

KIBERJINOYATLARNING TEXNOLOGIK XUSUSIYATLARI VA ULARNING IJTIMOIIY, IQTISODIY VA SIYOSIY TA'SIRI

TECHNOLOGICAL CHARACTERISTICS OF CYBERCRIME AND ITS SOCIAL, ECONOMIC, AND POLITICAL IMPACTS

ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ КИБЕРПРЕСТУПНОСТИ И ЕЁ СОЦИАЛЬНОЕ, ЭКОНОМИЧЕСКОЕ И ПОЛИТИЧЕСКОЕ ВЛИЯНИЕ

Sherqulov Sanjar Alisherovich

(O'zbekiston Respublikasi IIV Akademiyasi kursanti)

Iminov Abdurasul Abdulatipovich

(O'zbekiston Respublikasi IIV Akademiyasi

Raqamli texnologiyalar va axborot xavfsizligi kafedrası boshlig'i)

Annotatsiya: Ushbu maqolada bugungi global raqamli ekotizimda kiberjinoyatlarning texnologik transformatsiyasi, ularning rivojlanish tendensiyalari hamda jamiyat hayotining turli jabhalariga o'tkazayotgan ko'p qirrali salbiy oqibatlari tahlil qilinadi. Zamonaviy kibertahdidlar shunchaki texnik hodisa yoki oddiy dasturiy hujum bo'lmay, balki geosiyosiy, huquqiy, ijtimoiy va iqtisodiy miqyosda chuqur asoratlarni yuzaga keltiruvchi murakkab tizimga aylanganligi asoslab berilgan. IoT qurilmalari, bulutli tizimlar, 5G texnologiyalari, sun'iy intellekt va kriptotexnologiyalarning jadal rivojlanishi kiberjinoyatlarni yanada xavfli va noaniq shakllarga olib kelayotgani yoritilgan. Global miqyosdagi ushbu transformativ tahdidga samarali qarshi turish uchun malakali kadrlar tayyorlash, raqamli savodxonlik va kibermadaniyatni yuksaltirish, transmilliy hamkorlikni mustahkamlash hamda huquqiy standartlarni takomillashtirish kabi strategik tavsiyalar ilgari surilgan.

Kalit so'zlar: Kiberjinoyat, kibermakon, kiberxavfsizlik, raqamli tahdidlar, sun'iy intellekt, ijtimoiy muhandislik, iqtisodiy zarar, geostrategik maqsadlar, huquqiy tartibga

solish, xalqaro tajriba, raqamli jamiyat, kiberhujumlar, kiberfiribgarlik, ma'lumotlarni himoya qilish, kiberqonunchilik.

Abstract: This article analyzes the technological transformation of cybercrime in today's global digital ecosystem, its development trends, and its multifaceted negative impacts on various spheres of social life. It substantiates that modern cyber threats are no longer merely technical phenomena or simple software attacks, but have transformed into a complex system causing profound consequences in geopolitical, legal, social, and economic dimensions. The study highlights that the rapid advancement of the Internet of Things (IoT), cloud systems, 5G technologies, artificial intelligence, and cryptographic technologies is driving cybercrime toward increasingly dangerous and ambiguous forms. To effectively counter this global transformative threat, strategic recommendations such as training qualified specialists, enhancing digital literacy and cyberculture, strengthening transnational cooperation, and improving legal standards are proposed.

Keywords: Cybercrime, cyberspace, cybersecurity, digital threats, artificial intelligence, social engineering, economic damage, geostrategic goals, legal regulation, international experience, digital society, cyberattacks, cyberfraud, data protection, cyberlaw.

Аннотация: В данной статье анализируются технологическая трансформация киберпреступности в современной глобальной цифровой экосистеме, тенденции её развития и многоаспектное негативное влияние на различные сферы жизни общества. Обосновано, что современные киберугрозы перестали быть чисто техническим явлением или простой программной атакой, а превратились в сложную систему, вызывающую глубокие последствия в геополитическом, правовом, социальном и экономическом измерениях. Осмыслено, что стремительное развитие Интернета вещей (IoT), облачных систем, технологий 5G, искусственного интеллекта и криптографических технологий приводит к появлению всё более опасных и неопределённых форм киберпреступности. Для эффективного противодействия этой глобальной трансформационной угрозе выдвинуты такие стратегические рекомендации, как подготовка квалифицированных кадров,

повышение цифровой грамотности и киберкультуры, укрепление транснационального сотрудничества и совершенствование правовых стандартов.

Ключевые слова: Киберпреступность, киберпространство, кибербезопасность, цифровые угрозы, искусственный интеллект, социальная инженерия, экономический ущерб, геостратегические цели, правовое регулирование, международный опыт, цифровое общество, кибератаки, кибермошенничество, защита данных, киберзаконодательство.

Bugungi global raqamli ekotizimda axborot texnologiyalari va kommunikatsiya vositalarining misli ko‘rilmagan darajada jadal rivojlanishi, Internetning universal global tarmoq sifatida hayotimizning barcha jabhalariga kirib borishi insoniyat taraqqiyoti uchun yangi ufqlar ochdi. Sun’iy intellekt tizimlari, bulutli hisoblash platformalari, katta ma’lumotlar bazalari (Big Data) hamda blokcheyn texnologiyalarining ommalashuvi nafaqat davlat boshqaruvi va iqtisodiyotni modernizatsiya qildi, balki ijtimoiy munosabatlarning virtual makonga ko‘chishini ta’minladi. Biroq, ushbu global raqamli transformatsiya o‘zi bilan birga an’anaviy jinoyatchilikning ham jiddiy evolutsiyasini va uning kibermakonga to‘liq moslashishini boshlab berdi. Zamonaviy kiberjinoyatchilik bugungi kunda shunchaki dasturiy ta’minot yoki kompyuter tizimlariga qarshi qaratilgan texnik hodisa doirasidan chiqib, geosiyosiy, huquqiy, iqtisodiy va ijtimoiy o‘lchamlarga ega bo‘lgan o‘ta murakkab, tizimli va transmilliy tahdidga aylandi. Ushbu global transformatsiyaning mohiyatini anglash uchun birinchi navbatda kiberjinoyatlarning o‘ziga xos texnologik xususiyatlarini va ularning doimiy o‘zgaruvchan tendensiyalarini chuqur tahlil qilish lozim.

Zamonaviy kiberjinoyatlarning texnologik tabiati uning ko‘p qirrali, yuqori darajada avtomatlashtirilgan va kombinatsiyalashgan tabiati bilan xarakterlanadi. An’anaviy kiberhujumlar, masalan, ommaviy ravishda "soxta elektron xatlar yuborish" (fishing) kabi ibtidoiy shakllardan voz kechib, bugungi kunda sun’iy intellekt imkoniyatlaridan maksimal darajada foydalangan holda shakllantirilayotgan individuallashtirilgan ijtimoiy muhandislik hujumlariga aylanib ulgurdi. Jinoyatchilar endilikda maqsadli qurbonlarning xatti-harakatlarini, qiziqishlarini va zaif nuqtalarini real vaqt rejimida avtomatlashtirilgan

tizimlar yordamida tahlil qilib, ularga qarshi rad etib bo'lmaydigan virtual tuzoqlarni tayyorlamoqdalar. Sun'iy intellekt, shuningdek, tarmoqlar va operatsion tizimlardagi tizimli zaifliklarni (vulnerabilities) inson omilisiz, soniyalar ichida aniqlash va o'sha zaifliklardan foydalangan holda tizimga suqulib kirish imkonini bermoqda. Bunga qo'shimcha ravishda, Deepfake (soxta video va audio kontent yaratish) texnologiyalarining misli ko'rilmagan darajada mukammallashuvi shaxsni obro'sizlantirish, yuqori lavozimli shaxslar nomidan soxta buyruqlar berish va murakkab jinoiy aldovlar orqali strategik ma'lumotlarni qo'lga kiritish uchun xizmat qilayotgan asosiy texnologik kuchaytiruvchi omillardan biridir. Texnologik zanjirning yana bir xavfli yo'nalishi Internet buyumlari (IoT — Internet of Things), 5G tarmoqlari hamda bulutli (Cloud) serverlarning ommaviy infratuzilmaga aylanishi bilan bog'liq. "Aqlli uy" qurilmalari, masofaviy kameralar, datchiklar va maishiy aqlli texnikalar ko'pincha ishlab chiqarish jarayonida mukammal xavfsizlik protokollari va shifrlash tizimlari bilan ta'minlanmaganligi sababli, kiberjinoyatchilar uchun global tarmoqlarga suqulib kirishning ochiq eshigi bo'lib xizmat qilmoqda. Bulutli serverlar esa o'zida trillionlab korporativ, shaxsiy va davlat miqyosidagi maxfiy ma'lumotlarni jamlaganligi sababli kiberhujumchilarning markaziy nishoniga aylandi. Mazkur texnologik jarayonlar va ularning rivojlanish tezligi amaldagi kiberxavfsizlik mexanizmlarining va an'anaviy huquqiy normalarning juda tez eskirishiga olib kelmoqda, bu esa qonunchilik tizimi oldiga ulkan chaqiriqlar qo'ymoqda.

Kiberjinoyatchilikning texnologik jihatdan bunday mukammallashuvi uning ko'p tarmoqli salbiy oqibatlarini keltirib chiqarmoqda, bular orasida iqtisodiy ta'sir ko'lami eng birinchi navbatda ko'zga tashlanadi. Dastlabki davrlarda kiberhujumlar faqatgina individual hisob raqamlaridan pul o'g'irlash yoki kichik iqtisodiy zarar yetkazish bilan cheklangan bo'lsa, hozirgi davrda moliyaviy institutlar, yirik korporatsiyalar va FinTech (moliyaviy texnologiyalar) ekotizimi tizimli xavf ostida qolmoqda. Raqamli hamyonlar, onlayn kredit platformalari va mobil to'lov tizimlarining kundalik hayotga keng joriy etilishi, aholining kiber-savodxonligi pastligi sharoitida jinoyatchilar uchun misli ko'rilmagan iqtisodiy daromad manbaini yaratdi. Bundan tashqari, xalqaro miqyosda

kriptovalyutalarning ommalashuvi kiberjinoyatlarning moliyaviy ko'rinishini butunlay o'zgartirdi. Blokcheyn texnologiyasi o'z tabiatiga ko'ra tranzaksiyalarning shaffofligini ta'minlasa-da, kiberjinoyatchilar tranzaksiyalarni anonimlashtiruvchi maxsus mikser xizmatlari (kripto-miksyerlar) va anonim hamyonlardan foydalangan holda jinoiy daromadlarni legallashtirishmoqda va pul mablag'larini xalqaro miqyosda kuzatishni imkonsiz darajaga keltirishmoqda. Ayrim maqsadli va yuqori darajada uyushgan kiber-guruhlar tomonidan bank tarmoqlariga uyushtirilayotgan nishonli hujumlar global iqtisodiyotga milliardlab dollar zarar yetkazishga qodir ekanligi amaliyotda isbotlangan.

Iqtisodiy zararlar bilan bir qatorda, kiberjinoyatchilikning chuqur ijtimoiy ta'siri va oqibatlari jamiyat barqarorligiga rahna solmoqda. Ushbu transformativ jarayondagi eng zaif xalqqa — inson omilidir. Jamiyatning barcha qatlamlarida, ayniqsa internet makonida eng faol bo'lgan yoshlar orasida raqamli xavfsizlik bo'yicha fundamental bilimlarning yetishmasligi va kibermadaniyatning sustligi juda ayanchli oqibatlarga olib kelmoqda. Shaxsiy ma'lumotlarga nisbatan e'tiborsizlik, ijtimoiy tarmoqlarda haddan tashqari ishonuvchanlik, parollarning o'ta soddaligi va ularni himoya qilish madaniyatining yo'qligi sababli millionlab fuqarolar kiberfiribgarlikning bevosita qurboniga aylanmoqda. Shaxsga doir ma'lumotlarning ommaviy ravishda o'g'irlanishi, raqamli shaxsiyatning tortib olinishi, kiberbulling (virtual tazyiq) va onlayn tovlamachilik holatlari insonlarda ruhan tushkunlik, jamiyatda raqamli infratuzilmaga nisbatan umumiy ishonchsizlik va tizimli ijtimoiy xavovot muhitini shakllantirmoqda. Fuqarolarning shaxsiy daxlsizligi virtual olamda himoyasiz qolishi ijtimoiy davlat tamoyillariga to'g'ridan-to'g'ri tahdid soladi.

Ushbu iqtisodiy va ijtimoiy xavflarning eng yuqori nuqtasi kiberjinoyatchilikning siyosiy va geostrategik ta'sirida namoyon bo'ladi. Zamonaviy geosiyosiy qarama-qarshiliklar sharoitida kiberhujumlar shunchaki moddiy manfaat orttirish vositasi emas, balki davlatlararo yashirin urushlar va siyosiy bosim o'tkazish mexanizmiga aylandi. Bugungi kunda yirik xalqaro kompaniyalar, davlat hokimiyati idoralari hamda eng muhimi — strategik ahamiyatga ega bo'lgan kritik infratuzilma obyektlari (energetika tizimlari, atom elektrostansiyalari, harbiy boshqaruv tarmoqlari, transport va logistika markazlari)

tizimli kiberhujumlarning bosh nishoni hisoblanadi. Bir davlat hududida jismonan o‘tirgan holda, minglab kilometr uzoqlikdagi boshqa suveren davlatning hayotiy muhim tizimlarini ishdan chiqarish, siyosiy barqarorlikni buzish va strategik axborotlarni o‘g‘irlash imkoniyati kibermakonning chegarasiz (borderless) ekanligini anglatadi. Bu esa milliy xavfsizlik va mudofaa tushunchalarini tubdan qayta ko‘rib chiqishni talab etmoqda.

Kiberjinoyatchilikning ushbu texnologik evolutsiyasi va uning transmilliy, chegarasiz xarakteri mavjud milliy va xalqaro huquq tizimlari uchun misli ko‘rilmagan qiyinchiliklarni yuzaga keltirmoqda. Kiberjinoyatchilar muayyan bir davlat qonunchiligidagi bo‘shliqlardan unumli foydalangan holda, o‘zlari uchun huquqiy ta‘qib mavjud bo‘lmagan yoki ekstraditsiya shartnomalari ishlamaydigan “qulay yurisdiksiyalarga” o‘tib olishmoqda, bu esa xalqaro qidiruv va sud jarayonlarini o‘ta murakkablashtirmoqda. Shu sababli huquqiy amaliyotda jiddiy yuridik kolliziyalar (qaysi davlat qonuni qo‘llanilishi, raqamli dalillarni qanday qilib qonuniy rasmiylashtirish va xalqaro miqyosda tan oldirish kabilar) yuzaga kelmoqda. Har bir davlatning o‘ziga xos texnik va jinoyat-protsessual standartlari mavjudligi hamda xalqaro miqyosda majburiy bo‘lgan yagona, universallashtirilgan huquqiy normalarning yetishmasligi kiberjinoyatchilikka qarshi kurash samaradorligini pasaytirmoqda.

Xulosa qilib aytganda, global raqamli asr taqdim etayotgan cheksiz imkoniyatlardan xavfsiz va barqaror foydalanish uchun kiberjinoyatchilikning ushbu transformativ tendensiyalarini chuqur ilmiy va amaliy jihatdan tahlil qilish hayotiy zaruriyatdir. Ushbu global tahdidga samarali qarshi turish uchun davlatlar va xalqaro hamjamiyat faqatgina texnik choralarni ko‘rish bilan cheklanib qolmasligi kerak. Bu jarayon kiberxavfsizlik sohasida yuqori malakali, zamonaviy fikrlaydigan kadrlar tayyorlashga sarmoya kiritishni, jamiyatning barcha qatlamlarida raqamli savodxonlik va kibermadaniyatni tizimli ravishda yuksaltirishni talab etadi. Shu bilan birga, milliy qonunchilik tizimlarini takomillashtirish, raqamli dalillar bilan ishlashning protsessual asoslarini mustahkamlash hamda sun‘iy intellekt va blokcheyn kabi ilg‘or texnologiyalarga asoslangan milliy himoya tizimlarini faol joriy etish lozim. Eng asosiysi, kiberjinoyatchilikning chegarasiz tabiatini inobatga olgan holda, transmilliy hamkorlikni mustahkamlash va xalqaro huquqiy standartlarni

birlashtirish kelajakda global va milliy kiberxavfsizlikni ta'minlashning eng muhim va hal qiluvchi sharti bo'lib qoladi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi Konstitutsiyasi. – Toshkent, 2023;
2. O'zbekiston Respublikasi Jinoyat kodeksi. – Toshkent: Adliya vazirligi nashriyoti, 2023;
3. O'zbekiston Respublikasi “Axborotlashtirish to'g'risida”gi Qonuni (2003 yil 11 dekabr);
4. O'zbekiston Respublikasi “Shaxsga doir ma'lumotlar to'g'risida”gi Qonuni (2019 yil 2 iyul);
5. Ro'ziyev R.N., Salayev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar: monografiya. — Toshkent: TDYU, 2018;
6. Anorboyev A.U. Kiberjinoyatlarning jinoiy-huquqiy jihatlar: dissertatsiya. — Toshkent, 2020.