Tovlamachi dasturlar turlari va vektor hujumlar tahlili

Nosirov Amirxon Baxodir o‘g‘li

Tashkent State University of Law

a.nosirov.1111tsul@gmail.com

Annotatsiya

Ushbu maqolada tovlamachi dasturlar turlari va vektor hujumlar umumiy tushunchasi hamda kriminalistik tahlili bayon etilgan. Unda tovlamachi dasturlardan foydalanish bilan bog‘liq jinoyatining kriminalistik tavsif elementlari, ya’ni jinoyat predmeti, jinoyat sodir etish usullari, jinoyat izlari, jinoyatchining shaxsi haqidagi ma’lumotlar, jinoyat shart-sharoitlari yoritilgan.

Shu bilan birga, tovlamachi dasturlar bilan bog‘liq jinoyatini tergov qilishda raqamli izlar bilan ishlash jarayoni, milliy qonunchilik va huquqni qo‘llash amaliyotida yuzaga kelayotgan muammolar hamda bo‘shliqlar tanqidiy ko‘rib chiqilgan. Ularni bartaraf etishning ilmiy asoslangan yo‘llari va mezonlari ishlab chiqilgan. Maqola tovlamachi dasturlar va raqamli izlar bilan ishlash sohasida amalga oshirilgan ilmiy-amaliy tadqiqotlar, nazariyotchi olimlar hamda amaliyotchi xodimlar fikr-mulohazalari asosida tayyorlangan.

Bundan tashqari, onlayn jinoyat turlaridan biri bo‘lmish internet tovlamachilik jinoyatini bank kartalari bilan bog‘liq firibgarlik jinoyatiga o‘xshash jihatlari muhokama qilingan. Maqolada sohada yuzaga kelayotgan muammolar tizimli, huquqiy, ilmiy-amaliy jihatdan tahlil etilgan, bu yuzasidan mualliflik xulosalari shakllantirilgan. Qonun chiqaruvchi va uni qo‘llovchi subektlar uchun ilmiy asoslangan taklif hamda tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: kiberjinoyatchilik, tovlamachi dasturlar, tovlamachi dasturlar turlari, vektor hujumlar, jinoyat izlari, jinoyat usuli, jinoyatchi shaxsi.

Dissecting ransomware variants and attack vectors

Nosirov Amirkhon

Tashkent State University of Law

a.nosirov.1111tsul@gmail.com

Abstract

This article describes the general concept of malware types and vector attacks as well as criminalistic analysis. It covers the elements of the criminalistic description of the crime associated with the use of malware, that is, the subject of the crime, methods of committing a crime, traces of a crime, information about the identity of the offender, criminal conditions.

At the same time, the process of working with digital tracks in the investigation of a crime related to malware, the problems arising in national legislation and law enforcement practice, as well as loopholes are critically examined. Scientifically based ways and criteria for their elimination have been developed. The article is prepared on the basis of scientific and practical research carried out in the field of work with malware and digital traces, feedback from theoretical scientists and practicing personnel.

In addition, aspects of the internet extortion crime, one of the types of online crime, have been discussed similar to the fraud crime associated with bank cards. The article analyzes the problems arising in the field in a systematic, legal, scientific and practical way, on which author's conclusions are formulated. Scientifically based proposals and recommendations have been developed for the legislator and the subects that apply it.

Keywords: Cybercrime, Ransomware, Ransomware types, Vector attacks, Crime tracks, Crime method, Criminal personality.

I. Kirish

Bugungi kunda butun dunyo miqyosida ma’lumotlar markazlari, mudofaa, energetika, hukumat va moliya sektorlariga kiberhujumlarning ortib borayotgan tahdidi barchaga birdek xavf tug‘dirmoqda. Ushbu kiberhujumlarda moliyaviy o‘g‘irlik, josuslik, sabotaj, intellektual mulkni o‘g‘irlash va siyosiy maqsadlar uchun tovlamachi dasturlardan foydalanilmoqda. Kiberjinoyatchilar murakkablashib borayotgan va ilg‘or tovlamachi dastur hujumlarini amalga oshirayotgan bir paytda, bunday hujumlarni aniqlash va ularga javob berish kiberxavfsizlik bo‘yicha mutaxassislar uchun juda muhim vazifaga aylanmoqda.

Biroq, shunga qaramay sohaga doir ilmiy tadqiqotlarni etishmasligi hamda kadrlar tanqisligi bilan bog‘lik muammolar sohani tartibga solishda muayyan uslubiy qiyinchiliklarni yuzaga keltimoqda. Shu ma’noda, tovlamachi dasturlar tushunchasi, mazmun-mohiyati, turlari, xususiyatlari, ularni aniqlash, tahlil etish vositalari va usullarini bilish huquqni qo‘llovchi uchun muhim ahamiyatga ega.

Axborot texnologiyalarini rivojlanashi kiberjinoyatchilik faoliyatini ham keltirib chiqardi. Natijada, kompyuter vositalari yordamida jinoyatlarni sodir etish mexanizmi murakkablashib, tobora ommaviy xarakterga aylanib bormoqda. Ushbu jinoyatlarni sodir etish mexanizmidagi o‘ziga xosligi unga qarshi kurash uslubiyotini uzluksiz takomillashtishni taqozo etmoqda. Boshqacha qilib aytganda, jinoyatga tayyorgarlik ko‘rish va uni yashirishda jinoyatchilar tomonidan maxsus vositalarni (tovlamachi dasturlar) ishlab chiqarilishi yoki global Internet tarmog‘ini

jinoyatchilarning “kasbiy” ko‘nikmalarini rivojlantiruvchi kiber muhitga aylanib ulgurgani sohada muayyan tadqiqotlar olib borish dolzarbligini tasdiqlaydi.

Jinoiy maqsadni amalga oshirishda kompyuter texnikasidan asosiy vosita yoki quroli sifatida foydalanish kundan-kunga ommalashib bormoqda. Kompyuter texnikasini mehnat munosabatlarining asosiy vositasiga aylanishi va ma’lumotmotlar bazalari bilan samarali ishlash imkonini berishi moliyaviy xizmatlar ko‘rsatish sohasida inqilobiy o‘zgarishlarga olib kelmoqda. Xususan, bugun iqtisodiyot sohasida moliyaviy xizmatlar ko‘rsatishning turli shakllarini joriy etilishi bu borada bank plastik kartlari bilan bog‘liq kiberjinoyatlarni o‘sishi uchun ham zamin yaratmoqda.

2022 yil 28 yanvardagi O‘zbekiston Respublikasi Prezidentining “Yangi O‘zbekistonning 2022–2026 yillarga mo‘ljallangan taraqqiyot strategiyasi to‘g‘risida”gi PF–60-son Farmoni (keyingi o‘rinlarda Farmon deb yuritiladi) bilan tergov faoliyatini nazorat qilish, axborot texnologiyalaridan foydalangan holda sodir etilayotgan yangi turdagi jinoyatlar, shu jumladan kiberjinoyatlarni fosh etish bo‘yicha tezkor-qidiruv faoliyatini isloh qilish, qo‘shimcha kuch va vositalarni jalb qilish hamda ushbu jinoyatlarga qarshi kurashish jarayonlarida fuqarolarning qadr-qimmati va erkinligini himoya qilishning samaradorligini yanada oshirish bo‘yicha qator vazifalar belgilandi[1].

Farmonga binoan «2023–2026 yillarga mo‘ljallangan O‘zbekiston Respublikasining kiberxavfsizlik strategiyasi”ni ishlab chiqish vazifasi qo‘yildi.

Bunda, kiberjinoyatchilik uchun jinoiy javobgarlikni qayta ko‘rib chiqish, axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimini yanada takomillashtirish, xususan, kiberxavfsizlikning yagona tarmog‘ining texnik infratuzilmasini kengaytirish vazifalari belgilab olindi.

II. Metodologiya

“Tovlamachi dasturlar” (ransomware) bu kompyuter, server, mijoz yoki kompyuter tarmog‘ini buzish, shaxsiy ma’lumotlarni o‘g‘irlash, ma’lumotlar yoki tizimlarga ruxsatsiz kirish, foydalanuvchining kompyuter xavfsizligi va maxfiyligi to‘siqlarini buzib kirgan holda foydalanuvchilarni ma’lumotlarga kirishdan mahrum qiladigan har qanday dasturiy ta’minotdir[2].

Tovlamachi dasturlardan foydalanish bilan bog‘liq jinoyatlarni fosh etilishi juda qiyin bo‘lgan jinoyatlardan biri bo‘lib, puxta rejalashtirilganligi, o‘ta

[1] 2022 yil 28 yanvardagi O'zbekiston Respublikasi Prezidentining «Yangi O'zbekistonning 2022–2026 yillarga mo'ljallangan taraqqiyot strategiyasi to'g'risida»gi PF–60-son Farmoni.
[2] „Defining Malware: FAQ“. technet.microsoft.com.

murakkabligi hamda transchegaraviy xususiyatga egaligi bilan boshqa turdagi jinoyatlardan farq qiladi.

Qonunchiligimizda Tovlamachi dasturlardan foydalanish bilan bog‘liq jinoyatlar tushunchasi hali to‘liq va batafsil yoritilmagan. Hozirda Tovlamachi dasturlardan foydalanish bilan bog‘liq jinoyatlarni sodir etish holati va usuliga qarab, O‘zbekiston Respublikasi Jinoyat kodeksining **278[6]-moddasi**ga asosan **Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish** bilan bog‘liq jinoyatlarni sodir etilganda ushbu norma bilan kvalifikatsiya qilinadi.

Tovlamachi dasturlarning quyidagi turlari mavjud

Spyware (spyware) - bu dastur foydalanuvchilarning **shaxsiy ma‘lumotlarni to‘plash** va ularni dastur yaratuvchisiga yuborish yoki boshqa odamlar nomidan Internet tarmog‘i orqali, oldindan avtorizatsiya qilinmasdan kirishga mo‘ljallangan dasturdir.

Virus - bu o‘zini ko‘paytirish xususiyatiga ega, foydalanuvchi ma’lumotlarini zararlaydigan va shu kabi amallarni bajarish uchun ishlab chiqilgan va yozilgan zararli kompyuter dasturi.

Qurt - virusning o‘ziga xos turi bo‘lib, tarmoqqa ulangan terminallar orqali takrorlanadigan va fayl butligiga ta’sir qilishi mumkin bo‘lgan ba’zi bir harakatlarni bajaradigan operatsion dasturlar tizimi.

Troyan - bu oddiy ko‘rsatmalar ketma-ketligida kiritilgan, yaroqli dastur ko‘rinishini oladigan dastur. Aslida, u yashirin noqonuniy funktsiyani o‘z ichiga oladi va bu orqali kompyuter tizimining xavfsizlik mexanizmlari chetlab o‘tib fayllarni egallab olish, tahrirlash yoki yo‘q qilishga imkon beradigan zararli dastur.

Jinoyatlarni tergov qilishda xususiy kriminalistik uslubining muhim bo‘limlaridan biri jinoyatning kriminalistik tavsifidir[3]. Har qanday jinoyat, shu jumladan, Tovlamachi dasturlardan foydalanish bilan bog‘liq jinoyatlar ham o‘ziga xos bir hodisa, tarkibga ega bo‘lib, ularning majmui aniq qilmishni tergov qilish jarayonida umumlashtirishni taqozo etadi. Shunday tarzda sodir etilgan jinoyatlarni tipik xususiyatlariga qarab tizimlashtirish va guruhlarga ajratish orqali kriminalistik tavsifni tuzish bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatlarini tergov qilish uslubining asosini tashkil etadi.

[3] Jinoyatlarni tergov qilishning kriminalistik metodikasi: O‘quv qo‘llanma / R.R. Shakurov, Sh.T. Djumanov, N. Toshtemirov, D.R. Turaeva, O.D. Allanazarov. – T: O‘zbekiston Respublikasi IIV akademiyasi, 2013. – 5 b.

Jinoyat ishini qo‘zg‘atish masalasi va tergovni to‘g‘ri yo‘nalishda olib borish uchun ham tergovchi jinoyatning kriminalistik tavsifidan foydalanadi[4]. Shundan ko‘rinib turibdiki, jinoyat ishini tez va to‘g‘ri ochishning asosiy shartlardan biri kriminalistik tavsifni to‘g‘ri belgilab olish hisoblanadi. Tergov jarayonida jinoyat ishi bo‘yicha izchillik bilan qo‘shimchalar va aniqliklar kiritilganda, jinoyatning kriminalistik tavsifi qanday yangi tergov uslublarini qo‘llash va qanday tartibda olib borish mumkinligi kabilarga oydinlik kiritadi[5].

III. Natija

Mamlakatimizda kuzatilayotgan onlayn jinoyat turlaridan biri bo‘lmish Tovlamachi dasturlardan foydalanish bilan bog‘liq jinoyatlarga, quydagi vaziyat yorqin misol tariqasida keltirilishi mumkin.

Jinoyatchilar internet tarmog‘idagi pornografik materiallar, shavqatsizlikni targ‘ib qiluvchi saytlarda o‘zlarini huquqni muhofaza qiluvchi organlar yoxud IIV Kiberxavfsizlikga qarshi kurash bo‘limi tomonidan foydalanuvchi ma’muriy javobgarlikka tortilgani va ma’lum bir pul miqdorini belgilangan hisob raqamga ko‘chirishi shartligini talab qilishadi. *Masalan, “O‘zbekiston Respublikasi IIV Kiberjinoyatlarga qarshi kurash bo‘limidan bildirishnoma! Siz O‘zbekiston Respublikasi qonunchiligi bilan taqiqlangan materiallar, ya’ni pedofiliya, zo‘ravonlikni targ‘ib qilish elementlariga ega bo‘lgan pornografiya materiallari mavjud bo‘lgan pornografik saytlarga tashrif buyurganligingiz uchun blokirovka qilindingiz. Blokirovkani echish uchun Siz shu plastik hisobraqamiga yoki davlat hamyoniga 310.000 so‘m miqdorida jarima to‘lashingiz zarur”*[6].

Odatda, bunday noqulay vaziyatdan tezroq chiqish hamda sharmandalik va javobgarlikdan qutulish maqsadida talab qilingan pul summasini tegishli hisob raqamga o‘tkaziladi. Biroq, afsuski IIV Kiberjinoyatlarga qarshi kurash bo‘limi xech kimga bunday habar yubormaydi.

Ushbu holat o‘zida firibgarlik alomatlarini ham mujassamlashtirgan bo‘lib, bu vaziyatda biz onlayn firibgarlik va onlayn tovlamachilik tushunchalarini bir biridan ajratib olishimiz lozim. Sababi, ***birinchidan***, jinoyatchi o‘zini huquqni muhofaza qiluvchi organ hodimi deb tanishtirib, jabrlanuvchini aldaydi. ***Ikkinchidan***, jinoyatchi jabrlanuvchining internet tarmog‘idan foydalanish huquqini

[4] Baxin V.P. Kriminalisticheskaya xarakteristika prestupleniy kak element rassledovaniya // Vestnik kriminalistiki. – Moskva, 2006. – Vып. 1. – S. 140.

[5] Kudryavsev D.S. Osobennosti kriminalisticheskoy xarakteristiki ubiystv, zamaskirovannых pod bezvestnoe ischeznovenie cheloveka // Aktualnые problemы sovremennoy kriminalistiki i sudebnoy ekspertizы: materialы mejdunar. nauch.-prakt. konf., posvyaщ. 35-letiyu so dnya obrazovaniya kafedrы kriminalistiki Akad. MVD Resp. Belarus (Minsk, 3 iyunya 2011 g.). – Minsk: Akad. MVD, 2011. – S.160.

[6] https://iiv.uz/news/ogoh-boling-internet-tarmogida-firibgarlar

muayyan vaqt oralig‘ida cheklaydi. Blokirovkani echish uchun plastik hisob raqamiga yoki “davlat hamyoni”ga 310.000 so‘m miqdorida jarima to‘lashi zarurligiga ishontiradi. Aslida, ushbu holat raqamli qurilmani vaqtincha bloklab qo‘yilganiga ishontirish orqali amalga oshiriladi.

O‘zbekiston Respublikasi Oliy sudi Plenumining 2017 yil 11 oktyabrdagi ***“Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”***gi 35-son qaroriga muvofiq “firibgarlikda yolg‘on ma’lumotlarga jabrlanuvchini yanglishtirishga olib kelishi mumkin bo‘lgan har qanday holatlar, jumladan, yuridik fakt va voqealar, mulkning sifati, narxi, aybdorning shaxsi, uning vakolati, niyati (masalan, aybdor shaxs o‘zini mansabdor shaxs yoki huquqni muhofaza qiluvchi organ xodimi sifatida ko‘rsatishi) taalluqli bo‘lishi mumkin” – deyiladi[7].

Vektor hujumlar sirasiga DoS, DdoS hamda fishing firibgarligi yorqin misol bo‘la oladi. So‘nggi paytlarda hukumat saytlarining ish faoliyatida uzilishlarga olib keluvchi hujumlarga ko‘proq duch kelmoqda. **DoS va DDoS hujumlari** tashkilotlarga moddiy zarar etkazishi mumkin, shuningdek, resurslar va xizmatlarning vaqtinchalik ish faoliyatida uzilishlar tufayli tashkilotning sha’niga putur etkazish xavfi mavjud. Shu sababli, ushbu turdagi hujumlardan himoyani ta’minlash muhimdir. Xizmatni rad etish hujumi **(Distributed Denial-of-service, DDoS)** — bu ma‘lum bir axborot tizimi va resurslarning ish faoliyatini vaqtinchalik to’xtatish maqsadida amalga oshiriladigan hujum turidir. DoS va DDoS hujumlarining ko'plab shakllari mavjud bo'lsada, eng keng tarqalganlari: tarmoq resurslarining tugashi, protokol resurslarining tugashi, dastur resurslarining tugashidir. DDoS hujumi bir nechta hujum kompyuterlaridan amalga oshiriladi[8].

Fishing

Bank kartalari bilan bog‘liq firibgarlik jinoyatini sodir etish usullaridan biri bu “fishing” ya’ni “baliq ovi” usulidir. Bunda IT texnologiya sohasida etarli bilim va ko‘nikmalarga ega firibgarlar tomonidan foydalanuvchining ishonchiga kirib, bank kartasiga doir maxfiy ma’lumotlari egallanadi[9].

Jinoyatni sodir etish usulining o‘ziga xos xususiyati shundaki, jinoyatchi tomonidan masofadan turib aloqa vositalari yoxud sohta veb-sahifalar orqali foydalanuvchining ijtimoiy tarmog‘idagi akkaunti, elektron pochtasi yoki uyali

[7] O‘zbekiston Respublikasi Oliy sudi Plenumining 2017 yil 11 oktyabrdagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 35-son qarori 4-bandning ikkinchi xatboshisi.

[8] https://csec.uz/uz/news/maqolalar/ddos-hujumlarini-tushunish-va-ularga-chora-ko-rish/

[9] Шаззо С.К. Способи совершения мошенничества в отношении граждан [Метҳодс оф соммиттинг фрауд агаинст ситизенс]. Вестник Адигейского государственного университета. Серия 1: Юриспрудентсия. 2008. № 2. С. 5.

aloqa vositalariga sms habar yuboriladi. Bunda ijtimoiy muhandislik usullaridan foydalaniladi. Bu xususida quyida batafsil tushuntirish keltirib o‘tamiz.

“Fishing” bilan shug‘ullanuvchi jinoiy guruhlar jabrlanuvchidan shaxsiy ma’lumotlarini kiritishni so‘rab turli shaklda xabarnoma jo‘natishadi. Jabrlanuvchi bank xizmatlaridan foydalanish uchun bankning rasmiy veb-saytiga kirayotganliklariga ishonadi. Biroq, firibgarlar tomonidan yaratilgan tuzoqlarga laqqa tushadilar. Xususan, soxta saytga ism-sharifi, karta rekvizitlari, pin kodi kiritish orqali o‘zlari bilmagan holda “fishing”chilar qarmog‘iga ilinishadi[10]. Soxta saytlar yaratish bu zamonaviy fishing uslublaridan biridir. Bunday fishing saytlarini maxsus bilim va ko‘nikmalarsiz aniqlash juda mushkul.

IV. Munozara

Internet orqali sodir etiladigan jinoyatlarda anonimlikni saqlash prinsipial ahamiyatga ega. Shunga qaramay, ushbu jinoyatlarning deyarli barchasida texnik tavsifdagi izlar mavjud.

O.Y.Vvedenskaya raqamli izlar ro‘yxatiga IP-adreslar, ro‘yxatdan o‘tgan domen nomlari, foydalanuvchilarning akkaunt ma’lumotlari, log-fayllar, cookie fayllari, tashrif buyuurilgan saytlar kesh fayl ma’lumotlari (vaqtinchalik fayllar) va brauzer tarixi, DNS-serverlar bilan bog‘liq izlar, xosting-provayderlardagi izlar, reklama veb-sahifalari izlari, jabrlanuvchi raqamli qurilmasida saqlanib qolgan yozishmalar, qabul qilingan buyurtmalar izlari, mobil qurilma unikal raqami (IMEI), sim karta ma’lumotlari, bank karta hisob raqamlari, hisob raqamlardagi pul tushumi va chiqimi bilan bog‘liq izlarni kiritgan[11].

Kesh-xotira – inglizcha “cache memory” ya’ni, protsessor faoliyatini kutishdan xalos qiladigan tezlik bilan ishlaydigan buferli xotira qurilmasi bo‘lib, juda katta tezlik bilan ishlaydigan protsessorlarning paydo bo‘lishi, kesh-xotirani yaratish zaruratini keltirib chiqargan. Shu bilan birga, murakkab amaliy dasturlarning bajarilishi uchun katta xotira zarur edi. Shu sababli, operativ xotira bilan protsessor orasiga, kichkina sig‘imli yuqori tezlikli kesh-xotira deb atalgan buferni o‘rnatish amaliyoti boshlangan. Buning ustiga, uni protsessor ichiga o‘rnatilgan va tashqi turlari mavjud[12].

DNS keshi – bu inglizcha “domain name service” ya’ni, barcha so‘nggi tashriflar va boshqa veb-sayt IP manzillariga kirishga urinishlar yozuvlarini o‘z

[10] Изотов Д. С., Бикова Н. Н. Види мошенничества с банковскими картами [Сее банк сард фрауд]. Вестник НГИЕИ. 2015. – № 3. – С.49-52.

[11] Yuridicheskaya nauka i pravooxranitelnaya praktika 4 (34) 2015 Vvedenskaya O.Yu. Osobennosti sledoobrazovaniya pri sovershenii prestupleniy posredstvom seti internet. S 213-214.

[12] Amirov D.M., Atadjanov A.Yu., Atadjanov D.Yu., Ibragimov D.A., Rahimjonov Z.Yo., Saidxo‘jaev S.S. AXBOROT-KOMMUNIKATSIYa TEXNOLOGIYaLARI IZOHLI LUG‘ATI © BMTTDning O‘zbekistondagi vakolatxonasi, 2010 576-b.

ichiga olgan vaqtinchalik ma’lumotlar bazasidir. DNS keshi raqamli qurilma sahifaga yana tashrif buyurganingizda, ular tezroq ochilishi uchun qulaylik yaratadi.

URL – bu inglizcha “Uniform Resource Locator” ya’ni, resurs joyining universal ko‘rsatkichidir.

Kesh fayllar (vaqtinchalik fayllar) – bu HTML - fayllar nusxasi, veb-saytga kirgan paytta yuklanadigan suratlar va boshqa kichik fayllar. Bu ma’lumotlar lokal diskda saqlanib, yana shu sahifaga qaytganda sahifani tezroq yuklanishiga yordam beradi.

Jinoyatning issiq izidan borishda tergov va tezkor qidiruv xodimlari shaxsga doir ma’lumotlarni to‘plash maqsadida aloqa kompaniyalariga, bank yoki elektron to‘lov tizimlari operatorlariga so‘rov jo‘natishadi. Aloqa operatorlari shaxsni ro‘yxatdan o‘tgan sim kartalari, IMEI – raqamlari, kiruvchi va chiquvchi qo‘ng‘iroqlar sms xabarlari haqidagi barcha ma’lumotlarni taqdim etishadi.

Shu bilan birga, jinoyatchini ushlashda bank tomonidan taqdim etilgan ma’lumotlar ham muhim ahamiyat kasb etadi. Ushbu ma’lumotlarga banklar tomonidan taqdim etiladigan shaxsga doir ma’lumotlar, pul ko‘chirish bilan bog‘liq moliyaviy operatsiyalar, onlayn bank ma’lumotlari, valyuta konvertatsiyasi va boshqa ma’lumotlar kiradi[13].

Bank kartalari bilan bog‘liq firibgarlik jinoyatlarida hodisa sodir etilgan joyni aniqlash masalasi boshqa jinoyatlarga qaraganda ancha mushkul hisoblanadi. Sababi, bu toifadagi jinoyatlarda jinoyatchi asosan boshqa davlatdan turib jinoyatni sodir etadi. Ko‘p hollarda jinoyatchilar pullarni boshqa pul birligiga konvertatsiya qilib, bir davlat hududidan boshqa davlat hududiga o‘tkazib yuborishadi va bu holat ishni yanada chigallashtirib, yurisdiksiya (ekstraditsiya) bilan bog‘liq muammolarni keltirib chiqaradi.

V. Xulosa

Xulosa qilib aytganda, raqamli texnologiyalarning shiddat bilan rivojlanib borishi yangi munosabatlar vujudga kelishiga sabab bo‘lmoqda. Biroq, ushbu munosabatlarni o‘z vaqtida nazorat qilish va tartibga solish muayyan kriminalistik va huquqiy tadqiqotlarni olib borishni taqozo etmoqda. Aks holda, inson, jamiyat va davlat manfaatlari turli iqtisodiy, siyosiy, huquqiy va ma‘naviy tahdidlar ostida qolishi ayni haqiqatdir. Amaldagi qonunchilikda onlayn firibgarlik, o‘g‘rilik va tovlamachilik jinoyatlarini kvalifikatsiya qilish bo‘yicha huquqiy bo‘shliqlarning

[13] Lavrushkina A. A. Tipichnie sledstvennie deystviya v ramkax metodiki rassledovaniya moshennichestva s ispolzovaniem seti Internet i sredstv mobilnoy svyazi [Typical investigative actions within the methodology for investigating fraud using the Internet and mobile communications] Byulleten nauki i praktiki. 2018. T. 4. №4. S. 447-451. Rejim dostupa: http://www.bulletennauki.com/lavrushkina-a (data obrasheniya 15.04.2018).

mavjudligi huquqni qo‘llash sohasida muayyan uslubiy qiyinchiliklarni ham yuzaga keltirmoqda.

Shunga ko‘ra, amaldagi qonunchilikni takomillashtirish hamda huquqiy tartibga solishning samarali mexanizmlarini joriy etish bo‘yicha quyidagilar taklif etiladi:

1. Ushbu jinoyatlar yuzasidan alohida Oliy sud Plenumi qarorlarini va amaliyot xodimlariga mo‘ljallangan ilmiy, amaliy o‘quv qo‘llanmalarni ishlab chiqish;

2. O‘zbekiston Respublikasining 2022-2026 yillarga mo‘ljallangan Harakatlar strategiyasida kiberjinoyatlarni tergov qilish uslubiyotini takomillashtirish bo‘yicha alohida vazifalar belgilash;

3. O‘zbekiston Respublikasining “To‘lov va to‘lov tizimlari to‘g‘risida”gi qonunida to‘lov tashkilotlari (operatori) tomonidan amalga oshirilayotgan onlayn moliyaviy xizmatlar xavfsizligini ta‘minlash uchun to‘lov xizmatlaridan foydalanuvchilarni autentifikatsiya qilishning samarali mexanizmlarini joriy qilish;

4. Kadrlar masalasiga alohida e’tibor qaratish, xorijiy mutaxassislarni jalb qilgan holda tergov va sud tizimi xodimlarini kiberjinoyatlarni tergov qilish bilan bog‘liq bilim va ko‘nikmalarini shakllantirish maqsadida, o‘quv kurslarini tashkil etish va ularni malakasini oshirish.

Ushbu islohotlar o‘z navbatida qonunni to‘g‘ri va o‘z o‘rnida qo‘llashga, yuqorida keltirilgan jinoyatlarni oldini olishga va jinoyatchilikka qarshi murosasiz kurashishga xizmat qiladi.

References

1. 2022 yil 28 yanvardagi O'zbekiston Respublikasi Prezidentining «Yangi O'zbekistonning 2022–2026 yillarga mo'ljallangan taraqqiyot strategiyasi to'g'risida»gi PF–60-son Farmoni.
2. Jinoyatlarni tergov qilishning kriminalistik metodikasi: O‘quv qo‘llanma / R.R. Shakurov, Sh.T. Djumanov, N. Toshtemirov, D.R. Turaeva, O.D. Allanazarov. – T: O‘zbekiston Respublikasi IIV akademiyasi, 2013. – 5 b.
3. Kriminalistika. Darslik. Mualliflar jamoasi. Abdumajidov G‘.A. va b.q. – T.: Adolat, 2003. T. 2. – 74 b.
4. Baxin V.P. Kriminalisticheskaya xarakteristika prestupleniy kak element rassledovaniya // Vestnik kriminalistiki. – Moskva, 2006. – Vып. 1. – S. 140.

5. Kudryavsev D.S. Osobennosti kriminalisticheskoy xarakteristiki ubiystv, zamaskirovannых pod bezvestnoe ischeznovenie cheloveka
6. https://iiv.uz/news/ogoh-boling-internet-tarmogida-firibgarlar
7. O‘zbekiston Respublikasi Oliy sudi Plenumining 2017 yil 11 oktyabrdagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 35-son qarori 4-bandning ikkinchi xatboshisi.
8. https://csec.uz/uz/news/maqolalar/ddos-hujumlarini-tushunish-va-ularga-chora-ko-rish/
9. Shazzo S.K. Sposobi sovershеniya moshennichestva v otnoshenii grajdan [Methods of committing fraud against citizens]. Vestnik Adigeyskogo gosudarstvennogo universiteta. Seriya 1: Yurisprudentsiya. 2008. № 2. S. 5.
10. Izotov D. S., Bikova N. N. Vidi moshennichestva s bankovskimi kartami [See bank card fraud]. Vestnik NGIEI. 2015. – № 3. – S.49-52.