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

Kibertovlamachilik jinoyatining obyektiv va subyektiv belgilari: jinoiy-huquqiy tahlil

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

Abstract. This article examines the objective and subjective elements of cyber extortion from a criminal-law perspective. The study is based on the Criminal Code and Criminal Procedure Code of the Republic of Uzbekistan, national legislation on cybersecurity and personal data protection, relevant decisions of the Plenum of the Supreme Court, international instruments, foreign legislation and academic literature. The article argues that cyber extortion should not be limited to the traditional understanding of extortion committed through the Internet. In cyber extortion, the threat, the object of encroachment, the evidentiary base and the offender’s intent acquire specific digital characteristics. The objective side of the offence is expressed through a threat made by digital means, unlawful influence on an information resource, intimidation by disclosure of personal data, blocking of access to a system, or other coercive acts aimed at obtaining property-related benefits. The subjective side is characterized by direct intent, selfish purpose and conscious exploitation of the victim’s dependence on digital information, reputation or infrastructure.

Keywords: cyber extortion, extortion, objective elements, subjective elements, direct intent, selfish purpose, digital evidence, information resource, ransomware, cybercrime.

Аннотация. В статье проводится уголовно-правовой анализ объективных и субъективных признаков кибервымогательства. Исследование основано на Уголовном кодексе и Уголовно-процессуальном кодексе Республики Узбекистан, национальном законодательстве о кибербезопасности и персональных данных, постановлениях Пленума Верховного суда, международных документах, зарубежном законодательстве и научной литературе. В статье обосновывается, что кибервымогательство не следует ограничивать традиционным пониманием вымогательства, совершённого посредством сети Интернет. При кибервымогательстве угроза, объект посягательства, доказательственная база и умысел виновного приобретают особые цифровые признаки. Объективная сторона преступления выражается в угрозе с использованием цифровых средств, незаконном воздействии на информационный ресурс, угрозе раскрытия персональных данных, блокировании доступа к системе либо иных принудительных действиях, направленных на получение имущественной выгоды. Субъективная сторона характеризуется прямым умыслом, корыстной целью и сознательным использованием зависимости потерпевшего от цифровой информации, репутации или инфраструктуры.

Ключевые слова: кибервымогательство, вымогательство, объективные признаки, субъективные признаки, прямой умысел, корыстная цель, цифровые доказательства, информационный ресурс, ransomware, киберпреступность.

Annotatsiya. Ushbu maqolada kibertovlamachilik jinoyatining obyektiv va subyektiv belgilari jinoiy-huquqiy jihatdan tahlil qilinadi. Tadqiqot O‘zbekiston Respublikasi Jinoyat kodeksi, Jinoyat-protsessual kodeksi, kiberxavfsizlik va shaxsga doir ma’lumotlar sohasidagi milliy qonunchilik, Oliy sud Plenumi qarorlari, xalqaro hujjatlar, xorijiy davlatlar qonunchiligi hamda ilmiy adabiyotlar asosida olib borilgan. Maqolada kibertovlamachilikni oddiy tovlamachilikning internet orqali sodir etilgan ko‘rinishi bilan cheklab bo‘lmasligi asoslantiriladi. Kibertovlamachilikda tahdid, tajovuz obyekti, dalillar bazasi va aybdorning qasdi o‘ziga xos raqamli xususiyat kasb etadi. Jinoyatning obyektiv tomoni raqamli vositalar orqali tahdid qilish, axborot resursiga noqonuniy ta’sir ko‘rsatish, shaxsiy ma’lumotlarni oshkor qilish bilan qo‘rqitish, tizimga kirishni bloklash yoki boshqa majburlovchi

harakatlar orqali mulkiy manfaat olishga qaratiladi. Subyektiv tomoni esa to‘g‘ri qasd, g‘arazli maqsad hamda jabrlanuvchining raqamli axborot, obro‘ yoki infratuzilmaga bog‘liqligidan ongli foydalanish bilan tavsiflanadi.

Kalit so‘zlar: kibertovlamachilik, tovlamachilik, obyektiv belgilar, subyektiv belgilar, to‘g‘ri qasd, g‘arazli maqsad, raqamli dalil, axborot resursi, ransomware, kiberjinoyat.

1. Introduction

Kibertovlamachilik jinoyatini tahlil qilishda birinchi navbatda uning oddiy “internet orqali qo‘rqitish” emasligini aniqlab olish zarur. Bu jinoyatda tovlamachilikka xos bo‘lgan asosiy belgi — jabrlanuvchini qo‘rqitish orqali undan mulkiy manfaat talab qilish — saqlanib qoladi. Biroq kibermakon ushbu belgining namoyon bo‘lish shaklini o‘zgartiradi. Tahdid endi faqat jismoniy zo‘rlik, mulkka zarar yetkazish yoki sharmanda qiluvchi ma’lumotlarni tarqatish bilan cheklanmaydi. U axborot resursini egallab olish, tizimga kirishni bloklash, shaxsiy ma’lumotlarni ommaga chiqarish, elektron yozishmalarni tarqatish, akkauntni qaytarmaslik yoki ma’lumotlarni shifrlab qo‘yish shaklida ham yuzaga chiqadi.

O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasi tovlamachilik uchun javobgarlikni belgilaydi. Ushbu moddaning amaldagi mazmunida jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish bilan qo‘rqitish kabi belgilar aks etgani kibertovlamachilikni milliy jinoyat qonunchiligi doirasida baholash imkonini kuchaytiradi.[1] Bu holat mazkur jinoyatning nazariy tahlilini ham, amaliy kvalifikatsiyasini ham dolzarb qiladi. Chunki qonun chiqaruvchi axborot resursiga qaratilgan tahdidni tovlamachilik tarkibining mumkin bo‘lgan ko‘rinishi sifatida e’tirof etgan.

Shu bilan birga, kibertovlamachilikni faqat 165-modda doirasida ko‘rish yetarli emas. Amaliy holatlarda bu qilmish ko‘pincha kompyuter tizimiga ruxsatsiz kirish, zararli dasturdan foydalanish, shaxsiy ma’lumotlarni egallash, elektron yozishmalarni tarqatish bilan qo‘rqitish, kriptoaktivda to‘lov talab qilish va raqamli dalillarni baholash kabi bir nechta masalani bir vaqtda yuzaga chiqaradi. Shuning uchun mazkur maqolada kibertovlamachilik jinoyatining obyektiv va subyektiv belgilarini alohida emas, balki o‘zaro bog‘liq tarkibiy elementlar sifatida tahlil qilish maqsad qilingan.

Tadqiqotning asosiy savoli quyidagicha qo‘yiladi: kibertovlamachilikni klassik tovlamachilikdan farqlovchi obyektiv va subyektiv belgilar nimalardan iborat va ular huquqni qo‘llash amaliyotida qanday baholanishi kerak? Ushbu savolga javob berish uchun milliy qonunchilik, xorijiy tajriba, xalqaro standartlar va ilmiy adabiyotlar tahlil qilindi.

2. Materials and Methods

Tadqiqot materiali sifatida O‘zbekiston Respublikasi Jinoyat kodeksi, Jinoyat-protsessual kodeksi, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun, “Kiberxavfsizlik to‘g‘risida”gi Qonun, O‘zbekiston Respublikasi Oliy sudi Plenumining dalillar maqbulligiga oid qarori, shuningdek xalqaro va xorijiy manbalar tanlandi. Xalqaro-huquqiy manba sifatida Budapest konvensiyasi, elektron dalillar bo‘yicha xalqaro qo‘llanmalar, xorijiy qonunchilik manbalari sifatida esa AQShning 18 U.S.C. §1030 normasi, Buyuk Britaniyaning Computer Misuse Act 1990 hujjati va Germaniya Jinoyat kodeksining kompyuter ma’lumotlari bilan bog‘liq normalari o‘rganildi.

Maqolada formal-yuridik, qiyosiy-huquqiy, tizimli, mantiqiy va tahliliy metodlardan foydalanildi. Formal-yuridik metod yordamida tovlamachilik tarkibining milliy qonunchilikdagi mazmuni sharhlandi. Qiyosiy-huquqiy metod O‘zbekiston, AQSh, Buyuk Britaniya va Germaniya yondashuvlarini solishtirish imkonini berdi. Tizimli metod kibertovlamachilikni faqat mulkka qarshi jinoyat emas, balki axborot xavfsizligi, shaxsiy hayot daxlsizligi, raqamli dalillar va transmilliy jinoyatchilik bilan bog‘liq murakkab hodisa sifatida baholashga xizmat qildi. Ilmiy adabiyotlar tahlili orqali ransomware iqtisodiyoti, kriptoaktivlar orqali to‘lov talab qilish, kiberjinoyatchi shaxsining motivlari va raqamli dalillar muammolari bo‘yicha qarashlar umumlashtirildi.

3. Results

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

Tadqiqot natijasida kibertovlamachilik jinoyatining obyektiv va subyektiv belgilariga oid bir nechta asosiy xulosa shakllantirildi.

Birinchidan, kibertovlamachilikning obyektiv tomoni raqamli muhit orqali qo‘rqitish va shu qo‘rqitish asosida mulkiy manfaat talab qilishdan iborat. Bunda tahdid elektron pochta, messenjer, ijtimoiy tarmoq, zararli dastur, anonim akkaunt, serverga noqonuniy kirish, ma’lumotlarni shifrlash yoki shaxsiy ma’lumotlarni tarqatish orqali amalga oshirilishi mumkin.

Ikkinchidan, kibertovlamachilik ko‘p obyektli jinoyat xususiyatiga ega. Uning asosiy obyekti mulkiy munosabatlar bo‘lsa-da, qo‘shimcha obyekt sifatida axborot xavfsizligi, shaxsiy hayot daxlsizligi, tijorat siri, ishchanlik obro‘si va raqamli infratuzilma xavfsizligi namoyon bo‘ladi.

Uchinchidan, kibertovlamachilik uchun mulkiy talab zaruriy belgi hisoblanadi. Shaxsiy ma’lumotlarni noqonuniy egallash, kompyuter tizimiga ruxsatsiz kirish yoki zararli dastur yuborishning o‘zi har doim tovlamachilikni vujudga keltirmaydi. Tovlamachilik tarkibi tahdid mulkiy talab bilan bog‘langanda yuzaga keladi.

To‘rtinchidan, kibertovlamachilik subyektiv jihatdan odatda to‘g‘ri qasd bilan sodir etiladi. Aybdor jabrlanuvchiga tahdid qilayotganini, uning raqamli axborot, obro‘ yoki infratuzilmaga bog‘liqligidan foydalanayotganini anglaydi va mulkiy manfaat olishni xohlaydi.

Beshinchidan, kibertovlamachilikni isbotlashda raqamli dalillar hal qiluvchi ahamiyatga ega. Elektron yozishmalar, IP-manzillar, login tarixi, server loglari, skrinshotlar, kriptohamyon manzillari, tranzaksiya zanjiri, audio-video fayllar va metadata jinoyatning ham obyektiv, ham subyektiv belgilarini aniqlashga xizmat qiladi.

4. Discussion

4.1. Obyektiv belgilar: tahdid, raqamli vosita va mulkiy talab

Kibertovlamachilikning obyektiv tomonida eng muhim masala tahdid va mulkiy talab o‘rtasidagi bog‘liqlikdir. Tovlamachilik jinoyatini boshqa mulkiy yoki axborot texnologiyalari sohasidagi jinoyatlardan farqlovchi asosiy mezon ham shu yerda ko‘rinadi. Masalan, shaxsning akkauntiga ruxsatsiz kirish holati alohida baholanishi mumkin, lekin ushbu akkauntni qaytarish evaziga pul talab qilinsa, qilmishda tovlamachilik belgisi paydo bo‘ladi. Xuddi shuningdek, shaxsiy yozishmalarni qo‘lga kiritishning o‘zi boshqa huquqbuzarlik bo‘lishi mumkin, ammo ularni tarqatish bilan qo‘rqitib mulkiy manfaat talab qilish tovlamachilik tarkibini vujudga keltiradi.

Kibertovlamachilikda tahdidning shakli odatiy tovlamachilikka qaraganda ko‘proq axborotga qaratilgan bo‘ladi. “Pul yubormasang, fotosuratlaringni tarqataman”, “to‘lov qilmasang, serverlaringni ochmayman”, “kriptovalyutada pul yubormasang, mijozlar bazangni e’lon qilaman” kabi holatlar shuni ko‘rsatadiki, raqamli axborotning o‘zi bosim vositasiga aylanmoqda. Bu jihat klassik jinoyat-huquqiy yondashuvni kengroq talqin qilishni talab qiladi.

Laszka, Farhang va Grossklags ransomware iqtisodiyotiga bag‘ishlangan tadqiqotida jabrlanuvchi uchun to‘lov qilish yoki tizimni mustaqil tiklash masalasi oddiy texnik qaror emas, balki iqtisodiy va xavfsizlik nuqtai nazaridan murakkab tanlov ekanini ko‘rsatadi.[2] Bu yondashuv kibertovlamachilikdagi tahdidning kuchi aynan jabrlanuvchining raqamli infratuzilmaga qanchalik bog‘liqligida ekanini tushuntiradi. Agar tashkilotning barcha ish jarayoni elektron tizimga bog‘langan bo‘lsa, serverning bloklanishi unga oddiy texnik noqulaylik emas, balki faoliyatni to‘xtatib qo‘yuvchi bosim sifatida ta’sir qiladi.

Paquet-Clouston, Haslhofer va Dupont ransomware to‘lovlarining Bitcoin ekotizimidagi harakatini o‘rganar ekan, kriptoaktivlar bunday jinoyatlarda to‘lovni qabul qilish va yashirish mexanizmi sifatida ishlatilishini ko‘rsatadi.[3] Bu fikr kibertovlamachilik obyektiv tomonining yana bir xususiyatini ochadi: jinoyatchi faqat tahdid qilmaydi, balki to‘lovni qabul qilish uchun raqamli moliyaviy infratuzilmadan ham foydalanadi. Shu sababli kriptoaktiv orqali to‘lov talab qilish jinoyatning asosiy tarkibini o‘zgartirmasa-da, uning sodir etilish usulini murakkablashtiradi.

[2] Laszka A., Farhang S., Grossklags J. On the Economics of Ransomware // Decision and Game Theory for Security. — Springer, 2017. — P. 397–417.
[3] Paquet-Clouston M., Haslhofer B., Dupont B. Ransomware Payments in the Bitcoin Ecosystem // Journal of Cybersecurity. — 2019. — Vol. 5, Issue 1.

4.2. Jinoyat obyekti: mulk bilan cheklanmaydigan tajovuz

Kibertovlamachilikni faqat mulkka qarshi jinoyat sifatida ko‘rish nazariy jihatdan yetarli emas. Albatta, tovlamachilik tarkibida mulkiy manfaat talabi asosiy belgi bo‘lib qoladi. Lekin kibertovlamachilikda tajovuz ko‘pincha shaxsiy hayot daxlsizligi, axborot xavfsizligi, tijorat siri, ishchanlik obro‘si va raqamli infratuzilma barqarorligiga ham qaratiladi.

Masalan, shaxsiy fotosuratlar yoki yozishmalarni tarqatish bilan qo‘rqitib pul talab qilish holatida jabrlanuvchining mulkiy manfaatlari bilan birga uning sha’ni, qadr-qimmati va shaxsiy hayoti ham xavf ostida qoladi. Korxona serverini bloklab to‘lov talab qilishda esa asosiy bosim korxonaning axborot tizimiga qaratilgan bo‘ladi. Bunday hollarda zarar nafaqat talab qilingan pul miqdorida, balki ish jarayoni to‘xtashi, mijozlar ishonchi pasayishi, tijorat siri oshkor bo‘lishi yoki reputatsion yo‘qotishlarda ham namoyon bo‘ladi.

O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni shaxsiy ma’lumotlarning huquqiy himoyaga muhtoj alohida obyekt ekanini ko‘rsatadi.[4] Shu bois kibertovlamachilikda shaxsga doir ma’lumotlar bosim vositasiga aylanganda, qilmishning ijtimoiy xavfi oddiy mulkiy zarar doirasidan chiqib ketadi. Bu holat huquqni qo‘llash amaliyotida ham inobatga olinishi kerak.

4.3. Raqamli dalillar obyektiv belgilarni isbotlash vositasi sifatida

Kibertovlamachilikning obyektiv belgilarini isbotlash odatda raqamli dalillarsiz mumkin emas. Tahdid qayerdan yuborilgan, kim tomonidan yuborilgan, qaysi akkaunt ishlatilgan, serverga qachon kirilgan, fayllar qachon shifrlangan, to‘lov qaysi kriptohamyonga talab qilingan — bularning barchasi elektron izlar orqali aniqlanadi.

O‘zbekiston Respublikasi Jinoyat-protsessual kodeksida elektron ma’lumotlar va raqamli dalillar tushunchalarining kiritilishi bu borada muhim huquqiy asos yaratadi.[5] Ammo amaliyotda muammo faqat norma mavjudligida emas, balki dalilning qanday olingani, qanday saqlangani va sudda qanday baholanishidadir. Oddiy skrinshot ayrim hollarda dastlabki ma’lumot sifatida foydali bo‘lishi mumkin, lekin u mustaqil va yetarli dalil sifatida har doim ham ishonchli emas. Chunki skrinshotni tahrirlash, kontekstdan uzib olish yoki soxtalashtirish ehtimoli mavjud.

Oliy sud Plenumining dalillar maqbulligiga oid qarori dalillar qonuniy tartibda olingan, ishga aloqador va ishonchli bo‘lishi kerakligini anglatadi.[6] Kibertovlamachilikda bu talablar yanada muhimlashadi, chunki raqamli dalillar tez o‘chirilishi, o‘zgartirilishi yoki chet eldagi serverlarda saqlanishi mumkin. Shuning uchun elektron dalillarni asl manbadan olish, ularning yaxlitligini saqlash, mutaxassis yoki ekspert ishtirokida tekshirish va dalillar zanjirini hujjatlashtirish zarur.

4.4. Subyektiv belgilar: to‘g‘ri qasd va g‘arazli maqsad

Kibertovlamachilik subyektiv jihatdan odatda to‘g‘ri qasd bilan sodir etiladi. Aybdor jabrlanuvchiga tahdid qilayotganini, uni mulkiy manfaat berishga majbur qilayotganini anglaydi va aynan shu natijani xohlaydi. Masalan, jinoyatchi jabrlanuvchining ma’lumotlarini shifrlab, “to‘lov qilmasang, fayllaring ochilmaydi” desa, uning harakati tasodifiy emas. U jabrlanuvchini majburiy holatga solish orqali mulkiy foyda olishni ko‘zlaydi.

G‘arazli maqsad kibertovlamachilikning markaziy subyektiv belgilaridan biridir. Bu maqsad pul, kriptoaktiv, mulkiy huquq, xizmat yoki boshqa manfaat olishda namoyon bo‘lishi mumkin. Agar shaxs ma’lumotlarni faqat o‘ch olish yoki sharmanda qilish niyatida tarqatsa, qilmish boshqa jinoyat sifatida baholanishi mumkin. Ammo u ma’lumotlarni tarqatish bilan qo‘rqitib pul talab qilsa, tovlamachilikning subyektiv tomoni shakllanadi.

Lubin ransomware haqidagi tahlilida bunday jinoyatlarning kengayishida iqtisodiy manfaatdorlik, transmilliylik va javobgarlikka tortishdagi qiyinchiliklar muhim rol o‘ynashini qayd

[4] 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.
[5] 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
[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.

etadi.[7] Bu fikr kibertovlamachilik subyektiv tomonini tushunishda ahamiyatli: jinoyatchi o‘z harakatini foyda olish vositasi deb biladi va raqamli muhitning yashirinlik imkoniyatlaridan ongli foydalanadi.

Bada va Nurse kiberjinoyatchilar profili haqidagi tadqiqotida onlayn jinoyatchini faqat yuqori malakali texnik mutaxassis sifatida ko‘rish noto‘g‘ri ekanini ta’kidlaydi.[8] Bu xulosa kibertovlamachilik subyekti uchun ham muhim. Chunki bunday jinoyatni professional dasturchi, tayyor zararli dasturdan foydalanuvchi oddiy shaxs, uyushgan guruh a’zosi yoki shaxsiy adovat sababli harakat qilgan foydalanuvchi sodir etishi mumkin. Demak, subyektni baholashda faqat texnik malaka emas, balki qasd, maqsad va jabrlanuvchiga bosim o‘tkazish niyati asosiy o‘rinda turadi.

4.5. Raqamli anonimlik va qasdni aniqlash

Kibertovlamachilikda anonimlik alohida ahamiyatga ega. Aybdor soxta akkaunt, vaqtinchalik elektron pochta, VPN, xorijiy server, kriptohamyon yoki boshqa yashirish vositalaridan foydalanishi mumkin. Bunday vositalar ba’zan jinoyatchida “meni topishmaydi” degan xato tasavvurni shakllantiradi. Shu sababli raqamli anonimlik jinoyatning kriminologik omili sifatida ham, subyektiv tomonni baholashda bilvosita dalil sifatida ham ahamiyatga ega.

Masalan, shaxs maxsus soxta akkaunt ochib, jabrlanuvchiga tahdid yuborsa, keyin to‘lov uchun alohida kriptohamyon manzilini bersa, bu harakatlar odatda tasodifiy emas. Bunday ketma-ketlik oldindan o‘ylangan reja, javobgarlikdan qochish istagi va g‘arazli maqsad mavjudligini ko‘rsatishi mumkin. Albatta, bularning barchasi boshqa dalillar bilan birgalikda baholanishi kerak.

Germaniya Jinoyat kodeksida kompyuter ma’lumotlariga noqonuniy kirish, ma’lumotlarni qo‘lga kiritish va bunday harakatlarga tayyorgarlik ko‘rish bilan bog‘liq normalarning mavjudligi kibertovlamachilikning tayyorgarlik bosqichlariga ham e’tibor berish zarurligini ko‘rsatadi. Chunki ayrim hollarda pul talab qilish jinoyatning oxirgi bosqichi bo‘lishi mumkin; undan oldin parol yig‘ish, zararli dastur yuborish, ma’lumotlarni ko‘chirib olish yoki jabrlanuvchini kuzatish kabi harakatlar sodir etiladi.

4.6. Xorijiy qonunchilik bilan qiyosiy tahlil

AQSh qonunchiligida 18 U.S.C. §1030 kompyuter bilan bog‘liq jinoyatlarni, jumladan himoyalangan kompyuterga zarar yetkazish, axborot olish yoki bunday tahdid orqali pul yoki boshqa qiymat talab qilish holatlarini qamrab oladi.[9] Bu yondashuvning afzalligi shundaki, kompyuter tizimi jinoyatning muhim elementi sifatida alohida baholanadi. O‘zbekiston qonunchiligida esa kibertovlamachilik alohida modda sifatida ajratilmagan bo‘lsa-da, JK 165-moddasidagi axborot resursiga oid belgilar va axborot texnologiyalari sohasidagi jinoyatlar haqidagi normalar birgalikda qo‘llanishi mumkin.

Buyuk Britaniyaning Computer Misuse Act 1990 hujjatida kompyuter materiallariga ruxsatsiz kirish va keyingi jinoyatni sodir etish niyati bilan ruxsatsiz kirish alohida tartibga solinadi. Bu model kibertovlamachilikdagi tayyorgarlik bosqichini baholashda foydali. Chunki ko‘pincha jabrlanuvchiga tahdid yuborilishidan oldin uning akkauntiga kirish, ma’lumotini olish yoki tizimiga zarar yetkazish sodir bo‘ladi.

Germaniya qonunchiligida ham ma’lumotlarni yashirin egallash, ma’lumotlarni ushlab qolish va bunday harakatlarga tayyorgarlik ko‘rish bo‘yicha normalar mavjud. Bu tajriba shuni ko‘rsatadiki, kibertovlamachilikni faqat yakuniy “pul talab qilish” bilan bog‘lab qo‘yish yetarli emas. Huquqiy baholash jinoyatning butun mexanizmini qamrab olishi kerak.

4.7. Xalqaro hujjatlar va transmilliylik

Budapest konvensiyasi kiberjinoyatchilik va elektron dalillar bo‘yicha eng muhim xalqaro hujjatlardan biri hisoblanadi.[10] Garchi unda kibertovlamachilik alohida nom bilan ko‘rsatilmagan bo‘lsa-da, kompyuter tizimlariga noqonuniy kirish, ma’lumotlarga aralashish, tizim faoliyatiga zarar yetkazish va elektron dalillar bo‘yicha hamkorlik kabi masalalar ushbu jinoyatga bevosita aloqador.

Kibertovlamachilik ko‘pincha transmilliy xususiyatga ega bo‘ladi. Jinoyatchi bir davlatda,

[7] Lubin A. The Law and Politics of Ransomware // Vanderbilt Journal of Transnational Law. — 2022. — Vol. 55. — P. 1177–1216.
[8] Bada M., Nurse J.R.C. Profiling the Cybercriminal: A Systematic Review of Research // IEEE Cyber Science Conference. — 2021.
[9] United States Code. Title 18, §1030. Fraud and related activity in connection with computers.
[10] Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.

jabrlanuvchi ikkinchi davlatda, server uchinchi davlatda, to‘lov esa kriptoaktivlar orqali boshqa yurisdiksiyada harakatlanishi mumkin. Shu sababli jinoyatning obyektiv va subyektiv belgilarini isbotlash faqat milliy tergov harakatlari bilan cheklanib qolmasligi mumkin. Elektron dalillarni tezkor saqlash, chet el provayderlari bilan hamkorlik, xalqaro so‘rovlar va raqamli kriminalistika bu jarayonda muhim o‘rin tutadi.[11]

5. Conclusion

Kibertovlamachilik jinoyatining obyektiv belgilari raqamli vositalar orqali tahdid qilish, jabrlanuvchining axborot resursi, shaxsiy ma’lumotlari yoki raqamli infratuzilmasiga ta’sir ko‘rsatish, mulkiy manfaat talab qilish va bularni raqamli dalillar orqali isbotlash zaruratida namoyon bo‘ladi. Mazkur belgilar klassik tovlamachilik tarkibini inkor qilmaydi, lekin uning raqamli muhitdagi yangi mazmunini ochib beradi.

Subyektiv belgilar esa to‘g‘ri qasd, g‘arazli maqsad, jabrlanuvchini majburiy holatga solish istagi va raqamli vositalardan ongli foydalanish bilan tavsiflanadi. Aybdor jabrlanuvchining axborotga, obro‘ga, akkauntga yoki tizimga bog‘liqligini anglaydi va aynan shu zaiflikdan foydalanib mulkiy manfaat olishga intiladi.

Milliy qonunchilikda JK 165-moddasiga axborot resursiga oid tahdidlarning kiritilgani kibertovlamachilikni baholash uchun muhim asos yaratgan. Shu bilan birga, ushbu norma JPKdagi raqamli dalillar, Oliy sud Plenumi tushuntirishlari, kiberxavfsizlik qonunchiligi, xalqaro hamkorlik va xorijiy tajriba bilan uyg‘un qo‘llanilgandagina amaliy samaradorlikka ega bo‘ladi.

Shu asosda, kibertovlamachilikning obyektiv va subyektiv belgilarini chuqur tahlil qilish jinoyatlarni to‘g‘ri kvalifikatsiya qilish, o‘xshash qilmishlardan farqlash, raqamli dalillarni baholash va jabrlanuvchilarning huquqlarini himoya qilish uchun zarur ilmiy-amaliy shart hisoblanadi.

Declarations

Conflict of interest: The author declares no conflict of interest.

Funding: This research received no external funding.

Data availability: The study is based on open legal sources, international documents, foreign legislation and academic literature.

References

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 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar 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 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.
6. Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.
7. United Nations Office on Drugs and Crime. Practical Guide for Requesting Electronic Evidence Across Borders.
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.
11. Laszka A., Farhang S., Grossklags J. On the Economics of Ransomware. Decision and Game Theory for Security. Springer, 2017. P. 397–417.
12. Paquet-Clouston M., Haslhofer B., Dupont B. Ransomware Payments in the Bitcoin Ecosystem. Journal of Cybersecurity. 2019. Vol. 5, Issue 1.

[11] United Nations Office on Drugs and Crime. Practical Guide for Requesting Electronic Evidence Across Borders.

13. Lubin A. The Law and Politics of Ransomware. Vanderbilt Journal of Transnational Law. 2022. Vol. 55. P. 1177–1216.
14. Bada M., Nurse J.R.C. Profiling the Cybercriminal: A Systematic Review of Research. IEEE Cyber Science Conference. 2021.
15. National Cyber Security Centre; National Crime Agency. Ransomware, Extortion and the Cyber Crime Ecosystem. United Kingdom.
16. Cybersecurity and Infrastructure Security Agency. StopRansomware Guide: Ransomware and Data Extortion Prevention and Response.
17. Council of Europe. Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0.
18. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024.
19. Paquet-Clouston M., Romiti M., Haslhofer B., Charvat T. Spams Meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem. arXiv:1908.01051, 2019.
20. National Institute of Standards and Technology. Ransomware Risk Management: Cybersecurity Framework Profile.