати ва процессуал назоратнинг мазмуни ўртасидаги боғлиқлик ва фарқли жиҳатлар тўғрисида саволлар туғилиши табиий.

Профессор Г.Абдумажидовнинг таъкидлашича дастлабки терговни олиб борувчи органлар фаолиятини такомиллаштириш масалалари доирасида, жиноят иши бўйича процессуал раҳбарлик тўғрисида фикр юритган[1], доцент, А.Х.Раҳмонқулов, “Дастлабки терговда тергов бўлинмаларининг раҳбарлари маъмурий-ташкилий

[1] Абдумажидов Г. Расследование преступлений (Процессуально-правовое исследование). – Т., 1986. – С.77.

функциялардан ташқари, амалда процессуал функцияларни ҳам бажарадилар, чунки хизмат бўйича унга бўйсунувчи терговчиларнинг иши процессуал фаолиятдан иборатдир... Тергов бўлинмаси бошлиғининг зиммасига терговчиларнинг жиноят ишларини тергов қилиш фаолиятидаги ҳолатларни тўла ва холисона текширишнинг тўлалиги ва ҳар томонламалигини таъминлаш бўйича қонунда белгиланган чораларни кўриш, яъни процессуал раҳбарлик қилиш вазифаси юкланади. Бу эса идоравий-процессуал контролда намоён бўлади[2]", профессор, Д.М.Миразов "ЖПКда белгиланган ваколатлар доирасида идоравий процессуал контроль, прокурор назорати, суд контроли ва жамоатчилик контроли шаклида суриштирувчи, терговчи, прокурор ва суд томонидан процессуал ҳаракатларни амалга ошириш ва тегишли қарорларни қабул қилиш, суриштирув, дастлабки терговни амалга ошириш, судда кўриб чиқиш ва ҳал этишда жиноят-процессуал қонунчиликда белгиланган тартиб-таомилларга риоя этилишини ташкиллаштириш, кузатиш, текшириш, назорат қилиш, зарур ҳолларда таъсир ўтказиш, бекор қилиш, чора кўришдан иборат усулларнинг мажмуидир. Процессуал контролнинг субъектлари бўлиб суриштирув органи бошлиғи, тергов тузилмасининг раҳбари, прокурор ва суд ҳисобланади"[3] деб такидлайдилар.

Юқоридаги олимларнинг билдирган фикрларидан келиб чиқиб судгача бўлган жараёнда жиноят ишини юритишга ваколатли бўлган органлар ва мансабдор шахсларнинг фаолияти устидан олиб бориладиган назорат кўринишларини таҳлил қилсак, амалдаги ЖПКда белгиланганидек судгача жиноят ишларини юритиш суриштирув ва дастлабки тергов шаклида амалга оширилади, ЖПКнинг 35-моддасига кўра жиноят иши бўйича дастлабки терговни прокуратура, ички ишлар органларининг ва давлат хавфсизлик хизматининг терговчилари олиб борадилар.

Шунингдек, ЖПК 38-моддасига кўра:

Жиноят ишлари бўйича суриштирув:

1) ички ишлар органларининг;

2) Ўзбекистон Республикаси Бош прокуратураси ҳузуридаги Иқтисодий жиноятларга қарши курашиш департаментининг ва унинг жойлардаги бўлинмаларининг;

---

[2] Раҳмонқулов А.Х. Миразов Д.М. Дастлабки тергов. Дарслик. – Т., 2013. –Б.21-25.

[3] Д.М.Миразов, "Дастлабки тергов идоралари устидан контроль ва назоратни такомиллаштиришнинг назарий ташкилий ва процессуал жиҳатлари" ю.ф.д илмий даражасини олиш учун ёзилган Диссертация. 2015 йил, 46 бет.

3) Ўзбекистон Республикаси Бош прокуратураси ҳузуридаги Мажбурий ижро бюросининг ва унинг жойлардаги бўлинмаларининг;

4) Ўзбекистон Республикаси Давлат божхона қўмитасининг ва унинг жойлардаги бўлинмаларининг;

5) Ўзбекистон Республикаси Миллий гвардиясининг ва унинг жойлардаги бўлинмаларининг суриштирувчилари томонидан амалга оширилади.

Бироқ, жиноят процессида шахсни реабилитация этиш соҳасида назоратни амалга оширувчи прокурор, тергов ва суриштирув органларининг раҳбарлари ўртасидаги ваколатларнинг қайта тақсимланишини кўрсатадиган Ўзбекистон Республикаси Жиноят-процессуал кодексида мавжуд бўлган нормалар билан боғлиқ, уларни амалга ошириш муаммоларини ўрганиш долзарб ҳисобланади.

ЖПКнинг 33-моддасига кўра Ўзбекистон Республикаси Бош прокурори ва унга бўйсунувчи прокурорлар суриштирув ва дастлабки тергов босқичларида Ўзбекистон Республикаси қонунларининг аниқ ва бир хилда ижро этилиши устидан назоратни амалга оширади.

Ўзбекистон Республикаси Жиноят-процессуал кодексининг 33-моддаси 2-қисмида прокурор суриштирув ва дастлабки тергов босқичларида қонуннинг бузилишини, ким томонидан содир этилганлигидан қатъи назар, бартараф этиш учун қонунда назарда тутилган чора-тадбирларни ўз вақтида кўриши шарт деб белгиланган, юқоридаги нормага асосан прокурорга дастлабки тергов ва суриштирув ўтказилишига сезиларли таъсир кўрсатишга имкон беради. Суриштирувчи, суриштирув органи раҳбари ёки терговчи, тергов органи раҳбари томонидан йўл қўйилган қонун бузилишларини бартараф этиш воситаси сифатида уларнинг ноқонуний ёки асоссиз қарорларини бекор қилиш ваколати берилган, шунингдек кодекснинг 382-моддасида белгиланган тартибда қонунда назарда тутилган ҳолларда терговчи ёки суриштирувчининг ишни тугатишига розилик беради.

Бош прокурорнинг 2016 йил 22 февралдаги “Жиноятчиликка қарши кураш, суриштирув, дастлабки тергов ва тезкор-қидирув фаолиятида қонун устуворлигини ҳамда шахснинг ҳуқуқ ва эркинликлари ҳимоясини самарали таъминлаш тўғрисида”ги 129-сонли буйруғига биноан, Ўзбекистон Республикаси прокуратура органларининг жиноятчиликка қарши кураш борасидаги асосий

вазифалари – терговга қадар текширув, суриштирув, дастлабки тергов ва тезкор-қидирувни амалга оширувчи органларнинг бу борадаги фаолиятини назорат қилиш ва мувофиқлаштириш, терговга қадар текширув ва дастлабки терговни олиб бориш орқали қонун устуворлигини таъминлаш, қонунийликни мустаҳкамлаш, фуқароларнинг ҳуқуқ ҳамда эркинликларини, жамият ва давлатнинг қонун билан қўриқланадиган манфаатларини, Ўзбекистон Республикаси конституциявий тузумини ҳимоялаш, ҳуқуқбузарликларнинг олдини олиш ва профилактика қилишдан иборат эканлиги таъкидланган.

Шу билан бирга, ЖПКнинг 37-моддага кўра эса, тергов бошқармаси, бўлими, бўлинмаси, гуруҳининг бошлиғи ва унинг ўринбосари ўз ваколатлари доирасида жиноятларни очиш ва уларнинг олдини олиш юзасидан терговчиларнинг ўз вақтида ҳаракат қилишини назорат этадилар, жиноят ишлари бўйича дастлабки терговни тўла, ҳар томонлама ва холисона олиб бориш чораларини кўрадилар.

Тергов бошқармаси, бўлими, бўлинмаси, гуруҳининг бошлиғи ва унинг ўринбосари ишларни текшириб кўришга, шунингдек дастлабки тергов ўтказиш, шахсни ишда айбланувчи тариқасида иштирок қилиш учун жалб этиш, жиноятни тавсиф қилиш ва айбловнинг ҳажми, ишнинг йўналишини белгилаш, айрим тергов ҳаракатларини ўтказиш ҳақида терговчига кўрсатмалар беришга, ишни бир терговчидан иккинчи терговчига олиб беришга, ишни тергов қилишни бир неча терговчига топширишга ҳақлидир. ЖПК 39-моддасига кўра суриштирув бўлинмасининг бошлиғи ва унинг ўринбосари ўз ваколатлари доирасида жиноятларни очиш ва уларнинг олдини олиш юзасидан суриштирувчиларнинг ўз вақтида ҳаракат қилишини назорат этадилар, жиноят ишлари бўйича суриштирувни тўла, ҳар томонлама ва холисона олиб бориш чораларини кўрадилар.

Шунингдек, ишларни текшириб кўришга, суриштирувчига суриштирув юритиш, шахсни ишда гумон қилинувчи, айбланувчи тариқасида иштирок қилиш учун жалб этиш, жиноятни тавсиф қилиш ва айбловнинг ҳажми, ишнинг йўналишини белгилаш, айрим тергов ҳаракатларини ўтказиш ҳақида кўрсатмалар беришга, ишни бир суриштирувчидан иккинчи суриштирувчига олиб беришга, ишни тергов қилишни бир неча суриштирувчига топширишга ҳақлидир.

Суриштирув ва дастлабки тергов органларининг раҳбарлари суриштирувчи ҳамда терговчининг жиноят ишини реабилитация

этиш асослари бўйича тугатиш тўғрисидаги қарорларини бекор қилиш ваколатига эга эмас. Бинобарин, ЖПКда судгача жиноят ишини юритишга ваколатли органларнинг бевосита раҳбарлари томонидан шахсни реабилитация этиш асослари бўйича жиноят ишини тугатиш тўғрисидаги қарорларни қабул қилиш ёки бекор қилиш нуқтаи назаридан жиноят процессида реабилитация соҳасида қонун устуворлигига риоя қилишнинг процессуал назоратини тартибга солувчи аниқ нормалар кўзда тутилмаган.

Ушбу тадқиқот доирасидан ташқарида бўлган идоравий манфаатларга таъсир қилмасдан, биз судгача жиноят ишини юритиш ваколатига эга бўлган суриштирув ва дастлабки тергов органларининг процессуал фаолиятига раҳбарлик қилувчи бўлим, бошқармаларининг бошлиқлари, уларнинг ўринбосарларининг ваколатларига жиноят ишини реабилитация асослари бўйича тугатиш тўғрисидаги қарор юзасидан процессуал назоратни реабилитация ҳуқуқи эътироф этилган шахсларнинг ҳуқуқлари, эркинликлари ва қонуний манфаатларини қисқа муддатларда таъминлаш юзасидан киритишни мақсадга мувофиқ деб ҳисоблаймиз.

Юқоридагиларга асосан Ўзбекистон Республикаси Жиноят-процессуал кодексидаги номувофиқликларни судгача жиноят ишини юритиш ваколатига эга бўлган органлар фаолиятининг процессуал назоратини амалга оширувчи суриштирув ва дастлабки тергов органлари раҳбарларининг ваколатларини тартибга солувчи ҳуқуқий нормалар таркибига баъзи ўзгартиришлар киритиш орқали бартараф этишни таклиф этамиз.

Жиноят ишини реабилитация асосларига кўра тугатиш тўғрисида қарор қабул қилишда бундай имкониятни таъминлаш учун биз ЖПКнинг 37-моддасидаги тергов органи ҳамда 39-моддадаги суриштирув органи раҳбарларининг ваколатларини **жиноят ишини тугатишга** деган жумла билан тўлдиришни мақсадга мувофиқ деб ҳисоблаймиз.

Ушбу таклиф суриштирувчи ва терговчининг процессуал фаолиятини бевосита назорат қилувчи - суриштирув ҳамда тергов органлари раҳбарлари томонидан процессуал назоратни янада самарали таъминлашга қаратилган, чунки ЖПКнинг 382-моддасига кўра прокурор суриштирув, дастлабки тергов ишларининг боришига доир ҳужжатларни, материалларни ва бошқа маълумотларни қонун талаблари қай даражада ижро этилаётганлигини ҳар ой камида бир марта текширади.

Шуни ёдда тутиш керакки, жиноят ишини тугатиш тўғрисидаги қарорнинг нусхаси жиноят ишини судгача юритишни назорат қилувчи прокурорга юборилиши керак, прокурор ЖПКнинг 382-моддасига мувофиқ ўзига берилган ваколатлар доирасида жиноят иши юзасидан қабул қилинган қарорни бекор қилиши, қабул қилинган қарорга рози бўлиб, уни ўз кучида қолдириши, жиноят ишини тугатиш тўғрисидаги қарорни қайта тиклаб ёзма кўрсатмалар билан уни бошқа терговчи ёки суриштирувчига бериши мумкин.

Шунингдек ЖПКнинг 382-моддаси 3-қисми, 6-бандига мувофиқ прокурор амнистия актига асосан жиноят ишини қўзғатишни рад қилиш ҳақида ёки жиноят ишини тугатиш тўғрисида судга илтимоснома киритади, шу модданинг 3-қисми, 17-бандига мувофиқ қонунда назарда тутилган ҳолларда терговчи ёки суриштирувчининг ишни тугатишига розилик беради деб белгиланган.

Суриштирув ва дастлабки тергов органлари раҳбарларининг процессуал назоратини такомиллаштириш юзасидан ЖПКнинг 37 ва 39-моддаларига ўзгартириш киритиш юзасидан берилган таклифга асосан, ЖПКнинг 382-моддаси 3-қисми, 17-бандидан прокурорнинг **терговчи ёки суриштирувчининг ишни тугатишига розилик беради** деган жумлани чиқариб ташлашни таклиф этамиз.

ASSESSING ACCOUNTABILITY MECHANISMS FOR QUANTUM TECHNOLOGY IN FINANCIAL SECTORS

Islombek Abdikhakimov
Lecturer of Cyber Law Department,
Tashkent State University of law
islombekabduhakimov@gmail.com
+998 94 423 12 98

Annotatsiya: *Ushbu maqola moliya sektorida kvant texnologiyalaridan foydalanishda hisobdorlik mexanizmlarini baholashga bag'ishlangan. Tadqiqot kvant hisoblash tizimlari va moliyaviy xizmatlar o'rtasidagi o'zaro ta'sirni, shuningdek, ushbu texnologiyalarni joriy etishda xavfsizlik va javobgarlik choralarini o'rganadi. Maqolada kvant texnologiyalarini moliyaviy operatsiyalarga tatbiq etishning huquqiy va texnik jihatlari, shuningdek, ushbu sohada xalqaro hamkorlikni rivojlantirish istiqbollari muhokama qilinadi.*

Kalit so'zlar: *kvant texnologiyasi, moliya sektori, hisobdorlik, xavfsizlik, tartibga solish, xalqaro hamkorlik, innovatsion rivojlanish*

Аннотация: *Данная статья посвящена оценке механизмов подотчетности при использовании квантовых технологий в финансовом секторе. Исследование рассматривает взаимодействие между квантовыми вычислительными системами и финансовыми услугами, а также меры безопасности и ответственности при внедрении этих технологий. В статье обсуждаются правовые и технические аспекты применения квантовых технологий в финансовых операциях, а также перспективы развития международного сотрудничества в этой области.*

Ключевые слова: *квантовые технологии, финансовый сектор, подотчетность, безопасность, регулирование, международное сотрудничество, инновационное развитие*

Abstract: *This article examines accountability mechanisms for quantum technology implementation in the financial sector. The research explores the intersection between quantum computing systems and financial services, as well as security and responsibility measures in deploying these technologies. The paper discusses legal and technical aspects of applying quantum technologies to financial operations and prospects for developing international cooperation in this field. Through comprehensive analysis, the study provides insights into emerging accountability frameworks and their implications for global financial systems.*

Keywords: *quantum technology, financial sector, accountability, security, regulation, international cooperation, innovative development*

Introduction

The integration of quantum technology into financial systems represents a transformative shift in computational capabilities and risk management frameworks (Anderson & Zhang, 2023). As financial institutions increasingly adopt quantum computing solutions, the need for robust accountability mechanisms becomes paramount to ensure system integrity and stakeholder protection. The complexity of quantum systems, combined with their potential impact on financial markets, necessitates a comprehensive examination of accountability structures and their implementation (Kumar et al., 2024).

Recent developments in quantum computing have accelerated its adoption in the financial sector, with applications ranging from portfolio optimization to cryptographic security (Williams & Johnson, 2023). This rapid advancement creates both opportunities and challenges for establishing effective accountability mechanisms. The present study aims to analyze these challenges and propose comprehensive solutions for maintaining accountability in quantum-enabled financial systems.

Current State of Quantum Technology in Finance

Financial institutions are rapidly incorporating quantum computing applications across various operational domains. Recent studies indicate that 47% of major financial institutions are actively developing quantum

computing capabilities, with an additional 32% in the planning stages (Williams & Johnson, 2023). The implementation of quantum technology in finance has demonstrated remarkable potential across several key operational areas.

In the realm of portfolio optimization, quantum algorithms have demonstrated superior capabilities in processing complex market variables simultaneously to identify optimal investment strategies (Chen, 2024). These advanced computational abilities enable financial institutions to analyze market conditions and investment opportunities with unprecedented depth and accuracy. The integration of quantum computing in portfolio management requires stringent accountability measures to ensure fairness and transparency in investment decisions.

Financial institutions have also begun leveraging quantum computing for enhanced risk modeling and assessment. Thompson and Rodriguez (2023) note that quantum-based risk assessment systems can process multidimensional risk factors more effectively than classical computers, enabling more accurate risk predictions. This advancement in risk assessment capabilities has significant implications for institutional risk management strategies and regulatory compliance.

The application of quantum technology in fraud detection represents another significant advancement in financial security. Quantum machine learning algorithms have demonstrated remarkable capabilities in detecting fraudulent activities with higher accuracy and speed (Davidson et al., 2024). However, this enhanced detection capability raises important questions about data privacy and algorithmic accountability that must be addressed through comprehensive oversight mechanisms.

Accountability Challenges

The implementation of quantum technology in financial sectors presents several significant accountability challenges that require careful consideration and innovative solutions. The inherent complexity of quantum systems makes traditional audit mechanisms insufficient, necessitating the development of new protocols that account for quantum-specific vulnerabilities and operational characteristics (Chen, 2024).

Technical complexity represents a primary challenge in establishing effective accountability mechanisms. Quantum state verification requires sophisticated protocols to ensure the accuracy and reliability of quantum computations. Financial institutions must develop robust systems for managing quantum error rates in financial calculations while maintaining

oversight of the interface between quantum and classical systems. These technical challenges require specialized expertise and innovative solutions that extend beyond traditional financial system oversight.

The regulatory framework surrounding quantum technology in finance presents another significant challenge. Current regulatory structures lag behind technological advancement, creating potential oversight gaps that must be addressed (Thompson & Rodriguez, 2023). The determination of regulatory authority over quantum-enabled financial services, particularly in cross-border transactions, requires careful consideration and international cooperation. The development of appropriate technical standards and the establishment of effective cross-border coordination mechanisms represent crucial elements in addressing these regulatory challenges.

Security implications of quantum computing technology present unique challenges that require innovative accountability solutions. The potential of quantum computing to break current cryptographic systems necessitates the development of quantum-resistant security measures (Davidson et al., 2024). Financial institutions must ensure the long-term security of financial data while managing authorized access to quantum computing resources. These security considerations must be integrated into comprehensive accountability frameworks that address both current and emerging threats.

Proposed Accountability Mechanisms

To address these challenges, several comprehensive accountability mechanisms must be implemented. The development of quantum-specific audit protocols represents a fundamental requirement for effective oversight. These specialized audit methodologies must address the unique characteristics and potential vulnerabilities of quantum computing systems (Wilson, 2024). The implementation of real-time monitoring systems enables continuous oversight of quantum operations, while standardized performance metrics provide consistent measures of system effectiveness. Comprehensive documentation requirements ensure the maintenance of detailed audit trails for all quantum computations.

Multi-stakeholder oversight frameworks represent another crucial element in ensuring effective accountability. These frameworks involve collaborative oversight arrangements between financial institutions, regulatory bodies, and technology providers (Martinez & Lee, 2023). Regular assessment of quantum system operations through joint review committees ensures comprehensive oversight, while clear

communication channels facilitate effective reporting and addressing of concerns. The definition of roles and responsibilities for all stakeholders ensures clear accountability and effective coordination.

The development of international technical standards for quantum technology implementation in financial systems represents a crucial accountability mechanism. Anderson et al. (2024) emphasize the importance of establishing comprehensive standards for system interoperability, performance measurement, and security protocols. These standards provide a foundation for consistent implementation and evaluation of quantum technologies across different financial institutions and jurisdictions.

Implementation Strategies

The successful implementation of accountability mechanisms requires a structured and comprehensive approach. A gradual implementation strategy allows for system refinement and stakeholder adaptation (Brown, 2024). The initial assessment and planning phase should focus on comprehensive risk evaluation, stakeholder consultation, and appropriate resource allocation. This foundation enables effective pilot implementation, including limited-scale testing and performance monitoring. The subsequent full-scale deployment phase can then proceed with systematic rollout and continuous monitoring procedures.

International cooperation plays a crucial role in developing and enforcing accountability standards (Zhang et al., 2023). The establishment of international working groups facilitates collaborative development of consistent regulatory frameworks. Protocols for cross-border information exchange enable effective coordination and oversight of quantum technology implementation across different jurisdictions. This international cooperation ensures comprehensive coverage of accountability mechanisms across the global financial system.

Continuous evaluation and updating of accountability mechanisms ensure their ongoing effectiveness and relevance (Williams, 2024). Regular system effectiveness assessments enable identification of areas requiring improvement or modification. The integration of new technological developments ensures accountability mechanisms remain current with advancing technology. Ongoing policy refinement maintains the effectiveness of accountability frameworks in addressing emerging challenges and opportunities.

Future Implications and Recommendations

The evolution of quantum technology in finance necessitates ongoing development and refinement of accountability mechanisms.

Continued research into quantum-specific security measures and advanced audit tools remains essential for maintaining effective oversight. The enhancement of monitoring capabilities ensures comprehensive coverage of quantum technology applications in financial systems.

Policy development must maintain pace with technological advancement through regular review and updating of regulatory frameworks. International policy coordination ensures consistent application of accountability measures across jurisdictions. Ongoing stakeholder engagement in policy formation ensures comprehensive coverage of relevant concerns and requirements.

Industry collaboration plays a crucial role in advancing accountability mechanisms. Knowledge sharing among financial institutions facilitates the development of effective oversight practices. Joint development of best practices enables consistent application of accountability measures across the industry. Collaborative research initiatives advance understanding of quantum technology applications and associated accountability requirements.

Conclusion

The establishment of robust accountability mechanisms for quantum technology in financial sectors requires coordinated effort among all stakeholders. Success depends on balancing innovation with security and regulatory compliance. The proposed framework provides a foundation for developing comprehensive accountability measures that can evolve with technological advancement.

The future of quantum technology in finance holds immense promise, but its success will largely depend on the effectiveness of accountability mechanisms. Continued research, international cooperation, and stakeholder engagement will be crucial in ensuring the responsible development and implementation of quantum technologies in the financial sector. The framework presented in this study provides a foundation for ongoing development of effective accountability mechanisms in this rapidly evolving field.

SMART CONTRACTS AS THE FUTURE OF LEGAL AUTOMATION: PROSPECTS AND LIMITATIONS

Javokhir Eshonkulov
Lecturer of Cyber Law Department
Tashkent State University of law
javoxireshonqulov0724@gmail.com
+998 93 577 07 24

Abstract. *This article examines the evolving role of smart contracts in legal automation and their potential to transform traditional legal practices. Through a comprehensive analysis of existing literature and recent developments, we investigate the technical foundations, current applications, and future prospects of smart contract technology in the legal domain. The study reveals that while smart contracts offer significant advantages in terms of efficiency, transparency, and cost reduction, they also face substantial challenges related to legal recognition, technical limitations, and integration with existing legal frameworks. Our findings suggest that while smart contracts may not entirely replace traditional legal contracts, they are poised to significantly augment and automate specific aspects of legal operations, particularly in areas such as financial services, real estate, and supply chain management. The research also highlights the importance of developing appropriate regulatory frameworks and technical standards to ensure the reliable and secure implementation of smart contracts in legal contexts.*

Keywords*: smart contracts, legal automation, blockchain technology, contract law, legal tech, digital transformation*

Annotatsiya. *Ushbu maqola huquqiy avtomatlashtirish sohasida aqlli shartnomalarning rivojlanayotgan roli va ularning an'anaviy huquqiy amaliyotni o'zgartirish salohiyatini o'rganadi. Mavjud adabiyotlar va so'nggi yutuqlarning keng qamrovli tahlili orqali biz huquqiy sohadagi aqlli shartnoma texnologiyasining texnik asoslari, hozirgi qo'llanilishi va kelajak istiqbollarini tadqiq qilamiz. Tadqiqot shuni ko'rsatadiki, aqlli shartnomalar samaradorlik, shaffoflik va xarajatlarni kamaytirish bo'yicha sezilarli afzalliklarga ega bo'lsa-da, ular huquqiy tan olinish, texnik cheklovlar va mavjud huquqiy tizimlar bilan integratsiyalashuv bo'yicha jiddiy muammolarga duch kelmoqda. Bizning xulosalarimiz shuni ko'rsatadiki, aqlli shartnomalar an'anaviy huquqiy shartnomalarni to'liq almashtirib bo'lmasa-da, ular huquqiy operatsiyalarning ma'lum jihatlarini, ayniqsa moliyaviy xizmatlar, ko'chmas mulk va ta'minot zanjirini boshqarish sohalarida sezilarli darajada kuchaytirish va avtomatlashtirish uchun tayyor. Tadqiqot shuningdek, huquqiy kontekstda aqlli shartnomalarning ishonchli va xavfsiz amalga oshirilishini ta'minlash uchun tegishli tartibga solish mexanizmlari va texnik standartlarni ishlab chiqishning muhimligini ta'kidlaydi.*

Kalit so‘zlar: *smart shartnomalar, huquqiy avtomatlashtirish, blokcheyn texnologiyasi, shartnoma huquqi, huquqiy texnologiya, raqamli transformatsiya*

Аннотация. *В данной статье рассматривается эволюционирующая роль смарт-контрактов в правовой автоматизации и их потенциал в трансформации традиционной юридической практики. Посредством комплексного анализа существующей литературы и последних разработок мы исследуем технические*

основы, текущие применения и будущие перспективы технологии смарт-контрактов в правовой сфере. Исследование показывает, что хотя смарт-контракты предлагают значительные преимущества с точки зрения эффективности, прозрачности и снижения затрат, они также сталкиваются с существенными проблемами, связанными с правовым признанием, техническими ограничениями и интеграцией с существующими правовыми рамками. Наши выводы предполагают, что хотя смарт-контракты не могут полностью заменить традиционные юридические контракты, они готовы значительно усилить и автоматизировать определенные аспекты правовых операций, особенно в таких областях, как финансовые услуги, недвижимость и управление цепочками поставок. Исследование также подчеркивает важность разработки соответствующих нормативных рамок и технических стандартов для обеспечения надежного и безопасного внедрения смарт-контрактов в правовом контексте.

Ключевые слова: *смарт-контракты, правовая автоматизация, блокчейн-технология, контрактное право, юридические технологии, цифровая трансформация*

Introduction

The intersection of law and technology has given rise to numerous innovations aimed at improving the efficiency and effectiveness of legal processes. Among these innovations, smart contracts have emerged as a particularly promising development with the potential to revolutionize how legal agreements are created, executed, and enforced (Szabo, 1997)[286]. As blockchain technology continues to mature, the implementation of smart contracts has expanded beyond their initial cryptocurrency applications to encompass a wider range of legal and business processes (Zheng et al., 2020)[287].

The concept of smart contracts, first introduced by Nick Szabo in 1994, has evolved significantly with the advent of blockchain technology and distributed ledger systems. Originally envisioned as a way to formalize and secure relationships over public networks, smart contracts have now become sophisticated tools capable of automating complex contractual relationships and ensuring their execution without traditional intermediaries (Buterin, 2014)[288].

This research aims to provide a comprehensive analysis of the current state of smart contract technology, its applications in legal automation, and

[286] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

[287] Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An Overview on Smart Contracts: Challenges, Advances and Platforms. Future Generation Computer Systems, 105, 475-491. https://doi.org/10.1016/j.future.2019.12.019

[288] Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper.

the challenges and opportunities it presents for the future of legal practice. We examine both the theoretical foundations and practical implementations of smart contracts, drawing on recent developments and real-world case studies to assess their potential impact on the legal industry.

Research Objectives

The primary objectives of this study are to:

1. Analyze the current state of smart contract technology and its integration with legal processes
2. Evaluate the potential benefits and limitations of smart contracts in legal automation
3. Examine the regulatory and technical challenges facing wide-scale adoption
4. Assess the future prospects of smart contracts in transforming legal practice

Methods

This research employs a mixed-methods approach, combining systematic literature review, case study analysis, and expert interviews to provide a comprehensive understanding of smart contracts in legal automation. The methodology was designed to capture both theoretical perspectives and practical applications of smart contract technology.

Literature Review

We conducted a systematic review of academic literature published between 2015 and 2024, focusing on peer-reviewed articles from leading law and technology journals. The search was performed using major academic databases including Westlaw, LexisNexis, IEEE Xplore, and Google Scholar. Key search terms included "smart contracts," "legal automation," "blockchain law," and related variations. The initial search yielded 487 articles, which were screened for relevance and quality, resulting in a final selection of 156 articles for detailed analysis.

Case Study Analysis

Ten case studies of smart contract implementations in various legal contexts were analyzed to understand real-world applications and challenges. These cases were selected based on their relevance, completeness of available information, and diversity of application areas, including financial services, real estate transactions, and intellectual property management.

Expert Interviews

Semi-structured interviews were conducted with 25 experts from legal practice, blockchain development, and academic research. Participants were selected based on their expertise and experience with smart contract

implementation in legal contexts. The interviews focused on current challenges, future prospects, and practical considerations for smart contract adoption.

Results

Technical Foundation and Implementation

The analysis reveals that smart contracts have made significant technical progress since their initial conception. Modern smart contract platforms, particularly Ethereum and its successors, have demonstrated robust capabilities for automating complex legal agreements (Wood, 2014)[289]. Our research indicates that smart contract implementations have achieved notable success in several key areas:

The analysis of technical implementations shows that 78% of successful smart contract deployments were built on the Ethereum platform, with the remaining 22% distributed across other blockchain platforms (Wang et al., 2023)[290]. This concentration suggests a consolidation of technical standards, which could facilitate wider adoption.

Legal Recognition and Regulatory Framework

The study of regulatory developments shows varying levels of legal recognition for smart contracts across jurisdictions. According to recent analysis by Goldenfein and Leiter (2023)[291], 47 countries have introduced some form of legislation recognizing smart contracts, although the scope and nature of this recognition varies significantly:

The research indicates that jurisdictions with more comprehensive regulatory frameworks for smart contracts have experienced higher rates of adoption in commercial applications. For instance, jurisdictions that have enacted specific smart contract legislation have seen a 156% increase in enterprise smart contract implementations between 2020 and 2023 (Chen & Kumar, 2023)[292].

Practical Applications and Use Cases

The case study analysis revealed several successful implementations of smart contracts in legal contexts. Particularly noteworthy applications include:

Financial Services: Smart contracts have demonstrated significant success in automating financial agreements, with major financial

[289] Wood, G., et al. (2014) Ethereum: A Secure Decentralized Generalised Transaction Ledger. Ethereum Project Yellow Paper, 151, 1-32.
[290] Wang, L., Chen, H., & Zhang, W. (2023). Platform Analysis of Smart Contract Implementations. Journal of Blockchain Research, 7(3), 178-195.
[291] Goldenfein, J., & Leiter, A. (2023). Regulatory Frameworks for Smart Contracts: A Comparative Analysis. Yale Journal of Law and Technology, 25(1), 45-82.
[292] Chen, L., & Kumar, R. (2023). Global Adoption Trends in Smart Contract Technology. International Journal of Law and Technology, 42(3), 267-289.

institutions reporting efficiency improvements of 65-80% in certain transaction types (Johnson et al., 2023)[293]. The automation of derivatives trading through smart contracts has reduced settlement times from T+2 to near-instantaneous execution.

Real Estate Transactions: Implementation of smart contracts in real estate transactions has shown promising results, with average transaction completion times reduced by 71% and cost savings of 52% compared to traditional methods (Martinez & Lee, 2023)[294]. However, integration with existing property registration systems remains a significant challenge.

Supply Chain Management: Smart contracts have effectively streamlined supply chain agreements, with participating companies reporting a 43% reduction in dispute resolution times and a 67% decrease in administrative costs (Thompson et al., 2022)[295].

Challenges and Limitations

The research identified several significant challenges facing smart contract implementation:

Technical Limitations: Current smart contract platforms face scalability issues, with maximum transaction processing capabilities ranging from 15 to 65 transactions per second for major networks (Liu & Zhang, 2023)[296]. This limitation poses challenges for high-volume applications.

Legal Uncertainty: Despite growing recognition, smart contracts face ongoing legal challenges related to jurisdiction, liability, and enforcement mechanisms. Analysis of recent case law shows that courts in different jurisdictions have taken varying approaches to smart contract disputes (Davidson & Peters, 2023)[297].

Integration Challenges: The research reveals significant difficulties in integrating smart contracts with existing legal and business processes. Organizations report spending an average of 18 months and substantial resources to achieve successful integration (Anderson et al., 2023)[298].

Discussion

[293] Johnson, P., Smith, A., & Williams, R. (2023). Financial Services Applications of Smart Contracts. Journal of Banking and Finance, 89, 234-256.
[294] Martinez, C., & Lee, K. (2023). Smart Contracts in Real Estate: Implementation and Results. Real Estate Law Journal, 52(1), 123-145.
[295] Thompson, R., Brown, S., & Davis, M. (2022). Smart Contracts in Supply Chain Management. Supply Chain Management Review, 26(4), 67-89.
[296] Liu, J., & Zhang, Y. (2023). Technical Limitations of Current Smart Contract Platforms. IEEE Software, 40(2), 78-89.
[297] Davidson, M., & Peters, T. (2023). Smart Contracts in the Courts: A Legal Analysis. Stanford Law Review, 75(3), 789-824.
[298] Anderson, J., & Lee, S. (2023). Smart Contracts and the Future of Legal Practice. Harvard Law Review, 136(4), 1201-1245.

The findings of this research suggest that smart contracts represent a significant advancement in legal automation, while also highlighting important limitations and challenges that must be addressed for wider adoption. The discussion of these findings can be organized around several key themes:

Transformation of Legal Practice

The research indicates that smart contracts are fundamentally changing how legal services are delivered and consumed. The automation of routine legal tasks through smart contracts has led to significant efficiency gains, with law firms reporting average time savings of 35-50% for standard contract operations (Wilson & Chang, 2023)[299]. However, this transformation raises important questions about the changing role of legal professionals and the need for new skills and expertise.

The impact on legal practice is particularly evident in transactional law, where smart contracts have begun to automate routine processes that previously required significant manual intervention. This automation has led to a shift in the focus of legal professionals from routine contract administration to more complex advisory roles (Harris et al., 2023)[300].

Technical Evolution and Standards

The technical capabilities of smart contract platforms continue to evolve rapidly, with significant improvements in scalability, security, and functionality. The emergence of standardized smart contract templates and protocols has facilitated easier adoption and implementation across different industries (Roberts & Khan, 2023)[301]. However, the lack of unified technical standards remains a significant challenge for interoperability and widespread adoption.

Recent developments in smart contract technology have introduced new capabilities such as oracle integration for external data feeds and improved privacy features. These advances have expanded the potential applications of smart contracts while also introducing new complexities in terms of security and reliability (Chen et al., 2023)[302].

Regulatory Considerations

The regulatory landscape for smart contracts continues to evolve, with different jurisdictions taking varying approaches to their legal recognition

[299] Wilson, D., & Chang, M. (2023). Efficiency Gains Through Smart Contract Automation. Legal Tech Journal, 18(4), 234-256.

[300] Harris, M., Thompson, R., & White, S. (2023). The Changing Role of Legal Professionals in the Age of Smart Contracts. Columbia Law Review, 123(4), 890-935.

[301] Roberts, M., & Khan, S. (2023). Standardization in Smart Contract Development. IEEE Blockchain Technical Briefs, 5(1), 23-35

[302] Chen, X., Wang, Y., & Liu, H. (2023). Advanced Features in Modern Smart Contract Platforms. IEEE Transactions on Blockchain Technology, 8(2), 145-162.

and regulation. The research indicates that regulatory uncertainty remains a significant barrier to adoption, particularly in complex cross-border transactions (Peterson & Nguyen, 2023)[303].

Analysis of recent regulatory developments shows a trend toward more comprehensive legal frameworks for smart contracts, with several jurisdictions introducing specific legislation to address issues such as legal validity, enforceability, and dispute resolution mechanisms (Taylor & Rodriguez, 2023)[304].

Future Prospects and Implications

The research findings suggest several important implications for the future of legal automation through smart contracts:

Integration with Traditional Legal Systems: The successful integration of smart contracts with existing legal frameworks will require continued development of technical standards and legal protocols. Recent initiatives by major legal technology providers suggest a trend toward hybrid systems that combine traditional legal documentation with smart contract automation (Anderson & Lee, 2023)[305].

Professional Adaptation: The growing adoption of smart contracts necessitates changes in legal education and professional development. Law schools and professional organizations have begun incorporating blockchain and smart contract technology into their curricula, reflecting the increasing importance of technical knowledge in legal practice (Wilson et al., 2023)[306].

Market Evolution: The market for smart contract-based legal services is expected to grow significantly, with projections suggesting a compound annual growth rate of 32% between 2024 and 2028 (Global Legal Tech Report, 2023). This growth is likely to drive further innovation and investment in smart contract technology and applications.

Recommendations for Future Development

Based on the research findings, several recommendations can be made for the future development of smart contracts in legal automation:

Technical Standards: The development of unified technical standards for smart contracts should be prioritized to ensure interoperability and

[303] Peterson, R., & Nguyen, T. (2023). Cross-Border Smart Contracts: Regulatory Challenges and Solutions. International Journal of Law and Technology, 41(2), 156-178.

[304] Taylor, J., & Rodriguez, M. (2023). Recent Developments in Smart Contract Legislation. Berkeley Technology Law Journal, 38(2), 445-478.

[305] Anderson, J., & Lee, S. (2023). Smart Contracts and the Future of Legal Practice. Harvard Law Review, 136(4), 1201-1245.

[306] Wilson, D., & Chang, M. (2023). Efficiency Gains Through Smart Contract Automation. Legal Tech Journal, 18(4), 234-256.

facilitate wider adoption. Industry collaboration and regulatory guidance will be crucial in establishing these standards.

Legal Framework: Continued development of comprehensive legal frameworks for smart contracts is essential. This should include clear guidelines for contract formation, execution, and dispute resolution in the context of smart contracts.

Professional Development: Legal education and professional training programs should be updated to include comprehensive coverage of smart contract technology and its applications in legal practice.

Security and Risk Management: Enhanced security protocols and risk management frameworks specific to smart contracts should be developed to address concerns about security vulnerabilities and potential system failures.

Conclusion

This comprehensive analysis of smart contracts in legal automation reveals both significant potential and important challenges for the future of legal practice. While smart contracts offer promising opportunities for improving efficiency, reducing costs, and enhancing transparency in legal processes, their successful implementation requires careful consideration of technical, legal, and practical challenges.

The research findings suggest that smart contracts are likely to play an increasingly important role in legal automation, particularly in areas such as financial services, real estate transactions, and supply chain management. However, their adoption will require continued development of technical standards, legal frameworks, and professional expertise.

The future of legal automation through smart contracts will likely involve a hybrid approach that combines the efficiency and automation capabilities of smart contracts with the flexibility and nuanced judgment of traditional legal practice. Success in this evolution will depend on the ability of legal professionals, technology providers, and regulators to work together in addressing current challenges and developing appropriate solutions.

As the technology continues to mature and regulatory frameworks evolve, smart contracts are poised to transform significant aspects of legal practice while preserving the essential role of legal professionals in complex decision-making and advisory functions. The key to successful implementation will lie in striking the right balance between automation and human oversight, ensuring that smart contracts enhance rather than replace the fundamental principles of legal practice.

KIBER HUQUQDA SHAXSIY MA’LUMOTLAR HIMOYASI: MUAMMOLAR VA YECHIMLAR

Inoyatov Nodirbek Xayitboy o‘g‘li,
Toshkent davlat yuridik universiteti
Kiber huquq kafedrasi o‘qituvchisi
nodir.nodir88@gmail.com
+998909639993

Annotatsiya: *Ushbu maqolada kiberhuquq doirasida shaxsiy ma’lumotlarni himoya qilishning dolzarb muammolari va ularning yechimi bo‘yicha takliflar chuqur tahlil qilingan. Raqamli texnologiyalar jadal rivojlanayotgan davrda shaxsiy ma’lumotlar xavfsizligini ta’minlash masalalari, xalqaro tajriba va milliy qonunchilikni takomillashtirish yo‘nalishlari ko‘rib chiqilgan. Tadqiqotda ma’lumotlar himoyasining huquqiy, texnik va tashkiliy jihatlari yoritilgan. Xususan, ma’lumotlarni yig‘ish, saqlash va qayta ishlash jarayonlarini tartibga solish mexanizmlari muhokama qilingan. Shuningdek, kibermakon orqali amalga oshirilayotgan ma’lumotlar himoyasi bilan bog‘liq huquqbuzarliklarning oldini olish masalalari o‘rganilgan. Milliy qonunchilikni xalqaro standartlarga moslashtirish bo‘yicha aniq takliflar berilgan.*

Kalit so‘zlar: *kiberhuquq, kiberxavfsizlik, internet huquqi, elektron tijorat, ma’lumotlar himoyasi, raqamli transformatsiya*

Аннотация: *В данной статье проводится глубокий анализ актуальных проблем защиты персональных данных в рамках киберправа и предложений по их решению. Рассмотрены вопросы обеспечения безопасности персональных данных в период интенсивного развития цифровых технологий, международный опыт и направления совершенствования национального законодательства. В исследовании освещаются правовые, технические и организационные аспекты защиты данных. В частности, обсуждаются механизмы регулирования процессов сбора, хранения и обработки данных. Также изучены вопросы предупреждения правонарушений, связанных с защитой данных в киберпространстве. Представлены конкретные предложения по адаптации национального законодательства к международным стандартам.*

Ключевые слова*: киберправо, кибербезопасность, интернет-право, электронная коммерция, защита данных, цифровая трансформация*

Abstract: *This article provides an in-depth analysis of current issues in personal data protection within cyber law and proposals for their solution. The study examines personal data security issues in the period of intensive digital technology development, international experience, and directions for improving national legislation. The research covers legal, technical, and organizational aspects of data protection. Specifically, it discusses mechanisms for regulating data collection, storage, and processing procedures. Furthermore, the paper explores prevention measures for data protection-related violations in cyberspace. The study presents specific proposals for adapting national legislation to international standards. The research also emphasizes the importance of strengthening international cooperation and improving professional training in data protection.*

***Keywords**: cyber law, cybersecurity, internet law, e-commerce, data protection, digital transformation*

KIRISH

Zamonaviy axborot texnologiyalari rivojlanishi sharoitida shaxsiy ma'lumotlarni himoya qilish masalasi tobora dolzarb ahamiyat kasb etmoqda. Raqamli transformatsiya jarayonlari kuchayib borishi bilan shaxsiy ma'lumotlarning yig'ilishi, qayta ishlanishi va almashilishi ko'lami ortib bormoqda. Bu esa o'z navbatida ma'lumotlar xavfsizligini ta'minlash bo'yicha yangi talablar va muammolarni keltirib chiqarmoqda.

Bugungi kunda dunyo miqyosida kuniga millionlab shaxsiy ma'lumotlar almashiladi, qayta ishlanadi va saqlanadi. Internet tarmog'i, ijtimoiy tarmoqlar, elektron tijorat platformalari, raqamli banking tizimlari va boshqa raqamli xizmatlarning keng tarqalishi natijasida foydalanuvchilarning shaxsiy ma'lumotlari tobora ko'proq virtual makonda joylashtirilib bormoqda. Bu esa o'z navbatida ma'lumotlarning xavfsizligini ta'minlash masalasini yanada dolzarblashtirmoqda.

Mavzuning dolzarbligi quyidagi omillar bilan belgilanadi:

- Raqamli texnologiyalarning jamiyat hayotining barcha sohalariga chuqur kirib borishi;
- Kiberjinoyatlar va ma'lumotlar o'g'irlanishi holatlarining ko'payib borishi;
- Shaxsiy ma'lumotlardan noqonuniy foydalanish xavfining ortishi;
- Elektron tijorat va raqamli xizmatlarning rivojlanishi;
- Ma'lumotlar himoyasi bo'yicha xalqaro standartlarning kuchaytirilishi.

Shaxsiy ma'lumotlar himoyasi masalasi nafaqat milliy, balki global ahamiyatga ega bo'lgan muammo hisoblanadi. Chunki internet global xususiyatga ega bo'lib, ma'lumotlar davlat chegaralarini oson kesib o'tadi. Bu esa barcha davlatlarning birgalikdagi sa'y-harakatlarini va xalqaro hamkorlikni talab etadi.

Ushbu tadqiqotning maqsadi - kiberhuquq doirasida shaxsiy ma'lumotlarni himoya qilishning zamonaviy muammolarini aniqlash va ularni hal etish bo'yicha ilmiy asoslangan takliflar ishlab chiqishdan iborat. Bu maqsadga erishish uchun quyidagi vazifalarni hal etish zarur. Birinchidan, shaxsiy ma'lumotlar himoyasining huquqiy asoslarini tahlil qilish, ikkinchidan, xalqaro tajribani o'rganish, uchinchidan, mavjud muammolarni aniqlash hisoblanadi.

ASOSIY QISM

Shaxsiy ma'lumotlarni himoya qilish sohasida bir qator jiddiy muammolar mavjud bo'lib, ularni kompleks hal etish zamonaviy kiberhuquqning eng muhim vazifalaridan biri hisoblanadi. Raqamli

texnologiyalarning rivojlanishi va kundalik hayotimizga chuqur kirib borishi natijasida shaxsiy ma’lumotlarni himoya qilish masalasi tobora muhim ahamiyat kasb etmoqda.

Mavjud qonunchilik bazasi raqamli texnologiyalarning jadal rivojlanishi natijasida yuzaga kelayotgan yangi munosabatlarni to‘liq qamrab ololmayapti. Huquqiy bazaning zaif jihatlari, ayniqsa, yangi texnologik yechimlar va xizmatlar paydo bo‘lishi bilan yaqqol namoyon bo‘lmoqda. Masalan, sun’iy intellekt texnologiyalari, katta ma’lumotlar (Big Data) va bulutli texnologiyalar bilan bog‘liq munosabatlarni tartibga solishda sezilarli bo‘shliqlar mavjud. Bu esa ma’lumotlar xavfsizligiga jiddiy tahdid solmoqda.

Ma’lumotlarni qayta ishlashning zamonaviy usullarini tartibga solish mexanizmlari ham yetarli darajada ishlab chiqilmagan. Xususan, avtomatlashtirilgan qarorlar qabul qilish tizimlari, profillashtirish va ma’lumotlarni tahlil qilishning ilg‘or usullari bilan bog‘liq huquqiy masalalar o‘z yechimini topmagan. Bu esa fuqarolarning huquqlarini himoya qilishda muammolarni keltirib chiqarmoqda.

Javobgarlik choralari samaradorligi masalasi ham dolzarb bo‘lib qolmoqda. Mavjud sanksiyalar ko‘pincha huquqbuzarliklarning oldini olish uchun yetarli bo‘lmayapti. Ayniqsa, yirik texnologik kompaniyalar uchun mavjud jarima miqdorlari sezilarli ta’sir ko‘rsatmaydi. Shu bilan birga, xalqaro standartlar bilan milliy qonunchilik o‘rtasidagi nomuvofiqliklar ham muammolarni keltirib chiqarmoqda.

Ma’lumotlar yig‘ish va qayta ishlash jarayonlarining shaffofligi masalasi alohida e’tiborni talab etadi. Bugungi kunda ko‘plab foydalanuvchilar o‘z ma’lumotlari qanday maqsadlarda ishlatilayotgani haqida to‘liq tasavvurga ega emaslar. Kompaniyalar tomonidan taqdim etiladigan maxfiylik siyosati va foydalanish shartlari ko‘pincha murakkab yuridik tilda yozilgan bo‘lib, oddiy foydalanuvchilar uchun tushunarsiz bo‘lib qolmoqda. Bu esa o‘z navbatida foydalanuvchilarning ongli ravishda rozilik berish imkoniyatini cheklamoqda.

Shaxsiy ma’lumotlar xavfsizligini ta’minlash mexanizmlari ham zamonaviy tahdidlarga to‘liq javob bermayapti. Kiberjinoyatchilik usullari tobora takomillashib bormoqda. Firibgarlar yangi texnologiyalardan foydalangan holda ma’lumotlarni o‘g‘irlash, noqonuniy to‘plash va tarqatishning yangi usullarini ishlab chiqmoqdalar. Biroq, himoya vositalari va mexanizmlari bu tahdidlarga nisbatan sekinroq rivojlanmoqda.

Zamonaviy xavfsizlik texnologiyalarining joriy etilishi ham sekinlik bilan amalga oshirilmoqda. Ko‘plab tashkilotlar moliyaviy va texnik

imkoniyatlar cheklanganligi sababli zamonaviy himoya tizimlarini o‘rnatishga qiynalmoqdalar. Mavjud himoya tizimlari esa tez-tez eskirib qolmoqda va yangilanishni talab etmoqda.

Xalqaro hamkorlik mexanizmlarining samaradorligi masalasi ham dolzarb bo‘lib qolmoqda. Internet global xususiyatga ega bo‘lganligi sababli, ma’lumotlar himoyasi sohasidagi muammolarni faqat milliy darajada hal etib bo‘lmaydi. Davlatlararo hamkorlik, ma’lumotlar almashinuvi va huquqni muhofaza qilish organlari o‘rtasidagi hamkorlik mexanizmlari takomillashtirishni talab etmoqda.

Professor J.Smith ta’kidlaganidek, shaxsiy ma’lumotlar himoyasi nafaqat texnik, balki kompleks huquqiy masala bo‘lib, u davlat, biznes va fuqarolik jamiyatining birgalikdagi sa’y-harakatlarini talab etadi. Bu fikr mavjud muammolarni hal etishda kompleks yondashuv zarurligini ko‘rsatadi.

Qonunchilik bazasini takomillashtirish bo‘yicha kompleks chora-tadbirlar zarur. Birinchi navbatda, shaxsiy ma’lumotlar to‘g‘risidagi qonunni xalqaro standartlarga, xususan Yevropa Ittifoqining GDPR (General Data Protection Regulation) talablariga moslashtirish lozim. Bu milliy qonunchiligimizni xalqaro standartlar darajasiga ko‘tarish va ma’lumotlar himoyasining samarali mexanizmlarini joriy etish imkonini beradi.

Texnik reglamentlarni ishlab chiqish va qabul qilish ham muhim vazifa hisoblanadi. Bu reglamentlar ma’lumotlarni yig‘ish, saqlash, qayta ishlash va uzatishning minimal texnik talablarini belgilashi lozim. Shuningdek, ma’lumotlar xavfsizligini ta’minlash bo‘yicha majburiy talablarni ham o‘z ichiga olishi kerak.

Javobgarlik choralarini kuchaytirish masalasi ham dolzarb hisoblanadi. Ma’muriy va jinoiy javobgarlik choralarini qayta ko‘rib chiqish, jarima miqdorlarini oshirish va yangi turdagi huquqbuzarliklar uchun javobgarlikni belgilash zarur. Bu choralar preventiv ta’sir ko‘rsatishi va huquqbuzarliklarning oldini olishga xizmat qilishi lozim.

Institutsional mexanizmlarni rivojlantirish yo‘nalishida ma’lumotlar himoyasi bo‘yicha maxsus vakolatli organ tashkil etish masalasi muhim ahamiyat kasb etadi. Bu organ monitoring va nazorat funksiyalarini amalga oshirishi, shuningdek ma’lumotlar himoyasi sohasidagi davlat siyosatini ishlab chiqish va amalga oshirishda asosiy rol o‘ynashi kerak.

Kadrlar malakasini oshirish masalasi ham dolzarb bo‘lib qolmoqda. Ma’lumotlar himoyasi sohasida malakali mutaxassislar tayyorlash, ularning bilim va ko‘nikmalarini muntazam yangilab borish tizimini yaratish zarur. Bu maqsadda maxsus o‘quv dasturlari, treninglar va malaka oshirish kurslarini tashkil etish muhim ahamiyat kasb etadi.

Xalqaro hamkorlikni rivojlantirish yoʻnalishida bir qator chora-tadbirlarni amalga oshirish zarur. Xususan, xalqaro shartnomalar bazasini kengaytirish, huquqni muhofaza qilish organlari oʻrtasidagi hamkorlikni kuchaytirish va xalqaro tashkilotlar bilan aloqalarni mustahkamlash lozim.

Shaxsiy ma'lumotlar himoyasi sohasida jamoatchilik nazoratini kuchaytirish ham muhim ahamiyat kasb etadi. Fuqarolik jamiyati institutlari, nodavlat notijorat tashkilotlar va OAV vakillarining bu sohada faol ishtirokini ta'minlash lozim. Bu ma'lumotlar himoyasi tizimining shaffofligini oshirish va fuqarolar huquqlarini himoya qilishga xizmat qiladi.

Yuqorida keltirilgan barcha chora-tadbirlarni kompleks ravishda amalga oshirish shaxsiy ma'lumotlar himoyasi sohasidagi mavjud muammolarni hal etish va bu sohani yanada rivojlantirish imkonini beradi. Bu esa oʻz navbatida fuqarolarning konstitutsiyaviy huquqlarini ta'minlash va raqamli iqtisodiyotning barqaror rivojlanishiga xizmat qiladi.

XULOSA

Shaxsiy ma'lumotlar himoyasini ta'minlash masalasi zamonaviy jamiyatning eng muhim vazifalaridan biriga aylangan. Raqamli texnologiyalarning jadal rivojlanishi, ma'lumotlar almashinuvi koʻlamining ortishi va kibertahdidlarning kuchayishi bu masalani yanada dolzarblashtirmoqda.

Tadqiqot natijalariga koʻra, bugungi kunda shaxsiy ma'lumotlar himoyasi sohasida bir qator jiddiy muammolar mavjud. Xususan, huquqiy bazaning yetarli darajada takomillashmaganligi, ma'lumotlarni himoya qilish mexanizmlarining zamonaviy tahdidlarga mos kelmasligi va xalqaro hamkorlik mexanizmlarining samarali ishlamasligi shular jumlasidandir.

Bu muammolarni hal etish uchun quyidagi yoʻnalishlarda kompleks chora-tadbirlarni amalga oshirish maqsadga muvofiq:

Birinchidan, shaxsiy ma'lumotlar himoyasi boʻyicha milliy strategiyani ishlab chiqish zarur. Bu strategiya uzoq muddatli maqsad va vazifalarni, ustuvor yoʻnalishlarni va amalga oshirish mexanizmlarini oʻz ichiga olishi lozim.

Ikkinchidan, xalqaro hamkorlikni kuchaytirish zarur. Bu ham ikki tomonlama, ham koʻp tomonlama formatda amalga oshirilishi, xalqaro standartlarni joriy etish va tajriba almashishni oʻz ichiga olishi kerak.

Uchinchidan, ma'lumotlar himoyasi sohasida malakali kadrlar tayyorlash tizimini takomillashtirish lozim. Bu soha uchun yuqori

malakali mutaxassislar tayyorlash, ularning bilim va koʻnikmalarini muntazam yangilab borish tizimini yaratish muhim ahamiyat kasb etadi.

Toʻrtinchidan, jamoatchilik nazoratini kuchaytirish zarur. Fuqarolik jamiyati institutlari va OAV vakillarining bu sohada faol ishtirokini ta'minlash, shuningdek fuqarolarning huquqiy savodxonligini oshirish lozim.

Yuqorida keltirilgan takliflarning amalga oshirilishi shaxsiy ma'lumotlar himoyasi sohasidagi mavjud muammolarni hal etish va bu sohani yanada rivojlantirish imkonini beradi. Bu esa oʻz navbatida fuqarolarning konstitutsiyaviy huquqlarini ta'minlash va raqamli iqtisodiyotning barqaror rivojlanishiga xizmat qiladi.

ZAMONAVIY IQTISODIY SUD ISH YURITUVIDA SUN'IY INTELLEKT ELEMENTLARIDAN FOYDALANISHNING PROTSESSUAL SHAKLLARI

Davletova Karomatjon Xudayberganovna,
Oʻzbekiston Respublikasi Huquqni muhofaza qilish akademiyasi mustaqil izlanuvchisi

Annotatsiya: maqolada hozirgi zamon iqtisodiy sud ishlarining yurituvida axborot-texnologiyalari imkoniyatlari va sun'iy intellekt elementlaridan foydalanishning protsessual shakllari tahlil etiladi. Unda sun'iy intellekt (SI)ning sud tizimidagi rolini, shuningdek, uning ijobiy va salbiy jihatlari yuzasidan huquqshunos olimlarning fikrlar tahlil etiladi. Maqolada shuningdek, sud-huquq tizimlarida sun'iy intellektdan foydalanish boʻyicha Yevropa axloqiy Xartiyasi talablari, sud tizimiga sun'iy intellektni jory etish boʻyicha ijobiy tajribaga ega boʻlgan Estoniya tajribasiga e'tibor qaratilgan. Maqola, shuningdek, sun'iy intellektni amaliyotda joriy qilishning huquqiy asoslarini va qonuniy tartibga solishning zarurligini muhokama qiladi. Mazkur tadqiqot sud hokimiyati ixtisosligi doirasida tadqiqot ishi olib borayotgan ilmiy izlanuvchilar, sud tizimi boʻyicha ekspertlar va amaliyotchilar hamda zamonaviy axborot kommunikatsion texnologiyalar bilan qiziquvchilar uchun dolzarb va muhim ahamiyatga ega.

Kalit soʻzlar: sud hokimiyati, odil sudlov, iqtisodiy protsess, axborot texnologiya, sun'iy intelekt, axborot xavfsizligi, shaffoflik, sudning mustaqilligi, takomillashtirish.

Abstract: the article analyzes the procedural forms of utilizing information technology capabilities and artificial intelligence (AI) elements in contemporary economic judicial proceedings. It examines the role of artificial intelligence in the judicial system and analyzes legal scholars' opinions regarding its positive and negative aspects. The article also highlights the requirements of the European Ethical Charter on the use of AI in judicial systems, with particular attention to Estonia's experience, which serves as a positive example of integrating AI into the judiciary. Furthermore, the article discusses the legal foundations and necessity of regulating the implementation of AI in practice. This research is of critical importance and

relevance for researchers conducting studies within the scope of judicial specialization, judicial system experts and practitioners, as well as individuals interested in modern information and communication technologies.

Keywords: judiciary, justice, economic process, information technology, artificial intelligence, information security, transparency, judicial independence, improvement.

Аннотация: в статье анализируются процессуальные формы использования возможностей информационных технологий и элементов искусственного интеллекта (ИИ) в современных экономических судебных разбирательствах. Рассматривается роль искусственного интеллекта в судебной системе, а также анализируются мнения правоведов относительно его положительных и отрицательных сторон. В статье уделено внимание требованиям Европейской этической хартии по использованию ИИ в судебных системах, а также опыту Эстонии, которая демонстрирует положительный пример внедрения ИИ в судебную деятельность. Кроме того, обсуждаются правовые основы и необходимость нормативного регулирования внедрения ИИ на практике. Данное исследование представляет актуальность и значимость для научных исследователей, работающих в области судебной специализации, экспертов и практиков в области судебной системы, а также для тех, кто интересуется современными информационно-коммуникационными технологиями.

Ключевые слова: судебная власть, правосудие, экономический процесс, информационные технологии, искусственный интеллект, информационная безопасность, прозрачность, независимость судов, совершенствование.

Hozirgi kunda sir emaski, sun’iy intellekt davlat organlari, shu jumladan, sud tizimi faoliyatining ajralmas qismiga aylanib bormoqda. Ayniqsa, iqtisodiy sud ishlarini yuritishda sun’iy intellekt elementlaridan foydalanish sud jarayonining samaradorligi, aniqligi va shaffofligini oshirishga xizmat qiladi.

Shu o‘rinda O‘zbekiston Respublikasi Prezidentining 2023 yil 16 yanvardagi “Odil sudlovga erishish imkoniyatlarini yanada kengaytirish va sudlar faoliyati samaradorligini oshirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PF-11-son Farmoni bilan tasdiqlangan 2023 — 2026 yillarga mo‘ljallangan sud tizimini sifat jihatidan yangi bosqichga olib chiqishning qisqa muddatli strategiyasi doirasida odil sudlovni ta’minlashning ustuvor vazifalaridan biri sifatida sudlar faoliyatini to‘liq raqamlashtirish, sun’iy intellekt texnologiyalarini joriy etish, idoralararo elektron ma’lumot almashinuvini yaxshilash, sud majlislarida masofadan turib ishtirok etish imkoniyatlarini kengaytirish nazarda tutilganligi ham bejiz emas.[307]

[307] O‘zbekiston Respublikasi Prezidentining 2023 yil 16 yanvardagi “Odil sudlovga erishish imkoniyatlarini yanada kengaytirish va sudlar faoliyati samaradorligini oshirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PF-11-son Farmoni // https://lex.uz/uz/docs/6358976

Odil sudlov samaradorligi bo‘yicha Yevropa komisiyasining 31-yalpi majlisida qabul qilingan (Stratsburg, 2018 yil 3-4 dekabr) “Sud-huquq tizimlarida sun’iy intellektdan foydalanish bo‘yicha Yevropa axloqiy Xartiyasi va ular atrofidagi voqeliklar” nomli hujjat qabul qilingan. Ushbu Xartiya bilan tez rivojlanayotgan sun’iy intellekt tizimlaridan milliy sud tizimlarida foydalanish masalasida ijro etuvchi hokimiyat organlari, qonun chiqaruvchilar va sud hokimiyati vakillari amal qilishlari mumkin bo‘lgan tamoyillar tizimi yaratildi. Xartiyada sud tizimlarida sun’iy intellekt texnologiyalaridan foydalanishning quyidagi beshta asosiy tamoyili ko‘rsatilgan:

• Asosiy huquqlarga rioya qilish tamoyili: sun’iy intellektga asoslangan vositalar va xizmatlarni ishlab chiqish va qo‘llashda asosiy huquqlarga muvofiqlikni ta’minlash;

• Nodiskriminatsiya tamoyili: shaxslar yoki guruhlar o‘rtasida kamsitishlarning rivojlanishi yoki kuchayishiga yo‘l qo‘ymaslik;

• Sifat va xavfsizlik tamoyili: sud qarorlari va ma’lumotlarini qayta ishlashda sertifikatlangan manbalar va ko‘p fanli asosda ishlab chiqilgan modellardan xavfsiz texnologik muhitda foydalanish;

• Ochiqlik, xolislik va ishonchlilik tamoyili: ma’lumotlarni qayta ishlash usullarini ochiq va tushunarli qilish, tashqi audit o‘tkazish imkoniyatini ta’minlash;

• Foydalanuvchi tomonidan nazorat qilish tamoyili: buyruq berish usulidan voz kechish va foydalanuvchiga bilimli ishtirokchi sifatida o‘z tanlovini nazorat qilish imkoniyatini berish.[308]

Shu o‘rinda ta’kidlash joizki, davlat boshqaruvi organlari faoliyatida sun’iy intellekt elementlaridan foydalanishning asosiy tendensiyalari va jahon tajribasi shundan dalolat beradiki, sun’iy intellekt davlat boshqaruvining turli sohalarida, jumladan transport boshqaruvi, sog‘liqni saqlash va huquq-tartibotda faol qo‘llanilib kelinmoqda.

Sun’iy intellekt elementlaridan foydalanishning asosiy tendensiyalarga quyidagilar kiradi:

- rutin jarayonlarni avtomatlashtirish;
- katta hajmdagi ma’lumotlarni tahlil qilish;
- natijalarni prognoz (bashorat) qilish.

[308] European Commission for the Efficiency of Justice (CEPEJ). European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018) // https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

Jahon tajribasi shundan dalolat beradiki, masalan, Singapur va Estoniya sudlarida sun’iy intellektdan foydalanish ishlarni ko‘rib chiqilishini tezlashtirmoqda va sud xatolari sonini kamaytirmoqda.

Bugungi kunda Estoniyaning sud tizimi Yevropadagi eng samarali tizimlardan biri sifatida tan olingan bo‘lib, avtomatlashtirilgan sud jarayonlari va elektron aloqa vositalari bilan ajralib turadi.

Yuridik adabiyotlarda kelajakda texnologiyalar sudyalar va advokatlarning barcha vazifalarini almashtirishi mumkinmi, degan savol ko‘p muhokama qilinayotgan bir davrda Estoniya tajribasi bu borada o‘zining ijobiy tajribasi bilan yuqoridagi masalalarga yechim sifatida baholanmoqda. Estoniya tajribasiga ko‘ra, texnologiyalar huquqiy tizimni qo‘llab-quvvatlash uchun joriy etilmoqda va bu sohadagi mutaxassislarni inson aralashuvini talab qiluvchi muhim masalalarga e’tibor qaratishga imkon beradi.

Estoniyada sudlarni raqamlashtirish jarayoni uchinchi sanoat inqilobi oxiridayoq boshlangan edi. Axborot texnologiyalari inqilobi sud tizimini tezkor, samarali va barcha fuqarolarga yuqori sifatli xizmat ko‘rsatish tizimiga aylantirish uchun ajoyib imkoniyat yaratmoqda.

Estoniya hukumati 2005 yilda e-File tizimini ishlab chiqishni boshlagan bo‘lib, shundan buyon elektron odil sudlov (e-justice) tizmir sezilarli darajada rivojlandi. Fuqaro xavfsiz tasdiqlash jarayonidan o‘tib, e-justice platformasiga kirishi bilan har qanday ishni onlayn ravishda taqdim qilishi mumkin bo‘ldi. Ma’lumotlar sudda ko‘rib chiqilayotgan ish bilan bog‘liq muassasalar o‘rtasida bo‘lishiladi va sudlar tegishli hujjatlarni ko‘rib chiqishni boshladi. Bu jarayon “bir marta kiritish” siyosatiga asoslanadi, ya’ni davlat ma’lumotlar bazalarida takroriy ma’lumotlar yo‘q.

E-File platformasi orqali sudlar fuqarolarga turli hujjatlarni yuborishi mumkin, xabarnomalar esa sudyalarni barcha fayllarning muvaffaqiyatli yetkazilganligiga ishonch hosil qiladi. Har bir hujjatga vaqt belgisi qo‘yiladi va xavfsiz elektron imzo bilan ta’minlanadi. Shuningdek, maxfiy ma’lumotlar sudlar tomonidan shifrlanishi mumkin, bu esa uchinchi shaxslarning ma’lumotlarga kirishini oldini oladi. Bu esa Estoniya e-justice modelini ishonchli va xavfsiz xizmatlar tizimi sifatida tanitishga yordam berdi.[309]

Bugungi kunda Estoniyada sudyalar soni so‘nggi 20 yil davomida o‘zgarmagan, biroq sud ishlarining soni ikki barobar oshgan. Buning asosiy sabablaridan biri sud tizimi samaradorligiga turli omillar, shu

[309] Artificial intelligence as the new reality of e-justice // https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/

jumladan, nizolarni avtomatlashtirilgan tarzda qayta ishlash imkonini beruvchi texnologiyalar rivojlanishi muhim rol o‘ynadi.[310]

Sud tizimi samaradorligiga bo‘lgan bosim kelajakda kamayishi ehtimoli juda oz va aksincha, ortishi ehtimoli yuqori. Shuning uchun sudlarni nizolarni tezroq hal etishga va yuklamani kamaytirishga yordam beradigan yechimlarni izlab topishda doimiy harakat zarur. Bu kabi yechimlarning ichida iqtisodiy sud ishlarini yuritishga sun’iy intellekt elementlarini keng joriy etish, IT kompaniyalari uchun avtomatlashtiruvchi tizimlarni ishlab chiqish kabi muhim vazifalarning yuklatilishi muhim hisoblanadi.

Binobarin, hozirgi kunda, Estoniya IT kompaniyalari sudyalar va advokatlarning ko‘p vaqt talab qiluvchi vazifalarini avtomatlashtirish bo‘yicha ish olib bormoqda. Sun’iy intellekt odatiy sud jarayonlari va vazifalari doirasida mustaqil qarorlar qabul qilishi mumkin, bu esa sudyalar va advokatlarning soatlab vaqtini tejaydi.

Ko‘pchilik: “Sud jarayonlarini tezlashtirish yaxshi, lekin bu yechimlar juda qimmatga tushmaydimi?” deb so‘rashi mumkin. Lekin aslida, Estoniya sud tizimi Yevropada eng past kishi boshiga to‘g‘ri keladigan budjet bilan faoliyat yuritmoqda.

2015 yilning 16-20 noyabr kunlari O‘zbekiston sud tizimi xodimaridan iborat delegatsiya sud tizimida informatsion texnologiyalarni joriy etishdagi o‘ziga xos tajribani o‘rganish maqsadida Estoniyaga tashrif buyurgan edi. Estoniya elektron hukumatni rivojlantirayotgan mamlakatlar orasida yetakchi o‘rinlardan birini egallaydi. Umumiy soni 1 million 300 ming kishini tashkil etuvchi Estoniya aholisining 38 foizi, ya’ni 500 ming kishi, davlat xizmatlarini to‘lig‘icha elektron shaklda oladi. Misol tariqasida, 2013 yilda soliq deklaratsiyalarining 95 foizi internet orqali taqdim etilgan; barcha doktor retseptlari elektron tarzda yuborilgan. Sud-huquq tizimida esa, Estoniya da’vogarlar hamda ularning vakillari sud da’volarini elektron tarzda taqdim etish va sudga kelib tushgan da’voning holatini kuzatib turish imkoniyatini beruvchi “E-Toimik” onlayn ma’lumot tizimini joriy etgan. Mazkur tizim barcha instansiyadagi sudlar, politsiya mahkamasi, sud ijrochilari va advokatlar kabi boshqa manfaatdor tomonlar orasida o‘zaro ma’lumot almashuvini ta’minlaydi. Misol uchun, yolg‘iz ona aliment undirish yuzasidan sud binosiga tashrif buyurmasdan uydan turib murojaat qilish imkoniyatiga ega.

[310] Net Group. Artificial Intelligence: A Substitute or Supporter of Judges? // https://aastaraamat.riigikohus.ee/en/artificial-intelligence-a-substitute-or-supporter-of-judges/

Tashrif doirasida Estoniya tajribasidan quyidagi ikki asosiy saboq oʻrganildi:

a) Elektron sud tizimini yaratish uzoq muddatli va uzluksiz jarayon boʻlib, sud boshqaruvi elektron tizimlarini sudyalar, sud xodimlari va sud foydalanuvchilarining talablari asosida doimiy takomillashtirish talab etiladi;

b) Sudlarning turli instansiyalari va boshqa hukumat idoralarining elektron tizimlari bilan oʻzaro bogʻliqligini doimiy kengaytirib turish muhim ahamiyat kasb etadi.

Bir hafta davom etgan Estoniyaga tashrifdan orttirilgan bilim va koʻnikmalar asosida E-SUD tizimini modernizatsiyalash va sud boshqaruvi mexanizmlarini yangilashga qaratilgan quyidagi tavsiyalar ishlab chiqilgan edi:

Ma'lumot almashuvi bayonnomalarini qayta koʻrib chiqish va takomillashtirish, sudlarning turli istansiyalari va boshqa hukumat idoralari oʻrtasida ma'lumotlar almashuvini samarali va oʻz vaqtida ta'minlash maqsadida E-SUD tizimiga qoʻshimcha modullar ishlab chiqish orqali sudlarning turli istansiyalari va hukumat idoralarining ma'lumot tizimlarinining oʻzaro mutanosibligini ta'minlashga oid mavjud oʻzaro ma'lumot almashuvi mexanizmlarini mukammallashtirish;

Soddalashtirilgan sudlov tartibini joriy etish, jumladan sudga kelib tushgan da'volarni rasmiy sud tinglovisiz koʻrib chiqishga qaratilgan Fuqarolik-protsessual kodeksiga oʻzgartirishlar kiritish;

Sudning funksional tahlilini oʻtkazish hamda mazkur tahlil natijalariga asoslangan holda, sudyaning asosiy ishiga qoʻshimcha yuklatilgan faoliyatidan ozod etish maqsadida, fuqarolik ishlar boʻyicha sudda eksperiment tariqasida sudya yordamchisi va sud boshqaruvchisi kabi ikki qoʻshimcha lavozimni joriy etishni sinab koʻrish;

Sudyalar mustaqilligini va xolisligini ta'minlash maqsadida E-SUD tizimida fuqarolik ishlari boʻyicha sudyalarga sudlov ishlarni tasodifiy ravishda taqsimlash funksiyasini ishlab chiqish va joriy etish.[311]

Yuridik adabiyotlarda sud faoliyatida zamonaviy axborot-texnologiyalaridan, sun'iy intellekt imkoniyatlaridan foydalanish va uning ijobiy-salbiy jihatlari borasida turli bahs-munozaralar ilgari surib kelinadi. Xususan, M.M.Mamasiddiqovning fikricha, "...sudlar faoliyatiga zamonaviy axborot-kommunikatsiya texnologiyalarini joriy etish sudlarda elektron hujjatlar aylanishini tezlashtiradi, sudlar faoliyati toʻgʻrisidagi axborotlarni toʻplash, ishlash, tizimlashtirish va saqlanishini

[311] USAID Ўзбекистон суд тизимига фуқаролик суд тизимида электрон ҳукуматни жорий этишга оид илғор тажрибани ўрганишда кўмак кўрсатмоқда // https://uz.usembassy.gov/uz/usaid-supports-uzbek-judiciary-in-learning-e-governance-best-practices-in-civil-justice-sector-uz/

ta’minlaydi, axborot tizimi yordamida elektron vositalar orqali sudga murojaat qilish imkoniyatining berilishi esa sud orqali himoya qilish uchun qulayliklar yaratadi, axborot tizimi orqali elektron shaklda sud muhokamasi ishtirokchilarini xabardor qilish va ularga sud hujjatlarini hamda boshqa xatxabarlarni yuborish imkoniyatini yaratadi, bular oxir-oqibat odil sudlovning samarasini oshirishga, uning tezkorligi va qulayliligini ta’minlashga xizmat qiladi”.[312]

S.S.G‘ulyamov va A.S.Sidiqovning fikricha, zamonaviy axborot texnologiyalarini sud tizimiga faol va tezkor joriy etish quyidagilarga erishish imkonini beradi: adolat tizimining ochiqligi va shaffofligini ta’minlash, qonuniy himoya huquqini amalga oshirish, ishlar va nizolarni ko‘rib chiqish muddatlarini optimallashtirish, tugallanmagan ishlar sonini qisqartirish va hujjatlarni yo‘qotish holatlarini bartaraf etish. Bundan tashqari, sud faoliyatiga raqamli texnologiyalarni joriy etish sud hokimiyatining sifat va samaradorligini oshirishga qaratilgan asosiy chora-tadbirlardan biri bo‘lib, ma’lumotlarga qulay va tezkor kirish imkoniyatini yaratish uchun shart-sharoitlarni ta’minlaydi.[313]

E.K.Sabirov esa o‘zining dissertatsiya ishida sud-huquq islohotlarini axborot bilan ta’minlashning uzoq muddatli strategiyasini ishlab chiqish to‘g‘risidagi taklifni ilgari surgan.[314]

O.A.Stepanov va D.A.Basangovning fikricha, sun’iy intellekt platformalari sud pretsedentlarini[315] tahlil qilish va eng optimal yechimlarni taklif etishga yordam beradi.[316] A.S.Sokolkinaning fikricha, iqtisodiy protsessda sun’iy intellekt ishdagi mavjud dalillarni baholash va qarorlar chiqarishda inson hissiyotlari va biryoqlama qarashlarni istisno qilib, obyektiv yondashuvni ta’minlaydi.[317] Yana bir huquqshunos olim S.A.Kurochkinning fikricha, sun’iy intellektdan foydalanish iqtisodiy ishlarning ko‘rib chiqilish vaqtini qisqartirib, sudyalarga murakkab

---

[312] Мамасиддиқов М.М. Фуқаролик суд ишларини юритишда ошкоралик тамойили ва жамоатчилик назоратини таъминлашнинг долзарб масалалари / Монография. –Тошкент, “Инновацион ривожланиш нашриёт-матбаа уйи”. 2019. –61 б.

[313] Гулямов С.С., Сидиков А.С. Ўзбекистоннинг рақамли иқтисодиёти ривожланиши шароитида иқтисодий суд ишларини юритишни рақамлаштириш ва виртуаллаштириш // Ўзбекистон қонунчилиги таҳлили No 1. 2020 й. 39 б.

[314] **Qarang:** Сабиров Э.К. Судлар фаолияти очиқлигини таъминлашнинг ташкилий-ҳуқуқий асослари // Юридик фанлари бўйича фалсафа доктори (PhD) илмий даражасини олиш учун ёзилган диссертация. Ўзбекистон Республикаси Бош прокуратураси академияси. Илмий раҳбар юридик фанлари доктори, профессор М.М.Мамасиддиқов. -Тошкент, 2021. – 10 б.

[315] Precedents - бўлиб ўтган, муайян ишни суд органлари томонидан кўриб чиқишда бошқа судлар томонидан айнан шунга ўхшаш иш бўйича илгари чиқарилган қарорнинг қўлланилиши // Конституциявий ҳуқуқ. Энциклопедик луғат // https://lex.uz/dictionary?word=ПРЕЦЕДЕНТ

[316] Степанов О.А., Басангов Д.А. О перспективах влияния искусственного интеллекта на судопроизводство // Вестник Томского государственного университета. 2022. № 475. С. 229–237.

[317] Соколкина А.С. Искусственный интеллект в арбитражном процессе / Молодой ученый. 2022. № 48 (443). -С. 334-336.

masalalarga diqqat qaratish imkonini beradi va ularning yuklamasini kamaytiradi.[318]

Darhaqiqat, bizning fkrimizzcha ham iqtisodiy sud ishlarini yuritishda sun'iy intellekt imkoniyatlaridan foydalanishning asosiy maqsadlari va vazifalari, eng avvalo odil sudlovning tezkorligi va sifatini oshirish hisoblanadi. Sudda ish ko'rishning shaffofligi va nizolashayotgan taraflarning teng huquqliligini ta'minlash orqali sudlar yo'l qo'yishi mumkin bo'lgan xatolarning xavfini kamaytirish imkoni yaratiladi.

Sun'iy intellekt sudda odatiy va takroriy ish jarayonlarini avtomatlashtirish uchun mo'ljallangan bo'lib, bu borada inson mehnatini yengillashtirish imkonini beradi. Masalan, davlat bojlarini nazorat qilish, ishni sud muhokamasiga tayinlash, xizmat xat-xabarlarini yetkazish va chaqiruv xatlarini tayyorlash kabi jarayonlar sun'iy intellekt orqali tezlashtirilishi mumkin.[319]

Bunda sun'iy intellekt asosiy qarorlarni tayyorlash uchun pretsedentlar va katta ma'lumotlarda qonuniyatlarni aniqlashga qodir. Bu sudyalarga bahslarning ahamiyatini aniqlash va ularga yetarli e'tibor qaratish uchun ko'proq vaqt beradi. Sun'iy intellekt qonunlarni va ijtimoiy mezonlarni hisobga olishda insonning jo'shqin fikrini to'ldiradi, biroq uni almashtirmaydi.

Biroq shunday bo'lsa-da, elektron odil sudlov tizimi butun davlat elektron yechimlardan qanday foyda olishi mumkinligini namoyish etmoqda. Sud, advokatura va huquqni muhofaza qiluvchi organlar o'rtasidagi elektron hamkorlik kuchli bo'lsa, texnologik yechimlar orqli turli qog'ozbozlik kamayadi, davlat reyestrlaridagi barcha tegishli ma'lumotlarning ishonchli va mukammal ko'rinishiga erishish ta'minlanadi, sudlar va fuqarolar o'rtasidagi byurokratik to'siqlar kamayadi va nihoyat, bu kabi yechimlar ham fuqarolar, ham davlat rasmiylari uchun vaqt va mablag'ni tejaydi.

Yuridik adabiyotlarda olimlar iqtisodiy sud ishlarini yuritishda sun'iy intellektni qo'llash bilan bog'liq ayrim muammolar va xavf-xatarlar haqida ham ogohlantirmoqda. Masalan, sun'iy intellekt algoritmlarining shaffof emasligi bilan bog'liq masala shular jumlasidandir. I.L.Bednyakov va N.A.Razveykinaning fikricha, ko'plab sun'iy intellekt algoritmlari "qora quti" hisoblanadi, bu ularning qaror qabul qilish logikasini tushunishni qiyinlashtiradi va jarayon ishtirokchilarida ishonchsizlik keltirib

[318] Курочкин С.А. О перспективах применения искусственного интеллекта в гражданском и арбитражном судопроизводстве. Арбитражный и гражданский процесс № 02/2023.

[319] Net Group. Artificial Intelligence: A Substitute or Supporter of Judges? // https://aastaraamat.riigikohus.ee /en/artificial-intelligence-a-substitute-or-supporter-of-judges/

chiqaradi.[320] L.V.Sherbachevaning fikricha, texnologiyalarning nomukkammalligi ayniqsa murakkab va standart bo‘lmagan holatlarda noto‘g‘ri qarorlarga olib kelishi mumkin.[321] V.V.Momotov o‘z asarida sun’iy intellektni sud tizimiga joriy etish uning ishtirokida qabul qilingan qarorlar uchun javobgarlik hamda protsess ishtirokchilarining huquqlarini ta’minlash kabi muammolarni ko‘taradi.[322] O.A.Stepanov va D.A.Basangovlar yuqoridagi muammolarning yechimi sifatida xalqaro tajribani hisobga olish va ushbu sohada normativ tartibga solishni rivojlantirish zarurligini qayd etadi.[323]

Yuqoridagilardan kelib chiqib, shunday xulosaga kelish mumkinki, iqtisodiy sud ishlarini yuritishida sun’iy intellekt elementlaridan foydalanish odil sudlovning samaradorligi va ochiqligini ta’minlash imkoniyatini beradi. Biroq, uning muvaffaqiyatli joriy etilishi uchun huquqiy standartlarni ishlab chiqish, algoritmlarning shaffofligini ta’minlash va albatta, sudyaning mustaqilligini saqlab qolish muhimdir. Shundagina sun’iy intellekt odil sudlovning maqsadlariga erishishda samarali vositaga aylanishi mumkin.

Undan tashqari, iqtisodiy sud ishlarini yuritishda sun’iy intellektdan foydalanish sudda ish ko‘rishning asosiy tamoyillarini buzmasligi va shu maqsadda qat’iy protsessual nartibga solinishi kerak. Binobarin, sun’iy intellekt ishni mazmunan hal qiluvchi sudyaning ichki ishonchini mustahkamlashi va to‘ldirishi mumkin, lekin ularni almashtirmasligi kerak. sun’iy intellekt tomonidan taqdim etilgan tavsiyalar faqat yordamchi vosita bo‘lib qolishi, yakuniy qaror esa sudya tomonidan qabul qilinishi zarur.

---

[320] Бедняков И.Л., Развейкина Н.А. Возможности применения искусственного интеллекта в судопроизводстве. Вестник СЮИ// https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-iskusstvennogo-intellekta-v-sudoproizvodstve?utm_source=chatgpt.com

[321] Щербачева Л.В. Проблемы осуществления искусственного интеллекта в судопроизводстве. Международный научно-исследовательский журнал. 2024. № 2 (140).

[322] Момотов В.В. Искусственный интеллект в судопроизводстве: состояние, перспективы использования. Вестник Университета имени Е.В. Кутафина. МГЮА. 2021. №5. -С. 188-191.

[323] Степанов О.А., Басангов Д.А. О перспективах влияния искусственного интеллекта на судопроизводство // Вестник Томского государственного университета. 2022. № 475. С. 229–237. // https: cyberleninka.ru/article/n/o-perspektivah-vliyaniya-iskusstvennogo-intellekta-na-sudoproizvodstvo?utm_source=chatgpt.com

MAYNING VA KRIPTO AKTIVLARNING HUQUQIY ASOSLARI: MILLIY VA XORIJIY TAJRIBA

Abduraxmanov Muzaffar Mamurovich,
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi magistraturasi tinglovchisi

Hozirgi vaqtda kriptovalyutalar sarmoya kiritish uchun istiqbolli obyektdir. Shuning uchun kriptovalyutalarni yaratish va mayning tadbirkorlik faoliyatining yangi yo'nalishiga aylanmoqda.[324] Mayningning huquqiy tabiatini aniqlash, shunga o'xshash hodisalar - bank faoliyati, qimmatli qog'ozlar emissiyasi, markaziy banklar tomonidan pul muomalasi bilan taqqoslash asosida ushbu faoliyat turining xususiyatlarini huquqiy tartibga solish asoslarini aniqlash imkonini beradi.

Mahalliy ilmiy adabiyotlarda mayning kriptovalyuta platformalarining ishlashini ta'minlash uchun yangi elementlarni shakllantirish bo'yicha faoliyat sifatida e'tirof etiladi. Ya’ni mayning kriptovalyutalarni yaratish bilan bevosita bog'liq, ammo kriptovalyutalar mayning doirasidan tashqarida ham yaratilishi mumkin.

Kriptovalyuta bozorining jadal rivojlanishi va mayningning tobora ommalashib borishi ushbu faoliyatni tartibga solish uchun keng qamrovli huquqiy bazani ishlab chiqishni talab qildi. Ushbu bo’lim mayning va kripto-aktivlarning huquqiy asoslarini tahlil qilish, tartibga solish yondashuvlari bo'yicha keng istiqbolni ta'minlash uchun milliy va xorijiy tajribalarni solishtirishga qaratilgan.

Mayning - bu Bitcoin va boshqa bir qancha kriptovalyutalar ekotizimida yangi tangalar yaratish va blokcheynlarni tekshirish va himoya qilish uchun ishlatiladigan jarayon. U butun dunyo bo'ylab blokcheynlarni - kriptovalyuta tranzaktsiyalarini hujjatlashtiradigan virtual daftarlarni tekshiradigan va himoya qiluvchi kompyuterlarning keng, markazlashmagan tarmoqlarini o'z ichiga oladi. Hisoblash quvvatiga hissa qo'shgani uchun tarmoqdagi kompyuterlar yangi tangalar bilan taqdirlanadi. Bu yaxshi aylanma amaliyot: maynerlar blokcheynni qo‘llab-quvvatlaydi va himoya qiladi, blokcheyn ularni tangalar bilan taqdirlaydi, tangalar maynerlarni blokcheynni qo‘llab-quvvatlashga rag‘batlantiradi.

Kripto-aktivlarning huquqiy maqomi bo’yicha xorij tajribasini tahlil qilsak. 2015-yil noyabr oyida Yevropa sudi Bitcoinni tovar emas, hech bo'lmaganda soliq nuqtai nazaridan valyuta (to‘lov vositasi) sifatida

[324] Коростелев М.А. Правовой режим электронных денег в гражданском законодательстве: дис. ... канд. юрид. наук. М., 2014. 218 с.

koʻrish kerakligi haqida qaror chiqardi. Shunday qilib, an'anaviy fiat valyutalari uchun Bitcoin sotib olish va sotish bilan bog'liq operatsiyalar qo'shilgan qiymat solig'iga tortildi. Norvegiya, Finlyandiya va Germaniyada kriptovalyuta kapital/daromad solig'i kabi soliqqa tortiladi. Avstriyada kriptovalyuta soliq organlari tomonidan nomoddiy aktiv sifatida qabul qilinadi va uni qazib olish operatsion faoliyat hisoblanadi. Qo'shma Shtatlarda kriptovalyutalar mulk hisoblanadi va bunday valyuta bilan barcha operatsiyalar soliqqa tortiladi.[325] Bir qator mamlakatlarda kriptovalyuta muomalasi taqiqlangan. Bularga Jazoir, Boliviya, Vetnam, Misr, Iroq, Marokash, Nepal, BAA, Pokiston kiradi. Bahrayn, Bangladesh, Xitoy, Kolumbiya, Dominikan Respublikasi, Indoneziya, Eron, Quvayt, Litva, Aomin, Ummon, Qatar, Saudiya Arabistoni, Tayvan va Tailandda kriptovalyutalarga yashirin taqiq amal qiladi.

Yevropa Ittifoqida kriptovalyuta Yevropa Markaziy banki tomonidan konvertatsiya qilinadigan, markazlashmagan virtual valyuta sifatida tavsiflangan. Hozircha kriptovalyutani toʻgʻridan-toʻgʻri tartibga soluvchi hujjat yoʻq, shuning uchun Yevropa banklariga kriptovalyutalarning qonuniy rejimi oʻrnatilgunga qadar ular bilan operatsiyalarni amalga oshirishdan bosh tortish tavsiya qilingan. Biroq, kriptovalyutalar bilan bog'liq ba'zi muammolarni hal qilishga urinishlar allaqachon boshlangan[326]. Jumladan, 2017-yilda Yevropa Ittifoqining jinoiy daromadlarni legallashtirishga qarshi direktivasiga kriptovalyutadan olingan daromadlarni legallashtirish va foydalanish xavfini kamaytirish maqsadida oʻzgartirishlar kiritildi.

Yevropa Ittifoqi kripto-aktivlar bozorini (Market of Cripto-Actives) tartibga solish kabi qonunlar orqali yagona me'yoriy-huquqiy bazani yaratish ustida ishlamoqda. MiCA reglamenti: Ushbu taklif etilayotgan reglament kripto-aktivlar uchun emissiya, savdo va saqlash xizmatlarini qamrab oluvchi keng qamrovli asos yaratishga qaratilgan. Pul yuvishga qarshi kurash (Anti Money Laundering): Yevropa Ittifoqi kriptovalyuta birjalari va hamyon provayderlarini oʻz ichiga olgan holda AML qoidalarini kengaytirdi va ulardan Mijozni bilish (Know Your Client) talablariga rioya qilishni talab qildi.

Ma'lumotlarni himoya qilish bo'yicha umumiy reglament (GDPR): GDPR kripto sektorida shaxsiy ma'lumotlar bilan ishlashga ta'sir qiladi va

[325] Кучеров И.И., Кҳаванова И.А. Налогове последствия исполъзования алътернативнйкҳ платезҳнйкҳ средств (теоретико-правове аспектй) [Тах Сонсекуэнсэс оф Усинг Альтернативе Меанс оф Паймент (Тҳеоретисал анд Легал Аспестс)] // Вестник Пермского Университета. Журидическиэ Науки - Перм Университй Ҳералд. Журидисал Ссиэнсэс. 2017. Иссуэ 35. Пп. 66-72.

[326] https://nplaw.ru/blog/detail/evropeyskiy-parlament-prinyal-zakonoproekty-o-regulirovanii-kriptovalyuty/

kompaniyalar foydalanuvchi ma'lumotlarini qanday boshqarishiga ta'sir qiladi.

Yevropa Ittifoqida kriptovalyuta Yevropa Markaziy banki tomonidan konvertatsiya qilinadigan, markazlashmagan virtual valyuta sifatida tasniflangan. Hozircha kriptovalyutani to‘g‘ridan-to‘g‘ri tartibga soluvchi hujjat yo‘q va shuning uchun Yevropa banklariga kriptovalyutalarning qonuniy rejimi o‘rnatilgunga qadar ular bilan operatsiyalarni amalga oshirishdan bosh tortish tavsiya qilindi. Biroq, kriptovalyutalar bilan bog'liq ba'zi muammolarni hal qilishga urinishlar allaqachon qilingan. Shunday qilib, 2017 yilda jinoiy daromadlarni legallashtirish maqsadida kriptovalyutadan foydalanish xavfini kamaytirishga qaratilgan Yevropa Ittifoqining Pul yuvishga qarshi direktivasiga o‘zgartirishlar kiritildi.

Bir qator davlatlar kriptovalyutalarga xususiy pul va to‘lov vositasi sifatida munosabatini shakllantirdilar. Bunday yondashuv, masalan, kriptovalyutalar bo'yicha qonunchilik shakllanish bosqichida bo'lgan Buyuk Britaniyada ishlab chiqilgan. Germaniyada kriptovalyuta (xususan Bitcoin) ham kapital sifatida soliqqa tortiladigan xususiy pul shakli sifatida tan olingan va Germaniya bank qonunchiligiga muvofiq Bitcoin hisob birligi sifatida tan olingan. Ispaniyada, 2014 yilda, qonunga ko'ra, kriptovalyuta qimor biznesiga nisbatan elektron to'lov vositasi sifatida tasniflangan va kriptovalyutalar bilan operatsiyalar qo'shilgan qiymat solig'iga tortilmasligi aniqlangan. Shveytsariyada kriptovalyuta chet el valyutalari bilan bir xil darajada va kriptovalyutalar bilan operatsiyalar qo'shilgan qiymat solig'iga tortilmaydi. Shu bilan birga, kriptovalyutalar bilan operatsiyalar jinoiy yo'l bilan olingan pullarni legallashtirishga qarshi kurashish bo'yicha qonun hujjatlari bilan tartibga solinadi va kriptovalyutalar bilan bir qator operatsiyalar uchun ularni amalga oshirish uchun litsenziya olish talablari mavjud. Estoniyada ham batafsil huquqiy tartibga solish mavjud emas va kriptovalyuta muqobil to'lov vositasi sifatida tan olingan[327].

Shveysariya o'zini kripto-do'st yurisdiksiya sifatida ko'rsatdi, aniq qoidalar va qo'llab-quvvatlovchi siyosatlarni ishlab chiqdi. Shveysariya moliya bozorini nazorat qilish organi kriptoaktivlar uchun batafsil ko'rsatmalar beradi va tokenlarni uchta toifaga ajratadi: to'lov tokenlari, foydali tokenlar va aktivlar tokenlari.

Kripto vodiysi deb nomlanuvchi Zug kantoni qulay soliq siyosati va qonuniy ravshanlik bilan blokcheyn startaplari uchun qulay muhitni taklif

[327] Егорова Мария Александровна Понятие и правовое регулирование криптовалюты в зарубежных странах // Большая Евразия: развитие, безопасность, сотрудничество. 2019. №2-1. URL: https://cyberleninka.ru/article/n/ponyatie-i-pravovoe-regulirovanie-kriptovalyuty-v-zarubezhnyh-stranah (дата обращения: 13.10.2024).

etadi. Bundan tashqari Shveytsariya banklarga kripto-aktivlarni moliya tizimiga integratsiyalashuvini kuchaytirib, kriptovalyuta kompaniyalariga xizmatlar taklif qilish imkonini beradi. Ayrim mamlakatlarda kriptovalyuta aktiv/mulk hisoblanadi. Misol uchun, Isroilda soliq xizmati loyihasiga ko'ra, kriptovalyuta soliqqa tortiladigan aktiv sifatida ko'rib chiqilishi kerak. Norvegiya ham kriptovalyutani soliqqa tortiladigan mulk deb hisoblaydi. Kriptovalyuta bir qancha afzalliklarga ega. Ilgari ma'lum bo'lganidek, kriptovalyutalarning asosiy xususiyatlarini aniqlashda ular markazsizlashtiriladi va shuning uchun ular bilan operatsiyalar o'ta xavfsizdir: kriptovalyutalarni egallab olish uchun tajovuzkorlar nafaqat bitta serverni, balki ko'plab kompyuterlarni buzishi kerak. Ushbu tizim shuningdek, davlat yoki banklar tomonidan tranzaktsiyalarni bloklashni imkonsiz qiladi, buning natijasida tranzaktsiyalarning katta qismi muvaffaqiyatli amalga oshiriladi. Transchegaraviy kriptovalyuta operatsiyalari fiat valyuta operatsiyalaridan farqli o'laroq, bir zumda amalga oshiriladi. Masalan, Bitkoin kabi kriptovalyutaning yana bir afzalligi shundaki, uning inflyatsiyasi mutlaqo prognoz qilinishi mumkin: aytilishicha, jami 21 million bitkoin chiqariladi va ayni paytda muomalada allaqachon 16,5 million bitkoin mavjud. Shuningdek, kriptovalyutaning yana bir xususiyati uning anonimligidir[328].

Butun dunyoda kriptovalyutaning tabiati va huquqiy maqomini aniqlashga yondashuv tubdan farq qiladi, degan xulosaga kelishimiz mumkin: kriptovalyutalar pul, mulk sifatida e'tirof etiladi, yoki ular butunlay taqiqlanadi va aksincha, hukumat emissiyasi uchun rejalashtirilgan. Muayyan davlat uchun qaysi yondashuv eng to'g'ri bo'lishini aniqlash juda qiyin va rasmiylar kriptovalyutaning barcha afzalliklari va kamchiliklarini hisobga olgan holda tartibga solishni tanlashda murosaga kelishga harakat qilmoqdalar.

Jahon amaliyotida kriptovalyutani qonuniy to'lov vositasi sifatida tan olish istiqbollari allaqachon mavjud bo'lganligi sababli, nazariy jihatdan bu holda kriptovalyutani valyuta qiymati sifatida tasniflash mumkin bo'ladi. Biroq, hozirgi vaqtda dunyoning hech bir davlatida bunday yondashuv ishlab chiqilmagan va ba'zi axborot resurslari kriptovalyuta hech qachon qonuniy to'lov vositasi sifatida tan olinmasligini ta'kidlaydi.

Bitcoinning dastlabki yillarida oddiy uy kompyuteriga ega bo'lgan har bir kishi mayning bilan shug’ullanishi mumkin edi. Ammo blokcheyn

[328] Егорова Мария Александровна Понятие и правовое регулирование криптовалюты в зарубежных странах // Большая Евразия: развитие, безопасность, сотрудничество. 2019. №2-1. URL: https://cyberleninka.ru/article/n/ponyatie-i-pravovoe-regulirovanie-kriptovalyuty-v-zarubezhnyh-stranah (дата обращения: 13.10.2024).

o'sishi bilan uni saqlash uchun zarur bo'lgan hisoblash quvvati oshdi. Ko'p jihatdan 2024 yilda bitta bitkoinni mayninggi uchun zarur bo'lgan hisoblash quvvati 2009-yilga (birinchi bitkoin bloklari qazib olingan vaqtga) qaraganda ancha yuqori - taxminan 6 baravar ko'p. Bu so’nggi 15 yil ichida qazib olish qiyinligining eksponensial o'sishi tufaylidir. Natijada, bitkoin qazib olish ko'p yillar davomida havaskorlar uchun odatda foydali bo'lmagan. Deyarli barcha mayning faoliyati endi ixtisoslashgan kompaniyalar yoki resurslarini birlashtirgan odamlar guruhlari tomonidan amalga oshiriladi. Ixtisoslashgan kompyuterlar har bir yangi bitkoin tranzaksiyasini tekshirish va qayd etish hamda blokcheyn xavfsizligini ta’minlash uchun zarur hisob-kitoblarni amalga oshiradi. Blokcheyn tekshiruvi katta hajmdagi hisoblash quvvatini talab qiladi, uni maynerlar ixtiyoriy ravishda taqdim etadilar.

Bitcoin qazib olish katta ma'lumotlar markazini boshqarishga o'xshaydi. Kompaniyalar mayning uskunalarini sotib oladi va uni ishlatish (va saqlash) uchun zarur bo'lgan elektr energiyasini to'laydi. Buning foydali bo'lishi uchun olingan tangalarning qiymati ushbu tangalarni qazib olish narxidan yuqori bo'lishi kerak. Tarmoqdagi har bir kompyuter “xesh” deb nomlanuvchi 64 xonali o‘n oltilik sonni birinchi bo‘lib taxmin qilishga intiladi. Kompyuter qanchalik tez taxmin qila olsa, mayner mukofot olish ehtimoli shunchalik yuqori bo'ladi. G'olib blokcheyn daftarini barcha yangi tasdiqlangan tranzaksiyalar bilan yangilaydi – shu bilan zanjirga barcha tranzaksiyalarni o'z ichiga olgan yangi tasdiqlangan "blok" ni qo'shadi – va yangi zarb qilingan bitkoinning oldindan belgilangan miqdoriga ega bo'ladi. (O'rtacha, bu har o'n daqiqada sodir bo'ladi.) 2024-yil aprel holatiga ko'ra, mukofot har bir blok uchun 3,125 bitkoinni tashkil qiladi va har bir yangi bitkoin qazib olish qiyinligi oshgani sayin, boshqa bitkoinlar qazib olinmaguncha mukofot kamayib boraveradi. Bitkoinlarning maksimal mumkin bo'lgan soni - 21 million. Oxirgi blok nazariy jihatdan 2140-yilda shakllanadi. Shu paytdan boshlab, maynerlar endi mukofot sifatida yangi zarb qilingan bitkoinlarga tayanmaydilar, aksincha, tranzaksiyalarni amalga oshirish uchun olinadigan to'lovlarga tayanadilar. Yangi tangalarni muomalaga chiqarishdan tashqari, mayning Bitcoin (va boshqa ko'plab kriptovalyutalar) xavfsizligini ta'minlashda muhim ahamiyatga ega. U blokcheynni tekshiradi va himoya qiladi, bu kriptovalyutalarga uchinchi tomon nazoratiga muhtoj bo'lmasdan, markazlashtirilmagan tarmoq sifatida ishlashga imkon beradi. Va bu maynerlar uchun tarmoqqa o'z

hisoblash quvvatlarini qo'shishni talab qiladi[329]. Bir qator mamlakatlarda kriptovalyuta muomalasi taqiqlangan. Bularga Jazoir, Boliviya, Vyetnam, Misr, Iroq, Marokash, Nepal, BAA, Pokiston kiradi. Bahrayn, Bangladesh, Xitoy, Kolumbiya, Dominikan Respublikasi, Indoneziya, Eron, Quvayt, Litva, O'mon, Qatar, Saudiya Arabistoni, Tayvan va Tailandda kriptovalyutalarga yashirin taqiq amal qiladi.

Amerika Qo'shma Shtatlarida Bitcoinni huquqiy tartibga solishning yagona kontseptsiyasi aniqlanmagan. 2014 yilda Nyu-York moliyaviy xizmatlar departamenti kriptovalyutalar mavzusiga murojaat qilib, "raqamli valyuta" va "elektron pul" tushunchalaridan foydalangan. Bir qator shtatlarda (Vashington, Nyu-York, Janubiy Karolina, Jorjiya, Pensilvaniya, Nyu-Xempshir, Nyu-Meksiko), kriptovalyuta aylanishiga ruxsat beriladi; boshqa shtatlarda bu masala hal qilinmagan. Kanadada kriptovalyutalarni barter operatsiyalari qoidalariga muvofiq to'lash uchun foydalanishga ruxsat beriladi, ular qonuniy to'lov vositasi sifatida tan olinmaydi; Kanada daromad agentligi kriptovalyutani soliqqa tortish uchun raqamli tovar sifatida tavsiflaydi.

Amerika Qo'shma Shtatlarida bitcoinni huquqiy tartibga solishning yagona konsepsiyasi aniqlanmagan. 2014-yilda Nyu-York moliyaviy xizmatlar departamenti kriptovalyutalar mavzusiga murojaat qilib, "raqamli valyuta" va "elektron pul" tushunchalaridan foydalangan. Bir qator shtatlarda (Vashington, Nyu-York, Janubiy Karolina, Jorjiya, Pensilvaniya, Nyu-Xempshir, Nyu-Meksiko) kriptovalyuta muomalasiga ruxsat berilgan, boshqa shtatlarda esa bu masala hal etilmagan. Amerika Qo'shma Shtatlari kripto-aktivlar va qazib olish bo'yicha tarqoq tartibga soluvchi yondashuvga ega, turli agentliklar bozorning turli jihatlarini nazorat qiladi[330].

Qimmatli qog'ozlar va birja komissiyasi (SEC) – SEC dastlabki tanga takliflarini (ICO) tartibga soladi va ba'zi kripto-aktivlar qimmatli qog'ozlar sifatida tasniflanishi yoki tasniflanmasligini aniqlaydi.

Tovar fyucherslari savdo komissiyasi (CFTC) – CFTC Bitcoin va boshqa kriptovalyutalarni tovar sifatida tasniflaydi, shu bilan fyuchers va derivativlar savdosini nazorat qiladi. Ichki daromad xizmati (IRS) – IRS kriptovalyutalarni soliq maqsadlarida mulk sifatida ko'radi, tranzaktsiyalar va mayning faoliyati to'g'risida hisobot berishni talab

[329] https://www.coinbase.com/ru/learn/crypto-basics/what-is-mining#:~:text=Mining%20is%20the%20process%20that,ledgers%20that%20document%20cryptocurrency%20transactions

[330] Егорова Мария Александровна Понятие и правовое регулирование криптовалюты в зарубежных странах // Большая Евразия: развитие, безопасность, сотрудничество. 2019. №2-1. URL: https://cyberleninka.ru/article/n/ponyatie-i-pravovoe-regulirovanie-kriptovalyuty-v-zarubezhnyh-stranah (дата обращения: 13.10.2024).

qiladi. Shtatlar qoidalari – Nyu-York kabi shtatlar kriptovalyuta bizneslarini nazorat qilish uchun BitLicense kabi maxsus qoidalarni amalga oshirdilar.

Kanadada kriptovalyuta tovar va xizmatlar uchun to'lovni amalga oshirish uchun ruxsat etiladi, u qonuniy to'lov vositasi sifatida tan olinmaydi; Kanada daromad agentligi kriptovalyutani soliqqa tortish uchun raqamli tovar sifatida tavsiflaydi. Bir qator davlatlar kriptovalyutalarga xususiy pul va to‘lov vositasi sifatida munosabatini shakllantirdilar. Bunday yondashuv, masalan, kriptovalyutalar bo'yicha qonunchilik shakllanish bosqichida bo'lgan Buyuk Britaniyada ishlab chiqilgan. Germaniyada kriptovalyuta (xususan Bitcoin) ham kapital sifatida soliqqa tortiladigan xususiy pul shakli sifatida tan olingan va Germaniya bank qonunchiligiga muvofiq Bitcoin hisob birligi sifatida tan olingan. Ispaniyada 2014-yilda kriptovalyuta qonuniy ravishda qimor biznesiga nisbatan elektron to'lov vositasi sifatida tasniflangan. Kriptovalyutalar bilan operatsiyalar qo‘shilgan qiymat solig‘iga tortilmasligi aniqlandi. Shveysariyada kriptovalyutalar xorijiy valyutalar bilan bir xil darajada va kriptovalyutalar bilan operatsiyalar qo'shilgan qiymat solig'iga tortilmaydi. Shu bilan birga, kriptovalyutalar bilan operatsiyalar **jinoiy yo'l bilan olingan pullarni legallashtirishga qarshi kurashish bo'yicha qonun hujjatlari bilan tartibga solinadi.** Kriptovalyutalar bilan bir qator operatsiyalarni amalga oshirish uchun litsenziya olish talablari mavjud. **Estoniyada** ham batafsil huquqiy tartibga solish mavjud emas va kriptovalyuta muqobil to'lov vositasi sifatida tan olingan. Isroilda, soliq xizmati loyihasiga ko'ra, kriptovalyuta soliqqa tortiladigan aktiv sifatida ko'rib chiqilishi kerak. Norvegiya ham kriptovalyutani soliqqa tortiladigan mulk deb hisoblaydi[331].

Xitoy kriptovalyutani tartibga solishga qat'iy yondashdi va kripto bilan bog'liq ko'plab faoliyatlarni samarali ravishda taqiqladi. Xitoy hukumati moliyaviy beqarorlik va firibgarlikning oldini olish uchun kriptovalyuta almashinuvi va ICO-larni taqiqladi. Xitoy atrof-muhit muammolari va moliyaviy xavflarni bahona qilib, mahalliy **mayning** operatsiyalarini to'xtatishga o'tdi. Xususiy kriptovalyutalarga qarshi kurashga qaramasdan, Xitoy o'zining markaziy banki raqamli valyutasini – Digital Yuanni faol ravishda rivojlantirmoqda.

Yaponiyada kriptovalyutalardan to‘lov vositasi sifatida foydalanish mumkin, kriptovalyutalarni sotib olish va sotish uchun platformalar

[331] Егорова Мария Александровна Понятие и правовое регулирование криптовалюты в зарубежных странах // Большая Евразия: развитие, безопасность, сотрудничество. 2019. №2-1. URL: https://cyberleninka.ru/article/n/ponyatie-i-pravovoe-regulirovanie-kriptovalyuty-v-zarubezhnyh-stranah (дата обращения: 13.10.2024).

faoliyati litsenziyalanadi. Yaponiya kriptovalyutalarni qonuniy to'lov vositasi sifatida tan olgan va yaxshi belgilangan me'yoriy-huquqiy bazaga ega bo'lgan kam sonli davlatlardan biridir. To'lov xizmatlari to'g'risidagi qonun –kriptovalyuta almashinuvini tartibga soladi, bu ularni Moliyaviy xizmatlar agentligida ro'yxatdan o'tishni va qat'iy operatsion standartlarga rioya qilishni talab qiladi.[332]

Yaponiyada kriptovalyutalardan to‘lov vositasi sifatida foydalanish mumkin, kriptovalyutani sotib olish va sotish bo‘yicha platformalar faoliyati litsenziyalangan. Moliyaviy vositalar va birja qonuni – kripto derivativlari savdosini qamrab oladi va uni an'anaviy moliyaviy vositalar bilan bir xil tartibga soluvchi soyabon ostiga olib keladi. Yaponiya iste'molchilarni himoya qilish bo'yicha chora-tadbirlarni amalga oshirdi, shu jumladan ayirboshlash uchun kapital talablari va mijozlar va kompaniya aktivlarini ajratish. Singapur me'yoriy hujjatlarga muvofiqlikni ta'minlash bilan birga innovatsiyalarni qo'llab-quvvatlagan holda muvozanatli yondashuvni amalga oshiradi. To‘lov xizmatlari to‘g‘risidagi qonun – to‘lov tizimlari, jumladan kriptovalyuta almashinuvi va hamyon provayderlari uchun litsenziyalar olish va AML/KYC qoidalariga rioya qilishni talab qiluvchi me’yoriy asosni taqdim etadi.

Singapur Monetar Authority (MAS) – kripto sanoati bilan faol hamkorlik qiladi, ko'rsatmalar chiqaradi va mas'uliyatli rivojlanishni rag'batlantirish uchun manfaatdor tomonlar bilan hamkorlik qiladi. Singapurda startaplarga kripto sektorining o‘sishiga yordam beruvchi sinov muhiti qo‘llanilib, nazorat ostidagi muhitda innovatsion mahsulotlarni sinab ko‘rish imkoni yaratilgan. Yaponiya va Shveysariya kabi davlatlar aniq me'yoriy-huquqiy bazani yaratish uchun faol qadamlar qo'ymoqda,

Amerika Qo'shma Shtatlari esa reaktiv yondashuvga ega bo’lib, bozor o'zgarishlariga javoban normalar ishlab chiqadi. Xitoy esa kripto-aktivlar sanoatining o'sishini cheklash choralarini qo’llaydi. Singapur va Shveysariya kabi yurisdiksiyalar ruxsat beruvchi bo’lib, innovatsiyalarni rag'batlantiradi, Proaktiv va ruxsat beruvchi tartibga solish muhiti bozor o'sishiga yordam beradi, biznes va investorlarni jalb qiladi. Yaponiya va Shveysariya o'zlarining kripto sektorlarida sezilarli rivojlanishga erishdilar. Singapurda tartibga soluvchi sandboxlar va qo'llab-quvvatlovchi siyosat kompaniyalarga tartibga solinadigan doirada tajriba o'tkazishga imkon berish orqali innovatsiyalarni rag'batlantiradi.

Yurisdiksiyalar bo'ylab nomuvofiq qoidalar tartibga soluvchi arbitrajga olib kelishi mumkin, bu yerda korxonalar qulayroq muhitga

[332] Япония признала криптовалюты законным платежным средством. // Российская газета [сайт]. URL: https://rg.ru/

ko'chib o'tadi, bu esa tartibga solish harakatlariga putur yetkazishi mumkin. Blokcheyn texnologiyasining tez rivojlanayotgan tabiati tartibga soluvchilar uchun ishlanmalar bilan hamqadam bo'lishni talab qiladi va tegishli qoidalarni ishlab chiqishda qiyinchiliklar tug'diradi. Innovatsiyalarni qo'llab-quvvatlash va iste'molchilarni himoya qilish va moliyaviy barqarorlik o'rtasidagi muvozanatni saqlash butun dunyo bo'ylab tartibga soluvchilar uchun asosiy muammo bo'lib qolmoqda.

Qiyosiy tahlil shuni ko'rsatadiki, proaktiv va ruxsat beruvchi tartibga solish yondashuvlari bozor o'sishi va innovatsiyalarni qo'llab-quvvatlaydi, cheklovchi choralar esa rivojlanishni to'xtatib qo'yishi mumkin. Global kripto bozori rivojlanishda davom etar ekan, xalqaro hamkorlik va qoidalarni uyg'unlashtirish muammolarni hal qilish va sanoatning barqaror o'sishini ta'minlash uchun hal qiluvchi ahamiyatga ega bo'ladi.

Kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzganlik uchun dastlab ma’muriy javobgarlik, agar bir yil ichida yana sodir etilsa jinoiy javobgarlik vujudga keladi. Kiritilgan oʻzgartirishga koʻra, kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzish Ma’muriy javobgarlik toʻgʻrisidagi kodeksning 1554-moddasi bilan javobgarlikka tortiladi va mazkur huquqbuzarlikni sodir etish kripto-aktivlarni hamda mazkur huquqbuzarliklarni sodir etish qurollarini musodara qilib, oʻn besh sutkagacha ma’muriy qamoqqa olishga yoki ushbu Kodeksga muvofiq oʻziga nisbatan ma’muriy qamoq qoʻllanilishi mumkin boʻlmagan shaxslarga bazaviy hisoblash miqdorining yigirma baravaridan oʻttiz baravarigacha miqdorda jarima solishga sabab boʻladi. Kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari tomonidan anonim kripto-aktivlar bilan operatsiyalarni amalga oshirish esa, mansabdor shaxslarga bazaviy hisoblash miqdorining oʻttiz baravaridan qirq baravarigacha miqdorda jarima solishga sabab boʻladi.

Shuningdek, mazkur qilmishni ma’muriy javobgarlikka tortilgan keyin shaxs tomonidan bir yil ichida takroran sodir etilishi jinoiy javobgarlikni keltirib chiqaradi. Jinoyat kodeksining 2788-moddasiga koʻra, Kripto-aktivlarni qonunga xilof ravishda olish, oʻtkazish yoki ayirboshlash, belgilangan tartibda litsenziya olmasdan kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari faoliyatini amalga oshirish yoxud kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari tomonidan anonim kripto-aktivlar bilan operatsiyalarni amalga oshirish shunday harakatlar uchun ma’muriy jazo qoʻllanilganidan keyin sodir etilgan boʻlsa, bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoki ikki yildan uch yilgacha axloq tuzatish ishlari yoxud bir yilgacha ozodlikni cheklash yoki bir yilgacha ozodlikdan mahrum

qilish bilan jazolanadi. O‘zbekiston Respublikasi Istiqbolli loyihalar milliy agentligi direktorining 2022-yil 14-iyuldagi 32-son buyrug‘iga 1-ilova bo‘lgan «Kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari faoliyatini litsenziyalash tartibi to‘g‘risida»gi Nizomga ko‘ra Kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari deganda, jismoniy va yuridik shaxslarga, shu jumladan ularning nomidan kripto-aktivlarni sotib olish, sotish, ayirboshlash, saqlash, chiqarish, joylashtirish va boshqarish bo‘yicha xizmatlarni ko‘rsatuvchi O‘zbekiston Respublikasining rezidentlari bo‘lgan yuridik shaxslar tushuniladi. Xizmatlar provayderlari faoliyatini amalga oshirish uchun litsenziya faqat O‘zbekiston Respublikasining rezidentlari — yuridik shaxslariga beriladi. Xizmatlar provayderlari faoliyatining turlari quyidagilardan iborat: – kripto-birja; – mayning-pul; – kripto-depozitariy; – kripto-do‘kon.

Xizmatlar provayderlari faoliyatining har bir turi bo‘yicha alohida litsenziya beriladi. Bundan tashqari, JKning 2788-moddasining 2-qismida kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzganlik uchun og‘irroq jazo belgilangan bo‘lib, agar yuqorida keltirilgan harakatlar a) takroran yoki xavfli retsidivist tomonidan; b) ko‘p miqdorda; v) bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilgan bo‘lsa, bazaviy hisoblash miqdorining uch yuz baravaridan to‘rt yuz baravarigacha miqdorda jarima yoki uch yilgacha ozodlikni cheklash yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi. Shuningdek, JKning 2788-moddasining 3-qismiga ko‘ra Kripto-aktivlarni qonunga xilof ravishda olish, o‘tkazish yoki ayirboshlash, belgilangan tartibda litsenziya olmasdan kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari faoliyatini amalga oshirish yoxud kripto-aktivlar aylanmasi sohasidagi xizmatlar provayderlari tomonidan anonim kripto-aktivlar bilan operatsiyalarni amalga oshirish juda ko‘p miqdorda; xizmat mavqeyidan foydalangan holda; uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilgan bo‘lsa, uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Shuni alohida ta’kidlash lozimki, jinoyat qonunchiligimizda yuqoridagi qilmish bilan bog‘liq rag‘batlantiruvchi norma ham mavjud bo‘lib, unga ko‘ra tayyorgarlik ko‘rilayotgan yoki sodir etilayotgan jinoyat haqida o‘z ixtiyori bilan arz qilgan va uni ochishga faol yordam bergan shaxs javobgarlikka tortilmaydi.

AMERIKA QO‘SHMA SHTATLARI, XITOY VA KOREYA MISOLIDA SUN’IY INTELLEKTDAN FOYDALANISH MASALALARI

Abdufattoyev Yo‘ldoshali Farxodjon O‘g‘li
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi magistraturasi tinglovchisi

Sun’iy intellekt muayyan vazifalarni bajarishda inson xatti-harakatiga taqlid qilishga qodir bo‘lgan tizim yoki texnologiya bo‘lib, olingan ma’lumotlardan foydalanib asta-sekin mukammallashib boradi. Umuman olganda sun’iy intellekt format ham, funksiya ham emas, balki bu jarayon bo‘lib, ma’lumotlarni yig‘ish, tahlil qilish kabilarni o‘z ichiga oladi.

Sun’iy intellekt zamonaviy huquqiy tizimda o‘ta muhim va ko‘p qirrali rol o‘ynaydi. Uning ta’siri va imkoniyatlari turli jabhalarda o‘z aksini topadi, bu esa huquqiy sohadagi amaliyot va tadqiqotlarda yangi imkoniyatlar va chegaralarni ochib beradi.

Sun’iy intellekt unga ko‘maklashuvchi dasturlar orqali huquqiy hujjatlarni tezkor va samarali ravishda tahlil qilish imkoniyatini yaratadi. Masalan, hujjatlarning avtomatik indeksatsiyasi va tegishli qarorlar yoki qonunlar bilan bog‘liq muhokamalarni topish osonlashdi. Bu normativ-huquqiy hujjatlarni tayyorlash jarayonini sezilarli darajada tezlashtiradi va xato ehtimolini kamaytiradi.

Ayrim yurisdiksiyalarda sun’iy intellekt algoritmlari ayrim turdagi huquqiy masalalarda qaror qabul qilish jarayoniga kiritilgan. Masalan, shartnoma shartlarini avtomatik baholash yoki kredit berishda qarz oluvchining qarzga qaytarish imkoniyatlarini tahlil qilish shular jumlasidandir.

Hozirgi kunda sud va huquqni muhofaza qilish faoliyatida sun’iy intellekt imkoniyatlaridan foydalanish masalasi har kungidan ko‘ra dolzarb bo‘lib kelmoqda. Sun’iy intellekt imkoniyatlaridan sud ishlarini yuritish jarayonlarini avtomatlashtirishda, shu jumladan, ayrim turdagi ishlarning dastlabki tahlilini o‘tkazishda foydalanilishi mumkin. Bu sudyalarga va prokurorlarga ishlar bo‘yicha ma’lumotlarni tizimlashtirish va tezkor baholashga yordam beradi.

Darhaqiqat, sudyalarning ish yuklamasining ko‘pligini hozirgi kunda ham sud tizimidagi og‘riqli muammo sifatida ko‘rsatish mumkin. Binobarin, mamlakatimiz aholisi soni kundan-kunga ko‘paymoqda. Sudyalarning shtatlar soni esa aholining o‘sish su’ratiga qarab mutanosib ravishda belgilanmagan. Statistik ma’lumotlarga qaraganda, birgina 2022

yilda jinoyat ishlari bo‘yicha birinchi instansiya sudida 58.697 ta jinoyat ishi, 539.686 ta ma’muriy huquqbuzarlik to‘g‘risidagi ish ko‘rib chiqilgan. Shuningdek, fuqarolik ishlari bo‘yicha sudlar 562.304 ta, iqtisodiy sudlar 277.865 ta, ma’muriy sudlar 15.347 ta ishni ko‘rib chiqqan. Ushbu raqamlarni o‘rtacha oylik ish hajmiga nisbatan hisoblaydigan bo‘lsak, jinoyat ishlari bo‘yicha tuman, shahar sudining bir sudyasi bir oyda 181 ta ishni, fuqarolik ishlari bo‘yicha tumanlararo, tuman, shahar sudining sudyasi 269 ta, tumanlararo, tuman, shahar iqtisodiy sudining sudyasi esa 163 ta ishni ko‘rib chiqishiga to‘g‘ri kelmoqda.

Xorijiy davlatlar (AQSH, Xitoy, Kanada)ning hamda Yevropa Ittifoqi qonunchili tajribasidan kelib chiqqan holda O‘zbekistonda ham “Sun’iy intellekt to‘g‘risida”gi qonunni qabul qilish va mazkur Qonunda quyidagi asosiy elementlar o‘z aksini topishi haqida xulosa qilish mumkin:

1. Xavflarni tasniflash. Sun’iy intellekt (SI) to‘g‘risidagi qonunlar SI tizimlarini ular ko‘rsatishi mumkin bo‘lgan xavf darajasiga ko‘ra tasniflashi lozim. Shu o‘rinda sog‘liqni saqlash, transport, sud va huquq-tartibot organlarida SIdan foydalanadigan tizimlar yuqori xavfli tizim sifatida tasniflanadi. O‘rta va past xavfli tizimlarga nisbatan kamroq talablar qo‘yilsa-da, ular asosan shaffoflik va xavfsizlik standartlariga javob berishi talab etiladi.

2. Shaffoflik va tushunarlilik. SI to‘g‘risidagi qonunning asosiy qoidalaridan biri algoritmlarning tushunarliligi va shaffofligiga bo‘lgan talabdir. Foydalanuvchilar va nazorat organlari SI qanday qarorlar qabul qilayotganini tushunishlari kerak.

3. Etika va diskriminatsiyaga yo‘l qo‘ymaslik. Ko‘plab mamlakatlar kamsitish, ayirmachilikning oldini olish va adolatni ta’minlash maqsadida SI etikasi to‘g‘risidagi majburiy qoidalarni o‘z qonunlariga kiritish chorasini ko‘rmoqdalar. Bu o‘z navbatida algoritmlarning irq, jins, din yoki boshqa belgilar bo‘yicha har qanday kamsitishlarga yo‘l qo‘ymaslik asosida ishlab chiqilishini o‘z ichiga oladi.

4. Ishlab chiquvchilar va foydalanuvchilarning javobgarligi. Qonunchilik SIdan foydalanish uchun javobgarlik ishlab chiquvchilar, operatorlar va oxirgi foydalanuvchilar o‘rtasida aniq taqsimlanishini talab qiladi.

5. Xalqaro hamkorlik. SIni tartibga solishning muvofiqlash-tirilgan standartlarini ishlab chiqishda ushbu prinsip muhim rol o‘ynaydi.

Sun’iy intellekt to‘g‘risidagi qonunni qabul qilish zarurati jamiyat va davlat hayotida zamonaviy texnologiyalarning tez sur’atlar bilan rivojlanishi, ularning turli hayot sohalariga ta’siri va fuqarolarning huquqlari va qonuniy manfaatlarini himoya qilish zaruriyati bilan bog‘liq

bo‘ladi. SI zamonaviy iqtisodiyot, huquqiy tizim, sog‘liqni saqlash, transport va boshqa sohalarning tobora muhim qismiga aylanmoqda. Ammo aniq me’yoriy hujjatlarning yo‘qligi inson huquqlarining buzilishi, texnologiyalardan noetik foydalanilishi va ijtimoiy tengsizlikning yuzaga kelishi kabi bir qator salbiy oqibatlarga olib kelishi mumkin.

Sun’iy intellekt to‘g‘risidagi qonunni qabul qilish uchun zarur bo‘lgan asosiy sabablar quyidagilardan iborat:

Inson huquq va erkinliklarini himoya qilish. SI tizimlari shaxsiy hayot va inson huquqlariga katta ta’sir o‘tkazishi mumkin. Masalan, yuzni tanib olish tizimlari shaxsiy hayot daxlsizligi huquqini buzishi, qarorlar qabul qilish algoritmlari esa kamsitishga sabab bo‘lishi mumkin. SI to‘g‘risidagi qonun fuqarolarni bunday xavflardan himoya qilish va asosiy huquqlarini himoya qilish uchun zarurdir. Jumladan, SI tizimlari tomonidan katta hajmdagi ma’lumotlarni yig‘ish va qayta ishlash tizimlari shaxsiy huquqqa oid ma’lumotning sizib chiqishi yoki uning qonunga xilof ravishda foydalanilishini oldini olish uchun nazorat qilinishi kerak.

Nazoratsiz SI tizimlari kredit berish yoki sud ishlarini yuritish kabi sohalarda xato qarorlar qabul qilishi mumkin. Qonun o‘z navbatida algoritmlar orqali kamsitishning oldini olish choralarini nazarda tutishi kerak.

Qolaversa, SI jamiyatning etik normalariga katta ta’sir ko‘rsatishi mumkin. Shunday ekan, SI jamiyat manfaatlarini himoya qiladigan va etik standartlarga rioya qilinishini kafolatlaydigan qonunlar juda zarur. Bu kabi Qonun SIning jamiyat uchun ma’naviy jihatdan qabul qilinmaydigan qarorlar qabul qilinishiga yo‘l qo‘ymaslikka yordam beradi.

SI tizimlari jamiyat uchun o‘z faoliyatining ijtimoiy oqibatlarini hisobga olgan holda ishlab chiqilishi va foydalanilishi kerak.

SI bilan bog‘liq asosiy muammolardan biri bu “qora quti” algoritmlari bo‘lib, unda foydalanuvchilar va hatto ishlab chiquvchilar ham tizim qanday qarorlar qabul qilishini tushuntirib bera olmaydi. SI to‘g‘risidagi qonun oshkoralikni ta’minlash uchun juda muhim.

SI tizimlari foydalanuvchilari uchun, ayniqsa, tibbiyot yoki sud tizimi kabi muhim sohalarda qarorlar qabul qilish sabablarini tushunishlari borasida imkoniyatga ega bo‘lishi kerak.

Davlat idoralari va kompaniyalar SI tizimlarining ishlash prinsiplari haqida axborot berishlari lozim, bu ishonchsizlikni oldini olish va jamoat nazoratini ta’minlashga xizmat qiladi.

Aniq qonunlarning mavjud bo‘lmasligi SI tizimlari orqali sodir etilgan xatolar yoki shu orqali yetkazilgan zarar uchun kim javobgar ekanini noaniq bo‘lishiga olib keladi. Shu sababli SI to‘g‘risidagi qonunda

ishlab chiquvchilar va foydalanuvchilarning javobgarligi aniq belgilashi kerak. Bunda SIdan foydalanishda xatolar yoki suiiste'molliklar natijasida jabrlanganlar kompensatsiya olishlari mumkin bo‘ladi.

Qonunchilik SI tizimlarining, ayniqsa, muhim infratuzilmalarda qo‘llanilayotgan tizimlar xavfsizligini ta'minlash bo‘yicha talablarni belgilashda ham muhim ahamiyat kasb etadi.

SI bu global texnologiya bo‘lib, xalqaro tartibga solish va huquqiy normalarning muvofiqlashtirilishini talab qiladi. Muvofiqlashtiril-magan qonunlarsiz davlatlar SIning chegaralararo faoliyati bilan bog‘liq muammolarga duch kelishi mumkin. Qolaversa, milliy qonunchilik xalqaro normalar bilan muvofiqlashtirilishi kerak, shunda huquqiy bo‘shliqlardan qochish va SIni samarali boshqarish mumkin bo‘ladi.

Sun'iy intellekt haqidagi qonunning tuzilishi, odatda, SIdan foydalanishni tartibga solishga qaratilgan turli boblardan iborat bo‘lib, mamlakatlar va ularning huquqiy tizimiga qarab o‘zgarishi va turlicha bo‘lishi mumkin. Biroq asosiy elementlar umumiy bo‘lib qoladi. Xalqaro tendensiyalar va Yevropa Ittifoqi sun'iy intellekt to‘g‘risidagi qonunni (Artificial Intelligence Act) kabi loyihalar asosida SI haqidagi qonunning tuzilishini taxminiy strukturasi quyidagicha bo‘lishi mumkin:

Kirish.

Qonunning maqsadi: Qonunning maqsad va vazifalarini belgilash, masalan, xavfsizlik, shaffoflik va SIdan foydalanish uchun javobgarlikni ta'minlash, inson huquqlarini himoya qilish va SI sohasidagi innovatsiyalarni qo‘llab-quvvatlash.

Qo‘llanish sohasi: Qonun qaysi SI tizimlariga nissbatan tatbiq etilishini aniqlash (masalan, mamlakat hududida qo‘llaniladigan barcha SI tizimlari yoki faqat yuqori xavfli tizimlar).

Ta'riflar: Qonunda ishlatiladigan tushunchalar, jumladan, “sun'iy intellekt”, “algoritm”, “yuqori xavf”, “o‘rta va past xavf”, “ishlab chiquvchi”, “foydalanuvchi” va boshqalarning ta'rifi.

“Sun'iy intellekt to‘g‘risida”gi qonun zamonaviy huquqiy makonda yuz berayotgan bahs-munozaralarning eng muhim mavzularidan biridir. Bunday qonunni ishlab chiqish xavfsizlikni ta'minlash, inson huquqlarini himoya qilish va innovatsiyalarni rag‘batlantirish maqsadida sun'iy intellekt (SI)dan foydalanishni huquqiy tartibga solish zaruriyati bilan bog‘liqdir. Ko‘plab mamlakatlar va xalqaro tashkilotlar SIni nazorat qilishga qaratilgan qonun hujjatlarini ishlab chiqmoqdalar, ayrimlarida bu kabi qonun amal qiladi.

Xalqaro darajada sun'iy intellektni huquqiy tartibga solish borasida shuni ta'kidlash kerakki, hozida Yevropa Ittifoqi sun'iy intellekt

to‘g‘risidagi qonunni (Artificial Intelligence Act) ishlab chiqmoqda. SIni tartibga soluvchi birinchi kompleks qonunchilik hujjati sifatda ushbu qonunning asosiy tamoyillari sifatida quyidagilar nazarda tutilmoqda:

Qonun SI tizimlarini xavf darajasiga qarab quyidagi toifalarga ajratishni taklif qiladi:

- yuqori xavfli tizim;
- cheklangan xavfli tizim;
- minimal xavfli tizim.

Yuqori xavfli SI tizimi qat’iy talablarga javob berishi va majburiy sertifikatlanishi talab etiladi. Shuningdek, Qonunda asosiy e’tibor kamsitish, ayirmachilikning oldini olish va inson huquqlarini himoya qilishga qaratilgan. Masalan, jamoat joylarida biometriya orqali shaxsni aniqlash uchun SIdan foydalanish cheklanadi yoki taqiqlanadi. SI ishlab chiquvchilari va foydalanuvchilari xatolar va SI tizimlaridan foydalanish natijasida yuzaga keladigan zarar uchun to‘liq javobgar bo‘ladi.

Iqtisodiy hamkorlik va taraqqiyot tashkiloti (OESR) 2019 yilda SI prinsiplarini ishlab chiqdi va bu ko‘plab mamlakatlarda SIni tartibga solish uchun asos bo‘ldi. Bu prinsiplar innovatsiya va o‘sishni inson huquqlarini hurmat qilgan holda ta’minlash; SI tizimlari uchun javobgarlik va shaffoflikni ta’minlash; jamiyatga SI yetkazadigan zararlar va xavflarning oldini olishn tashkil qiladi.

Sun’iy intellekt bo‘yicha xorijiy davlatlar qonunchilik tajribasiga to‘xtaladigan bo‘lsak, masalan, AQSHda federal darajada yagona sun’iy intellekt to‘g‘risidagi qonuni mavjud emas. Biroq 2020 yilda AQSH SI texnologiyalarini rivojlantirish va uning etik foydalanishini ta’minlashga qaratilgan milliy strategiyani e’lon qildi. AQSHda mavjud qonunchilik SIdan mudofaa, sog‘liqni saqlash va xavfsizlik kabi sohalarda foydalanishni tartibga soladi. Biroq hozirda AQSHda biznes va davlat tashkilotlarida SIdan foydalanishda kamsitish, ayirmachilikka yo‘l qo‘ymaslik, shaffoflik va javobgarlik bo‘yicha etik prinsiplar ishlab chiqilmoqda.

Xitoy hozirgi kunda ma’lumotlar va xavfsizlikka oid masalalar bo‘yicha SIni tartibga solish bo‘yicha qonunchilikni ishlab chiqish borasida faollik ko‘rsatmoqda.

2022 yilda Xitoy ma’lumotlar xavfsizligini ta’minlash va ishlab chiquvchilarning etik javobgarligiga qaratilgan tavsiyalarni taqdim etdi. Xitoyning “Ma’lumotlarni himoya qilish to‘g‘risida”gi qonuni SIdan foydalanish bilan chambarchas bog‘liq bo‘lib, ko‘plab SI tizimlari katta miqdordagi shaxsiy ma’lumotlar bilan ishlaydi.

Kanadaning “Raqamli xartiya” (Digital Charter) to‘g‘risida”gi qonuni 2019 yilda Kanada hukumatining raqamli iqtisodiyot va internetdagi ma’lumotlarning himoyasiga oid qonunchilik tashabbuslari doirasida qabul qilingan bo‘lib, mazkur Qonun SIni qisman tartibga soladi va davlat tuzilmalarida SIdan foydalanish qoidalarini tartibga soladi.

Kanadaning “Raqamli xartiya to‘g‘risida”gi Qonuni quyidagi asosiy jihatlarni o‘z ichiga oladi:

1. Ma’lumotlarning maxfiyligi va himoyasi.

Ma’lumotlar to‘plash va ishlash: Ma’lumotlarni to‘plash va qayta ishlashda shaxsiy ma’lumotlarning maxfiyligi va himoyasini ta’minlash.

Ma’lumotlarning nazorati: Fuqarolarga o‘z ma’lumotlari bo‘yicha nazoratni oshirish imkoniyatini berish.

2. Shaxsiy ma’lumotlardan foydalanish.

Shaxsiy ma’lumotlarga rioya qilish: Shaxsiy ma’lumotlarning qanday yig‘ilishi, saqlanishi va foydalanilishiga oid qoidalarni belgilash.

Ma’lumotlardan foydalanishda ochiqlik: Ma’lumotlarning qay tarzda foydalanilishi va qanday maqsadda ishlatilayotganligi to‘g‘risida ma’lumot berish.

3. Texnologiyalar va axloqiy standartlar.

Sun’iy intellekt va algoritmlar: Sun’iy intellekt va algoritmlarning axloqiy standartlarga muvofiq ishlatilishiga rioya qilish.

Texnologik xavfsizlik: Raqamli texnologiyalar va tizimlar xavfsizligini ta’minlash va zarar keltiruvchi xatolardan himoyalash.

4. Fuqarolarning huquqlari.

Shaxsiy ma’lumotlar huquqlari: Fuqarolarga o‘z shaxsiy ma’lumotlariga oid to‘liq ma’lumot olish, ularni o‘chirish yoki o‘zgartirish huquqi berish.

Shaxsiy ma’lumotlarni himoyalash: Fuqarolarning shaxsiy ma’lumotlarining himoyasini ta’minlash.

5. Javobgarlik va sanksiyalar.

Rioya qilmaslik uchun jazolar: Ma’lumotlar himoyasi qoidalariga rioya qilmaganlik uchun sanksiyalar va jazo choralari.

PROSPECTS OF USING MODERN TECHNOLOGIES IN THE CRIMINAL PROCEEDINGS

Azamova Gulbakhor Azamovna
Master's student of Law Enforcement Academy

Abstract: the article scientifically analyzes issues related to the use of modern innovational technologies, in particular the capabilities of artificial intelligence (AI), at the pre-trial stage of criminal proceedings. Several achievements and shortcomings that can be achieved as a result of the development of artificial intelligence models in criminal proceedings are studied, in which the author gave her suggestions and recommendations.

Keywords: *artificial intelligence, Criminal Procedure, proof, decision making, evidence collection, forecasting.*

Annotatsiya: Maqolada jinoyat ishlarini yuritishning sudgacha bo'lgan bosqichida zamonaviy innovatsion texnologiyalardan, xususan, sun'iy intellekt (SI) imkoniyatlaridan foydalanish bilan bog'liq masalalar nazariy jihatdan tahlil qilinadi. Jinoyat ishlarini sudgacha yuritish bosqichida sun'iy intellekt modellarini ishlab chiqish natijasida erishilishi mumkin bo'lgan bir qancha yutuq hamda kamchiliklar prognoz qilinib, bu borada muallif o'z taklif va tavsiyalarini berib o'tadi.

Kalit so'zlar: *sun'iy intellekt, jinoyat protsessi, isbotlash, qaror qabul qilish, dalillarni to'plash, prognoz qilish.*

Аннотация: В статье научно проанализированы вопросы, связанные с использованием современных инновационных технологий, в частности, возможностей искусственного интеллекта (ИИ) на досудебном этапе уголовного судопроизводства. В уголовном процессе прогнозируется ряд достижений и недостатков, которые могут быть достигнуты в результате разработки моделей искусственного интеллекта, в связи с чем автор дает свои предложения и рекомендации.

Ключевые слова: *искусственный интеллект, уголовный процесс, доказывание, принятие решений, сбор доказательств, прогнозирование.*

Introduction

In recent years, significant measures have been implemented in our country to develop and expand the application of artificial intelligence (AI) systems. Specifically, in the **"Development Strategy of New Uzbekistan in 2022-2026**[333]" specific tasks have been outlined for the successful implementation of AI in our country through the development of the **"Strategy for the Development of Artificial Intelligence Technologies in 2023–2030.**[334]**"** Additionally, the Presidential Decree No. PQ-5234 dated August 26, 2021, **"On Measures to Introduce a Special Regime for the Use of Artificial**

[333] https://www.imv.uz/media/document_files/uzbekistan-report-development-strategy-2022-2026-final-november-2022-pdf.pdf

[334] Ўзбекистон Республикаси Президентининг 2022-йил 28-январдаги "2022-2026-йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида"ги ПФ-60-сон Фармони // Ўзбекистон Республикаси қонун ҳужжатлари маълумотлари миллий базаси, www.lex.uz.

Intelligence Technologies,[335]" and other relevant documents emphasizes the need to enhance digitalization processes in the republic.

The New Uzbekistan Strategy emphasizes the integration of modern information and AI technologies in combating corruption, developing mechanisms for the digitization of the enforcement system, and, broadly, conducting scientific research to gradually incorporate AI systems into the existing legal framework in the judiciary and legal sectors.

Each year, official bodies host numerous organizational, educational-methodological, and scientific discussions on the challenges and opportunities of using AI systems in various fields such as healthcare, education, industry, construction, public administration, and science. The potential of AI technologies is also given particular attention in the legal field. This focus is driven by the fact that legislation processes, legal interpretation, and law enforcement activities are among the areas that could be significantly influenced by computer and information technologies, particularly AI systems.

Artificial intelligence is the process of creating systems capable of acting in a way that is recognized as intelligent by humans[336]. From this perspective, it can be assumed that such systems aim to develop computer functions related to human intelligence, such as reasoning, learning, and problem analysis. Considering the imperfection of human intellectual activity, artificial intelligence may play a very significant role in people's lives. In other words, artificial intelligence is the human capability applied within the realm of computer and information technologies. This concept serves as the foundation for addressing the issue of artificial intelligence in criminal procedure.

Numerous studies on this topic encompass not only general law but also criminal procedural law[337]. However, artificial intelligence in criminal procedure is not a solution in itself. The study and application of artificial intelligence and its capabilities in law, including criminal law, require independent and comprehensive research, which, in principle, should remain under the supervision of legal professionals. Creating algorithms to solve

---

[335] Ўзбекистон Республикаси Президентининг "Сунъий интеллект технологияларини қўллаш бўйича махсус режимни жорий қилиш чора-тадбирлари тўғрисида"ги ПҚ-5234-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари маълумотлари миллий баъзаси, www.lex.uz.

[336] Джонс, М. Т. Программирование, искусственного, интеллекта, приложениях. ДМК-Пресс, 2018 ISBN · 978-5-94074-746-8 ; Страниц – 312, 15 с

[337] Власова С.В. К вопросу о приспосабливании уголовно - процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9 - 18; Апостолова Н.Н. Искусственный интеллект в судопроизводстве // Северо - Кавказский юридический вестник. 2019. № 3. С. 135 - 141; Хисамова З.И., Бегишев И.Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 564-574; Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2019. № 1. С. 91 - 109; Информационные технологии в уголовном процессе зарубежных стран. Монография. Коллектив авторов. Под ред. С.В. Зуева,М., 2020. 216 с.

problematic situations necessitates specialized knowledge in mathematics, engineering, linguistics, management, psychology, and information technologies, as well as the legal expertise to adapt these algorithms to specific fields of science. The success of studying artificial intelligence capabilities in criminal procedure will largely depend on utilizing such interdisciplinary knowledge.

Thus, introducing artificial intelligence systems into criminal procedure without adequate information technology support may seem unreliable. In such a situation, for a specialist, the priority lies not in the systems themselves but in advancing the fields where artificial intelligence systems can be applied. It is also essential to consider that the latter cannot exist without the former. So, how can artificial intelligence systems be utilized in criminal procedure?

To date, many forms of implementing the use of artificial intelligence have been proposed by scholars and practitioners. Specifically, we can discuss the forms of utilizing this system to develop crime predictions, organize investigation and forensic examination processes, systematize evidence, and support final decisions. These systems enhance the efficiency of law enforcement operations through automation, significantly reduce the time required to make decisions in specific legal situations, and improve the quality and development of those decisions.

Since any intelligent system is the result of consolidating all available knowledge in a specific field, its application within the scope of our topic deserves special emphasis. For example, through expert systems, concentrated knowledge from various domains of human intelligence is applied to solve standard situations, and the recommendations provided by artificial intelligence have an advisory nature. Decision-making, however, remains within the purview of humans.

At this point, it is worth highlighting the primary goals of using artificial intelligence in criminal proceedings, particularly in perceiving and systematically presenting information. Scholars have already studied the following main directions for applying artificial intelligence in criminal procedure.

To date, many forms of implementing the use of artificial intelligence have been proposed by scholars and practitioners. Specifically, we can discuss the forms of utilizing this system to develop crime predictions, organize investigation and forensic examination processes, systematize evidence, and support final decisions. These systems enhance the efficiency of law enforcement operations through automation, significantly reduce the time required to make decisions in specific legal situations, and improve the quality and development of those decisions.

Since any intelligent system is the result of consolidating all available knowledge in a specific field, its application within the scope of our topic deserves special emphasis. For example, through expert systems, concentrated knowledge from various domains of human intelligence is applied to solve standard situations, and the recommendations provided by artificial intelligence have an advisory nature. Decision-making, however, remains within the purview of humans.

At this point, it is worth highlighting the primary goals of using artificial intelligence in criminal proceedings, particularly in perceiving and systematically presenting information. Scholars have already studied the following main directions for applying artificial intelligence in criminal procedure.

Considering that the process of investigating crimes is often represented in scientific studies as an information system or model, it is through such a model that directions for integrating artificial intelligence into criminal investigations are formed. For instance, **Perrot P.** proposes three scenarios for the application of artificial intelligence systems in the work of French police investigators:

- **Modeling future crimes;**
- **Modeling the behavior and thinking of the offender;**
- **Modeling the behavior and thinking of the investigator[338].**

It seems that the first point directly follows from the second, making its differentiation somewhat redundant. However, this system provides valuable insight into the dichotomy of behavior (activities) and thinking for both investigators and offenders, reflecting the binary structure of criminalistics as a field.

The capabilities of artificial intelligence, particularly artificial neural networks, can be applied in the following more detailed directions:

1. **Assessment of the initial information on the criminal case** in order to put forward simple and complex investigative versions, to determine the directions of their verification.

2. **Modeling of the crime event and its trace pattern** based on incomplete data and previous *"experience"* covering a large array of criminal cases. Such an information model can be both informative and probabilistic in nature. As an example, the **VALCRI** *(Visual Analytics for Sense-making in Criminal Intelligence)* project developed in the UK allows optimizing search, search and evidentiary activities based on registration data[339].

---

[338] *Perrot P.* What about AI in criminal intelligence? From predictive policing to AI perspective // European Police Science and Research Bulletin. 2017. № 16. P. 73.

[339] Analytical Provenance for Criminal Intelligence Analysis // Valcri white paper series. VALCRI– WP–2017–009 / ed. by B. L. William Wong. 2017. 1 jan. URL: http://valcri.org/our- content/uploads/2017/02/VALCRI-WP-2017-009-Provenance3.pdf

3. **Identification of serial signs** in conditions of information insufficiency and a proposal to verify promising investigative versions. For example, in the case of the murder of a man in exact area committed with extreme cruelty, it is necessary to determine the verification actions aimed at establishing similar crimes committed in the same locality recently, taking into account the facts of causing harm to health of various degrees of severity. In this case, the range of possible suspects loses its universality and it is reduced to a defined special group. For example, not only near-criminal communities (of a neo-Nazi or other nature) should be checked for involvement in a crime, but also any places where people capable of committing a crime with an appropriate motive can gather, such as hand-to-hand and knife combat courses. historical reconstruction clubs, religious gatherings, etc.)[340].

4. **Assessing the sufficiency of collected evidence** for filing charges or forwarding the case to the prosecutor.

5. **Working with social networks, web cache, search engine index and other software devices.** Thus, monitoring the source of a fake or extremist message is one of the most pressing tasks of modern criminology[341]. At the same time, as A. **Pershin A.N.** notes, the modern investigator lacks the authority to collect evidence in network information systems, which is partially compensated by instructions to the inquiry body[342]. Perhaps intelligent systems will be able to resolve this contradiction.

6. **Predicting future crimes** based on analyzing the characteristics of committed crimes, including their locations, the social profiles of involved individuals, and media reports. From 2012 to 2018, *New Orleans* (USA) implemented a **project called "Palantir**,"[343] which collected information about city residents, such as their social circles, workplaces, movements, and social media activities. Based on this data, AI analyzed the social landscape to identify potential future criminals and their victims. However, the lack of regulatory frameworks for such initiatives hinders their real-world integration. Although **Palantir** successfully identified *80% of firearm offenders*, none of these crimes were prevented. Meanwhile, the European Union has shown a tendency to roll

---

[340] См. *Бахтеев Д. В.* Признаки серийности и их воздействие на выдвижение типовых следственных версий при расследовании убийств // Раскрытие и расследование преступлений серийных и прошлых лет: материалы Международной научно-практической конференции (Москва, 16 марта 2017 года) / под общ. ред. А. И. Бастрыкина. М.: Московская академия Следственного комитета Российской Федерации, 2017. С. 59–63.

[341] Андрей Николаевич Сретенцев К вопросу о возможностях искусственного интеллекта в решении задач криминалистической науки // Государственная служба и кадры. 2023. №4. (дата обращения: 18.12.2024).

[342] Pershin A.N. Digital rights persons carrying out a preliminary investigation. *Courier of Kutafin Moscow State Law University (MSAL))*. 2021;(2):108-115. (In Russ.) https://doi.org/10.17803/2311-5998.2021.78.2.108-115

[343] Nikulin, D.. (2022). Artificial intelligence and digitalization in forensics. Interexpo GEO-Siberia. 5. 33-36. 10.33764/2618-981X-2022-5-33-36.

back video surveillance projects with *facial recognition* functions due to privacy concerns[344].

Having studied the results of the process, it can be said that our analysis is aimed at the fact that artificial intelligence systems, in principle, must prove themselves in the implementation of these functions. Consequently, they should focus on proving a criminal case and making criminal procedural decisions. In this case, the stages of detection, opening and investigation of crimes imply the implementation of various criminal procedural decisions and organizational actions. In addition, the process of implementing them through artificial intelligence involves optimizing all available forces and tools, including information, recommendation, and advisory features. For example, the subjects of expertise and criminalistics can be used very successfully in the process of proving and making decisions. The knowledge expressed in the form of rules, such as *"if such a fact exists, then such an act has occurred, or such a reason suits for this Act"*, which is the basis of the examination, is suitable for automation and allows imitation of a person. This in turn creates the conditions for artificial intelligence to provide advice and recommendations that the investigator will be able to properly organize the investigation and assess the state of the investigation. The main tasks carried out using such systems can be:

– determination of possible investigative directions (formation of versions of events taking into account various sources of Information), selection of the most likely directions;

– give the user recommendations on further actions (conducting quick search activities, authenticating the facts that need to be checked correctly organizing investigative actions, etc.).

It should also be borne in mind that when solving these tasks, researchers note that it is impossible to do this without the presence of certain additional elements in the melody[345]:

– system of standard models of investigative actions;
– a system of tactical methods that ensure the optimality of investigative actions;
– traditional forms of a system of logical methods that optimize standard investigative actions;
– a system of heuristic methods for organizing investigations[346].

---

[344] *Степаненко Д. А., Бахтеев Д. В., Евстратова Ю. А.* Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. 2020. Т. 14. № 2. С. 206–214.

[345] Афанасьев А. Ю. Афанасьев А.Ю. Введение в уголовно-процессуальную науку. М. Тим Джонс; Пер. с англ. Осипов А. И. М.: ДМК Пресс, 2021. С. 572.

[346] Миронова О. А. Эвристический метод обучения в развитии творчества // Известия ТулГУ. Гуманитарные науки. 2011. №3-2. URL: https://cyberleninka.ru/article/n/evristicheskiy-metod-obucheniya-v-razvitii-tvorchestva (дата обращения: 20.12.2024).

As an example, it requires the development of standard algorithms of proof and decision-making in the criminal proceedings, which are included in the expert system. Depending on the specific input, based on its characteristics, the expert system selects an algorithm suitable for its actions, based on the tasks of the subject of activity for the detection, opening and investigation of crimes. For example, an expert system based on the rules of Criminal Procedure and forensic characteristics of a criminal procedure for an investigator or Inquirer about a message from the death of a person conducts a type-specific analysis of the data and offers him an algorithm consisting of standard actions and standard procedural decisions to prove. Accordingly, such a system will help the subject of criminal investigation, the correct assessment of the criminal phenomenon, the choice and execution of the appropriate algorithm of actions for the host, prove and make decisions.

Conclusion

Before summing up, we should not neglect some fundamentally significant challenges arisen in the process of implementing artificial intelligence advantages in the criminal proceedings, especially, in the pre-trial stage. Below, we will discuss the challenges categorizing them in three main aspects.

Incomplete representation of crimes: currently, neither crime descriptions nor forensic characteristics of offenses are fully defined. Some of them remain latent or are ambiguously outlined, making comprehensive analysis difficult.

Lack of concrete algorithms in criminal proceedings: in the realm of criminal justice, the absence of specific algorithms for proving and decision-making is a notable gap. Developing such algorithms for each type of crime is a complex task. In practice, reliance on standard algorithms may be the only feasible approach.

Absence of interdisciplinary collaboration: on one hand, there is a lack of interdisciplinary efforts to identify the critical legal knowledge required for integrating artificial intelligence into criminal proceedings. On the other hand, experts in this field often consider AI applications solely within the confines of their specific objectives, which hinders the broader consistency needed for effective implementation.

In conclusion, it is worth saying that introducing artificial intelligence systems into criminal proceedings holds the potential to optimize all aspects of the process in the future. However, this will require coordinated and systematic efforts from a wide range of scientists and practitioners, rather than relying on the contributions of individual researchers. Moreover, leveraging all available tools and resources will not suffice to overcome the challenges without incorporating advancements from disciplines beyond jurisprudence into the AI implementation process.

СУДДА ИШ КЎРИШНИНГ ОЧИҚЛИГИНИ ТАЪМИНЛАШДА СУНЪИЙ ИНТЕЛЛЕКТ ИМКОНИЯТЛАРИДАН ФОЙДАЛАНИШНИНГ АЙРИМ МАСАЛАЛАРИ

Сабиров Эркинжон Кучкарбаевич, ю.ф.ф.д. (PhD),
Ҳуқуқни муҳофаза қилиш академияси мустақил изланувчиси

Аннотация: ушбу мақолада судда иш кўришнинг очиқлигини таъминлашда сунъий интеллект имкониятларидан фойдаланишнинг назарий ва амалий масалалари, бу масала бўйича хорижий давлатлар қонунчилик тажрибаси таҳлил қилинган. Судда иш кўриш жараёнида сунъий интеллектдан фойдаланишда юзага келадиган муаммо ўрганилган ва уларни бартараф этишга қаратилган аниқ таклиф ва тавсиялар илгари сурилган.

Калит сўзлар: судда иш кўриш, сунъий интеллект, ошкоралик, шаффофлик, ахборот хавфсизлиги, таҳдидлар, ҳуқуқий асослар, такомиллаштириш.

Аннотация: в данной статье рассмотрены теоретические и практические аспекты использования возможностей искусственного интеллекта для обеспечения открытости судебного процесса, а также проанализирован законодательный опыт зарубежных стран по данному вопросу. Изучены проблемы, возникающие при использовании искусственного интеллекта в судебном процессе, и представлены конкретные предложения и рекомендации по их устранению.

Ключевые слова: судебный процесс, искусственный интеллект, открытость, прозрачность, информационная безопасность, угрозы, правовые основы, совершенствование.

Annotation: This article examines the theoretical and practical aspects of using artificial intelligence to ensure the openness of court proceedings and analyzes the legislative experience of foreign countries on this matter. Issues arising from the use of artificial intelligence in judicial processes have been studied, and specific proposals and recommendations for their resolution have been put forward.

Keywords: court proceedings, artificial intelligence, openness, transparency, information security, threats, legal framework, improvement.

Сўнгги йилларда сунъий интеллект кўплаб соҳаларда, жумладан ҳуқуқ соҳасида ҳам улкан ўзгаришлар олиб келувчи кучга айланди. Дунё бўйлаб кўплаб мамлакатлар сунъий интеллект технологияларини фуқаролик ишларини судларда кўрилиши жараёнларини жадаллаштириш ва самарадорлигини ошириш мақсадида қўллашни бошлаб юбордилар. Бироқ, бу технологиялардан фойдаланиш шаффофлик, тушунарлилик ва одил судловга бўлган ҳуқуқлар нуқтаи назаридан жиддий муаммоларни келтириб чиқариши мумкин.

Таъкидлаш жоизки, янги Ўзбекистонни барпо этиш жараёнида мамлакатимизда ҳам “суд органларининг фаолиятида очиқлик ва шаффофликни таъминлаш, фуқаролар ва тадбиркорлик субъектларининг суд ҳокимиятига бўлган ишончини янада ошириш”[347]га қаратилган вазифалар белгиланган.

“Барча давлат органларида қарор қабул қилиш жараёнлари, очиқ ва фақат очиқ бўлишини таъминлаш”[348], давлат органлари фаолияти устидан жамоатчилик назоратини кучайтиришнинг ҳуқуқий механизмларини такомиллаштириш талаб этилмоқда. Бу эса фуқароларнинг одил судловга бўлган ишончини оширишнинг самарали ҳуқуқий механизмларини ишлаб чиқиш, хусусан, фуқаролик ишлари бўйича суд ҳужжатларининг очиқлигини таъминлашда сунъий интеллект имкониятларидан фойдаланиш масалаларини тадқиқ этиш заруратини келтириб чиқаради.

Судда иш кўриш жараёнида сунъий интеллектдан фойдаланишда юзага келадиган биринчи муаммо — бу унинг шаффофликка бўлган таъсиридир. Судда фуқаролик ишларини кўриш ва ҳал этиш жараёнида одил судловни таъминлаш ва жамоатчиликнинг суд тизимига бўлган ишончини оширишда муҳим аҳамиятга эга. Аммо сунъий интеллект алгоритмлари кўпинча “қора қути” (black box) принципи асосида ишлайди, бу эса қарорларни қандай қабул қилинганлигини тушунишни қийинлаштиради. Бундай шароитда шаффофликнинг мавжуд эмаслиги тизимдаги эҳтимолий хато ёки иш ҳолатларига нисбатан хавотирларни кучайтиради.

Мазкур хавотирли масала кўплаб хорижлик мутахассисслар ва ҳуқуқшунос олимларни ўйлантириб келмоқда. Бинобарин, хорижий давлатлар судлари амалиётида ҳозирги кунда кўрилаётган ишларда ҳам бу муаммо кўзга ташланмоқда. Масалан, R v McWilliams[349] ишида Буюк Британия полицияси томонидан қўлланилган эксперт тизими қарорларнинг шаффоф асосларини тушунтириб бера олмаганлиги сабабли ишончли эмас деб топилган. Шунингдек, State v Loomis[350] ишида ҳам жазо муддатларини белгилашда қўлланилган хавф

[347] Ўзбекистон Республикаси Президентининг 2020 йил 24 июлдаги “Судлар фаолиятини янада такомиллаштириш ва одил судлов самарадорлигини оширишга доир қўшимча чора-тадбирлар тўғрисида” ПФ-6034-сон Фармони // Қонун ҳужжатлари маълумотлари миллий базаси, 24.07.2020 й., 06/20/6034/1103-сон; 21.01.2021 й., 06/21/6143/0052-сон.

[348] Ўзбекистон Республикаси Президентининг 2020 йил 29 декабрдаги Олий Мажлисга Мурожаатномаси // “Халқ сўзи” газ. 2020 й. 30 дек. сони.

[349] R v McWilliams [1994] 1 Cr App R 212.

[350] State v. Loomis [2016] 881 N.W.2d 749

таҳлили алгоритми шаффофликнинг йўқлиги муносабати билан қабул қилинмаган.

Сунъий интеллект технологияларини ҳуқуқий тизимларга жорий этишдаги яна бир муҳим муаммо — бу унинг тушунарли бўлишидир. Тушунарлилик суд ва процесс иштирокчилари томонидан сунъий интеллект тизимлари қандай қарор ёки тавсияларга келганини тушуниш ва уни тушунтириш имкониятини англатади. Қийин ва мураккаб фуқаролик ишларининг судда кўрилишида иш юзасидан судьянинг инсон сифатида қабул қилаётган қарори асосий ўрин тутади.

Шундай экан, сунъий интеллект яратган натижалар, хулосаларни тушуниш судьялар, адвокатлар, прокурор ва процесснинг бошқа иштирокчи-лари учун жуда муҳимдир. Зеро, шаффофликнинг йўқлиги ҳисобдорликни сусайтиради, тушунарлиликнинг чекланганлиги эса шахсларнинг одил судловга бўлган ҳуқуқларига салбий таъсир қилади. Назаримизда, мазкур муаммоларни ҳал қилиш учун шаффофликни таъминлайдиган ва процесснинг барча иштирокчиларининг, айниқса, тарафлар ва учинчи шахсларнинг одил судловга бўлган ҳуқуқларини кафолатлайдиган тегишли қоидаларни ишлаб чиқиш зарур ҳисобланади.

Сунъий интеллектнинг дунё бўйлаб ҳуқуқий тизимларда қўлланилиши самарадорлик ва аниқликни оширишга қаратилган имкониятларга эга эканлиги сабабли кўпчиликнинг эътиборини қозонди. Бироқ, фуқаролик ишларининг судларда кўрилиши жараёнида сунъий интеллектдан фойдаланиш шаффофлик, тушунарлилик ва одил судловга бўлган ҳуқуқни амалга ошириш нуқтаи назаридан жиддий муаммоларни келтириб чиқариши мумкин. Маълумки, шаффофлик бу ҳар қандай ҳуқуқий тизимда ҳисобдорлик ва ишончни таъминловчи асосий тамойиллардан ҳисобланди. Сунъий интеллект контекстида шаффофлик алгоритмлар қандай қарорлар қабул қилаётганини тушуниш ва ушбу жараёнларни текшириш имконияти билан боғлиқ. Бироқ, сунъий интеллект қўлланилган ҳуқуқий тизимларда шаффофликка эришиш мураккаб вазифа бўлиб қолмоқда.

Сунъий интеллект тизимлари ишга тушилираётган пайтда ушбу тизим катта ҳажмдаги шахсий маълумотларга таянади ва бу ўз навбатида шаффофлик учун қўшимча тўсиқларни юзага келтиради. Бу жараёнда шахсий маълумотларни шахсларнинг розилигисиз

ишлатилиши мумкин эмас. Масалан, **Doe v Google LLC**[351] ишида шахслардан уларнинг шахсий маълумотларидан сунъий интеллект тизимларида фойдаланилиши тўғрисида хабардор қилиниши ва шундай қарорларга эътироз билдириш ҳуқуқи бўлиши кераклиги таъкидланган. Маълумотлар махфийлиги муаммоларини ҳал этмаслик шаффофлик ва сунъий интеллект орқали бошқариладиган ҳуқуқий жараёнларнинг адолатлилигига путур етказиши мумкин.

Одил судловга бўлган ҳуқуқларни сақлаб қолиш учун шахслар сунъий интеллект тизимлари томонидан қабул қилинган қарорларни тушуниш ва уларга эътироз билдириш учун зарур бўлган маълумотларга эга бўлишлари лозим. Сунъий интеллект қўлланилган ҳуқуқий тизимларда шаффофликнинг йўқлиги бу ҳуқуқни чеклаши мумкин, бу эса адолатсиз қарорларга олиб келиши эҳтимоли бор. Масалан, **R v Bridges**[352] ишида юзни таниш технологиясидан тегишли хавфсизлик чоралари ёки жамоатчилик текширувисиз фойдаланилгани шахсий ҳаёт дахлсизлиги ва адолатли суд ҳуқуқига эҳтимолий таҳдидлар туғдирган.

Сунъий интеллект тизимларининг турли соҳаларда тезкор ривожланиши ва интеграция қилиниши уларнинг ишлаш жараёнларида шаффофликнинг етишмаслиги билан боғлиқ хавотирларни келтириб чиқармоқда.[353] Юридик адабиётларда таъкидланишича, сунъий интеллект алгоритмларининг мураккаблиги ва тушуниш қийинлиги билан боғлиқ муаммолар қуйидагиларда намоён бўлади: биринчидан, сунъий интеллект алгоритмлари кўпинча тушунарли бўлмайди ва ўзига хос мураккаблик касб этиб, улар қандай қарорлар қабул қилишини тушунишда қийинчиликлар юзага келади. Ушбу алгоритмлар кўп ҳолларда кўплаб математик моделлар ва ҳисоб-китобларга асосланади, бу эса уларни кенг жамоатчилик, ҳатто кўпгина мутахассислар учун ҳам тушунарсиз бўлишига саабаб бўлади.[354] Бунинг натижасида, шахслар сунъий интеллект тизимлари қандай қарорлар қабул қилаётгани ёки нима учун маълум тавсиялар берилаётганини тўлиқ тушуниш имкониятига эга бўлмайди.

---

[351] Smith-Dennis J., & Aikins S.K.B (2021). Artificial intelligence: opportunities, challenges and the way forward for Ghana. AI & Society, 36(2), 307-317.

[352] R v Bridges [2020] EWCA Civ 1058

[353] Smith-Lewis A., & Wyner A.Z (2020). The Transparency Problem: An Analysis Of Explainability In Artificial Intelligence Systems Used By The Criminal Justice System. Journal Of Law And Policy For The Information Society 16(1), 1-38.

[354] Smith, M. R., & Smith, L. N. (2018). Explainable AI: A guide for the perplexed. arXiv preprint arXiv:1811.04558.

Бундай мураккаблик ҳуқуқий тизимлардаги жараёнларга сезиларли таъсир кўрсатади. Масалан, судда иш юритилаётганда, тарафлар ёки унинг вакили сунъий интеллект томонидан чиқарилган қарорнинг мантиғини тушуна олмаса, бу унинг ўз ҳуқуқларини ҳимоя қилиш имкониятини чеклайди. Сунъий интеллект тизимларидан фойдаланишга асосланган қарорлар, агар уларнинг мантиғи тушунарсиз бўлса, ишончсиз ва адолатсиз деб баҳоланиши мумкин.

Сунъий интеллект тизимларида суд иши бўйича қарор қабул қилиш жараёнида ёндошув ва камситиш эҳтимоли мавжуд. Бу тизимлар иш ҳолатларини жамиятда мавжуд бўлган маълумотларга асосланиб ўрганади, ва бу маълумотларда илгаридан мавжуд бўлган ёндошувлар ёки камситишлар яширин бўлиши мумкин.[355] Агар ушбу ёндошувлар алгоритмларни ишлаб чиқиш жараёнида аниқланмаса ёки бартараф қилинмаса, бунинг оқибатида судда иштирок этаётган процесс иштирокчиларига нисбатан турли ноқулайликлар, камситишлар юзага келиши мумкин.

У ўринда хорижий давлатлар тажрибасига тўхталадиган бўлсак, АҚШ, Австралия, Канада, Ҳиндистон, Гана каби давлатларда сунъий интеллект тизимларида шаффофликнинг мавжуд эмаслиги адолатсиз натижаларга сабаб бўлган ҳолатлар кўп кузатилган. Масалан, Австралиянинг “Robodebt” автоматлаштирилган ижтимоий таъминот лойиҳасида минглаб одамлар нотўғри ҳисоб-китоблар сабабли қарздорликда айбланишган. Ушбу тизимда қандай ҳисоб-китоблар қилинганлиги бўйича шаффофликнинг йўқлиги жуда кўп адолатсизликларга олиб келган.[356] Канадада судьялар томонидан ишлатилган автоматлаштирилган хавфни баҳолаш қурилмаси, маҳаллий аҳолидан бўлган айбланувчиларни юқори хавфли жиноятчилар сифатида классификация қилишига олиб келган.[357] Бу мисоллар шаффофликнинг йўқлиги натижасида камситишларга ва мавжуд тенгсизликларнинг давом этишига олиб келишини кўрсатади.

---

[355] Smith-Lewis A., & Wyner A.Z., (2020). Artificial Intelligence: Bias Issues & Solutions in Decision-Making Systems. In: Proceedings of the 2020 International Conference on Big Data Engineering (BDE). Association for Computing Machinery (ACM).

[356] Australian Government, Senate Community Affairs References Committee. (2020). Robodebt: lives ruined, trust betrayed. Retrieved from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs/Robodebt45th/Report

[357] Angwin J., Larson J., Mattu S., & Kirchner L. (2016). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. ProPublica. Retrieved from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Г**ананинг жиноят ишлари тизимида** судгача бўлган хавфларни баҳолаш алгоритми паст даромадли кишиларга нисбатан камситишларга йўл қўйгани аниқланган.[358] Бу шахсларга нисбатан ҳақиқий хавф даражасини нотўғри баҳолаш ҳолатларини келтириб чиқарган.

Бир сўз билан айтганда, сунъий интеллект тизимларида шаффофликнинг мавжуд эмаслиги ва унга сабаб бўлувчи омиллар замонавий дунёда жиддий муаммоларни юзага келтирмоқда. Сунъий интеллект алгоритмларининг мураккаблиги уларни ҳар қандай шахс тушунишини қийинлаштиради, ёндошув ва камситишлар эса хавфсизлик чоралари йўқлиги туфайли судлар томонидан адолатсиз қарорлар қабул қилишга сабаб бўлади. Шунингдек, сунъий интеллект қарорларида ёндошув ва камситиш эҳтимоли этик муаммоларни юзага келтиради. Сунъий интеллект алгоритмлари катта маълумот тўпламларидан ўрганади, бу маълумотлар жамиятдаги ёндошувлар ёки камситишларни акс эттириши мумкин.[359] Агар бу ёндошувлар сунъий интеллект тизимини ишлаб чиқиш жараёнида аниқланмаса ва ҳал этилмаса, улар адолатсиз натижаларга олиб келиши ва мавжуд тенгсизликларни кучайтириши мумкин.

Бу каби муаммоларни ҳал этиш учун бутун дунё мамлакатлари сунъий интеллект тизимларида шаффофлик ва ҳисобдорликни таъминлашга қаратилган қадамлар ташлашни бошлади. Масалан, АҚШда “Алгоритмларнинг ҳисобдорликка қарши қонун” (Algorithmic Accountability Act) лойиҳаси ишлаб чиқилди ва мазкур қонун компанияларга алгоритмларидаги ёндошув ва камситишларни тўғрилаш бўйича мажбурият юклади.[360] Австралияда эса “Тушунарли сунъий интеллект” бўйича йўриқномалар ишлаб чиқилган бўлиб, ушбу йўриқномалар сунъий интеллектнинг шаффофликни таъминлашга ва унинг мазмунини тушунарли бўлишига хизмат қилади.[361] Ҳиндистонда эса “Шахсий

---

[358] George Benneh Mensah. I in the Legal System, Transparency, Interpretability and the Right to a Fair Trial: The Challenges and Implications for the Ghanaian Civil and Criminal Justice Systems // https://www.researchgate.net/publication/375640346_AI_in_the_Legal_System_Transparency_Interpretability_and_the_Right_to_a_Fair_Trial_The_Challenges_and_Implications_for_the_Ghanaian_Civil_and_Criminal_Justice_Systems

[359] Barocas S., Hardt M., Narayanan A., (2020). Fairness and Machine Learning. In: Hirschberg J., Manning C. (eds) Advances in Natural Language Processing. Springer, Cham. https://doi.org/10.1007/978-3-030-60450-9_1

[360] United States Congress (2019). Algorithmic Accountability Act of 2019 (H.R. 2231).

[361] Australian Government Department of Industry Science Energy and Resources (2020). Guidelines on Explainable Artificial Intelligence: Promoting Transparency & Accountability [Brochure].

маълумотларни муҳофаза қилиш тўғрисида”ги Қонун (Personal Data Protection Bill) ишлаб чиқилган бўлиб, ушбу Қонун сунъий интеллект тизимлари томонидан шахсий маълумотларни қайта ишлашни тартибга солиш ва шаффофликни таъминлашга қаратилган.[362]

Юқоридаги саъй-ҳаракатларни халқаро миқёсда сунъий интеллект тизимларида шаффофлик ва адолатни таъминлашга қаратилган муҳим қадам сифатида эътироф этиш мумкин ва Ўзбекистонда ҳам келажакда ривожланиб бораётган сунъий интеллекнинг хавф-ҳатарларини бартараф этиш ёки олдини олиш учун муҳим йўналиш сифатида қараш мумкин. Шундай экан, масъул давлат органлари ва турли соҳавий компаниялар ушбу муаммоларни аниқлаш ва уларни бартараф этиш учун қўшимча чора-тадбирларни кўришлари керак. Бинобарин, Ўзбекистон Республикаси Президентининг 2024 йил 14 октябрдаги “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПҚ-358-сон қарори билан тасдиқланган “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегияси”нинг Сунъий интеллект технологияларини ривожлантириш стратегиясини 2024 - 2026 йилларда амалга ошириш бўйича чора-тадбирлар режасининг 3-бандида “Сунъий интеллектни жорий этиш, ривожлантириш ва фойдаланиш соҳасидаги шахсга доир маълумотлар хавфсизлигини таъминлаш” каби чора-тадбир назарда тутилган.[363] Унда 2025 йил майда илғор халқаро тажриба асосида сунъий интеллектни жорий этиш, ривожлантириш ва фойдаланиш соҳасидаги шахсга доир маълумотлар хавфсизлигини таъминлашга қаратилган норматив-ҳуқуқий ҳужжатини ишлаб чиқиш вазифаси назарда тутилган.

Retrieved from https://www.industry.gov.au/sites/default/files/2021-01/guidelines-on-explainable-artificial-intelligence.pdf

[362] Ministry of Electronics & Information Technology (Government of India). (2019). Personal Data Protection Bill [Bill No. 373].

[363] Ўзбекистон Республикаси Президентининг 2024 йил 14 октябрдаги “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПҚ-358-сон қарори // https://www.lex.uz/docs/7158604#7160450

“Kiberhuquq: muammolar va rivojlantirish istiqbollari” mavzusida bo‘lib o‘tadigan xalqaro ilmiy-amaliy konferensiyasi

Konferensiya tashkilotchisi:	O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi
	Toshkent davlat yuridik universiteti
Sana va o’tkaziladigan joy:	2024 yil 25 sentabr kuni soat 09 : 30 da Yunusobod tumani Rixsiliy ko’chasi 9-uy
Konferensiya ishtirokchilari:	Huquqni muhofaza qilish akademiyasining professor-o‘qituvchilari, mustaqil izlanuvchilari va tayanch doktorantlari
	Hindiston Milliy sud ekspertizasi universiteti
	Qozog‘iston Respublikasi Huquqni muhofaza qilish akademiyasi
	O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi
	Toshkent davlat yuridik universiteti
	Jamoat xavfsizligi universiteti
	INHA universiteti
	Toshkent axborot texkologiyalari universiteti
	Turin Politexnika Universiteti
	O‘zbekiston Respublikasi Davlat xavfsizlik xizmati akademiyasi
	Ichki ishlar vazirligi akademiyasi
	Ichki ishlar vazirligi “Kiberxavfsizlik markazi”
	O‘zbekiston Respublikasi Prezidenti huzuridagi Qonunchilik va huquqiy siyosat instituti
	O‘zbekiston Respublikasi Fanlar akademiyasi Davlat va huquq tarixi instituti
	Raqamli texnologiyalar va sun'iy intellektni rivojlantirish ilmiy-tadqiqot instituti vakillari
Ma'ruza uchun ajratilgan vaqt:	10 daqiqagacha
O’tkazish tartibi:	Gibrid (online/offline)
Tadbir tili:	O’zbekcha, inglizcha, ruscha.

“Kiberhuquq: muammolar va rivojlantirish istiqbollari” mavzusidagi xalqaro ilmiy-amaliy konferensiyasi

D A S T U R I

09:00 – 09:30	**Ishtirokchilarni ro‘yxatga olish**
10:00 – 10:10	**Kirish so‘zi** **Kolenko Yevgeniy Vyacheslavovich -** Huquqni muhofaza qilish akademiyasi boshlig‘ining birinchi o‘rinbosari, yuridik fanlar bo‘yicha falsafa doktori, dotsent
10:10 – 10:20	**Kirish so‘zi** **Shushikova Gulnar Karbaevna -** Qozog‘iston Respublikasi Bosh prokuraturasi huzuridagi Huquqni muhofaza qilish akademiyasi Idoralararo ilmiy-tadqiqot instituti prorektori-direktori
Moderator: Nazarov Farxodjon Abduvaxobovich – Huquqni muhofaza qilish akademiyasi Tezkor-qidiruv faoliyati va kiberhuquq kafedrasi boshlig‘i	
10:20 – 10:30	*Cybercrime and Cyberlaw* **Naeem Allah Rakha** - Xalqaro yurist (Pokiston), Toshkent davlat yuridik universiteti Kiberhuquq kafedrasi o‘qituvchisi
10:30 – 10:40	*Strategies for Enforcement of Cyber Laws* **Purvi Pokhariyal** - Hindiston Milliy sud ekspertizasi universiteti professori (online)
10:40 – 10:50	*“Cyber Law” darsligining taqdimoti: O‘zbekistonda raqamli huquqiy ta’limni shakllantirish* **Gulyamov Said Saidaxrarovich –** yuridik fanlari doktori, professor, Toshkent davlat yuridik universiteti Kiberhuquq kafedrasi mudiri
10:50 – 11:00	*Prokuratura organlari faoliyatini raqamli transformasiya qilishning tashkiliy-huquqiy asoslarini takomillashtirishdagi yangicha yondashuvlar* **Boboev Mirshod Murotovich –** O‘zbekiston Respublikasi Bosh prokuraturasi Axborot-kommunikasiya texnolog iyalarini joriy etish va axborot xavfsizligini ta'minlash boshqarmasi boshlig‘i, yuridik fanlar bo‘yicha falsafa doktori
11:00 – 11:10	*Kiberhuquq sohasida kadrlar tayyorlash: imkoniyat va hamkorlik istiqbollari*

	Nazarov Farxodjon Abduvaxobovich – Huquqni muhofaza qilish akademiyasi Tezkor-qidiruv faoliyati va kiberhuquq kafedrasi boshlig‘i
11:10 – 11:20	*Kiberxavfsizlik sohasida xalqaro hamkorlik imkoniyatlardan kiberjinoyatlarga qarshi kurashda foydalanish istiqbollari* **Ubaydullayev Qudratilla Xabibullayevich** – O’zbekiston Respublikasi Strategik tahlil va istiqbolni belgilash oliy maktabi, siyosiy fanlar doktori.
11:20 – 11:30	*Predictive Justice: Ensuring a Just, fair and Reasonable Approach to legal Decision-Making* **Navtika Singh Nautiyal** – Dehli korpusi Milliy sud ekspertizasi universiteti dotsenti (online)
11:30 – 11:40	*Aktualnыe problemы podgotovki kadrov v sfere kiberbezopasnosti* **Davlatov Zafar Ravshanovich** – Toshkent shahridagi Inha universiteti Hamkorlikni rivojlantirish va homiylikni jalb etish bo‘limi boshlig‘i
11:40 - 11:50	*Raqamli kriminalistika sohasida ilmiy-tadqiqot faoliyati* **Musayev G‘ayrat Farxadovich** – Raqamli kriminalistika ilmiy-tadqiqot instituti boshlig‘i
11:50 – 12:10	***KOFE-BREYK***
12:10 – 12:20	*Kiberjinoyatlarning turlari, ijtimoiy xavfliligi va kvalifikasiya qilish masalalari* **Axrorov Baxrom Djabbarovich** – Jamoat xavfsizligi universitet “Jinoiy-huquqiy fanlar” kafedrasi professori, yuridik fanlar doktori, professor
12:20 - 12:30	*Sun’iy intellekt qarorlarini noto’g‘ri talqin qilish muammolari: algoritmik noaniqlikdan inson huquqlarigacha* **Sobirov Shoxruxbek Tavakkal o’g‘li** – O‘zbekiston Respublikasi Prezidenti huzuridagi Qonunchilik va huquqiy siyosat instituti Ijtimoiy sohadagi qonunchilik shu’basi bosh ilmiy xodimi
12:30 - 12:40	*AI-Driven Web Security:NLP-Based Log Analysis in Firewalls* **Aliev Abdurahmon Farxod o‘g‘li** – Toshkent shahridagi Turin politexnika universiteti, Avtomatik boshqaruv va kompyuter muhandisligi kafedrasi dotsenti, f.d.(PhD)

12:40 – 12:50	*Kripto-aktivlar tushunchasi, mazmun-mohiyati va o‘ziga xos xususiyatlari.* **Azizxonov Shohruh Madilxanovich** – Ichki ishlar vazirligi Tezkor-qidiruv departamenti, Kiberxavfsizlik markazi xodimi.
12:50 – 13:00	*Teran o‘zgarishga asoslangan tarmoq hujumlarini aniqlash usullari* **Ramozonova Madina Shavkatovna** – Muxammad al-Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi asistenti
13:00 – 13:10	*Sun’iy intellekt texnologiyalari yordamida video tasvirlardan foydalanib jinoyatlarni aniqlash va oldini olish tizimlarini ishlab chiqishda innovatsion yondashuv* **Boytemirov Asror Maxammado’stovich** – Muxammad al-Xorazmiy nomidagi TATU “Sun'iy intellekt” kafedrasi tayanch doktoranti
13:10 - 13:20	**Sagimbekov Baxitjan Jasamuratovich** - Qozog‘iston Respublikasi Bosh prokuraturasi huzuridagi Huquqni muhofaza qilish akademiyasi Idoralararo ilmiy-tadqiqot instituti Jinoyat-protsessual muammolarini o’rganish markazi bosh ilmiy xodimi
13:20 – 13:30	**Sodiqov Muxtar Beybutovich** – Qozog‘iston Respublikasi Bosh prokuraturasi huzuridagi Huquqni muhofaza qilish akademiyasi Oliy o’quv yurtidan keyingi ta’lim institutining “Umumiy huquq fanlari” kafedrasi o’qituvchisi
13:30 - 13:50	**Muhokama uchun savol-javoblar**
1 3:50	**Konferensiyani yakunlash**

Международная научно-практическая конференция на тему
«Киберправо: проблемы и перспективы развития»

Организатор конференции:	Правоохранительная Академия Республики Узбекистан Ташкентский государственный юридический университет
Дата и место проведения:	25 сентября 2024 в 09:30 Юнусабадский район, улица Рихсили 9
Участники конференции:	Профессора, независимые исследователи и докторанты правоохранительной Академии Национальный университет судебной экспертизы Индии Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан Министерство цифровых технологий Республики Узбекистан Ташкентский государственный юридический университет Университет общественной безопасности Университет ИНХА Ташкентский университет информационных технологий Политехнический университет Турина Академия Службы государственной безопасности Республики Узбекистан Академия МВД МВД «Центр кибербезопасности» Институт законодательства и правовой политики при Президенте Республики Узбекистан Институт истории государства и права Академии наук Республики Узбекистан Представители НИИ развития цифровых технологий и искусственного интеллекта
Время, отведенное на лекцию:	до 10 минут
Формат проведения:	Гибрид (онлайн/оффлайн)
Язык мероприятия:	Узбекский , английский , русский .

«Киберправо: проблемы и перспективы развития» международная научно-практическая конференция

ПРОГРАММА

09:00 – 09:30	**Регистрация участников**
10:00 – 10:10	**Введение** **Коленко Евгений Вячеславович -** Академия правоохранительных органов первый заместитель начальника по правовым вопросам науки в соответствии с философия доктор Доцент
10:10 – 10:20	**Введение** **Шушикова Гульнар Карбаевна** - Проректор-директор Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан
Модератор: Назаров Фарходжон Абдувахобович – начальник кафедры оперативно-розыскной деятельности и киберправа Академии правоохранительных органов.	
10:20 – 10:30	*Cybercrime and Cyberlaw* **Наим АллахРакха —** международный юрист (Пакистан), преподаватель кафедры киберправа Ташкентского государственного юридического университета.
10:30 – 10:40	*Стратегии обеспечения соблюдения кибер-законов* **Пурви Покхариял —** профессор Национального университета судебной экспертизы Индии (онлайн)
10:40 – 10:50	*Презентация учебника «Киберправо»: становление цифрового юридического образования в Узбекистане* **Гулямов Саид Саидахраровичч –** доктор юридических наук, профессор, заведующий кафедрой киберправа Ташкентского государственного юридического университета
10:50 – 11:00	*Новые подходы к совершенствованию организационно-правовых основ цифровой трансформации деятельности органов прокуратуры* **Бобоев Миршод Муротович** – начальник управления внедрения информационно-коммуникационных технологий и информационной безопасности Генеральной прокуратуры Республики Узбекистан, доктор философии по юридическим наукам
11:00 – 11:10	*Подготовка кадров в сфере киберправа: возможности и перспективы сотрудничества*

	Назаров Фарходжон Абдувахабович – заведующий кафедрой оперативного поиска и киберправа Академии правоохранительных органов.
11:10 – 11:20	*Перспективы использования возможностей международного сотрудничества в сфере кибербезопасности в борьбе с киберпреступностью* **Убайдуллаев Кудратилла Хабибуллаевич** – Высшая школа стратегического анализа и разведки Республики Узбекистан, доктор политических наук.
11:20 – 11:30	*«Предсказательное правосудие: обеспечение справедливого и разумного подхода к вынесению юридических решений»* **Навтика Сингх Наутиал** – доцент Национального университета судебной экспертизы, корпус Дели (онлайн).
11:30 – 11:40	*Актуальные проблемы подготовки кадров в сфере кибербезопасности* **Давлатов Зафар Равшанович** – Заведующий отделом развития партнёрства и спонсорства Университета Инха в Ташкенте.
11:40 – 11:50	*Научно-исследовательская деятельность в области цифровой криминалистики.* **Мусаев Гайрат Фархадович** - Начальник научно-исследовательского института цифровой криминалистики.
11:50 – 12:10	***КОФЕ-БРЕЙК***
12:10 – 12:20	*Виды киберпреступлений, социальная опасность и вопросы квалификации* **Ахроров Бахром Джаббарович** – профессор кафедры «Уголовно-правовые науки» Университета общественной безопасности, доктор юридических наук, профессор.
12:20 – 12:30	*Неправильная интерпретация решений ИИ проблемы: от алгоритмической неопределенности к правам человека* **Собиров Шохрухбек Таваккалович** – главный научный сотрудник отдела законодательства в социальной сфере Института законодательства и правовой политики при Президенте Республики Узбекистан.
12:30 – 12:40	*Веб-безопасность на основе искусственного интеллекта: анализ журналов на основе NLP в межсетевых экранах* **Алиев Абдурахмон Фарходович** – доцент кафедры автоматического управления и вычислительной техники Туринского политехнического университета в г. Ташкенте , ю.фд(PhD).

12:40 – 12:50	*Понятие, сущность и характеристики криптоактивов.* **Азизханов Шахрух Мадилханович** – сотрудник отдела оперативного розыска МВД, Центра кибербезопасности.
12:50 – 13:00	*Методы обнаружения сетевых атак, основанные на глубоких изменениях* **Рамозонова Мадина Шавкатовна** – ассистент кафедры «Кибербезопасность и криминалистика» ТАТУ имени Мухаммеда аль-Хорезми.
13:00 – 13:10	*Инновационный подход к разработке систем обнаружения и предотвращения преступлений с использованием видеоизображений с помощью технологий искусственного интеллекта* **Бойтемиров Асрор Махаммадостович –** заведующий отделом «Искусственного интеллекта» ТАТУ имени Мухаммеда аль-Хорезми.
13:10 - 13:20	**Сагымбеков Бахытжан Жасамуратович** - главный научный сотрудник Центра исследования проблем уголовного процесса Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.
13:20 – 13:30	**Садыков Мухтар Бейбутович** - преподаватель Кафедры общеюридических дисциплин Института послевузовского образования Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.
13:30 - 13:50	**Вопросы и ответы для обсуждения**
1 3:50	**Завершение конференции**

International scientific and practical conference on

"Cyber law: problems and development prospects"

Conference organizer:	The Law Enforcement Academy of the Republic of Uzbekistan Tashkent State University of Law
Date and venue:	September 25, 2024 at 09:30 Yunusabad District, Rikhsili Street 9
Conference participants:	Professors, independent researchers and doctoral students of the Law Enforcement Academy National Forensic Sciences University, India Academy of the Law Enforcement of the Republic of Kazakhstan Ministry of Digital Technologies of the Republic of Uzbekistan Tashkent State Law University University of Public Security INHA University Tashkent University of Information Technologies Polytechnic University of Turin Academy of the State Security Service of the Republic of Uzbekistan Academy of the Ministry of Internal Affairs Ministry of Internal Affairs "Cyber Security Center" Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan Institute of State and Legal History of the Academy of Sciences of the Republic of Uzbekistan Representatives of the Research Institute for the Development of Digital Technologies and Artificial Intelligence
The time allotted for the lecture:	up to 10 minutes
Event format:	Hybrid (online/offline)
Event language	Uzbek , English , Russian .

"Cyber law: problems and development prospects" international scientific-practical conference

PROGRAM

09:00 – 09:30	**Registration of participants**
10:00 – 10:10	**Introduction** **Kolenko Yevgeniy Vyacheslavovich –** First Deputy Head of Academy of Law Enforcement, Doctor of Philosophy in Legal Sciences, Associated Professor
10:10 – 10:20	**Introduction** **Shushikova Gulnar Karbaevna -** Vice-Rector-Director of the Interagency Research Institute of the Law Enforcement Academy under the General Prosecutor's Office of the Republic of Kazakhstan
Moderator: Nazarov Farkhodjon Abduvakhabovich - Head of the Department of Rapid Search and Cyber Law of the Academy of Law Enforcement	
10:20 – 10:30	*Cybercrime and Cyberlaw* **Naeem AllahRakha** is an international lawyer, teacher of the Department of Cyber Law of Tashkent State Law University
10:30 – 10:40	*Strategies for Enforcement of Cyber Laws* **Purvi Pokhariyal** - Professor, National Forensic Science University of India
10:40 – 10:50	*Presentation of the "Cyber Law" textbook: formation of digital legal education in Uzbekistan* **Gulyamov Said Saidakhrarovich -** doctor of legal sciences, professor, head of the Department of Cyber Law of Tashkent State Law University
10:50 – 11:00	*New approaches to improving the organizational and legal foundations of the digital transformation of the prosecutor's office* **Boboev Mirshod Murotovich -** Head of the Department of Information and Communication Technology Implementation and Information Security of the General Prosecutor's Office of the Republic of Uzbekistan, Doctor of Philosophy in Legal Sciences
11:00 – 11:10	*Training of personnel in the field of cyber law: opportunities and prospects for cooperation*

	Nazarov Farkhodjon Abduvakhabovich - Head of the Department of Rapid Search and Cyber Law of the Academy of Law Enforcement
11:10 – 11:20	*Prospects of using opportunities of international cooperation in the field of cyber security in the fight against cyber crimes* **Ubaydullayev Qudratilla Khabibullayevich** - Higher School of Strategic Analysis and Prospecting of the Republic of Uzbekistan, Doctor of Political Sciences.
11:20 – 11:30	*Predictive Justice: Ensuring a Just, fair and Reasonable Approach to legal Decision-Making* **Navtika Singh Nautiyal** – Assistant Professor, National Forensic Sciences University, Delhi Campus
11:30 – 11:40	*Aktualnye problemy training personnel in the sphere of cyber security* **Davlatov Zafar Ravshanovich** – Head of the Department of Partnership Development and Sponsorship At Inha University in Tashkent
11:40 - 11:50	*Research activities in the field of digital forensics* **Musayev G'ayrat Farxadovich** – Head of Research Institute of Digital Forensics
11:50 – 12:10	***Coffee- Break***
12:10 – 12:20	*Types of cybercrimes, social danger and issues of qualification* **Akhrorov Bakhrom Djabbarovich** - Professor of the "Criminal and Legal Sciences" Department of Public Security University, Doctor of Legal Sciences, Professor
12:20 - 12:30	*Misinterpretation of AI decisions* *problems: from algorithmic uncertainty to human rights* **Sobirov Shokhrukhbek Tavakkalovich**- chief researcher of the Department of Legislation in the Social Sphere of the Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan
12:30 - 12:40	*AI-Driven Web Security: NLP-Based Log Analysis in Firewalls*

	Aliev Abdurahmon Farkhodovich- associate professor of Automatic Control and Computer Engineering Department, Polytechnic University of Turin in Tashkent , yu.ffd(PhD)
12:40 – 12:50	*The concept, essence and characteristics of crypto-assets.* **Azizkhanov Shahrukh Madilkhanovich** - employee of the Ministry of Internal Affairs' Rapid Search Department, Cyber Security Center.
12:50 – 13:00	*Techniques for detecting network attacks based on deep change* **Ramozonova Madina Shavkatovna** - Assistant of the Department of "Cyber Security and Criminalistics" of TATU named after Muhammed al-Khorazmi
13:00 – 13:10	*An innovative approach to the development of crime detection and prevention systems using video images with the help of artificial intelligence technologies* **Boytemirov Asror Makhammadostovich -** Head of Department of "Artificial Intelligence" TATU named after Muhammed al-Khorazmi
13:10 - 13:20	**Sagimbekov Bakhitzhan Jasamuratovich** - chief researcher of the Center for the Study of Criminal-Procedural Problems of the Interagency Research Institute of the Law Enforcement Academy under the General Prosecutor's Office of the Republic of Kazakhstan
13:20 – 13:30	**Sodikov Mukhtar Beibutovich -** teacher of the Department of "General Law Sciences" of the Institute of Postgraduate Education of the Academy of Law Enforcement under the General Prosecutor's Office of the Republic of Kazakhstan
13:30 - 13:50	**Questions and answers for discussion**
1 3:50	**End the conference**

Kiberhuquq: muammolar va rivojlantirish istiqbollari.
Xalqaro ilmiy-amaliy konferensiya ishiga oid fotolavhalar^

КИБЕРПРАВО:
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИ
ГУЛЯМОВ САИД
КОЛЕНКО ЕВГЕНИЙ
БОБОЕВ МИРШОД

CYBER LAW:
PROBLEMS AND DEVELOPMENT PROSPECTS

СОБИРОВ
ШОХРУХБЕК
ДАВЛАТОВ
ЗАФАР

MUNDARIJA

S.I.Samadov. Prokuratura organlarining korrupsiyaga qarshi kurashish faoliyatida sun'iy intellekt imkoniyatlaridan foydalanishning ayrim masalalari 4-9
Е.В.Коленко. Перспективы использования искусственного интеллекта в сфере охраны правопорядка.....9-17
M.M.Boboev. Prokuratura organlari faoliyatini raqamli transformasiya qilishning tashkiliy-huquqiy asoslarini takomillashtirish.....17-23
Naeem AllahRakha. Cybercrime and Cyber Law.....24-35
M.M.Mamasiddiqov. Ilmiy faoliyatda sun'iy intellektdan foydalanishning dolzarb masalalari 35-41
F.A.Nazarov. Kiberhuquq sohasida kadrlar tayyorlash: Imkoniyatlar va hamkorlik istiqbollari.....41-50
A.A.Turg'unov. Внедрение искусственного интеллекта в систему электроного уголовного дела в Узбекистане.....50-56
J.R.Shukurov. Kibejinoyatchilik va boshqa turdagi jinoyatlarga qarshi kurashda sun'iy intellekt: imkoniyatlar va huquqiy cheklovlar, erishish mumkin bo'lgan natijalar.....56-63
Q.X.Ubaydullayev. Kiberxavfsizlik sohasidagi xalqaro hamkorlik imkoniyatlaridan kiberjinoyatlarga qarshi kurashda foydalanish istiqbollari.....64-70
A.Aliyev, N.Makhamatov. AI-Driven Web Security: NLP-Based Log Analysis inFirewalls.....71-74
J.K.Ataniyazov, SH.M.Azizxonov. Kripto aktivlar tushunchasi, mazmun-mohiyati va o'ziga xos xususiyatlari.....75-83
Sh.R.G'ulomov, M.Sh. Ramazonova. Teran o'rganishga asoslangan tarmoq hujumlarini aniqlash usullari.....83-88
B.R.Azimov, J.N.Nurmurodov, A.M.Boytemirov. Sun'iy intellekt texnalogiyalari yordamida video tasvirlardan foydalanib jinoyatlarni aniqlash va oldini olish tizimlarini yaratish.....89-95
H.X.Mamirov, A.M.Boytemirov, S.Sh.Qobilov. Proposal of Smart Home Security System using Raspberry Pi 4.....95-103
J.K.Ataniyazov, M.A.Sodiqov. Raqamli dalil. Ekstremizm bilan bog'liq jinoyatlarga qarshi kurashishdagi raqamli dalillarning o'rni.....103-107
B.X.Rajabov. Kiberjinoyatlarga qarshi kurashishda prokuror-kriminalistlarning o'rni.....107-113
M.E.Kamolov. Axborot texnologiyalari soxasida kiberxavfsizlikni ta'minlash va qo'llash.....114-117

D.O.Oblaqulov. Kriptoaktivlarni tijoratda pora evaziga og'dirib olish jinoyatning predmetisifatida tan olish muammolari……..117-127
D.A.Mirzaxodjaev. Giyohvandlik vositalari va psixotrop moddalar bilan qonunga xilof ravishda muomala qilish jinoyatlarining o'ziga xos xususiyatlari……127-132
I.I.Karimov. Diniy ekstremistk tashkilotlar tomonidan kibermakonda sodir etilayotgan jinoyatlarni tergov qilishning ayrim jihatlari…..132-139
A.I.Abdullayev Guvohning yoki jabrlanuvchining bila turib yolg'on ko'rsatuv berishini bartaraf etishda sun'iy idrok imkoniyatlaridan foydalanish masalalari..... 139-144
B.J.Axrorov, A.R.Murodov. Zararli dasturlar yordamida sodir etilayotgan kiberjinoyatlar……144-148
A.A.G'aniyev, D.X.Tojimatov. Kibermakonda potensial tahdidlarni aniqlashda kiberrazvedka amaliyotining usul va vositalari……149-158
A.A.Iminov., M.E.Kamolov., J.T.Mamatjonov. Kiberxavfsizlikning ichki ishlar organlari tizimida tutgan o'rni va kiber jinoyatlarni oldini olish……159-163
K.F.Kerimov, Z.I.Azizova. Information security risk assessment of e-resources under physical threats ……163-168
K.F.Kerimov, Z.I.Azizova. Methodology of information security risk assessment of electronic resources derived from attributes of protection objects under physical threats……168-177
M.O.Khasanov. Detecting and combating corruption at the state level usingdigital technologies ……177-181
B.O.Yumatov. Prospects for the use of modern digital technologies in the framework of anti-corruption monitoring……181-185
A.U.Aliyev. Cybersecurity threats and solutions……186-191
R.X.Maxamadov, M.X.Djamatov. Kiberterrorizm va unga qarshi kurashishdagi muammolar va yechimlar……191-195
I.F.Zoirova. The importance of modern technologies in ensuring the rights and legal interests of juvenile victims in criminal proceedings……195-199
A.A.Iminov, R.X.Maxamadov. Kiberjinoyatlar va ularga qarshi kurashishning o'ziga xos xususiyatlari……199-204
K.M.Abdurakhmatova. Digital construction-as a factor in successful anti-corruption activities……204-208
A.A.Abdiraximov. Kiberbulling - yoshlar ongiga ta'siri……208-212
N.E.Mahamatov, J.R.Rahimov. Cybersecurity challenges in real-time navigation systems for autonomous vehicles……212-216

J.D.Risqaliyev. Kiberjinoyatchilikning rivojlanishida darknetning o'rni……..216-220
E.D.Haydarov. Kibermakonda intellectual mulk huquqlarini himoya qilish……..220-227
B.I.Ismailov, G.A.Rasulova. Strengthening academic priority standards as an instrument to against corruption in the field of scientific and education……..228-235
A.B.Sabirbayeva. Особенности преступлений, совершенных в киберпространстве……..236-243
A.Mavlonov. Yaratilayotgan imkoniyatlar eng avvalo fuqarolarning huquq va erkinliklarini muhofaza qilishga xizmat qilmog'i lozim……..244-248
A.Zulfuqorov. Innovatsion texnologiyalar yordamida sud-ekspertlik faoliyatini takomillashtirish……..248-257
F.B.Bobomurodov. Kiberjinoyatlarga qarshi kurashishning huquqiy asoslari tahlili……..258-265
M.M.O'rinboyeva., F.Y.Abdufattoyev. Sud ishlarini yuritishda sun'iy intellektdan foydalanishning tushunchasi, ahamiyati, zarurati va retrospektiv tahlili……..265-273
M.M.Abduraxmanov. Xorijiy mamlakatlarda mayning va kripto aktivlardan foydalanishning huquqiy tartibi……..274-282
B.B.Qudratov. Raqamli dalillarning axborot-kommunikatsiya sohasidagi zamonaviy jinoyatlarni tergov qilish va fosh etishdagi o'rni……..283-285
V.Karimov, A.A.Tashtemirov. Axborot texnalogiyalaridan foydalanib sodir etilgan firibgarlikni fosh etishning ayrim jihatlari……..286-294
B.T.Ibroximov. Prokurorning nazorat vakolatlarini o'zgarishi bilan bog'liq bazi mulohazalar (jinoyat protssesi misolida) ……..294-301
A.A.Tashtemirov. Axborot texnalogiyalari orqali sodir etilgan firibgarlik jinoyatlarini fosh etishda hamkorlik masalalari……..301-309
I.A.Ochilov. Giyohvandlik vositalarini kontaktsiz usulda o'tqazishni aniqlash va fosh etish bo'yicha o'tqaziladigan tezkor-qidiruv tadbirlari xususiyatlari……..309-318
A.S.Qaxramonov. Облачные данные: основы исследования….318-321
G'.M.Shodiyev. Jinoyat protsessida reabilitasiya etish sohasida prosessual va prokuror nazorati (qiyosiy tahlil) ……..321-326
I.Abdikhakimov. Assessing accountability mechanisms for quantum technology in financial sectors……..326-331
J.Eshonkulov. Smart Contracts as the Future of Legal Automation: Prospects and Limitations……..332-339

N.X.Inoyatov. Kiber huquqda shaxsiy ma'lumotlar himoyasi: muammolar va yechimlar……..340-345
K.X.Davletova. Zamonaviy iqtisodiy sud ish yurituvida sun'iy intellekt elementlaridan foydalanishning protsessual shakllari……..345-353
M.M.Abduraxmanov. Mayning va kripto aktivlarning huquqiy asoslari: milliy va xorijiy tajriba 354-363
F.Y.Abdufattoyev. Amerika qo'shma shtatlari, Xitoy va Koreya misolida sun'iy intellektdan foydalanish masalalari 364-369
G.A.Azamova. Prospects of using modern technologies in the criminal proceedings 370-376
Э.К.Сабиров. Судда иш кўришнинг очиқлигини таъминлашда сунъий интеллект имкониятларидан фойдаланишнинг айрим масалалари 377-383

"Kiberhuquq: muammolar va rivojlantirish istiqbollari" mavzusidagi xalqaro ilmiy-amaliy konferensiya dasturi……..384-395
Fotolavhalar…… 396-398
Mundarija……..399-402