Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

KIBERTOVLAMACHILIK JINOYATLARINING TASNIFI VA JAVOBGARLIK BELGILASHNING IJTIMOIY-HUQUQIY ZARURIYATI

Abduraxmonov Abduazim Ravshanbek o‘g‘li

Toshkent davlat yuridik universiteti

Kiber huquq mutaxassisligi magistranti

Doi: https://doi.org/10.5281/zenodo.20603219

Annotatsiya: Ushbu maqolada kibertovlamachilik jinoyatlarining tasnifi hamda bunday qilmishlarga nisbatan jinoiy javobgarlik belgilashning ijtimoiy-huquqiy zaruriyati tahlil qilinadi. Tadqiqotda kibertovlamachilikning ransomware, shaxsiy ma’lumotlar orqali shantaj, akkauntni egallab olish, kriptoaktivlar orqali to‘lov talab qilish, tashkilotlarning axborot tizimlarini bloklash va raqamli obro‘ga bosim o‘tkazish kabi shakllari alohida ko‘rib chiqiladi. Maqolada O‘zbekiston Respublikasi jinoyat qonunchiligi, jinoyat-protsessual normalar, kiberxavfsizlikka oid milliy qonunchilik, xalqaro hujjatlar va xorijiy davlatlar tajribasi asosida kibertovlamachilikning ijtimoiy xavflilik darajasi ochib beriladi. Mualliflik pozitsiyasi sifatida kibertovlamachilikni faqat mulkka qarshi jinoyat sifatida emas, balki axborot xavfsizligi, shaxsiy hayot daxlsizligi, raqamli iqtisodiyot va jamiyatning raqamli muhitga bo‘lgan ishonchiga zarar yetkazuvchi kompleks jinoyat-huquqiy hodisa sifatida baholash taklif qilinadi.

Kalit so‘zlar: kibertovlamachilik, tovlamachilik, tasnif, ransomware, sextortion, kriptoaktiv, raqamli dalil, axborot resursi, jinoiy javobgarlik, kiberxavfsizlik.

Abstract: This article analyzes the classification of cyber extortion offences and the socio-legal necessity of establishing criminal liability for such acts. The study examines the main forms of cyber extortion, including ransomware, blackmail through personal data, account takeover, demands for payment through crypto-assets, blocking of organizational information systems, and pressure on digital reputation. Based on the criminal legislation and criminal procedural rules of the Republic of Uzbekistan, national cybersecurity legislation, international instruments, and foreign legal experience, the article reveals the public danger of cyber extortion. The author argues that cyber extortion should not be treated only as a property-related offence, but also as a complex criminal-law phenomenon affecting information security, privacy, the digital economy, and public trust in cyberspace.

Keywords: cyber extortion, extortion, classification, ransomware, sextortion, crypto-assets, digital evidence, information resource, criminal liability, cybersecurity.

Аннотация: В данной статье анализируются классификация преступлений, связанных с кибервымогательством, а также социально-правовая необходимость установления уголовной ответственности за такие деяния. В исследовании рассматриваются основные формы кибервымогательства, включая ransomware, шантаж с использованием персональных данных, захват аккаунтов, требование платежей через криптоактивы, блокирование информационных систем организаций и давление на цифровую репутацию. На основе уголовного и уголовно-процессуального законодательства Республики Узбекистан, национального законодательства в сфере кибербезопасности, международных документов и зарубежного опыта раскрывается общественная опасность кибервымогательства. Автор обосновывает, что кибервымогательство следует рассматривать не только как преступление против собственности, но и как комплексное уголовно-правовое явление, посягающее на информационную безопасность, неприкосновенность частной жизни, цифровую экономику и доверие общества к киберпространству.

Ключевые слова: кибервымогательство, вымогательство, классификация, ransomware, sextortion, криптоактивы, цифровые доказательства, информационный ресурс, уголовная ответственность, кибербезопасность.

Kirish

Kibertovlamachilik jinoyatlarini ilmiy tahlil qilishda bir masalani aniq belgilab olishimiz zarur: ushbu qilmish oddiy tovlamachilikning faqat internet orqali sodir etiladigan ko‘rinishi emas. Albatta, uning markazida tovlamachilikka xos bo‘lgan “qo‘rqitish orqali mulkiy manfaat talab qilish” belgisi turadi. Biroq kibermakon mazkur jinoyatning sodir etilish usulini, jabrlanuvchiga ta’sir ko‘lamini, dalillar tizimini va xavflilik darajasini sezilarli darajada o‘zgartiradi. Shu sababli kibertovlamachilikni tasniflash va unga nisbatan jinoiy javobgarlik belgilash zaruriyatini alohida o‘rganish mavzuning nazariy hamda amaliy qiymatini oshiradi.

O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasida tovlamachilik uchun javobgarlik belgilangan bo‘lib, ushbu norma kibermakonda sodir etiladigan tovlamachilik holatlarini baholashda asosiy jinoyat-huquqiy tayanch hisoblanadi.[1] Ayniqsa, so‘nggi yillarda mazkur modda dispozitsiyasida jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish bilan qo‘rqitish kabi belgilar aks etgani kibertovlamachilikni milliy qonunchilik doirasida tahlil qilish imkonini kengaytirdi.[2] Bu o‘zgarish shuni ko‘rsatadiki, qonun chiqaruvchi tovlamachilikning raqamli muhitdagi xavfini e’tirof etgan.

Shu bilan birga, kibertovlamachilikni to‘g‘ri tushunish uchun uni faqat JK 165-modda bilan cheklab bo‘lmaydi. Bunday jinoyatlar, odatda, kompyuter tizimiga ruxsatsiz kirish, zararli dasturdan foydalanish, shaxsiy ma’lumotlarni noqonuniy egallash, elektron yozishmalarni tarqatish bilan qo‘rqitish, kriptoaktivlar orqali to‘lov talab qilish kabi murakkab harakatlar bilan bog‘liq bo‘ladi. Bu esa jinoyatni kvalifikatsiya qilishda jinoyat huquqi, jinoyat-protsessual huquq, raqamli kriminalistika va kiberxavfsizlik sohalarining o‘zaro bog‘liq tahlilini talab qiladi.

Mazkur maqolada kibertovlamachilikning asosiy shakllari tasniflanadi, ularning ijtimoiy xavfi ochib beriladi, shuningdek, bunday qilmishlarga nisbatan jinoiy javobgarlik belgilash nima uchun zarurligi milliy qonunchilik, xalqaro hujjatlar va xorijiy tajriba asosida tahlil qilinadi.

1. Kibertovlamachilikni jinoyatini tasniflashning nazariy va amaliy ahamiyati

Jinoyatlarni tasniflash ularning mazmunini soddalashtirish uchun emas, balki huquqiy baholashni aniqlashtirish uchun zarur. Ayniqsa kibertovlamachilik kabi murakkab qilmishda tasniflash masalasi amaliy ahamiyatga ega. Chunki har bir shaklda jinoyatchining harakat usuli, qo‘rqitish vositasi, jabrlanuvchiga yetkaziladigan zarar va dalillar turi turlicha bo‘ladi.

Kibertovlamachilikni birinchi navbatda sodir etish usuliga ko‘ra tasniflash mumkin. Bu mezon bo‘yicha ransomware orqali tovlamachilik, shaxsiy ma’lumotlar bilan shantaj qilish, akkauntni egallab olib pul talab qilish, zararli dastur orqali tizimni bloklash, DDoS hujumi bilan qo‘rqitish, kriptoaktivlar orqali to‘lov talab qilish kabi shakllar ajratiladi.

Ikkinchi mezon — jabrlanuvchi subyekti. Kibertovlamachilik jismoniy shaxsga, tadbirkorlik subyektiga, bank-moliya tashkilotiga, davlat organiga, ta’lim yoki tibbiyot muassasasiga, shuningdek muhim axborot infratuzilmasi obyektlariga nisbatan sodir etilishi mumkin. Jabrlanuvchi kim ekaniga qarab jinoyatning ijtimoiy xavflilik darajasi ham o‘zgaradi. Masalan, oddiy foydalanuvchining shaxsiy

[1] O‘zbekiston Respublikasi Jinoyat kodeksi. 165-modda. Tovlamachilik. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.
[2] 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.

akkaunti egallab olinishi bilan tibbiyot muassasasi serverining bloklanishi bir xil oqibat keltirib chiqarmaydi.

Uchinchi mezon — talab qilinayotgan manfaat turi. Aybdor naqd pul, bank o‘tkazmasi, elektron pul, kriptoaktiv, xizmat ko‘rsatish, raqamli aktiv yoki boshqa mulkiy manfaat talab qilishi mumkin. Mazkur belgi jinoyatni boshqa raqamli huquqbuzarliklardan farqlashda muhimdir. Chunki tovlamachilik uchun qo‘rqitishning o‘zi yetarli emas, unda mulkiy talab ham bo‘lishi kerak.

To‘rtinchi mezon — dalillar shakli. Kibertovlamachilik odatda elektron yozishmalar, IP-manzillar, login tarixi, server loglari, elektron fayllar, skrinshotlar, kriptohamyon manzillari va boshqa raqamli izlar orqali isbotlanadi. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksida elektron ma’lumotlar va raqamli dalillar alohida tartibga solingani bu turdagi jinoyatlarni isbotlashda muhim huquqiy asos vazifasini bajaradi.

Shu jihatdan kibertovlamachilikni tasniflash nazariy jihatdan jinoyatning mazmunini ochib bersa, amaliy jihatdan tergovchi, prokuror va sudga qilmishning huquqiy bahosini aniqlashda yordam beradi.

2. Ransomware orqali sodir etiladigan kibertovlamachilik

Kibertovlamachilikning eng xavfli shakllaridan biri ransomware orqali sodir etiladigan qilmishlardir. Ransomware — zararli dastur bo‘lib, u jabrlanuvchining kompyuter tizimidagi fayllarni shifrlaydi yoki tizimga kirishni bloklaydi. Shundan keyin jinoyatchi ma’lumotlarni tiklash yoki tizimni qayta ochish evaziga to‘lov talab qiladi.[3]

Bu shaklning xavfi shundaki, u faqat alohida foydalanuvchiga emas, balki butun tashkilot faoliyatiga ta’sir qilishi mumkin. Masalan, tibbiyot muassasasi axborot tizimlari bloklansa, bemorlar haqidagi ma’lumotlardan foydalanish qiyinlashadi. Bank yoki to‘lov tizimiga nisbatan bunday hujum sodir etilsa, moliyaviy operatsiyalar izdan chiqishi mumkin. Davlat organi serverlari bloklansa, aholiga ko‘rsatiladigan elektron xizmatlar to‘xtab qoladi. Demak, ransomware orqali sodir etilgan kibertovlamachilikda zarar faqat talab qilingan pul miqdori bilan o‘lchanmaydi.

Ransomware jinoyatlari ichida ikki tomonlama tovlamachilik — double extortion alohida e’tiborga loyiq. Bunday holatda jinoyatchi ma’lumotlarni nafaqat shifrlaydi, balki ularni oldindan o‘g‘irlaydi va to‘lov qilinmasa ommaga tarqatish bilan qo‘rqitadi. Bu usul jabrlanuvchini ikki tomonlama bosim ostiga oladi: bir tomondan, tizim ishlamaydi, ikkinchi tomondan, maxfiy ma’lumotlar oshkor bo‘lishi mumkin.

Bunday holatlarda profilaktika va javob choralari ham kompleks bo‘lishi kerak. Faqat zaxira nusxa yaratish yetarli emas, chunki ma’lumotlar allaqachon jinoyatchining qo‘lida bo‘lishi mumkin. Shu bois ransomware va data extortion holatlariga qarshi kurashda texnik himoya, huquqiy javobgarlik va dalillarni tezkor saqlab qolish mexanizmlari birgalikda ishlashi zarur.[4]

3. Shaxsiy ma’lumotlar va intim materiallar orqali kibertovlamachilik

Kibertovlamachilikning keng tarqalgan yana bir shakli shaxsiy ma’lumotlar, fotosuratlar, videolar yoki yozishmalar orqali bosim o‘tkazishdir. Amaliyotda bu ko‘pincha sextortion deb ataladi. Bunda aybdor jabrlanuvchining intim yoki shaxsiy xarakterdagi ma’lumotlarini qo‘lga kiritadi yoki soxta material yaratadi, keyin esa ularni tarqatish bilan qo‘rqitib pul talab qiladi.

[3] National Cyber Security Centre. Ransomware, Extortion and the Cyber Crime Ecosystem. United Kingdom NCSC and National Crime Agency.
[4] Cybersecurity and Infrastructure Security Agency. StopRansomware Guide: Ransomware and Data Extortion Prevention and Response. CISA.

Ushbu shaklda zarar faqat mulkiy zarar bilan chegaralanmaydi. Jabrlanuvchining sha'ni, qadr-qimmati, oilaviy munosabatlari, ruhiy holati va ijtimoiy mavqei xavf ostida qoladi. Ayrim hollarda jabrlanuvchi jinoyat haqida xabar berishdan ham qo'rqadi. Chunki u ma'lumotlar oshkor bo'lib ketishi, yaqinlari yoki ish joyi oldida obro'sizlanishi mumkin deb o'ylaydi. Aynan shu omil kibertovlamachilikning yashirinligini kuchaytiradi.

Bu turdagi qilmishlarni baholashda mulkiy talab mavjudligi asosiy farqlovchi mezon hisoblanadi. Agar shaxs faqat shaxsiy ma'lumotni noqonuniy tarqatsa, bu boshqa jinoyat tarkibi doirasida baholanishi mumkin. Agar u ushbu ma'lumotlarni tarqatish bilan qo'rqitib pul yoki boshqa mulkiy manfaat talab qilsa, tovlamachilik belgisi yuzaga keladi. O'zbekistonning shaxsga doir ma'lumotlar to'g'risidagi qonunchiligi shaxsiy ma'lumotlarni axborot texnologiyalari vositasidan qat'i nazar himoya qilish zarurligini belgilaydi.[5] Demak, bunday holatlarda mulkka qarshi jinoyat bilan birga shaxsiy hayot daxlsizligiga tajovuz ham e'tiborga olinishi lozim.

4. Akkauntni egallab olish orqali sodir etiladigan tovlamachilik

Bugungi kunda ijtimoiy tarmoq, messenjer, elektron pochta va boshqa onlayn xizmatlardagi akkauntlar insonning raqamli shaxsiyati bilan uzviy bog'liq. Shu sababli akkauntni egallab olish orqali pul talab qilish ham kibertovlamachilikning alohida shakli sifatida ko'rilishi kerak.

Bunday holatda aybdor jabrlanuvchining akkauntiga kiradi, parolni o'zgartiradi, yozishmalarni ko'radi, shaxsiy yoki ishga oid ma'lumotlarni nazorat qiladi. Keyin akkauntni qaytarish yoki ma'lumotlarni tarqatmaslik evaziga pul talab qiladi. Ayrim hollarda jinoyatchi jabrlanuvchi nomidan uning tanishlariga xabar yuborib, ulardan ham pul so'rashi mumkin. Bu esa tovlamachilik, firibgarlik va shaxsiy ma'lumotlar bilan bog'liq qilmishlarning bir-biriga qo'shilib ketishiga olib keladi.

Akkauntni egallab olish orqali sodir etilgan kibertovlamachilikda raqamli dalillar alohida ahamiyatga ega. Login qilingan vaqt, IP-manzil, qurilma ma'lumotlari, parol o'zgartirilgan payt, telefon raqami yoki elektron pochtaga bog'langan tasdiqlash xabarlari, chat yozishmalari va to'lov rekvizitlari ish bo'yicha asosiy dalillar bo'lishi mumkin. Shu bilan birga, bunday dalillar qonuniy tartibda olingan va yaxlitligi saqlangan bo'lishi shart. Dalilning maqbulligi masalasi Oliy sud Plenumi qarorlarida ham alohida e'tibor qaratilgan protsessual talablar bilan bog'liq.[6]

5. Kriptoaktivlar orqali to'lov talab qilish

Kibertovlamachilikda to'lovni kriptoaktivlar orqali talab qilish holatlari tobora ko'proq uchramoqda. Jinoyatchilar bunday vositani tanlash orqali an'anaviy bank nazoratidan chetda qolishga, to'lovni tez qabul qilishga va shaxsini yashirishga harakat qiladi. Albatta, blokcheyn tranzaksiyalari mutlaqo izsiz emas. Ammo ularni jinoyatchi shaxs bilan bog'lash maxsus texnik bilim, raqamli kriminalistika va xalqaro hamkorlikni talab qiladi.

Kriptoaktiv orqali to'lov talab qilishning o'zi kibertovlamachilikning alohida tarkibini yaratmaydi, lekin jinoyatni sodir etish usulini murakkablashtiradi. Bunday holatda tergov organlari nafaqat tovlamachilik faktini, balki to'lov yo'nalishi, kriptohamyon manzili, almashuv platformasi, tranzaksiya zanjiri va ehtimoliy vositachilarni ham aniqlashi kerak bo'ladi.

[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: lex.uz.
[6] 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.

FBI IC3 hisobotlarida internet jinoyatlari bo‘yicha murojaatlar va zararlar yildan yilga juda katta miqdorda qayd etilayotgani ko‘rsatiladi.[7] Bu ma’lumotlar O‘zbekiston uchun ham ogohlantiruvchi ahamiyatga ega. Chunki raqamli moliyaviy vositalar kengaygan sari tovlamachilikning to‘lov mexanizmi ham murakkablashib boradi.

6. Tashkilotlar va muhim axborot infratuzilmasiga nisbatan kibertovlamachilik

Kibertovlamachilik jismoniy shaxslarga nisbatan sodir etilganda ham xavfli. Biroq u tashkilotlar, davlat organlari, banklar, tibbiyot muassasalari, transport tizimlari yoki energetika sohasi axborot tizimlariga qaratilganda uning xavfi ancha ortadi. Chunki bunday holatda jabrlanuvchi doirasi bitta shaxs bilan cheklanmaydi.

Masalan, korxonaning ma’lumotlar bazasi bloklansa, xodimlar ish jarayoni, mijozlar bilan munosabatlar va moliyaviy operatsiyalar izdan chiqishi mumkin. Tibbiyot muassasasida axborot tizimiga kirish imkoni cheklansa, bemorlar haqidagi zarur ma’lumotlar vaqtida olinmasligi ehtimoli yuzaga keladi. Bank yoki to‘lov tizimi nishonga olinsa, nafaqat moliyaviy zarar, balki butun raqamli xizmatlarga bo‘lgan ishonchning kamayishi kuzatiladi.

“Kiberxavfsizlik to‘g‘risida”gi Qonun kiberxavfsizlik sohasidagi munosabatlarni tartibga solishi bilan mazkur yo‘nalish uchun umumiy huquqiy asos yaratadi.[8] Bu qonun bevosita jinoiy javobgarlikni belgilamaydi, ammo axborot tizimlari va raqamli muhitni himoya qilish davlat siyosati darajasidagi vazifa ekanini ko‘rsatadi. Shunday ekan, muhim axborot infratuzilmasiga nisbatan sodir etilgan kibertovlamachilikni ijtimoiy xavflilik darajasi yuqori bo‘lgan qilmish sifatida baholash asosli bo‘ladi.

7. Kibertovlamachilikka nisbatan javobgarlik belgilashning ijtimoiy zaruriyati

Jinoiy javobgarlik har qanday nojo‘ya harakat uchun emas, balki jamiyat uchun eng xavfli qilmishlar uchun belgilanadi. Kibertovlamachilik aynan shunday qilmishlar qatoriga kiradi. Chunki unda bir vaqtning o‘zida bir nechta ijtimoiy munosabatlarga tajovuz qilinadi: mulk, shaxsiy hayot daxlsizligi, axborot xavfsizligi, ishchanlik obro‘si va raqamli muhitga bo‘lgan ishonch.

Birinchi ijtimoiy zarurat — jabrlanuvchining huquq va erkinliklarini himoya qilishdir. Kibertovlamachilik jabrlanuvchini kuchli ruhiy bosim ostiga oladi. Ayniqsa shaxsiy ma’lumotlar, fotosuratlar yoki yozishmalar orqali shantaj qilingan shaxs o‘zini himoyasiz his qilishi mumkin. Jinoiy javobgarlik bunday holatda davlatning shaxsni raqamli muhitda ham himoya qilish majburiyatini ifodalaydi.

Ikkinchi zarurat — mulk va raqamli iqtisodiyotni himoya qilishdir. Bugungi kunda ko‘plab iqtisodiy munosabatlar elektron platformalar orqali amalga oshiriladi. Shartnomalar, to‘lovlar, hisob-kitoblar, davlat xizmatlari va biznes jarayonlari raqamli tizimlarga bog‘langan. Agar kibertovlamachilikka nisbatan qat’iy huquqiy munosabat bo‘lmasa, fuqarolar va tadbirkorlik subyektlarining raqamli xizmatlarga ishonchi susayadi.

Uchinchi zarurat — jinoyatlarning yashirinligi va transmilliyligini hisobga olishdir. Europolning kiberjinoyatlar bo‘yicha tahlillarida ransomware, onlayn firibgarlik va boshqa kiberjinoyatlar zamonaviy jinoyatchilikning jiddiy yo‘nalishlari sifatida qayd etiladi. Kibertovlamachilik ham ko‘pincha bir necha davlat hududi, chet eldagi serverlar va xalqaro to‘lov vositalari bilan bog‘liq bo‘ladi. Shu sababli faqat milliy darajadagi oddiy choralar yetarli emas, xalqaro hamkorlik ham zarur.

[7] Federal Bureau of Investigation. Internet Crime Complaint Center. 2024 Internet Crime Report.
[8] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

To‘rtinchi zarurat — profilaktika vazifasidir. Jinoiy javobgarlikning maqsadi faqat jazolash emas. U jamiyatga bunday qilmishlarga nisbatan murosasiz huquqiy munosabat mavjudligini ko‘rsatadi. Ayniqsa yoshlar va texnik bilimga ega shaxslar o‘rtasida “internetda qilingan harakat javobsiz qoladi” degan noto‘g‘ri tasavvurni bartaraf etish muhimdir.

8. Xalqaro hujjatlar va xorijiy tajriba bilan qiyosiy tahlil

Kibertovlamachilikka qarshi kurashda xalqaro hujjatlar muhim o‘rin tutadi. Budapest konvensiyasi kiberjinoyatchilik va elektron dalillar bo‘yicha eng asosiy xalqaro hujjatlardan biri bo‘lib, u davlatlar uchun milliy qonunchilikni rivojlantirish va xalqaro hamkorlikni yo‘lga qo‘yishda muhim yo‘nalish beradi.[9] Kibertovlamachilik unda alohida nom bilan ko‘rsatilmagan bo‘lsa-da, kompyuter tizimlariga noqonuniy kirish, ma’lumotlarga aralashish, tizim faoliyatiga zarar yetkazish va elektron dalillar bilan ishlash masalalari ushbu jinoyatga bevosita aloqador.

AQSh qonunchiligida 18 U.S.C. §1030 kompyuterlar bilan bog‘liq jinoyatlarni, jumladan kompyuterga zarar yetkazish yoki tahdid orqali qiymat talab qilish holatlarini qamrab oladi. Bu yondashuvning afzalligi shundaki, kompyuter tizimi jinoyatning alohida muhim elementi sifatida e’tirof etiladi.

Buyuk Britaniyada Computer Misuse Act 1990 ruxsatsiz kirish, keyingi jinoyatni sodir etish maqsadida ruxsatsiz kirish va kompyuter faoliyatiga zarar yetkazuvchi harakatlar uchun javobgarlikni belgilaydi.[10] Bu model kibertovlamachilikning pul talab qilinishidan oldingi bosqichlarini ham huquqiy baholashga yordam beradi.

Germaniya Jinoyat kodeksida esa ma’lumotlarni yashirin egallash, phishing va bunday harakatlarga tayyorgarlik ko‘rish bilan bog‘liq normalar mavjud.[11] Bu tajriba shuni ko‘rsatadiki, kibertovlamachilikka qarshi kurashda faqat yakuniy “to‘lov talab qilish” holatini emas, balki unga olib keluvchi texnik bosqichlarni ham nazoratga olish zarur.

O‘zbekiston tajribasi ushbu davlatlar tajribasidan to‘g‘ridan-to‘g‘ri nusxa olishi shart emas. Biroq qiyosiy tahlil shuni ko‘rsatadiki, milliy qonunchilikda mavjud 165-modda axborot texnologiyalari sohasidagi jinoyatlar haqidagi normalar, raqamli dalillarni tartibga soluvchi protsessual qoidalar va xalqaro hamkorlik mexanizmlari bilan uzviy qo‘llanilganda samaraliroq natija beradi.

9. Raqamli dalillar va isbotlash muammosi

Kibertovlamachilik uchun javobgarlikni belgilashning o‘zi yetarli emas. Agar qilmishni isbotlash mexanizmi ishlamasa, norma amaliyotda kutilgan natijani bermaydi. Bunday jinoyatlarda asosiy dalillar ko‘pincha raqamli shaklda bo‘ladi: elektron yozishmalar, skrinshotlar, server loglari, IP-manzillar, qurilma identifikatori, kriptohamyon manzili, tranzaksiya zanjiri, audio va video fayllar, metadata va boshqa elektron ma’lumotlar.

Raqamli dalillarning murakkabligi shundaki, ular tez o‘chirilishi, o‘zgartirilishi yoki chet eldagi serverlarda saqlanishi mumkin. Shu sababli tergov organlari dalillarni tezkor saqlab qolish, ularning yaxlitligini ta’minlash va protsessual tartibda rasmiylashtirishga alohida e’tibor qaratishi kerak. Elektron dalillar bilan ishlash bo‘yicha xalqaro amaliy qo‘llanmalarda ham bunday dalillarni olish, saqlash va transchegaraviy so‘rash masalalari kiberjinoyatlarni tergov qilishning asosiy shartlaridan biri sifatida ko‘rsatiladi.

[9] Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.
[10] Computer Misuse Act 1990. United Kingdom.
[11] German Criminal Code (Strafgesetzbuch — StGB). Sections 202a, 202b, 202c.

Fikrimizcha, kibertovlamachilik bo‘yicha tergov amaliyotida raqamli dalilni oddiy skrinshot bilan cheklash noto‘g‘ri bo‘ladi. Skrinshot yordamchi dalil bo‘lishi mumkin, lekin u manba, vaqt, qurilma va yozishmaning yaxlitligi bilan birga tekshirilmasa, uning ishonchlilik darajasi past bo‘lib qoladi. Shu sababli mutaxassis ishtiroki, ekspertiza, elektron ma’lumotni asl manbadan olish va dalillar zanjirini saqlash juda muhim.

10. Mualliflik pozitsiyasi

Yuqoridagi tahlillardan kelib chiqib, kibertovlamachilikni uch jihatdan baholash maqsadga muvofiq deb hisoblaymiz. Birinchidan, u mulkka qarshi qaratilgan jinoyat, chunki aybdor jabrlanuvchidan pul, kriptoaktiv yoki boshqa mulkiy manfaat talab qiladi. Ikkinchidan, u axborot xavfsizligiga qarshi qaratilgan jinoyat, chunki tahdid ko‘pincha axborot resursi, ma’lumotlar bazasi yoki kompyuter tizimi orqali amalga oshiriladi. Uchinchidan, u shaxsiy hayot va raqamli obro‘ga tahdid qiluvchi qilmish, chunki jabrlanuvchining shaxsiy ma’lumotlari, yozishmalari yoki fotosuratlari bosim vositasiga aylanishi mumkin.

Shuning uchun kibertovlamachilikni tasniflashda faqat texnik mezon bilangina cheklanmaslik kerak. Masalan, “ransomware”, “sextortion” yoki “akkauntni egallash” texnik yoki amaliy shaklni ko‘rsatadi. Jinoyat-huquqiy bahoda esa qo‘rqitish mazmuni, mulkiy talab, jabrlanuvchi holati, zarar xavfi, dalillar turi va jinoyatning boshqa tarkiblar bilan bog‘liqligi ham aniqlanishi kerak.

O‘zbekiston qonunchiligida JK 165-moddaga axborot resursiga oid tahdidlarning kiritilgani ijobiy holat. Lekin amaliyotda bu normani to‘g‘ri qo‘llash uchun sud-tergov organlari kibertovlamachilikning turli shakllarini farqlay olishi lozim. Kelgusida bu borada sud amaliyoti umumlashtirilishi, raqamli dalillarni baholash bo‘yicha tushuntirishlar kengaytirilishi va muhim axborot infratuzilmasiga qaratilgan tovlamachilik holatlari alohida e’tiborda bo‘lishi zarur.

Xulosa

Kibertovlamachilik jinoyatlarining tasnifi ushbu qilmishning murakkab tabiatini ochib berish uchun zarur hisoblanadi. Mazkur jinoyat ransomware, shaxsiy ma’lumotlar orqali shantaj, akkauntni egallab olish, kriptoaktivlar orqali to‘lov talab qilish, tashkilotlar axborot tizimlarini bloklash va muhim axborot infratuzilmasiga tahdid qilish kabi shakllarda namoyon bo‘ladi. Har bir shaklning o‘ziga xos dalillanish mexanizmi, jabrlanuvchiga yetkazadigan zarari va huquqiy baholash mezonlari mavjud.

Kibertovlamachilikka nisbatan jinoiy javobgarlik belgilashning ijtimoiy zaruriyati shaxs huquqlari, mulk, axborot xavfsizligi, raqamli iqtisodiyot va jamiyatning kibermakonga bo‘lgan ishonchini himoya qilish ehtiyoji bilan belgilanadi. Bu jinoyatning xavfi shundaki, u moddiy zarar bilan birga ruhiy bosim, reputatsion zarar, axborot tizimlarining izdan chiqishi va transmilliy jinoyatchilik xavfini ham yuzaga keltiradi.

O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasida axborot resursiga qaratilgan tahdidlarning aks ettirilishi kibertovlamachilikka qarshi kurashning muhim huquqiy asosi hisoblanadi. Shu bilan birga, mazkur norma axborot texnologiyalari sohasidagi jinoyatlar, raqamli dalillar haqidagi protsessual normalar, kiberxavfsizlik qonunchiligi va xalqaro hamkorlik mexanizmlari bilan uyg‘un qo‘llanilgandagina amaliy samaradorlikka ega bo‘ladi.

Shunday qilib, kibertovlamachilik jinoyatlarining tasnifi va bunday qilmishlarga nisbatan javobgarlik belgilash masalasi faqat nazariy mavzu emas. Bu O‘zbekistonning raqamli xavfsizligi, fuqarolarning huquqiy himoyasi, biznes muhitining barqarorligi va raqamli davlat xizmatlariga bo‘lgan ishonchni ta’minlash bilan bevosita bog‘liq dolzarb ilmiy-huquqiy masaladir.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Jinoyat kodeksi. 1994-yil 22-sentabr. — Qonunchilik ma’lumotlari milliy bazasi.
2. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi. 1994-yil 22-sentabr. — 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 2018-yil 24-avgustdagi 24-son “Dalillar maqbulligiga oid jinoyat-protsessual qonuni normalarini qo‘llashning ayrim masalalari to‘g‘risida”gi qarori. — Qonunchilik ma’lumotlari milliy bazasi.
7. Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.
8. United Nations Office on Drugs and Crime. Practical Guide for Requesting Electronic Evidence Across Borders.
9. United States Code. Title 18, §1030. Fraud and related activity in connection with computers.
10. Computer Misuse Act 1990. United Kingdom.
11. German Criminal Code (Strafgesetzbuch — StGB). Sections 202a, 202b, 202c
12. National Cyber Security Centre; National Crime Agency. Ransomware, Extortion and the Cyber Crime Ecosystem. — United Kingdom.
13. Cybersecurity and Infrastructure Security Agency. StopRansomware Guide: Ransomware and Data Extortion Prevention and Response.
14. Federal Bureau of Investigation. Internet Crime Complaint Center. 2024 Internet Crime Report.
15. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024.