RAQAMLI TEXNOLOGIYALAR ORQALI SODIR ETILADIGAN TOVLAMACHILIK JINOYATLARIGA QARSHI KURASHISHNING O‘ZIGA XOS JIHATLARI

Tashtemirov Anvar Aliqulovich
O‘zbekiston Respublikasi IIV Akademiyasi, Ma’muriy huquq kafedrasi dotsenti. E-mail: anvartoshtemirov05031979@gmail.com.
Botirov Aslbek Bahodir o‘g‘li
IIV Akademiyasi 3-o‘quv kursi, 317 guruh kursanti.

Annotatsiya: *Ushbu maqolada raqamli texnologiyalar orqali sodir etiladigan tovlamachilik jinoyatlari tushunchasi, uning zamonaviy ko‘rinishlari va jamiyat hayotiga salbiy ta’sirlari tahlil qilingan holda, qonunchilikdagi mavjud bo‘shliqlarning bunday turdagi jinoyatlarga qarshi kurashish samaradorligiga salbiy ta’siri, kiberxavfsizlikni ta’minlash bo‘yicha raqamli texnologiyalardan samarali foydalanish qoidalarining ahamiyati hamda bu borada innovatsion yondashuvlar bo‘yicha taklif va tavsiyalar berilgan.*

Kalit so‘zlar: *tovlamachilik, raqamli texnologiya, axborot xavfsizligi, kiberjinoyatchilik, shaxsiy ma’lumotlar, kiberxavfsizlik, huquqiy baza, profilaktika choralari, innovatsion raqamli tovlamachilik.*

Аннотatsiя: *В данной статье проанализированы понятие вымогательства, совершаемого с использованием цифровых технологий, его современные формы и негативное влияние на общественную жизнь. Рассмотрено, как существующие пробелы в законодательстве отрицательно сказываются на эффективности борьбы с этим видом преступлений, а также подчеркнута важность эффективного использования правил кибербезопасности в цифровых технологиях. В статье предложены инноватsионные подходы, рекомендatsии и предложения по данному вопросу.*

Ключевые слова: *вымогательство, цифровые технологии, информatsионная безопасность, киберпреступность, персональные данные, кибербезопасность, правовая база, профилактические меры, инноватsионное цифровое вымогательство.*

Annotation: *This article analyzes the concept of extortion committed using digital technologies, its modern forms, and its negative impact on social life. It examines how existing gaps in legislation adversely affect the effectiveness of combating this type of crime, and highlights the importance of effective use of cybersecurity regulations in digital technologies. The article also proposes innovative approaches, recommendations, and suggestions on this issue.*

Keywords: *extortion, digital technologies, information security, cybercrime, personal data, cybersecurity, legal framework, preventive measures, innovative digital extortion.*

Bugungi kunda zamonaviy axborot texnologiyalarining rivojlanishi insonlar o‘rtasida muloqot shakllarini o‘zgartirib, global axborot almashish maydonini shakllantirmoqda. Shuningdek, innovatsion axborot texnologiyalarining imkoniyatlarini suiiste’mol qiluvchi kiberjinoyatchilik subyektlari tomonidan turli xil huquqbuzarliklar sodir etilishi kuzatilmoqda.

Raqamli texnologiyalar va internet sohasining jadal rivojlanishi natijasida tovlamachilik jinoyatlarining ham yangi ko‘rinishlari paydo bo‘ldi. Endi tovlamachilik faqatgina an’anaviy usullarda emas, balki turli raqamli vositalar orqali ham sodir etiladi.

Raqamli texnologiyalar orqali tovlamachilik jinoyatlari — bu zamonaviy axborot-kommunikatsiya vositalari (internet, elektron pochta, ijtimoiy tarmoqlar, messenjerlar, mobil ilovalar va boshqa raqamli platformalar)dan foydalangan holda odamlarni qo‘rqitish, bosim o‘tkazish va ulardan moddiy manfaatlar talab qilishga qaratilgan jinoyat turidir.

Bu turdagi tovlamachilik jinoyatlari quyidagi xususiyatlarga ega:

An’anaviy tovlamachilik usullarining raqamli texnologiyalar bilan birlashishi: Masalan, qo‘rqitish va bosimni matnli xabarlar, ovozli qo‘ng‘iroqlar yoki video yozishmalar orqali amalga oshirish;

Jabrlanuvchilarning anonimligi va masofadan boshqarish: Jinoyatchilar o‘z shaxsini yashirish uchun maxsus texnik vositalardan foydalanadi, shuning uchun jinoyatlarni aniqlash va tergov qilish qiyinlashadi;

Shaxsiy ma’lumotlarni noqonuniy foydalanish: Tovlamachilar jabrlanuvchilarning shaxsiy va moliyaviy ma’lumotlarini bosim o‘tkazish uchun ishlatadi;

Kiberqahramonlik elementlari: Ba’zi hollarda tovlamachilik jinoyatlari kompyuter viruslari, shifrlash (shifrovka) dasturlari yoki xakerlik yo‘li bilan amalga oshiriladi, masalan, kompyuterlarni yoki telefonlarni bloklab, ularni ochish uchun pul talab qilish;

Jinoyatlarni tezkor va keng ko‘lamda sodir etish imkoniyati: Raqamli texnologiyalar orqali tovlamachilik jinoyatlari tez tarqaladi va keng auditoriyaga ta’sir ko‘rsatishi mumkin.

Raqamli texnologiyalar orqali sodir etiladigan tovlamachilik jinoyatlari jamiyatga katta zarar keltiradi, shaxsiy xavfsizlikni va moliyaviy manfaatlarni ta’minlashni murakkablashtiradi. Shu bois, ularga qarshi kurashish uchun huquqiy bazani takomillashtirish, kiberxavfsizlikni ta’minlash va jamoatchilik o‘rtasida profilaktika ishlarini kuchaytirish zarur.

Tovlamachilik jinoyatlarini axborot texnologiyalaridan foydalanib amalga oshirish bugungi kunda keng tarqalib, shaxsiy va korporativ ma’lumotlar xavfsizligiga jiddiy tahdid solmoqda. O‘zbekiston Respublikasining Jinoyat kodeksi 165-moddasi hamda “Axborotlashtirish to‘g‘risida”gi Qonunlarida axborot xavfsizligini ta’minlash masalalari yoritilgan bo‘lsa-da, raqamli jinoyatchilikning murakkabligi ushbu sohada chuqurroq tadqiqotlar o‘tkazishni taqozo etmoqda. Tovlamachilikning yangi shakllari

— ijtimoiy tarmoqlar, elektron pochta, messenjerlar orqali tahdid qilish, nojo‘ya kontentlar tarqatish kabi holatlar kiberxavfsizlikni kuchaytirish zaruratini keltirib chiqarmoqda. Ushbu maqolani yoritish jarayonida dastavval “tovlamachilik”, “kiberjinoyatchilik” so‘zining terminologik tushunchalariga to‘xtalib o‘tishimiz va ularning mazmunini tushunib olishimiz maqsadga muvofiqdir, negaki ijtimoiy va boshqa yuridik adabiyotlarda mazkur terminlar turlicha talqin qilinadi. Jumladan, “tovlamachilik” deganda, jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish, uni sharmanda qiladigan uydirmalar tarqatish bilan qo‘rqitib mulk talab qilish tushuniladi. Mobil qurilmalar hamda ijtimoiy tarmoq va messenjerlardagi akkaunt yoki kanallarga zararli dastur yuborish yo‘li bilan bloklab (to‘sib) qo‘yish, ma’lumotlarini o‘chirib yuborish, o‘zgartirish yoki olib qo‘yish bilan qo‘rqitib shaxslardan pul yoki boshqa moddiy manfaatdorlik talab qilish holatlari kuzatilmoqda.

Har qanday holatda ham tovlamachilik qurboni – bu muayyan talab bilan tahdid qilingan jismoniy yoki yuridik shaxsdir. Ma’lumki, ularning aksariyati bu borada huquqni muhofaza qiluvchi organlarga murojaat qilishni afzal ko‘rmaydi. Tovlamachilik o‘zgadan mulkni yoki mulkiy huquqni topshirishni, mulkiy manfaatlar berishni yoxud mulkiy yo‘sindagi harakatlar sodir etishni talab qilishdan iborat. Ya’ni:

- jabrlanuvchi yoki uning yaqin kishilariga zo‘rlik ishlatish bilan qo‘rqitish; - mulkka shikast yetkazish yoki uni nobud qilish bilan qo‘rqitish;

- (jabrlanuvchi yoki uning yaqinlari uchun) sir saqlanishi lozim bo‘lgan ma’lumotlarni oshkor qilish bilan qo‘rqitish;

- jabrlanuvchini o‘z mulki yoki mulkka bo‘lgan huquqini berishga majbur qiladigan sharoitga solib qo‘yish tovlamachilikni sodir etish hisoblanadi.

Tovlamachining talablari og‘zaki, telefon, faks, xat orqali va boshqa usullarda amalga oshirilishi mumkin. Jabrlanuvchi shaxsning asosiy alomatlari quyidagilardan iborat:

-Jinoyatga nisbatan zaiflik – ya’ni zarur belgilar mavjudligi (ko‘pincha bu to‘lovga qodirlik, yuqori obro‘ va jinsiy tovlamachilik holatlarida – jins va jinsiy xususiyatlar);

-Zaiflik – ya’ni jismoniy yoki ma’naviy jihatdan zaif bo‘lish , tovlamachiga samarali qarshilik ko‘rsata olmaslik (ko‘plab hodisalar anonim bo‘ladi, jabrlanuvchiga juda kam vaqt beriladi, transchegaraviy xususiyatlar mavjud bo‘ladi, ya’ni jinoyatchilar jabrlanuvchidan yoki unga tegishli huquqni muhofaza qiluvchi organlardan uzoqda joylashgan bo‘ladi).

-Yuqori darajadagi internet faolligi. Onlayn tarmoqlarda faol bo‘lgan shaxslar (ayniqsa, ijtimoiy tarmoqlarda) haqida ko‘p miqdorda axborot mavjud bo‘lgani sababli, ular osongina aniqlanadi va nishonga olinadi.

-Huquqiy va texnik himoyaning pastligi. Ko‘pchilik jabrlanuvchilar axborot xavfsizligi bo‘yicha yetarli bilim va vositalarga ega emas, bu esa ularni oson nishonga aylantiradi.

- Jabrlanuvchi osonlik bilan tahdid ostida qoladigan, tarqatilishi mumkin bo‘lgan shaxsiy yoki maxfiy ma’lumotlarga ega bo‘ladi.

Tovlamachilikdagi qo‘rqitishga quyidagi:

birinchidan, o‘zida jabrlanuvchi yoki uning yaqin qarindoshlariga nisbatan zo‘rlik ishlatish, mulkka zarar yetkazish yoxud ular uchun sir saqlanishi lozim bo‘lgan ma’lumotlarni oshkor qilish niyati bildirilgan bo‘lishi;

ikkinchidan, tahdid real, ya’ni agar jabrlanuvchi, tovlamachining talablarini bajarmasa tahdid amalga oshirilishi mumkinligidan xavotir bo‘lishi kerakligi kabi alomatlarga ega bo‘lishi lozim.

Axborot-kommunikatsiya texnologiyalarining global miqyosda keng qo‘llanilishi kiberjinoyatchilik, xususan, tovlamachilikning yangi shakllarini yuzaga keltirdi; bu holatda jinoyatchilar jabrlanuvchining shaxsiy yoki tijorat ma’lumotlarini noqonuniy yo‘l bilan qo‘lga kiritib, ularni fosh qilish tahdidi ostida moliyaviy yoki boshqa turdagi manfaatlarni talab qilishadi. Bunday holatlar, ayniqsa, ma’lumotlar bazalarining yetarli darajada himoyalanmaganligi, foydalanuvchilarning kiberhujumlarga tayyor emasligi va xalqaro huquqiy mexanizmlarning to‘liq ishlamasligi sababli tez-tez sodir bo‘lmoqda.

Tovlamachilik jinoyatini kiber hujumchilar turli usullar orqali amalga oshirmoqda:

- Hujumchi qurbonning kompyuter tizimiga zararli dastur kiritadi, bu dastur qurbonning fayllarini shifrlaydi va ularni ochish uchun to‘lov (odatda kriptovalyutalarda) talab qiladi. Agar qurbon to‘lovni amalga oshirmasa, ularning ma’lumotlari o‘chiriladi yoki umumiy foydalanishga beriladi. Bu hujum asosan yirik biznes va korxonalarga uyushtiriladi.

-DoS hujumi – hujum qilinayotgan server ni faoliyatini vaqtinchalik to‘xtatib qo‘yish. Bunda hujum qiluvchi nishondagi mavjud xatoliklardan foydalanib unga maxsus noto‘g‘ri so‘rovlar orqali murojaat qilib buffer to‘lishini yuzaga keltiradi.

-Kiber shantaj va ma’lumotlarni o‘g‘irlash: Xakerlar shaxsiy yoki korporativ ma’lumotlarni o‘g‘irlab, ular bilan shantaj qilishadi. Ma’lumotlar tarqatilishi yoki sotilishi bilan tahdid qilinadi, agar qurbon to‘lovni amalga oshirmasa.

-Doxing hujumi -bu qurbonning shaxsiy yoki maxfiy ma’lumotlarini, masalan, uy manzili, telefon raqami yoki bank ma’lumotlarini kashf qilish yoki ommaga oshkor qilishni anglatadi, odatda zarar yoki bezovtalik keltirish maqsadida. Agar hakkerning talablariga amal qilmasa, extortsionistlar ma’lum shaxslar yoki guruhlar ustidan doxing tahdidlarini kiritishlari mumkin. Tovlamachilik – bu jinoyat talablari qo‘yilgan paytdan boshlab sodir etilgan jinoyat deb hisoblanadi. Tovlamachilik uchun jazoni og‘irlashtiruvchi holatlar quyidagilar: jinoyatni oldindan til biriktirgan guruh tomonidan sodir etilishi; zo‘ravonlik qo‘llanilishi; katta miqdorda sodir etilishi; uyushgan jinoiy guruh tomonidan juda katta miqdorda mulkni qo‘lga kiritish maqsadida sodir etilishi; jabrlanuvchiga og‘ir tan jarohati yetkazilishi.

Tovlamachilik bilan yuzma-yuz kelganda eng muhim qoidalar quyidagilar: tovlamachi bilan bog‘lanmaslik, muzokara qilmaslik, unga qo‘ng‘iroq qilmaslik yoki xat yozmaslik va eng asosiysi – unga pul yubormaslik. Nega tovlamachilarga pul to‘lash mumkin emas: Birinchidan, jinoyatchi o‘z va’dasini bajarishiga hech qanday kafolat yo‘q. Ikkinchidan, siz pul yuborsangiz, jinoyatchiga bu narsa siz uchun juda muhim ekanini ko‘rsatasiz. Uchinchidan, siz ularning talablariga bo‘ysunsangiz, ular yanada ko‘proq pul talab qilishni davom ettiradi va o‘z narxlarini oshiradi.

Internetda tovlamachilik qurboniga aylanmaslik va xavf-xatarni kamaytirish uchun quyidagi asosiy xavfsizlik tavsiyalariga amal qilish zarur:

- ikki bosqichli autentifikatsiyani (ikki faktorli tekshiruvni) qo‘llash;

- zaxira nusxalarini saqlash ya’ni eng kerakli ma’lumotlarni muntazam ravishda zaxiralash, ransomware hujumlari kabi vaziyatlar uchun foydali bo‘ladi.

Agar tizimga hujum qilinsa, zaxira nusxalari yordamida ma’lumotlarni tiklash mumkin.

Kompyuterlar va serverlarga yangi xavfsizlikni ta’minlash yangilanishlarini o‘rnatish, shuningdek, xavfsiz parollarni ishlatish orqali tizimni mustahkamlash lozim; - parollarni qayta-qayta ishlatishdan saqlanish, chunki bir hisob qaydnomasi buzilgach, kiberjinoyatchilar boshqa barcha hisoblarga ham kirish imkoniyatiga ega bo‘lishi mumkin; -zararlangan elektron pochta ilovalari va havolalaridan ehtiyot bo‘lish: Phishing xabarlari orqali zararli dasturlarni tarqatish keng tarqalgan. Elektron pochta ilovalarini va havolalarni ochishda ehtiyot bo‘lish, noma’lum manbalardan kelgan xabarlarga ishonmaslik zarur. - murakkab va kam ma’lum bo‘lgan iboralardan tashkil topgan ishonchli parollardan foydalanish; -shaxsiy va korporativ ma’lumotlarni himoya qilish. Eng asosiysi shaxsiy ma’lumotlarni internetda kamroq oshkor qilish, ijtimoiy tarmoqlarda ehtiyotkorlik bilan bo‘lishish, ma’lumotlar bazasining xavfsizligini ta’minlash juda muhim.

Shantaj, zo‘ravonlik va extortsion har kimga, ayniqsa bolalarga jiddiy zarar etkazishi mumkin. Bu holatlarda qurbonlar psixologik travma, o‘ziga zarar yetkazish yoki yanada og‘irroq holatga duchor bo‘lishi mumkin. Har qanday tergovchining maqsadi — bu qurbonlarga yordam berish va ularga kerakli qo‘llab-quvvatlashni taqdim etishdir. Shuning uchun bu juda muhimdir.Stable Diffusion kabi vositalar onlayn muhitni tubdan o‘zgartirib yubordi va ular yangi, to‘liq o‘zgacha qiyinchiliklarni keltiradi. Masalan, yaratilgan tasvirlar har qachongidan ham realistik bo‘lib borayotgani, tergovchilarga bu tasvirlarning qurboni mavjudligini aniqlashni juda qiyinlashtiradi.

Xulosa qilib aytadigan bo‘lsak, axborot texnologiyalari yordamida sodir etiladigan tovlama jinoyatlari hozirgi kunda global muammoga aylangan. Mazkur jinoyatlarning oldini olish uchun, birinchidan, axborot tizimlarining muntazam yangilanishini ta’minlash, ikkinchidan, foydalanuvchilarni kiberxavfsizlikning asosiy prinsiplari bo‘yicha o‘qitish, uchinchidan esa, xalqaro axborot xavfsizligi standartlarini joriy etish zarur. Shuningdek, yuridik shaxslar darajasida maxfiy ma’lumotlarga doir siyosatlarni

ishlab chiqish va huquqni muhofaza qiluvchi organlar bilan tezkor axborot almashinuvini yo‘lga qo‘yish kiber tovlamachilikning ijtimoiy xavfini kamaytiradi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoevning O‘zbekiston Respublikasi davlat mustaqilligining o‘ttiz to‘rt yilligiga bag‘ishlangan tantanali marosimdagi nutqi. https://president.uz/uz/lists/view/8440.

2. O‘zbekiston Respublikasining 2024 yil 14 noyabrdagi “Bolalarni zo‘ravonlikning barcha shakllaridan himoya qilish to‘g‘risida”gi O‘RQ-996-son qonuni.

3. O‘zbekiston Respublikasi Prezidentining 2023 yil 21 dekabrdagi «Mahalla institutining jamiyatdagi rolini tubdan oshirish va uning aholi muammolarini hal etishda birinchi bo‘g‘in sifatida ishlashini ta’minlashga qaratilgan chora-tadbirlar to‘g‘risida» PF-209-son Farmoni.

4. Таштемиров А. А. Ахборот технологиялари орқали содир этиладиган жиноятларни фош этишнинг ҳуқуқий ва ташкилий жиҳатлари //World of Science. – 2023. – Т. 6. – №. 6. – С. 169-175.

5. Таштемиров А., Курчибоев Ж. Вояга етмаганлар ҳуқуқбузарлигининг профилактикасида таълим ва тарбиянинг ўрни ва аҳамияти //Евразийский журнал права, финансов и прикладных наук. – 2023. – Т. 3. – №. 12. – С. 130-135.

6. Таштемиров А. А., Калауов С. А. Йўл ҳаракати хавфсизлиги ривожланиш концепциясининг истиқболлари ва киберхавфсизлигини таъминлаш зарурати //barqarorlik va etakchi tadqiqotlar onlayn ilmiy jurnali. – 2022. – Т. 2. – №. 8. – С. 245-250.

7. Таштемиров А. А. и др. Ижтимоий тармоқлар орқали содир этилаётган жиноятларга қарши курашиш чора-тадбирлари //Models and methods for increasing the efficiency of innovative research. – 2023. – Т. 2. – №. 21. – С. 24-31.

8. Таштемиров А. А. и др. Ижтимоий профилактика объекти сифатида алкоголизм таъсиридаги шахслар билан ишлаш фаолиятини такомиллаштириш //So ‘ngi ilmiy tadqiqotlar nazariyasi. – 2023. – Т. 6. – №. 12. – С. 552-558.

9. Tashtemirov A., Po‘latov A. Ayollar jinoyatchiligining oldini olish chora-tadbirlari //Инновatsионные исследования в науке. – 2024. – Т. 3. – №. 1. – С. 75-78.

10. Таштемиров А., Нурматов Н. Айрим хорижий давлатларнинг тезкор қидирув фаолиятида соҳавий ҳамкорликнинг таҳлили //Инновatsионные исследования в науке. – 2024. – Т. 3. – №. 5. – С. 190-197.

11. Таштемиров А. А. и др. Зўравонлик билан боғлиқ ҳуқуқбузарликлар профилактикаси тушунчаси ва ўзига хослиги //Innovative achievements in science 2024. – 2025. – Т. 4. – №. 37. – С. 82-90.