

KIBERJINOYATLARNING RIVOJLANISH TENDENSIYALARI VA ULARNING TAHLILI

TRENDS IN CYBERCRIME DEVELOPMENT AND THEIR ANALYSIS

ТЕНДЕНЦИИ КИБЕРПРЕСТУПНОСТИ И ИХ АНАЛИЗ

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)

<https://doi.org/10.5281/zenodo.18830898>

Annotatsiya: Ushbu maqolada bugungi global raqamli ekotizimda kiberjinoyatlar misli ko'rilmagan darajada rivojlanib borayotgani, ularning faqat texnik hodisa emas, balki geosiyosiy, huquqiy, ijtimoiy va iqtisodiy miqyosda murakkab tizimga aylanayotgani yoritilgan. IoT (internetga ulangan qurilmalar), bulutli tizimlar, 5G texnologiyalari, sun'iy intellekt va kriptotexnologiyalarning jadal rivojlanishi kiberjinoyatlarni yanada xavfli va noaniq shakllarga olib kelayotgani asoslab berilgan. Shu sababli davlatlar va xalqaro hamjamiyat oldida malakali kadrlar tayyorlash, raqamli savodxonlik va kibermadaniyatni yuksaltirish, transmilliy hamkorlikni mustahkamlash, zamonaviy texnika va texnologiyalar hamda huquqiy standartlarni takomillashtirish kabi dolzarb vazifalar turgani ta'kidlangan. Kiberjinoyatlarning rivojlanish tendensiyalarini chuqur tahlil qilish hamda ularning oldini olish va ularga qarshi kurashish strategiyalarini ishlab chiqish kelajakda kiberxavfsizlikni ta'minlashning muhim sharti ekanligi xulosalangan.

Kalit so'zlar: Kiberjinoyat, kibermakon, kiberxavfsizlik, raqamli tahdidlar, kiberhuquq, axborot xavfsizligi, huquqiy tartibga solish, xalqaro tajriba, texnologik xavfsizlik, raqamli jamiyat, kiberhujumlar, kiberfiribgarlik, ma'lumotlarni himoya qilish, elektron infratuzilma, onlayn jinoyatchilik, shaxsiy ma'lumotlar xavfsizligi, kiberqonunchilik, axborot tizimlari, strategik kiberxavfsizlik.

Abstract: This article highlights that cybercrime in today's global digital ecosystem is developing at an unprecedented pace, transforming from a purely technical phenomenon into a complex system encompassing geopolitical, legal, social, and economic dimensions. It substantiates 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. In this context, it is emphasized that states and the international community face urgent tasks such as training qualified specialists, enhancing digital literacy and cyberculture, strengthening transnational cooperation, and improving modern technologies and legal standards. The study concludes that an in-depth analysis of cybercrime development trends, along with the formulation of strategies for its prevention and counteraction, constitutes a crucial prerequisite for ensuring cybersecurity in the future.

Keywords: Cybercrime, cyberspace, cybersecurity, digital threats, cyberlaw, information security, legal regulation, international experience, technological security, digital society,

cyberattacks, cyberfraud, data protection, electronic infrastructure, online crime, personal data security, information systems, strategic cybersecurity.

Аннотация: В статье показано, что киберпреступность в современной глобальной цифровой экосистеме развивается беспрецедентными темпами, превращаясь из сугубо технического явления в сложную систему, охватывающую геополитические, правовые, социальные и экономические измерения. Обосновано, 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. В этой связи подчёркивается, что перед государствами и международным сообществом стоят актуальные задачи подготовки квалифицированных кадров, повышения цифровой грамотности и киберкультуры, укрепления транснационального сотрудничества, а также совершенствования современных технических средств, технологий и правовых стандартов. Сделан вывод о том, что глубокий анализ тенденций развития киберпреступности и разработка стратегий её предупреждения и противодействия являются важнейшим условием обеспечения кибербезопасности в будущем.

Ключевые слова: Киберпреступность, киберпространство, кибербезопасность, цифровые угрозы, киберправо, информационная безопасность, правовое регулирование, международный опыт, технологическая безопасность, цифровое общество, кибератаки, кибермошенничество, защита данных, электронная инфраструктура, онлайн-преступность, безопасность персональных данных, киберправо, информационные системы, стратегическая кибербезопасность.

Raqamli texnologiyalar va axborot-kommunikatsiya texnologiyalarining rivojlanishi, Internetning global tarmoq sifatida keng quloch yoyishi, sun'iy intellektning rivojlanishi, bulutli hisoblash tizimlarining, katta ma'lumotlar bazalarining va blokcheyn texnologiyalarining ommalashuvi nafaqat jamiyatning iqtisodiy, ijtimoiy va siyosiy jabhalarini rivojlantirishga yangi imkoniyatlar yaratdi, balki jamiyatda kiberjinoyatlarning ham rivojlanishiga misli ko'rilmagan darajada ta'sir qildi. Bugungi kunda sodir etilayotgan kiberjinoyatlarning turlari, usullari va mazmuni an'anaviy jinoyatlardan tubdan farq qiladi. Ular an'anaviy doiradan chiqib, ko'p qirrali, texnologik va yuqori darajada avtomatlashtirilgan shakllarga ega. Hozirgi kunda kiberjinoyatlarda kombinatsiyalashgan va ko'p bosqichli hujumlar kengaydi, ya'ni fishing endi oddiy "soxta xatlar yuborish"dan iborat emas. Ular sun'iy intellekt imkoniyatlaridan maksimal darajada foydalangan holda, o'z "o'lja"lariga individuallashtirilgan shakllarga ega ijtimoiy muhandislik usullari yordamida hujum qilishmoqda.

Kiberjinoyatlar ko'proq iqtisodiy maqsadlar uchun sodir qilingan. Masalan, pulni o'g'irlash va maxfiy axborot shaklida iqtisodiy zarar yetkazishi mumkin. Hozirgi kunda moliyaviy manfaatlar bilan bir vaqtda geostrategik va siyosiy maqsadlar ham paydo bo'lmoqda. Katta kompaniyalar, davlat idoralari, strategik ahamiyatga ega bo'lgan infratuzilma obyektlari kiberhujumlarning asosiy nishoniga aylanib qolmoqda. Sun'iy intellekt ham so'nggi davrda zamonaviy kiberjinoyatchilikning asosiy kuchaytiruvchi omiliga aylanib bormoqda. Deepfake texnologiyalari yordamida ishlab chiqarilayotgan yolg'on kontentlar shaxsni obro'sizlantirish, firibgarlik va jinoiy aldovlar uchun xizmat qilmoqda. Zamonaviy texnologiyalar va sun'iy intellektning rivojlanishi natijasida kiberjinoyatchilar uchun zaifliklarni real vaqt rejimida

tahlil qilish imkoniyatlarini kengaytirmoqda. Ular tarmoqlarning qaysi nuqtalarida zaiflik mavjudligini tezda topishib, ulardan foydalanishmoqdalar. Ushbu jarayonlar huquq tizimlari uchun ham ulkan chaqiriq bo'lib, qonunchilik va normativ-huquqiy hujjatlarni qayta ko'rib chiqishni talab etadi.¹

Kiberjinoyatlarning eng sezilarli tendensiyalaridan biri sifatida ularning chegarasiz va transmilliy xarakteriligidir. Kiberjinoyatchilar bir davlat hududidan turib boshqa davlatning infratuzilmalari va boshqa obyektlariga zarar yetkazishi mumkin. Bu jarayon quyidagi muammolarni yuzaga keltirmoqdalar:

1. Yuridik kolliziyalar (ushbu holatda qaysi davlat qonuni qo'llanilishi yoki qo'lga kiritilgan shaxsiy ma'lumotlar qaysi davlat fuqarosiga tegishli ekanligi kabilar);

2. Xalqaro ekstraditsiya jarayonlarining murakkabligi (kiberjinoyatlarni sodir etuvchi shaxslar huquqdagi mavjud bo'shliqlardan foydalanib, o'ziga qulay yurisdiksiyalarga o'tmoqda);

3. Bir xil standartlarning yo'qligi (har bir davlatning texnik, jinoyat, jinoyat-protsessual va boshqa normativ-huquqiy hujjatlari mavjud bo'lib, ular bir-biridan farq qilmoqda).

Yuqoridagi muammolar yuzaga kelayotganligi sababli, xalqaro darajadagi konvensiyalar, standartlar, birlashtirilgan huquqiy mexanizmlarga ehtiyoj va talab ortib bormoqda.

So'nggi davrda xalqaro miqyosda elektron to'lovlar va kriptovalyutalarning ommalashuvi natijasida kiberjinoyatlarning moliyaviy ko'rinishini sezilarli darajada kengaytirdi. Bu jarayon quyidagi ko'rinishlarda namoyon bo'lmoqda:

- Kriptovalyutalardan jinoiy daromadlarni legallashtirishda foydalanilmoqda (blokcheynning shaffofligi mavjud bo'lsa-da, ularni anonimlashtiruvchi xizmatlar jinoyatchilar uchun qulay vositaligicha qolmoqda);

- Bank tarmoqlariga nishonli hujumlar ko'paymoqda (Ayrim kiberjinoyatlarni amalga oshiruvchi guruhlar milliardlab zarar yetkazishga qodir);

- FinTech (Moliyaviy texnologiyalar) xizmatlarining rivojlanishi (onlayn kredit, investitsiya platformalari, kriptovalyutalar, mobil to'lovlar, raqamli hamyonlar kabilar foydalanuvchilar uchun qulayligi, ammo kiberjinoyatchilar aholining kiber savodxonligi pastligidan foydalanib, ularga kirish imkoniyatini yaratmoqda).

Bundan tashqari tahdidlarning IoT (internetga ulanish imkoniyati mavjud qurilmalar), bulutli tizimlari va 5G texnologiyalari bilan bog'liqligi ham mavjud bo'lib, zamonaviy axborot – kommunikatsiya texnologiyalarining rivojlanishi natijasida kiberhujumlar faqat kompyuter va telefonlarga emas balki “Aqlli uy” qurilmalari, kameralar, sensorlar, smart TVlar xavfsizlik protokollariga ega emasligi sababli hujumlar uchun ochiqsigicha qolmoqda. Bulutli serverlar hujumchilarning markaziy nishoniga aylanib bormoqda. Sababi u yerda katta miqdordagi korporativ hamda shaxsiy ma'lumotlar saqlanadi.

Tadqiqotlar shuni ko'rsatmoqdaki, IoT qurilmalari (internetga ulanish imkoniyati mavjud qurilmalar), bulutli tizimlar (cloud systems), 5G texnologiyalari, sun'iy intellekt (AI) va kriptotexnologiyalarning jadal rivojlanishi kiberjinoyatlarga yangi, yanada xavfli va noaniq shakllar berayotganligi yorqin namoyon bo'lmoqda. Bu esa mavjud kiberjinoyatlarga qarshi kurashish mexanizmlarining tezda eskirishiga olib kelmoqda.

¹ Ro'ziyev R.N., Salayev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar: monografiya. — Toshkent: TDYU, 2018, 22-bet.

Hozirgi kunda kiberjinoyatlarning rivojlanishiga sabab bo'layotgan eng asosiy omillardan biri bu – aholining katta qismida raqamli xavfsizlik bo'yicha bilimlarning yetishmasligidir. Ayniqsa, yoshlarning ijtimoiy tarmoqlardan haddan tashqari ishonch bilan foydalanishi, shaxsiy ma'lumotlarga nisbatan e'tiborsizlik, ularni himoyalash madaniyatining sustligi, parollardan noto'g'ri foydalanish va ularning juda soddaligi, firibgarlar tomonidan ishlab chiqilayotgan usullarga tezda moslasha olmayotganligi kabi omillar ushbu turdagi jinoyatlarning ko'payishiga sabab bo'lmoqda.

Global miqyosdagi ushbu transformativ tahdidga samarali qarshi turish uchun davlatlar va xalqaro hamjamiyat oldida bir qator dolzarb vazifalar turgani ta'kidlanmoqda. Jumladan, kiberxavfsizlik sohasida malakali kadrlar tayyorlashga sarmoya kiritish, raqamli savodxonlikni hamda kibermadaniyatni jamiyatning barcha qatlamlarida izchil va tizimli yuksaltirish, kiberjinoyatlarning transmilliy xususiyatini inobatga olgan holda xalqaro va mintaqaviy hamkorlik tizimini har tomonlama mustahkamlash ustuvor ahamiyat kasb etmoqda. Bundan tashqari, kiberhujumlarga qarshi kurashishda zamonaviy texnika va texnologiyalarni (masalan, AIga asoslangan himoya tizimlari, blokcheyn texnologiyasi) faol joriy etish, shuningdek, kiberjinoyatlarni aniq ta'riflovchi, ularga qarshi samarali jazo choralarini belgilovchi va raqamli dalillar bilan ishlashning protsessual asoslarini mustahkamlovchi huquqiy standartlarni doimiy ravishda takomillashtirish zarurligini taqozo etmoqda.

Xulosa qilib aytganda, kiberjinoyatlarning rivojlanish tendensiyalarini chuqur ilmiy tahlil qilish hamda ularning sodir etilishini oldini olish va samarali kurashish bo'yicha strategik yondashuvlarni ishlab chiqish kelajakda barqaror kiberxavfsizlikni ta'minlashning eng muhim va hal qiluvchi shartlaridan biri bo'lib qoladi. Faqatgina kompleks, ko'p qirrali va dinamik yondashuv orqali biz raqamli asrning imkoniyatlaridan to'liq foydalana olamiz va uning xavf-xatarlaridan o'zimizni himoya qilishimiz mumkin.

Adabiyotlar, References, Литературы:

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.