KIBERTOVLAMACHILIK JINOYATLARINING PROFILAKTIKASINI TA’MINLASHNING KRIMINOLOGIK, HUQUQIY VA TASHKILIY ASOSLARI

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

Annotatsiya. Ushbu maqolada kibertovlamachilik jinoyatlarining profilaktikasini ta’minlash masalalari kriminologik, jinoyat-huquqiy, tashkiliy va texnologik jihatdan tahlil qilinadi. Tadqiqot O‘zbekiston Respublikasining huquqbuzarliklar profilaktikasi, kiberxavfsizlik, shaxsga doir ma’lumotlar va jinoiy javobgarlikka oid qonunchiligi, xalqaro hujjatlar, xorijiy tajriba, ilmiy maqolalar, doktorlik dissertatsiyalari hamda kiberxavfsizlik bo‘yicha amaliy adabiyotlar asosida olib borilgan. Maqolada kibertovlamachilik profilaktikasi jinoyat sodir etilgandan keyin aybdorni jazolash bilan cheklanmasligi asoslantiriladi. Samarali profilaktika xavf omillarini erta aniqlash, jinoyatchi imkoniyatlarini kamaytirish, potensial jabrlanuvchilarni himoya qilish, raqamli savodxonlikni oshirish, idoralararo hamkorlik, tezkor javob mexanizmlari, raqamli dalillarni saqlab qolish va kiberjinoyatchilik ekotizimini izdan chiqarish choralarini o‘z ichiga olishi kerak. Maqolada routine activity theory, situational crime prevention, cybercriminal profiling, ransomware va double-extortion ransomware bo‘yicha ilmiy ishlar tahliliga alohida e’tibor qaratiladi.

Kalit so‘zlar: kibertovlamachilik, huquqbuzarliklar profilaktikasi, kiberxavfsizlik, ransomware, situatsion profilaktika, routine activity theory, raqamli dalil, shaxsga doir ma’lumotlar, kiberjinoyatchi profili, jabrlanuvchini himoya qilish.

1. Introduction

Kibertovlamachilik jinoyatlarining profilaktikasini ta’minlash masalasi raqamli jamiyat sharoitida alohida dolzarblik kasb etmoqda. An’anaviy jinoyatchilikda profilaktika ko‘proq jismoniy muhit, shaxslararo munosabatlar, nazorat, tarbiya va ijtimoiy shart-sharoitlar bilan bog‘liq bo‘lsa, kibertovlamachilikda jinoyat sodir etilishiga imkon beruvchi omillar raqamli muhitning o‘zida shakllanadi. Zaif parollar, ikki bosqichli autentifikatsiyaning yo‘qligi, xodimlarning phishing xabarlarini ajrata olmasligi, zaxira nusxalarning mavjud emasligi, shaxsiy ma’lumotlarning ehtiyotsiz saqlanishi, platformalarda tezkor shikoyat mexanizmlarining sustligi va jabrlanuvchining sharmandalikdan qo‘rqib murojaat qilmasligi bunday jinoyatlar uchun qulay sharoit yaratadi.

Kibertovlamachilikning xavfi shundaki, jinoyat sodir etilgandan keyin ko‘riladigan choralar ko‘pincha zararni to‘liq tiklay olmaydi. Shaxsiy fotosurat yoki yozishmalar tarqalgan bo‘lsa, ularni internetdan butunlay olib tashlash qiyin. Korxona serverlari ransomware orqali bloklangan bo‘lsa, faoliyatning to‘xtashi mijozlar ishonchi va iqtisodiy barqarorlikka zarar yetkazadi. Ma’lumotlar bazasi o‘g‘irlangan bo‘lsa, hatto tizim tiklanganidan keyin ham ma’lumotlarning oshkor etilishi xavfi saqlanib qoladi. Shu bois kibertovlamachilik profilaktikasi jinoyat sodir etilgandan keyingi jazolash mexanizmi emas, balki jinoyatning oldini olish, jabrlanuvchini himoya qilish va kiberjinoyatchilik imkoniyatlarini kamaytirish tizimi sifatida ko‘rilishi kerak.

O‘zbekiston Respublikasining “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonuni huquqbuzarliklar profilaktikasi sohasidagi munosabatlarni tartibga soladi va profilaktika faoliyatining umumiy asoslarini belgilaydi.[1] Ushbu qonundagi yondashuv kibertovlamachilikka nisbatan ham muhim: profilaktika huquqbuzarliklarning sabablarini va ularga imkon berayotgan shart-sharoitlarni aniqlash hamda bartaraf etishga qaratilishi lozim. Biroq kibertovlamachilikda bunday sabab va shart-sharoitlar faqat ijtimoiy yoki tarbiyaviy omillar bilan cheklanmaydi; ular texnik, tashkiliy, psixologik, huquqiy va xalqaro xususiyatga ega.

Maqolaning maqsadi kibertovlamachilik jinoyatlarining profilaktikasini ta’minlashning kriminologik, huquqiy va tashkiliy asoslarini tahlil qilishdan iborat. Tadqiqotning asosiy savoli quyidagicha qo‘yiladi: kibertovlamachilikning oldini olishda jinoyat-huquqiy javobgarlikdan tashqari qaysi ilmiy-nazariy, tashkiliy, texnik va ijtimoiy choralar samarali bo‘lishi mumkin?

2. Materials and Methods

Tadqiqot materiali sifatida O‘zbekiston Respublikasining Jinoyat kodeksi, Jinoyat-protsessual kodeksi, “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonuni, “Kiberxavfsizlik to‘g‘risida”gi Qonuni, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, shuningdek xalqaro hujjatlar va xorijiy ilmiy manbalar o‘rganildi. Xalqaro manbalar sifatida Budapest konvensiyasi, UNODCning cybercrime prevention va digital evidence bo‘yicha materiallari, NCSC va NCAning ransomware va extortion ekotizimi haqidagi oq kitobi, CISAning StopRansomware qo‘llanmasi hamda NIST ransomware risk management bo‘yicha yondashuvlari tahlil qilindi.

Ilmiy adabiyotlar qatorida E.R. Leukfeldtning routine activity theory va cybercrime profilaktikasi bo‘yicha ishlari, Bada va Nursening kiberjinoyatchilar profiliga oid tizimli sharhi, Bhardwaj va hammualliflarning ransomware haqidagi maqolasi, Vasoya, Bhavsar va Patelning ransomware hujumlari bo‘yicha tizimli

[1] O‘zbekiston Respublikasining 2014-yil 14-maydagi O‘RQ-371-son “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi: lex.uz.

adabiyotlar sharhi, Tom Meursning double-extortion ransomware bo‘yicha PhD dissertatsiyasi, Europolning yoshlarning kiberjinoyatchilikka kirib kelish yo‘llari haqidagi oq kitobi va kiberxavfsizlikka oid amaliy qo‘llanmalar asosiy nazariy manba sifatida foydalanildi.[2]

Maqolada formal-yuridik, qiyosiy-huquqiy, tizimli, kriminologik va tahliliy metodlar qo‘llandi. Formal-yuridik metod milliy qonunchilik normalarini sharhlash uchun, qiyosiy-huquqiy metod xalqaro va xorijiy yondashuvlarni solishtirish uchun, kriminologik metod esa kibertovlamachilikka olib keluvchi sabab va shart-sharoitlarni aniqlash uchun ishlatildi. Tizimli yondashuv profilaktikani jinoiy javobgarlik, raqamli savodxonlik, texnik himoya, jabrlanuvchini qo‘llab-quvvatlash, dalillarni saqlash va xalqaro hamkorlik bilan birgalikda baholash imkonini berdi.

3. Results

Tadqiqot natijasida kibertovlamachilik profilaktikasiga oid quyidagi asosiy natijalar shakllantirildi.

Birinchidan, kibertovlamachilik profilaktikasi bir subyekt zimmasidagi vazifa emas. U davlat organlari, huquqni muhofaza qiluvchi organlar, kiberxavfsizlik subyektlari, ta’lim muassasalari, banklar, internet-platformalar, provayderlar, tashkilotlar va fuqarolarning hamkorligini talab qiladi. Jinoyatchi raqamli muhitdagi bo‘shliqdan foydalanganligi sababli profilaktika ham faqat jinoyat-huquqiy ta’sir bilan cheklanmasligi kerak.

Ikkinchidan, kibertovlamachilik profilaktikasida jinoyatchining imkoniyatini kamaytirish, potensial jabrlanuvchining himoyasini kuchaytirish va raqamli muhitda himoya qiluvchi institutlar rolini oshirish asosiy yo‘nalishlar hisoblanadi. Bu yondashuv routine activity theory va situational crime prevention nazariyalariga mos keladi.[3]

Uchinchidan, ransomware va double-extortion holatlarida profilaktika faqat antivirus yoki texnik himoya bilan cheklanmaydi. Tashkilotlarda zaxira nusxalar, tarmoq segmentatsiyasi, xodimlarni o‘qitish, phishingga qarshi treninglar, incident response rejasi, ma’lumotlar chiqib ketishini monitoring qilish va tezkor xabar berish tartibi bo‘lishi kerak.

To‘rtinchidan, shaxsiy ma’lumotlar va intim materiallar orqali sodir etiladigan kibertovlamachilikda jabrlanuvchining ruhiy holati va ijtimoiy obro‘si alohida e’tiborga olinishi lozim. Bunday holatlarda profilaktika faqat texnik himoyadan iborat

[2] Leukfeldt E.R. Comparing Victims of Phishing and Malware Attacks: Unraveling Risk Factors and Possibilities for Situational Crime Prevention. 2015; Bada M., Nurse J.R.C. Profiling the Cybercriminal: A Systematic Review of Research. 2021; Meurs T. Double-Extortion Ransomware: A Study of Cybercriminal Profit, Effort, and Risk. PhD dissertation. University of Twente, 2025.

[3] Leukfeldt E.R., Yar M. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behavior. 2016.

bo‘la olmaydi; unda maxfiy murojaat kanallari, psixologik yordam, platformalar bilan tezkor hamkorlik va jabrlanuvchini ayblamaslik madaniyati muhim.

Beshinchidan, raqamli dalillarni tezkor saqlab qolish profilaktikaning ajralmas qismidir. Jinoyat haqida kech xabar berish, dalillarni noto‘g‘ri saqlash, yozishmalarni o‘chirib yuborish yoki platforma ma’lumotlarini vaqtida olmaslik jinoyatchining javobgarlikdan qochish imkoniyatini oshiradi.

Oltinchidan, transmilliylik kibertovlamachilik profilaktikasini xalqaro hamkorlik bilan bog‘laydi. Jinoyatchi, server, to‘lov vositasi va jabrlanuvchi turli davlatlarda bo‘lishi mumkin. Shu sababli elektron dalillarni saqlash, xalqaro so‘rovlar, platformalar bilan hamkorlik va kiberjinoyatchilik infratuzilmasini izdan chiqarish muhim profilaktik ahamiyatga ega.

4. Discussion

4.1. Kibertovlamachilik profilaktikasining mazmuni

Kibertovlamachilik profilaktikasini to‘g‘ri tushunish uchun uni uch bosqichli jarayon sifatida ko‘rish maqsadga muvofiq. Birinchi bosqich — jinoyat sodir etilishidan oldingi oldini olish. Bu bosqichda potensial jabrlanuvchilarni himoya qilish, zaif akkauntlar va tizimlarni mustahkamlash, fuqarolarning raqamli savodxonligini oshirish, tashkilotlarda xavfsizlik siyosatini joriy etish va xodimlarni o‘qitish muhim. Ikkinchi bosqich — jinoyat sodir etilayotgan paytdagi tezkor javob. Bu bosqichda dalillarni saqlash, tahdidni to‘xtatish, jabrlanuvchiga yordam ko‘rsatish, akkaunt yoki tizimga kirishni tiklash, zararli dastur ta’sirini kamaytirish zarur. Uchinchi bosqich — jinoyatdan keyingi profilaktika. Bu bosqichda aybdorni javobgarlikka tortish, jabrlanuvchining huquqlarini tiklash, tashkilotning tizimini qayta mustahkamlash va kelgusida shunga o‘xshash holatlarning oldini olish choralari ko‘riladi.

Bunday yondashuv “profilaktika”ni faqat ma’ruza, targ‘ibot yoki umumiy ogohlantirish darajasida qoldirmaydi. Aksincha, u profilaktikani raqamli xavf boshqaruvi, jinoyat-huquqiy ta’sir, jabrlanuvchini himoya qilish va kiberxavfsizlik choralari bilan birlashtiradi. Kibertovlamachilikning murakkabligi ham aynan shuni talab qiladi.

4.2. Routine activity theory va situatsion profilaktika

Kibertovlamachilik profilaktikasini ilmiy asoslashda routine activity theory muhim nazariy poydevor bo‘lib xizmat qiladi. Mazkur nazariyaga ko‘ra, jinoyat sodir bo‘lishi uchun uchta omil bir vaqtda mavjud bo‘ladi: motivatsiyaga ega jinoyatchi, mos nishon va samarali himoyaning yo‘qligi. Kibermakonda bu omillar jismoniy hudud bilan bog‘lanmagan, lekin ularning mazmuni saqlanib qoladi. Motivatsiyaga ega jinoyatchi anonim akkaunt yoki zararli dastur orqali harakat qiladi, mos nishon sifatida zaif akkaunt, himoyasiz server yoki ehtiyotsiz foydalanuvchini tanlaydi, samarali himoyaning yo‘qligi esa profilaktikaning zaifligini bildiradi.

Leukfeldt phishing va malware qurbonlari bo‘yicha tadqiqotida profilaktikani faqat foydalanuvchining o‘ziga yuklash yetarli emasligini ko‘rsatadi. Uning xulosasiga ko‘ra, jinoyatchilar ko‘proq ommabop onlayn joylarga qiziqadi, shuning uchun “virtual joylar” egalari ham o‘z foydalanuvchilarini himoya qilishda faol rol o‘ynashi kerak.[4] Bu fikr kibertovlamachilik profilaktikasida juda muhim. Ijtimoiy tarmoqlar, messenjerlar, bulutli xizmatlar, hostinglar va to‘lov platformalari jinoyatchi bilan jabrlanuvchi uchrashadigan raqamli muhitni yaratadi. Agar platformalar shikoyat, bloklash, dalillarni saqlash va zararli kontentni olib tashlash mexanizmlarini samarali yo‘lga qo‘ymasa, jinoyatchi uchun qulay sharoit saqlanib qoladi.

Situational crime prevention yondashuvi esa jinoyatchi imkoniyatlarini kamaytirishga qaratiladi. Kibertovlamachilikda bu yondashuv quyidagi choralarni o‘z ichiga olishi mumkin: ikki bosqichli autentifikatsiya, kuchli parol siyosati, zaxira nusxalar, tarmoq segmentatsiyasi, administrator vakolatlarini cheklash, xodimlarni phishing bo‘yicha o‘qitish, shubhali kirishlarni monitoring qilish, ma’lumotlarni shifrlash, platformalarda tezkor shikoyat tizimi va jabrlanuvchilar uchun maxfiy murojaat kanallari. Bu choralarning umumiy maqsadi jinoyatchi uchun foydani kamaytirish, xavfni oshirish va hujumni amalga oshirishni qiyinlashtirishdir.

4.3. Ransomware va double-extortion profilaktikasi

Ransomware kibertovlamachilikning eng xavfli shakllaridan biri hisoblanadi. Bunday hujumda jinoyatchi jabrlanuvchining ma’lumotlarini shifrlaydi yoki tizimga kirishni bloklaydi, keyin esa tizimni tiklash evaziga to‘lov talab qiladi. Double-extortion holatlarida esa ma’lumotlar nafaqat shifrlanadi, balki o‘g‘irlanadi va to‘lov qilinmasa, ularni tarqatish bilan qo‘rqitiladi. Bu holat jabrlanuvchining zaxira nusxasi bo‘lsa ham xavfni to‘liq bartaraf etmaydi, chunki ma’lumotlar oshkor bo‘lishi ehtimoli saqlanadi.

Bhardwaj va hammualliflar ransomware’ni yangi davrning raqamli tovlamachiligi sifatida tahlil qilib, u faqat zararli dastur emas, balki majburlash va iqtisodiy manfaat olishga qaratilgan mexanizm ekanini ko‘rsatadi.[5] Vasoya, Bhavsar va Patelning tizimli adabiyotlar sharhi ham ransomware hujumlariga qarshi kurashda texnik himoya bilan birga foydalanuvchi xulqi, tashkilot tayyorgarligi va javob berish mexanizmlari muhimligini ko‘rsatadi.[6]

Tom Meursning double-extortion ransomware bo‘yicha PhD dissertatsiyasi bu masalaga jinoyatchining iqtisodiy hisob-kitobi nuqtai nazaridan yondashadi. Dissertatsiyada jinoyatchining foyda, xarajat va xavfni qanday baholashi tahlil

[4] Leukfeldt E.R. Comparing Victims of Phishing and Malware Attacks: Unraveling Risk Factors and Possibilities for Situational Crime Prevention. 2015.

[5] Bhardwaj A., Subrahmanyam G.V.B., Avasthi V., Sastry H. Ransomware: A Rising Threat of New Age Digital Extortion. arXiv:1512.01980, 2015.

[6] Vasoya S., Bhavsar K., Patel N. A Systematic Literature Review on Ransomware Attacks. arXiv:2212.04063, 2022.

qilinadi.[7] Ushbu yondashuv profilaktika uchun muhim xulosani beradi: agar jinoyatchining kutilayotgan foydasi kamaytirilsa, hujum xarajati oshirilsa va aniqlanish xavfi kuchaytirilsa, kibertovlamachilik kamroq “jozibador” bo‘ladi. Bu esa profilaktikani faqat jazoni kuchaytirish bilan emas, balki jinoyatni iqtisodiy va texnik jihatdan foydasiz qilish bilan bog‘lash zarurligini anglatadi.

NCSC va NCAning ransomware va extortion ekotizimi haqidagi oq kitobida ransomware va tovlamachilik hujumlari professional jinoyatchilik modeliga aylangani, jinoyatchilar o‘z biznes-modelini foydani oshirishga moslashtirib borayotgani qayd etiladi.[8] Bundan kelib chiqadigan xulosa shuki, profilaktika faqat alohida jinoyatchini ushlash bilan cheklanmasligi kerak. Zararli dastur ishlab chiquvchilar, kirish ma’lumotlarini sotuvchilar, phishing infratuzilmasi, to‘lov vositachilari va ma’lumotlarni sizdirish saytlariga qarshi ham tizimli kurash zarur.

4.4. Kiberjinoyatchi shaxsini o‘rganish va yoshlar profilaktikasi

Kibertovlamachilik profilaktikasida jinoyatchi shaxsini o‘rganish ham muhim ahamiyatga ega. Bada va Nurse kiberjinoyatchilar profiliga oid tizimli sharhida bu sohada yagona umumiy yondashuv yetishmasligini, mavjud tadqiqotlarda ko‘pincha “hacker” obraziga haddan tashqari urg‘u berilganini ko‘rsatadi.[9] Amaliyotda esa kibertovlamachilikni yuqori malakali dasturchi, tayyor zararli vositadan foydalanuvchi oddiy shaxs, uyushgan guruh a’zosi, sobiq xodim, o‘smir yoki shaxsiy adovat bilan harakat qilayotgan foydalanuvchi sodir etishi mumkin.

Bu holat profilaktika choralarini ham differensiallashtirishni talab qiladi. Professional uyushgan guruhlarga qarshi texnik, xalqaro va moliyaviy izlarni kuzatish choralari muhim bo‘lsa, yoshlar orasida profilaktika boshqacha bo‘lishi kerak. Europolning “Youth Pathways into Cybercrime” oq kitobi yoshlarning kiberjinoyatchilikka kirib kelishida qiziqish, texnik qobiliyat, onlayn guruhlar ta’siri, e’tirofga ehtiyoj va nazoratsiz tajriba muhim rol o‘ynashini ko‘rsatadi.[8]

O‘zbekiston sharoitida bu xulosa ta’lim muassasalari uchun muhim. Texnik qobiliyatga ega yoshlarni faqat taqiqlash yoki jazolash orqali emas, balki qonuniy kiberxavfsizlik faoliyatiga yo‘naltirish zarur. Ethical hacking musobaqalari, raqamli xavfsizlik darslari, shaxsiy ma’lumotlarni himoya qilish bo‘yicha mashg‘ulotlar, “internetdagi harakat ham javobgarlikka olib keladi” degan huquqiy tushuntirishlar yoshlar profilaktikasining asosiy yo‘nalishlaridan biri bo‘lishi kerak. “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonunda ta’lim muassasalarining profilaktika sohasidagi vazifalari ko‘rsatilgani ushbu yondashuvni milliy huquqiy asos bilan bog‘lash imkonini beradi.

[7] Meurs T. Double-Extortion Ransomware: A Study of Cybercriminal Profit, Effort, and Risk. PhD dissertation. University of Twente, 2025.

[8] National Cyber Security Centre; National Crime Agency. Ransomware, Extortion and the Cyber Crime Ecosystem. United Kingdom, 2023.

4.5. Jabrlanuvchiga yo‘naltirilgan profilaktika

Kibertovlamachilikda jabrlanuvchi ko‘pincha jinoyatchi bilan yolg‘iz qoladi. Ayniqsa shaxsiy ma’lumotlar, intim materiallar, oilaviy sirlar yoki biznes obro‘si bilan bog‘liq tovlamachilikda jabrlanuvchi yordam so‘rashdan qo‘rqishi mumkin. Bu holatda jinoyatchining asosiy quroli faqat texnik vosita emas, balki jabrlanuvchining uyat, qo‘rquv va ijtimoiy bosimdan cho‘chishidir.

Shu sababli profilaktika tizimida jabrlanuvchilar uchun ishonchli, maxfiy va tezkor murojaat mexanizmlari zarur. Bunday mexanizm uch vazifani bajarishi kerak: birinchidan, jabrlanuvchiga huquqiy va psixologik yordam berish; ikkinchidan, raqamli dalillarni to‘g‘ri saqlash bo‘yicha yo‘l-yo‘riq ko‘rsatish; uchinchidan, jinoyatchining qo‘shimcha bosimini to‘xtatish.

Sextortion yoki shaxsiy materiallar orqali tovlamachilik holatlarida jabrlanuvchiga “pul bermang” deyishning o‘zi yetarli emas. Agar shaxs o‘z ma’lumotlari tarqalishidan qo‘rqsa, u baribir jinoyatchi talabini bajarishi mumkin. Shu bois platformalar, huquqni muhofaza qiluvchi organlar va maslahat xizmatlari jabrlanuvchiga ma’lumotlarni olib tashlash, akkauntni himoyalash, tahdid yuborgan shaxsni bloklash, yozishmalarni saqlab qolish va tegishli organga murojaat qilish tartibini sodda va tushunarli ko‘rsatishi kerak.

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga soladi. Ushbu qonunning profilaktik ahamiyati shundaki, kibertovlamachilikda shaxsiy ma’lumotlar ko‘pincha bosim vositasiga aylanadi. Ma’lumotlarning noqonuniy to‘planishi, saqlanishi yoki tarqalishi oldindan cheklansa, jinoyatchining shantaj qilish imkoniyati ham kamayadi.

4.6. Tashkilotlar darajasida profilaktika va “resilience” yondashuvi

Kibertovlamachilik tashkilotlarga nisbatan sodir etilganda profilaktika faqat “hujumni oldini olish”dan iborat bo‘la olmaydi. Chunki real hayotda hech bir axborot tizimi mutlaq xavfsiz emas. Shu sababli tashkilotlar “resilience”, ya’ni hujum sodir bo‘lsa ham tez tiklanish, zarar ko‘lamini cheklash va jinoyatchiga to‘lov qilishga majbur bo‘lmaslik qobiliyatiga ega bo‘lishi kerak.

CISAning StopRansomware qo‘llanmasi ransomware va data extortion holatlariga qarshi oldini olish hamda javob berish bo‘yicha amaliy choralarni ko‘rsatadi. Unda zaxira nusxalar, ko‘p faktorli autentifikatsiya, xodimlarni o‘qitish, tizimlarni yangilash, incident response rejasi va ma’lumotlar chiqib ketishiga qarshi choralar muhimligi ta’kidlanadi. NIST ransomware risk management profili esa ransomware hodisalarini aniqlash, ulardan himoyalanish, javob berish va tiklanish bo‘yicha xavfni boshqarish yondashuvini beradi.

Bu manbalar asosida O‘zbekiston tashkilotlari uchun quyidagi amaliy xulosalar muhim: har bir tashkilotda zaxira nusxalarni alohida saqlash, xodimlar uchun muntazam phishing treninglar o‘tkazish, administrator huquqlarini cheklash, xizmat

yozishmalari va shaxsiy akkauntlarni ajratish, hodisa yuz berganda kim javob berishini oldindan belgilash, dalillarni saqlash tartibini ishlab chiqish va huquqni muhofaza qiluvchi organlarga murojaat qilish algoritmini yaratish zarur.

4.7. Raqamli dalillar va tezkor xabar berish

Kibertovlamachilik profilaktikasida raqamli dalillarni to‘g‘ri saqlash alohida o‘rin tutadi. Ko‘p hollarda jabrlanuvchi qo‘rqib yozishmalarni o‘chirib yuboradi, tahdid yuborgan akkauntni bloklaydi, lekin dalillarni saqlamaydi yoki jinoyatchiga to‘lov qilib, keyin murojaat qiladi. Bunday harakatlar jinoyatchini aniqlashni qiyinlashtiradi.

O‘zbekiston Respublikasi Jinoyat-protsessual kodeksida elektron ma’lumotlar va raqamli dalillar bo‘yicha alohida normalar mavjud. Profilaktika nuqtai nazaridan bu normalar shuni anglatadiki, fuqarolar va tashkilotlar raqamli dalillarni qanday saqlashni bilishi kerak: tahdid xabarini o‘chirmaslik, skrinshot bilan birga havola, akkaunt nomi, vaqt, telefon raqami yoki elektron pochta ma’lumotlarini saqlash, kriptohamyon manzilini qayd etish, fayllar va yozishmalarni asl holatda saqlab qolish, zarur bo‘lsa mutaxassisga murojaat qilish.

UNODC kiberjinoyatlar bo‘yicha materiallarida raqamli dalillar turli qurilmalar, tizimlar va serverlarda joylashishi mumkinligi, ular tez o‘zgarishi yoki yo‘qolishi ehtimoli borligi qayd etiladi. Shu sababli tezkor xabar berish va dalillarni saqlash nafaqat tergov uchun, balki profilaktika uchun ham muhimdir. Jinoyatchi javobgarlikdan qochmasligini bilsa, bunday jinoyatni sodir etishga bo‘lgan motivatsiyasi kamayadi.

4.8. Xalqaro hamkorlik va kiberjinoyatchilik ekotizimini izdan chiqarish

Kibertovlamachilik ko‘pincha transmilliy xususiyatga ega. Jinoyatchi bir davlatda, jabrlanuvchi ikkinchi davlatda, server uchinchi davlatda, to‘lov esa kriptoaktivlar orqali boshqa yurisdiksiyada harakatlanishi mumkin. Shu sababli profilaktika faqat milliy choralar bilan cheklanib qolmasligi kerak.

Budapest konvensiyasi kiberjinoyatlar va elektron dalillar bo‘yicha xalqaro hamkorlikning muhim huquqiy asoslaridan biridir. Konvensiya kiberjinoyatlarga qarshi kurashni faqat jinoyat tarkibini belgilash bilan cheklamaydi, balki tergov vakolatlari, elektron dalillar va davlatlararo hamkorlik masalalarini ham qamrab oladi. Kibertovlamachilik profilaktikasida bu juda muhim, chunki jinoyatchilik zanjirini uzish uchun xalqaro axborot almashinuvi, platformalardan ma’lumot olish va zararli infratuzilmani bloklash talab etiladi.

NCSC va NCA ransomware va extortion ekotizimini tahlil qilar ekan, cyber extortion zamonaviy uyushgan jinoyatchilikning murakkab biznes-modeliga aylanganini ko‘rsatadi. Bundan kelib chiqadigan profilaktik xulosa shuki, faqat alohida jinoyatchini ushlash yetarli emas. Jinoyatga xizmat qiluvchi infratuzilma — phishing sahifalari, zararli dastur tarqatish kanallari, kirish ma’lumotlari bozori, to‘lov

vositachilari, leak site’lar va anonim aloqa kanallari ham izdan chiqarilishi kerak. Bu yondashuv kiberjinoyatchilikni “shaxsga qarshi kurash” emas, balki “jinoyat imkoniyatlari tizimini kamaytirish” sifatida tushunishga yordam beradi.

4.9. Milliy qonunchilik doirasida profilaktikani kuchaytirish

O‘zbekiston qonunchiligida kibertovlamachilik profilaktikasi uchun zarur bo‘lgan bir nechta huquqiy asos mavjud. Jinoyat kodeksining 165-moddasi tovlamachilik uchun javobgarlikni belgilaydi va axborot resursiga qaratilgan tahdidlarni ham qamrab oladi. “Kiberxavfsizlik to‘g‘risida”gi Qonun kiberxavfsizlik sohasidagi munosabatlarni tartibga soladi. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun shaxsiy ma’lumotlarni himoya qilishga qaratilgan. “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonun esa profilaktika faoliyatining umumiy mexanizmini belgilaydi.

Biroq ushbu normalar amaliyotda bir-biri bilan bog‘langan holda ishlashi kerak. Masalan, shaxsiy ma’lumotlar orqali tovlamachilik sodir etilganida shaxsga doir ma’lumotlarni himoya qilish, jinoyat huquqi, platforma siyosati, raqamli dalillar va jabrlanuvchiga psixologik yordam masalalari bir vaqtda hal qilinadi. Ransomware holatida esa kiberxavfsizlik, jinoyat-protsessual dalillar, tashkilotning ichki xavfsizlik siyosati, huquqni muhofaza qiluvchi organlar va xalqaro hamkorlik birgalikda ishlashi lozim.

Shu sababli milliy profilaktika mexanizmlarini kuchaytirish uchun quyidagi takliflarni ilgari surish mumkin: kibertovlamachilik bo‘yicha metodik tavsiyalar ishlab chiqish; jabrlanuvchilar uchun maxfiy va tezkor murojaat kanallarini kuchaytirish; ta’lim muassasalarida onlayn shantaj va raqamli xavfsizlik bo‘yicha maxsus o‘quv materiallari joriy etish; tashkilotlar uchun ransomware readiness bo‘yicha minimal talablar ishlab chiqish; raqamli dalillarni saqlash bo‘yicha huquqni muhofaza qiluvchi organlar, provayderlar va platformalar o‘rtasida amaliy tartiblarni takomillashtirish.

4.10. Mualliflik pozitsiyasi

Fikrimizcha, kibertovlamachilik profilaktikasi uch darajada tashkil etilishi kerak.

Birinchi daraja — umumiy profilaktika. Bu aholining raqamli savodxonligini oshirish, shaxsiy ma’lumotlarni himoya qilish madaniyatini shakllantirish, yoshlar orasida kiberjinoyatlarning huquqiy oqibatlarini tushuntirish, tashkilotlarda kiberxavfsizlik siyosatini joriy etish va platformalar mas’uliyatini oshirishdan iborat.

Ikkinchi daraja — maxsus profilaktika. Bu xavfi yuqori guruhlar va obyektlar bilan ishlashni anglatadi: voyaga yetmaganlar, ijtimoiy tarmoqlarda faol shaxslar, davlat organlari, banklar, tibbiyot tashkilotlari, ta’lim muassasalari, kichik va o‘rta biznes subyektlari, muhim axborot infratuzilmasi obyektlari. Bu guruhlarda kibertovlamachilik xavfi turlicha bo‘lgani uchun profilaktik choralar ham moslashtirilgan bo‘lishi kerak.

Uchinchi daraja — individual va jabrlanuvchiga yo‘naltirilgan profilaktika. Bunda oldin kibertovlamachilik qurboni bo‘lgan shaxslar, jinoyatchi bilan muloqotda bo‘lgan foydalanuvchilar, ma’lumotlari sizib chiqqan tashkilotlar, sextortion xavfiga duch kelgan shaxslar va kiberjinoyat sodir etishga moyil shaxslar bilan alohida ishlash zarur.

Shu yondashuvdan kelib chiqib, kibertovlamachilik profilaktikasini faqat jazoni kuchaytirish orqali ta’minlash mumkin emas. Jazo zarur, lekin profilaktikaning o‘rnini bosa olmaydi. Samarali profilaktika jinoyatchining imkoniyatini kamaytiradi, jabrlanuvchining himoyasini kuchaytiradi, dalillarni saqlab qoladi, kiberjinoyatchilik infratuzilmasini izdan chiqaradi va jamiyatda raqamli xavfsizlik madaniyatini shakllantiradi.

5. Conclusion

Kibertovlamachilik jinoyatlarining profilaktikasini ta’minlash raqamli jamiyat sharoitida dolzarb jinoyat-huquqiy va kriminologik masalalardan biridir. Mazkur jinoyat mulk, shaxsiy hayot daxlsizligi, axborot resurslari, raqamli obro‘, biznes barqarorligi va jamiyatning kibermakonga bo‘lgan ishonchiga bir vaqtning o‘zida zarar yetkazadi. Shu bois profilaktika faqat jinoyat sodir etilgandan keyin javobgarlikka tortish bilan cheklanmasligi kerak.

Ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, kibertovlamachilikning oldini olishda routine activity theory, situational crime prevention, cybercriminal profiling, ransomware risk management va double-extortion bo‘yicha tadqiqotlar muhim nazariy asos beradi. Bu yondashuvlarning umumiy xulosasi shuki, jinoyatni kamaytirish uchun jinoyatchining foydasini kamaytirish, xarajatini oshirish, aniqlanish xavfini kuchaytirish, potensial jabrlanuvchini himoyalash va raqamli muhitda samarali himoya institutlarini yaratish zarur.

O‘zbekiston qonunchiligida kibertovlamachilik profilaktikasi uchun asos bo‘ladigan bir nechta manbalar mavjud: huquqbuzarliklar profilaktikasi qonunchiligi, kiberxavfsizlik qonunchiligi, shaxsga doir ma’lumotlarni himoya qilish normalari, Jinoyat kodeksining tovlamachilikka oid qoidalari hamda Jinoyat-protsessual kodeksining raqamli dalillarga oid normalari. Biroq ushbu normalar amaliyotda bir-biri bilan bog‘langan holda ishlashi lozim.

Shu asosda xulosa qilish mumkinki, kibertovlamachilik profilaktikasi kompleks tizim bo‘lishi kerak. Bu tizim huquqiy javobgarlik, raqamli savodxonlik, texnik himoya, tashkilotlar tayyorgarligi, jabrlanuvchini qo‘llab-quvvatlash, raqamli dalillarni saqlash, xalqaro hamkorlik va kiberjinoyatchilik ekotizimini izdan chiqarish choralarini o‘z ichiga oladi. Faqat shunday yondashuv orqali kibertovlamachilik xavfini kamaytirish va raqamli muhitda fuqarolar hamda tashkilotlarning huquqiy xavfsizligini ta’minlash mumkin.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Jinoyat kodeksi. 1994-yil 22-sentabr. Qonunchilik ma’lumotlari milliy bazasi.
2. O‘zbekiston Respublikasining 2014-yil 14-maydagi O‘RQ-371-son “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi.
3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi.
4. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni.
5. Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001.
6. United Nations Office on Drugs and Crime. Cybercrime Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics.
7. United Nations Office on Drugs and Crime. Cybercrime Module 8: Cybersecurity and Cybercrime Prevention — Strategies, Policies and Programmes.
8. National Cyber Security Centre; National Crime Agency. Ransomware, Extortion and the Cyber Crime Ecosystem. United Kingdom, 2023.
9. Cybersecurity and Infrastructure Security Agency. StopRansomware Guide: Ransomware and Data Extortion Prevention and Response.
10. National Institute of Standards and Technology. Ransomware Risk Management: Cybersecurity Framework Profile. NIST IR 8374, 2022.
11. Leukfeldt E.R. Comparing Victims of Phishing and Malware Attacks: Unraveling Risk Factors and Possibilities for Situational Crime Prevention. 2015.
12. Bada M., Nurse J.R.C. Profiling the Cybercriminal: A Systematic Review of Research. IEEE Cyber Science Conference. 2021.
13. Bhardwaj A., Subrahmanyam G.V.B., Avasthi V., Sastry H. Ransomware: A Rising Threat of New Age Digital Extortion. arXiv:1512.01980, 2015.
14. Vasoya S., Bhavsar K., Patel N. A Systematic Literature Review on Ransomware Attacks. arXiv:2212.04063, 2022.
15. Meurs T. Double-Extortion Ransomware: A Study of Cybercriminal Profit, Effort, and Risk. PhD dissertation. University of Twente, 2025.
16. Europol. Youth Pathways into Cybercrime. White Paper, 2016.
17. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024.
18. Pattnaik N., Nurse J.R.C., Turner S., Mott G., MacColl J., Huesch P., Sullivan J. It’s More Than Just Money: The Real-World Harms from Ransomware Attacks. 2023.