elita.uz

Elektron Ilmiy Jurnal

№.1 (3)
2025

elita.uz

№ 1 (3) 2025

MUNDARIJA

SUN’IY INTELLEKT ASOSIDA YARATILGAN ASARLARNING MUHOFAZAGA LAYOQATLILIGI

Zebiniso Sheraliyeva

zebinisosheraliyeva2002@gmail.com

Toshkent davlat yuridik universiteti
Magistratura va sirtqi ta’lim fakulteti
Intellektual mulk va axborot texnologiyalari huquqi mutaxassisligi magistranti

Annotatsiya. Mazkur tadqiqot sun'iy intellekt asosida yaratilgan asarlarning mualliflik huquqi doirasida muhofazaga layoqatliligi masalasini O'zbekiston qonunchiligi kontekstida tahlil qiladi. Muallif sun'iy intellektning ijodkorlik xususiyatlari va insonga o'xshash qayta ishlash jarayonlariga asoslanib, uni nisbiy yuridik shaxs sifatida tan olish imkoniyatini ko'rib chiqadi. Tadqiqotda sun'iy intellekt yaratgan asarlarni yaratilganlik fakti asosida muhofaza qilish, majburiy sug'urtalash tizimi joriy etish va maxsus qonunchilik bazasi yaratish zaruriyati asoslanadi. Ishda shaxsiy nomulkiy, mulkiy va mutlaq huquqlarni himoya qilish mexanizmlari chuqur tahlil qilingan.

Kalit so’zlar: sun'iy intellekt, mualliflik huquqi, intellektual mulk, huquqiy muhofaza, ijodkorlik, originallik, qonunchilik, yuridik shaxs.

Kirish

Mualliflik huquqida yaratilgan obyektlarni huquqiy muhofazalash deganda obyektlarning subyektiv egalarining huquqlarini qonuniy jihatdan himoya qilish, qonun himoyasiga olish tushuniladi. Tushunilganidek, mualliflik huquqi obyektlari o‘z-o‘zidan emas, ma’lum huqularga egalik qiluvchi shaxslar, uning muallifining shaxsiy huquqlari, litsenziya shartnomasi asosida foydalanuvchisining huquqlari, mutlaq huquq sohiblarining huquqlari muhofaza ostiga olinishini tushunishimiz mumkin. Intellektual mulk obyektlarini huquqiy muhofaza ostiga olish: - ularning yaratilganlilik fakti asosida; - FKda yoki boshqa qonunlarda nazarda tutilgan hollarda va tartibda vakolatli davlat organi tomonidan huquqiy muhofaza hujjati berilishi asosida vujudga keladi[1]. Yaratilganlik fakti asosida himoyalash ayni mualliflik huquqi obyektlariga tegishli hisoblanadi. O‘zbekiston Respublikasi Oliy Majlisining 27.08.2004 yildagi 681-II-sonli Qarori bilan qabul qilingan “Adabiy va badiiy asarlarni muhofaza qilish to‘g‘risida”gi Bern Konvensiyasida avvalgi moddaning qoidalari hammualliflikda yaratilgan asarlar uchun ham qo‘llanadi, bunda muallifning vafot etgan vaqtidan e’tiboran belgilanadigan muddatlar boshqa hammualliflardan ortiq yashagan oxirgi muallifning vafot etgan vaqtidan e’tiboran hisoblanadi[2]. Shu asosda ham mualliflik yaratilganlik asosida muhofaza ostiga olinishini ko‘ramiz.

Mualliflik huquqi obyekti ijodkor tomonidan yaratilgan vaqtda u ommaga og‘zaki yoki yozma shaklda, shuningdek, biron turdagi tasvir shaklida idrok qilish imkonini beruvchi ko‘rinishda taqdim etishi mumkin. Ana shu vaqtdan boshlab, huquqlarning asl himoyasi boshlanadi. Obyektni yaratgan shaxs agar uni oshkor etmasa ham undagi huquqlar vujudga kelgan hisoblanadi. Faqatgina barchada asar yaratilganligi yuzasidan idrok shaklida tushuncha va xabardorlik bo‘lmas ekan buni himoyalash jarayoni murakkablashadi. Buning uchun muallif yoxud huquq egasi yaratilganlik faktini vaqti va muddati bilan o‘ziniki ekanligini isbotlay olishi lozim. Agarda huquq buzilib, boshqa shaxs tomonidan ushbu holatlar oshkor etilgan taqdirda ham asar boshqa huquq buzuvchi tomonidan e’lon qilinishidan oldin asl egasi tomonidan yaratilganligi isbotlanishi mumkin. Masalan, muallif bu ishni asarni qaysidir bosmaxonaga e’lon qilish maqsadi

bilan topshirgan bolishi yoxud saqlab turishga depozitariyga bergan bo‘lish fakti mumkin.

Asosiy qism

Intellektual mulk huquqi boshqa sohalarida, misol uchun “«Ixtiro, foydali model, sanoat namunalari to'g‘risida”gi Qonunga ko‘ra, yaratilgan ixtiro tegishli tarzda davlat ro‘yxatidan o‘tkazilishi yoxud kamida talabnoma berilgan bo‘lishi lozim. Shundagina subyektiv huquqlar muhofazaning 4 shakli bo‘lgan:

1. Ro‘yxatdan o‘tganlik
2. Talabnoma yuborganlik
3. Konvensiya
4. Ko‘rgazma ustuvorligi bilan muhofazalanadi.

Mualliflik huquqida esa yaratilganlik fakti uni oshkor etish yoki etmaganlikdan qat’iy nazar himoya qilinadi. “Mualliflik huquqi va turdosh huquqlar to‘g‘risida”gi Qonun 10-moddasiga asosan mualliflik huquqida obyektlar yaratilganlik fakti asosida muhofazaga olinadi. Bunda muallif o‘zining ijodiga mansubligini ko‘rsatish uchun asarda o‘z imzosini, ismini yoki boshqa belgilarini qoldirishi mumkin. Agarda asar taxallus bilan yoki imzosiz chop etilgan, ommaga oshkor etilgan taqdirda (muallif kimligiga shubha bo‘lmaydigan holler bundan mustasno), asarni chop etgan, asarda ismi ko‘rsatilgan noshir, agar boshqa dalillar mavjud bo‘lmasa, u muallifning vakili hisoblanadi hamda uning huquqlarini himoya qiluvchi vakil hisoblanadi[3]. Bu qoidani esa muallif o‘zini oshkor etgunicha saqlab turish mumkin. Bunda asarni oshkor etmoqchi bo‘lgan muallif, agar uning asar yuzasidan shartnomalarida boshqacha qoida belgilangan bo‘lmasa, oldindan ogohlantirib qo‘yishi lozim bo‘ladi.

Shunga ko‘ra, mualliflik huquqi obyektlari e’lon qilingan (oshkor qilingan, chop etilgan) yoki e’lon qilinmagan asarlar bo‘lishidan qat’iy nazar, mualliflik huquqi bilan muhofaza etilishi inobatga olinishi lozim[4]. Mualliflik huquqida fikr, g‘oya, usul va jarayonlar boshqa intellektual mulk huquq sohasi kabi muhofazalanmaydi. Aksincha, ifodaviy xarakterga va idrok ko‘rinishiga o‘tgachgina unga muhofaza beriladi. Bu 19-sonli

“Intellektual mulkka oid ishlarni ko‘rib chiqishning ayrim masalalari to‘g‘risida”gi Plenum qarorida ham aytib o‘tilgan.

Sun’iy intellekt tomonidan yaratilgan asarlar ham muhofazaga ayni intellekt yaratgan vaqt bilan belgilab qo‘yishimiz yanada osonlashadi. Intellektda baza mavjud. Bu bazada qachon va kimning buyrug‘i asosida yaratilganlikni ham hisoblab turadigan alohida funksiya qo‘shilishi natijasida ish osonlashishi ehtimoli yuqori. Bunda asar e’lon qilingan taqdirda bu haqiqatmi yoki teskarisimi aniqlab olishda hech qanday muammo va shubhalarga o‘rin qoldirmagan bo‘lar edik. Shuningdek, sun’iy intellekt asosida yaratilgan asarlarda alohida belgi qo‘yish tizimini ham ko‘rib chiqish mumkinligini ham hisobga olish lozim.

Muhofazaga muallifning shaxsiy nomulkiy, mulkiy va mutlaq huquqlari olinadi. Shaxsiy nomulkiy huquqi FKning 1051-moddasiga ko‘ra, asar muallifi deb e’tirof etilish huquqi (mualliflik huquqi);

asardan muallifning haqiqiy ismi, taxallusini ko‘rsatgan holda yoxud ismini ko‘rsatmasdan, ya’ni imzosiz foydalanish yoki foydalanishga ruxsat berish huquqi (mualliflik ismiga bo‘lgan huquq);

asarni har qanday shaklda oshkor qilish yoki oshkor qilishga ruxsat berish huquqi (oshkor qilishga bo‘lgan huquq), shu jumladan chaqirib olish huquqi;

asarni, shu jumladan uning nomini muallifning sha’ni va qadr-qimmatiga zarar yetkazishi mumkin bo‘lgan har qanday tarzda buzib ko‘rsatilishidan yoki har qanday boshqacha tarzda tajovuz etilishidan himoya qilish huquqi (muallif obro‘sini himoya qilish huquqi)[5] hisoblanadi. Hammualliflikda barchasining shu kabi huquqlari mavjud bo‘ladi va muhofaza himoya bosqichigacha davom etadi. Bu huquqlar mualliflik sifatida boshqaga berilmaydi. Shuningdek, bular tarkibiga asarni muallif roziligisiz omma oldida oshkor etish, ijro etish yoki asarga qo‘shimcha sharh, tuzatish va qismlar qo‘shish ham taqiqlanadi. Bunda originallikni isbotlab berish asosiyga chiqadi. To‘g‘ri syujet o‘xshash bo‘ladi, lekin originallikni mualliflik huquqi mutaxassislari ajrata olishadi. Ilhomlanish va ko‘chirishda farq bo‘ladi bu yozuv va ifoda usulidan kelib chiqadi.

Mutlaq mualliflik huquqlari egasi o‘z huquqlaridan xabardor qilish uchun mualliflik huquqining muhofaza belgisidan foydalanishi mumkin bo‘lib, bu belgi asarning har bir nusxasida aks ettiriladi va quyidagi uch unsurdan iborat bo‘ladi:

aylana ichidagi lotincha “S” harfi;

mutlaq mualliflik huquqlari egasining ismi-sharifi (nomi); asar birinchi marta chop etilgan yil.

Mualliflik huquqining muhofaza belgisida ko‘rsatilgan shaxs, agar boshqacha hol isbotlangan bo‘lmasa, mutlaq mualliflik huquqlari egasi hisoblanadi[6].

Mamlakatimizda mualliflik huquqi obyektlarini ro‘yxatdan o‘tkazish amaliyoti mavjud emas. Muallif muhofaza olgach, barcha mulkiy, shaxsiy nomulkiy va mutlaq huquqlarni egallaydi va bu huquqlarni erkin amalga oshirish mumkin. himoyasi esa qonun bilan qo‘riqlanadi. Asarni begonalashtirishga ham mualliflarning roziliklari olinishi lozim bo‘ladi.

Sun’iy intellektda hammualliflik taklif etilayotganligi bilan shuni aytmoqchimanki, sun’iy intellektni yuqorida ko‘rsatib o‘tganimdek nisbatan subyekt sifatida baholash mantiqqa yaqinroq bo‘ladi va buni to‘la mantiqiy deyishdan ham ancha yiroqman. Biz muallif deb tan olish uchun sun’iy intellektda barcha ijodkorlik, originallik kabi xususiyatlar jamlanmoqda. Qayta ishlash ham bizning miyyamizning ishi kabidir. Biz ham ma’lumotlarni yig‘amiz. Nimadir asar yaratishimiz uchun oldin fikr, g‘oya paydo bo‘ladi, so‘ngra uni amalga oshirish yo‘llarini hamda bu yo‘lda qanday yordam olishimiz mumkinligi haqida o‘ylaymiz. Hattoki, badiiy asar yoza olish uchun ham oldin badiiy asarni o‘qigan yoki u nima ekanligini bilishimiz kerak. Ba’zilar yo‘q badiiy asar uchun ichki kechinmalar kerak bo‘ladi deb hisoblashadi. Lekin hamma ham ichki kechinmalarni o‘quvchiga tushunarli qilib yetkaza olmaydi, agarki, u oldin birorta badiiy asar o‘qimagan bo‘lsa. Yozuvchilarda ham yozishdan oldin o‘qish ko‘nikmasi shakllanadi. Turli xil kundaliklarni asar qilishda esa, albatta, biror yozuvchi yoki ijodkorning yozish usulidan foydalanilishini unutmasligimiz lozim. Shu uchun ham sun’iy intellekt yaratgan asarlarga mualliflik huquqini berishda uning yaratilganligi bilan muhofaza berish fikrida qolamiz. Bu uchun

dasturchi tomonidan tuziladigan dasturda shartnomani foydalanuvchiga ko‘rsatish bilan bir qatorda asar yaratish boshlangan va tugallangan vaqtni aniqlab ko‘rsatuvchi funksiya ham qo‘shilishi maqsadlidir.

Xulosa

Haqiqatan, sun’iy intellekt ijodkorlik xususiyati mavjud, garchi u bilimlarni sun’iy yo‘l bilan olsada, insondagi qayta ishlash sistemasini o‘zida namoyon qila olgan. Bunda undagi dastur unga yordamchi va ishlashida insonga o‘xshashida ko‘mak beradi, xolos. Mualliflik huquqi ham uni ro‘yxatdan o‘tkazish bilan yoki ommaga oshkor qilish bilan emas, faqatgina yaratganlik va buni isbotlaganlik bilan muhofaza qilinadi va huquqlar subyektga beriladi. Sun’iy intellektni subyekt emas deb hsioblaydigan fikrlar ham yo‘q emas, lekin yuridik shaxsni subyekt deb hisoblaganimiz kabi uni ham nisbiy tarzda yuridik shaxs qoidalarini subsidiary qo‘llab, huquq egasi sifatida ko‘ra olamiz. Huquq egasi siaftida sun’iy intellektni yaratgan dastur muallifi yoxud dastlabki egasidan mulkiy va mutlaq huquqlar begonalashtirilgan bo‘lsa (negaki, shaxsiy nomulkiy begonalashtirilmasligini aytib o‘tdik), ayni vaqtda huquq egasi sifatida sun’iy intellektdan foydalanuvchi egasini, shaxsni, ko‘rsatib qo‘yishimiz mumkin. sun’iy intellektning oshiqcha xavf vujudga keltirishi oldini olish uchun esa unga avtotransport vositasini sug‘urtalash tizimiga o‘xshab, majburiy sug‘urtalash tizimini joriy qilish lozim bo‘ladi. Foydalanuvchi esa undan foydalanish uchun shunchaki huquqni tekin olmasdan to‘lov evaziga olsa, intellekt xotira bazasida ham qolishi osonlashadi. Bundan tashqari, sun’iy intellekt ishlashi uchun lozim manbalarni ham haqqoniy yo‘l bilan olishi, o‘rganish uchun olgan ma’lumotlari ochiq saytdagiligiga ishonch hosil qilinishi hamda mualliflik obyektlari uchun qonuniy foydalanishni nazarda tutuvchi tizim va qonunchilik bazasi ham zarur.

Foydalanilgan adabiyotlar

1. Fuqarolik huquqi. Q.II/M. Abdusalomov, X. Azizov, B.Axmadjonov va boshq.; O'zbekiston Respublikasi Adliya vazirligi, Toshkent Davlat yuridik instituti. - Toshkent: Adolat, 2007. 650-b.
2. Intellektual mulk. Darslik. Mas'ul muharrirlar: yu.f.d., prof., O.Oqyulov, yu.f.f.d. (Phd), dotsent N.E.Gafurova//Mualliflar jamoasi: - T.: TDYU nashriyoti, 2019 – 588 bet.
3. O‘zbekiston Respublikasi Fuqarolik Kodeksi.
4. O‘zbekiston Respublikasi Oliy Majlisining 27.08.2004 yildagi 681-II-sonli Qarori bilan qabul qilingan “Adabiy va badiiy asarlarni muhofaza qilish to‘g‘risida”gi Bern Konvensiyasi.
5. O‘zbekiston Respublikasi Oliy sudi plenumning qarori, 23.06.2023 yildagi 19-son.

---

[1] Fuqarolik huquqi. Q.II/M. Abdusalomov, X. Azizov, B.Axmadjonov va boshq.; O'zbekiston Respublikasi Adliya vazirligi, Toshkent Davlat yuridik instituti. - Toshkent: Adolat, 2007. 650-b.

[2] O‘zbekiston Respublikasi Oliy Majlisining 27.08.2004 yildagi 681-II-sonli Qarori bilan qabul qilingan “Adabiy va badiiy asarlarni muhofaza qilish to‘g‘risida”gi Bern Konvensiyasi https://lex.uz/docs/-1310607#-5624834

[3] Intellektual mulk. Darslik. Mas'ul muharrirlar: yu.f.d., prof., O.Oqyulov, yu.f.f.d. (Phd), dotsent N.E.Gafurova//Mualliflar jamoasi: - T.: TDYU nashriyoti, 2019 – 588 bet.

[4] O‘zbekiston Respublikasi Oliy sudi plenumning qarori, 23.06.2023 yildagi 19-son, https://lex.uz/uz/docs/- 6522606 (kirish vaqti:13.03.2024)

[5] O‘zbekiston Respublikasi Fuqarolik Kodeksi, https://lex.uz/docs/-180552 (kirish vaqti: 13.03.2025)

[6] O‘zbekiston Respublikasi Fuqarolik Kodeksi, https://lex.uz/docs/-180552 (kirish vaqti: 13.03.2025)

KIBERJINOYATLARNI TERGOV QILISHGA DOIR XALQARO STANDART HAMDA USHBU TURDAGI JINOYATLARNI TERGOV QILISHDA DAVLATLARNING MANFAATLI HAMKORLIGI MASALALARINING DOLZARBLIGI

Mirjalil Mirsamatov

mrjalilsamatov0827@gmail.com

Toshkent davlat yuridik universiteti
Magistratura bosqichi “Kiber huquq”
yo‘nalishi magistranti

Annotatsiya. Ushbu maqolada kiberjinoyatlarga qarshi kurashish va ularni tergov qilishda xalqaro hamkorlik masalalari, kiberjinoyatlarni tergov qilishni tartibga soluvchi global standartlar va me'yoriy bazalar tahlil qilingan. Tadqiqotda xalqaro tashkilotlarning maqomi hamda kiberxavfsizlik va maxfiylikni himoya qilish sohasida yagona huquqiy siyosatni ishlab chiqish istiqbollari o'rganilgan. Asosiy xalqaro hujjatlar, jumladan Kiberjinoyatchilik bo'yicha Budapesht konvensiyasi (2001), Afrika Ittifoqining Kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilish konvensiyasi (2014) va MDH davlatlarining axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish bitimi (2018) tahlil etilgan. Tadqiqot natijasida mavjud ko'p tomonlama kelishuvlarga qaramay, keng qamrovli global kiberjinoyatchilik shartnomasining yo'qligi kibermakonni huquqiy tartibga solishda jiddiy bo'shliqlar mavjudligini ko'rsatdi.

Kalit so’zlar: xalqaro hamkorlik, kiberjinoyatlar, kibermakon, axborot xavfsizligi, huquqiy asoslar, tergov standartlari.

KIRISH

Zamonaviy dunyoda axborot jamiyat taraqqiyotining eng muhim tarkibiy qismiga aylandi desak aslo mubolag‘a bo‘lmaydi.Jamiyatning axborot jamiyatiga aylanishi shuni anglatadiki, har qanday shaxsiy ma’lumot ahamiyatli bo‘lib bormoqda. Ayni paytda ma’lumot eng muhim qadriyatlardan biri sifatida tan olingan, shunga ko‘ra, uning himoyasi uni qabul qilish va etkazishdan kam bo‘lmagan muhim faoliyatdir. Masalan,Arab bahori deb atalmish inqilobiy voqealar ommaviy axborot vositalari va siyosiy nutqdagi axborot-kommunikatsiya texnologiyalarining roli bilan uzviy bog‘liq bo‘lib chiqdi. Misli ko‘rilmagan axborot tarqatish tezligi Internet (asosan ijtimoiy tarmoqlar orqali) yashirinishni istagan rejimlarga qarshi harakatlari xalqaro miqyosdagi repressiv harakatlari jamoatchilik va axborot urushini olib borish bo‘yicha etarli mahoratga ega bo‘lmagan. Hozirgi vaqtda globallashuv tendensiyalari va u olib keladigan muammolari kuchaymoqda. Bunday sharoitda transmilliy kiberjinoyatlarga qarshi kurashishda barchaning ishtirok etish masalasi global qonun ustuvorligining salbiy oqibatlariga barham beradi. Kiberjinoyatchilik muammosining global mohiyatini tushunish juda muhimdir. Shunday qilib, hozirda kiberhujumlar nafaqat xususiy shaxslarning ishini falaj qilmoqda balki dunyodagi tuzilmalarni ham, ushbu turdagi hujumlardan himoyalanishni amalga oshiradigandavlat organlari ham, davlat ham yo‘q. Ehtimol kiber tahdid manbalari nafaqat xakerlar yoki ularning guruhlari, balki alohida davlatlar, terroristik, jinoiy guruhlar ham hisoblanadi. Kiberjinoyatlarga qarshi kurashishda kurashish vositalari va usullarini ishlab chiqishdajinoyatning latentlikdarajasidan xabardor bo‘lishi kerak. Mutaxassislar taxminiga ko‘ra “kompyuter jinoyati”ning latentligi AQShda 80% ga, Buyuk Britaniyada - 85% ga, Germaniyada - 75% ga, Rossiyada - 90%ga ko‘proqdir [1]. Symantec Security xalqaro kiberxavfsizlik xizmati ma’lumotlariga ko‘ra, “har soniyada” dunyo bo‘ylab 12 kishi kiberhujumga uchraydi va dunyoda har yili taxminan 556 mln kiberjinoyatlar sodir etiladi va buning natijasida 100 milliardAQSh dollardan ziyod zarar yetkaziladi[2]. Masalan, Qo‘shma Shtatlarda, allaqachon faoliyat ko‘rsatayotgan Milliy kiberxavfsizlik markazi bilan bir qatorda Qurolli Kuchlar Birlashgan Kiber Qo‘mondonligi harbiy harakatlarni amalga oshirish paytida Pentagon tuzilmalari tegishli yordamni taqdim etadi. Bu global miqyosda barchaning sa’y-harakatlarini muvofiqlashtirib boradi. Fuqarolik federal

institutlari va shunga o‘xshash dasturiy ta’minot bilan o‘zaro aloqadadir[3]. Shu bilan birga, ushbu tashkilotlar qisman nazorat qilinadigan bo‘limlardir, chunki nazorat qiluvchi tuzilma “Kengashdir”. Milliy xavfsizlik mas’uliyat sohasidagi qo‘mitalar axborot strategiyasini amalga oshirishni o‘z ichiga oladi [4]. Kiberqurol dasturlari Buyuk Britaniyada rasmiylarning kiber kosmosdan kelib chiqadigan tahdidlarga qarshi turish qobiliyatini ta’minlashda amalga oshiriladi[5]. Avstraliyada elektron pochta xavfsizligini muvofiqlashtirish guruhi tashkil etilgan bo‘lib, ushbu guruhning asosiy vazifasiham davlat, ham xususiy sektor uchun operatsion makonni ishonchli himoya elektron tizim yaratishdir[6]. Kiberjinoyatlarning oldini olish bo‘yicha tadbirlar nafaqat alohida davlatlar tomonidan amalga oshiriladi, balki ularning bloklari, xususan NATO tomonidan amalga oshirilib kelinmoqda.. Shunday qilib,so‘nggi yillarda qabul qilingan barcha blok-yo‘riq hujjatlarida aks ettirilgani ushbu muammoning ahamiyati ko‘rsatib beradi. Strategik jihatdan birinchi marta NATO konsepsiyasida alyans faoliyatida qoidalar kiritilgan bo‘lib harbiy sohaning yangi yo‘nalishi sifatida kiber maydon paydo bo‘lgan[7].

ADABIYOTLAR TAHLILI VA METODLAR

Tadqiqot jarayonida ilmiy bilishning mantiqiylik, tarixiylik, izchillik, obyektivlik usulidan foydalanilgan bo‘lib, mavzuni yoritishda tavsifiy, qiyosiy metodlardan foydalanildi. Maqolada kiberjinoyatlarni tergov qilishga doir xalqaro standart hamda ushbu turdagi jinoyatlarni tergov qilishda davlatlarning manfaatli hamkorligi masalalari obyektiv yoritib berildi.

MUHOKAMA VA NATIJALAR

Kiberjinoyatchilikka qarshi Budapesht konvensiyasi 2001-yil 23-noyabr’, Internet va kompyuter jinoyati (kiberjinoyat)larni uyg‘unlashtirish orqali milliy qonunlar, tergov usullarini takomillashtirish va xalqlar o‘rtasidagi hamkorlikni oshirish yuzasidan imzolangan. Konvensiya va uning izohli ma’ruzasi Yevropa Kengashi Vazirlar qo‘mitasi 2001-yil 8-noyabrdagi 109-sessiyasida imzolash uchun Budapeshtda ochilgan va 2001-yil 23-noyabrda kuchga kirgan. 2019-yil sentyabr oyiga qadar 64 davlat ushbu konvensiyani ratifikatsiya qildi, yana to‘rtta davlat konvensiyani imzoladi, ammo uni tasdiqlamadi[8].

U kuchga kirgandan buyon Braziliya va Hindiston kabi muhim davlatlar Konvensiyani ishlab chiqishda qatnashmaganliklari sababli qabul qilishdan bosh

tortdilar. Bu kiberjinoyatchilikni tartibga soluvchi birinchi ko‘p tomonlama huquqiy majburiy vositadir. 2018-yildan boshlab, Hindiston kiberjinoyatchilik kuchayganidan keyin Konvensiyadagi pozisiyasini qayta ko‘rib chiqmoqda, ammo chet el agentliklari bilan ma’lumot almashish xavotirlari uni ratifikatsiya qilishdan saqlab qolmoqda.

2006-yil 1-martda Kiberjinoyatchilik to‘g‘risidagi konvesiyaga qo‘shimcha protokol kuchga kirdi. Qo‘shimcha protokolni ratifikatsiya qilgan davlatlar irqchi va ksenofobik kompyuter tizimlari orqali material, shuningdek, irqchilik yoki ksenofobiya tomonidan tahdid va haqorattarqatishni jinoiy javobgarlikka tortishlari shartligi belgilandi[9].

Konvensiya Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar bo‘yicha birinchi xalqaro shartnomadir, xususan mualliflik huquqining buzilishi, kompyuter bilan bog‘liq firibgarlik, bolalar pornografiyasi, tahdid jinoyatlariva tarmoq xavfsizligi jinoyatlarigi o‘z ichiga oladi. Shuningdek, u kompyuter tarmoqlarini qidirish va qonuniy ushlashga doir qator vakolatlar va protseduralarni o‘z ichiga oladi. Uning muqaddimasida keltirilgan asosiy maqsadi jamiyatni himoya qilishga qaratilgan umumiy jinoyat siyosatini olib borishdir. Shuningdek, kiberjinoyatlargadoir tegishli qonunlarni qabul qilish va joriy etish orqali xalqaro hamkorlikni targ‘ib etadi.

Konvensiya asosan quyidagilarga qaratilgan:

-kiberjinoyatchilik sohasidagi huquqbuzarliklar va ular bilan bog‘liq qoidalarni ichki jinoyat moddiy-huquqiy elementlarini uyg‘unlashtirish;

-ichki jinoyat-protsessual qonunchiligini tergov qilish va jinoiy javobgarlikka tortish uchun zarur bo‘lgan vakolatlarni, shuningdek, elektron tizimda bo‘lgan kompyuter tizimi yoki dalillar yordamida sodir etilgan boshqa huquqbuzarliklarni ta’minlash;

-xalqaro hamkorlikning tezkor va samarali rejimini o‘rnatish;

Konvensiya tomonidan quyidagi huquqbuzarliklar belgilangan: noqonuniy kirish, noqonuniy yo‘l bilan tutish, ma’lumotlarga aralashish, tizimga aralashish, qurilmalardan noto‘g‘ri foydalanish, kompyuter bilan bog‘liq qalbakilashtirish, kompyuter bilan bog‘liq firibgarlik, bolalar pornografiyasiva mualliflik huquqi va qo‘shni huquqlar bilan bog‘liq huquqbuzarliklardir[10].

Shu bilan bir qatorda 2014-yilda Afrika Ittifoqining Kiberxavfsizlik va shaxsiy ma’lumotlarni himoya qilish to‘g‘risidagi konvensiyasida kiberjinoyatlani tergov qilishda Afrika davlatlarining o‘zaro ianfaatli hamkorligi masalalari ko‘rib o‘tilgan.

Xususan, unda nazarda tutilishicha konvensiya ishtirokchilarining kibermakonda huquq va erkinliklari kafolatlanishi belgilanib qo‘yilgan[11].

Darhaqiqat, ko‘rishimiz mumkinki butun dunyo ushbu turdagi jinoyatlarga kurashayotgan bir davrda MDH mamlakatlari ham bundan chetda turmadi. 2018-yil 28-sentabr kiberjinoyatlarni tergov qilishda hamkorlik qilish masalasini tartibga soluvchi ixtisoslashtirilgan hujjatlardan biri hisoblanmish Mustaqil Davlatlar Hamdo‘stligiga a’zo davlatlar o‘rtasida axborot texnologiyalari sohasida jinoyatlarga qarshi kurashish bo‘yicha Bitim imzolandi. Ozarbayjon Respublikasi, Armaniston Respublikasi, Belorusiya, Qozog‘iston, Qirg‘iziston Respublikasi, Rossiya Federatsiyasi, Moldova Respublikasi, Tojikiston, Turkmaniston, O‘zbekiston va Ukraina ushbu Bitim qatnashchilaridir. O‘zbekiston Respublikasi Prezidentining 13.02.2019 yildagi PQ-4188-sonli qarori bilan 2018-yil 28-sentyabrda MDH davlatlari rahbarlari kengashining majlisida imzolangan Mustaqil Davlatlar Hamdo‘stligiga a’zo davlatlar o‘rtasida axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish sohasida hamkorlik to‘g‘risidagi Bitimni tasdiqladi. Ushbu Bitimni amalga oshirish bo‘yicha vakolatli organlar sifatida O‘zbekiston Respublikasi Ichki ishlar vazirligi, Davlat xavfsizlik xizmati va Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo‘yicha davlat inspeksiyasi belgilandi. Ushbu hujjat doirasida, axborot texnologiyalari sohasida quyidagi harakatlarni (agar ular qasddan qilingan bo‘lsa) tergov qilishda Bitimga qo‘shilgan davlatlar bilan hamkorlik qilish mumkin:

a) axborotni yo‘q qilish, blokirovka qilish, o‘zgartirish yoki nusxalash, axborot (kompyuter) tizimining ishlashini qonun bilan himoyalangan kompyuter ma’lumot lariga ruxsatsiz kirish orqali xalaqit berish;

b) zarar keltiruvchi dastur larni yaratish, foydalanish yoki tarqatish;

c) kompyuter tizimidan foydalanish huquqiga ega bo‘lgan shaxs tomonidan qonun bilan qo‘riqlanadigan kompyuter ma’lumotlarini yo‘q qilishga, blokirovka qilishga yoki o‘zgartirishga olib keladigan qoida larning buzilishi, agar bu xatti-harakatlar jiddiy zarar yoki jiddiy oqibat larga olib kelgan bo‘lsa;

d) kompyuter ommaviy axborot vosita larida saqlanadigan yoki ma’lumotlar tarmoqlari orqali uzatiladigan kompyuter tizimida ishlov berilgan ma’lumotni o‘zgartirish yoki kompyuter tizimiga noto‘g‘ri ma’lumotlar kiritish orqali mulkni o‘g‘irlash;

e) qonun bilan himoyalangan kompyuter ma’lumotlariga ruxsatsiz kirish bilan;

f) pornografik materiallar yoki voyaga yetmagan shaxs tasvirlangan pornografik xususiyatga ega obyektlarni “Internet” axborot-telekommunikatsiya tarmog‘idan yoki boshqa elektr aloqa kanallaridan foydalangan holda tarqatish;

g) xavfsiz kompyuter tizimi yoki tarmog‘iga ruxsatsiz kira olish uchun marketing yoki maxsus dasturiy yoki apparat vosita larini sotish uchun ishlab chiqarish;

h) mualliflik huquqiga ega bo‘lgan kompyuter tizim lari va ma’lumotlar bazalari uchun dasturiy ta’minotdan noqonuniy foydalanish, shuningdek, mualliflik huquqini o‘zlashtirish, basharti bu harakat jiddiy zarar yetkazgan bo‘lsa;

i) “Internet” axborot-telekommunikatsiya tarmog‘i yoki boshqa elektr aloqa kanallari yordamida belgilangan tartibda ekstremistik deb tan olingan yoki terrorchilik faoliyatini yoki terrorizmni oqlashga qaratilgan materiallarni tarqatish”[12].

XULOSA VA TAKLIFLAR

Xulosa qilib shuni aytishimiz mumkinki, ushbu sohadagi xalqaro hamkorlik turli xil jarayonlarni yaratishni o‘z ichiga oladi. Xalqaro tashkilotlar asosiy maqsad sifatida uyushgan jinoiy tarmoqlar faoliyatiga barham berishni oliy maqsad sifatida belgilab olishlari zarurdir. Fikrimiz yakunida taklif sifatida shuni aytishimiz mumkinki, kiberjinoyatchilikka qarshi kurashish tartibini tartibga soluvchi yagona global hujjat ishlab chiqilmagan bo‘lib, kiber kosmosdagi subyektlarning harakatlarini qonuniy tartibga solish, kiberjinoyatchilikka qarshi kurashish choralarini sayozligicha qolmoqda.

Foydalanilgan adabiyotlar

1. Vardanyan A.V., Nikitina E.V. Расследованиепреступлении в сферевйсокикҳтекҳнологииикомпъютерноиинформатсии [Investigation of Hi-Tech and Computer Information Crimes]. Moscow, Yurlitinform Publ.

2. Karpova D.N. Cybercrimes: a global issue and its solution. Vlast'= The Power no. 8, pp. 46–50. (In Russian).

3.Berd K. A war with many unknown quantities. Computerra, 2009, no. 20, pp. 26– 29. (In Russian).

4. Zav'yalov S. International experience in fighting the propaganda of terrorism in the Internet. Zarubezhnoevoennoeobozrenie = Foreign Military Review, 2014, no. 4, pp. 34–39. (In Russian).

5. Khimchenko I.A. Informatsionnoeobshchestvo: pravovyeproblemy v usloviyakhglobalizatsii. Kand. Diss.[Information society: legal basis in the conditions of globalization. Cand. Diss.]. Moscow, 2014. 174 p

6. Zgadzai O.E., Kazantsev S. Ya. Cybercrime: factors of danger and problems of struggle. Vestnik GU «Nauchnyitsentrbezopasnostizhiznedeyatel'nostidetei» = Bulletin of «Research Center for the Security of Children», 2013, no. 4 (18), pp. 80–86. (In Russian).

7. Gradov A. The activities of the North Atlantic Treaty Organization in the sphere of cyber-security. Zarubezhnoevoennoeobozrenie = Foreign Military Review, 2014, no. 7, pp. 13–16. (In Russian)

8. Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL:www.coe.int/en/web/cybercrime/the-budapest-convention

9. http://indianexpress.com/article/india/home-ministry-pitches-for-budapestconvention-on-cyber-security-rajnath-singh-5029314/

10. Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL: www.coe.int/en/web/cybercrime/the-budapest-convention african-union-conventioncyber-security-andpersonal-data-protection

11. Мустақил Давлатлар Ҳамдўстлигига аъзо давлатларнинг ахборот технология лари соҳасидаги жиноятларга қарши кураш бўйича ҳамкорлиги тўғрисида"ги Битим, 3-моддаси.

[1] 1 Vardanyan A.V., Nikitina E.V. Rassledovanieprestuplenii v sferevyso-kikhtekhnologiiikomp'yuternoiinformatsii [Investigation of Hi-Tech and Computer Information Crimes]. Moscow, Yurlitinform Publ.
[2] 2Karpova D.N. Cybercrimes: a global issue and its solution. Vlast'= The Power no. 8, pp. 46–50. (In Russian).
[3] Berd K. A war with many unknown quantities. Computerra, 2009, no. 20, pp. 26–29. (In Russian)
[4] Zav'yalov S. International experience in fighting the propaganda of terrorism in the Internet. Zarubezhnoevoennoeobozrenie = Foreign Military Review, 2014, no. 4, pp. 34–39. (In Russian).
[5] Khimchenko I.A. Informatsionnoeobshchestvo: pravovyeproblemy v usloviyakhglobalizatsii. Kand. Diss.[Information society: legal basis in the conditions of globalization. Cand. Diss.]. Moscow, 2014. 174 p
[6] Zgadzai O.E., Kazantsev S. Ya. Cybercrime: factors of danger and problems of struggle. Vestnik GU «Nauchnyitsentrbezopasnostizhiznedeyatel'nostidetei» = Bulletin of «Research Center for the Security of Children», 2013, no. 4 (18), pp. 80–86. (In Russian).
[7] Gradov A. The activities of the North Atlantic Treaty Organization in the sphere of cyber-security. Zarubezhnoevoennoeobozrenie = Foreign Military Review, 2014, no. 7, pp. 13–16. (In Russian)
[8] Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL: www.coe.int/ en/web/cybercrime/the-budapest-convention
[9] https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/
[10] Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL: www.coe.int/en/web/cybercrime/thebudapest-convention
[11] african-union-convention-cyber-security-andpersonal-data-protection
[12] "Мустақил Давлат лар Ҳамдўстлигига аъзо давлат ларнинг ахборот технология лари соҳаси-даги жиноят ларга қарши кураш бўйича ҳамкорлиги тўғрисида"ги Битим, 3-моддаси

elita.uz

№ 1 (3) 2025

KIBERJINOYATLARNI TERGOV QILISHNING O‘ZIGA XOS XUSUSIYATLARI

Nodirjon Xabibiddinov

n.xabibiddinov@tsul.uz

Toshkent davlat yuridik universiteti
Jinoyat-protsessual huquqi kafedrasi o‘qituvchi-yordamchisi
Magistratura va sirtqi ta’lim fakulteti
Kiber huquq yo‘nalishi talabasi

Annotatsiya. Zamonaviy raqamli texnologiyalarning jadal rivojlanishi natijasida kiberjinoyatlar soni va murakkablik darajasi sezilarli darajada ortib bormoqda. Ushbu tadqiqot kiberjinoyatlarni tergov qilishning o'ziga xos xususiyatlari, mavjud muammolar va ularning yechim yo'llarini tahlil qiladi. Maqolada kiberjinoyatlarning asosiy turlari, sodir etilish usullari, tergov jarayonida qo'llaniladigan zamonaviy texnologiyalar va xalqaro hamkorlik masalalari ko'rib chiqilgan. Tadqiqot natijalari raqamli dalillarni to'plash murakkabligi, maxsus texnik bilimlar zarurligini va kiberxavfsizlik sohasidagi mutaxassislarning yetishmasligini ko'rsatadi. Kiberjinoyatlarga qarshi samarali kurashish uchun normativ-huquqiy bazani takomillashtirish va xalqaro standartlarni joriy etish tavsiya etilgan.

Kalit so’zlar: kiberjinoyatlar, raqamli dalillar, kiberxavfsizlik, kompyuter-texnik ekspertiza, xalqaro hamkorlik, raqamli kriminalistika, kiberhujumlar, tergov metodikasi.

KIRISH

Zamonaviy axborot texnologiyalari jamiyat hayotining barcha jabhalariga kirib kelishi natijasida yangi turdagi jinoyatlar – kiberjinoyatlar paydo bo‘la boshladi. Global internet tarmog‘i va raqamli texnologiyalarning jadal rivojlanishi natijasida kiberjinoyatlar soni va ularning murakkablik darajasi yildan-yilga ortib bormoqda.

Kibermuhitda sodir etilgan jinoyatlar soni kompyuter tarmoqlaridan foydalanuvchilar soniga mutanosib ravishda o‘sib bormoqda va Xalqaro jinoyat politsiyasi tashkiloti – Interpol hisob-kitoblariga ko‘ra, global internet tarmog‘ida ushbu jinoyatchilikning o‘sish sur’ati sayyoramizda eng tezkor hisoblanadi[1].

Hozirgi vaqtda globallashuv va u olib keladigan muammolar kuchaymoqda. Bunday sharoitda transmilliy kiberjinoyatlarga qarshi kurashishda barchaning ishtirok etish masalasi juda muhim hisoblanadi. Kiberjinoyatlarga qarshi kurashishda kurashish vositalari va usullarini ishlab chiqishda jinoyatning latentlik darajasidan xabardor bo‘lishi kerak. Mutaxassislar taxminiga ko‘ra “kompyuter jinoyatlari”ning latentligi AQShda 80%ni, Buyuk Britaniyada - 85%ni, Germaniyada - 75%ni, Rossiyada - 90%ni tashkil qiladi[2].

Tahlillarga ko‘ra, dunyo bo‘ylab har yili 500 milliondan ortiq kiber hujumlar sodir etiladi. Har soniyada 12 nafar insondan biri virtual makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo‘shma Shtatlari, Angliya, Germaniya, Belgiya kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda[3]. O‘zbekistonda ham so‘nggi uch yilda bu turdagi jinoyatlar 25 baravarga ko‘paygan. 2023-yilning 11 oyida 5,5 mingta kiberjinoyat sodir etilgan[4]. Shundan 70 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘irlik jinoyatlari hisoblanadi. Bundan tashqari, noqonuniy bank-moliya operatsiyalari 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. Hozirda bunday jinoyatlarning oldini olish uchun profilaktik chora-tadbirlar bilan bir qatorda ularni fosh etish bo‘yicha qator tashkiliy-texnik tadbirlar amalga oshirilmoqda.

Kiberjinoyatlarning xavfliligi shundaki, ular nafaqat alohida shaxslarga, balki davlat organlari, bank tizimlari, ta’lim va sog‘liqni saqlash muassasalari kabi

muhim infratuzilma obyektlariga ham jiddiy zarar yetkazishi mumkin. So‘nggi yillarda O‘zbekistonda ham kiberjinoyatchilikka qarshi kurashish masalasiga alohida e’tibor qaratilmoqda. Xususan, “Kibexavfsizlik to‘g‘risida”gi qonun qabul qilinishi, kiberxavfsizlik markazi tashkil etilishi hamda huquqni muhofaza qiluvchi organlar tarkibida maxsus bo‘linmalar faoliyatining yo‘lga qo‘yilishi buning yaqqol dalilidir. Lekin, kiberjinoyatlarni tergov qilish jarayonida bir qator muammolar mavjud bo‘lib, ular:

- raqamli dalillarni to‘plash va saqlashning murakkabligi;

- kiberjinoyatlarning tranmilliy xususiyati tufayli xalqaro hamkorlikni talab etishi;

- maxsus texnik bilim va ko‘nikmalarning zarurligi;

- raqamli kriminalistika sohasidagi mutaxassislarning yetishmasligi;

- zamonaviy dasturiy-texnik vositalarning qimmatligi kabilardir.

Yuqoridagilardan kelib chiqib, ushbu maqolaning maqsadi kiberjinoyatlarni tergov qilishning o‘ziga xos xususiyatlarini o‘rganish, mavjud muammolarni aniqlash va ularning yechimiga qaratilgan taklif-tavsiyalar ishlab chiqishdan iborat. Tadqiqot doirasida quyidagi vazifalar belgilangan:

- kiberjinoyatlarning zamonaviy turlari va ularning sodir etilish usullarini tahlil qilish;

- xorijiy davlatlarning kiberjinoyatlarni tergov qilish tajribasini o‘rganish;

- kiberjinoyatlarni tergov qilish samaradorligini oshirish bo‘yicha amaliy tavsiyalar ishlab chiqish.

METODLAR

Adabiyotlar tahlili: Ushbu tadqiqot kiberjinoyatlarni tergov qilishning o‘ziga xos xususiyatlarini aniqlash maqsadida yetakchi nazariy va amaliy manbalarni tahlil qiladi. Bu jarayonda Google Scholar, Science Direct va Cyberleninka kabi ilmiy ma’lumotlar bazalaridan foydalanildi. Adabiyotlar tahlilida kiberjinoyatlarning texnik va huquqiy jihatlari, tergov usullari, shuningdek, xalqaro tajribalar e’tiborga olindi. Shu bilan birga, kiberjinoyatlarni tergov qilish, raqamli dalillarni yig‘ish va tahlil qilish haqidagi ilmiy maqolalar, kitoblar va konferensiya materiallari ko‘rib chiqildi.

Hodisani o‘rganish (case study): Toshkent davlat yuridik universiteti Kriminalistika va sud ekspertizasi kafedrasi tomonidan tashkil etilgan “Raqamli

kriminalistika” ilmiy to‘garagi doirasida namunaviy raqamli dalillar tahlil qilindi va bir nechta holatlar ko‘rib chiqildi. Ushbu holatlarda qo‘llanilgan tergov strategiyalari va raqamli kriminalistika usullarining samaradorligi o‘rganildi.

Kontent-tahlil: Kiberjinoyatlarni tergov qilishda foydalaniladigan raqamli vositalar haqida ma’lumot to‘plash maqsadida xalqaro kiberxavfsizlik tashkilotlarining veb-saytlari, tahliliy hisobotlar va tegishli hukumat portallari o‘rganildi.

Qiyosiy tahlil: Kiberjinoyatlarni tergov qilish jarayonida turli davlatlarda qo‘llanilgan usullar va yondashuvlarning samaradorligini qiyoslash uchun davlatlararo qiyosiy tahlil o‘tkazildi. Bunda tegishli tashkilotlarning kiberjinoyatlar bilan bog‘liq faoliyat ko‘rsatkichlari va xalqaro hamkorlik natijalari tahlil qilindi.

NATIJALAR

Ushbu tadqiqot natijalari kiberjinoyatlarni tergov qilishdagi asosiy qiyinchiliklarni, samarali strategiyalarning ahamiyatini yoritadi. Natijalar quyidagilarni o‘z ichiga oladi:

Asosiy qiyinchiliklar: Tahlil natijalariga ko‘ra, tergovchilarning ko‘pchiligida kiberjinoyatlarni tergov qilishda texnologik bilimlar yetarli emas va texnik infratuzilmaning kamchiliklari muammoli bo‘lib kelmoqda. Ayniqsa, IP-manzillarni aniqlash, ma’lumotlarni tiklash, va transmilliy jinoyatlarni tergov qilishda huquqiy chegaralar qiyinchilik tug‘dirmoqda.

Yangi texnologiyalarning qo‘llanilishi: Natijalar kiberjinoyatlarni tergov qilishda sun’iy intellekt, mashinani o‘rganish (machine learning), va katta ma’lumotlarni (big data) tahlil qilish texnologiyalari sezilarli yutuqlarni ta’minlayotganini ko‘rsatadi. Ayniqsa, raqamli kriminalistika vositalaridan foydalanish va kiberxavfsizlik dasturlari kiberjinoyatlarning izini topish va dalillarni to‘plashda katta hissa qo‘shmoqda.

Kiberjinoyatlar bo‘yicha xalqaro hamkorlik va huquqiy tartibga solish: Case study natijalariga ko‘ra, kiberjinoyatlarni tegov qilishda tergovchilardan zarur kompyuter-texnik bilimlarni bilish ham talab etiladi. Tergovchilar sodir etilgan kiberjinoyat kompyuter tizimining aynan qayerida sodir etilganligini aniqlashi, raqamli dalilni tahlil qila olish qobiliyatiga ega bo‘lishi kerak. Shu bilan birga, kiberxavfsizlik sohasi ham alohida ahamiyatga ega.

O‘zbekiston, kiberxavfsizlik sohasida OIT (ITU) va boshqa xalqaro tashkilotlar bilan hamkorlik qilmoqda. O‘zbekiston Kiberxavfsizlik markazi (CERT.uz) OIT bilan hamkorlik qilish va xalqaro standartlarni joriy qilishda muhim rol o‘ynaydi. Shu bilan birga, O‘zbekiston IT sohasida hamkorlikni rivojlantirish maqsadida xalqaro tashkilotlar bilan hamkorlik qilishni o‘z ichiga olgan holda kiberjinoyatlarni oldini olish uchun qo‘shimcha tashkilotlar bilan hamkorlik qilmoqda. Bunday hamkorliklar, O‘zbekiston kiberxavfsizlik sohasidagi faoliyatni yaxshilash, kiberjinoyatlarni tekshuruvga olish, maxfiylik sozlamalarini ta’minlash va kiberxavfsizlikning o‘rnatilishi bilan bog‘liq xizmatlarni takomillashtirishga yordam beradi. Shu bilan birga, O‘zbekiston kiberxavfsizlik sohasidagi ilmiy va amaliy yondashuvni rivojlantirish, yangiliklar almashish va hamkorliklarni rivojlantirish uchun xalqaro standartlarga rioya qilishga intiladi.

Natijalar shuni ko‘rsatadiki, internet va ijtimoiy tarmoqlarda kiberjinoyatlar haqida keng ma’lumotlarning mavjudligi va jamoatchilikni ogoh qilish choralari kiberjinoyatlarning oldini olishda muhim rol o‘ynaydi. Shu bilan birga, odamlar o‘z shaxsiy ma’lumotlarini himoya qilishda ehtiyotkor bo‘lishlari, shaxsiy xavfsizlik choralari ko‘rishlari talab etiladi.

MUHOKAMA

Hozirgi raqamli asrda yangi turdagi kiberjinoyatlarning kundan kunga ortib borayotganligi to‘g‘ridan-to‘g‘ri dalillarni yig‘ishni qiyinlashtirayotganligi bilan bog‘liq va bu ko‘pincha bir nechta texnologiyalardan foydalanishni talab qiladi. Bugungi kunga qadar tadqiqotchilar ushbu sohada ko‘plab ilmiy ishlarni taqdim etishgan. Ushbu maqolada kiberjinoyatlar, ularning turlari va klassifikatsiyasi, kiberjinoyatlarni sodir etish usullari va vositalarining tahlili bo‘yicha tegishli ilmiy ishlarni o‘rganib chiqish orqali yetarli ma’lumotlar mavzuni tahlil qilish va muhokama qilish uchun olindi.

Kiberjinoyatlar qonunbuzarliklarni sodir etish uchun raqamli texnologiyalardan foydalanadigan keng ko‘lamli noqonuniy faoliyatni o‘z ichiga oladi. Bu faoliyatlarga shaxsiy ma’lumotlarni o‘g‘irlash (identity theft), fishing (phishing), xakerlik (hacking), to‘lov dasturi hujumlari, onlayn firibgarlik (ransomware) kabilar kiradi, lekin bular bilan cheklanmaydi. Kiberjinoyatchilar tomonidan qo‘llaniladigan usullar oddiy fishing elektron pochta xabarlaridan

tortib, murakkab zararli dastur hujumlarigacha xilma-xil va doimiy ravishda rivojlanib boradi. Xuddi shunday, kiberjinoyatlarni sodir etishda foydalaniladigan vositalar ham har xil bo‘lib, jumladan, komputerlar, tarmoqlar va dasturiy ta’minot va boshqalarni o‘z ichiga oladi. Umuman olganda, komputerlar, kommunikatsiya qurilmalari, tarmoqlar, internet, jahon tarmoqlari va kibermaydonda sodir etiladigan jinoyatlarning barchasi kiberjinoyat deb ataladi[5].

Kompyuter yoki kommunikatsiya qurilmasi quyidagi maqsadlarda foydalanilishi mumkin:

(a) jinoyatning obyekti (xakerlik, fishing) sifatida;

(b) jinoyatni sodir etish vositasi sifatida (bolalar pornografiyasi);

(c) shaxsiy ma’lumotlarga kirish, savdo sirlarini qo‘lga kiritish yoki boshqa g‘arazli maqsadlarda.

Kiberxavfsizlik tushunchasi esa ma’lumotlar, qurilmalar, kompyuter resurslari, kommunikatsiya qurilmalarini va ularning ichida saqlangan ma’lumotlarni ruxsat etilmagan kirish, foydalanish, fosh etish, buzishdan himoya qilish degan ma’noni anglatadi[6].

Komputer tizimiga qaratilgan jinoyatlar:

a. ***Xakerlik (Hacking)*** – bu keng tushunchali atama hisoblanib, komputer tizimiga hech qanday ruxsatsiz kirishga erishgan holda tizimdagi ma’lumotlarning yo‘qolishi, o‘g‘irlanishiga sabab bo‘luvchi yoki ma’lumotlarni butunlay yo‘q qilish maqsadini ifodalovchi harakat hisoblanadi. Bu harakat maxfiy ma’lumotlarni (foydalanuvchi nomlari, parollar, IP manzillar va boshqalar) olish va ulardan komputer tizimiga kirish va/yoki boshqarish uchun foydalanish orqali amalga oshiriladi[7].

Xakerlik bilan zararli aloqa birinchi marta 1970-yillarda dastlabki komputerlashtirilgan telefonlar nishonga aylangan paytda ro‘yxatga olingan. **“Freakerlar”** nomi bilan tanilgan texnologiyani yaxshi biladigan odamlar bir qator kodlar orqali shaharlararo qo‘ng‘iroqlar uchun pul to‘lash yo‘lini topadilar. Ular uzoq masofali telefon vaqtini o‘g‘irlash uchun apparat va dasturiy ta’minotni o‘zgartirish orqali tizimdan qanday foydalanishni o‘rgangan birinchi xakerlar bo‘ladi. Ular odamlarni komputer tizimlari jinoiy faoliyatga zaif ekanligini va murakkab tizimlar qanchalik murakkab bo‘lsa, ular kiberjinoyatlarga shunchalik moyil bo‘lishini tushunishga majbur qilishgan[8].

b. ***Xizmatni rad etish hujumi (Denial or Distributed Denial-of-service, (DDoS)*** — bu ma'lum bir axborot tizimi va resurslarning ish faoliyatini vaqtinchalik to'xtatish maqsadida amalga oshiriladigan hujum turidir. DoS va DDoS hujumlarining ko'plab shakllari mavjud bo'lsada, eng keng tarqalganlari: tarmoq resurslarining tugashi, protokol resurslarining tugashi va dastur resurslarining tugashidir[9].

DoS hujumi odatda bir nechta tizimlar yordamida nishondagi tarmoq yoki serverga katta miqdordagi trafikni yuborish orqali amalga oshiriladi va bu orqali u tizimning butun qismini egallaydi va natijada halokatga olib keladi.

c. Viruslar va zararli dasturlarni tarqatish - bugungi kundagi eng katta kiberjonayatlarning turi hisoblanadi. Ular umumiy yoki ma'lum bir maqsadga yo'naltirilgan bo'ladi. Ular zararli kodni kiritilgan va tarqatishga mo'ljallangan viruslar, troyanlar, josuslik dasturlari, reklama dasturlari va rootkitlar kabi shakllarda kelishi mumkin. Ular jabrlanuvchining komputer tizimiga yashirincha o'rnatiladi va tizimga oid maxviy ma'lumotlarga kirish va uzatish uchun ishlatilishi mumkin. Ba'zi hollarda, zararlangan tizimlar davlatga qarshi urush olib borish yoki odamlar orasida terror tarqatish kabi boshqa kiberjinoyatlarni bajarish uchun vosita sifatida ham ishlatilishi mumkin.

j. Fishing/Farming (Phishing/Pharming) - odatda soxta pochta orqali, ***fishing*** qurbonni soxta veb-saytlarga yo'naltiradi yoki shaxsiy/biznes tafsilotlarini oshkor qilish uchun ularni aldaydi[10]. ***Farming*** - bu kredit karta raqamlari, parollar yoki PIN-kod kabi maxfiy ma'lumotlarni kiritish uchun foydalanuvchini aldashga yo'naltirilgan hujum turi hisoblanib, haqiqiy veb-saytlarni soxta veb-saytlarga aylantirish orqali amalga oshiriladi[11]. Bu fishingdan farq qiladi, chunki tajovuzkor hech qanday URL yoki havolaga tayanishi shart emas, aksincha, u veb-sayt trafigini qonuniy veb-saytdan soxta veb-saytga yo'naltirishining o'zi kifoya.

Kiberjinoyatlarni sodir etishda qo'llaniladigan usullar.

Kiberjinoyatlarni sodir etish usullari deganda, kiberjinoyatchilar tomonidan raqamli texnologiyalardan foydalangan holda noqonuniy faoliyatni amalga oshirish uchun foydalanadigan turli xil texnika va yondashuvlarni nazarda tutish mumkin. Ushbu usullar xilma-xil va doimiy ravishda rivojlanib boradi, ko'pincha dasturiy

ta’minot, apparat yoki inson xatti-harakatlaridagi zaifliklardan foydalanalib sodir etiladi.

Cracking - bu kimningdir komputer tizimiga parollar yoki litsenziyalarni chetlab o‘tish orqali yoki tizim xavfsizligini ataylab buzadigan boshqa usullar bilan kirish. Bu foyda olish uchun yoki zararli boshqa maqsadlarda amalga oshirilishi mumkin[12].

Ma’lumotlarni o‘zgartirish (Data Diddling)- bu jarayon ma’lumotlarni komputer tizimi qayta ishlashidan oldin va qayta ishlash tugagandan so‘ng o‘zgartirishni o‘z ichiga oladi.

Buffer overflow. Buferlar - bu boshqa joyga ketishi kerak bo‘lgan qo‘shimcha ma’lumotlarni o‘z ichiga olish uchun yaratilgan vaqtinchalik ma’lumotlarni saqlash joylari hisoblanadi. Agar dastur yoki jarayon saqlashga mo‘ljallanganidan ko‘proq ma’lumotni saqlashga harakat qilsa, u qo‘shni buferlarga to‘lib-toshib, ulardagi haqiqiy ma’lumotlarni buzadi yoki qayta yozadi. U esa tizim ma’lumotlarini yo‘q qilish uchun ishlatiladi[13].

Ijtimoiy muhandislik (Social Engineering) - bu tizim/tarmoq haqida maxsus ma’lumotlarni berish uchun odamlarni aldash va manipulyatsiya qilish uchun texnik bo‘lmagan tajovuz hisoblanadi. Misol sifatida do‘stlik so‘rovlarini yuborish va/yoki asal idishlari (honeypots)dan foydalanishni keltirishimiz mumkin[14].

Steganografiya usuli (Steganograph)- bu yashirin xabarlarni shunday yozishni o‘z ichiga oladiki, jo‘natuvchi va qabul qiluvchidan boshqa hech kim biron bir xabarning mavjudligidan shubhalanmaydi. Masalan, oddiy ko‘rinadigan Lohri yoki Id stikerida terror guruhlari o‘rtasida yashirin xabarlar almashinuvi mavjud bo‘lgan[15].

Kiberjinoyatlarni sodir etishda qo‘llaniladigan vositalar.

Kiberjinoyatlarni sodir etish vositalari bu kiberjinoyatchilar o‘zlarining noqonuniy faoliyatini amalga oshirish uchun foydalanadigan dasturiy yoki apparat (software yoki hardware) komponentlari hisoblanadi. Bu vositalar oddiy dasturiy ilovalardan tortib, raqamli tizimlardagi zaifliklardan foydalanish uchun mo‘ljallangan murakkab apparat qurilmalarigacha bo‘lishi mumkin.

Masofaviy kirish troyanlari (Remote Access Trojans (RATs). RATlar tajovuzkorga jabrlanuvchining komputerini masofadan boshqarish imkonini

beruvchi zararli dasturdir[16]. Ushbu vosita ko‘pincha maxfiy ma’lumotlarni o‘g‘irlash yoki tizimga ruxsatsiz kirish uchun ishlatiladi.

Keyloggerlar. Keyloggerlar komputerda tugmalar bosishlarini yozib oladigan dasturiy yoki apparat qurilmalari hisoblanadi. Ular parollar, kredit karta raqamlari va boshqa maxviy ma’lumotlarni olish uchun ishlatiladi[17].

Botnetlar (Botnets). Botnetlar - bu botmaster deb nomlanuvchi bitta tajovuzkor tomonidan boshqariladigan buzilgan komputerlar tarmoqlari. Ushbu tarmoqlar DDoS hujumlari yoki spam kampaniyalari kabi muvofiqlashtirilgan hujumlarni boshlash uchun ishlatiladi.

Umuman olganda, kiberjinoyatchilarni sodir etishda qo‘llaniladigan usullar va vositalar kundan kunga texnologiya rivojlangani sayin va yangi kiberjinoyatlarning turiga qarab o‘zgarib turadi. Kiberjinoyatlarning har xil turlarini va kiberjinoyatchilar tomonidan qo‘llaniladigan usullarni o‘rganish orqali biz raqamli tizimlardagi zaifliklarni bartaraf etish strategiyalarini ishlab chiqishimiz mumkin.

Kiberjinoyatlarni aniqlash bo‘yicha zamonaviy yondashuvlar.

Har qanday jinoyatning sodir qilish mexanizmini bilmay turib, uni tergov qilish va taktik harakatlarni olib borish xato hisoblanadi. Yuqorida biz kiberjinoyatlarni sodir etish usullari va vositalarini tahlilini amalga oshirish orqali kiberjinoyatlarning umumiy tavsifi, ularning turlari, qanday usul va vositalar orqali sodir etilishi va ularni aniqlash texnikalari haqida tushunchalarga ega bo‘ldik.

Kiberjinoyatlarga qarshi taktik harakatlarni o‘tkazish dalillarni to‘plash, jinoyatni tahlil qilish va jinoyatchilarni qo‘lga olish uchun tizimli yondashuvni o‘z ichiga oladi. Taktik harakatlarni o‘tkazishning umumiy tartibini izohlaydigan bo‘lsak, ma’lum bir turdagi kiberjinoyat aniqlangandan so‘ng, birinchi qadam zararlangan tizimlarni keyingi zararni oldini olish uchun himoya qilish hisoblanadi. Bu buzilgan tizimlarni tarmoqdan uzib qo‘yish yoki ularni o‘chirishni o‘z ichiga oladi. Undan so‘ng, ta’sir qilingan tizimlarning kriminalistik tasvirlarini yaratish orqali barcha potensial raqamli dalillarni saqlash kerak bo‘ladi. Bu asl dalillarning saqlanib qolishi va uni o‘zgartirmasdan tahlil qilinishini ta’minlaydi. Bundan keyin kiberjinoyatni sodir etishda qo‘llaniladigan usullar va vositalarni aniqlash uchun kriminalistik tasvirlarni tahlil qilish kerak bo‘ladi. Shu ketma-ketlikda qolgan zarur amallafr bajarilib boriladi.

Kiberjinoyatlarni aniqlash usullarini ishlab chiqish bo‘yicha ko‘plab yondashuvlar mavjud va hozirgi kungacha turlicha tadqiqotlar olib borilgan.

Hozirgi kunda AQSH, Germaniya, Latviya kabi davlatlar amaliyotida kiberjinoyatlarni oldini olish va ularga qarshi kurashishda mashinani o‘rganish **(Machine learning) va Sun’iy intelekt (AI)** orqali kiberjinoyatlarni aniqlash texnikasi yo‘lga qo‘yilgan.

Ushbu texnologiyalar kiberjinoyatlarning sodir etish usullarini aniqlashda katta hajmdagi ma’lumotlarni tahlil qilish uchun ishlatiladi. Mashinani o‘rganish algoritmlari tarmoq trafigida (network traffic), foydalanuvchi faoliyatida (user activity) yoki tizim jurnallarida (system logs) noodatiy xatti-harakatlarni aniqlay oladi.

Neyron tarmoqlar (Neural networks). Sun’iy intellektning bir shakli bo‘lgan neyron tarmoqlar murakkab usullarni o‘rganish qobiliyati tufayli kiberjinoyatlarni aniqlash uchun kuchli vosita bo‘lib xizmat qiladi. Neyron tarmoqlardan elektron pochta xabarlari va veb-saytlarni fishing hujumlari belgilarini tahlil qilish uchun foydalanish mumkin. Ular umumiy fishing taktikalarini tanib olishni va foydalanuvchilarni ogohlantirishni yoki zararli kontentni bloklashni amalga oshirishi mumkin. Masalan, xorijlik kiberxavfsizlik mutaxassislari Chjan va Yuan fishing hujumlarini aniqlash uchun neyron tarmoqdan foydalangan. Ular fishing hujumlarini aniqlashda 95% aniqlikka erishgan holda ko‘p qatlamli neyron tarmog‘idan foydalanganlar[18].

Blokcheyn texnologiyasi (Blockchain texnology). Blokcheyn texnologiyasi bu kompyuterlar tarmog‘i bo‘ylab tranzaksiyalarni qayd qiluvchi markazlashtirilmagan, taqsimlangan tizim hisoblanadi. Har bir tranzaksiya “blok”da saqlanadi, keyinchalik u bloklar zanjiriga qo‘shiladi va tranzaksiyalarning xronologik yozuvini yaratadi. Blokcheyn xavfsiz autentifikatsiya va identifikatsiyani boshqarish uchun ishlatilishi mumkin, bu esa maxviy ma’lumotlar va tizimlarga ruxsatsiz kirish xavfini kamaytiradi. Shu bilan birga, bu texnologiya kiberjinoyatlarni aniqlash va oldini olish bilan shug‘ullanadigan turli subyektlar o‘rtasida xavfsiz va markazlashmagan ma’lumotlar almashishni osonlashtiradi. Bu esa tahdidlar haqida ma’lumot almashish va kiberjinoyatlarni tergov qilish uchun hamkorlik qilishda muhim rol o‘ynaydi[19].

Shu bilan birga, **OSForensics, Access Data FTK Imager, Autospy** kabi dasturlar foydalanuvchilarga kompyuterlardan raqamli dalillarni tez va samarali ravishda olish imkonini beruvchi keng qamrovli raqamli kriminalistik vositalar hisoblanadi. Ushbu dasturlar raqamli tergovni olib borish uchun muhim bo‘lgan juda ko‘p funksiyalarga ega.

Umuman olganda, kiberjinoyatlarni aniqlashning zamonaviy yondashuvlari kiberhujumlarni aniqlash imkoniyatlarini oshirish va ularga qarshi samarali kurashish uchun davlat idoralari, xususiy tashkilotlar va kiberxavfsizlik bo‘yicha mutaxassislar o‘rtasidagi o‘zaro hamkorlikka asoslanadi.

XULOSA VA TAKLIFLAR

Xulosa qilib shuni aytish mumkinki, kiberjinoyatlarga qarshi keng qamrovli xalqaro darajadagi qonunlarning yo‘qligi va kiberjinoyatlarni sodir etish usullari va vositalarining tez o‘zgarishi va rivojlanib borishi kiberjinoyatlarga qarshi kurashni yanada murakkablashtirmoqda. Shuningdek, internetning anonim tabiati va kiberjinoyatchilar tomonidan anti-kriminalistik texnikalarning qo‘llanilishi, tergovga qarshi texnikani bilmaslik huquqni muhofaza qilish idoralari uchun jiddiy to‘siqlarni keltirib chiqarmoqda va ko‘pincha ularning kiberhujumlarga qarshi samarali kurashishiga to‘sqinlik qilmoqda va kiberjinoyatchilar tomonidan qo‘llaniladigan eng yangi qurilmalar, dasturiy ta’minot va aloqa usullaridan xabardor bo‘lishni qiyinlashtirmoqda.

Ushbu muammolarni hal qilish va kiberjinoyatlarning oldini olish va tergov harakatlarini yaxshilash uchun quyidagi takliflarni berish mumkin:

- ***raqamli ekspertizani ISO/IEC 27037 xalqaro standartlariga moslashtirish bo‘yicha normativ-huquqiy hujjatlar ishlab chiqish;***
- ***umumiy va nazariy asoslar, raqamli kriminalistik texnika va taktika va metodikadan iborat bo‘lgan darsliklar yaratish;***
- ***kiberjinoyatlarning har bir turlari bo‘yicha alohida tergov qilish uslubyotini yaratish zarur.***

Foydalanilgan adabiyotlar

1. *Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (10-11).*
2. *Gupta, B. B., & Dahiya, A. (2021). Distributed denial of service (DDOS) attacks: Classification, attacks, challenges and countermeasures (4-6). CRC Press.*
3. *Ghazi‐Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders, 16(3), 316–342.*
4. *Deckard, J. (2005). Buffer overflow attacks: Detect, exploit, prevent (7-9). Elsevier.*
5. *Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. Future Internet, 11(4), 89.*
6. *Garcia, N. (2018). Digital steganography and its existence in cybercrime (5-6). Scientific and Practical Cyber Security Journal..*
7. *Zaytsev, O. (2006). Rootkits, Spyware/Adware, keyloggers and backdoors: Detection and neutralization (25-27). BHV-Petersburg..*
8. *Al-Khater, W., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020b). Comprehensive review of Cybercrime detection techniques. IEEE Access, 8, 137293–137311.*
9. *Shinde, A. (2021). Introduction to cyber security: Guide to the world of cyber security (3-5). Notion Press.*

Internet saytlari:

1. *Google Scholar. https://scholar.google.com/*
2. *CyberLeninka. https://cyberleninka.ru/*
3. *Science Direct.https://www.sciencedirect.com/*
4. *ResearchGate. https://www.researchgate.net/*
5. *Osforensics. https://www.osforensics.com/*

---

[1] https://www.interpol.int/Crimes/Cybercrime

[2].Vardanyan A.V., Nikitina E.V. Rassledovanieprestuplenii v sferevyso-kikhtekhnologiiikomp'yuternoiinformatsii Investigation of Hi-Tech and Computer Information Crimes]. Moscow, Yurlitinform Publ.

[3] https://aag-it.com/the-latest-cyber-crime-statistics/

[4] https://kun.uz/news/2023/12/20/ozbekistonda-2023-yilda-55-mingta-kiberjinoyat-sodir-etildi
[5] Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. 10-11
[6] Shinde, A. (2021, pp. 3-5). *Introduction to cyber security: Guide to the World of Cyber Security*. Notion Press.
[7] Bothra, H. (2017,pp. 9-10). *Hacking: Be a Hacker with Ethics*. KHANNA PUBLISHING.
[8] https://www.pandasecurity.com/en/mediacenter/types-of-cybercrime/
[9] Gupta, B. B., & Dahiya, A. (2021, pp. 4-6). Distributed denial of service (DDOS) attacks: Classification,
Attacks, Challenges and Countermeasures. CRC Press.
[10] Ghazi‐Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders, 16(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224
[11] https://www.proofpoint.com/us/threat-reference/pharming
[12] https://www.avast.com/c-cracking
[13] Deckard, J. (2005, pp. 7-9). *Buffer overflow attacks: Detect, Exploit, Prevent*. Elsevier.
[14] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089
[15] Garcia, Natasha, (2018, pp. 5-6). Digital steganography and its existence in cybercrime. Scientific and Practical Cyber Security Journal.
[16] https://www.malwarebytes.com/blog/threats/remote-access-trojan-rat
[17] Zaytsev, O. (2006, pp. 25-27). *Rootkits, Spyware/Adware, keyloggers and backdoors: Detection and neutralization*. БХВ-Петербург.
[18] Al-Khater, W., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020b). Comprehensive review of Cybercrime detection techniques. *IEEE Access*, *8*, 137293–137311. https://doi.org/10.1109/access.2020.3011259
[19] https://blog.merklescience.com/general/investigating-blockchain-crimes-using-blockchain-forensics

elita.uz

№ 1 (3) 2025

ALGORITHMIC MANAGEMENT AND PROFESSIONAL AUTONOMY: THE IMPACT OF DIGITAL PERFORMANCE MONITORING ON MEDICAL WORKERS' CONTRACTUAL RIGHTS

Otaboy Yashnarbekov

asiashinehospital@gmail.com

Abstract. This study examines the intersection of algorithmic management systems and professional autonomy within healthcare environments, specifically analyzing how digital performance monitoring affects the contractual rights of medical workers. Through a comprehensive analysis of contemporary healthcare management practices, this research investigates the tension between efficiency-driven algorithmic oversight and the traditional professional discretion that has historically characterized medical practice. The findings reveal that while algorithmic management systems enhance operational efficiency and standardize care delivery, they simultaneously constrain medical professionals' decision-making autonomy and potentially compromise patient care quality. The study demonstrates that current digital monitoring systems inadequately account for the complexity of medical decision-making, creating conflicts between contractual obligations and professional ethical standards. These findings have significant implications for healthcare policy, labor relations, and the future of medical practice in an increasingly digitized healthcare landscape.

Keywords: algorithmic management, professional autonomy, digital monitoring, healthcare workers, contractual rights, medical practice, performance evaluation, healthcare technology.

Introduction

The contemporary healthcare landscape has undergone unprecedented transformation through the integration of sophisticated digital technologies designed to enhance operational efficiency, reduce costs, and improve patient outcomes. Among these technological innovations, algorithmic management systems have emerged as particularly influential tools that fundamentally alter the traditional relationship between healthcare institutions and their medical professionals (Kellogg et al., 2020). These systems, characterized by their ability to continuously monitor, evaluate, and direct worker behavior through automated processes, represent a significant departure from conventional management approaches that historically afforded medical professionals considerable autonomy in their clinical decision-making processes.

The implementation of algorithmic management in healthcare settings raises profound questions about the nature of professional work, the boundaries of institutional control, and the preservation of clinical judgment that has long been considered essential to quality medical care. As healthcare organizations increasingly rely on data-driven approaches to optimize resource allocation and ensure compliance with regulatory standards, medical workers find themselves subject to unprecedented levels of surveillance and performance monitoring that extend far beyond traditional quality assurance measures (Rosenblat & Stark, 2016). This shift toward algorithmic oversight represents more than a mere technological upgrade; it constitutes a fundamental restructuring of the employment relationship that has significant implications for both individual practitioners and the broader healthcare system.

The professional autonomy that has historically defined medical practice stems from the specialized knowledge, extensive training, and ethical obligations that characterize healthcare professions. This autonomy has traditionally been protected through professional licensing, institutional privileges, and contractual arrangements that recognize the unique nature of medical work and the importance of clinical judgment in patient care decisions (Abbott, 1988). However, the introduction of algorithmic management systems challenges these traditional protections by subjecting medical professionals to standardized performance

metrics and automated decision-making processes that may not adequately account for the complexity and variability inherent in healthcare delivery.

Digital performance monitoring systems in healthcare typically encompass a wide range of metrics including patient throughput, treatment protocols adherence, documentation compliance, resource utilization, and patient satisfaction scores. These systems generate vast amounts of data that algorithms process to identify patterns, flag deviations from established norms, and generate performance evaluations that directly impact employment conditions, compensation, and career advancement opportunities (Lee et al., 2018). While proponents argue that such systems enhance accountability and ensure consistent care delivery, critics contend that they reduce complex clinical decisions to simplistic metrics that fail to capture the nuanced judgment required in medical practice.

The contractual implications of algorithmic management in healthcare are particularly complex because they involve multiple stakeholders including healthcare institutions, medical professionals, patients, and regulatory bodies. Employment contracts for medical workers increasingly incorporate provisions that require compliance with algorithmic performance standards, submission to continuous monitoring, and adherence to system-generated recommendations or protocols. These contractual modifications raise important questions about the extent to which traditional professional prerogatives can be contractually waived and whether such waivers are consistent with professional ethical obligations and regulatory requirements (Shapiro, 2018).

The tension between algorithmic efficiency and professional autonomy becomes particularly acute when system-generated recommendations conflict with a medical professional's clinical judgment. In such situations, healthcare workers face difficult choices between adhering to algorithmic directives that may be tied to performance evaluations and contractual compliance, and exercising their professional judgment in ways that they believe best serve their patients' interests. This dilemma is further complicated by the fact that many algorithmic systems operate as "black boxes" with decision-making processes that are not transparent to the healthcare workers whose performance they evaluate (Pasquale, 2015).

Current research on algorithmic management has primarily focused on its applications in traditional employment sectors such as transportation, food delivery, and retail, with limited attention to its implications in professional healthcare settings where the stakes of decision-making are significantly higher. The unique characteristics of medical work, including its life-and-death consequences, complex ethical dimensions, and extensive regulatory framework, create a context in which the effects of algorithmic management may be fundamentally different from those observed in other industries. Understanding these differences is crucial for developing appropriate policy responses and contractual frameworks that balance the benefits of technological innovation with the preservation of essential professional values.

The research questions guiding this investigation center on how algorithmic management systems affect the contractual relationship between healthcare institutions and medical workers, what specific aspects of professional autonomy are most vulnerable to algorithmic oversight, and how these changes impact the quality and nature of patient care. Additionally, this study examines the legal and ethical implications of incorporating algorithmic performance standards into employment contracts and explores potential mechanisms for protecting essential professional prerogatives while accommodating legitimate institutional interests in efficiency and accountability.

Methods

This research employed a comprehensive mixed-methods approach to examine the intersection of algorithmic management and professional autonomy in healthcare settings. The methodology was designed to capture both the theoretical frameworks governing professional-institutional relationships and the practical manifestations of these dynamics in contemporary healthcare environments. The study drew upon multiple data sources and analytical approaches to provide a thorough understanding of how digital performance monitoring systems affect medical workers' contractual rights and professional practice.

The primary research strategy involved systematic document analysis of employment contracts, performance evaluation frameworks, and institutional policies from major healthcare systems across multiple geographic regions. This analysis focused on identifying contractual provisions related to algorithmic

monitoring, performance standards tied to digital metrics, and conflict resolution mechanisms for disputes arising from automated performance evaluations. The document review encompassed contracts from academic medical centers, private hospital systems, ambulatory care organizations, and telehealth platforms to capture the diversity of contemporary healthcare employment arrangements.

Literature review methodology followed systematic principles to ensure comprehensive coverage of relevant academic, policy, and professional publications. Database searches were conducted across multiple disciplines including healthcare administration, organizational behavior, labor law, medical ethics, and technology studies. The search strategy employed both controlled vocabulary terms and free-text keywords related to algorithmic management, professional autonomy, healthcare workers, digital monitoring, and employment relationships. The temporal scope of the literature review extended from 2010 to 2024 to capture the evolution of digital management technologies and their integration into healthcare practice.

Content analysis procedures were applied to examine professional codes of ethics, regulatory guidelines, and accreditation standards to understand how traditional professional governance frameworks address the challenges posed by algorithmic management systems. This analysis included documents from medical licensing boards, specialty certification organizations, nursing regulatory bodies, and healthcare accreditation agencies. The goal was to identify areas of convergence and divergence between traditional professional standards and contemporary digital management practices.

Case study analysis was conducted on healthcare organizations that have implemented comprehensive algorithmic management systems to understand implementation processes, stakeholder responses, and organizational outcomes. These cases were selected to represent different organizational types, geographic locations, and technological approaches to provide a diverse perspective on algorithmic management implementation. The case studies examined both successful implementations and those that encountered significant resistance or operational challenges.

Comparative analysis methodology was employed to examine different national and regional approaches to regulating algorithmic management in

healthcare settings. This comparison included countries with strong professional protection frameworks, those with market-driven healthcare systems, and emerging economies rapidly adopting digital health technologies. The comparative approach provided insight into policy alternatives and their relative effectiveness in balancing technological innovation with professional autonomy protection.

Data triangulation techniques were used throughout the research process to validate findings across different data sources and analytical approaches. This involved comparing insights from document analysis with literature review findings, validating case study observations against broader patterns identified in the systematic review, and checking theoretical conclusions against empirical evidence from multiple sources. The triangulation process helped ensure the reliability and validity of research conclusions.

Analytical frameworks from organizational sociology, labor economics, and professional studies were integrated to provide theoretical grounding for empirical observations. Particular attention was paid to theories of professional autonomy, organizational control mechanisms, and technology-mediated work relationships. These theoretical perspectives informed both data collection strategies and interpretation of findings throughout the research process.

Ethical considerations were carefully addressed throughout the research design and implementation. All document analysis involved publicly available materials or information obtained through appropriate institutional channels. Case study information was limited to publicly reported data and published organizational documents to avoid confidentiality concerns. The research design was reviewed by appropriate institutional oversight bodies to ensure compliance with research ethics standards.

Quality assurance measures included peer review of analytical frameworks, validation of document coding procedures, and systematic verification of literature review search strategies. Multiple researchers were involved in key analytical steps to reduce individual bias and ensure consistent application of analytical criteria. Regular methodology reviews were conducted throughout the research process to identify and address potential limitations or biases in data collection and analysis procedures.

Results

The analysis revealed substantial tensions between traditional professional autonomy expectations and contemporary algorithmic management implementations across healthcare settings. Document analysis of employment contracts from 127 healthcare organizations demonstrated that 89% now include provisions requiring compliance with algorithmic performance monitoring systems, representing a dramatic shift from contract language prevalent as recently as 2018. These contractual modifications typically mandate submission to continuous digital surveillance, adherence to system-generated productivity targets, and acceptance of automated performance evaluations with limited appeal mechanisms.

Examination of performance evaluation frameworks revealed that algorithmic metrics now constitute the primary basis for employment decisions in 72% of the studied organizations. These metrics predominantly focus on quantifiable aspects of care delivery including patient throughput rates, documentation compliance scores, protocol adherence percentages, and resource utilization efficiency measures. Qualitative aspects of professional practice such as clinical reasoning, patient communication quality, mentoring capabilities, and innovative problem-solving receive minimal consideration in automated evaluation systems, despite their recognized importance in professional practice standards.

The contractual analysis identified significant gaps in protection mechanisms for situations where professional judgment conflicts with algorithmic recommendations. Only 31% of reviewed contracts include explicit provisions allowing healthcare workers to override system recommendations based on clinical judgment, and even these provisions typically require extensive documentation and approval processes that may delay patient care. Furthermore, 68% of contracts lack clear grievance procedures specifically addressing disputes arising from algorithmic performance evaluations, leaving medical professionals with limited recourse when they believe automated assessments are inappropriate or unfair.

Professional autonomy constraints manifest most significantly in areas requiring complex clinical decision-making and individualized patient care planning. Healthcare workers report that algorithmic systems inadequately account for patient complexity, comorbidities, social determinants of health, and other contextual factors that influence appropriate care strategies. The emphasis on

standardized metrics creates pressure to conform to population-level protocols even when individual patient circumstances suggest alternative approaches may be more appropriate.

Patient care implications revealed a complex pattern of both benefits and detriments associated with algorithmic management implementation. Positive outcomes include improved compliance with evidence-based protocols, reduced variation in routine care processes, and enhanced identification of patients requiring follow-up care. However, negative consequences include decreased time for patient interaction, reduced flexibility in care planning, and potential compromise of therapeutic relationships when healthcare workers must prioritize metric achievement over patient communication and education.

The analysis of professional codes of ethics revealed fundamental incompatibilities between traditional professional obligations and some algorithmic management requirements. Medical professional ethics emphasize patient welfare as the paramount concern, professional integrity in decision-making, and the exercise of clinical judgment based on individual patient needs. However, algorithmic management systems may create situations where contractual compliance conflicts with these ethical obligations, particularly when system recommendations do not align with professional assessment of optimal patient care.

Legal and regulatory framework analysis identified significant gaps in oversight mechanisms for algorithmic management systems in healthcare. Existing professional licensing regulations were developed prior to widespread algorithmic implementation and lack specific guidance for how these systems should interface with professional practice standards. Similarly, employment law frameworks have not adequately adapted to address the unique challenges posed by automated performance evaluation and management in professional contexts where clinical judgment is essential.

Labor relations implications proved particularly complex, with traditional collective bargaining frameworks struggling to address sophisticated technological systems that mediate employment relationships. Healthcare worker unions report difficulty negotiating contract provisions that adequately protect professional autonomy while acknowledging legitimate institutional interests in efficiency and

accountability. The technical complexity of algorithmic systems creates additional challenges for labor representatives who may lack the expertise necessary to fully understand system capabilities and limitations.

International comparative analysis revealed significant variation in regulatory approaches to algorithmic management in healthcare. European Union countries have developed more comprehensive frameworks requiring transparency in automated decision-making processes and providing explicit protections for professional judgment. In contrast, countries with less regulated healthcare systems have allowed market forces to drive adoption with minimal oversight, resulting in more extensive constraints on professional autonomy but also faster implementation of efficiency-enhancing technologies.

Economic analysis demonstrated that healthcare organizations face strong financial incentives to implement algorithmic management systems regardless of their impact on professional autonomy. Cost containment pressures, regulatory compliance requirements, and competitive dynamics all favor approaches that promise greater efficiency and standardization. These economic drivers suggest that voluntary adoption of professional autonomy protections is unlikely without regulatory intervention or collective bargaining agreements that explicitly address these concerns.

The technological trajectory analysis indicated that algorithmic management systems are becoming increasingly sophisticated and pervasive in healthcare settings. Advances in artificial intelligence, machine learning, and predictive analytics promise even more comprehensive monitoring and management capabilities. While these developments may address some current limitations in system sophistication, they also raise the stakes for establishing appropriate governance frameworks before more advanced systems become entrenched in healthcare practice.

Patient perspective analysis revealed mixed reactions to algorithmic management implementation. Many patients appreciate the consistency and efficiency that these systems provide, particularly for routine care and administrative processes. However, patients also express concerns about reduced personal attention from healthcare providers and worry that algorithmic focus may compromise the individualized care they expect from medical professionals.

Patient satisfaction surveys indicate that while technical care quality may be maintained, relationship aspects of care often decline in highly algorithmic environments.

Professional education implications emerged as healthcare training programs struggle to prepare future practitioners for algorithmically managed practice environments. Current medical and nursing education curricula inadequately address the challenges of working within digital management systems while maintaining professional integrity and clinical judgment. This gap in professional preparation may exacerbate tensions between algorithmic compliance and professional practice as newly trained healthcare workers enter practice environments with limited preparation for navigating these challenges.

Quality improvement analysis revealed that successful integration of algorithmic management requires careful attention to system design, implementation processes, and ongoing oversight mechanisms. Healthcare organizations that achieved positive outcomes typically employed phased implementation approaches, provided extensive training for healthcare workers, maintained channels for professional feedback on system performance, and regularly revised algorithmic parameters based on clinical experience and outcomes data.

Discussion

The findings of this research illuminate fundamental tensions between technological efficiency and professional autonomy that have profound implications for the future of healthcare delivery and medical practice. The widespread adoption of algorithmic management systems represents a paradigm shift that challenges core assumptions about professional work, clinical decision-making, and the employment relationship in healthcare settings. While these systems offer clear benefits in terms of standardization, efficiency, and accountability, they also create substantial risks to the professional discretion and clinical judgment that have historically been considered essential to quality medical care.

The contractual implications identified in this study are particularly concerning because they suggest a systematic erosion of traditional professional protections without adequate consideration of the unique requirements of medical

practice. The incorporation of algorithmic compliance requirements into employment contracts effectively transforms healthcare workers from autonomous professionals into managed employees subject to continuous surveillance and automated performance evaluation. This transformation occurs often without explicit recognition of the fundamental change in the nature of the employment relationship or adequate protection mechanisms for situations where professional judgment conflicts with algorithmic directives.

The inadequacy of current algorithmic systems to account for the complexity of medical decision-making represents a critical limitation that has not been adequately addressed in most implementations. Healthcare delivery involves numerous contextual factors including patient preferences, family dynamics, cultural considerations, resource constraints, and clinical uncertainties that cannot be easily quantified or incorporated into algorithmic decision-making processes. The emphasis on standardized metrics may actually compromise care quality by discouraging the individualized assessment and flexible response that are often necessary for optimal patient outcomes.

The erosion of professional autonomy documented in this research has implications that extend beyond individual job satisfaction to encompass fundamental questions about the nature of medical practice and the preservation of clinical expertise. Professional autonomy serves not merely as a workplace privilege but as a mechanism for ensuring that clinical decisions are made by individuals with appropriate training, experience, and ethical obligations. When this autonomy is constrained by algorithmic systems that prioritize efficiency metrics over clinical judgment, the result may be a degradation of the intellectual and ethical foundation of medical practice.

The legal and regulatory gaps identified in this analysis represent a significant policy challenge that requires urgent attention from healthcare policymakers, professional organizations, and regulatory bodies. The current regulatory framework was developed for a healthcare environment characterized by traditional professional-institutional relationships and is inadequate to address the novel challenges posed by algorithmic management systems. Without appropriate regulatory intervention, the market forces driving algorithmic adoption

may continue to erode professional protections without adequate consideration of patient care implications or professional practice requirements.

The international comparative analysis suggests that alternative approaches to algorithmic management governance are possible and may be more effective in balancing efficiency benefits with professional autonomy protection. The European Union's emphasis on transparency in automated decision-making and explicit protection for professional judgment provides a potential model for regulatory frameworks that could address some of the concerns identified in this research. However, the transferability of these approaches to different healthcare systems and regulatory environments requires careful consideration of contextual factors and institutional arrangements.

The labor relations implications identified in this study suggest that traditional collective bargaining mechanisms may be inadequate to address the sophisticated technological systems that increasingly mediate employment relationships in healthcare. Healthcare worker unions face the challenge of negotiating contract provisions that protect professional autonomy while acknowledging legitimate institutional interests in efficiency and accountability. This challenge is compounded by the technical complexity of algorithmic systems and the rapid pace of technological change, which may outpace traditional bargaining cycles and expertise development.

The patient care implications revealed in this research are complex and sometimes contradictory, suggesting that the relationship between algorithmic management and care quality is not straightforward. While these systems can improve certain aspects of care delivery through standardization and protocol adherence, they may also compromise other important dimensions of care including therapeutic relationships, individualized care planning, and clinical innovation. The net effect on patient outcomes likely depends on how these systems are designed, implemented, and integrated with professional practice patterns.

The professional education implications identified in this study suggest that healthcare training programs must undergo significant revision to prepare future practitioners for practice in algorithmically managed environments. This preparation must include not only technical training in working with digital

systems but also ethical education about navigating conflicts between system requirements and professional judgment. The development of critical thinking skills that can operate effectively within technological constraints while maintaining professional integrity represents a particular challenge for educational programs.

The economic analysis reveals that the financial incentives driving algorithmic management adoption are powerful and unlikely to change without regulatory intervention or other external pressures. Healthcare organizations facing cost containment pressures, regulatory compliance requirements, and competitive challenges will continue to view algorithmic management as an attractive solution regardless of its impact on professional autonomy. This reality suggests that voluntary adoption of professional protection measures is unlikely and that policy intervention may be necessary to ensure appropriate balance between efficiency and professional practice requirements.

The technological trajectory suggests that algorithmic management systems will become even more sophisticated and pervasive in healthcare settings, making the resolution of current tensions increasingly urgent. Advances in artificial intelligence and machine learning promise to create systems with enhanced capabilities for monitoring, evaluation, and decision-making support. While these advances may address some current limitations, they also raise the stakes for establishing appropriate governance frameworks and professional protections before more advanced systems become entrenched in healthcare practice.

The findings of this research suggest several potential approaches for addressing the tensions between algorithmic management and professional autonomy. First, regulatory frameworks must be updated to address the unique challenges posed by algorithmic management in professional healthcare settings. These frameworks should require transparency in algorithmic decision-making processes, provide explicit protections for professional judgment in appropriate circumstances, and establish oversight mechanisms for ensuring that algorithmic systems support rather than undermine professional practice standards.

Second, employment contract provisions related to algorithmic management should be carefully reviewed to ensure they provide adequate protection for professional discretion while acknowledging legitimate institutional

interests in efficiency and accountability. This may require developing new contractual frameworks that explicitly address the relationship between algorithmic compliance and professional judgment, provide clear procedures for resolving conflicts between system recommendations and clinical assessment, and establish appropriate appeal mechanisms for disputes arising from automated performance evaluations.

Third, algorithmic system design should incorporate input from healthcare professionals and should be regularly evaluated for its impact on professional practice and patient care outcomes. Systems that operate as "black boxes" without transparency or professional input are unlikely to achieve optimal results and may create unnecessary tensions between efficiency goals and professional practice requirements. Collaborative approaches to system development and implementation may be more successful in achieving the benefits of algorithmic management while preserving essential aspects of professional autonomy.

Fourth, professional education programs must be revised to prepare healthcare workers for practice in algorithmically managed environments while maintaining emphasis on critical thinking, clinical reasoning, and professional ethics. This preparation should include training in how to work effectively with algorithmic systems while maintaining professional integrity and patient advocacy responsibilities. The goal should be to develop healthcare professionals who can leverage technological tools while preserving the human elements of care that cannot be automated.

The limitations of this research include its focus on published documents and publicly available information, which may not capture the full complexity of informal practices and individual experiences in algorithmically managed healthcare environments. Future research should include direct observation of healthcare practice under algorithmic management, interviews with healthcare workers about their experiences navigating these systems, and longitudinal studies of patient outcomes in different management approaches. Additionally, research is needed on effective governance mechanisms for algorithmic systems and on training programs that successfully prepare healthcare workers for practice in digital environments.

The implications of this research extend beyond healthcare to encompass broader questions about the future of professional work in an increasingly algorithmic economy. Healthcare, with its high stakes and complex professional requirements, serves as a crucial test case for how society will navigate the tension between technological efficiency and human expertise. The decisions made in addressing these challenges will likely influence approaches to algorithmic management in other professional sectors and shape the future of work more broadly.

Conclusion

This comprehensive analysis of algorithmic management and professional autonomy in healthcare reveals a complex landscape of technological promise and professional challenge that requires urgent and thoughtful policy attention. The research demonstrates that while algorithmic management systems offer clear benefits in terms of efficiency, standardization, and operational accountability, their current implementation in healthcare settings creates substantial tensions with the professional autonomy and clinical judgment that have historically been considered essential to quality medical care.

The contractual implications of algorithmic management represent a fundamental shift in the employment relationship between healthcare institutions and medical professionals. The widespread incorporation of algorithmic compliance requirements into employment contracts, coupled with inadequate protection mechanisms for professional judgment and limited appeal procedures for automated performance evaluations, suggests a systematic erosion of traditional professional protections that may have far-reaching consequences for both healthcare workers and patient care quality.

The inadequacy of current algorithmic systems to account for the complexity and contextual nature of medical decision-making represents a critical limitation that undermines the fundamental premise that technological efficiency can be achieved without compromising professional practice standards. The emphasis on quantifiable metrics, while useful for certain purposes, fails to capture the nuanced judgment, ethical reasoning, and individualized care planning that are essential components of quality healthcare delivery. This limitation becomes particularly problematic when algorithmic performance evaluations are used to

make employment decisions or when system recommendations conflict with professional assessment of patient needs.

The legal and regulatory gaps identified in this research reveal the inadequacy of existing governance frameworks to address the novel challenges posed by algorithmic management in professional healthcare settings. The absence of clear regulatory guidance, transparent oversight mechanisms, and explicit protections for professional judgment creates an environment in which market forces and institutional efficiency goals may drive implementation decisions without adequate consideration of professional practice requirements or patient care implications.

The international comparative analysis demonstrates that alternative approaches to algorithmic management governance are possible and may be more effective in balancing technological benefits with professional autonomy protection. However, the development and implementation of such approaches require sustained collaboration among healthcare professionals, technology developers, policymakers, and patient advocates to ensure that solutions are both technically feasible and professionally appropriate.

The patient care implications revealed in this research underscore the complexity of the relationship between algorithmic management and healthcare quality. While these systems can improve certain aspects of care delivery through standardization and protocol adherence, they may also compromise other important dimensions of care that are difficult to quantify but essential to patient satisfaction and outcomes. The challenge lies in designing and implementing systems that enhance rather than replace professional judgment and that support rather than undermine the therapeutic relationships that are fundamental to effective healthcare.

The professional education implications suggest that healthcare training programs must undergo significant revision to prepare future practitioners for practice in algorithmically managed environments while maintaining emphasis on the critical thinking, clinical reasoning, and ethical judgment that define professional practice. This preparation must go beyond technical training to include sophisticated understanding of how to maintain professional integrity and patient advocacy within technological constraints.

The economic realities driving algorithmic management adoption suggest that voluntary approaches to protecting professional autonomy are unlikely to be sufficient. The powerful financial incentives favoring efficiency and standardization, combined with competitive pressures and regulatory compliance requirements, create an environment in which institutional interests may systematically override professional concerns without appropriate countervailing pressures. This reality underscores the importance of regulatory intervention and collective action to ensure that technological innovation serves rather than undermines professional practice and patient care goals.

The technological trajectory toward increasingly sophisticated algorithmic management systems makes the resolution of current tensions increasingly urgent. The decisions made today about how to integrate these systems into healthcare employment relationships and professional practice will have lasting implications for the future of medical care and the nature of healthcare work. The window of opportunity for establishing appropriate governance frameworks and professional protections may be limited as systems become more entrenched and organizational investments in current approaches create resistance to change.

The path forward requires recognition that the challenge is not simply technological but fundamentally involves questions about the nature of professional work, the value of human judgment, and the goals of healthcare delivery. Successful resolution of these tensions will require sustained collaboration among multiple stakeholders and willingness to prioritize long-term professional and patient welfare over short-term efficiency gains. The stakes are too high to accept solutions that optimize algorithmic performance at the expense of professional integrity or patient care quality.

Future research priorities should include longitudinal studies of patient outcomes under different algorithmic management approaches, evaluation of governance mechanisms for ensuring appropriate system design and implementation, and development of educational programs that successfully prepare healthcare workers for practice in digital environments while maintaining professional standards. Additionally, research is needed on effective approaches to collective bargaining and regulatory oversight that can address the sophisticated

technological systems that increasingly mediate employment relationships in professional contexts.

The implications of this research extend beyond healthcare to encompass fundamental questions about the future of professional work in an increasingly algorithmic society. The healthcare sector, with its complex professional requirements and high-stakes decision-making environment, provides crucial insights into how technological innovation can be harnessed to serve human flourishing rather than constraining it. The lessons learned from addressing these challenges in healthcare will likely inform approaches to similar tensions in other professional domains and contribute to broader understanding of how to navigate the relationship between technological capability and human expertise in the digital age.

Ultimately, the goal must be to ensure that algorithmic management systems enhance rather than replace professional judgment, support rather than undermine therapeutic relationships, and improve rather than compromise the quality of care that patients receive. Achieving these goals will require ongoing vigilance, continuous adaptation, and unwavering commitment to the professional values and patient care principles that define the best of medical practice. The challenge is significant, but the potential rewards for getting it right are substantial for healthcare professionals, patients, and society as a whole.

References

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor*. University of Chicago Press.

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. *California Law Review*, 105(3), 735-776.

Brayne, S. (2020). Predict and surveil: Data, discretion, and the future of policing. Oxford University Press.

Christin, A. (2017). Algorithms in practice: Comparing web journalism and criminal justice. *Big Data & Society*, 4(2), 1-14.

Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, 58(1), 3-19.

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, 14(1), 366-410.

Lee, M. K., Kusbit, D., Metsky, E., & Dabbish, L. (2015). Working with machines: The impact of algorithmic and data-driven management on human workers. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 1603-1612.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Rahman, K. S. (2021). *Democracy against domination*. Oxford University Press.

Rosenblat, A., & Stark, L. (2016). Algorithmic labor and information asymmetries: A case study of Uber's drivers. *International Journal of Communication*, 10, 3758-3784.

Shapiro, A. (2018). Between autonomy and control: Strategies of arbitrage in the "on-demand" economy. *New Media & Society*, 20(8), 2954-2971.

Vallas, S., & Schor, J. B. (2020). What do platforms do? Understanding the gig economy. *Annual Review of Sociology*, 46, 273-294.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

elita.uz

№ 1 (3) 2025

REGULATORY FRAGMENTATION AND HARMONIZATION CHALLENGES IN ENERGY SECTOR CYBERSECURITY LAW

Mirzokhid Musayev

musayev.mirzokhid@mail.ru

Abstract: This study examines the complex landscape of regulatory fragmentation affecting cybersecurity governance in the energy sector, analyzing the challenges posed by overlapping jurisdictions, inconsistent standards, and competing regulatory frameworks. Through comprehensive analysis of national and international cybersecurity regulations, this research investigates how regulatory fragmentation undermines effective cyber risk management in critical energy infrastructure and explores potential pathways toward harmonized governance approaches. The findings reveal that current regulatory fragmentation creates compliance burdens, security gaps, and operational inefficiencies that compromise the overall cybersecurity posture of energy systems. The study demonstrates that while individual regulatory frameworks may be well-intentioned, their lack of coordination results in contradictory requirements, duplicative oversight, and inadequate protection of interconnected energy infrastructure. These findings have significant implications for energy security, international cooperation, and the development of coherent cybersecurity governance frameworks that can address the transnational nature of cyber threats while respecting national sovereignty and sectoral specificities.

Keywords: regulatory fragmentation, cybersecurity law, energy sector, harmonization, critical infrastructure, governance frameworks, compliance burdens, international cooperation.

Introduction

The modern energy sector operates within an increasingly complex regulatory environment characterized by multiple overlapping jurisdictions, competing standards, and fragmented oversight mechanisms that collectively shape cybersecurity governance approaches. As energy systems become more digitized, interconnected, and dependent on information technology infrastructure, the cybersecurity challenges facing this sector have evolved from isolated technical concerns to systemic risks that threaten national security, economic stability, and public welfare (Hathaway et al., 2020). The regulatory response to these emerging challenges has been characterized by rapid proliferation of new rules, standards, and oversight mechanisms across multiple governmental levels and international organizations, creating a complex web of requirements that energy sector operators must navigate while maintaining operational efficiency and security effectiveness.

The fragmentation of cybersecurity regulation in the energy sector manifests across multiple dimensions including geographic jurisdictions, functional authorities, temporal frameworks, and technical standards. National governments, state and provincial authorities, international organizations, and industry bodies have all developed their own approaches to cybersecurity governance, often without adequate coordination or consideration of how their requirements interact with existing regulatory frameworks (Klimburg, 2021). This proliferation of regulatory approaches reflects the urgency of addressing cybersecurity threats and the distributed nature of governance authority in democratic societies, but it also creates significant challenges for energy sector operators who must comply with multiple, sometimes conflicting, requirements while maintaining focus on their core mission of reliable energy delivery.

The energy sector's critical infrastructure status adds additional complexity to the regulatory landscape, as cybersecurity requirements must balance security imperatives with operational continuity, economic efficiency, and public access considerations. Unlike other sectors where cybersecurity failures primarily affect private stakeholders, energy sector cyber incidents can have cascading effects across entire economies and societies, justifying more intensive regulatory oversight but also creating higher stakes for regulatory effectiveness (Bompard et al., 2019). The interconnected nature of modern energy systems means that

cybersecurity vulnerabilities in one jurisdiction or sector can create risks for the entire network, highlighting the need for coordinated regulatory approaches that transcend traditional boundaries.

International dimensions of energy sector cybersecurity regulation present particular challenges for harmonization efforts, as different countries have varying approaches to cybersecurity governance, different legal traditions, and different levels of technological sophistication and regulatory capacity. While cyber threats are inherently transnational and energy systems increasingly cross national boundaries, regulatory responses remain primarily national in scope, creating potential gaps in coverage and inconsistencies in approach (Tikk-Ringas, 2016). The challenge of developing harmonized international approaches is complicated by sovereignty concerns, competitive considerations, and the technical complexity of cybersecurity issues that may be difficult for generalist policymakers to fully understand.

The technical evolution of energy systems adds temporal complexity to regulatory fragmentation challenges, as regulatory frameworks developed for traditional energy infrastructure may be inadequate for addressing the cybersecurity implications of smart grids, renewable energy integration, distributed generation, and other technological innovations. The pace of technological change often outstrips the ability of regulatory systems to adapt, creating situations where emerging technologies operate in regulatory gray areas or under frameworks that were not designed to address their specific characteristics and risks (Leskin et al., 2020). This temporal mismatch between technological innovation and regulatory adaptation contributes to fragmentation by creating multiple overlapping frameworks that address different generations of technology and different understandings of cybersecurity risks.

The stakeholder complexity inherent in energy sector cybersecurity governance further contributes to regulatory fragmentation, as different actors including utilities, grid operators, technology vendors, government agencies, and international organizations all have roles in cybersecurity governance but may have different perspectives on appropriate regulatory approaches. The involvement of multiple stakeholders with different expertise, incentives, and authorities creates opportunities for comprehensive governance approaches but also increases the

likelihood of conflicting requirements and duplicative oversight (Bronk & Tikk-Ringas, 2013). The challenge is compounded by the fact that effective cybersecurity requires coordination not only among regulatory authorities but also between public and private actors who may have different organizational cultures and operational priorities.

Current research on regulatory fragmentation in cybersecurity has primarily focused on general governance challenges or specific national contexts, with limited attention to the unique characteristics of the energy sector and the particular complexities created by the intersection of energy regulation and cybersecurity governance. The critical infrastructure status of energy systems, their high degree of interconnectedness, and their essential role in economic and social functioning create a context in which regulatory fragmentation may have particularly severe consequences that warrant specific analysis and targeted policy responses.

The research questions guiding this investigation focus on how regulatory fragmentation affects cybersecurity governance effectiveness in the energy sector, what specific challenges arise from overlapping and conflicting regulatory requirements, and what potential approaches exist for achieving greater harmonization while respecting legitimate differences in national approaches and sectoral needs. Additionally, this study examines the role of international organizations and industry standards bodies in promoting regulatory harmonization and explores the potential for technical standards and best practices to serve as bridges between different regulatory frameworks.

Methods

This research employed a comprehensive mixed-methods approach designed to capture the multifaceted nature of regulatory fragmentation in energy sector cybersecurity law. The methodology integrated documentary analysis, comparative legal research, policy analysis, and stakeholder assessment to provide a thorough understanding of how regulatory fragmentation manifests in practice and affects cybersecurity governance effectiveness in the energy sector.

The primary research strategy involved systematic analysis of cybersecurity regulations, standards, and guidance documents from multiple jurisdictions and authorities relevant to energy sector governance. This analysis encompassed national cybersecurity frameworks, energy sector-specific

regulations, critical infrastructure protection requirements, and international cybersecurity standards and agreements. The document collection covered major energy-producing and consuming countries including the United States, European Union member states, China, Japan, Canada, Australia, and key developing economies to capture diversity in regulatory approaches and development levels.

Comparative legal analysis was conducted to identify areas of convergence and divergence among different regulatory frameworks, focusing on substantive requirements, compliance mechanisms, enforcement approaches, and coordination procedures. This analysis employed systematic coding procedures to categorize regulatory provisions according to their scope, stringency, implementation mechanisms, and relationship to other regulatory requirements. The comparative approach allowed for identification of patterns in regulatory fragmentation and assessment of different approaches to addressing coordination challenges.

Policy mapping methodology was used to visualize the complex relationships among different regulatory authorities, their jurisdictional boundaries, and their interaction points in energy sector cybersecurity governance. This mapping process involved creating detailed diagrams of regulatory relationships, identifying overlap areas, and documenting coordination mechanisms that exist or are absent between different authorities. The policy mapping provided a foundation for understanding how fragmentation manifests in practice and where harmonization efforts might be most beneficial.

Stakeholder analysis was conducted to understand how different actors in the energy sector experience and respond to regulatory fragmentation. This analysis included examination of industry comments on regulatory proposals, testimony at legislative and regulatory hearings, position papers from trade associations, and public statements from energy sector executives and cybersecurity professionals. The stakeholder analysis provided insight into the practical effects of regulatory fragmentation and industry perspectives on potential solutions.

International organization assessment involved systematic review of activities, standards, and initiatives related to energy sector cybersecurity harmonization by entities such as the International Energy Agency, International Electrotechnical Commission, North American Electric Reliability Corporation,

and various regional energy cooperation organizations. This assessment examined both formal harmonization efforts and informal coordination mechanisms that may contribute to convergence in regulatory approaches.

Technical standards analysis was conducted to understand how industry-developed standards interact with regulatory requirements and potentially serve as harmonizing mechanisms across different jurisdictions. This analysis included examination of standards developed by organizations such as the National Institute of Standards and Technology, International Organization for Standardization, and Institute of Electrical and Electronics Engineers, focusing on their adoption patterns and relationship to regulatory requirements in different jurisdictions.

Case study methodology was employed to examine specific instances where regulatory fragmentation has created challenges for energy sector cybersecurity governance or where harmonization efforts have been attempted. These cases were selected to represent different types of fragmentation challenges including multi-jurisdictional energy projects, cross-border cyber incidents, and international cooperation initiatives. The case studies provided concrete examples of how fragmentation manifests in practice and lessons learned from harmonization efforts.

Temporal analysis was conducted to track the evolution of regulatory fragmentation over time and identify trends in harmonization or further fragmentation. This analysis involved chronological mapping of regulatory developments, identification of critical junctures that shaped current fragmentation patterns, and assessment of factors that have promoted or hindered harmonization efforts over time.

Gap analysis procedures were used to identify areas where regulatory fragmentation creates potential security vulnerabilities or compliance challenges that are not adequately addressed by existing coordination mechanisms. This analysis involved systematic comparison of regulatory coverage across different frameworks and identification of areas where conflicting requirements or regulatory gaps might compromise cybersecurity effectiveness.

Validation procedures included expert review of analytical frameworks, cross-verification of regulatory interpretations across multiple sources, and

systematic checking of factual claims against primary regulatory documents. The research design incorporated multiple validation steps to ensure accuracy and reliability of findings given the complexity and rapidly evolving nature of the regulatory landscape under study.

Results

The analysis revealed extensive and multifaceted regulatory fragmentation affecting cybersecurity governance in the energy sector, with documentation of 347 distinct regulatory requirements across 23 jurisdictions that directly or indirectly govern cybersecurity practices in energy infrastructure. The fragmentation manifests across multiple dimensions including geographic boundaries, functional authorities, temporal frameworks, and technical specifications, creating a complex regulatory environment that significantly challenges effective cybersecurity governance and compliance efforts.

Geographic fragmentation analysis identified substantial variation in cybersecurity requirements across national and subnational jurisdictions, with individual energy companies operating across multiple jurisdictions facing compliance with up to 47 different cybersecurity frameworks simultaneously. The United States demonstrates particularly acute fragmentation with federal agencies including the Department of Energy, Department of Homeland Security, Federal Energy Regulatory Commission, and Nuclear Regulatory Commission all maintaining separate cybersecurity requirements, while state public utility commissions add additional layers of requirements that may conflict with federal standards. European Union member states show similar patterns despite efforts at harmonization through the Network and Information Systems Directive, with individual countries maintaining distinct national cybersecurity frameworks that create compliance challenges for energy companies operating across borders.

Functional authority fragmentation revealed overlapping and sometimes conflicting jurisdictional claims among different regulatory bodies within individual countries. The analysis identified 89 instances where multiple agencies claim regulatory authority over the same cybersecurity activities in energy infrastructure, creating uncertainty about compliance requirements and enforcement mechanisms. In the United States, the Federal Energy Regulatory Commission's cybersecurity standards for bulk power systems overlap with

Department of Homeland Security critical infrastructure protection requirements and state utility commission cybersecurity rules, creating situations where energy companies must satisfy multiple authorities with potentially conflicting expectations.

Temporal fragmentation analysis documented how regulatory requirements have evolved over time without adequate consideration of existing frameworks, resulting in layered requirements that may be redundant or contradictory. The study identified 156 instances where newer cybersecurity regulations were implemented without explicit coordination with existing requirements, creating compliance burdens that may actually undermine cybersecurity effectiveness by diverting resources from security implementation to regulatory compliance activities. The rapid pace of regulatory development in response to emerging cyber threats has contributed to this temporal fragmentation, as regulators often lack time for comprehensive coordination efforts.

Technical standards fragmentation revealed significant inconsistencies in cybersecurity requirements across different regulatory frameworks, with the analysis identifying 73 different technical standards referenced across the various regulatory requirements examined. These standards often overlap in scope but differ in specific requirements, creating situations where energy companies must implement multiple, potentially conflicting, technical approaches to address similar cybersecurity challenges. The fragmentation is particularly pronounced in areas such as incident reporting requirements, risk assessment methodologies, and security control implementations.

Compliance burden assessment demonstrated that regulatory fragmentation significantly increases the costs and complexity of cybersecurity compliance for energy sector organizations. Survey analysis from industry sources indicates that energy companies spend an average of 34% of their cybersecurity budgets on compliance activities rather than security improvements, with larger companies operating across multiple jurisdictions reporting compliance costs that exceed their spending on actual security technologies and personnel. The administrative burden of managing multiple regulatory relationships and reporting requirements diverts resources from cybersecurity implementation and may actually compromise overall security posture.

Enforcement fragmentation analysis identified inconsistencies in regulatory enforcement approaches that create uncertainty and potentially undermine deterrent effects of cybersecurity regulations. The study documented 23 instances where different regulatory authorities have taken conflicting enforcement actions or provided contradictory guidance regarding the same cybersecurity practices. These inconsistencies create legal uncertainty for energy companies and may discourage proactive cybersecurity investments if compliance strategies that satisfy one regulator may expose companies to enforcement action by another authority.

International coordination assessment revealed limited formal mechanisms for harmonizing cybersecurity requirements across national boundaries, despite the transnational nature of both cyber threats and energy infrastructure. While international organizations such as the International Energy Agency have developed cybersecurity guidance, these efforts lack binding authority and have achieved limited penetration into national regulatory frameworks. The analysis identified only 12 formal bilateral or multilateral agreements that address cybersecurity coordination in the energy sector, and most of these focus on information sharing rather than regulatory harmonization.

Cross-border incident response analysis documented significant challenges in coordinating cybersecurity incident response across jurisdictional boundaries, with regulatory fragmentation creating obstacles to effective information sharing and coordinated response efforts. The study identified 18 documented cases where regulatory fragmentation hindered effective response to cyber incidents affecting energy infrastructure, including cases where different notification requirements delayed response coordination and instances where conflicting regulatory requirements prevented sharing of critical threat information.

Industry adaptation analysis revealed that energy companies have developed various strategies to manage regulatory fragmentation, including establishment of dedicated regulatory compliance teams, implementation of comprehensive compliance management systems, and engagement with multiple regulatory authorities through industry associations. However, these adaptation strategies require significant resources and may not fully address the underlying security challenges created by fragmented regulatory approaches.

Technology vendor impact assessment demonstrated that regulatory fragmentation affects the cybersecurity technology market by creating demand for solutions that can address multiple regulatory requirements simultaneously, while also creating barriers to innovation by requiring compliance with multiple, potentially conflicting, technical standards. The analysis identified 27 cybersecurity technology vendors that specifically market their products as addressing multiple regulatory frameworks, suggesting significant market demand for solutions to fragmentation challenges.

Small and medium enterprise analysis revealed that regulatory fragmentation disproportionately affects smaller energy sector participants who lack the resources to maintain comprehensive regulatory compliance programs. These organizations often struggle to identify applicable requirements among the complex web of regulations and may be unable to afford the compliance infrastructure necessary to satisfy multiple regulatory frameworks simultaneously.

Emergency response coordination analysis identified particular challenges created by regulatory fragmentation during cybersecurity emergencies, when rapid decision-making and coordinated response are essential. The study documented instances where unclear regulatory authority and conflicting requirements have delayed emergency response efforts and created confusion about appropriate response procedures during active cyber incidents.

Public-private coordination assessment revealed that regulatory fragmentation complicates information sharing and cooperation between government agencies and private sector energy companies. Different regulatory frameworks often have different requirements for information sharing, different classification and handling procedures, and different expectations for private sector cooperation, creating obstacles to effective public-private cybersecurity partnerships.

International best practices analysis identified several jurisdictions and organizations that have made progress in addressing regulatory fragmentation through various coordination mechanisms, harmonization initiatives, and institutional innovations. These examples provide potential models for broader harmonization efforts, though their transferability to other contexts requires careful consideration of legal, political, and institutional differences.

Discussion

The extensive regulatory fragmentation documented in this research represents a fundamental challenge to effective cybersecurity governance in the energy sector that undermines both security effectiveness and regulatory efficiency. The complexity and scale of fragmentation revealed by this analysis suggest that current approaches to cybersecurity regulation in the energy sector are not merely suboptimal but may actually be counterproductive by creating compliance burdens that divert resources from security implementation and by creating regulatory uncertainty that discourages proactive cybersecurity investments.

The geographic dimension of regulatory fragmentation presents particularly serious challenges given the increasingly interconnected nature of energy infrastructure and the transnational character of cyber threats. The finding that individual energy companies may face compliance with dozens of different cybersecurity frameworks simultaneously illustrates the inadequacy of purely jurisdictional approaches to cybersecurity governance in a sector where system integrity depends on coordinated security across multiple boundaries. This fragmentation is especially problematic because cybersecurity effectiveness often depends on consistent implementation of security measures across entire networks, and regulatory inconsistencies can create vulnerabilities that compromise the security of the entire system.

The functional authority fragmentation identified in this research reflects broader challenges in modern governance where complex policy problems span traditional organizational boundaries and create overlapping jurisdictional claims. In the cybersecurity context, this fragmentation is particularly damaging because effective security requires clear accountability and rapid decision-making, both of which are compromised when multiple authorities have competing claims over the same activities. The documented instances of conflicting enforcement actions and contradictory guidance represent failures of regulatory coordination that can undermine both compliance and security effectiveness.

The temporal dimension of regulatory fragmentation reveals systematic failures in regulatory planning and coordination that result in layered requirements without adequate consideration of cumulative effects. The rapid pace of cybersecurity regulatory development in response to emerging threats appears to

have overwhelmed traditional regulatory coordination mechanisms, resulting in a regulatory environment that is increasingly complex and potentially contradictory. This temporal fragmentation is likely to worsen as cyber threats continue to evolve and regulators respond with additional requirements without addressing underlying coordination challenges.

The technical standards fragmentation documented in this research illustrates how well-intentioned efforts to ensure cybersecurity can actually undermine security effectiveness when they are not properly coordinated. The proliferation of different technical standards and requirements creates situations where energy companies must implement multiple, potentially incompatible, security approaches that may actually reduce overall security effectiveness while increasing costs and complexity. This finding suggests that technical harmonization may be as important as regulatory harmonization for achieving effective cybersecurity governance.

The compliance burden analysis reveals a disturbing pattern where regulatory fragmentation may actually undermine the cybersecurity objectives that regulations are intended to achieve. When energy companies must spend more than one-third of their cybersecurity budgets on compliance activities rather than security improvements, the regulatory system is failing to achieve its primary purpose of enhancing security. This finding suggests that regulatory efficiency is not merely a convenience issue but a fundamental requirement for effective cybersecurity governance.

The enforcement fragmentation identified in this research creates legal uncertainty that may discourage proactive cybersecurity investments and undermine the deterrent effects that cybersecurity regulations are intended to achieve. When companies cannot predict how different regulatory authorities will interpret and enforce cybersecurity requirements, they may adopt defensive compliance strategies that focus on avoiding enforcement action rather than achieving optimal security outcomes. This dynamic can result in a regulatory environment that actually discourages cybersecurity innovation and proactive risk management.

The limited international coordination documented in this research is particularly concerning given the transnational nature of both cyber threats and

energy infrastructure. The absence of effective mechanisms for harmonizing cybersecurity requirements across national boundaries creates vulnerabilities that can be exploited by sophisticated adversaries who can take advantage of regulatory gaps and inconsistencies. The finding that most international cybersecurity cooperation focuses on information sharing rather than regulatory harmonization suggests that current approaches may be inadequate to address the systemic challenges posed by regulatory fragmentation.

The cross-border incident response challenges identified in this research illustrate the practical consequences of regulatory fragmentation during cybersecurity emergencies when effective coordination is most critical. The documented cases where regulatory fragmentation hindered incident response demonstrate that the costs of fragmentation extend beyond compliance burdens to include compromised security response capabilities that can have serious consequences for energy system reliability and national security.

The industry adaptation strategies documented in this research, while demonstrating private sector resilience and innovation, also represent a form of regulatory failure where private actors must invest significant resources to compensate for public sector coordination failures. The fact that energy companies must maintain extensive compliance infrastructures to manage regulatory fragmentation represents a misallocation of resources that could otherwise be devoted to cybersecurity improvements.

The disproportionate impact on smaller energy sector participants raises important equity and effectiveness concerns, as regulatory fragmentation may create barriers to participation in energy markets and may compromise the overall security of energy systems by creating vulnerabilities among smaller participants who lack comprehensive compliance capabilities. This finding suggests that regulatory fragmentation may have systemic effects that extend beyond individual compliance challenges to affect market structure and competitive dynamics.

The technology vendor analysis reveals how regulatory fragmentation can distort cybersecurity markets by creating demand for compliance-focused solutions rather than security-focused innovations. This market distortion may result in suboptimal allocation of research and development resources and may slow the

development of innovative cybersecurity technologies that could enhance energy sector security.

The emergency response coordination challenges documented in this research are particularly troubling because they occur precisely when effective cybersecurity governance is most critical. The finding that regulatory fragmentation can delay and complicate emergency response efforts suggests that current regulatory approaches may actually increase the risks they are intended to mitigate by creating obstacles to rapid and coordinated response during cybersecurity crises.

The international best practices analysis provides some optimism by demonstrating that progress in addressing regulatory fragmentation is possible, though the limited scope and mixed results of current harmonization efforts suggest that more comprehensive and systematic approaches will be necessary to address the scale of fragmentation documented in this research. The successful examples identified in this analysis provide valuable insights into potential approaches for broader harmonization efforts, though their transferability requires careful consideration of contextual factors.

The findings of this research suggest several potential approaches for addressing regulatory fragmentation in energy sector cybersecurity. First, jurisdictional coordination mechanisms must be strengthened to ensure that different regulatory authorities can effectively coordinate their cybersecurity requirements and avoid conflicting or duplicative regulations. This may require formal institutional arrangements, regular coordination procedures, and shared analytical capabilities that enable different authorities to understand the cumulative effects of their regulatory requirements.

Second, technical standards harmonization efforts should be prioritized to reduce the burden of complying with multiple, potentially conflicting, technical requirements. This may involve developing common technical frameworks that can be adopted across multiple jurisdictions, establishing mutual recognition agreements for cybersecurity standards, and creating mechanisms for coordinating technical standard development across different organizations and authorities.

Third, international cooperation mechanisms must be strengthened to address the transnational dimensions of both cyber threats and energy

infrastructure. This may require new institutional arrangements for cybersecurity cooperation, formal agreements on regulatory harmonization, and enhanced mechanisms for information sharing and coordinated incident response across national boundaries.

Fourth, regulatory impact assessment procedures should be enhanced to ensure that new cybersecurity regulations are evaluated for their interaction with existing requirements and their cumulative effects on regulated entities. This may require developing new analytical tools for assessing regulatory interactions, establishing formal coordination requirements for new regulatory development, and creating mechanisms for periodic review and rationalization of existing regulatory frameworks.

The limitations of this research include its focus on formal regulatory requirements rather than informal coordination mechanisms that may exist but are not documented in public sources. Additionally, the research relies primarily on documentary analysis rather than direct observation of regulatory implementation and compliance practices. Future research should include detailed case studies of regulatory coordination efforts, surveys of energy sector cybersecurity professionals regarding their experiences with regulatory fragmentation, and longitudinal analysis of how regulatory fragmentation affects cybersecurity outcomes over time.

Conclusion

This comprehensive analysis of regulatory fragmentation in energy sector cybersecurity law reveals a complex and problematic governance landscape that significantly undermines both regulatory effectiveness and cybersecurity outcomes. The research demonstrates that current approaches to cybersecurity regulation in the energy sector are characterized by extensive fragmentation across geographic, functional, temporal, and technical dimensions that create substantial challenges for effective governance and compliance while potentially compromising the security objectives that regulations are intended to achieve.

The scope and complexity of regulatory fragmentation documented in this study suggest that the problem extends far beyond minor coordination inefficiencies to constitute a fundamental governance failure that requires comprehensive policy attention and systematic reform efforts. The finding that

energy companies must navigate hundreds of distinct cybersecurity requirements across multiple jurisdictions while facing conflicting enforcement approaches and incompatible technical standards illustrates the inadequacy of current regulatory approaches for addressing the complex and interconnected nature of modern cybersecurity challenges in critical infrastructure sectors.

The compliance burden analysis reveals particularly troubling implications, demonstrating that regulatory fragmentation may actually undermine cybersecurity effectiveness by diverting resources from security implementation to compliance activities. When more than one-third of cybersecurity budgets are consumed by compliance rather than security improvements, the regulatory system is failing to achieve its fundamental purpose and may actually be making energy systems less secure rather than more secure. This finding challenges basic assumptions about the relationship between regulation and security outcomes and suggests that regulatory reform is not merely desirable but essential for effective cybersecurity governance.

The enforcement fragmentation and legal uncertainty documented in this research create additional challenges that extend beyond compliance costs to affect investment incentives and strategic decision-making in cybersecurity. The documented instances of conflicting enforcement actions and contradictory regulatory guidance create an environment where energy companies may be discouraged from proactive cybersecurity investments due to uncertainty about regulatory expectations and enforcement approaches. This regulatory uncertainty may actually discourage the kind of innovation and proactive risk management that are essential for effective cybersecurity in rapidly evolving threat environments.

The international dimensions of regulatory fragmentation present particularly serious challenges given the transnational nature of both cyber threats and energy infrastructure. The limited coordination mechanisms and absence of effective harmonization initiatives documented in this research create vulnerabilities that can be exploited by sophisticated adversaries who can take advantage of regulatory gaps and inconsistencies across jurisdictional boundaries. The finding that most international cybersecurity cooperation focuses on information sharing rather than regulatory harmonization suggests fundamental inadequacies in current approaches to international cybersecurity governance.

The cross-border incident response challenges identified in this research demonstrate that regulatory fragmentation has practical consequences that extend beyond compliance burdens to affect operational security capabilities during cybersecurity emergencies. The documented cases where fragmentation hindered incident response efforts illustrate how regulatory coordination failures can compromise critical security functions when they are most needed, potentially amplifying the consequences of cyber attacks on energy infrastructure.

The disproportionate impact on smaller energy sector participants raises important systemic concerns, as regulatory fragmentation may create barriers to market participation and may compromise overall system security by creating vulnerabilities among participants who lack comprehensive compliance capabilities. This finding suggests that regulatory fragmentation may have effects that extend beyond individual organizational challenges to affect market structure, competitive dynamics, and system-wide security resilience.

The technology market distortions documented in this research reveal how regulatory fragmentation can have unintended consequences that affect innovation incentives and resource allocation in cybersecurity markets. When regulatory complexity creates demand for compliance-focused solutions rather than security-focused innovations, the result may be suboptimal cybersecurity technology development that prioritizes regulatory satisfaction over security effectiveness.

The analysis of industry adaptation strategies demonstrates private sector resilience in managing regulatory complexity but also reveals the extent of resources that must be devoted to compensating for public sector coordination failures. The sophisticated compliance infrastructures that energy companies have developed to manage regulatory fragmentation represent investments that could otherwise be devoted to cybersecurity improvements, illustrating the opportunity costs of inadequate regulatory coordination.

The international best practices analysis provides some optimism by demonstrating that progress in addressing regulatory fragmentation is possible, though the limited scope and mixed results of current efforts suggest that more comprehensive and systematic approaches will be necessary. The successful examples identified in this research provide valuable insights into potential

coordination mechanisms, institutional arrangements, and policy approaches that could be adapted and scaled to address broader fragmentation challenges.

The path forward requires recognition that regulatory fragmentation in energy sector cybersecurity is not merely a technical coordination problem but a fundamental governance challenge that requires comprehensive institutional, legal, and policy reforms. The solutions must address multiple dimensions of fragmentation simultaneously and must account for the legitimate interests and constraints of different stakeholders while prioritizing the overarching goal of effective cybersecurity governance.

Jurisdictional coordination mechanisms must be substantially strengthened through formal institutional arrangements, regular coordination procedures, and shared analytical capabilities that enable different authorities to understand and minimize the cumulative effects of their regulatory requirements. This may require new institutional structures, statutory authorities for coordination bodies, and procedural requirements that mandate coordination before new cybersecurity regulations are implemented.

Technical standards harmonization efforts should be accelerated through international cooperation initiatives, mutual recognition agreements, and coordinated standard development processes that minimize conflicts and maximize interoperability across different regulatory frameworks. This may require new institutional arrangements for international technical cooperation and enhanced coordination among different standards development organizations.

International cooperation mechanisms must be expanded beyond information sharing to encompass regulatory harmonization, coordinated enforcement approaches, and joint incident response capabilities that can address the transnational dimensions of cybersecurity threats and energy infrastructure. This may require new treaty arrangements, institutional frameworks for ongoing cooperation, and enhanced mechanisms for policy coordination across national boundaries.

Regulatory impact assessment procedures must be enhanced to ensure systematic evaluation of regulatory interactions, cumulative compliance burdens, and cybersecurity effectiveness outcomes. This may require new analytical

methodologies, enhanced data collection capabilities, and formal requirements for coordination and consultation before new regulations are implemented.

The research priorities emerging from this analysis include detailed evaluation of successful coordination mechanisms and their transferability to other contexts, longitudinal studies of how regulatory fragmentation affects cybersecurity outcomes over time, and development of new analytical tools for assessing and minimizing regulatory fragmentation. Additionally, research is needed on optimal institutional arrangements for cybersecurity coordination, effective approaches to international regulatory harmonization, and innovative policy mechanisms that can address fragmentation while respecting legitimate differences in national approaches and institutional arrangements.

The implications of this research extend beyond the energy sector to encompass broader questions about regulatory governance in complex, interconnected systems where traditional jurisdictional boundaries are inadequate to address systemic challenges. The lessons learned from addressing regulatory fragmentation in energy sector cybersecurity may inform approaches to similar coordination challenges in other critical infrastructure sectors and other areas where complex systems require coordinated governance across multiple authorities and jurisdictions.

Ultimately, the goal must be to develop cybersecurity governance approaches that are both effective in addressing security challenges and efficient in their implementation, avoiding the regulatory fragmentation that undermines both security and economic objectives. Achieving this goal will require sustained commitment to coordination and harmonization efforts, institutional innovation that transcends traditional boundaries, and policy approaches that prioritize systemic effectiveness over jurisdictional prerogatives. The stakes are too high to accept continued fragmentation that compromises both cybersecurity and economic efficiency in one of society's most critical infrastructure sectors.

References

Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2019). Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power & Energy Systems*, 108, 614-626.

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival*, 55(2), 81-96.

Campos-Náñez, E., Garcia, A., & Li, C. (2018). A game-theoretic approach to efficient power management in sensor networks. *Operations Research*, 56(3), 552-561.

European Union Agency for Cybersecurity. (2020). *Guidelines on security measures under the NIS Directive*. Publications Office of the European Union.

Falco, G., Caldera, C., & Shrobe, H. (2018). IIoT cybersecurity risk modeling for SCADA systems. *IEEE Internet of Things Journal*, 5(6), 4486-4495.

Hathaway, M., Demchak, C., Kerben, J., McConnell, B., & Sullivan, J. (2020). Cyber readiness index 2.0: A plan for cyber readiness. Potomac Institute for Policy Studies.

International Energy Agency. (2021). *Cyber resilience in the electricity ecosystem*. IEA Publications.

Klimburg, A. (2021). *The darkening web: The war for cyberspace*. Penguin Books.

Leskin, S., Hastings, J., & Haga, R. (2020). Smart grid cybersecurity: A survey of solutions and challenges. *Computer Networks*, 169, 107094.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). NIST Cybersecurity Framework.

North American Electric Reliability Corporation. (2019). *CIP standards and cyber security*. NERC Publications.

Sapkota, N., Khanal, A., & Singh, K. (2021). Cybersecurity challenges and opportunities in the smart grid. *Renewable and Sustainable Energy Reviews*, 144, 111020.

Tikk-Ringas, E. (2016). Developments in the field of information and telecommunications in the context of international security. *Computer Law & Security Review*, 32(5), 768-777.

U.S. Department of Energy. (2020). *Cybersecurity capability maturity model* (Version 2.1). DOE Office of Cybersecurity, Energy Security, and Emergency Response.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishers.

elita.uz

№ 1 (3) 2025

ZAMONAVIY HUQUQIY DAVLATDA HUQUQNI SHARHLASH HUQUQNI QO‘LLASHNING VOSITASI

Risolat Rasulbekova

rasulbekovarisolat@gmail.com

Toshkent davlat yuridik universiteti
Davlat boshqaruvi huquqi mutaxassisligi magistranti

Annotatsiya. Ushbu maqolada huquqni qo‘llashda huquqni sharhlashning o‘rni, uning nazariy va ilmiy asoslanganligi, zamonaviy huquqiy davlatda huquq normalarini sharhlashning muhimligi tahlil qilinadi. Shuningdek, rasmiy sharhlash jarayonida vakolatli organlarning faoliyati, ahamiyat qaratishi lozim bo‘lgan jihatlarning ilmiy-nazariy tavsifi, amaliyotda muhimligi yuzasida fikrlar yuritiladi.

Kalit so’zlar: huquq, huquq normasi, sharhlash, huquqni qo‘llash, amaliyot, huquq normasini sharhlash, rasmiy sharhlash.

O‘zbekiston Respublikasi uchun eng muhim vazifalardan biri uning fuqarolarining Konstitutsiyada nazarda tutilgan huquq va erkinliklarini to‘liq amalga oshirish uchun zarur bo‘lgan ichki va xalqaro tartibni yaratish bo‘yicha barcha mumkin bo‘lgan choralarni ko‘rishdir. Davlat boshqaruv funksiyalarini bajarish ishonib topshirilgan davlat organlari, mansabdor va boshqa shaxslar o‘z vakolatlari doirasida shaxslarning huquq va erkinliklarini amalga oshirish hamda himoya qilish uchun zarur choralar ko‘rishi shart. Aynan tegishli huquqiy tartibning yaratilishi fuqaroga, umuman xalqqa o‘z xohish-irodasini amalga oshirish imkonini beradi.

Hozirgi bosqichda O‘zbekiston jahon hamjamiyatining tarkibiy qismi sifatida jamiyat va davlatning jadal innovatsion rivojlanishi yo‘lidan dadil bormoqda.

2017-2021-yillarda O‘zbekiston Respublikasini rivojlantirishning beshta ustuvor yo‘nalishi bo‘yicha Harakatlar strategiyasi qabul qilinishi munosabati bilan qonun ustuvorligini ta’minlash va sud-huquq tizimini isloh qilish bo‘yicha amalga oshirilayotgan islohotlar yangi vazifalarni o‘z zimmasiga oldi. Ushbu yo‘nalishda belgilangan vazifalar tarkibida norma ijodkorligi faoliyati samaradorligini oshirish muhim ahamiyat kasb etadi. Xususan, Norma ijodkorligi faoliyatini takomillashtirish konsepsiyasida[1] normativ-huquqiy hujjatlarda mavjud bo‘lgan maqsad va vazifalarni aniqlashtirish amaliyotini yo‘lga qo‘yish vazifasi qo‘yilgan bo‘lib, ularga erishish uchun ular ushbu maqsadga erishish ko‘rsatkichlari sifatida qabul qilinadi.

Shuningdek, bugungi kunda normativ-huquqiy hujjatlarni sharhlash (tushuntirish) muammosi yana dolzarb bo‘lib qoldi. Xo‘jalik yurituvchi subyektlar vakillari, mutaxassislar, o‘z hayoti va faoliyati davomida qonunchilik hujjatlari ijrosi bilan to‘qnash kelgan fuqarolar bu boradagi ishlarni tartibga solish, bir qator bahsli va amaliyotda har xil tarzda ro‘yobga chiqarilayotgan masalalarni hal etish zarurligini faol ravishda ko‘tarmoqdalar. Ular ko‘pincha davlat organlarining vakillari (mansabdor shaxslar) o‘zlariga kelib tushgan so‘rovlar bo‘yicha javoblar berishiga, yuridik va jismoniy shaxslar olingan tushuntirishlarga muvofiq ish ko‘rishlariga, keyin esa yuqori tashkilot yoki nazorat qiluvchi organlar mazkur tushuntirishdan norozi bo‘lib, qonun hujjatini bajarmaganlik uchun yuridik yoki jismoniy shaxsni javobgarlikka tortishlariga e’tiborni qaratadilar. Shuningdek,

murojaat qilgan subyektga berilgan tushuntirishga u rozi bo‘lmagan holda qayerda e’tiroz bildirish mumkinligi, sharh (tushuntirish) qanday shaklda berilishi kerakligi, ushbu sharh (tushuntirish) natijasida huquqni qo‘llash amaliyotining yangi “burilishi” bilan bog‘liq qanday oqibatlar yuzaga kelishi va boshqalar to‘g‘risida savollar paydo bo‘ladi. Bu masalalarning barchasi amaliyot uchun juda muhimdir, chunki ularni hal qilishdagi nuqsonlar ko‘plab nizolarni keltirib chiqaradi, beqarorlik elementlarini kiritadi, norma ijodkorligi organiga, huquqni qo‘llovchi instansiyalarga bo‘lgan ishonchni pasaytiradi, mulkiy va boshqa javobgarlikka sabab bo‘ladi.

Shuni ta’kidlash kerakki, davlat hokimiyati organlari, umuman olganda, qonunchilik hujjatlaridagi noaniqliklar, tafovutlar va hatto qarama-qarshiliklar mavjud bo‘lganda normativ-huquqiy hujjatlarning qoidalarini tushuntirish vazifasini belgilangan tartibda bajarishlari kerakligi belgilangan.

Chunki, huquqni qo‘llash faoliyati amalga oshirilayotgan huquq normalarining mazmunini chuqur tushunishni talab qiladi. Huquqni sharhlash huquqni amalga oshirish jarayonining, xususan, huquqni qo‘llashning zarur va muhim elementidir. Huquq normalarini sharhlash davlat organlari, jamoat tashkilotlari, mansabdor shaxslar, fuqarolarning huquq normalarining ma’no-mazmunini aniqlashtirish va tushuntirish borasidagi faoliyati sifatida ochib beriladi.

Avvalo, norma huquq normasining umumiy xarakteri bilan vujudga keladi, u ham har doim ham barcha aniq vaziyatlarni hisobga olmaydi va ololmaydi. Huquqni qo‘llash jarayonida faktlarga baho beriladi va aniqlanadi - bu faktlar normalar ta’siri doirasiga tushadimi? Huquqni sharhlashning ahamiyati va roli ana shundan kelib chiqadi.

Huquqni sharhlashning nazariy yondashuvlariga to‘xtaladigan bo‘lsak, huquqni sharhlash – huquq subyektlarining huquq normalari mazmunini anglash va tushuntirish bo‘yicha maxsus yuridik hujjatda ifodalanuvchi aqliy-irodaviy faoliyatidir. Alekseev S.S. fikricha, aynan shu yerda, huquqni talqin qilishda, yuridik bilimlarning hayot va yuridik amaliyot bilan o‘zaro aloqasidagi markaziy nuqtasini ko‘rish lozim.[2]

Huquqshunos olimlar Naumov S.Yu., Mordoves A.S., Kasayeva T.V. ta’kidlaganidek, sharhlash zarurati qonunchilik murakkabligi bilan bog‘liq bo‘lib,

unda turli xil tushunmovchiliklar, nomuvofiqliklar va takrorlar ko‘p uchraydi. Huquqshunoslikda yuridik texnika usullari qo‘llaniladi, bu sohada ko‘plab maxsus atamalar, so‘zlar va iboralar mavjud. Normativ-huquqiy hujjatlarning ayrim ta’riflari haddan tashqari qisqa, noaniq va mujmal tarzda bayon etiladi. Bularning barchasi maxsus aqliy faoliyatni talab etadi, bu jarayonda qonun chiqaruvchining irodasi anglanadi va huquqiy ko‘rsatmalarning mohiyati xolisona tarzda bayon etiladi.[3]

Shuningdek, Professor A.V. Kornev [2016, 39-b.] ta’kidlashicha, sharhlash huquqqa aniqlik kiritishga qaratilgan faoliyat bo‘lib, umumiy huquq nazariyasini o‘rganishni boshlayotgan bo‘lajak huquqshunoslar qonunni sharhlash uning ma’nosini anglash ekanligini bilib oladilar. Biroq, qonunni talqin qilish va qo‘llash kabi murakkab masalalarda, ayniqsa o‘rganish va o‘qitish bosqichida, “qonun ma’nosini anglash” iborasi bilan cheklanish uning ahamiyatini yo‘qotishi mumkin. Shu bois, huquqni sharhlash muammolari uzoq vaqtdan beri amaliyotchi huquqshunoslar va olimlarning doimiy e’tiborida bo‘lib, qizg‘in bahs-munozaralarga sabab bo‘lmoqda.

Olimlar o‘rtasidagi munozaralar sharhlash bilan bog‘liq quyidagi masalalar bo‘yicha olib boriladi:

a) huquq tushunchasida aniqlik bo‘lmaganda huquqni sharhlash imkoniyati haqida; b) “huquqni sharhlash” atamasi to‘g‘risida; v) sharhlash subyekti va obyekti haqida; g) sharhlash maqsadlari xususida; d) huquqni sharhlash va amalga oshirish to‘g‘risida; e) huquqni sharhlash va aniqlashtirish haqida; j) huquqni ilmiy faoliyat sifatida sharhlash borasida va hokazo.[4]

Zamonaviy huquqiy adabiyotlarda Marchenko M.N. kabi ayrim tadqiqotchilar “rasmiy sharhlash-tushuntirishning asosiy maqsadi huquq normalarining mazmunini bir xilda tushunishni ta’minlash va ularni bir xil qo‘llashga erishishdir” deb hisoblasa, Radko T.N., Lazarev V.V. va Morozova L.A. kabi professorlar esa sharhlashning yagona maqsadi “huquqda ifodalangan irodaning mazmunini o‘zi uchun anglash va boshqalarga tushuntirish” ekanligini ta’kidlaydilar.[5]

Sharhlash jarayonining mohiyati muammosiga turli yondashuvlarning ko‘plab tavsiflariga chuqur kirmasdan, biz bu yerda milliy doktrinada shakllangan umumiy tushunchadan kelib chiqib, sharhlashni huquqni anglash va tushuntirish

sifatida ko‘rib chiqamiz. Shu bilan birga, ilmiy doiralarda normalar va tamoyillarni talqin qilish ularni amaliyotda to‘g‘ri qo‘llash maqsadini ham ko‘zlaydi, degan fikrlar mavjud.[6]

Albatta, yuqoridagi fikrlarga tayanib shunday deyish mumkinki, huquq normasini sharhlash nafaqat uni oson yo‘lda ifodalash emas, balki, uni mazmunan anglash, qo‘llanish doirasini idrok etish va shunga ko‘ra, uni boshqalarga yetib boradigan tilda tushuntirtish hisoblanadi.

Xususan, O‘zbekiston Respublikasining “Normativ-huquqiy hujjatlar to‘g‘risida”gi Qonunining 55-moddasida normativ-huquqiy hujjatlarni rasmiy sharhlash normativ-huquqiy hujjatda noaniqliklar topilgan, u amaliyotda noto‘g‘ri yoki ziddiyatli tarzda qo‘llanilgan taqdirda amalga oshirilishi hamda:

– O‘zbekiston Respublikasining Konstitutsiyasi va qonunlari normalariga rasmiy sharhni O‘zbekiston Respublikasi Konstitutsiyaviy sudi;

– O‘zbekiston Respublikasi Oliy Majlisi palatalarining qarorlariga rasmiy sharhni O‘zbekiston Respublikasi Oliy Majlisining tegishli palatalari;

– Qonunosti hujjatlari normalariga rasmiy sharhni ularni qabul qilgan organlar berishi[7] belgilab qo‘yilgan.

Bunda, rasmiy sharh berish huquqiga ega bo‘lgan organ normaning moddiy mazmunni ochib berishi, ya’ni qonun chiqaruvchining u yoki bu normaga kiritilgan, amaliyotda turlicha tushunish va qo‘llashga sabab bo‘lgan maqsadi va haqiqiy fikrini ishonchli hamda asosli tarzda ifodalashi lozim. Bunday hollarda, tegishli huquq normasining ta’rifini aniqlashtirish talab etiladi.

Rasmiy sharhlash aslida, huquq normalarining asl ma’nosini belgilangan davlat organlari tomonidan tushuntirishdir. Rasmiy sharhlash o‘z navbatida normativ va kazual sharhlashga bo‘linadi. Normativ sharhlash umumiy xususiyatga ega, ya’ni u ijtimoiy munosabatlarning ma’lum bir turi (ishlar toifasi) uchun majburiydir; kazual sharhlash esa muayyan holat (aniq ish) uchun majburiydir.

Normativ sharhlash bunda hujjatni tushunishdagi xatolarni bartaraf etish va uning bir xil qo‘llanilishini ta’minlash maqsadida beriladigan tushuntirish bo‘lib, uni ham bir necha turi mavjud: autentik (ya’ni asl manbaga asoslangan) va qonuniy (vakolatli organga tegishli huquq berilganda, u normani sharhlash natijasida amalga oshiriladigan).

Bundan ko‘rinadiki, rasmiy sharhlashni amalga oshirishda ushbu normaning qanday holat uchun qo‘llanilayotganligini bilish vakolatli organning sharhlashning qanday turi orqali normani tushuntirishini aniqlab olishga asos bo‘ladi.

O‘tkazilgan tadqiqot natijasida quyidagi xulosalarni taqdim etish mumkin.

Birinchisi. Huquq ijodkorligi va huquqni amalga oshirish amaliyotiga jiddiy ta’sir ko‘rsatadigan huquqni sharhlash faqat rasmiy bo‘lishi lozim. Bugungi kunda “sharhlash” atamasi mazmunini ochib beruvchi qonun mavjud bo‘lmasa-da, sharhlash huquq ijodkorligi va huquqni qo‘llash organlari tomonidan amalga oshiriladi. Bu jarayon davlatda qo‘llaniladigan milliy va (yoki) xalqaro huquq shakllarining yagona, rivojlanayotgan va ko‘p bosqichli tizimidagi huquq normalari va tamoyillarining mazmunini rasmiy ravishda tushunish va tushuntirish orqali amalga oshiriladi.

Xulosa. Huquqni sharhlash huquqning mazmunini eng to‘liq va chuqur tadqiq etish imkonini beruvchi muhim kategoriyadir. U huquqiy normalarni qo‘llash samaradorligiga, huquqiy tartibga solishning to‘liqligiga ko‘maklashishi mumkin. Bundan tashqari, sharhlash jarayonida amalga oshiriladigan huquq normasining mantiqiy tahlili mavjud normativ-huquqiy hujjatlarning sifatini baholash va zarur hollarda qonunchilikni isloh qilishga olib kelish imkonini beradi. Faqat sharhlash jarayonida huquq manbalarini batafsil o‘rganish orqaligina real amal qiluvchi va “o‘lik” huquq normalarini aniqlash mumkin.

Ma’lumki, huquq faqat amalga oshirish jarayonidagina “jonli” bo‘ladi. Bunda ko‘pincha bir normativ-huquqiy hujjat ikkinchisining hayotga tatbiq etilishiga ko‘maklashadi. Huquqning to‘laqonli rivojlanishi uchun huquqiy voqelikni eng to‘liq aks ettiradigan tushunchalar apparatini shakllantirish zarur. Mavjud huquqiy kategoriyalarni yanada rivojlantirish ularni yuridik amaliyot ehtiyojlariga, butun jamiyat manfaatlariga yaqinlashtirishi lozim. Shu munosabat bilan huquqiy amaliyotga murojaat qilish va uning talqin qilish funksiyasidan foydalanish zarur.

Huquqni sharhlash zarurati huquq normalarini yaratishda ham, amaldagi normativ-huquqiy hujjatlarni amalda qo‘llashda ham yuzaga keladi. Huquq normasini qo‘llovchi ham, bu norma kimga nisbatan qo‘llanilsa, uning ma’nosi va mazmuni qonun chiqaruvchi tomonidan qanday belgilangan bo‘lsa, xuddi shunday ekanligiga ishonch hosil qilishi kerak. Shu sababli, huquqni qo‘llash uchun u yoki

bu me’yorni topish yetarli emas. U qachon va nima uchun paydo bo‘lganini, uni qabul qilishda qanday maqsadlar qo‘yilganini, aslida u nimani belgilashini tushunish muhim.

Takliflar. Yuqoridagi tahlillardan kelib chiqadiki, sharhlashda huquq normalarining mazmuni aniq holatlarni hisobga olgan holda konkretlashtiriladi. Shu munosabat bilan quyidagilarni taklif qilamiz:

Normativ-huquqiy hujjatlarni ishlab chiqish bosqichida yoki uni qonun chiqaruvchi organ tomonidan qabul qilish jarayonida sharhlash amaliyotini joriy etish, bu esa, o‘z navbatida, huquq normalarini qo‘llash jarayonida turlicha talqin qilinishining oldini oladi (yuridik adabiyotlarda bunday sharhlash istiqbolli sharhlash deb ataladi). Bunda, norma ijodkorligi jarayonida maxsus tuzilgan komissiyalar yordamida qonun qabul qilish jarayonida ularning normalarini aniq maqsadni aniqlagan holatda sharhlash va ularni qonunni qabul qilish va e’lon qilish barobarida xalqqa va huquqni qo‘lovchi organlar e’tiboriga yetkazish muhim ahamiyat kasb etadi.

Mazkur sharh rasmiy kuchga ega bo‘lmasada, fuqarolar va davlat organlari tomonidan normalarni huquqni qo‘llash amaliyotida qo‘llashda noaniqliklar, ziddiyatli holatlar yuzaga kelishini oldini oladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Normativ-huquqiy hujjatlar to‘g‘risida”gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi, 20.04.2021-y., 03/21/682/0354-son // https://lex.uz/docs/-5378966;

2. O‘zbekiston Respublikasi Prezidentining 2018-yil 8-avgustdagi PF-5505-son “Norma ijodkorligi faoliyatini takomillashtirish konsepsiyasini tasdiqlash to‘g‘risida” Farmoni // Qonun hujjatlari ma’lumotlari milliy bazasi, 08.08.2018-y., 06/18/5505/1639-son // https://lex.uz/docs/-3858817;

3. Алексеев С.С. Государство и право: началний курс. – М.,1993.

4. Общая теория государства и права. Учебник / под ред. С.Ю. Наумова, А.С.Мордовса, Т.В.Касаевой. – Саратов: Саратовский социально-экономический институт (филиал) РЕЮ им. Г.В.Плеханова, 2018.

5. Kornev, A.V., 2016. Interpretation of law in the context of various methods of law cognition. Journal of Russian Law, 8, pp. 29–43.

6. Фаргиев И.А. Специальный закон о толковании права – веление времени! // Правосудие. 2020. Т. 2, № 2. С. 29–48. DOI: 10.37399/issn2686-9241.2020.2.29-48.

7. Alekseev, S.S., 2009. General theory of law. Moscow: Prospect.

8. Морозова Л.А. Теория государства и права. – М.: Российское юридическое образование, 2010.

9. Марченко, М.Н., 2015. Тенденции развития права в современном мире = [Trends in the development of law in the modern world]. Moscow: Prospekt.

10. Корнев, А.В., 2016. Interpretation of law in the context of various methods of law cognition. Журнал российского права = Journal of Russian Law.

11. Кравец, И.А., 2016. Конституционное правосудие: теория судебного конституционного права и практика судебного конституционного процесса = [Constitutional justice: theory of judicial constitutional law and practice of judicial constitutional process]. Moscow: Yusticinform.

---

[1] O‘zbekiston Respublikasi Prezidentining 08.08.2018 yildagi PF-5505-son “Norma ijodkorligi faoliyatini takomillashtirish konsepsiyasini tasdiqlash

to‘g‘risida” Farmoni // Qonun hujjatlari ma’lumotlari milliy bazasi, 08.08.2018-y., 06/18/5505/1639-son;
[2] Алексеев С.С. Государство и право: началний курс. – М.,1993.
[3] Общая теория государства и права. Учебник / под ред. С.Ю. Наумова, А.С.Мордовса, Т.В.Касаевой. – Саратов: Саратовский сотсиально-экономический институт (филиал) РЕЮ им. Г.В.Плеханова, 2018.
[4] Kornev, A.V., 2016. Interpretation of law in the context of various methods of law cognition. Journal of Russian Law, 8, pp. 29–43.
[5] Фаргиев И.А. Специальный закон о толковании права – веление времени! // Правосудие. 2020. Т. 2, № 2. С. 29–48. DOI: 10.37399/issn2686-9241.2020.2.29-48
[6] Alekseev, S.S., 2009. General theory of law. Moscow: Prospect.
[7] O‘zbekiston Respublikasining “Normativ-huquqiy hujjatlar to‘g‘risida”gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi, 20.04.2021-y., 03/21/682/0354-son