INTERNETDAGI TOVLAMACHILIK: ZAMONAVIY TAHDIDLAR VA ULARGA QARSHI KURASH

Ilhomjon Abdullayev
IIV Akademiyasi kursanti

Annotatsiya: *Internet texnologiyalarining jadal rivojlanishi inson hayotining barcha sohalariga ijobiy ta’sir ko‘rsatayotgan bo‘lsa-da, u bilan birga yangi xavf-xatarlar, xususan raqamli tovlamachilik (cyber extortion) kabi jinoyatlarning paydo bo‘lishiga ham sabab bo‘lmoqda. Ushbu maqolada internetdagi tovlamachilik holatlari, ularning zamonaviy shakllari, psixologik, texnologik va ijtimoiy jihatlari chuqur o‘rganilgan. Tovlamachilik jinoyati o‘z mohiyati jihatidan boshqa shaxs yoki tashkilotga nisbatan qo‘rqitish, tahdid yoki shantaj orqali moliyaviy foyda yoki boshqa manfaatni qo‘lga kiritishga qaratilgan bo‘lib, internet muhitida u yanada murakkab va yashirin shakllarda amalga oshirilmoqda. Maqolada internetda amalga oshiriladigan tovlamachilik turlariga, jumladan, seks-tovlamachilik (sextortion), ransomware, DDoS tahdidlari orqali tovlamachilik, shaxsiy ma’lumotlar bilan bog‘liq tahdidlar, kompaniyalarga nisbatan korporativ tovlamachilik va boshqa shakllariga alohida e’tibor qaratilgan. Bu jinoyatlarda jinoyatchilar ko‘pincha texnik jihatdan ilg‘or vositalardan foydalanadilar, masalan, anonimlashtiruvchi dasturlar, kriptovalyuta orqali to‘lovlar, yoki feyk akkauntlar orqali tahdidlar yuborish kabi usullar. Bundan tashqari, maqolada jabrlanuvchilarning psixologik holati, ularning tovlamachilarning bosimiga qanday javob berishi, va tovlamachilikka qarshi immunitet qanday shakllanishi mumkinligi tahlil etilgan. Shu bilan birga, hukumat va nodavlat tashkilotlarning kiberjinoyatchilikka qarshi kurashdagi roli, xalqaro tajribalar, raqamli xavfsizlikni ta’minlashda ilg‘or amaliyotlar keltirilgan. Kiber xavfsizlik bo‘yicha profilaktika choralari, xususan, ijtimoiy muhofaza, ta’lim va axborot texnologiyalari sohasi mutaxassislarini jalb etish zarurati alohida ta’kidlangan. Tadqiqotlar shuni ko‘rsatadiki, kiber jinoyatchilik tobora ko‘proq tashkillashtirilgan xarakterga ega bo‘lib bormoqda, u transmilliy xususiyatga ega bo‘lib, faqat bir davlat chegarasida uni aniqlash yoki jazolash deyarli imkonsizdir. Shu sababli maqolada internetdagi tovlamachilikka qarshi kurashda xalqaro hamkorlik, huquqiy mexanizmlarni uyg‘unlashtirish va ma’lumot almashinuvining ahamiyati keng yoritilgan. Umuman olganda, bu maqola raqamli xavfsizlik sohasidagi tahdidlarni anglash, foydalanuvchilarni xabardor qilish, va muhim qarorlar qabul qilish uchun ilmiy-amaliy asos bo‘lib xizmat qiladi.*

Kalit so’zlar: *Internetdagi tovlamachilik, raqamli xavfsizlik, kiber jinoyat, shantaj, sextortion, ransomware, psixologik bosim, axborot tahdidi, xalqaro hamkorlik, jabrlanuvchi himoyasi*

Аннотация: *Бурное развитие интернет-технологий, с одной стороны, открывает перед человечеством новые возможности, а с другой — порождает новые угрозы, среди которых особое место занимает интернет-рэкет (цифровой шантаж). В данной статье рассматриваются современные формы интернет-*

рэкета, его психологические, технологические и социальные аспекты. Речь идёт о преступлениях, в которых злоумышленники добиваются материальной выгоды или других интересов путём угроз, шантажа и психологического давления, используя интернет как основную платформу для воздействия. Особое внимание уделено таким видам цифрового шантажа, как сексуальный шантаж (sextortion), программы-вымогатели (ransomware), угрозы DDoS-атак, корпоративный шантаж, а также шантаж, связанный с утечкой личных данных. В современных условиях преступники всё чаще используют анонимайзеры, криптовалюту и фальшивые аккаунты, что значительно усложняет их выявление. Анализируется психологическое состояние жертв, механизмы манипуляции и внушения страха, а также способы формирования устойчивости к давлению со стороны преступников. Рассматриваются стратегии борьбы с интернет-рэкетом как на уровне частных лиц, так и со стороны государственных структур, неправительственных организаций и международных институтов. Также приведены примеры передовых практик обеспечения кибербезопасности, в том числе профилактика, повышение цифровой грамотности населения и обучение специалистов. Одной из ключевых идей статьи является то, что интернет-рэкет всё чаще приобретает организованный и транснациональный характер, требующий скоординированных международных усилий. Авторы подчёркивают важность сотрудничества между странами, гармонизации законодательств и систем обмена информацией. В целом, статья представляет собой научно-практическую основу для понимания цифровых угроз и формирования эффективных механизмов защиты в условиях современной информационной среды.

Ключевые слова: *Интернет-рэкет, цифровая безопасность, киберпреступность, шантаж, сексуальный шантаж, программы-вымогатели, психологическое давление, информационные угрозы, международное сотрудничество, защита жертв*

Abstract: *The rapid advancement of internet technologies has brought immense benefits to various spheres of human life, yet it has also given rise to new threats, particularly in the form of digital extortion or cyber extortion. This article explores the phenomenon of online extortion in depth, analyzing its modern forms, psychological mechanisms, technological tools, and social impact. Cyber extortion involves coercing individuals or organizations into providing financial or other benefits through threats, intimidation, or blackmail, all facilitated via digital platforms. The article outlines various forms of internet extortion including sextortion, ransomware attacks, DDoS-based blackmail, threats involving the exposure of personal data, and corporate-level digital extortion. Cybercriminals are increasingly using advanced tools such as anonymizing software, cryptocurrency payments, and fake social media profiles to evade detection and enhance their leverage. Furthermore, the article delves into the psychological state of victims, examining how they respond to digital threats, the emotional toll they suffer, and how psychological resilience to such pressure can be developed. It highlights the role of*

governments, NGOs, and cybersecurity organizations in combating cyber extortion and promoting digital safety. The discussion includes best practices for prevention, awareness-building, education, and cross-sector collaboration. Studies show that cyber extortion is becoming more organized and transnational in nature, making it difficult to address within a single national jurisdiction. Therefore, the article stresses the need for international cooperation, legal harmonization, and timely information exchange. Overall, this paper serves as a comprehensive academic and practical resource to better understand online threats, raise public awareness, and develop informed strategies to enhance cybersecurity in the digital age.

Key words: *Cyber extortion, digital security, cybercrime, blackmail, sextortion, ransomware, psychological pressure, information threats, international cooperation, victim protection*

KIRISH

So‘nggi o‘n yilliklar ichida internet texnologiyalarining keskin rivojlanishi insoniyat hayotining barcha sohalarini tubdan o‘zgartirib yubordi. Bugungi kunda internet nafaqat axborot almashinuvi, muloqot va ta’lim vositasi, balki moliyaviy operatsiyalar, biznes yuritish va davlat boshqaruvida ham asosiy infratuzilmaga aylanib bormoqda. Shu bilan birga, bu raqamli inqilob insoniyat uchun yangi xavf-xatarlarni, xususan, kiber jinoyatlar va ular orasida eng xavflilaridan biri bo‘lgan internetdagi tovlamachilik (cyber extortion) kabi tahdidlarni yuzaga keltirmoqda. Tovlamachilik — bu ma’lum shaxs yoki tashkilotni tahdid, qo‘rqitish, shantaj yoki boshqa yo‘llar bilan moliyaviy yoki boshqa manfaatli imtiyozlar olish maqsadida bosim ostida ushlab turishdir. An’anaviy shakllarda bu jinoyat asosan jismoniy bosim, shaxsiy uchrashuvlar yoki telefon qo‘ng‘iroqlari orqali amalga oshirilgan bo‘lsa, bugungi raqamli asrda bu jinoyat turi internet orqali, anonim va yashirin shakllarda amalga oshirilmoqda. Bu esa jinoyatni aniqlash, huquqiy javobgarlikni ta’minlash va jabrlanuvchini himoya qilishni yanada murakkablashtiradi. Internet orqali amalga oshirilayotgan tovlamachilik jinoyatlarining xilma-xilligi yildan yilga oshib bormoqda. Masalan, sextortion (ya’ni, jinsiy xarakterdagi materiallar bilan tahdid qilish), ransomware (kompyuter tizimlarini bloklab, ma’lumotlarni tiklash evaziga to‘lov talab qilish), DDoS hujumlari orqali tovlamachilik, shaxsiy ma’lumotlarni fosh qilish bilan tahdid qilish, kompaniya yoki tashkilot rahbariyatiga qarshi shantaj kabi holatlar kiber jinoyatlarning eng keng tarqalgan shakllariga aylanmoqda. Bunday jinoyatlar nafaqat yirik kompaniyalar va davlat tashkilotlari, balki oddiy internet foydalanuvchilari uchun ham jiddiy tahdid bo‘lib qolmoqda. Kiber jinoyatchilar, odatda, texnologiyalardan yuqori darajada xabardor bo‘lib, tarmoqdagi xavfsizlik bo‘shliqlarini mohirona aniqlay oladi. Ular maxfiylikni saqlash uchun turli anonimlashtiruvchi vositalar, masalan, Tor tarmog‘i, VPN, virtual pochta qutilari va kriptovalyutalar (ayniqsa Bitcoin) orqali to‘lovlarni amalga oshirishni talab qiladilar. Bu holat ularni aniqlash va qonuniy javobgarlikka tortishni murakkablashtiradi. Shu sababli internetdagi tovlamachilik nafaqat texnik va huquqiy, balki psixologik va sotsiologik tahlilni ham talab qiladigan ko‘p qirrali muammodir. Afsuski, bu jinoyat turining psixologik jihatlari ko‘pincha yetarli darajada o‘rganilmaydi. Tovlamachilar ko‘pincha

jabrlanuvchining ruhiy zaif tomonlarini aniqlab, ularni qo‘rqitish, sharmandali ma’lumotlarni tarqatish bilan tahdid qilish yoki oila va yaqinlariga zarar yetkazishni aytish orqali boshqaradilar. Jabrlanuvchilar esa ko‘pincha stress, xavotir, o‘zini aybdor his qilish, ijtimoiy izolyatsiya va hatto depressiya holatiga tushib qoladilar. Ko‘pchilik bu kabi tahdidlarga huquq-tartibot organlariga murojaat qilmasdan, o‘z-o‘zini ayblash holatida yakkalanib qoladi. Mazkur maqola aynan mana shu muammo — internetdagi tovlamachilikning zamonaviy shakllari, ularning psixologik va texnologik asoslari, jabrlanuvchilar holati, huquqiy mexanizmlar va ularga qarshi samarali kurash yo‘llarini o‘rganishga bag‘ishlangan. Maqolada quyidagi ilmiy savollarga javob izlanadi: internetdagi tovlamachilikning asosiy turlari qanday? Jinoyatchilar qanday psixologik va texnologik strategiyalardan foydalanadi? Jabrlanuvchilar qanday zaifliklarga ega? Qanday oldini olish va profilaktika choralarini ishlab chiqish mumkin? Ushbu savollarga javob berish orqali maqola raqamli xavfsizlikni ta’minlash, axborot texnologiyalari sohasida profilaktika strategiyalarini ishlab chiqish hamda ijtimoiy ongni oshirishga hissa qo‘shadi. Shuningdek, maqolada xalqaro tajriba va milliy qonunchilik tahlil qilinib, kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikning o‘rni ham muhokama qilinadi. Raqamli xavfsizlikka oid siyosatni ishlab chiqishda multidisiplinar (psixologiya, kriminologiya, IT, huquqshunoslik) yondashuv zarurati alohida ta’kidlanadi. Umuman olganda, kirish qismidagi tahlillar internetdagi tovlamachilik muammosining dolzarbligi, uning ko‘p qirrali va chuqur ijtimoiy-psixologik ildizlari mavjudligini ko‘rsatadi. Maqolaning keyingi boblarida mazkur holatga tegishli ilmiy izlanishlar, empirik dalillar va taklif etilayotgan strategiyalar keng yoritiladi.

ASOSIY QISM

Internetdagi tovlamachilik (cyber extortion) — bu axborot texnologiyalarining rivojlanishi bilan birgalikda kiberjinoyatlarning o‘ziga xos va xavfli shaklini tashkil qilmoqda. Tovlamachilikning internetda yuzaga kelgan shakllari boshqa jinoyatlardan farq qiladi, chunki bu jinoyatlar asosan raqamli muhitda amalga oshiriladi va jinoyatchilar ko‘pincha o‘z shaxsini yashirib, anonim ravishda hujumlar uyushtiradilar. Internet orqali amalga oshiriladigan tovlamachilikning ayrim turlari an’anaviy jinoyatlar bilan o‘xshashlik ko‘rsatsa-da, ularning texnologik yondoshuv va usullari boshqa — yanada ilg‘or va qiyin aniqlanadigan xususiyatlarga ega.

1. Sextortion (seks-tovlamachilik)

Sextortion — bu jinsiy xarakterdagi materiallar yordamida insonlarni qo‘rqitish yoki shantaj qilishning internetda yuzaga kelgan shaklidir. Bu turdagi tovlamachilikda jinoyatchilar odatda jabrlanuvchilardan shaxsiy ma’lumotlarni yoki maxfiy rasmlarni olishadi, keyinchalik esa bu materiallar bilan tahdid qilib, moliyaviy yoki boshqa manfaatlarni talab qilishadi. Bunday jinoyatlar ko‘pincha yoshlar va kattalar orasida uchraydi va ko‘plab hollarda jabrlanuvchilar jismoniy yoki ruhiy bosim ostida qoladilar. Jinoyatchilar, shuningdek, internetda anonim bo‘lish imkoniyatini yaxshi biladilar, shuning uchun ularning shaxsini aniqlash juda qiyin bo‘ladi. Shaxsiy rasmlar yoki videolarni tarqatish bilan tahdid qilish, jabrlanuvchilarni psixologik jihatdan zaiflashtiradi va

ko‘pincha ular huquq-tartibot organlariga murojaat qilishdan qochadilar, chunki o‘zlari aybdor bo‘lib qolishdan qo‘rqishadi.

2. Ransomware (yopiq dastur orqali tovlamachilik)

Ransomware — bu foydalanuvchi kompyuter tizimlarini yoki ma’lumotlarni qulflash, so‘ngra uni tiklash uchun to‘lov talab qilishni o‘z ichiga olgan bir turdagi tovlamachilikdir. Ransomware hujumlari nafaqat individual foydalanuvchilar, balki yirik korporatsiyalar, davlat idoralari va tibbiyot tashkilotlarini ham nishonga olishga moyil. Bu jinoyatlar ko‘pincha shifrlash texnologiyalaridan foydalangan holda amalga oshiriladi. Jinoyatchilar kompyuter tizimlarini bloklab, ma’lumotlarga kirishni cheklaydi va foydalanuvchilardan kriptovalyuta kabi anonim to‘lov shakllarini talab qiladi. Bunday hujumlar global miqyosda keng tarqalgan va ko‘plab tashkilotlar uchun katta moliyaviy zararlarga olib keladi. Tibbiyot sohasidagi kompaniyalar, masalan, bemorlar haqida ma’lumotlarni saqlaydigan tibbiyot tashkilotlari, xavf ostida bo‘lgan sektorlarning biri hisoblanadi. Ransomware orqali amalga oshiriladigan tovlamachilikda jabrlanuvchilar ko‘pincha ikkilanishadi — tizimni tiklashga majbur bo‘lishadi yoki to‘lovni amalga oshiradilar, bu esa nafaqat material zarar, balki katta ijtimoiy ishonch yo‘qotilishiga ham olib keladi.

3. DDoS hujumlari orqali tovlamachilik

DDoS (Distributed Denial of Service) hujumlari internet tarmog‘idagi xizmatni to‘xtatish yoki unga kira olmaslik holatini yaratish uchun amalga oshiriladi. Bunday hujumlar orqali jinoyatchilar ma’lum bir tizim yoki xizmatga kirishni bloklab, undan qaytarib olish uchun to‘lov talab qilishadi. Bu usulda jinoyatchilar ko‘plab kompyuterlarni birlashtirib, internet orqali ma’lum bir xizmatga hujum qiladi. Bu kabi hujumlar ko‘pincha katta miqdordagi ma’lumotlarni tarqatish orqali tizimni to‘liq ishlamas holatiga keltiradi, shu bilan birga xizmatni to‘xtatish orqali tashkilotlardan pul talab qilinadi.

4. Shaxsiy ma’lumotlarni fosh qilish orqali tovlamachilik

Shaxsiy ma’lumotlarni fosh qilish bilan bog‘liq tovlamachilik so‘nggi yillarda juda keng tarqalgan. Jinoyatchilar o‘z qurbonlaridan shaxsiy ma’lumotlarni to‘plash orqali, ularni noqonuniy ravishda tarqatish yoki ular bilan tahdid qilishadi. Bu ma’lumotlar turli shakllarda bo‘lishi mumkin — kredit kartalari raqamlari, pasport ma’lumotlari, elektron pochta manzillari yoki hatto shaxsiy foto va videolar. Jabrlanuvchilar bunday ma’lumotlarning tarqatilishidan qo‘rqib, ko‘pincha to‘lovni amalga oshiradilar.

5. Internetdagi tovlamachilikka qarshi kurashish choralar

Internetdagi tovlamachilikka qarshi kurashishda eng muhim masalalardan biri – foydalanuvchilarni ogoh qilishdir. Kiber xavfsizlikning yuqori darajadagi darajasini ta’minlash, xavfsizlik dasturlaridan foydalanish, kuchli parollar yaratish va onlayn xavfsizlikni ta’minlovchi yondoshuvlarni rivojlantirish muhim ahamiyatga ega. Shu bilan birga, huquqiy mexanizmlar ham alohida e’tibor talab etadi. Xalqaro hamkorlik, kiber jinoyatlarni oldini olish uchun yagona standartlarni yaratish va ularga amal qilish zarur. Internetdagi tovlamachilikka qarshi kurashishda hukumatlar, maxsus organlar va ijtimoiy tashkilotlar o‘rtasida hamkorlik alohida ahamiyatga ega. Tovlamachilikka qarshi kurashda xalqaro hamkorlikni rivojlantirish, kiber xavfsizlikka oid qonunchilikni mustahkamlash,

ma’lumotlarning maxfiyligini ta’minlash va foydalanuvchilarni xabardor qilish zarurati doimiy ravishda ta’kidlanadi.

XULOSA

Internetning jadal rivojlanishi bilan birgalikda kiber jinoyatlar, xususan, internetdagi tovlamachilik (cyber extortion) xavfi sezilarli darajada oshdi. Ushbu jinoyat turi hozirgi kunda nafaqat individual foydalanuvchilar, balki yirik tashkilotlar va davlat idoralari uchun ham katta tahdidlarga aylangan. Internetdagi tovlamachilik an’anaviy shantaj va tovlamachilik usullarining yangi, raqamli shakllari bo‘lib, ularning texnologik va psixologik jihatlari jiddiy tahlilni talab qiladi. Maqolada, avvalo, internetdagi tovlamachilikning turli shakllari va ularga qarshi kurashishning samarali yo‘llari o‘rganildi. Bunday jinoyatlar nafaqat texnologik jihatlarni, balki insonlarning psixologik zaifliklarini ham hisobga olgan holda amalga oshiriladi. Tovlamachilikning internetda ko‘rish mumkin bo‘lgan shakllari, jumladan, sextortion (seksual shantaj), ransomware (kompyuter tizimlarini qulflash va ma’lumotlarni tiklash evaziga to‘lov talab qilish), DDoS hujumlari orqali amalga oshiriladigan tovlamachilik, shaxsiy ma’lumotlarni fosh qilish bilan bog‘liq shantaj, — bularning har biri o‘ziga xos xususiyatlarga ega va har biri alohida tahlilni talab etadi. Sextortion kabi jinsiy xarakterdagi materiallar bilan tahdid qilish, ayniqsa, yoshlar orasida ko‘plab qiyinchiliklar va ruhiy salomatlikka ta’sir qiluvchi omillarni keltirib chiqaradi. Bunday jinoyatlar ko‘plab jabrlanuvchilarni ijtimoiy izolyatsiya va psixologik bosim ostida qoldiradi, ularning ko‘pchiligi sharmandalikdan qo‘rqib huquq-tartibot organlariga murojaat qilmaslikka harakat qiladi. Ransomware hujumlari esa tashkilotlarga katta moliyaviy zarar yetkazish bilan birga, ma’lumotlar xavfsizligini ta’minlashda muhim ahamiyatga ega bo‘lgan muammolarni keltirib chiqaradi. Bunday hujumlar tufayli foydalanuvchilar hamda kompaniyalar ko‘plab noxush holatlarga duch kelishadi va ko‘pincha jinoyatchilarga to‘lovni amalga oshiradilar, bu esa xavfli aylanma tizimlarni yaratadi. Bundan tashqari, shaxsiy ma’lumotlarni fosh qilish va DDoS hujumlari orqali amalga oshiriladigan tovlamachilik turli yo‘llar bilan jinoyatkorlar tomonidan qo‘llaniladi. Jinoyatchilar bu usullardan foydalangan holda jabrlanuvchilarni ko‘pincha psixologik jihatdan zo‘rlashadi, ularni qo‘rqitishadi va moliyaviy manfaat olishni maqsad qiladilar. Jabrlanuvchilar o‘zlarining shaxsiy ma’lumotlari tarqatilishidan, ijtimoiy obro‘dan ayrilishidan qo‘rqib, ko‘pincha jinoyatchilarga to‘lov qilishga rozi bo‘ladi. Ushbu holatlar nafaqat shaxsiy xavfsizlikni, balki umumiy ijtimoiy muhitni ham buzadi. Internetdagi tovlamachilikning texnologik rivojlanishi bu jinoyatlarning yanada kuchayishiga olib kelmoqda. Kompyuter tizimlarining xavfsizligi, foydalanuvchi ma’lumotlarini himoya qilish, shaxsiy ma’lumotlarni xavfsiz saqlash, xavfsizlik dasturlaridan samarali foydalanish — bu kabi masalalar nafaqat shaxsiy xavfsizlikni ta’minlash, balki jamiyatni kiberjinoyatlarga qarshi kurashish bo‘yicha targ‘ib qilishning muhim omillaridan biridir. Kiber xavfsizlik sohasidagi yangi texnologiyalar va yondashuvlar orqali, ayniqsa, kriptovalyutalar va anonimlashtiruvchi vositalar yordamida amalga oshiriladigan jinoyatlarga qarshi kurashish zarurati yuzaga kelmoqda. Bu texnologiyalar jinoyatchilarning shaxsini yashirish, ularni aniqlashni qiyinlashtirish, shuningdek, jinoyatchilik faoliyatlarini oldini olishni murakkablashtiradi. Shu bilan birga, huquqiy mexanizmlar ham muhim ahamiyatga ega.

Xalqaro hamkorlik, kiber jinoyatlarni oldini olish uchun yagona standartlarni yaratish va ularga amal qilish zarur. Bugungi kunda ko‘plab davlatlar kiberjinoyatlarga qarshi kurashish uchun yangi qonunchilik va huquqiy mexanizmlar ishlab chiqishmoqda, ammo bu boradagi ishlar hali ham davom etmoqda. Xalqaro hamkorlik va o‘zaro tajriba almashish, kiberjinoyatlarga qarshi kurashishda samarali strategiyalarni ishlab chiqishga yordam beradi. Shuningdek, ijtimoiy ongni oshirish va foydalanuvchilarning internet xavfsizligi bo‘yicha bilimlarini yaxshilash zarurati mavjud. Internetdagi tovlamachilikka qarshi kurashishda multidisiplinar yondashuv juda muhimdir. Bu yondashuvda psixologiya, kriminologiya, huquqshunoslik, axborot texnologiyalari va ijtimoiy fanlar mutaxassislarining birgalikdagi faoliyati ko‘rinadi. Jabrlanuvchilarni qo‘llab-quvvatlash, ularning psixologik jihatlarini inobatga olish, xavfsiz va qonuniy muhit yaratish orqali tovlamachilik jinoyatlarining oldini olish mumkin. Bunday yondashuv kiberjinoyatlarga qarshi kurashishda yanada samarali natijalar keltiradi. Umuman olganda, internetdagi tovlamachilik — bu o‘zgarmas va murakkab muammo bo‘lib qolmoqda. Ushbu jinoyatga qarshi kurashishda ilg‘or texnologiyalar, xalqaro hamkorlik, huquqiy mexanizmlar va ijtimoiy ongni oshirishning ahamiyati katta. Foydalanuvchilarni internetda xavfsiz yurish va o‘zlarini himoya qilish bo‘yicha ongli qilish zarur. Kiberjinoyatlarga qarshi kurashishda ko‘p tomonlama yondashuv, ishonchli himoya mexanizmlarini ishlab chiqish va samarali profilaktika strategiyalarini amalga oshirish, shuningdek, zamonaviy texnologiyalardan foydalanishni mustahkamlash lozim.

FOYDALANILGAN ADABIYOTLAR:

1. Brown. T. & Matthews, D. (2020). "Ransomware: A Growing Cyber Threat." International Journal of Information Security, 25(3), 134-148.

Ushbu ilmiy ishda ransomware (yopiq dastur orqali tovlamachilik) turidagi kiberjinoyatlar va ularni oldini olish choralariga alohida e'tibor qaratilgan.

2. Kovacs. E. (2022). "Cybercrime and the Law: Addressing Online Extortion." Global Cybersecurity and Law Review, 8(4), 210-229.

Bu asar kiberjinoyatlarga qarshi huquqiy mexanizmlar va dunyo miqyosidagi qonunlar haqida batafsil tahlil beradi.

3. Jones. S. (2018). "The Role of Technology in Cyber Extortion." Journal of Digital Law, 13(2), 85-100.