WORLDLY KNOWLEDGE
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCHERS
ISSN : 3030-332X IMPACT FACTOR (Research bib) – 7,293

Xushnud Kazakov

Toshkent davlat iqtisodiyot universiteti Samarqand filiali,

Moliya, soliq va bank ishi kafedrasi katta o'qituvchisi

O'ZBEKISTON RESPUBLIKASI TIJORAT BANKLARIDA MIJOZLARNING BANK PLASTIK KARTALARI MABLAG'LARINING XAVFSIZLIGI VA KIBERJINOATCHILIKKA QARSHI KURASHISH VA OLDINI OLISH

Annotatsiya: Ushbu maqola O'zbekiston Respublikasi tijorat banklarida bank plastik kartochkalarida saqlanadigan mijozlar pul mablag'larini himoya qilishning muhim masalasini ko'rib chiqadi. Maqola kiberjinoyatlar keltirib chiqaradigan muammolarni o'rganib chiqadi, xavfsizlikni kuchaytirish uchun banklar va hukumat tomonidan amalga oshirilayotgan turli choralarni ta'kidlaydi. Maqolada, shuningdek, jamoatchilikni xabardor qilish tashabbuslari muhokama qilinadi va O‘zbekistonda raqamli moliyaviy ekotizimni mustahkamlashning kelajakdagi yo‘nalishlari o‘rganiladi.

Kalit so'zlar: Kiberjinoyat, Bank plastik kartalari, Kiberxavfsizlik, O‘zbekiston, Firibgarlikning oldini olish, Ma’lumotlar xavfsizligi, Aholini xabardor qilish, Moliyaviy inklyuziya, Raqamli Transformatsiya.

Raqamli texnologiyalar va onlayn tranzaktsiyalarning jadal rivojlanishi butun dunyo bo'ylab bank landshaftini o'zgartirdi. O‘zbekiston, boshqa ko‘plab davlatlar singari, raqamli inqilobni qabul qilmoqda, naqd pulsiz jamiyatni rivojlantirmoqda va moliyaviy inklyuzivlikni qo‘llab-quvvatlamoqda. Biroq, bu raqamli evolyutsiya, ayniqsa, kiberxavfsizlik sohasida yangi muammolarni keltirib chiqaradi. Kiberjinoyat, shu jumladan bank plastik kartalariga qaratilgan firibgarlik ham jismoniy shaxslar, ham moliya institutlari uchun jiddiy xavf tug‘diradi. Ushbu maqola O‘zbekistonda mijozlarning bank plastik kartochkalarida saqlanadigan mablag‘larini himoya qilish, kiberjinoyatlarga qarshi kurashish va xavfsiz raqamli moliyaviy ekotizimni yaratish bo‘yicha ko‘rilayotgan chora-tadbirlarni o‘rganadi.

Tijorat banki – tijorat asosida bank faoliyati, ya'ni mablag‘larni jalb qilish va kreditlarni taqdim etish, bank hisobvaraqlarini ochish va uni yuritish hamda to‘lovlarni o‘tkazish kabi amaliyotlarni amalga oshiruvchi kredit tashkilotidir. Tijorat banklari – bo’sh pulga (jamg‘armaga) ega va pulga muhtoj bo‘lganlar o‘rtasidagi vositachilardan biri hisoblanadi.

Kiber jinoyat kuchli hackerlar tomonidan amalga oshiriladi. Davlatga, jamiyatga xavf tug'diradigan harakatlarni paydo qiladi. Bunda asosiy maqsad pul undurish va yuqorida aytganimizdek xavfli harakatlarni vujudga keltirishdir. Kiberjinoyat kompyuterlardan foydalangan holda amalga oshiriladi. Bunda kompyuter qurol vazifasini bajaradi. Banklardan pul undurish, har xil tashkilot, korxonalardan har xil yo'l bilan pul undurishadi. Bundan tashqari, fuqarolarning plastik kartalaridan pul yechib olish kabi firigbarliklar avj olmoqda. Kiberjinoyatchilikning ko'plab turlari bor. Masalan, kiberpornografiya, kiberjinoyat, iqtisodiy firibgarlik jinoyati, kiberterrorchilik, zararli dasturlar orqali kiberjinoyat, atribut firibgarlik.

Kartochka ostida firibgarlik deganda ayrim shaxslarning bank kartalaridan foydalanishga asoslangan va karta egalarining karta hisobvaraqlariga joylashtirilgan pul mablag'larini ruxsatsiz olish yoki kartochkalar bo'yicha operatsiyalarni amalga oshirish uchun savdogarlar tomonidan amalga oshirilgan qasddan firibgarlik harakatlari tushuniladi.

Bugungi kunda elektron to‘lovlar, plastik kartalar, kompyuter tarmoqlarining keng tarqalishi natijasida bevosita ham banklar, ham bank mijozlarining pul mablag‘lari axborot hurujlarining ob’yektiga aylanmoqda. Pul o‘g‘irlashga har qanday g‘arazli shaxs urinib ko‘rishi mumkin – buning uchun unda

kompyuter va internet tarmog‘i bo‘lsa bas. Bunda bank ichiga jismonan kirish ham shart emas, minglab kilometr uzoqlikdagi masofadan ham firibgar maqsadini amalga oshiraveradi.

Bankning axborot xavfsizligida esa quyidagi maxsus omillarni hisobga olish zarur:

Haqiqiy pul mablag‘lari aks etuvchi va bank tizimlarida saqlanuvchi hamda ishlanuvchi ma’lumot. Kompyuter ma’lumotlariga asosan to‘lovlar amalga oshirilishi, kreditlar ochilishi, katta miqdordagi mablag‘lar hisobdan hisobga o‘tkazilishi mumkin. Ushbu ma’lumotlardan noqonuniy ravishda foydalanish jiddiy zararlarga olib kelish mumkinligi barchaga ayon. Bu xususiyat banklarga nisbatan (masalan, ichki ma’lumoti juda kam shaxslarga qiziq bo‘lgan sanoat kompaniyalaridan farqli ravishda) tajovuz qiluvchi jinoyatchilar doirasini shiddat bilan kengaytiradi.

Bank tizimlaridagi ma’lumotlar ko‘p sonli odamlar va tashkilotlar — mijozlarning manfaatlarini qamrab oladi. Odatda, ushbu ma’lumotlar maxfiy bo‘ladi va bank o‘z mijozlari oldida ularning talab darajasidagi maxfiyligini ta’minlash uchun javobgar bo‘ladi. Mijozlar ham o‘z bankiga ishonishga haqli, aks holda bank reputatsiyasini, ya’ni obro‘yini yo‘qotishi mumkin.

Bankning raqobatbardoshligi mijozlarga yaratilgan qulaylik, ko‘rsatilayotgan xizmatlar spektrining kengligi, masofadan xizmatlar ko‘rsata olishiga bog‘liq. Mijoz o‘z mablag‘larini tezkorlik bilan boshqarish imkoniyatiga ega bo‘lishi zarur. Biroq bunday qulaylik bank tizimlariga jinoyatchilarning onlayn-hujumi ehtimolini kuchaytiradi. Bankning axborot xavfsizligi kompyuter tizimlarining ishini hatto favqulodda holatlarda ham yuqori darajadagi ishonchlilik bilan ta’minlashi zarur, chunki bank nafaqat o‘z mablag‘lari, balki mijozlar pullari uchun ham javobgar hisoblanadi.

Afsuski, bugungi kunda hatto maxfiy ma’lumotlardan foydalanishga oid o‘ta qat’iy choralar ham kiberjinoyatlarning yo‘lini to‘liq to‘sib qo‘ya olmaydi. Shuning uchun ma’lumotlarni himoyalashning tizimli yondashuvida axborot xavfsizligini ta’minlash uchun bank tomonidan foydalanilayotgan vositalar va harakatlar (tashkiliy, jismoniy dasturiy-texnik) o‘zaro chambarchas bog‘liq. Bunda choralarning yagona kompleksi ishlab chiqilishi talab etiladi. Ushbu kompleks nafaqat ma’lumotlarni saqlashga, ularni tasodifiy yo‘q qilish, o‘zgartirish yoki oshkora qilishni oldini olishga ham yo‘naltirilgan bo‘lishi zarur.

O'zbekiston Respublikasida kiberjinoyatga qarshi kurashish uchun davlat va tijorat banklari tomonidan bir qancha xavfsizlik choralari amalga oshirilmoqda.

1. Firibgarlikni aniqlashning ilg‘or tizimlari yaratilmoqda. O‘zbekiston tijorat banklari sun’iy intellekt va mashinani o‘rganish algoritmlari bilan ta’minlangan firibgarlikni aniqlashning murakkab tizimlarini bosqichma-bosqich o‘zlashtirmoqda. Ushbu tizimlar real vaqt rejimida tranzaksiya shakllarini tahlil qiladi, anomaliyalarni aniqlaydi va shubhali harakatlar haqida ogohlantirishlarni ishga tushiradi.

2. Bank kartalari uchun EMV chip texnologiyasining qabul qilinishi xavfsizlikni sezilarli darajada oshirdi. Ushbu chiplar ilg'or shifrlash va raqamli imzolardan foydalanadi, bu ularni an'anaviy magnit chiziqli kartalarga qaraganda qalbakilashtirish va kartadagi firibgarlikka nisbatan ancha chidamli qiladi.

3. Ko‘pgina banklar onlayn va mobil banking tranzaksiyalari uchun 2FAni joriy qilgan. Ushbu qo'shimcha xavfsizlik qatlami foydalanuvchilardan parolidan tashqari mobil telefon yoki elektron pochta kabi ikkinchi qurilma yoki usul yordamida o'z shaxsini tasdiqlashni talab qiladi.

4. Banklar firibgarlik ko‘rsatkichlari bo‘yicha tranzaktsiyalarni doimiy ravishda tahlil qilish uchun real vaqt rejimida tranzaksiya monitoringi tizimlaridan foydalanadilar. Bu tezkor aralashuv va shubhali harakatlarni blokirovka qilish imkonini beradi.

5. Biometrik autentifikatsiya. Ba’zi banklar xavfsizlikni kuchaytirish va foydalanuvchilarga qulayroq tajribani ta’minlash uchun barmoq izi yoki yuzni tanish kabi biometrik autentifikatsiya usullarini joriy qilmoqda.

6. O‘zbekistonda kiberjinoyatlarga qarshi kurashish bo‘yicha qonunchilik bazasi mustahkamlandi. Qonunlar turli kiber huquqbuzarliklarni jinoiy javobgarlikka tortadi, ma'lumotlarni himoya qilish standartlarini belgilaydi va xalqaro hamkorlik mexanizmlarini belgilaydi. O'zbekiston Respublikasi Prezidentining 2018-yil 14-maydagi "Jinoyat va jinoyat-protsessual qonunchiligi tizimini tubdan takomillashtirish chora-tadbirlari to'g'risida"gi PQ-3723-sonli Qarorida "Texnologik taraqqiyot, jumladan kiberjinoyat bilan bog'liq jinoyat turlarining kengayganligini hisobga olgan holda axborot texnologiyalari sohasida javobgarlikni nazarda tutuvchi normalarni qayta ko'rib chiqish" nazarda tutilgan. Undan tashqari O'zbekiston Respublikasi Jinoyat kodeksining 278^5-moddasiga ko'ra, o'zganing kompyuter uskunasini qasddan ishdan chiqarish, xuddi shuningdek kompyuter tizimini buzish (kompyuter sabotaji):

-3 yilgacha muayyan huquqdan mahrum qilib, 66 mln 900 ming so'mdan 89 mln 200 ming so'mgacha miqdorda jarima;

-2 yilgacha ozodlikni cheklash;

-2 yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

-shuningdek, mazkur harakatlami guruh bo'lib, takroran yoki xavfli residivist tomonidan sodir etish 3 yilgacha ozodlikdan mahrum qilish bilan jazolashga sabab bo'lishi mumkin.

7. O‘zbekiston Markaziy banki bank sektori uchun kiberxavfsizlik qoidalarini belgilash va amalga oshirishda hal qiluvchi rol o‘ynaydi. Ushbu qoidalar xavflarni boshqarish, hodisalarga javob berish, ma'lumotlar xavfsizligi protokollari va bank xodimlari uchun kiberxavfsizlik bo'yicha treningni o'z ichiga oladi.

8. Xalqaro tashkilotlar bilan hamkorlik. O‘zbekiston INTERPOL, Yevropada Xavfsizlik va Hamkorlik Tashkiloti (EXHT) kabi xalqaro tashkilotlar va boshqa tegishli organlar bilan axborot, ilg‘or tajriba almashish va kiberjinoyatga qarshi kurashda salohiyatni oshirish maqsadida faol hamkorlik qiladi.

O'zbekiston Respublikasi tijorat banklarida mijozlarning bank plastik kartalari mablag'larining xavfsizligi va kiberjinoatchilikka qarshi kurashish va oldini olishga juda katta e'tibor berilmoqda. Banklar, xavfsizlik sohasida kiberatakalar va xavfsizlik tinchlik tizimlari yaratish uchun keng ko'lamli chora-tadbirlar olib borishadi. Kiberjinoyatning global xarakterini hisobga olgan holda, kuchli xalqaro hamkorlik chegaralar osha kiberjinoyatchilarning samarali oldini olish, tergov qilish va jinoiy javobgarlikka tortish uchun muhim ahamiyatga ega. Kiberjinoyatchilikka qarshi Budapesht konvensiyasi 2001 yil 23-noyabr, Internet va kompyuter jinoyati (kiberjinoyat)larni uyg'unlashtirish orqali milliy qonunlar, tergov usullarini takomillashtirish va xalqlar o'rtasidagi hamkorlikni oshirish yuzasidan imzolangan.

2006 yil 1 martda Kiberjinoyatchilik to'g'risidagi konvesiyaga qo'shimcha protokol kuchga kirdi. Qo'shimcha protokolni ratifikatsiya qilgan davlatlar irqchi va ksenofobik kompyuter tizimlari orqali material, shuningdek, irqchilik yoki ksenofobiya tomonidan tahdid va haqorattarqatishni jinoiy javobgarlikka tortishlari shartligi belgilandi.

Konvensiya Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar bo'yicha birinchi xalqaro shartnomadir, xususan mualliflik huquqining buzilishi, kompyuter bilan bog'liq firibgarlik, bolalar pomografiyasi, tahdid jinoyatlariva tarmoq xavfsizligi jinoyatlarigi o'z ichiga oladi. Shuningdek, u kompyuter tarmoqlarini qidirish va qonuniy ushlashga doir qator vakolatlar va protseduralarni o'z ichiga oladi. Uning muqaddimasida keltirilgan asosiy maqsadi jamiyatni himoya qilishga qaratilgan umumiy jinoyat siyosatini olib borishdir. Shuningdek, kiberjinoyatlarga doir tegishli qonunlarni qabul qilish va joriy etish orqali xalqaro hamkorlikni targ'ib etadi.

9. Jamoatchilikni xabardor qilish va kiberxavfsizlik bo‘yicha ogohlik kampaniyalari. Hukumat va moliya institutlari fuqarolarni kibertahdidlar, xavfsiz bank amaliyotlari va shaxsiy ma’lumotlarni onlayn himoya qilish muhimligi haqida ma’lumot berish maqsadida jamoatchilikni xabardor qilish kampaniyalarini faol o‘tkazmoqda. Ushbu kampaniyalar turli kanallardan, jumladan, ijtimoiy media, an'anaviy media va ta'lim dasturlaridan foydalanadi. Moliyaviy savodxonlikni oshirish kiberxavfsizlik sohasidagi sa’y-harakatlarning muhim tarkibiy qismidir. Moliyaviy savodxonlik dasturlari jismoniy shaxslarga asosiy moliyaviy tushunchalarni tushunish, fishing urinishlarini tan olish, firibgarliklardan qochish va xavfsiz onlayn xatti-harakatlarni amalga oshirish imkonini beradi.

Ammo bir qancha qiyinchiliklar ham mavjud. Kiberjinoyatchilar o‘z taktikalarini doimiy ravishda moslashtirib, xavfsizlik choralarini paydo bo‘layotgan tahdidlarga qarshi turishni talab qiladilar. Buning uchun fuqarolardan ogohlik, kodlar va ma'lumotlarini begona shaxslarga aytmaslik talab qilinadi.

Hozirgi rivojlangan XXI-asrda hayotimizni zamonaviy axborot texnologiyalarisiz tasavvur qilishimiz qiyin shu jumladan yashash tarzimizni osonlashtirgan, foydali taraflari ko'p bo'lgan bilan albatta foydasiz taraflari ham bor. Tangani ikki tarafi bo'lgani kabi yaxshi va yomon jihatlari bor. Har birimiz ishlayotgan kompyuter, telefon, smartfon va hokozolarni ishlatish bilan birga ehtiyot bo'lishimiz kerak. Bulardan eng asosiysi xavfsizlik turidir. Ya'ni biz foydalanayotgan mobil telefon, kompyuterlarimizda shaxsiy ma'lumotlarimizni saqlaymiz. Deyarli ko'p odamlar hozirda online viza kartalar ochishgan, click, payme kabilardan onlayn pul o'tkazmalaridan foydalanib kelishadi. Albatta bu ilovalardan foydalanishdan oldin registratsiyadan o'tasiz, shaxsiy ma'lumotlaringiz bilan. Endi hozirda juda ko'p uchrayotgan jinoyatchilik turlaridan biri bu kiberjinoyatchilikdir. Kiberjinoyatni ommaviy axborot vositalarida, ijtimoiy tarmoqlarda, har bir odamning telefon raqamlariga hatto sms yuborilib bizni ogohlantirishmoqda. Afsuski shuncha ogohlantirishlar bilan o'zimiz bilmagan holda kiberjinoyatning qurboni bo'lib qolyapti. Axborot texnologiyalari rivojlanishi bilan kiberjinoyatchilik ortmoqda.

AQSH davlati rivojlangan davlatlardan biri sanaladi. Aqshda 2012-yil onlayn kridet va kartalardagi jinoyatlar 1.5 mlrd dollarni tashkil qilgan. Rossiyada esa 2013-yilda kartalar bo'yicha firibgarlik yevropada 4-o'rinni 4, 6 mlrd rublni tashkil etgan. Kiberjinoyatni oldini olishning asosiy yo'llaridan biri bu davlatlar o'rtasidagi kiberxavfsizlik bo'yicha tuziladigan shartnomalardir. Bunda davlatlarning qo'llagan ko'proq samarali usullaridan foydalanishadi, mustahkam, puxta reja tuzilib shu bo'yicha ish olib boriladi.

Kiberjinoyatga mustahkam bardosh bera oladigan dastur yoki web ilovalar, antivirus dasturlari yo'q albatta. Faqat hozirda zamonaviy axborot texnologiyalari davrida, zamonaviy kiberhujumlarga dosh bera oladigan, har xil sharoitga moslasha oladigan turli qurilmalar, himoyalangan dasturlar yaratishni imkoni bor. Kiberxavfsizlikka kurashish, kiberjinoyatlarning oldini olish uchun yagona chora bu himoyalangan kuchli platforma bo'lishidir. Albatta har bir tashkilotning kiberxavfsizligi yuqori darajada. bo'lsagina bunday vaziyatda g'olib bo'la olishadi. Kiberjinoyatchilar avvalo ma'lumot o'g'irlashmi, hujjatlar, bankdn pul undurish, id-karta, viza kartadan pul o'g'irlash va boshqa hamma kiberjinoyatlarda kodlarni buzib kirish uchun eng avvalo keng tarqalgan usullardan foydalanishadi. Hozirda eng oddiy, sodda va ko'p qo'llaniladigan parollar juda ommalashgan.

Kiberjinoyatlar axborot texnologiyalari sohasidagi jamoatchilik munosabatlariga jiddiy tahdid soladi va shuning uchun zamonaviy sharoitda ularga qarshi kurashish davlat va fuqarolar uchun jiddiy muammoga aylandi. Davlatning huquqni muhofaza qilish organlari ularni zararsizlantirish bo'yicha qarshi choralarni ishlab chiqmoqda, kiberjinoyatlarga qarshi kurashish strategiyasi va taktikasini ishlab chiqmoqda.

Xulosa sifatida aytishimiz mumkinki, O‘zbekistonda mijozlarning bank plastik kartochkalarida saqlanayotgan mablag‘larini himoya qilish va kiberjinoyatlarga qarshi kurashish borasida sezilarli yutuqlarga erishildi. Ilg'or xavfsizlik choralarini amalga oshirish, qonunchilik bazasini mustahkamlash va aholini xabardor qilish tashabbuslari raqamli moliyaviy landshaftni yanada xavfsizroq qilishga yordam berdi. Biroq, rivojlanayotgan tahdidlarga doimiy moslashish, kiberxavfsizlik infratuzilmasiga

barqaror sarmoya kiritish va mustahkam xalqaro hamkorlik chinakam mustahkam raqamli moliyaviy ekotizimni yaratish uchun juda muhim. Ushbu muammolarni samarali hal etish orqali O‘zbekiston o‘z fuqarolari mablag‘larining xavfsizligi va xavfsizligini ta’minlab, dinamik va inklyuziv raqamli iqtisodiyotning o‘sishiga yordam berishi mumkin.

Foydalanilgan adabiyotlar ro'yxati:

1. Pronkin Leonid, Pudalev Timofey, Holmatov Farruh, Yavnoshanov Dmitriy Analysis of security risks to network transactions // Евразийский научный журнал. 2015. №12.
2. Umarov Zafar. A, Toshpulatova Shakhrizoda. Sh. COVID-19 AND THE BANKING INDUSTRY IN UZBEKISTAN: IMPACT AND SOLUTIONS // Austrian Journal of Humanities and Social Sciences. 2020. №3-4. URL: https://cyberleninka.ru/article/n/covid-19-and-the-banking-industry-in-uzbekistan-impact-and-solutions
3. To’xtayev Sardor Sulton O’G’Li RAQAMLI TEXNOLOGIYALAR SOHASIDAGI HUQUQBUZARLIKLARGA QARSHI KURASHISH HAMDA AXBOROT XAVFSIZLIGINI TA`MINLASHNING TASHKILIY-HUQUQIY MASALALARI // SAI. 2022. №Special Issue 2.
4. Isoqova Muxlisa Faxriddin Qizi KIBER JINOYATLAR // ReFocus. 2023. №3.
5. https://hi-in.facebook.com/hackituz/posts/kiber-jinoyatchilik-va-uning-turlarikiber-jinoyat-turli-shakllarda-bolishi-mumki/107669145001486/
6. https://lex. uz/uz/docs/-5960604
7. https://iiv.uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik