INNOVATIONS IN TECHNOLOGY AND SCIENCE EDUCATION
ISSN 2181-371X
https://sr-journals.org/index.php/ITSE

Kibermakonda sodir etilgan tovlamachilik jinoyati uchun jazo tayinlash va uni ijro etishning jinoiy-huquqiy masalalari

Abduraxmonov Abduazim Ravshanbek o‘g‘li
Toshkent davlat yuridik universiteti
Huquq va texnologiyalar sho‘basi Kiber huquq mutaxassisligi magistranti
abdurakhmonovabduazim3282@gmail.com

Abstract. This article analyzes the issues of sentencing and execution of punishment for extortion committed in cyberspace. The study is based on the Criminal Code, Criminal Procedure Code and Penal Enforcement Code of the Republic of Uzbekistan, decisions of the Plenum of the Supreme Court, national legislation on cybersecurity and digital evidence, as well as foreign and international legal sources. The article argues that sentencing for cyber extortion should not be limited to the amount of property demanded by the offender. Courts should also consider the digital method of committing the offence, the nature of the threat, the use of information resources, reputational harm, the psychological pressure placed on the victim, the risk to digital infrastructure, the role of digital evidence and the possibility of repeated cyber-offending. The article also examines the execution of punishment, especially the practical importance of probation control, restrictions related to digital conduct and rehabilitation measures aimed at preventing reoffending in the cyber environment.

Keywords: cyber extortion, sentencing, execution of punishment, probation, imprisonment, restriction of liberty, digital evidence, information resource, criminal liability, cybercrime prevention.

Аннотация. В статье анализируются вопросы назначения и исполнения наказания за вымогательство, совершённое в киберпространстве. Исследование основано на Уголовном кодексе, Уголовно-процессуальном кодексе и Уголовно-исполнительном кодексе Республики Узбекистан, постановлениях Пленума Верховного суда, национальном законодательстве о кибербезопасности и цифровых доказательствах, а также зарубежных и международных правовых источниках. В статье обосновывается, что при назначении наказания за кибервымогательство суд не должен ограничиваться только размером требуемого имущества. Необходимо учитывать цифровой способ совершения преступления, характер угрозы, использование информационных ресурсов, репутационный вред, психологическое давление на потерпевшего, риск для цифровой инфраструктуры, значение цифровых доказательств и возможность повторного совершения киберпреступлений. Также рассматриваются вопросы исполнения наказания, включая значение пробационного контроля, ограничений, связанных с цифровым поведением, и реабилитационных мер, направленных на предупреждение повторных преступлений в киберсреде.

Ключевые слова: кибервымогательство, назначение наказания, исполнение наказания, пробация, лишение свободы, ограничение свободы, цифровые доказательства, информационный ресурс, уголовная ответственность, профилактика киберпреступности.

Annotatsiya. Ushbu maqolada kibermakonda sodir etilgan tovlamachilik jinoyati uchun jazo tayinlash va uni ijro etish masalalari jinoiy-huquqiy jihatdan tahlil qilinadi. Tadqiqot O‘zbekiston Respublikasi Jinoyat kodeksi, Jinoyat-protsessual kodeksi, Jinoyat-ijroiya kodeksi, Oliy sud Plenumi qarorlari, kiberxavfsizlik va raqamli dalillarga oid milliy qonunchilik, shuningdek xorijiy va xalqaro huquqiy manbalar asosida olib borilgan. Maqolada kibertovlamachilik uchun jazo tayinlashda faqat talab qilingan pul yoki mulk miqdori bilan cheklanib qolmaslik, balki jinoyatning raqamli usuli, tahdidning xususiyati, axborot resursidan foydalanish, reputatsion zarar, jabrlanuvchiga ruhiy bosim, raqamli infratuzilmaga xavf, raqamli dalillarning ahamiyati va takroran kiberjinoyat sodir etish

ehtimoli ham hisobga olinishi zarurligi asoslantiriladi. Shuningdek, jazoni ijro etishda probatsiya nazorati, raqamli xulq-atvorga oid cheklovlar va qayta jinoyat sodir etishning oldini olishga qaratilgan tarbiyaviy-profilaktik choralar ahamiyati yoritiladi.

Kalit so‘zlar: kibertovlamachilik, jazo tayinlash, jazoni ijro etish, probatsiya, ozodlikdan mahrum qilish, ozodlikni cheklash, raqamli dalil, axborot resursi, jinoiy javobgarlik, kiberjinoyatlar profilaktikasi.

1. Introduction

Kibermakonda sodir etilgan tovlamachilik jinoyati uchun jazo tayinlash masalasi oddiy nazariy muammo emas, balki sud amaliyoti, raqamli dalillar, jabrlanuvchini himoya qilish va qayta jinoyat sodir etishning oldini olish bilan bog‘liq murakkab masaladir. An’anaviy tovlamachilikda jazo tayinlashda odatda tahdidning mazmuni, talab qilingan mulk miqdori, zo‘rlik ishlatilgan-ishlatilmagani, jabrlanuvchiga yetkazilgan zarar va aybdorning shaxsi baholanadi. Kibertovlamachilikda esa ushbu mezonlarga qo‘shimcha ravishda jinoyatning raqamli usuli, axborot resursiga ta’siri, shaxsiy ma’lumotlarning oshkor bo‘lish xavfi, kriptoaktivlar orqali to‘lov talab qilingani, elektron dalillar bilan isbotlanish darajasi va jinoyatchining texnik imkoniyatlari ham ahamiyat kasb etadi.

O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasi tovlamachilik uchun javobgarlikni belgilaydi. Mazkur moddaning amaldagi tahririda jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish bilan qo‘rqitish belgisi ham nazarda tutilgan.[1] Bu esa kibermakonda sodir etiladigan tovlamachilik holatlarini milliy jinoyat qonunchiligi doirasida baholash imkonini beradi. Biroq bunday qilmishlar uchun jazo tayinlashda faqat 165-modda sanksiyasini mexanik qo‘llash yetarli emas. Sud jinoyatning raqamli xususiyatini, jabrlanuvchiga yetkazilgan moddiy va nomoddiy zararlarni, jinoyatning davomiyligini, texnik tayyorgarlik darajasini va raqamli muhitda qayta jinoyat sodir etish xavfini ham hisobga olishi lozim.

Mazkur maqolaning maqsadi kibermakonda sodir etilgan tovlamachilik jinoyati uchun jazo tayinlash va jazoni ijro etish tartibining jinoyat-huquqiy hamda jinoyat-ijroiya jihatlarini chuqur tahlil qilishdan iborat. Tadqiqotda quyidagi savollarga javob izlanadi: kibertovlamachilik uchun jazo tayinlashda qanday mezonlar ustuvor bo‘lishi kerak; axborot resursiga qaratilgan tahdid jazo og‘irligiga qanday ta’sir qiladi; ozodlikni cheklash va ozodlikdan mahrum qilish jazolarini ijro etishda raqamli xulq-atvor ustidan nazorat qanday ahamiyat kasb etadi; xorijiy tajriba O‘zbekiston qonunchiligi uchun qanday xulosalar beradi?

2. Materials and Methods. Tadqiqot materiallari sifatida O‘zbekiston Respublikasi Jinoyat kodeksi, Jinoyat-protsessual kodeksi, Jinoyat-ijroiya kodeksi, “Kiberxavfsizlik to‘g‘risida”gi Qonun, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun, O‘zbekiston Respublikasi Oliy sudi Plenumining jazo tayinlash va dalillar maqbulligiga oid qarorlari, shuningdek xalqaro va xorijiy huquqiy manbalar o‘rganildi. Xalqaro manbalar sifatida Budapest konvensiyasi, elektron dalillar bo‘yicha xalqaro qo‘llanmalar, xorijiy huquqiy tajriba sifatida AQSh, Buyuk Britaniya va Germaniya qonunchiligidagi kiberjinoyatlar hamda kompyuter orqali tovlamachilikka oid yondashuvlar tahlil qilindi.

Maqolada formal-yuridik, qiyosiy-huquqiy, tizimli, mantiqiy va tahliliy metodlardan foydalanildi. Formal-yuridik metod yordamida Jinoyat kodeksining 165-moddasi va jazo tayinlashga oid umumiy qoidalar sharhlandi. Qiyosiy-huquqiy metod O‘zbekiston tajribasini AQSh, Buyuk Britaniya va Germaniya yondashuvlari bilan solishtirish imkonini berdi. Tizimli metod orqali jazo tayinlash masalasi faqat sanksiya doirasida emas, balki raqamli dalillar, jabrlanuvchi huquqlari, probatsiya nazorati va jazoni ijro etish samaradorligi bilan bog‘liq holda tahlil qilindi.

3. Results

Tadqiqot natijasida quyidagi asosiy natijalar shakllantirildi.

Birinchidan, kibertovlamachilik uchun jazo tayinlashda jinoyatning ijtimoiy xavflilik darajasi nafaqat talab qilingan mulk miqdori, balki tahdidning raqamli xususiyati, jabrlanuvchining axborot

[1] O‘zbekiston Respublikasi Jinoyat kodeksi, 165-modda. Tovlamachilik. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

resursiga ta’sir ko‘lami, shaxsiy ma’lumotlar bilan bog‘liq xavf va reputatsion zarar ehtimoli bilan belgilanadi.

Ikkinchidan, JK 165-moddasida nazarda tutilgan sanksiyalar doirasida jazo tanlashda sud JK 54-moddadagi umumiy mezonlardan kelib chiqishi kerak: qilmishning xususiyati, ijtimoiy xavflilik darajasi, sabab, zarar miqdori, aybdor shaxsi, yengillashtiruvchi va og‘irlashtiruvchi holatlar.[2] Kibertovlamachilikda ushbu mezonlar raqamli muhitga mos ravishda talqin qilinishi lozim.

Uchinchidan, kibertovlamachilikda raqamli dalillar jazo tayinlashga ham ta’sir qiladi. Elektron yozishmalar, server loglari, IP-manzillar, kriptohamyon manzillari, ma’lumotlarning shifrlanishi yoki tarqatilish xavfi jinoyatning real xavfini aniqlashga yordam beradi.[3]

To‘rtinchidan, jazoni ijro etish bosqichida ozodlikni cheklash probatsiya nazorati bilan uzviy bog‘liq. Kibertovlamachilik sodir etgan shaxsga nisbatan qo‘llanadigan cheklovlar uning raqamli muhitdagi xulq-atvorini nazorat qilish, yangi akkauntlar ochish orqali jabrlanuvchiga qayta bosim o‘tkazishining oldini olish va zararli raqamli faoliyatni cheklashga xizmat qilishi mumkin.[4]

Beshinchidan, ozodlikdan mahrum qilish jazosini ijro etishda ham kiberjinoyatchilar bilan ishlashda alohida yondashuv talab qilinadi. Chunki bunday shaxslar texnik bilimga ega bo‘lishi, muassasa ichida yoki tashqaridagi aloqalar orqali qayta raqamli jinoyat sodir etish xavfini yuzaga keltirishi mumkin. Shuning uchun jazoni ijro etish faqat izolyatsiya emas, balki qayta jinoyat sodir etish xavfini kamaytirishga qaratilgan tarbiyaviy, profilaktik va nazorat choralarini ham o‘z ichiga olishi kerak.

4. Discussion

4.1. Kibertovlamachilik uchun jazo tayinlashning umumiy huquqiy asoslari. Jazo tayinlash jinoyat-huquqiy javobgarlikning eng muhim bosqichlaridan biridir. Jinoyat kodeksining umumiy qoidalariga ko‘ra, jazo jinoyat sodir etishda aybli deb topilgan shaxsga nisbatan davlat nomidan sud hukmi bilan qo‘llanadigan majburlov chorasi hisoblanadi.[5] Jazoning maqsadi esa mahkumni axloqan tuzatish, uning jinoiy faoliyatini davom ettirishiga to‘sqinlik qilish va yangi jinoyatlar sodir etilishining oldini olishdan iborat. Shu sababli kibertovlamachilik uchun tayinlanadigan jazo ham faqat o‘ch olish yoki jazolash ma’nosida emas, balki tuzatish, ogohlantirish va raqamli muhitdagi xavfni kamaytirish vositasi sifatida tushunilishi kerak.

JK 165-moddasining birinchi qismida tovlamachilik uchun uch yildan besh yilgacha ozodlikni cheklash yoki uch yildan besh yilgacha ozodlikdan mahrum qilish nazarda tutilgan. Ikkinchi qismda takroran, xavfli retsidivist tomonidan, ko‘p miqdorda yoki bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilgan tovlamachilik uchun besh yildan o‘n yilgacha ozodlikdan mahrum qilish belgilanadi. Uchinchi qismda esa juda ko‘p miqdorda, o‘ta xavfli retsidivist tomonidan, uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilgan tovlamachilik uchun o‘n yildan o‘n besh yilgacha ozodlikdan mahrum qilish nazarda tutilgan.[6] Ushbu sanksiyalar kibertovlamachilikka nisbatan ham qo‘llanishi mumkin. Biroq kibermakondagi tovlamachilikni baholashda sud oddiy “pul talab qilindi — demak 165-modda” degan yondashuv bilan cheklanmasligi kerak. Masalan, jabrlanuvchining shaxsiy fotosuratlarini tarqatish bilan qo‘rqitib pul talab qilish bilan yirik korxonaning serverlarini bloklab, minglab mijozlar ma’lumotlarini oshkor qilish bilan tahdid qilishning ijtimoiy xavflilik darajasi bir xil emas. Har ikkisi tovlamachilik bo‘lishi mumkin, ammo jazo tayinlashda ularning xavfi, oqibati va jabrlanuvchiga ta’siri alohida baholanadi.

4.2. Jazo individuallashtirilishi va kibertovlamachilikning raqamli xususiyati. O‘zbekiston Respublikasi Jinoyat kodeksining 54-moddasi sud jazo tayinlashda sodir etilgan jinoyatning xususiyati

[2] O‘zbekiston Respublikasi Jinoyat kodeksi. 54-modda. Jazo tayinlashning umumiy asoslari. Qonunchilik ma’lumotlari milliy bazasi: lex.uz

[3] O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi. 204¹-modda “Elektron ma’lumotlar”, 204²-modda “Raqamli dalillar”, 205-modda va 208-modda. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

[4] O‘zbekiston Respublikasi Jinoyat-ijroiya kodeksi. Ozodlikni cheklash tariqasidagi jazoni ijro etishga oid normalar. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

[5] O‘zbekiston Respublikasi Jinoyat kodeksi. 42-modda. Jazo tushunchasi va maqsadlari. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

[6] O‘zbekiston Respublikasi Jinoyat kodeksi. 165-modda. Tovlamachilik sanksiyalari. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

va ijtimoiy xavflilik darajasini, qilmishning sababini, yetkazilgan zararning xususiyati va miqdorini, aybdorning shaxsini hamda yengillashtiruvchi va og‘irlashtiruvchi holatlarni hisobga olishini belgilaydi. Mazkur qoida kibertovlamachilik uchun ayniqsa muhim. Chunki bunday jinoyatlarda zarar ko‘pincha faqat pul miqdori bilan o‘lchanmaydi.

Kibertovlamachilikda jazo individuallashtirilayotganda quyidagi omillar alohida e’tiborga olinishi kerak.

Birinchidan, tahdidning shakli. Shaxsiy ma’lumotlarni tarqatish tahdidi, axborot tizimini bloklash tahdidi, serverdagi ma’lumotlarni o‘chirish tahdidi yoki korxona faoliyatini to‘xtatib qo‘yish tahdidi turlicha xavf tug‘diradi.

Ikkinchidan, jabrlanuvchi turi. Agar jinoyat oddiy fuqaro, voyaga yetmagan shaxs, davlat organi, bank, tibbiyot muassasasi yoki muhim axborot infratuzilmasi obyektiga nisbatan sodir etilgan bo‘lsa, ularning har birida ijtimoiy xavf darajasi farq qiladi.

Uchinchidan, texnik tayyorgarlik. Jinoyatchi tayyor soxta akkauntdan foydalanganmi yoki zararli dastur yaratganmi; u shunchaki yozishma orqali qo‘rqitganmi yoki serverga noqonuniy kirganmi; ma’lumotlarni nusxalaganmi yoki faqat tahdid qilganmi — bular jazoning og‘ir-yengilligiga ta’sir qilishi kerak.

To‘rtinchidan, zarar turi. Kibertovlamachilikda moddiy zarar bilan birga reputatsion zarar, ruhiy zarar, mijozlar ishonchining yo‘qolishi, tijorat siri oshkor bo‘lishi va tashkilot faoliyatining to‘xtashi kabi nomoddiy oqibatlar ham yuzaga kelishi mumkin.

Beshinchidan, jinoyatning davomiyligi. Bir martalik tahdid bilan uzoq davom etgan, bosqichma-bosqich kuchaytirilgan, turli akkauntlar orqali takrorlangan bosim bir xil baholanmasligi kerak.

Shu jihatdan, kibertovlamachilikda jazo tayinlash individual yondashuvni talab qiladi. Jinoyatning raqamli shakli uni avtomatik ravishda og‘irlashtiruvchi holatga aylantirmaydi, lekin raqamli vosita jinoyatning xavfini kuchaytirgan bo‘lsa, sud buni jazo tayinlashda hisobga olishi lozim.

4.3. Axborot resursiga qaratilgan tahdidning jazo tayinlashdagi ahamiyati. JK 165-moddasining hozirgi tahririda jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish bilan qo‘rqitish tovlamachilik dispozitsiyasida bevosita aks etadi.[7] Bu o‘zgarish kibertovlamachilik bo‘yicha jazo tayinlashda muhim ahamiyatga ega. Chunki endilikda axborot resursi faqat texnik obyekt sifatida emas, balki jabrlanuvchini majburiy holatga soluvchi bosim vositasi sifatida ham e’tirof etiladi.

Axborot resursiga qaratilgan tahdidning xavfi shundaki, u jabrlanuvchining kundalik hayoti yoki tashkilot faoliyati uchun muhim bo‘lgan ma’lumotlarga ta’sir qiladi. Masalan, korxonaning mijozlar bazasi, shartnomalari, moliyaviy hujjatlari, elektron yozishmalari yoki ishlab chiqarish jarayonlari boshqariladigan tizimlari bloklangan bo‘lsa, tovlamachilikning ta’siri faqat mulkiy talab doirasida emas, balki butun faoliyatning izdan chiqishi bilan baholanadi.

Bunday vaziyatda jazo tayinlashda “zarar yetkazildimi yoki faqat tahdid qilindimi?” degan savol bilan cheklanmaslik kerak. Ba’zan tahdidning o‘zi jabrlanuvchini jiddiy ruhiy va tashkiliy bosim ostiga qo‘yadi. Masalan, ma’lumotlar hali tarqatilmagan bo‘lsa ham, jinoyatchi ularning bir qismini ko‘rsatib, qolganini oshkor qilish bilan qo‘rqitsa, jabrlanuvchi real xavf ostida qoladi. Shuning uchun axborot resursiga qaratilgan tahdid jazo tayinlashda mustaqil baholanishi kerak bo‘lgan muhim omil hisoblanadi.

4.4. Raqamli dalillar va jazo tayinlash. Raqamli dalillar odatda jinoyatni isbotlash vositasi sifatida ko‘riladi. Biroq kibertovlamachilikda ular jazo tayinlashga ham bevosita ta’sir qiladi. Chunki raqamli dalillar orqali tahdidning real yoki soxta ekanligi, jinoyatning davomiyligi, jabrlanuvchiga qancha marta murojaat qilingani, ma’lumotlar haqiqatan ham egallanganmi yoki yo‘qmi, to‘lov qaysi yo‘l bilan talab qilingani va aybdorning texnik tayyorgarligi aniqlanadi.

Jinoyat-protsessual kodeksida elektron ma’lumotlar hamda raqamli dalillar bo‘yicha maxsus normalarning mavjudligi bu turdagi jinoyatlar uchun muhim protsessual asosdir. Masalan, chat

[7] O‘zbekiston Respublikasining 2024-yil 19-yanvardagi O‘RQ-899-son Qonuni bilan Jinoyat kodeksining 165-moddasiga kiritilgan o‘zgartirishlar. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

yozishmalari, elektron pochta sarlavhalari, IP-manzillar, server loglari, kriptohamyon manzillari, audio-video fayllar, skrinshotlar va metadata kabi ma'lumotlar nafaqat aybdorlikni, balki jazoning og'ir-yengilligiga ta'sir qiluvchi holatlarni ham ko'rsatishi mumkin.

Oliy sud Plenumining dalillar maqbulligiga oid qarorida dalillar qonuniy tartibda olingan, ishga aloqador va ishonchli bo'lishi kerakligi yuzasidan muhim yondashuvlar mavjud. Kibertovlamachilikda bu talablar alohida ahamiyatga ega. Agar raqamli dalil noto'g'ri olingan, asl manbasi aniqlanmagan yoki yaxlitligi saqlanmagan bo'lsa, sud tahdidning real darajasini noto'g'ri baholashi mumkin. Bu esa jazo tayinlashda nomutanosiblikka olib keladi.

Shu sababli kibertovlamachilik bo'yicha jazo tayinlash jarayonida raqamli dalillarni oddiy texnik ma'lumot sifatida emas, balki jinoyatning xususiyati, xavflilik darajasi va aybdorning qasdini ko'rsatuvchi muhim huquqiy manba sifatida baholash zarur.

4.5. Yengillashtiruvchi va og'irlashtiruvchi holatlarni baholash. Kibertovlamachilik uchun jazo tayinlashda yengillashtiruvchi va og'irlashtiruvchi holatlarni baholash alohida masala hisoblanadi. An'anaviy jinoyatlar uchun xos bo'lgan holatlar bu yerda ham qo'llanadi, biroq kibermakon sharoitida ularning mazmuni ayrim jihatdan o'zgaradi.

Masalan, aybdorning aybini tan olishi, jabrlanuvchidan kechirim so'rashi, talab qilingan pulni olmagan bo'lishi, yetkazilgan zararni qoplagani, ma'lumotlarni tarqatmaganligi yoki tizimga kirishni tiklab berganligi yengillashtiruvchi omil sifatida baholanishi mumkin. Lekin bu holatlarning o'zi har doim jazoning keskin yengillashishiga asos bo'lmasligi kerak. Chunki jabrlanuvchi allaqachon ruhiy bosim ostida qolgan, shaxsiy ma'lumotlar xavf ostida bo'lgan yoki tashkilot faoliyati izdan chiqqan bo'lishi mumkin. Og'irlashtiruvchi holatlar esa ko'p qirrali bo'lishi mumkin: jinoyatning bir guruh shaxslar tomonidan sodir etilishi, takroran sodir etilishi, uyushgan guruh manfaatlarini ko'zlashi, jabrlanuvchi sifatida voyaga yetmagan yoki himoyasiz shaxsning tanlanishi, davlat organi yoki muhim axborot infratuzilmasiga nisbatan hujum, zararli dasturdan foydalanish, ma'lumotlarni ommaga tarqatish yoki tarqatish uchun real harakatlar qilinishi, kriptoaktivlar orqali izni yashirishga urinish kabi holatlar jazo tayinlashda jiddiy baholanishi kerak.

Bu yerda muhim nuqta shundaki, har bir raqamli belgi avtomatik og'irlashtiruvchi holat deb olinmasligi kerak. Sud har bir holatning real xavfini, jabrlanuvchiga ta'sirini va aybdorning qasdini tahlil qilishi lozim. Masalan, shaxs faqat messenjer orqali pul talab qilgani bilan murakkab ransomware hujumini amalga oshirgan shaxs bir xil xavflilik darajasiga ega emas.

4.6. Xorijiy tajriba: jazo tayinlashda raqamli omillarni hisobga olish. Xorijiy davlatlar tajribasi kibertovlamachilik uchun jazo tayinlashda raqamli omillarni alohida baholash zarurligini ko'rsatadi. AQSh qonunchiligida kompyuterlar bilan bog'liq jinoyatlar, jumladan himoyalangan kompyuterga zarar yetkazish yoki kompyuter bilan bog'liq tahdid orqali pul talab qilish holatlari maxsus norma doirasida baholanadi.[8] Bu yondashuvda kompyuter tizimi jinoyatning oddiy vositasi emas, balki huquqiy baholashning muhim elementi sifatida ko'riladi.

Buyuk Britaniyada Computer Misuse Act 1990 orqali kompyuter materiallariga ruxsatsiz kirish, keyingi jinoyatni sodir etish niyati bilan kirish va tizimga zarar yetkazuvchi harakatlar alohida tartibga solinadi.[9] Bu tajriba shuni ko'rsatadiki, kibertovlamachilikka olib kelgan texnik bosqichlar ham jazo tayinlashda e'tibordan chetda qolmasligi kerak. Agar shaxs avval tizimga kirib, ma'lumotlarni o'g'irlab, keyin to'lov talab qilgan bo'lsa, jinoyatning tayyorgarlik va amalga oshirish bosqichlari birgalikda baholanishi zarur.

Germaniya Jinoyat kodeksida kompyuter ma'lumotlariga noqonuniy kirish, ma'lumotlarni ushlab qolish va bunday harakatlarga tayyorgarlik ko'rish bilan bog'liq normalarning mavjudligi kiberjinoyatlarning oldingi bosqichlarini ham huquqiy nazoratga olish zarurligini ko'rsatadi.[10] O'zbekiston uchun ushbu tajribalardan olinadigan xulosa shuki, kibertovlamachilikda jazo tayinlash faqat yakuniy pul talab qilishga emas, balki jinoyatning butun raqamli mexanizmiga asoslanishi kerak.

[8] United States Code. Title 18, §1030. Fraud and related activity in connection with computers
[9] Computer Misuse Act 1990. United Kingdom.
[10] German Criminal Code (Strafgesetzbuch — StGB). Sections 202a, 202b, 202c.

4.7. Jazoni ijro etishning umumiy tartibi. Jazo tayinlash sud hukmi bilan yakunlanmaydi. Uning ijro etilishi jinoyat-huquqiy ta’sirning amalda ishlashini ta’minlaydi. Jinoyat-ijroiya kodeksida jazoni ijro etish uchun sudning qonuniy kuchga kirgan hukmi, ajrimi yoki qarori asos bo‘lishi belgilangan.[11] Demak, kibertovlamachilik uchun tayinlangan jazo ham qonuniy kuchga kirgan sud qarori asosida ijro qilinadi.

Jinoyat-ijroiya qonunchiligining vazifasi faqat mahkumni jazolash emas, balki jazo ijrosini ta’minlash, mahkumlarni axloqan tuzatish, yangi jinoyatlarning oldini olish hamda mahkumlarning huquqlari va qonuniy manfaatlarini himoya qilishdan iborat.[12] Bu qoida kibertovlamachilik uchun juda muhim. Chunki bunday jinoyatni sodir etgan shaxsni faqat jamiyatdan ajratish bilan muammo hal bo‘lmaydi. U raqamli muhitda qanday harakat qilgan, qanday ko‘nikmalardan foydalangan, qayta jinoyat sodir etish xavfi bormi — bular jazoni ijro etish jarayonida ham inobatga olinishi kerak.

Agar shaxsga ozodlikni cheklash jazosi tayinlangan bo‘lsa, uning ijrosi probatsiya bo‘linmasi yoki sud belgilagan boshqa organ tomonidan nazorat qilinadi.[13] Kibertovlamachilik holatlarida probatsiya nazorati faqat mahkumning yashash joyidan chiqish-chiqmasligini kuzatish bilan cheklanmasligi kerak. Sud belgilagan taqiqlar va cheklovlar doirasida mahkumning jabrlanuvchi bilan qayta aloqa qilmasligi, yangi akkauntlar orqali bosim o‘tkazmasligi, ma’lum raqamli faoliyat bilan shug‘ullanmasligi yoki muayyan texnik vositalardan qonunga xilof tarzda foydalanmasligi ustidan nazorat masalasi ham dolzarb bo‘lishi mumkin.

4.8. Ozodlikni cheklash jazosini ijro etishda raqamli xulq-atvor nazorati. Ozodlikni cheklash sud tomonidan mahkumga nisbatan uy-joyini tark etishni butunlay taqiqlash yoki ma’lum vaqtlar doirasida cheklashdan iborat jazo hisoblanadi. Shu bilan birga, sud qo‘shimcha taqiqlarni ham yuklashi mumkin, jumladan muayyan joylarga bormaslik, ommaviy tadbirlarda ishtirok etmaslik yoki muayyan faoliyat bilan shug‘ullanmaslik kabi cheklovlar mavjud.[14] Kibertovlamachilik kontekstida “muayyan faoliyat bilan shug‘ullanmaslik” mazmuni raqamli muhitdagi ayrim xavfli faoliyatlarni cheklash masalasini ham kun tartibiga olib chiqadi.

Masalan, sud mahkumga jabrlanuvchi bilan internet orqali aloqa qilmaslik, ayrim platformalar orqali unga murojaat qilmaslik, jinoyatda ishlatilgan akkauntlar yoki qurilmalardan foydalanmaslik, zararli dasturlar bilan bog‘liq faoliyat yuritmaslik kabi cheklovlarni belgilashi mumkinmi, degan masala amaliy jihatdan muhim. Amaldagi qonunchilikda bunday cheklovlar har doim ham maxsus “kibercheklov” sifatida ko‘rsatilmagan bo‘lsa-da, ozodlikni cheklash mazmuni va sud belgilaydigan taqiqlar doirasida raqamli xavfga mos yondashuv ishlab chiqish zarur.

Bunday yondashuv jazoni ijro etishning profilaktik maqsadiga mos keladi. Agar shaxs kibertovlamachilikni ijtimoiy tarmoq, messenjer yoki boshqa onlayn platforma orqali sodir etgan bo‘lsa, uni faqat jismoniy harakatlar bo‘yicha nazorat qilish yetarli bo‘lmasligi mumkin. Uning raqamli muhitdagi xulq-atvori ham qayta jinoyat sodir etish xavfini kamaytirish nuqtai nazaridan muhimdir.

4.9. Ozodlikdan mahrum qilish jazosini ijro etish va kiberxavf. JK 165-moddasining og‘irroq qismlarida ozodlikdan mahrum qilish asosiy jazo sifatida nazarda tutilgan. Ozodlikdan mahrum qilish jazosining ijrosi jazoni ijro etish muassasalari tomonidan amalga oshiriladi. Kibertovlamachilik sodir etgan shaxsga nisbatan ozodlikdan mahrum qilish jazosini ijro etishda ikki jihatga e’tibor qaratish zarur.

Birinchi jihat — xavfsizlik. Agar mahkum texnik bilimga ega bo‘lsa, u jazoni o‘tash jarayonida ham boshqa shaxslar orqali, noqonuniy aloqa vositalari yoki tashqi aloqalar yordamida kiberjinoyatga aloqador harakatlarni davom ettirishga urinishi mumkin. Bu barcha mahkumlarga nisbatan umumiy shubha bilan qarash kerak degani emas, lekin kiberjinoyatlar bo‘yicha mahkumlar bilan ishlashda xavfni baholash alohida ahamiyatga ega.

---

[11] O‘zbekiston Respublikasi Jinoyat-ijroiya kodeksi. 5-modda. Jazoni ijro etish asosi. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.
[12] O‘zbekiston Respublikasi Jinoyat-ijroiya kodeksi. 2-modda. Jinoyat-ijroiya qonunchiligining vazifasi. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.
[13] O‘zbekiston Respublikasi Jinoyat-ijroiya kodeksi. 44¹-modda. Ozodlikni cheklash tariqasidagi jazoni ijro etish. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.
[14] O‘zbekiston Respublikasi Jinoyat kodeksi. 48¹-modda. Ozodlikni cheklashda qo‘shimcha taqiqlar va cheklovlar. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

Ikkinchi jihat — tuzatish va qayta ijtimoiylashuv. Kiberjinoyatchilikning oldini olish faqat taqiq bilan hal etilmaydi. Mahkumning texnik bilimini qonuniy faoliyatga yo‘naltirish, huquqiy ongini oshirish, raqamli etika va kiberxavfsizlik mas’uliyati bo‘yicha tarbiyaviy ishlar olib borish muhim. Aks holda, mahkum ozodlikka chiqqandan keyin ham o‘z bilimidan noqonuniy foydalanish xavfi saqlanib qoladi. Shu sababli kibertovlamachilik bo‘yicha jazoni ijro etish tizimida raqamli xavfga asoslangan individual yondashuv muhim. Bu yondashuv mahkumning texnik ko‘nikmalari, jinoyat sodir etishdagi roli, uyushgan guruh bilan aloqasi, jabrlanuvchi bilan qayta aloqa o‘rnatish xavfi va zararli raqamli faoliyatni davom ettirish imkoniyatlarini baholashni talab qiladi.

4.10. Jabrlanuvchini himoya qilish va zarar oqibatlarini bartaraf etish. Kibertovlamachilikda jazo tayinlash va ijro etish masalalarini jabrlanuvchini himoya qilishdan ajratib bo‘lmaydi. Chunki bu jinoyatda jabrlanuvchi ko‘pincha uzoq muddatli ruhiy bosim, shaxsiy ma’lumotlar xavfi, obro‘ga putur yetishi yoki biznes faoliyatining izdan chiqishi bilan yuzma-yuz keladi. Jazo tayinlashda sud yetkazilgan moddiy zarar bilan birga nomoddiy zarar va tahdidning jabrlanuvchi hayotiga real ta’sirini ham hisobga olishi zarur.

Jazoni ijro etish bosqichida ham jabrlanuvchini himoya qilish davom etishi kerak. Masalan, ozodlikni cheklash jazosini o‘tayotgan shaxs jabrlanuvchi bilan qayta aloqa qilmasligi, unga yangi akkauntlar orqali bosim o‘tkazmasligi yoki avvalgi ma’lumotlardan foydalanib qayta shantaj qilmasligi nazorat qilinishi kerak. Bu masala ayniqsa shaxsiy ma’lumotlar yoki intim materiallar orqali sodir etilgan kibertovlamachilikda muhim.

Bundan tashqari, ma’lumotlar tarqalgan yoki tarqalish xavfi mavjud bo‘lgan holatlarda jabrlanuvchining raqamli xavfsizligini tiklash bo‘yicha amaliy choralar ham muhim. Masalan, akkauntlarni tiklash, parollarni almashtirish, ikki bosqichli autentifikatsiyani yo‘lga qo‘yish, zararli dasturlarni bartaraf etish, oshkor qilingan ma’lumotlarni platformalardan olib tashlash bo‘yicha tegishli choralar ko‘rilishi kerak. Bu choralarning barchasi jinoyat-ijroiya qonunchiligida bevosita jazo sifatida ko‘rsatilmagan bo‘lishi mumkin, ammo jabrlanuvchini himoya qilish va jinoyat oqibatlarini kamaytirish nuqtai nazaridan muhimdir.

4.11. Mualliflik pozitsiyasi. Fikrimizcha, kibertovlamachilik uchun jazo tayinlashda uch pog‘onali yondashuv zarur.

Birinchi pog‘ona — klassik jinoyat-huquqiy baholash. Bunda JK 165-moddasi doirasida tovlamachilik belgilari, talab qilingan mulkiy manfaat, takroriylik, guruh bo‘lib sodir etilganlik, zarar miqdori va boshqa kvalifikatsion belgilar aniqlanadi.

Ikkinchi pog‘ona — raqamli xavfni baholash. Bunda jinoyatda axborot resursi qanday rol o‘ynagan, tahdid qanchalik real bo‘lgan, ma’lumotlar egallanganmi, tizim bloklanganmi, zararli dastur ishlatilganmi, jabrlanuvchining shaxsiy ma’lumotlari yoki obro‘siga xavf tug‘ilganmi, to‘lov kriptoaktivda talab qilinganmi, degan savollar tahlil qilinadi.

Uchinchi pog‘ona — jazoni ijro etish va profilaktika choralarini moslashtirish. Bunda mahkumning qayta raqamli jinoyat sodir etish xavfi, jabrlanuvchi bilan qayta aloqa qilish ehtimoli, texnik ko‘nikmalari va probatsiya nazorati doirasida unga nisbatan qo‘llanishi mumkin bo‘lgan cheklovlar baholanadi.

Shu yondashuv asosida aytish mumkinki, kibertovlamachilik uchun jazo tayinlashning asosiy maqsadi faqat shaxsni jazolash emas, balki jabrlanuvchini himoya qilish, raqamli muhitdagi xavfni kamaytirish, mahkumni tuzatish va kiberjinoyatchilikning oldini olishdan iborat bo‘lishi kerak.

5. Conclusion. Kibermakonda sodir etilgan tovlamachilik jinoyati uchun jazo tayinlash masalasi an’anaviy tovlamachilikka nisbatan murakkabroq yondashuvni talab qiladi. Chunki bunday jinoyatda tahdid raqamli vositalar orqali amalga oshiriladi, axborot resurslari bosim vositasiga aylanadi, jabrlanuvchiga moddiy zarar bilan birga reputatsion, ruhiy va tashkiliy zarar ham yetkaziladi, dalillar esa ko‘pincha elektron shaklda bo‘ladi. O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasida axborot resursiga qaratilgan tahdidlarning aks ettirilgani kibertovlamachilik uchun jazo tayinlashda muhim huquqiy asosdir. Biroq sud jazo tayinlashda faqat sanksiya doirasini emas, balki jinoyatning raqamli xususiyati, jabrlanuvchi holati, zarar miqdori va turi, aybdorning shaxsi, texnik tayyorgarlik darajasi, raqamli dalillar ishonchliligi va qayta jinoyat sodir etish xavfini ham hisobga olishi zarur.

Jazoni ijro etish bosqichida esa ozodlikni cheklash va ozodlikdan mahrum qilish jazolari kibertovlamachilikning xususiyatlariga mos tarzda amalga oshirilishi kerak. Ayniqsa probatsiya nazoratida raqamli xulq-atvor, jabrlanuvchi bilan qayta aloqa o‘rnatmaslik, zararli raqamli faoliyatni davom ettirmaslik va qayta jinoyat sodir etishning oldini olish masalalari muhim ahamiyat kasb etadi.

Shu asosda xulosa qilish mumkinki, kibertovlamachilik uchun jazo tayinlash va ijro etish tartibi nafaqat jinoyat-huquqiy repressiya, balki kiberxavfsizlik, jabrlanuvchini himoya qilish, raqamli dalillarni to‘g‘ri baholash va mahkumni raqamli jamiyatga qonuniy faoliyat subyekti sifatida qaytarishga qaratilgan kompleks huquqiy mexanizm sifatida tushunilishi lozim.

References

1. O‘zbekiston Respublikasi Jinoyat kodeksi. 1994-yil 22-sentabr. Qonunchilik ma’lumotlari milliy bazasi(lex.uz).
2. O‘zbekiston Respublikasi Jinoyat-ijroiya kodeksi. 1997-yil 25-aprel. Qonunchilik ma’lumotlari milliy bazasi.
3. O‘zbekiston Respublikasining 2024-yil 19-yanvardagi O‘RQ-899-son “O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi.
4. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi.
5. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi.
6. O‘zbekiston Respublikasi Oliy sudi Plenumining 2006-yil 3-fevraldagi 1-son “Sudlar tomonidan jinoyat uchun jazo tayinlash amaliyoti to‘g‘risida”gi qarori.
7. O‘zbekiston Respublikasi Oliy sudi Plenumining 2018-yil 24-avgustdagi 24-son “Dalillar maqbulligiga oid jinoyat-protsessual qonuni normalarini qo‘llashning ayrim masalalari to‘g‘risida”gi qarori.
8. Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.
9. Council of Europe. Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0.
10. United Nations Office on Drugs and Crime. Practical Guide for Requesting Electronic Evidence Across Borders.
11. United States Code. Title 18, §1030. Fraud and related activity in connection with computers.
12. Computer Misuse Act 1990. United Kingdom.
13. German Criminal Code (Strafgesetzbuch — StGB). Sections 202a, 202b, 202c.
14. National Cyber Security Centre; National Crime Agency. Ransomware, Extortion and the Cyber Crime Ecosystem. United Kingdom.
15. Cybersecurity and Infrastructure Security Agency. StopRansomware Guide: Ransomware and Data Extortion Prevention and Response.
16. Lubin A. The Law and Politics of Ransomware. Vanderbilt Journal of Transnational Law. 2022. Vol. 55. P. 1177–1216.
17. Paquet-Clouston M., Haslhofer B., Dupont B. Ransomware Payments in the Bitcoin Ecosystem. Journal of Cybersecurity. 2019. Vol. 5, Issue 1.
18. Laszka A., Farhang S., Grossklags J. On the Economics of Ransomware. Decision and Game Theory for Security. Springer, 2017. P. 397–417.
19. Bada M., Nurse J.R.C. Profiling the Cybercriminal: A Systematic Review of Research. IEEE Cyber Science Conference. 2021.