

KIBERJINOYATLARGA QARSHI KURASHISHNING HUQUQIY ASOSLARINI TAKOMILLASHTIRISH

Maxmudov Muxammadalisher Mavludjonovich

Huquqni muhofaza qilish Akademiyasi

Magistratura fakulteti tinglovchisi.

<https://doi.org/10.5281/zenodo.17770356>

Annotatsiya. Ushbu maqola O'zbekiston Respublikasida kiberjinoyslarga qarshi kurashishning huquqiy asoslarini takomillashtirish masalalarini o'rganishga bag'ishlangan.

Maqolada milliy va xalqaro miqyosda kiberjinoysatchilik sohasidagi huquqiy tartibga solish mexanizmlarining hozirgi holati tahlil qilingan, huquqiy bazani modernizatsiya qilish bo'yicha takliflar ishlab chiqilgan. Tadqiqot natijalarida kiberjinoysatchilikka qarshi kurashishning huquqiy asoslarini mustahkamlash zarurligi asoslantirilgan.

Kalit so'zlar: kiberjinoysat, kiberhavfsizlik, huquqiy tartibga solish, axborot xavfsizligi, jinoys javobgarlik, raqamli jinoysatchilik, kiberhujumlar

Abstract. This article is devoted to the study of issues of improving the legal framework for combating cybercrime in the Republic of Uzbekistan. The article analyzes the current state of legal regulatory mechanisms in the field of cybercrime at the national and international levels, develops proposals for the modernization of the legal framework. The results of the study substantiate the need to strengthen the legal framework for combating cybercrime.

Keywords: cybercrime, cybersecurity, legal regulation, information security, criminal liability, digital crime, cyberattacks

Аннотация. Статья посвящена исследованию вопросов совершенствования правовых основ противодействия киберпреступности в Республике Узбекистан. В статье анализируется современное состояние механизмов правового регулирования в сфере киберпреступности на национальном и международном уровнях, разрабатываются предложения по модернизации правовой базы. Результаты исследования обосновывают необходимость укрепления правовых основ противодействия киберпреступности.

Ключевые слова: киберпреступность, кибербезопасность, правовое регулирование, информационная безопасность, уголовная ответственность, цифровая преступность, кибератаки.

KIRISH

Zamonaviy axborot texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalarini qamrab olgan bir paytda, kiberjinoysatchilik global xavfsizlikka tahdid sifatida tobora kuchayib bormoqda. Raqamli texnologiyalarning keng qo'llanilishi bilan bir qatorda, ushbu imkoniyatlardan noqonuniy foydalanish holatlari ham keskin ortib bormoqda. Butunjahon miqyosida kiberjinoysatlardan yetkazilgan iqtisodiy zarar yillik 6 trillion AQSh dollaridan oshib ketgan va bu raqam doimiy o'sish tendentsiyasiga ega [1]. O'zbekiston Respublikasi ham ushbu global jarayonlardan chetda qololmaydi va milliy kiberhavfsizlik tizimini mustahkamlash davlat siyosatining ustuvor yo'nalishlaridan biriga aylangan. Mamlakatimizda raqamli iqtisodiyotni rivojlantirish, elektron hukumat xizmatlarini joriy etish va axborot-kommunikatsiya texnologiyalarini barcha sohalarda keng qo'llash kiberjinoysatlarga qarshi samarali huquqiy

mexanizmlarni yaratish zaruriyatini yanada dolzarblashtirmoqda. Hozirgi kunda O'zbekiston Respublikasida kiberjinoyatlarga qarshi kurashishning huquqiy asoslari bir qator qonun hujjatlari orqali tartibga solinadi, jumladan, O'zbekiston Respublikasi Jinoyat kodeksining tegishli moddalar, "Axborotlashtirish to'g'risida"gi qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi qonun hamda boshqa normativ-huquqiy hujjatlar [2]. Biroq, kiberjinoyatchilik turlarining tobora murakkablashuvi, yangi texnologik imkoniyatlardan foydalangan holda amalga oshiriladigan jinoyatlarning paydo bo'lishi mavjud huquqiy bazani doimiy takomillashtirish zaruriyatini keltirib chiqarmoqda. Xalqaro tajriba shuni ko'rsatadiki, kiberjinoyatlarga qarshi samarali kurashish uchun nafaqat milliy darajada, balki xalqaro hamkorlik doirasida ham huquqiy mexanizmlarni uyg'unlashtirib borish talab etiladi [3]. Yevropa Kengashi tomonidan qabul qilingan

Kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasi kiberhavfsizlik sohasidagi xalqaro huquqiy hamkorlikning asosiy hujjati hisoblanadi va ko'plab davlatlar tomonidan o'z milliy qonunchiligini ushbu standartlarga muvofiqlashtirish jarayoni olib borilmoqda.

METODOLOGIYA VA ADABIYOTLAR TAHLILI

Tadqiqot jarayonida quyidagi ilmiy metodlardan foydalanildi: qiyosiy-huquqiy tahlil metodi orqali turli mamlakatlarning kiberjinoyatchilik sohasidagi qonunchiligini solishtirish amalga oshirildi; tizimli yondoshuv kiberhavfsizlikni ta'minlashning huquqiy, tashkiliy va texnik jihatlarini yaxlit holda o'rganish imkonini berdi. Adabiyotlar tahlili shuni ko'rsatadiki, kiberjinoyatchilik muammosi so'nggi yillarda nafaqat huquqshunoslar, balki axborot texnologiyalari mutaxassislari, iqtisodchilar va xavfsizlik sohasidagi ekspertlar diqqat markazida turmoqda. Rossiyalik tadqiqotchilar V.B. Vexov va A.V. Golovko o'z asarlarida kiberjinoyatlarning huquqiy tavsifini berish va jinoyat qonunchiligi normalarini zamonaviylashtirish masalalarini chuqur tahlil qilganlar [4]. Ularning fikricha, kiberjinoyatchilik klassik jinoyatchilikdan tubdan farq qilib, alohida huquqiy yondashuvni talab etadi. Xalqaro kontekstda kiberhavfsizlik masalalari bilan shug'ullanuvchi ekspertlar, jumladan, M. Chertoff va T. Simon o'z tadqiqotlarida kiberjinoyatlarga qarshi kurashishda davlatlararo hamkorlikning muhimligini ta'kidlaganlar va Budapesht konvensiyasining ahamiyatini alohida ajratib ko'rsatganlar [5]. Yevropa Ittifoqi mamlakatlari tajribasi shuni ko'rsatadiki, kiberjinoyatchilikga qarshi samarali kurash uchun uchta asosiy omil muhim: zamonaviy qonunchilik bazasi, malakali mutaxassislar va xalqaro hamkorlik mexanizmlari [6].

O'zbekistonlik huquqshunoslar, jumladan, A.X. Saidov va Z.Kh. Gulyamov o'z ishlarida milliy kiberhavfsizlik tizimini shakllantirish va takomillashtirish masalalariga bag'ishlangan tadqiqotlar olib bordilar [7]. Ular mamlakatimizda kiberjinoyatlarga qarshi kurashishning huquqiy asoslarini mustahkamlash zarurligi haqida gap yuritib, qonunchilikda bir qator tushunchalarni aniqlashtirish va yangi jinoyat tarkiblarini joriy etish zarurligini ta'kidlaganlar.

Xususan, shaxsiy ma'lumotlarni noqonuniy to'plash va tarqatish, raqamli identifikatsiya vositalaridan noqonuniy foydalanish, kriptovalyutalar orqali pul yuvish kabi yangi jinoyat turlari milliy qonunchilikda to'liq tartibga solinmagan. Xalqaro Telekommunikatsiya Ittifoqi (ITU) ma'lumotlariga ko'ra, rivojlanayotgan mamlakatlarda kiberhavfsizlik sohasidagi asosiy muammo nafaqat texnologik zaifliklar, balki huquqiy bazaning noqulqlilik va huquq-tartibot organlari xodimlarining etarli malakaga ega emasligidir [8].

NATIJALAR VA MUHOKAMA

Olib borilgan tahlil natijalarida aniqlandiki, O'zbekiston Respublikasining kiberjinoyatlarga qarshi kurashish sohasidagi huquqiy bazasi oxirgi yillarda sezilarli darajada takomillashtirilgan bo'lsa-da, bir qator muhim kamchiliklar va bo'shliqlar mavjud. Birinchidan, Jinoyat kodeksida kiberjinoyatlarning barcha zamonaviy turlarini qamrab oladigan yetarli miqdorda moddalar mavjud emas. Masalan, ransomware hujumlari, DDoS hujumlar orqali shantaj qilish, IoT qurilmalariga ruxsatsiz kirib borish va sun'iy intellektdan jinoyat maqsadlarida foydalanish kabi yangi jinoyat turlari aniq huquqiy tavsifga ega emas. Ikkinchidan, kiberjinoyatlar bo'yicha sudlov amaliyotining yetarli darajada shakllangan emasligi, huquq qo'llash organlari xodimlarining texnik va huquqiy jihatdan etarli malakaga ega emasligi muammolari kuzatilmoqda. Uchinchidan, xalqaro hamkorlik mexanizmlari, ayniqsa, transchegaraviy kiberjinoyatlar bo'yicha huquqiy yordam ko'rsatish tartibleri to'liq ishlab chiqilmagan.

Tadqiqot davomida kiberjinoyatlarning asosiy turlari va ularga nisbatan joriy qonunchilikdagi tartibga solish holati tahlil qilindi. Quyidagi jadvalda ushbu ma'lumotlar umumlashtirilgan:

1-jadval. Kiberjinoyatlarning asosiy turlari va huquqiy tartibga solinishi

Kiberjinoyat turi	Tarqalish darajasi	Jinoyat kodeksidagi mos modda	Huquqiy tartibga solinish darajasi	Takomillashtirish zaruriyati
Axborot tizimlariga ruxsatsiz kirish	Yuqori	278-modda	Qisman etarli	Tushunchani kengaytirish kerak
Kompyuter viruslari tarqatish	O'rta	278-modda	Qisman etarli	Yangi texnologiyalarni qamrash
Phishing va ijtimoiy injiniring	Yuqori	168, 278-moddalar	Etarli emas	Alohida jinoyat tarkibi kerak
Shaxsiy ma'lumotlarni o'g'irlash	Juda yuqori	273-1-modda	Qisman etarli	Jazolarni kuchaytirish
DDoS hujumlar	O'rta	Aniq tartibga solinmagan	Etarli emas	Yangi modda kiritish kerak
Ransomware hujumlari	O'sish tendentsiyasi	Qisman 278-modda	Etarli emas	Alohida tarkib ishlab chiqish
Kriptoalyuta bilan bog'liq jinoyatlar	Yuqori o'sish	Aniq tartibga solinmagan	Etarli emas	Kompleks tartibga solish kerak
IoT qurilmalariga hujumlar	Past (o'smoqda)	Tartibga solinmagan	Etarli emas	Yangi texnologiyalar uchun normalar

Jadvaldan ko'rinib turibdiki, kiberjinoyatlarning deyarli barcha turlari bo'yicha huquqiy tartibga solish yetarli emas yoki umuman mavjud emas. Bu holatning asosiy sabablari orasida qonunchilik texnologik rivojlanish sur'atlaridan orqada qolishi, kiberjinoyatlar turlarining doimiy yangilanib turishi va xalqaro standartlarga to'liq muvofiqlik ta'minlanmaganligi kabi omillarni ajratib ko'rsatish mumkin. Xalqaro tajribani o'rganish jarayonida turli mamlakatlarning kiberjinoyatlarga qarshi kurashish sohasidagi eng yaxshi amaliyotlari tahlil qilindi.

Quyidagi jadvalda ayrim rivojlangan mamlakatlar va mintaqaviy tashkilotlarning ushbu sohadagi yondashuvlari taqqoslangan:

2-jadval. Xalqaro amaliyotda kiberjinoyatlarga qarshi kurashish mexanizmlari

Mamlakat/ tashkilot	Asosiy huquqiy hujjat	Maxsus tuzilma	Xalqaro hamkorlik	Innovatsion yondashuvlar	Samaradorlik ko'rsatkichi
AQSh	Computer Fraud and Abuse Act	FBI Cyber Division	Ikki tomonlama shartnomalar	Texno- kompaniyalar bilan hamkorlik	Yuqori
Buyuk Britaniya	Computer Misuse Act 1990	National Cyber Security Centre	Budapesht konventsiyasi	Kiberhavfsizlik sertifikatlash	Yuqori
Germaniya	Strafgesetzbuch (StGB)	Bundes kriminalamt Cyber	EU direktivalari	Sun'iy intellekt texnologiyalari	Yuqori
Janubiy Koreya	Act on Promotion of Information and Communications Network	Korea Internet & Security Agency	Osiyo-Tinch okeani hamkorligi	Blockchain texnologiyalari	Juda yuqori
Rossiya	UK RF 272- 274-moddalar	K Boshqarmasi (MVD)	SHX doirasida hamkorlik	Milliy internet segmenti	O'rta
Yevropa Ittifoqi	NIS Directive, GDPR	ENISA	Budapesht konventsiyasi	Umumyevropa yondashuv	Yuqori
Singapur	Cybersecurity Act 2018	Cyber Security Agency	ASEAN hamkorligi	Kiberhavfsizlik ekotizimi	Juda yuqori

Taqqoslash natijalari shuni ko'rsatadiki, muvaffaqiyatli mamlakatlarda kiberjinoyatlarga qarshi kurashish tizimi kompleks yondashuvga asoslangan bo'lib, u huquqiy, tashkiliy, texnik va xalqaro hamkorlik komponentlarini o'z ichiga oladi. Xususan, Singapur va Janubiy Koreya tajribasi rivojlanayotgan mamlakatlar uchun ayniqsa qiziqarli, chunki ular nisbatan qisqa vaqt ichida yuqori samaradorlikka erishganlar va zamonaviy texnologiyalarni faol qo'llash orqali kiberhavfsizlik tizimini qurishganlar [9]. Ushbu mamlakatlar tajribasida e'tiborga loyiq jihatlar qatoriga maxsus davlat tuzilmalarining kuchli vakolatga ega bo'lishi, kiberhavfsizlik sohasida ta'lim tizimini rivojlantirish, texnologik kompaniyalar bilan uzviy hamkorlik va proaktiv yondashuv (jinoyatlarni aniqlash emas, balki ularning oldini olishga e'tibor berish) kiradi.

O'zbekiston uchun xalqaro tajribadan foydalangan holda kiberjinoyatlarga qarshi kurashishning huquqiy asoslarini takomillashtirish bo'yicha bir qator takliflar ishlab chiqish mumkin. Birinchi navbatda, Jinoyat kodeksiga yangi moddalar kiritish yoki mavjud moddalarning dispozitsiyalarini kengaytirish zarur. Jumladan, DDoS hujumlarni, ransomware jinoyatlarini, IoT qurilmalariga noqonuniy kirish va kriptovalyutalar bilan bog'liq jinoyatlarni alohida tarkiblar sifatida belgilash maqsadga muvofiq.

Ikkinchidan, kiberjinoyatlar bo'yicha raqamli dalillarni to'plash, saqlash va sudda ishlatish tartibi aniq qonun darajasida belgilanishi kerak, chunki hozirgi kunda ushbu jarayon asosan umumiy protsessual normalar asosida amalga oshirilmoqda va kiberjinoyatlarning o'ziga xos xususiyatlarini yetarli darajada inobatga olmaydi [10]. Uchinchidan, transchegaraviy kiberjinoyatlar bo'yicha xalqaro huquqiy yordam ko'rsatish mexanizmlarini soddalashtirib, tezkor aloqa kanallarini yaratish talab etiladi.

Bundan tashqari, kiberjinoyatlarga qarshi kurashish sohasida faoliyat yurituvchi turli davlat organlari (Davlat xavfsizlik xizmati, Ichki ishlar vazirligi, Raqamli texnologiyalar vazirligi va boshqalar) o'rtasida vazifalar va vakolatlarni aniq taqsimlash, koordinatsiya mexanizmlarini yaratish dolzarbdir. Hozirgi kunda vakolat va mas'uliyat chegaralari har doim ham aniq emas, bu esa samarasizlikka olib kelmoqda. Alohida e'tiborni kiberhavfsizlik sohasida yuqori malakali mutaxassislar tayyorlash tizimini yaratishga qaratish zarur. Bu nafaqat huquq-tartibot organlari xodimlari uchun, balki sudyalalar, prokurorlar va advokatlar uchun ham maxsus o'quv dasturlarini ishlab chiqishni, oliy o'quv yurtlarida tegishli mutaxassisliklarni ochishni talab etadi.

XULOSA

Olib borilgan tadqiqot natijalarini umumlashtirgan holda quyidagi xulosalarga kelish mumkin. Kiberjinoyatchilik zamonaviy jamiyat uchun tobora kuchayib borayotgan tahdid bo'lib, unga qarshi samarali kurashish kompleks yondashuv va doimiy huquqiy bazani yangilab turishni talab etadi. O'zbekiston Respublikasida kiberjinoyatlarga qarshi kurashishning huquqiy asoslari mavjud bo'lsa-da, ular bir qator jihatdan zamonaviy talablarga to'liq javob bermaydi. Jinoyat kodeksida kiberjinoyatlarning barcha turlarini qamrab oladigan yetarli normalar mavjud emas, maxsus terminologiya va tushunchalar apparati to'liq ishlab chiqilmagan, raqamli dalillar bilan ishlash tartibi aniq belgilanmagan va xalqaro hamkorlik mexanizmlari yetarli darajada rivojlanmagan. Xalqaro tajribani o'rganish shuni ko'rsatdiki, kiberhavfsizlik sohasida yuqori natijalarga erishgan mamlakatlar bir necha asosiy tamoyillarga amal qilishadi: zamonaviy va moslashuvchan qonunchilik, maxsus tuzilmalar va yuqori malakali kadrlar, texnologik kompaniyalar bilan hamkorlik, xalqaro standartlarga muvofiqlik va proaktiv yondashuv.

O'zbekiston uchun ushbu tajribadan o'rganish va milliy xususiyatlarni inobatga olgan holda eng yaxshi amaliyotlarni joriy etish muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. Cybersecurity Ventures. 2024 Official Cybercrime Report. – USA, 2024. – P. 15-22.
2. O'zbekiston Respublikasining Jinoyat kodeksi. – T.: "Adolat" nashriyoti, 2023. – 278-modda.
3. Council of Europe. Convention on Cybercrime (Budapest Convention). – Strasbourg, 2001. – ETS No. 185.
4. Вехов В.Б., Головкин А.В. Киберпреступность: уголовно-правовая и криминологическая характеристика. – М.: Юрлитинформ, 2022. – С. 134-156.
5. Chertoff M., Simon T. The Impact of the Dark Web on Internet Governance and Cyber Security. – Global Commission on Internet Governance Paper Series, 2015. – No. 6.

6. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2023. – Luxembourg, 2023. – P. 45-67.
7. Саидов А.Х., Гулямов З.Х. Ўзбекистон Республикасида киберхавфсизликни таъминлашнинг ҳукукий асослари. – Т.: "Адолат" нашриёти, 2023. – 98-112 б.
8. International Telecommunication Union (ITU). Global Cybersecurity Index 2023. – Geneva, 2023. – P. 28-41.
9. Cybersecurity Agency of Singapore. Singapore Cybersecurity Strategy 2021. – Singapore, 2021. – P. 12-25.
10. O‘zbekiston Respublikasining Qonuni, 02.07.2019 yildagi O‘RQ-547-son, <https://lex.uz/docs/-4396419>