KIBERJINOYATLAR BO‘YICHA XALQARO STANDARTLAR VA XORIJIY DAVLATLAR TAJRIBASIDA KIBERO‘G‘RILIK JINOYATLARI KVALIFIKATSIYASI

SAIDOV
Boboqul Yoriqulovich
Huquqni muhofaza qilish Akademiyasi magistranti

Annotatsiya. *Maqolada kiberjinoyatlar bo‘yicha xalqaro standartlar hamda xorijiy davlatlar tajribasi asosida AKT orqali sodir etiladigan o‘g‘rilik jinoyatlarini kvalifikatsiya qilish masalalari tahlil qilingan. Shuningdek, kompyuter tizimiga noqonuniy kirish, ma’lumotlarga aralashuv va mulkiy manfaatga erishish holatlarini kompleks kvalifikatsiya qilish zarurati asoslab berilgan.*
Kalit so‘zlar: *kiberjinoyat, kibero‘g‘rilik, AKT, Budapesht konvensiyasi, xalqaro standartlar, xorijiy tajriba, kompyuter firibgarligi, texnologik neytrallik, elektron dalillar, mulkiy zarar, jinoyatni kvalifikatsiya qilish, raqamli jinoyatlar.*

Аннотация. *В статье анализируются вопросы квалификации преступлений, связанных с кражей, совершенных с использованием ИКТ, на основе международных стандартов по киберпреступности и опыта зарубежных стран. Также обосновывается необходимость всесторонней квалификации случаев незаконного доступа к компьютерной системе, вмешательства в информационную систему и получения имущественной выгоды.*
Ключевые слова: *киберпреступность, киберпреступность, ИКТ, Будапештская конвенция, международные стандарты, зарубежный опыт, компьютерное мошенничество, технологический нейтралитет, электронные доказательства, причинение имущественного ущерба, квалификация преступления, цифровые преступления.*

Abstract. *This article analyzes the issues of qualifying theft crimes committed through information and communication technologies (ICT), based on international standards on cybercrime and the experience of foreign states. Furthermore, the article substantiates the necessity of comprehensively qualifying cases involving unauthorized access to computer systems, interference with data, and the unlawful acquisition of property interests.*
Keywords: *cybercrime, cyber theft, ICT, Budapest Convention, international standards, foreign experience, computer fraud, technological neutrality, electronic evidence, property damage, qualification of crimes, digital crimes.*

Axborot kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberjinoyatchilik, xususan, AKT orqali sodir etiladigan o‘g‘rilik jinoyatlari an’anaviy jinoiy-huquqiy yondashuvlardan tashqariga chiqib, transmilliy va murakkab huquqiy hodisaga aylandi. Bunday jinoyatlar bir vaqtning o‘zida bir nechta davlat hududida sodir etilishi, jinoyat subyekti, obyekti va oqibatlarining turli yurisdiksiyalarda joylashishi bilan tavsiflanadi. Shu sababli kiberjinoyatlarni, jumladan kibero‘g‘rilik jinoyatlarini to‘g‘ri kvalifikatsiya qilish xalqaro standartlar va xalqaro hamkorlik mexanizmlariga tayangan holda hal etilishi zarur bo‘lgan masala sifatida e’tirof etiladi [1].

Kiberjinoyatlar sohasida universal xalqaro standartlarni o‘zida jamlagan eng muhim hujjat 2001-yil 23-noyabrda qabul qilingan “Kiberjinoyatlar to‘g‘risida”gi Budapesht konvensiyasi hisoblanadi [2]. Mazkur Konvensiya kompyuter tizimlariga noqonuniy kirish, kompyuter ma’lumotlarini egallash, ularni o‘zgartirish, yo‘q qilish hamda axborot texnologiyalaridan foydalanib mulkiy zarar yetkazish bilan bog‘liq qilmishlarni jinoyat sifatida e’tirof etish bo‘yicha yagona yondashuvni shakllantiradi [3]. Konvensiya doirasida AKT orqali sodir etiladigan o‘g‘rilik jinoyatlari alohida nom bilan ajratilmagan bo‘lsa-da, ularni kompyuter ma’lumotlarini noqonuniy egallash yoki firibgarlik orqali mulkiy manfaatga erishish shakli sifatida kvalifikatsiya qilish tavsiya etiladi. Bu esa jinoyatni baholashda texnik vosita emas, balki mulkiy zarar yetkazish fakti ustuvor ekanini ko‘rsatadi.

Xalqaro standartlarga ko‘ra, kiberjinoyatlarni kvalifikatsiya qilishda texnologik neytrallik prinsipi muhim ahamiyat kasb etadi. Unga ko‘ra axborot texnologiyalari jinoyatning mustaqil obyektiv tomoni emas, balki uni sodir etish usuli sifatida baholanadi. Shu asosda Germaniya, Fransiya va Italiya kabi davlatlar jinoyat qonunchiligida AKT orqali sodir etilgan o‘g‘rilik jinoyatlari alohida jinoyat tarkibi sifatida emas, balki mulkka qarshi jinoyatlarning murakkab yoki og‘irlashtiruvchi shakli sifatida kvalifikatsiya qilinadi [4]. Masalan, Germaniya Jinoyat kodeksida kompyuter tizimlaridan foydalanib sodir etilgan mulkiy jinoyatlar uchun javobgarlik kuchaytirilgan bo‘lsa-da, ular klassik o‘g‘rilik yoki firibgarlik tarkibi doirasida baholanadi.

Kiberjinoyatlarga qarshi kurashish xalqaro hamkorliksiz samarali bo‘lishi mumkin emas. Shu bois xalqaro standartlarda davlatlar o‘rtasida tezkor huquqiy yordam, elektron dalillarni saqlash va uzatish, jinoyatchilarni ekstraditsiya qilish mexanizmlarini soddalashtirish masalalariga alohida e’tibor qaratilgan. Budapesht konvensiyasi doirasida joriy etilgan “24/7 Network” tizimi ishtirokchi davlatlarga vakolatli organlar bilan kiberjinoyatlar yuzasidan tezkor axborot almashish imkonini beradi [5]. Bu mexanizm AKT orqali sodir etilgan o‘g‘rilik jinoyatlarini aniqlashda muhim ahamiyatga ega, chunki raqamli dalillar qisqa muddat ichida yo‘qolishi yoki o‘zgartirilishi mumkin [6].

Xorijiy davlatlar tajribasi shuni ko‘rsatadiki, “kibero‘g‘rilik”, odatda, ikki qatlamli yondashuv asosida kvalifikatsiya qilinadi. Bir tomondan, kompyuter tizimi va ma’lumotlariga tajovuzni jinoyat deb belgilovchi maxsus “kompyuter (kiber) jinoyatlari” tarkiblari qo‘llanadi, ikkinchi tomondan esa mulkka qarshi jinoyatlar (o‘g‘rilik, firibgarlik, xizmatlarni aldov yo‘li bilan olish, noqonuniy boyish va h.k.) yoki moliyaviy jinoyatlar bilan qo‘shib kvalifikatsiya qilinadi. Bunday yondashuv xalqaro standartlarda ham aks etgan. Jumladan, aynan Budapesht konvensiyasi “noqonuniy kirish”, “ma’lumotlarga aralashuv”, “tizimga aralashuv” bilan bir qatorda “kompyuterga oid firibgarlik”ni ham alohida jinoyat sifatida ko‘rsatadi, ya’ni kiberhujumning texnik komponenti va mulkiy zarar komponentini ajratib, har biriga mos huquqiy reaksiya berish konsepsiyasi shakllangan. Shu mantiq Yevropa Ittifoqining 2013/40/YEU direktivasida ham mustahkamlanib, a’zo davlatlarda “axborot tizimlariga hujumlar” bo‘yicha minimal jinoyat tarkiblari va sanksiyalarni uyg‘unlashtirish, vakolatli organlar hamkorligini kuchaytirish ko‘zda tutilgan.

Angliya va Uels amaliyotida kibero‘g‘riliklarni baholash ko‘pincha “kirish/zarar yetkazish” qismi “Computer Misuse Act 1990” doirasida, mulkiy manfaatni qo‘lga kiritish qismi esa “Fraud Act 2006” yoki “Theft Act 1968” doirasida yoritiladi. “Computer Misuse Act 1990” kompyuter materialiga ruxsatsiz kirish, ruxsatsiz kirib keyingi jinoyatni sodir etish niyati, shuningdek tizim yoki ma’lumotlarni buzish kabi holatlarni jinoiy ravishda kvalifikatsiya qiladi. Bu, masalan, fishing havolasi orqali bank akkauntiga kirib olish yoki zararli dastur bilan autentifikatsiya ma’lumotlarini qo‘lga kiritish holatlarida “kiber tajovuz” komponentini nazarda tutadi. “Fraud Act 2006” esa firibgarlikni bir nechta usul orqali sodir etish (xususan, yolg‘on taqdim etish orqali) va “xizmatlarni qonunga xilof tarzda qo‘lga kiritish”ni jinoyat deb belgilaydi. Amaliyotda karta rekvizitlari bilan noqonuniy tranzaksiya qilish, onlayn bankingda aldovli tasdiqlash (Social Engineering) orqali pul yechish aynan shu “mulkiy tajovuz” komponenti bilan bog‘lanadi. Bunda “Theft Act 1968” o‘g‘rilikning klassik ta’rifini beradi, biroq raqamli muhitda “mulk” va “egallash” kategoriyalarini qo‘llash doim ham samarali emas. Ayrim holatlarda “pul mablag‘i” bank hisobvarag‘idagi talab huquqi sifatida, ayrim holatlarda “xizmat”

sifatida baholanadi va shunga mos ravishda firibgarlik yoki xizmatlarni noqonuniy yo‘l bilan olish tarkibi ustuvor bo‘lib qoladi.

AQSHda kibero‘g‘riliklarni kvalifikatsiya qilishda “himoyalangan kompyuterga ruxsatsiz kirish yoki vakolatdan chetga chiqib kirish” hamda firibgarlik niyati bilan “moddiy belgi”ni qo‘lga kiritish holatlari “Computer Fraud and Abuce Act (CFAA)” doirasida markaziy o‘rin tutadi. CFAA konstruksiyasi, ayniqsa, bank tizimlariga yoki Internet orqali bog‘langan infratuzilmaga noqonuniy kirish bilan moliyaviy foyda ko‘rish sxemalarida “kirish – egallash – natija” zanjirini isbotlashga qulay. Shu bilan birga, mulkiy zarar, odatda, qo‘shimcha ravishda umumiy firibgarlik tarkiblari (masalan, elektron aloqa vositalari orqali firibgarlik kabi) bilan ham bog‘lanadi. Natijada, kvalifikatsiya “kiberkirish” va “mulkiy aldov”ning yig‘ma huquqiy bahosiga aylanadi.

Fransiyada kiberjinoyatlar klassik “Godfrain” yondashuvi asosida Jinoyat kodeksida avtomatlashtirilgan ma’lumotlarni qayta ishlash tizimiga “firibgarlik yo‘li bilan kirish yoki unda qolish”ni jinoyat sifatida belgilaydi. Bu norma bevosita “hasking” faktini qamrab oladi. Agar ruxsatsiz kirish natijasida ma’lumotlar o‘zgartirilsa, o‘chirib yuborilsa yoki tizim ishlashi buzilsa, javobgarlik kuchaytiriladigan holatlar vujudga keladi, ya’ni qonun texnik tajovuzning og‘irlashgan oqibatini alohida yuridik ahamiyatga ega belgi sifatida ko‘radi.

Kibero‘g‘rilikning “mulk” komponenti esa ko‘pincha klassik o‘g‘rilik tushunchasi bilan yoki “aldov”ga yaqin tarkiblar bilan bog‘lanadi. Fransiya huquqida o‘g‘rilik “birovning narsasini firibgarlik yo‘li bilan olib qo‘yish” sifatida ta’riflanadi, ammo raqamli aktivlar, hisobdagi mablag‘ va identifikatsiya ma’lumotlari bilan bog‘liq ishlar amaliyotda ko‘proq avtomatlashtirilgan ma’lumotlarni qayta ishlash tizimiga noqonuniy kirish va iqtisodiy zarar mantig‘ida kompleks baholanadi. Shu bois fransuz modeli kibero‘g‘rilikni “tizimga tajovuz” orqali ijtimoiy xavflilikni birinchi o‘ringa chiqarib, mulkiy natijani esa qo‘shimcha kvalifikatsiya yoki jazoni individuallashtirish mezoni sifatida yoritishga moyil.

Iqtisodiy rivojlangan xorijiy davlatlar JKlarida tatbiq etilayotgan jinoyatlar: a) mulkka qarshi jinoyatlar to‘g‘risidagi huquqiy normalar keng talqin qilingan va kompyuter talon-torojliklari qonun analogiyasi bo‘yicha kvalifikatsiya qilinadigan davlatlar; b) kompyuter talon-torojliklari og‘irlashtiruvchi yoki yengillashtiruvchi holat sifatida mulkka qarshi jinoyatlar uchun javobgarlik belgilangan normalar bilan kvalifikatsiya qilinadigan davlatlar; v) mulkka qarshi jinoyatlarga maxsus qonunlar tatbiq etiladigan davlatlar (bunda kompyuter talon-torojliklari uchun JKda emas, balki alohida qonun hujjatlarida javobgarlik nazarda tutiladi); g) kompyuter yordamida talon-torojlik sodir etganlik uchun jinoyat qonuni alohida moddasida javobgarlik nazarda tutilgan davlatlar.

Quyida ayrim xorijiy davlatlarning jinoyat qonunchiligida ushbu masalalar talqinini ko‘rib chiqamiz.

1. AQSHning kompyuter jinoyatchiligiga bag‘ishlangan qonunchiligi alohida xususiyatga egaligi va doimiy yangilanib turishi bilan farqlanadi. AQSHda kompyuter jinoyatchiligiga bag‘ishlangan Asosiy qonun 1986-yilda ishlab chiqilgan bo‘lib, “Kompyuter bilan bog‘liq firibgarlik va suiiste’mol qilish” deb nomlanadi. Keyinchalik “kompyuterdan foydalanib, firibgarlik jinoyati” AQSHning qonunlar to‘plamiga kiritildi. Qonunlar to‘plamining 1030 (a) (4) paragrafida firibgarlik, ya’ni qiymatga ega har qanday narsaga egalik qilish maqsadida kompyuterdan foydalanib, yil davomida 5 ming AQSH dollaridan ortiq bo‘lgan, kompyuter vaqtidan noqonuniy foydalanish, ya’ni kompyuter serveri va ulanish tizimidan bepul foydalanish uchun javobgarlik belgilangan [7].

AQSH federal qonunchiligida kompyuterdan foydalanib aldash deganda, kompyuter texnologiyalaridan o‘zganing mulkini qo‘lga kiritish maqsadida yangi ma’lumotlar yaratish yoki mavjud ma’lumotlarni buzib ko‘rsatish yo‘li bilan qonunga xilof ravishda foydalanish tushuniladi. AQSH Qonunlar to‘plamining 1030 (a) (4)-§da biror-bir mol-mulkni aldov yo‘li bilan olish maqsadida himoyalangan kompyuterdan qonunga xilof ravishda (ruxsatsiz) foydalanish, bir yil davomida 5000 AQSH dollaridan ortiq miqdorda kompyuterdan foydalanish natijasida mol-mulkni qo‘lga kiritish, 1030 (a) (6)-§da qasddan, aldash niyatida kompyuter axborotining g‘ayriqonuniy trafigini amalga oshirish natijasida davlatlararo yoki tashqi savdoga zarar yetkazish, 1644-§da savdo sohasida kredit kartalari bilan g‘ayriqonuniy tranzaksiyalarni amalga oshirish uchun javobgarlik nazarda tutilgan.

2. Avstriya Jinoyat kodeksining 148a-moddasida ma’lumotlarga avtomatlashtirilgan usulda ishlov berish jarayonlariga maxsus dasturlar yordamida ta’sir ko‘rsatish, ma’lumotlarni kiritish, o‘zgartirish yoki yo‘q qilish yoxud ma’lumotlarni yo‘q qilish yo‘li bilan yoki ma’lumotlarga ishlov berish jarayoniga ta’sir ko‘rsatadigan boshqa usulda g‘ayriqonuniy mulkiy naf ko‘rish maqsadida yetkazgan mulkiy zarar uchun jinoiy javobgarlik nazarda tutilgan. Firibgarlik harakatlaridan ko‘rilgan zarar miqdori 3 ming yevrodan ortiq bo‘lsa, qilmish 3 yilgacha muddatga ozodlikdan mahrum qilish bilan jazolanadi, agar yetkazilgan zarar 50 ming yevrodan ziyod bo‘lsa, aybdor 1 yildan 5 yilgacha muddatga ozodlikdan mahrum qilish bilan jazolanadi [8].

3. Bolgariya Jinoyat kodeksida kompyuter firibgarligi uchun javobgarlik “Mulkka qarshi jinoyatlar” deb nomlangan 5-bobning 212a-moddasida nazarda tutilgan. 212a-moddaning 1-qismiga muvofiq, agar shaxs tamagirlik niyatida kompyuter ma’lumotlarini kiritish, o‘zgartirish yoki o‘chirib tashlash yo‘li bilan yoki elektron imzoni qalbakilashtirish orqali birovni chalg‘itgan bo‘lsa, unga kompyuter firibgarligi uchun 6 ming bolgar levi miqdorida jarima solinib, 1 yildan 6 yilgacha muddatga ozodlikdan mahrum qilish bilan jazolanadi [9].

4.Germaniya Jinoyat kodeksining 263a-moddasiga muvofiq, o‘zi yoki uchinchi shaxs uchun mulkiy naf ko‘rish niyatida harakat qilib, ma’lumotlarga ishlov berish natijasida dasturlarni noto‘g‘ri yaratish, noto‘g‘ri yoki noto‘liq dasturlardan foydalanish yo‘li bilan ta’sir ko‘rsatish, qonunga xilof ravishda foydalanib, ma’lumotlarga ishlov berish natijasiga g‘ayriqonuniy ta’sir ko‘rsatish orqali o‘zga shaxsning mol-mulkiga zarar yetkazgan shaxs jinoiy javobgarlikka tortilishi lozim (besh yilgacha muddatga ozodlikdan mahrum qilish yoki jarima bilan jazolanadi). Mazkur moddaning 2-qismida kompyuter firibgarligi sodir etishga tayyorgarlik ko‘rganlik: kompyuter dasturini yaratganlik, tegishli asbob-uskunalarni egallaganlik uchun javobgarlik nazarda tutilgan (uch yilgacha muddatga ozodlikdan mahrum qilish yoki jarima bilan jazolanadi).

A.E.Jalinskiy qayd etganidek, nemis qonun chiqaruvchisi tomonidan firibgarlikning ikki turi aniq belgilangan: 1) an’anaviy firibgarlik; 2) axborot sohasida firibgarlik (kompyuter firibgarligi). Kompyuter firibgarligining mazmuni shundaki, aldash odamga nisbatan emas, balki dasturga nisbatan amalga oshiriladi, chunki mol-mulkka zarar yetkazish axborotga ishlov berish jarayoniga ta’sir ko‘rsatish va dasturni noto‘g‘ri o‘rnatish, noto‘g‘ri yoki noto‘liq ma’lumotlardan foydalanish yo‘li bilan, shuningdek ma’lumotlardan qonunga xilof ravishda foydalanish yoki ma’lumotlarga ishlov berish jarayonlariga g‘ayriqonuniy ta’sir ko‘rsatish yo‘li bilan amalga oshiriladi [10].

Ko‘rib turganimizdek, kompyuter firibgarligi bilan bog‘liq manipulyatsiyalar quyidagi maxsus kriminologik belgilarga ega:

birinchidan, ma’lumotlarga ishlov berish jarayoniga ta’sir ko‘rsatishning to‘g‘ridan-to‘g‘ri natijasi o‘zganing mulkiga zarar yetkazilishida ifodalanishi lozim;

ikkinchidan, firibgarlikning asosiy tarkibidan farqli o‘laroq, kompyuter firibgarligi insonga emas, balki dasturga qaratilgan aldovni o‘z ichiga oladi, ayni holda yetkazilgan zarar axborotga ishlov berish jarayoniga ta’sir ko‘rsatish natijasi hisoblanadi. Boshqa vaziyatda aldov kompyuter tizimi yoki kompyuter axborotiga emas, balki insonga qaratilgan holda, qilmish asosiy firibgarlik (Germaniya JKning 263-§) sifatida kvalifikatsiya qilinadi.

1993-yilda Gollandiyada “Kompyuter jinoyatlari to‘g‘risida”gi maxsus qonunning qabul qilinganligi ushbu jinoyatlarga qarshi kurashni yanada mustahkamladi. Gollandiya JK ushbu qonun asosida normativ baza bilan to‘ldirilgan. Ushbu davlat Jinoyat kodeksining o‘ziga xos muhim jihatlaridan biri – unda qonun chiqaruvchining kompyuter jinoyatchiligi sohasidagi atamalarni izohlab berganligidadir. Chunonchi, Gollandiya JKning 80 moddasida “ma’lumot”, “kompyuter qurilmalari va tizimlari” (elektron qurilmalardagi ma’lumotlarni saqlash va qayta ishlashga mo‘ljallangan qurilmalar) kabi atamalarining mazmuni ochib berilgan [11].

Kompyuter firibgarligini kriminallashtirishning shunga o‘xshash modeli Daniya (279a-modda) [12] va Norvegiya JKda (270-modda 2-qismi) [13] ham qo‘llanilgan.

Latviya JKning 177.1-moddasida avtomatlashtirilgan tizimidan foydalanib ma'lumotlarga ishlov berish (firibgarlik) uchun jinoiy javobgarlik nazarda tutilgan. Mazkur jinoyat uchun 3 yilgacha muddatga ozodlikdan mahrum qilish belgilangan. Kompyuter firibgarligini oldindan til biriktirgan bir guruh shaxs tomonidan sodir etilishi (2-qism – 5 yilgacha muddatga ozodlikdan mahrum qilish bilan jazolanadi) va uyushgan guruh tarkibida yoki ko'p miqdorda (3-qism – 2 yildan 10 yilgacha muddatga ozodlikdan mahrum qilish bilan jazolanadi) javobgarlikni og'irlashtiruvchi holat sifatida nazarda tutilgan.

Xulosa qilib aytganda, kiberjinoyatlar bo'yicha xalqaro standartlar va xorijiy davlatlar tajribasida AKT orqali sodir etilgan o'g'rilik jinoyatlarini kvalifikatsiya qilishda universal, texnologik neytral va natijaga yo'naltirilgan yondashuvlar shakllangan. Ushbu yondashuvlar jinoyatni sodir etish vositasidan qat'i nazar, mulkiy zarar yetkazish fakti va aybdorning g'arazli maqsadini asosiy mezon sifatida belgilaydi. Mazkur ijobiy tajribalar O'zbekiston Respublikasida AKT orqali sodir etilgan o'g'rilik jinoyatlarini kvalifikatsiya qilishni takomillashtirishda muhim nazariy va amaliy ahamiyatga ega.

Foydalanilgan manbalar

1. *Brenner S.* Cybercrime and the Law: Challenges, Issues, and Outcomes. – Boston: Northeastern University Press, 2010. – P. 25–27.
2. Council of Europe. Convention on Cybercrime (Budapest Convention), 23 November 2001 // ETS No.185. – URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention
3. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society // Computer Law & Security Review. – 2016. – Vol. 32. – No. 4. – P. 500–515.
4. *Ambos K.* Economic Crime and Cybercrime in European Criminal Law // European Criminal Law Review. – 2018. – No. 3. – P. 289–305.
5. Council of Europe. Cybercrime Convention Committee (T-CY): 24/7 Network Guidelines. — Strasbourg, 2020. URL: https://www.coe.int/en/web/cybercrime/24-7-network
6. INTERPOL. Global Cybercrime Strategy and Operations. – Lyon, 2021. – URL: https://www.interpol.int/en/Crimes/Cybercrime
7. *Степанов-Егиянц В.* Ответственность за компьютерные преступления // Законность, 2005. – № 12. – С. 51.
8. *Фролов М.Д.* Уголовная ответственность за мошенничество в сфере компьютерной информации по законодательству стран Европы и СНГ // Ученые труды Российской академии адвокатуры и нотариата, 2015. – №4 (39). – С. 152
9. Уголовный Кодекс Республики Болгария. – Санкт-Петрбург. Юридический центр Пресс, 2001 / Под редакцией к.ю.н. *А.И.Лукашова.*
10. *Жалинский А.Э.* Современное немецкое уголовное право. – М., 2004. – С. 462-463.
11. Уголовный кодекс Голландии / Науч. ред. д-ок. юрид. наук Б.В. Волженкин, пер с анг. И.В. Мироновой. 2-е изд. – СПб.: Юридический центр Пресс, 2015.
12. Criminal Code of Denmark as of 2012. // https://www.unodc.org/ cld/document/dnk/2011/criminal_code_of_denmark_as_of_2012_danish_version.html?
13. The General Civil Penal Code of Norway. With subsequent amendments, the latest made by Act of 21 December 2005 No. 131. Act of 22 May 1902 No. 10. // www.app.uio.no/ub/ujur/oversatte-lover/data/lov-19020522-010-eng.pdf.

KOREYA VA O'ZBEKISTON RESPUBLIKALARI MA'MURIY-HUQUQBUZARLIKLAR TO'G'RISIDAGI QONUNCHILIGINING QIYOSIY-HUQUQIY TAHLILI: MILLIY MA'MURIY QONUNCHILIKNI MODERNIZATSIYA QILISH YO'LLARI

MAXSADOV
Maxsatullo Ismatovich
O'zbekiston Respublikasi Jamoat xavfsizligi universiteti, yuridik fanlar doktori (DSc), professor

Annotatsiya. *Ushbu maqolada Koreya Respublikasi va O'zbekiston Respublikasining ma'muriy javobgarlikka tortish asoslari hamda ma'muriy huquqbuzarliklar to'g'risidagi qonunchiligi qiyosiy-huquqiy jihatdan tahlil qilingan. Tadqiqot davomida Janubiy Koreyaning ilg'or tajribasi, xususan, ma'muriy tartib-taomillarni raqamlashtirish, jarimalar tizimining o'ziga xos xususiyatlari va huquqbuzarliklarning oldini olishdagi samarali mexanizmlari o'rganilgan. Tahlil natijalariga asoslanib, O'zbekiston milliy ma'muriy qonunchiligini takomillashtirish va modernizatsiya qilish, jazo choralarini liberallashtirish va xorijiy tajribani implementatsiya qilish bo'yicha ilmiy-amaliy taklif hamda tavsiyalar ishlab chiqilgan.*
Kalit so'zlar: *ma'muriy huquqbuzarlik, qiyosiy-huquqiy tahlil, ma'muriy javobgarlik, Janubiy Koreya qonunchiligi, milliy qonunchilikni modernizatsiya qilish, ma'muriy tartib-taomillar, huquqiy implementatsiya.*

Аннотация. *В данной статье проводится сравнительно-правовой анализ законодательства об административных правонарушениях и основ привлечения к административной ответственности Республики Корея и Республики Узбекистан. В ходе исследования изучен передовой опыт Южной Кореи, в частности, цифровизация административных процедур, специфические особенности системы штрафов и эффективные механизмы предотвращения правонарушений. На основе результатов анализа разработаны научно-практические предложения и рекомендации по совершенствованию и модернизации национального административного законодательства Узбекистана, либерализации мер наказания и имплементации зарубежного опыта.*
Ключевые слова: *административное правонарушение, сравнительно-правовой анализ, административная ответственность, законодательство Южной Кореи, модернизация национального законодательства, административные процедуры, правовая имплементация.*

Abstract. *This article provides a comparative legal analysis of the legislation on administrative offenses and the grounds for administrative responsibility in the Republic of Korea and the Republic of Uzbekistan. During the study, the advanced experience of South Korea was examined, particularly the digitalization of administrative procedures, the specific features of the fine system, and effective mechanisms for preventing offenses. Based on the analytical results, scientific and practical proposals and recommendations have been developed for the improvement and modernization of the national administrative legislation of Uzbekistan, the liberalization of penalties, and the implementation of foreign experience.*
Keywords: *administrative offense, comparative legal analysis, administrative responsibility, legislation of South Korea, modernization of national legislation, administrative procedures, legal implementation.*