ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

KIBERTOVLAMACHILIK JINOYATI TUSHUNCHASINING NAZARIY-HUQUQIY TAHLILI, KELIB CHIQISH TARIXI VA MAZMUNI

Abduraxmonov Abduazim Ravshanbek o‘g‘li
Toshkent davlat yuridik universiteti
Kiber huquq mutaxassisligi magistranti

Annotatsiya. Ushbu maqolada kibertovlamachilik jinoyatining nazariy-huquqiy mazmuni, tarixiy shakllanishi va zamonaviy jinoyat-huquqiy tizimdagi o‘rni tahlil qilinadi. Mavzu O‘zbekiston Respublikasi Jinoyat kodeksi, Jinoyat-protsessual kodeksi, kiberxavfsizlikka oid milliy qonunchilik, Oliy sud Plenumi qarorlari, shuningdek AQSh, Buyuk Britaniya, Germaniya tajribasi hamda Budapest konvensiyasi yondashuvlari asosida o‘rganiladi. Maqolada kibertovlamachilik oddiy tovlamachilikning internetdagi shakli sifatida emas, balki mulk, axborot resursi, shaxsiy ma’lumotlar, raqamli obro‘ va iqtisodiy xavfsizlikka bir vaqtning o‘zida tajovuz qiluvchi kompleks jinoyat-huquqiy hodisa sifatida asoslantiriladi.

Kalit so‘zlar: kibertovlamachilik, tovlamachilik, kibermakon, axborot resursi, ransomware, raqamli dalil, elektron ma’lumot, shaxsiy ma’lumotlar, kiberxavfsizlik, jinoiy-huquqiy tahlil.

Abstract. This article analyzes the theoretical and legal essence, historical development, and contemporary criminal-law significance of cyber extortion. The study examines the issue on the basis of the Criminal Code and Criminal Procedure Code of the Republic of Uzbekistan, national legislation on cybersecurity, relevant decisions of the Plenum of the Supreme Court, as well as the experience of the United States, the United Kingdom, Germany, and the approaches reflected in the Budapest Convention on Cybercrime. The article substantiates that cyber extortion should not be viewed merely as an online form of traditional extortion, but rather as a complex criminal-law phenomenon that simultaneously infringes upon property, information resources, personal data, digital reputation, and economic security.

Keywords: cyber extortion, extortion, cyberspace, information resource, ransomware, digital evidence, electronic data, personal data, cybersecurity, criminal-law analysis.

Аннотация. В данной статье анализируются теоретико-правовая сущность, историческое развитие и современное уголовно-правовое значение кибервымогательства. Исследование проводится на основе Уголовного кодекса и Уголовно-процессуального кодекса Республики Узбекистан, национального законодательства в сфере кибербезопасности, соответствующих постановлений Пленума Верховного суда, а также опыта США, Великобритании, Германии и подходов, отражённых в Будапештской конвенции о киберпреступности. В статье обосновывается, что кибервымогательство не следует рассматривать лишь как интернет-форму традиционного вымогательства, а необходимо оценивать как комплексное уголовно-правовое явление, одновременно посягающее на собственность, информационные ресурсы, персональные данные, цифровую репутацию и экономическую безопасность.

Ключевые слова: кибервымогательство, вымогательство, киберпространство, информационный ресурс, ransomware, цифровые доказательства, электронные данные, персональные данные, кибербезопасность, уголовно-правовой анализ.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

Kirish

Raqamli texnologiyalar inson hayotining kundalik, iqtisodiy va ijtimoiy munosabatlariga chuqur kirib borgan sari jinoyatchilikning an'anaviy shakllari ham yangi vositalar orqali namoyon bo'la boshladi. Bir qarashda tovlamachilik qadimdan mavjud jinoyat: aybdor shaxs jabrlanuvchini qo'rqitadi, unga bosim o'tkazadi va shu yo'l bilan mulk yoki mulkiy manfaat talab qiladi. Biroq kibermakon ushbu jinoyatning tashqi ko'rinishini ham, xavflilik darajasini ham o'zgartirib yubordi. Endilikda tovlamachilik bevosita uchrashuv yoki jismoniy tahdid orqali emas, balki messenjer xabari, elektron pochta, soxta akkaunt, zararli dastur, shaxsiy ma'lumotlarni oshkor qilish tahdidi, kriptohamyon orqali to'lov talab qilish yoki korxona serverini bloklash shaklida sodir etilishi mumkin.

Shu sababli "kibertovlamachilik" atamasi amaliyotda tobora faol ishlatilayotgan bo'lsa-da, uni jinoyat-huquqiy jihatdan aniq tushuntirish zarurati saqlanib qolmoqda. O'zbekiston Respublikasi Jinoyat kodeksida "kibertovlamachilik" nomli alohida modda mavjud emas. Lekin JK 165-moddasining hozirgi tahriri tovlamachilik tarkibiga jabrlanuvchining axborot resursiga zarar yetkazish, uni egallab olish, o'zgartirish yoki to'sib qo'yish bilan qo'rqitish holatlarini ham qamrab oladi.[1] Mazkur holat shuni ko'rsatadiki, milliy qonunchilik tovlamachilikning raqamli muhitdagi ko'rinishlarini e'tibordan chetda qoldirmagan.

Shu bilan birga, masalani faqat JK 165-modda doirasida izohlash yetarli emas. Chunki kibertovlamachilik aksariyat hollarda boshqa jinoiy harakatlar bilan uzviy bog'liq bo'ladi. Masalan, aybdor avval jabrlanuvchining akkauntiga ruxsatsiz kiradi, shaxsiy yozishmalar yoki fotosuratlarni qo'lga kiritadi, kompyuter tizimiga zararli dastur yuboradi yoki ma'lumotlar bazasini shifrlaydi, shundan keyin pul talab qiladi. Bunday vaziyatda tovlamachilik jinoyati axborot texnologiyalari sohasidagi boshqa jinoyatlar bilan tutashadi. Demak, kibertovlamachilikni tahlil qilishda jinoyatning faqat yakuniy natijasiga emas, balki uning sodir etilish mexanizmiga ham e'tibor qaratish kerak.

Maqolaning asosiy maqsadi kibertovlamachilik tushunchasini nazariy-huquqiy jihatdan ochib berish, uning kelib chiqish sharoitlarini ko'rsatish, milliy va xorijiy qonunchilikdagi yondashuvlarni qiyosiy tahlil qilish hamda mazkur jinoyatning jinoyat-huquqiy mazmuni bo'yicha mustaqil xulosalar ishlab chiqishdan iborat.

1. Kibertovlamachilik tushunchasining nazariy-huquqiy mohiyati

Tovlamachilikning markaziy belgisi — jabrlanuvchini muayyan mulkiy harakatni sodir etishga majbur qilishdir. Bunda aybdor shaxs jabrlanuvchiga nisbatan qo'rqitish vositasidan foydalanadi. An'anaviy yondashuvda bu qo'rqitish zo'rlik ishlatish, mulkka zarar yetkazish, sharmanda qiluvchi ma'lumotlarni tarqatish yoki boshqa salbiy oqibatlar bilan bog'liq bo'lgan. Kibertovlamachilikda esa qo'rqitishning asosiy maydoni raqamli muhitga ko'chadi.

Kibertovlamachilikni quyidagicha ta'riflash mumkin: kibertovlamachilik — bu axborot-kommunikatsiya texnologiyalari, kompyuter tizimlari, elektron tarmoqlar, ijtimoiy platformalar yoki boshqa raqamli vositalardan foydalangan holda jabrlanuvchini mulk, mulkiy huquq, pul mablag'i, kriptoaktiv yoki boshqa mulkiy manfaat berishga majbur qilish maqsadida uning axborot resursi, shaxsiy ma'lumotlari, raqamli obro'si, mulki yoki qonuniy manfaatlariga zarar yetkazish bilan qo'rqitishda ifodalanadigan ijtimoiy xavfli qilmishdir.

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

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

Ushbu ta’rifda bir nechta muhim jihat bor. Birinchidan, kibertovlamachilikda jinoyatni sodir etish vositasi raqamli texnologiyalar bilan bog‘liq bo‘ladi. Ikkinchidan, aybdorning asosiy maqsadi mulkiy manfaat olishga qaratiladi. Uchinchidan, jabrlanuvchiga nisbatan tahdid real yoki hech bo‘lmaganda jabrlanuvchi uchun ishonarli ko‘rinishda bo‘lishi kerak. To‘rtinchidan, tajovuz faqat moddiy mulkka emas, balki axborot, shaxsiy hayot daxlsizligi, ishchanlik obro‘si va raqamli xavfsizlikka ham qaratiladi.

Aynan shu jihatlar kibertovlamachilikni oddiy “internet orqali pul talab qilish” holatidan ajratadi. Masalan, agar shaxs ijtimoiy tarmoqda boshqa shaxsni haqorat qilib, pul talab qilmasa, bu tovlamachilik bo‘lmasligi mumkin. Agar shaxs jabrlanuvchining shaxsiy fotosuratlarini tarqatish bilan qo‘rqitib pul talab qilsa, bunda tovlamachilikning zaruriy belgisi — mulkiy talab mavjud bo‘ladi. Agar shaxs korxona serverini bloklab, uni ochish evaziga to‘lov talab qilsa, bu holatda ham tovlamachilikning mazmuni mavjud, biroq jinoyatni sodir etish usuli axborot texnologiyalari bilan bog‘liq bo‘ladi.

Shu sababli kibertovlamachilik ikki qirrali jinoyat sifatida talqin qilinishi lozim. Bir tomondan, u mulkka qarshi jinoyatlar tizimida baholanadi. Ikkinchi tomondan, u axborot xavfsizligi, shaxsiy ma’lumotlar va raqamli dalillar bilan bog‘liq maxsus xususiyatlarga ega. Amaliyot uchun eng muhim masala shundaki, tergovchi yoki sud qilmishni baholayotganda faqat pul talab qilingan-qilinmaganini emas, balki tahdid qaysi raqamli vosita orqali amalga oshirilganini, ma’lumotlar qanday qo‘lga kiritilganini, jabrlanuvchiga qanday real zarar xavfi tug‘ilganini ham aniqlashi kerak.

2. Kibertovlamachilikning kelib chiqish tarixi va rivojlanish bosqichlari

Kibertovlamachilik mutlaqo yangi jinoyat emas; u an’anaviy tovlamachilikning raqamli muhitda o‘zgargan shaklidir. Tarixan tovlamachilik shaxsni zo‘rlik, qo‘rqitish yoki sharmanda qilish tahdidi ostida mulk berishga majbur qilish bilan bog‘liq bo‘lgan. Raqamli texnologiyalar rivojlangach, ayni shu jinoyat yangi imkoniyatlarga ega bo‘ldi: jinoyatchi jabrlanuvchidan uzoqda turib ham unga bosim o‘tkaza oladi, o‘z shaxsini yashirishi osonlashadi, bir vaqtning o‘zida ko‘plab shaxslarni nishonga olishi mumkin bo‘ladi.

Dastlabki bosqichlarda kibertovlamachilik ko‘proq shaxsiy yozishmalar, fotosuratlar, elektron pochta yoki akkauntlarga oid tahdidlar orqali ko‘rinish bergan. Keyinchalik zararli dasturlar, ayniqsa ransomware turidagi hujumlar keng tarqala boshladi. Ransomware mohiyatan shunday mexanizmga ega: jinoyatchi jabrlanuvchining kompyuter tizimiga zararli dastur joylashtiradi, fayllarni shifrlaydi yoki tizimga kirishni to‘sib qo‘yadi, keyin esa ma’lumotlarni tiklash evaziga pul talab qiladi.[2]

Ransomware bilan bog‘liq muhim jihat shundaki, bu yerda jabrlanuvchi ko‘pincha ikki tomonlama bosim ostida qoladi. Birinchi bosim — tizim yoki ma’lumotlardan foydalana olmaslik. Ikkinchi bosim — o‘g‘irlangan ma’lumotlarning ommaga tarqatilishi xavfi. Amaliyotda “double extortion” deb ataladigan usul aynan shuni anglatadi: jinoyatchi faqat ma’lumotlarni shifrlamaydi, balki ularni oldindan qo‘lga kiritib, oshkor qilish bilan ham tahdid qiladi. Ayrim hollarda bosim jabrlanuvchining mijozlari, hamkorlari yoki xodimlariga ham qaratiladi. Bu esa kibertovlamachilikni nafaqat shaxsga, balki butun tashkilot yoki biznes muhitiga qarshi xavfli jinoyatga aylantiradi.

[2] National Cyber Security Centre. Ransomware, extortion and the cyber crime ecosystem. United Kingdom NCSC.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

Kibertovlamachilik rivojiga kriptoaktivlar ham ta’sir ko‘rsatdi. To‘lovlarni an’anaviy bank tizimi orqali emas, kriptohamyonlar orqali talab qilish jinoyatchilarga tranzaksiyalarni yashirish yoki murakkablashtirish imkonini beradi. Albatta, blokcheyn tranzaksiyalari butunlay izsiz emas, ammo ularni aniqlash, bog‘lash va jinoyatchi shaxsini topish maxsus texnik bilim va xalqaro hamkorlikni talab qiladi. Shu bois kibertovlamachilikning tarixiy rivojlanishi oddiy shantajdan murakkab, transmilliy va texnik jihatdan tashkil etilgan jinoyatchilik shakliga qarab siljiganini ko‘rsatadi.

3. O‘zbekiston qonunchiligida kibertovlamachilikning huquqiy asoslari

O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasi kibertovlamachilikni baholashda asosiy norma hisoblanadi. Ushbu modda tovlamachilikni o‘zganing mulkini yoki mulkiy huquqini topshirishni, mulkiy manfaatlar berishni yoxud mulkiy yo‘sindagi harakatlar sodir etishni talab qilish sifatida tavsiflaydi. Muhimi, amaldagi tahrirda jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish bilan qo‘rqitish ham tovlamachilik dispozitsiyasida aks ettirilgan.[3]

Bu o‘zgarish kibertovlamachilik mavzusi uchun juda muhim. Chunki ilgari axborot resursiga qaratilgan tahdidni klassik tovlamachilik tarkibiga kiritish masalasida nazariy bahslar yuzaga kelishi mumkin edi. Hozir esa qonun chiqaruvchi axborot resursiga qaratilgan tahdidni bevosita tovlamachilikning bir ko‘rinishi sifatida tan olgan. Shu nuqtai nazardan, O‘zbekiston jinoyat qonunchiligi kibermakondagi tovlamachilikni baholash uchun muayyan asos yaratgan.

Biroq bu holat barcha muammolar hal bo‘ldi degani emas. Masalan, jabrlanuvchining elektron pochtasi buzib kirilgan, ma’lumotlari olingan, keyin esa pul talab qilingan bo‘lsa, qilmish faqat 165-modda bilan tugamaydi. Bunda kompyuter axborotidan qonunga xilof ravishda foydalanish, zararli dasturlardan foydalanish yoki shaxsiy ma’lumotlarni noqonuniy egallash kabi qo‘shimcha belgilar ham bo‘lishi mumkin.[4] Demak, kibertovlamachilikni kvalifikatsiya qilishda jinoyatning “talab qilish” qismi bilan birga unga olib kelgan texnik harakatlar ham alohida baholanishi kerak.

“Kiberxavfsizlik to‘g‘risida”gi Qonun ham mazkur mavzuda umumiy huquqiy fon vazifasini bajaradi. Ushbu Qonunning maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat bo‘lib, kiberxavfsizlik to‘g‘risidagi qonunchilik ushbu Qonun va boshqa qonunchilik hujjatlaridan tashkil topishi belgilangan.[5] Mazkur qonun bevosita jinoyat tarkibini yaratmasa-da, kibermakondagi tahdidlar davlat siyosati, muhim axborot infratuzilmasi va axborot tizimlarini himoya qilish bilan bog‘liq ekanini ko‘rsatadi.

Jinoyat-protsessual kodeksdagi so‘nggi o‘zgarishlar ham kibertovlamachilikni tergov qilishda katta ahamiyatga ega. JPKda elektron ma’lumotlar hamda raqamli dalillar alohida tushuncha sifatida belgilandi.[6] Raqamli dalillar jumlasiga elektron fayllar, audio va video yozuvlar, internetda saqlanayotgan ma’lumotlar hamda boshqa elektron ma’lumotlar kirishi mumkin. Bu kibertovlamachilik ishlarida chat yozishmalari, skrinshotlar, IP-manzillar, domen ma’lumotlari,

[3] 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.

[4] O‘zbekiston Respublikasi Jinoyat kodeksi. XX¹ bob. Axborot texnologiyalari sohasidagi jinoyatlar. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

[5] O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764-son, 15.04.2022. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

[6] 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.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

server loglari, kriptohamyon manzillari va metadata kabi ma'lumotlarni protsessual baholash imkoniyatini kengaytiradi.

O'zbekiston Respublikasi Oliy sudi Plenumining dalillar maqbulligiga oid qarorlari ham bu jarayonda ahamiyatli. Chunki kibertovlamachilikda mavjud dalilning o'zi yetarli emas; u qonuniy tartibda olingan, saqlangan va sudda tekshiriladigan bo'lishi kerak. Agar raqamli ma'lumotning yaxlitligi buzilgan, uning qayerdan olingani noma'lum yoki protsessual tartibga rioya qilinmagan bo'lsa, u sudda ishonchli dalil sifatida baholanishi qiyinlashadi.[7]

4. Xorijiy davlatlar qonunchiligida kibertovlamachilikka yondashuv

Qiyosiy tahlil shuni ko'rsatadiki, xorijiy davlatlar kibertovlamachilikni turli usullar bilan tartibga soladi. Ayrim davlatlar uni kompyuter jinoyatlari bilan bog'liq maxsus norma orqali ko'rsa, boshqalari tovlamachilik, ruxsatsiz kirish, shaxsiy ma'lumotlarni buzish va zararli dasturlar haqidagi normalarni birgalikda qo'llaydi.

AQSh qonunchiligida Computer Fraud and Abuse Act doirasidagi 18 U.S.C. §1030 normasi alohida ahamiyatga ega. Ushbu norma himoyalangan kompyuterga zarar yetkazish, undan ruxsatsiz axborot olish yoki kompyuter tizimi bilan bog'liq tahdidlar orqali pul yoki boshqa qiymat talab qilish holatlarini qamrab oladi.[8] Bu yondashuvning afzalligi shundaki, kompyuter bilan bog'liq tovlamachilik mustaqil xavf sifatida e'tirof etilgan. Bunday model huquqni qo'llovchi organlarga jinoyatning raqamli mexanizmini aniqroq baholash imkonini beradi.

Buyuk Britaniya tajribasida Computer Misuse Act 1990 muhim o'rin tutadi. Ushbu qonun kompyuter materiallariga ruxsatsiz kirish, keyingi jinoyatni sodir etish maqsadida ruxsatsiz kirish hamda kompyuter faoliyatiga zarar yetkazuvchi ruxsatsiz harakatlarni qamrab oladi.[9] Prokuratura amaliy izohlarida ruxsatsiz kirish keyinchalik boshqa jinoyat, jumladan shaxsni shantaj qilish maqsadida sodir etilishi mumkinligi ko'rsatiladi. Bu jihat kibertovlamachilikning tayyorgarlik bosqichini baholashda muhim.

Germaniya jinoyat qonunchiligida esa ma'lumotlarni yashirin egallash, ma'lumotlarni ushlab qolish, bunday harakatlarga tayyorgarlik ko'rish va phishing bilan bog'liq normalar mavjud.[10] Germaniya modeli shuni ko'rsatadiki, kibertovlamachilik faqat pul talab qilingan paytdan boshlanmaydi. Ba'zan jinoyatning xavfli bosqichi undan oldin — parollarni qo'lga kiritish, zararli dastur tayyorlash, tizimga kirish yoki shaxsiy ma'lumotlarni yig'ish jarayonida yuzaga keladi.

Ushbu davlatlar tajribasidan kelib chiqib, O'zbekiston uchun bir nechta xulosa chiqarish mumkin. Birinchidan, JK 165-moddasida axborot resursiga oid tahdid kiritilgani ijobiy holat. Ikkinchidan, kibertovlamachilikni amaliyotda to'g'ri baholash uchun 165-modda axborot texnologiyalari sohasidagi jinoyatlar haqidagi normalar bilan tizimli qo'llanishi kerak. Uchinchidan, tergov amaliyotida raqamli dalillarni yig'ish va saqlash bo'yicha aniq standartlar muhim ahamiyat kasb etadi. To'rtinchidan, qonunchilikni takomillashtirishda xorijiy davlatlar tajribasidan to'g'ridan-to'g'ri nusxa olish emas, balki milliy huquqiy tizimga mos xulosalar chiqarish maqsadga muvofiq.

---

[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] United States Code. Title 18, §1030. Fraud and related activity in connection with computers.

[9] Computer Misuse Act 1990. United Kingdom; Crown Prosecution Service. Computer Misuse Act prosecution guidance.

[10] German Criminal Code (Strafgesetzbuch — StGB). Sections 202a, 202b, 202c. Official English translation.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

5. Xalqaro hujjatlar doirasida kibertovlamachilik

Kibertovlamachilikning eng murakkab jihatlaridan biri uning transmilliy tabiatidir. Jinoyatchi bir davlatda, jabrlanuvchi ikkinchi davlatda, server uchinchi davlatda, to‘lov esa kriptoaktiv orqali boshqa yurisdiksiyaga o‘tgan bo‘lishi mumkin. Shu sababli bunday jinoyatlar faqat milliy qonunchilik bilan emas, xalqaro hamkorlik mexanizmlari bilan ham bog‘liq.

Bu borada Budapest konvensiyasi alohida o‘rin tutadi. U kiberjinoyatchilik va elektron dalillar bo‘yicha eng muhim xalqaro hujjatlardan biri sifatida e’tirof etiladi. Konvensiya davlatlarga kiberjinoyatlar bo‘yicha milliy qonunchilikni shakllantirishda yo‘riqnoma, xalqaro hamkorlikda esa amaliy mexanizm vazifasini bajaradi. Garchi unda “kibertovlamachilik” alohida jinoyat tarkibi sifatida batafsil ko‘rsatilmagan bo‘lsa-da, kompyuter tizimlariga noqonuniy kirish, ma’lumotlarga aralashish, tizim faoliyatiga zarar yetkazish va elektron dalillarni olish masalalari kibertovlamachilikka qarshi kurash uchun bevosita ahamiyatga ega.

Xalqaro hujjatlar tahlilidan ko‘rinadiki, kiberjinoyatlarga qarshi kurashning asosiy yo‘nalishi faqat jazo belgilash bilan cheklanmaydi. Unda dalillarni tezkor saqlab qolish, xizmat ko‘rsatuvchi provayderlardan ma’lumot olish, xalqaro so‘rovlarni yuborish, mutaxassislar hamkorligini kuchaytirish va jabrlanuvchilarni himoya qilish masalalari ham muhim. Kibertovlamachilikda bu ayniqsa zarur, chunki raqamli dalillar tez o‘chirilishi, o‘zgartirilishi yoki boshqa davlat hududida saqlanishi mumkin.

Shu nuqtai nazardan, O‘zbekistonning milliy qonunchiligi xalqaro standartlar bilan uyg‘unlashib borishi kerak. Bu degani xorijiy hujjatlarni ko‘r-ko‘rona ko‘chirish emas. Aksincha, milliy jinoyat-huquqiy tizimning o‘ziga xosligi saqlangan holda, kiberjinoyatlar bo‘yicha xalqaro hamkorlik, elektron dalillar, raqamli tergov va tezkor ma’lumot almashish mexanizmlari yanada takomillashtirilishi lozim.

6. Kibertovlamachilikning mazmuniy belgilari

Kibertovlamachilikning jinoyat-huquqiy mazmunini aniqlashda bir nechta belgi alohida ajratilishi kerak.

Birinchi belgi — raqamli vositaning mavjudligi. Jinoyat internet, kompyuter tizimi, telefon, ijtimoiy tarmoq, messenjer, elektron pochta, zararli dastur yoki boshqa axborot texnologiyasi orqali sodir etiladi. Biroq faqat raqamli vositadan foydalanishning o‘zi kibertovlamachilik uchun yetarli emas. Masalan, shaxs telefon orqali pul so‘rashi hali tovlamachilik emas. Tovlamachilik uchun qo‘rqitish va mulkiy talab birgalikda mavjud bo‘lishi kerak.

Ikkinchi belgi — tahdid. Kibertovlamachilikda tahdid shaxsiy ma’lumotlarni oshkor qilish, fotosurat yoki videoni tarqatish, akkauntni qaytarmaslik, serverni bloklash, ma’lumotlar bazasini o‘chirish, korxona faoliyatini izdan chiqarish yoki shaxsning obro‘siga putur yetkazish shaklida namoyon bo‘lishi mumkin. Bu yerda tahdidning albatta amalga oshirilgan bo‘lishi shart emas; jabrlanuvchini mulkiy harakatga majbur qiladigan real xavf tug‘dirishi yetarli.

Uchinchi belgi — mulkiy talab. Aybdor pul, kriptoaktiv, mulkiy huquq, xizmat yoki boshqa manfaat talab qilishi mumkin. Agar talab mulkiy xususiyatga ega bo‘lmasa, qilmish boshqa jinoyat tarkiblari doirasida baholanishi mumkin. Shu sababli kibertovlamachilikni shaxsiy hayot daxlsizligini buzish, tuhmat, haqorat yoki axborotdan ruxsatsiz foydalanishdan farqlashda aynan mulkiy talab hal qiluvchi mezonlardan biridir.

To‘rtinchi belgi — jabrlanuvchini majburiy holatga solish. Kibertovlamachilikda jabrlanuvchi ko‘pincha “tanlovsiz” holatga tushadi: to‘lov qilmasa, ma’lumotlari tarqalishi, biznesi to‘xtashi,

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

oilaviy yoki ishchanlik obro‘siga putur yetishi mumkin. Bu holat jinoyatning ruhiy bosim xususiyatini kuchaytiradi.

Beshinchi belgi — raqamli dalillar bilan isbotlanish zarurati. An’anaviy tovlamachilikda guvoh ko‘rsatmalari, audioyozuv, pul berish jarayoni yoki tezkor tadbir muhim bo‘lsa, kibertovlamachilikda chat yozishmalari, IP-manzillar, qurilma identifikatorlari, server loglari, elektron fayllar, skrinshotlar, kriptohamyon manzillari va boshqa raqamli izlar alohida ahamiyatga ega bo‘ladi. Bunday dalillarni to‘g‘ri olish va saqlash jinoyatni isbotlashning markaziy sharti hisoblanadi.

7. Mualliflik pozitsiyasi va nazariy xulosa

Fikrimizcha, kibertovlamachilikni faqat klassik tovlamachilikning internetdagi shakli sifatida baholash tor yondashuv bo‘ladi. Chunki bunday yondashuv jinoyatning axborot xavfsizligi, shaxsiy ma’lumotlar, raqamli dalillar, transmilliylik va kriptoaktivlar bilan bog‘liq xususiyatlarini yetarli ochib bermaydi. Shu bilan birga, kibertovlamachilikni faqat texnik kiberhujum sifatida talqin qilish ham to‘g‘ri emas. Chunki uning asosida baribir jabrlanuvchidan mulkiy manfaat talab qilish, ya’ni tovlamachilikka xos asosiy belgi mavjud.

Shu bois kibertovlamachilikni kompleks jinoyat-huquqiy hodisa sifatida ko‘rish maqsadga muvofiq. Unda asosiy tarkib tovlamachilik bo‘lsa-da, jinoyatni sodir etish usuli axborot texnologiyalari bilan bog‘liq bo‘ladi. Bunday yondashuv amaliyotda ham foydali: sud-tergov organlari qilmishni baholashda bir tomondan JK 165-moddasidagi tovlamachilik belgilari, ikkinchi tomondan axborot texnologiyalari sohasidagi jinoyatlarga oid belgilarni birgalikda tekshiradi.

Milliy qonunchilikning hozirgi rivojlanish bosqichi kibertovlamachilikni baholash uchun muhim asos yaratgan. Ayniqsa JK 165-moddasiga axborot resursiga oid tahdidlarning kiritilishi va JPKda raqamli dalillarning alohida belgilanishi ijobiy o‘zgarishdir. Biroq amaliyotda ushbu normalarning samarali ishlashi uchun tergov organlari, sudlar, ekspertlar va kiberxavfsizlik mutaxassislari o‘rtasidagi hamkorlik yanada kuchaytirilishi kerak.

Kelgusida kibertovlamachilikni kvalifikatsiya qilish bo‘yicha amaliy tavsiyalar ishlab chiqilishi, raqamli dalillarni olish va saqlash tartibiga oid standartlar kengroq tushuntirilishi, shuningdek xorijiy tajribadan kelib chiqib axborot resursiga qaratilgan tovlamachilikning og‘irlashtiruvchi belgilarini yanada aniqlashtirish masalasi muhokama qilinishi mumkin.

Xulosa

Kibertovlamachilik jinoyati zamonaviy jinoyatchilikning eng murakkab va ijtimoiy xavfli ko‘rinishlaridan biridir. Uning nazariy-huquqiy mazmuni shundan iboratki, klassik tovlamachilikka xos bo‘lgan qo‘rqitish va mulkiy talab belgisi kibermakon imkoniyatlari bilan qo‘shilib ketadi. Natijada jinoyatning sodir etilish usuli, jabrlanuvchiga ta’sir ko‘lami va dalillar tizimi keskin o‘zgaradi.

O‘zbekiston jinoyat qonunchiligida kibertovlamachilik alohida modda sifatida ajratilmagan bo‘lsa-da, JK 165-moddasining amaldagi tahriri uni baholash uchun asos beradi. Ayniqsa jabrlanuvchining axborot resursiga oid tahdidlarning tovlamachilik tarkibiga kiritilgani milliy qonunchilikning raqamli jinoyatlarga moslashayotganidan dalolat beradi. Shu bilan birga, bunday qilmishlar ko‘pincha axborot texnologiyalari sohasidagi boshqa jinoyatlar bilan birga sodir etilishi sababli ularni kompleks kvalifikatsiya qilish talab etiladi.

Xorijiy davlatlar tajribasi shuni ko‘rsatadiki, AQSh, Buyuk Britaniya va Germaniya kabi

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

davlatlarda kompyuter tizimlariga ruxsatsiz kirish, zararli dasturlardan foydalanish, ma’lumotlarni egallash va tovlamachilik maqsadida tahdid qilish holatlari turli huquqiy mexanizmlar orqali baholanadi. Xalqaro miqyosda esa Budapest konvensiyasi kiberjinoyatlar va elektron dalillar bo‘yicha umumiy yo‘nalish beruvchi muhim hujjat sifatida namoyon bo‘ladi.

Shu asosda aytish mumkinki, kibertovlamachilikni oddiy tovlamachilikdan farqlovchi asosiy mezon — jinoyatning raqamli vositalar orqali sodir etilishi emas, balki raqamli vositalar jinoyatning qo‘rqitish, majburlash, zarar yetkazish va dalillanish mexanizmini tubdan o‘zgartirishidir. Shuning uchun kibertovlamachilikka qarshi kurashda jinoyat-huquqiy normalar, kiberxavfsizlik choralari, raqamli dalillar protsessual tartibi va xalqaro hamkorlik birgalikda qo‘llanishi zarur.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

I. Normativ-huquqiy hujjatlar

1. O‘zbekiston Respublikasi Konstitutsiyasi. — Qonunchilik ma’lumotlari milliy bazasi.

2. O‘zbekiston Respublikasi Jinoyat kodeksi. 1994-yil 22-sentabr. — Qonunchilik ma’lumotlari milliy bazasi.

3. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi. 1994-yil 22-sentabr. — Qonunchilik ma’lumotlari milliy bazasi.

4. 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.

5. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni. — Qonunchilik ma’lumotlari milliy bazasi.

6. 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.

II. Xalqaro hujjatlar va xalqaro-amaliy qo‘llanmalar

1. Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.
2. Council of Europe. Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0.
3. United Nations Office on Drugs and Crime. Practical Guide for Requesting Electronic Evidence Across Borders.
4. United Nations Office on Drugs and Crime. Cybercrime Module 4: Introduction to Digital Forensics and Digital Evidence.

III. Xorijiy davlatlar qonunchiligi

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

IV. Ilmiy va amaliy manbalar

1. Lubin A. The Law and Politics of Ransomware // Vanderbilt Journal of Transnational Law. — 2022. — Vol. 55. — P. 1177–1216.
2. Vasoya S., Bhavsar K., Patel N. A Systematic Literature Review on Ransomware Attacks. — arXiv:2212.04063, 2022.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

3. Pattnaik N., Nurse J.R.C., Turner S., Mott G., MacColl J., Huesch P., Sullivan J. It's More Than Just Money: The Real-World Harms from Ransomware Attacks // Human Aspects of Information Security and Assurance. — 2023. — P. 261–274.
4. Laszka A., Farhang S., Grossklags J. On the Economics of Ransomware. — arXiv:1707.06247, 2017.
5. Allah Rakha N. Cybercrime and the Law: Addressing the Challenges of Digital Forensics // Mexican Law Review. — 2024.
6. Akbarov A.A. Elektron pochta dalillari va raqamli kriminalistika masalalari // Ilmiy-amaliy maqola.
7. Muminov B. Kiberjinoyatlar tendensiyasi va ularga qarshi kurashish masalalari // Ijtimoiy-huquqiy tadqiqotlar.
8. Rustambayev M.X. O'zbekiston Respublikasi jinoyat huquqi kursi. Maxsus qism. — Toshkent: TDYU
9. Qodirov R.Q., Abdurasulova Q.R. Jinoyat huquqi. Maxsus qism. — Toshkent
10. Inlibrary.uz platformasidagi kiberjinoyatlar va raqamli dalillarga oid ilmiy maqolalar.