UZMETKOMBINAT

“O‘zmetkombinat” AJ

KOMPLAYENS – XIZMATI

KORPORATIV FIRIBGARLIKGA QARSHI KURASHIHGA OID MA’LUMOTLAR O‘QUV QO‘LLANMASI

Bekobod - 2025yil

Korporativ firibgarlik tushunchasi

Korporativ firibgarlik bir vaqtning o‘zida yashirin, latent va Jamiyat uchun o‘ta xavfli hodisadir. U kompaniyalar va fuqarolarga zarar yetkazadi, jiddiy moliyaviy zararga olib keladi, mamlakatning investitsiyaviy jozibadorligiga jiddiy putur yetkazadi. Bundan tashqari, aktivlarning sezilarli qismi qonuniy aylanishdan chiqariladi, buning natijasida davlat byudjeti va muayyan kompaniya benefitsiarlari daromadlarning bir qismidan mahrum bo‘ladi.

Biznes egalarini korporativ firibgarlikdan himoya qilish zarurati biznes muhitini barqarorlashtirish bilan bog‘liq. Bozorni qayta taqsimlash, reyderlik bosqinlari, korporativ urushlar davri o‘tmishda qoldi, huquqiy maydon barqarorlashdi va o‘z maqomiga ishongan mulkdorlar o‘zlarini yollanma menejerlar va xodimlar tomonidan aktivlarni o‘g‘irlashdan himoya qilishni xohlashdi. Bunday talon-torojlarning umumiy atamasi - korporativ firibgarlik - aktivlar va mol-mulkni talon-toroj qilish va o‘zlashtirishning keng ko‘lamli shakllari va usullari majmuini nazarda tutadi.

Rossiya qonun chiqaruvchisi atamaga mustaqil ta’rif bermagan, uning doktrinal talqinidan kelib chiqish yoki unga xos bo‘lgan bir nechta belgilar bilan tavsiflash kerak. Bu javobgarlikka tortish qiyin bo‘lgan muammolardan biridir. Ikkinchi murakkablik shundaki, huquqni muhofaza qilish organlari amaliyotida uzoq vaqtdan beri mavjud bo‘lgan, Sobiq Ittifoq davridan beri o‘zgarishsiz qolgan qo‘shib yozish, o‘g‘irlash, smetani oshirishga qarshi kurashish usullari moliyaviy hisobotlarni buzib ko‘rsatish, biznesni maydalash, pullarni chet elga olib chiqish va shunga o‘xshash firibgarlikning texnologik va zamonaviy usullari bilan bog‘liq vaziyatlarda samarasiz bo‘lib qolmoqda.

Sovet maktabi davlat moliyasi sohasidagi sezilarli miqdordagi jinoyatlarni rejalashtirish va nazorat qilish orqali aniqlash imkonini beradi, ammo moliyaviy hisobot bilan bog‘liq korporativ firibgarliklarni aniqlash uchun ba’zan xorijiy tajribaga murojaat qilish talab etiladi. Xorijiy amaliyotda uch turdagi qoidabuzarliklar korporativ firibgarlik deb e’tirof etiladi:

moliyaviy hisobotning buzib ko‘rsatilganligi;

korporativ darajadagi korrupsiya;

aktivlarni o‘g‘irlash va olib chiqib ketish. Bu yerda “firibgarlik”, “o‘zlashtirish yoki talon taroj qilish”, “qasddan bankrotlik”, “vakolatni suiiste’mol qilish” kabi tarkiblar ayblanishi mumkin.

Rossiya amaliyotida ushbu qilmishlarning har biri o‘ziga xos jinoiy-huquqiy kvalifikatsiyaga ega bo‘ladi, ayrim turlari esa, masalan, hisobot bilan bog‘liq firibgarliklar faqat moliya tashkilotlari, banklar sohasida jinoiy javobgarlikka tortiladi.

Korporativ firibgarlikning odatiy xususiyatlari

Tergov korporativ firibgarlik alomatlariga ega bo‘lgan jinoyatlarni aniqlash bo‘yicha ma’lum tajribaga ega bo‘lib, ularning quyidagi tipik belgilarini ajratib ko‘rsatadi:

muayyan korporativ subyektning aktivlari talon-toroj qilish obyektiga aylanadi. Shunday qilib, jabrlanuvchilar umuman fuqarolar emas, balki tadbirkorlik muomalasiga jalb qilingan alohida shaxslardir. Bular - kompaniyalarning aksiyadorlari va mulkdorlari, tijorat banklari va moliya tashkilotlari bilan bog‘liq vaziyatlarda - ularning mijozlari va omonatchilari;

jinoyat sodir etayotgan shaxslar boshqa tomondan korporativ subyektga aloqador bo‘lib, ular uning insayderlari hisoblanadi;

firibgarlik harakatlarini sodir etish jarayoni deyarli har doim moliyaviy hisobotga, uyushgan qimmatli qog‘ozlar bozorida aksiyalarni joylashtirish maqsadida tuziladigan hisobotga puxta o‘ylangan buzib ko‘rsatishlar kiritish bilan birga kechadi;

jinoyat sodir etish usullarini operatsiyalarning turlari va jinoyatchining javobgarlik darajasiga qarab tasniflash mumkin.

Ushbu belgilarning yig‘indisi korporativ firibgarlikni sodir etishning deyarli har bir holati uchun xosdir. Uni deyarli hech qachon intellektual tarkibiy qismga ega bo‘lmagan o‘g‘irliklardan farqlash kerak.

ACFE tomonidan taklif etilgan tasnifga asoslanib, har qanday murakkab va uyushgan korporativ firibgarlik osonlik bilan yig‘iladigan majburiy elementlar to‘plami bo‘lgan “firibgarlik konstruktori” ni ko‘rish mumkin. Bular:

aktivlarni talon-toroj qilish va o‘zlashtirishning barcha turlari, masalan, ko‘chmas mulkni qayta baholash va olib qo‘yish, soxta qarzdorlikni yuzaga keltirish, kompaniyaga soxta hisobvaraqlar qo‘yish, rastratalar va boshqalar;

mustaqil korrupsiyaviy harakatlar (pora-berish, pora-minnatdorchilik bildirish, umumiy homiylik uchun haq to‘lash - biznesning top-menejeri o‘z xizmat mavqeidan kompaniya manfaatlariga zid ravishda shaxsiy foyda olish maqsadida moliyaviy-xo‘jalik operatsiyalariga ta’sir o‘tkazish uchun foydalanadigan barcha holatlar);

moliyaviy hisobot bilan bog‘liq firibgarlik - moliyaviy hisobotni yaxshilash maqsadida uni buzib ko‘rsatishga imkon beradigan turli xil mexanizmlar, masalan, investor, kreditor, biznes xaridorini aldash uchun kattaroq daromad yoki aktivlarning katta qiymatini ko‘rsatish, shuningdek, ayrim ko‘rsatkichlarni yomonlashtirish va zararni shakllantirish (soliq jinoyatlari).

Korporativ firibgarlik subyektlari

Korporativ firibgarlikning har bir ta’rifi uning subyekti sifatida kompaniya rahbari, mansabdor shaxsi yoki xodimini tan oladi. Ayrim korporativ normativ hujjatlarda, masalan, “Gazprom neft” OAJning “Korrupsiya va firibgarlikka qarshi kurashish siyosati”da yuridik shaxslar ham mustaqil subyektlar bo‘lishi mumkin.

Quyidagi tasnifni tuzish mumkin:

korporativ subyektlar - firibgarlikka ixtisoslashgan yoki firibgarlikni sodir etish quroli sifatida maxsus tashkil etilgan yuridik shaxslar;

aktivlarni boshqa mulkdorlarga zarar yetkazgan holda undan chiqarayotgan biznes aksiyadorlari va mulkdorlari;

mulkni talon-toroj qilish sxemalarini yaratuvchi va aksiyadorlarga zarar yetkazuvchi rahbarlar va top-menejerlar;

yollanma xodimlar.

Ko‘pincha turli subyektlar barqaror uyushgan guruhlarni tashkil etadilar va ularning faoliyatini aniqlash va to‘xtatish juda qiyin, chunki hujjatlarni soxtalashtirish va dalillarni yashirish bo‘yicha ularning tajribasi ishni tekshirish topshirilgan auditorlar yoki tergovchilarga qaraganda ancha ko‘p bo‘lishi mumkin.

Korporativ firibgarlik zarari

Yo‘qotilgan aktivlar yoki pul mablag‘lari korporativ firibgarlikdan ko‘rilgan zararning yagona turi bo‘lishi mumkin, deb hisoblamaslik kerak. Nomoddiy yo‘qotishlar ham mavjud bo‘lib, ularga obro‘-e’tiborni yo‘qotish, malakali kadrlarni ishga qabul qilishdagi qiyinchiliklar va boshqalar kiradi. Quyidagi asosiy zarar turlarini ajratib ko‘rsatish mumkin:

aktivlarni to‘g‘ridan to‘g‘ri olib chiqish, ularni hisobdan chiqarish, xorijga olib chiqish;

agar kompaniyalar aksiyalarining qiymati sun’iy ravishda oshirilganligi ma’lum bo‘lib qolsa, ular qiymatining pasaytirilishi;

foydali shartnomalarning yo‘qotilishi;

noqulay shartlarda kontraktlar tuzishda mablag‘larning yo‘qotilishi;

mijozlarni yo‘qotish;

bozor ulushini yo‘qotish.

Bu oqibatlarning barchasi boy berilgan foyda bilan birga keladi. Amaliyot shuni ko‘rsatadiki, korporativ firibgarlardan yetkazilgan zararni qoplash tartibida mablag‘larni undirish dargumon, chunki ularni sudga jalb qilish juda kam hollarda, ayniqsa, sxemaning tashkilotchisi biznes egasi yoki top-menejerning o‘zi bo‘lgan hollarda mumkin.

Audit va korporativ firibgarlik

Yevropa va AQShda xatolar va moliyaviy firibgarliklarni aniqlashga ixtisoslashgan auditorlik kompaniyalari auditorlik faoliyatining maxsus yo‘nalishi - fraud auditingni yaratdilar. Ushbu faoliyat yo‘nalishi firibgarlikning odatiy holatlarini aniqlash, shuningdek, mablag‘larni o‘g‘irlash mexanikasi doimiy ravishda takomillashib borayotgani sababli yangi ishlanmalarni topishga qaratilgan standartlar va amaliyotlarni ishlab chiqdi. 1990-2000-yillarda xorijiy bozorlarni larzaga keltirgan bir qator yirik firibgarliklar korporativ qonunchilikni jiddiy qayta qurishni talab qildi. Firibgarliklarning tashabbuskor auditi korporativ firibgarlikka qarshi kurashish tizimining poydevoriga aylandi. U korporativ nazorat va hisobotlarning ishonchliligini aniqlaydigan oddiy auditni istisno qilmaydi, balki o‘z bozor sektorida faol rivojlanayotgan mustaqil xizmatdir.

Ammo bu sohada ham korporativ firibgarliklarni aniqlash va oldini olishning umume’tirof etilgan metodologiyasini ishlab chiqishga muvaffaq bo‘lindi, deb bo‘lmaydi. U yoki bu darajada samarali bo‘lgan chora-tadbirlar majmuasidan foydalanilmoqda, ularning ba’zilari allaqachon Rossiya hududida sinovdan o‘tgan. Turli auditorlik kompaniyalari, alohida tadqiqotchilar, detektiv agentliklar va boshqa professionallar faoliyatini muvofiqlashtirish uchun Korporativ firibgarliklarni aniqlash, tergov qilish va oldini olish bo‘yicha sertifikatlangan mutaxassislar xalqaro assotsiatsiyasi (***ACFE - Association of Certified Fraud Examiners***) mas’uldir. Ushbu tashkilot dunyoning aksariyat mamlakatlarida o‘z oldiga “oq yoqalilar” deb ataladigan jinoyatchilikning rolini kamaytirishni maqsad qilib qo‘ygan 40 mingdan ortiq ishtirokchini birlashtiradi. Rossiyada assotsiatsiya bo‘limi 2007-yildan beri faoliyat yuritib kelmoqda.

Korporativ firibgarlikka qarshi kurashish sohasida Rossiyaning o‘z uslubiy ishlanmalari deyarli mavjud emas, shuning uchun huquqni muhofaza qilish organlarida qabul qilingan an’anaviy tergov usullariga yoki auditorlik standartlariga tayanishga to‘g‘ri keladi.

Korporativ firibgarlikka qarshi kurashish usullari

Amaliyot korporativ firibgarlikka qarshi kurashish usullarining bir nechta guruhlarini ishlab chiqdi. Ular uch guruhga bo‘linadi:

ogohlantirish usullari;

aniqlash usullari;

tergov usullari.

Uchta guruhning har birida tashkiliy va texnik usullarni ajratib ko‘rsatish, shuningdek, tergovning tezkor usulini alohida ko‘rib chiqish mumkin.

Tashkiliy

Korporatsiyalarda firibgarliklarni aniqlash va oldini olishda rivojlangan huquqiy va uslubiy bazaga asoslangan tashkiliy usullar eng katta rol o‘ynaydi. Ogohlantirishning tashkiliy choralari sifatida quyidagilar ajratib ko‘rsatiladi:

taqiqlangan xatti-harakatlarning barcha turlarini va ular uchun javobgarlik choralarini tavsiflovchi normativ-huquqiy hujjatlarni qabul qilish, xodimlarni ushbu hujjatlar bilan tanishtirish;

firibgarlik sodir etish imkoniyatini to‘liq istisno etadigan kompaniyada korporativ madaniyatni yaratish;

barcha aybdor shaxslarni ham intizomiy, ham jinoiy javobgarlikka tortishning keng amaliyoti;

xodimlarning shartnomalariga ularni ishdan bo‘shatishni soddalashtirish imkonini beruvchi normalarni kiritish;

kompaniyada nazorat uchun mas’ul bo‘lgan bo‘linmalar: iqtisodiy xavfsizlik va ichki audit xizmatlarini tashkil etish.

Bundan tashqari, aniqlash choralari sifatida muntazam ravishda kompaniya faoliyatini alohida va to‘liq tekshirish, taftish, inventarizatsiya o‘tkazish zarur. Mustaqil auditorlik kompaniyasini jalb qilish huquqni muhofaza qilish organlari jinoiy ish qo‘zg‘atishi mumkin bo‘lgan dalillar bazasini olish imkonini beradi.

Texnik

Texnik usullarni dasturiy va boshqa usullarga bo‘lish mumkin. Dasturiy vositalarga quyidagilarga imkon beruvchi barcha dasturiy mahsulotlar kiradi:

moliyaviy tusdagi axborotni unga buzib ko‘rsatishlar kiritilishidan himoya qilish;

kompaniyadan axborot chiqib ketishining oldini olish;

hisobotlarda va ma’lumotlar bazalarida firibgarlik sodir etilganligi faktini ko‘rsatuvchi xatolarni, nomuvofiqliklarni aniqlash.

Axborot perimetrini himoyalashni DLP-tizimlar va SIEM-tizimlar xususiyatlariga ega bo‘lgan dasturiy mahsulotlarni o‘rnatish orqali amalga oshirish mumkin. Bundan tashqari, xodimlarning foydalanish darajasini nazorat qilish, ruxsatsiz aralashuvning har bir holatini aniqlashga va xavfsizlik xizmatlarini o‘z vaqtida xabardor qilishga yordam beradigan moliyaviy ma’lumotlar va parollarni himoya qilishning bunday darajalaridan foydalanish zarur.

Hisobot va hujjatlarni tahlil qilishda ba’zi jihatlar Project Expert dasturini aniqlashga yordam beradi, auditorlar turli yillardagi ko‘rsatkichlarni taqqoslash va jinoyat sodir etilganligi hamda aktivlar olib chiqib ketilganligidan dalolat berishi mumkin bo‘lgan eng yuqori buzilishlarni aniqlash imkonini beruvchi o‘z uslubiyotlariga ega.

Tezkor va tergov

Korporativ firibgarliklarning oldini olish usullari orasida tezkor usullar unchalik katta rol o‘ynamaydi. Bu juda kamdan-kam hollarda kompaniyalar firibgarlik alomatlari mavjud bo‘lgan qilmishni aniqlash bosqichida huquqni muhofaza qilish organlaridan mutaxassislarni taklif qilish to‘g‘risida qaror qabul qilishlari bilan bog‘liq. Kompaniyalarning xavfsizlik xizmatlari uchun tezkor usullardan mustaqil foydalanish esa qonunchilikni buzish uchun bahona bo‘lishi mumkin.

Shunga qaramay, quyidagi choralarga yo‘l qo‘yiladi:

xonalarni videonazorat va ovoz yozish tizimlari bilan jihozlash;

nazorat xaridlarini o‘tkazish;

shaxsiy hayotga tajovuz qilish bilan bog‘liq bo‘lmagan firibgarlikda gumon qilingan xodimning turmush tarzini o‘rganish.

Bu usullarning barchasi gumonni ishonchga aylantirishga yordam beradi, ammo aksariyat hollarda, surishtiruv organlarining harakatlaridan farqli o‘laroq, ularning natijalari jinoyat ishi bo‘yicha sud uchun maqbul dalil bo‘la olmaydi. Dastlabki bosqichda surishtiruv va tergov organlarini jalb qilish zarur dalillarni to‘plash uchun ularning ishlab chiqilgan tahliliy apparati, dasturiy mahsulotlari, SMS xabarlari va ijtimoiy tarmoqlardagi muzokaralarni nazorat qilish

usullaridan foydalanish imkonini beradi. Mutaxassislar tezkor harakatlarni amalga oshirish jarayonida quyidagilarni aniqlashlari mumkin:

jinoyatning bevosita aybdorlari va ularning yordamchilari;

jinoyat sodir etish motivlari, har doim ham ular bilan faqat boylik orttirish bo‘lmaydi, ba’zan tashqi bosim, tahdid, qo‘rqitish muhim omillarga aylanadi;

jinoyatni sodir etish mexanizmi, zararning xususiyati va miqdori.

Muhimi, huquq-tartibot idoralari kompaniyani firibgarlardan himoya qilish uchun mas’ul bo‘lgan ichki subyektlar bilan yaqin hamkorlikda ishlashi mumkin. Ularga quyidagilar kirishi mumkin:

xavfsizlik xizmati xodimlari;

taftishchilar, auditorlar;

Direktorlar kengashi a’zolarining korporativ nazoratni amalga oshiruvchi vakillari.

Bir kunlik firmalar sxemalarida tez-tez foydalanish Rossiya biznesining o‘ziga xos xususiyatiga aylanmoqda. Ularni aniqlash soliq organlari bilan yaqin aloqada ishlash orqali amalga oshirilishi mumkin. Ko‘pincha bitta xususiy sxemaning aniqlanishi keng tarqalgan tarmoqning ochilishiga olib keladi, uning doirasida naqdlashtirish, pul yuvish, davlat xizmatchilarini sotib olish sodir bo‘ladi. Kompleks ishlar Rossiya bozorini 90-yillarning ko‘plab qoldiqlaridan tozalashga yordam beradi.

Korporativ firibgarlik jiddiy ijtimoiy muammo. Uni aniqlash va oldini olish usullari jamiyat va fuqarolar manfaatlariga zarar yetkazishni istisno etishi kerak, bu esa mamlakatning jahon maydonida investitsion jozibadorligini oshirishga, soliq intizomini kuchaytirishga, byudjetni sezilarli darajada to‘ldirishga va jinoyatchilikni moliyalashtirishga to‘sqinlik qilishga olib keladi.

Milliy tajriba

Firibgarlik tovar ayirboshlash munosabatlarida paydo bo‘lgan, bunda jinoyatchi o‘zi uchun maksimal foyda olishga umid qilishi mumkin edi. Davlatimizning o‘sishi va rivojlanishi bilan birga firibgarlik yo‘nalishidagi jinoyatlar soni ham ortib bordi. Albatta, hukumat yangi hodisalarga munosabat bildirishga va bunday qilmishlarga qarshi kurashga qaratilgan choralarni ko‘rishga harakat qildi. Firibgarlik yo‘nalishidagi jinoyatlar uchun javobgarlikni nazarda tutuvchi normalar sonining ko‘payishi ularning tarqalganlik va ijtimoiy xavflilik darajasidan dalolat berishi mumkin. Bugungi kunda ushbu qilmishga qarshi kurashishning dolzarbligi aslo kamaygani yo‘q, aksincha, yanada oshdi. Davlat iqtisodiyoti, mulkchilik institutining jadal sur’atlar bilan rivojlanishi, shartnomaviy munosabatlar sonining ko‘payishi firibgarlarni befarq qoldirmadi, albatta. Shu munosabat bilan, fuqarolarning pul mablag‘larini aldash va o‘zlashtirish imkonini beruvchi firibgarlikning yangi turlari paydo bo‘lishiga olib keldi.

Bugungi kunda ko‘plab turli xil yuqori texnologiyali qurilmalar - plastik kartalar, mobil telefonlar va kompyuterlar ishlatilmoqda. Doimiy ravishda yangi modellar, dasturlar va xizmatlar paydo bo‘lmoqda.

MUHOKAMA VA NATIJALAR

Shu munosabat bilan O‘zbekiston Respublikasi Prezidentining 2018-yil 21-noyabrdagi “Axborot texnologiyalari va kommunikatsiyalarini joriy etishni nazorat qilish, tashkil etish va himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi 4024-sonli qarori qabul qilindi. Zero, O‘zbekistonda davlat va jamiyat boshqaruvi sohasida zamonaviy axborot-kommunikatsiya tizimlarining joriy etilishi firibgarlik harakatlariga olib keldi va bu bilan deyarli har ikkinchi fuqaro to‘qnash kelmoqda. Bu yovuz niyatli kimsalarning qurboni faqat keksalar

bo‘ladi, deb o‘ylash soddalikdir, aslida unday emas. Jinoiy unsurlar qarmog‘iga mutlaqo har kim ilinishi mumkin.

Shu munosabat bilan, firibgarlikning yangi turlari paydo bo‘lmoqda. O‘zbekiston Jinoyat kodeksining 168-moddasiga ko‘ra, firibgarlik aldash yoki ishonchni suiiste’mol qilish yo‘li bilan o‘zganing mulkini yoki o‘zganing mulkiga bo‘lgan huquqni qo‘lga kiritishdir. Firibgarlikning boshqa mulkiy jinoyatlardan farqi shundaki, firibgarlikda jabrlanuvchilar firibgarga o‘z mol-mulkini va mol-mulkka bo‘lgan huquqini o‘z xohishiga ko‘ra beradi.

Jinoyat kodeksining 168-moddasida firibgarlik 5-qismga bo‘lingan. 4-qismda qaysi hollarda og‘irlashtiruvchi kvalifikatsiya qo‘llanilishi ko‘rsatilgan. Beshinchi qismda javobgarlikni yengillashtiruvchi holatlar bayon etilgan. Ya’ni, agar jinoyat sodir etilgandan keyin yetkazilgan zarar to‘liq qoplangan bo‘lsa, ayblanuvchi, gumon qilinuvchi yoki sudlanuvchiga nisbatan ozodlikdan mahrum qilish jazosi qo‘llanilmasligi mumkin.

Hozirgi vaqtda “firibgarlik” tushunchasining zamonaviy ta’rifiga turli sohalarda, shu jumladan bank faoliyati, uyali aloqa va zamonaviy axborot texnologiyalari sohasida ko‘plab noqonuniy xatti-harakatlar kiradi. Texnologiyadagi farqlarga qaramay, bu harakatlarning barchasi bir qator umumiy xususiyatlarni birlashtiradi:

- Aldamchi harakatlar; - Ishonchni suiiste’mol qilish;
- Faktlarni qasddan buzib ko‘rsatish yoki sukut saqlash;
- o‘zgalar mulkini talon-toroj qilish;
- o‘zganing mulkiga bo‘lgan huquqlarni qonunga xilof ravishda qo‘lga kiritish;

Aksariyat hollarda firibgarlik jabrlanuvchisi o‘z mulki yoki unga bo‘lgan huquqlarini jinoyatchilarga mustaqil ravishda va ixtiyoriy ravishda topshiradi. Masalan, banklardagi firibgarlik harakatlarini shartli ravishda bir necha guruhga bo‘lish mumkin:

Kreditlashdagi firibgarlik - qarzni to‘lash uchun mo‘ljallangan summalarni boshqa hisobvaraqlarga o‘tkazish, mavjud bo‘lmagan qarz oluvchilarga kreditlarni rasmiylashtirish, mijozlarga bildirmasdan kreditlarni rasmiylashtirish;

Hisob-kitob-kassa xizmati ko‘rsatishdagi firibgarlik - hisobvaraqdan summalarni ruxsatsiz yechib olish, kupyuralarni qalbakilari bilan almashtirish, qayta sanalgan pachkadan banknotlarni chiqarib olish;

Depozitlar bilan bog‘liq firibgarlik - kiritilgan mablag‘larni olib qo‘yish, hujjatlardagi summalarni kamaytirib ko‘rsatish, mijozga bildirmasdan mablag‘larni hisobdan chiqarish.

Aksariyat bank firibgarliklari yirik bosh ofislarda emas, balki kamroq nazorat qilinadigan bank filiallari va bo‘limlarida amalga oshiriladi. Bunday sharoitda xodimlar soni kamroq bo‘ladi, ammo ular ko‘proq biznes jarayonlariga jalb qilinadi, bu esa noqonuniy faoliyat uchun kengroq imkoniyatlar ochadi

Elektron to‘lovlar va onlayn xaridlar bozorining faol o‘sishi munosabati bilan axborot texnologiyalaridan foydalangan holda firibgarlikning yangi zamonaviy shakllari ham rivojlanmoqda. Internetdagi eng keng tarqalgan firibgarlik turlari quyidagi firibgarliklardir:

Fishing - bank kartasidan mablag‘larni o‘g‘irlash maqsadida shaxsga doir ma’lumotlarni (parol, login) o‘g‘irlash. Asosan fishing uchun soxta saytlarga havolalarni o‘z ichiga olgan pochta xabarnomasidan foydalaniladi;

Elektron pochta orqali firibgarlik - "Nigeriya xatlari" deb ataladi. Ularda afsonaviy qarindoshdan meros qolganligi haqidagi chiroyli afsona va advokat xizmatlari uchun to‘lov yoki komissiya to‘lovini olish uchun hisob raqamiga pul o‘tkazish iltimosi mavjud;

Internet-hamyon bilan bog‘liq firibgarliklar - ko‘pincha bunday hollarda xaridor sotuvchiga oldindan to‘lovni internet-hamyonga o‘tkazadi, ammo natijada na tovar, na pul oladi.

Uyali aloqa orqali firibgarlikni shartli ravishda ikki guruhga bo‘lish mumkin. Birinchisiga bevosita raqam egasining hisobvarag‘idan uning xabardorligisiz pul yechib olishni kiritish lozim.

Bunday firibgarliklar bilan uyali aloqa operatorlarining o‘zlari ham, ularning kompaniyalariga aloqasi bo‘lmagan firibgarlar ham shug‘ullanishi mumkin. Firibgarliklarning ikkinchi guruhiga abonentning o‘zi ko‘rsatilgan hisob raqamiga pul o‘tkazishi yoki ularni to‘g‘ridan-to‘g‘ri qo‘liga berishi yoxud firibgarlar ko‘rsatgan joyda qoldirib ketishi holatlarini kiritish mumkin. Bunday firibgarliklarda uyali aloqa faqat sahnalashtirish vositasi sifatida namoyon bo‘ladi. Masalan, yaqin qarindoshining qo‘ng‘irog‘i o‘ynaladi, u qiyin ahvolga tushib qolgan va zudlik bilan pulga muhtoj.

Pul bilan bog‘liq firibgarlik eng katta va keng qamrovli guruhlardan biridir, chunki deyarli har qanday firibgarlik, u yoki bu tarzda, o‘zganing pul mablag‘larini noqonuniy o‘zlashtirishni nazarda tutadi. Biroq, naqd pullar bilan bilvosita yoki bevosita bog‘liq bo‘lgan firibgarlikning bir nechta usullarini ajratib ko‘rsatish mumkin. Bu usullarni do‘konlarda, do‘konchalarda, ayirboshlash shoxobchalarida qo‘llash mumkin. Eng oddiy va keng tarqalgan firibgarlik qadoqdagi haqiqiy pullarni qalbaki pullarga almashtirishdir (asosan, yuqorida va pastda - haqiqiy, o‘rtada - qalbaki yoki oddiy qog‘oz). Shuningdek, “yetishmovchilik” amaliyoti ham qo‘llaniladi - allaqachon sanab bo‘lingan pullar to‘plamidan bir nechta banknotalar chiqariladi. Firibgarlik shaxsiy ma’lumotlarni o‘qiydigan datchik o‘rnatilgan bankomat yordamida naqd pul yechib olishga urinishda ham amalga oshirilishi mumkin.

Bugungi kunda turli xil firibgarliklarning “assortimenti” sezilarli darajada kengaydi, bu asosan kundalik hayotga zamonaviy texnologiyalar - internet, uyali aloqa, onlayn xaridlar va bank xizmatlari kirib kelishi bilan bog‘liq. Biroq, firibgarlikning an’anaviy turlari ham hali ham rivojlanmoqda. Ular orasida qimmatbaho buyumlarni sotib olishni taklif qiluvchi ko‘cha firibgarlari, avtohalokatlar uyushtiruvchi va shu yerning o‘zida kelishib olishni taklif qiluvchi soxta shaxslarni sanab o‘tish mumkin. Firibgarlikning eng yirik va bir vaqtning o‘zida ko‘p sonli odamlarni jalb qiladigan turlaridan biri moliyaviy piramidadir.

XULOSA

Firibgarlikning eng keng tarqalgan barcha turlari yuqorida keltirilgan va ular bitta umumiy maxraj bilan birlashtiriladi - ular firibgarlarning potensial qurbonlari psixologiyasini hisobga olgan holda amalga oshiriladi. Firibgarlar eng mayda tafsilotlargacha o‘ylangan bo‘lib, hatto eng ehtiyotkor va e’tiborli odamlarning ham hushyorligini aldashga qodir. Aynan shuning uchun bank kartasidagi parol, login, bank hisob raqami, kod so‘zi, CVV2 kodi kabi shaxsiy ma’lumotlarni uchinchi shaxslarga berish mumkin emasligini yodda tutish lozim.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining Konstitutsiyasi.

2. O‘zbekiston Respublikasi Oliy sudi Plenumining 11.10.2017-yildagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida” gi 35-sonli qarori.

3. O‘zbekiston Respublikasining Jinoyat kodeksi.

4. O‘zbekiston Respublikasining 2014-yil 14-maydagi O‘RQ-371-son “Huquqbuzarliklar profilaktikasi to‘g‘risida” gi Qonuni.

5. O‘zbekiston Respublikasi Prezidentining 2017-yil 14-martdagi “Huquqbuzarliklar profilaktikasi va jinoyatchilikka qarshi kurashish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida” gi 2833-sonli Qarori.

6. O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalarini joriy etishni nazorat qilish, ularni himoya qilishni tashkil etish tizimini takomillashtirish chora-tadbirlari to‘g‘risida” 2018-yil 21-noyabrdagi PQ-4024-son qarori.

7. O‘zbekiston Respublikasi jinoyat huquqi kursi. Rustambayev M.X. Umumiy qism. 1-jild. 2009. 8. N.A.Yegorova, N.N. B.

Понятие корпоративного мошенничества

Корпоративное мошенничество – одновременно и скрытое, латентное, и крайне опасное для общества явление. Оно причиняет вред компаниям и гражданам, приводит к серьезному финансовому ущербу, серьезно ухудшает инвестиционную привлекательность страны. Помимо этого, существенная часть активов выводится из легального оборота, благодаря чему бюджет государства и бенефициары конкретной компании лишаются части доходов.

Необходимость защиты собственников бизнеса от корпоративного мошенничества обусловлена стабилизацией бизнес-среды. Эпоха передела рынка, рейдерских захватов, корпоративных войн ушла в прошлое, правовое поле стабилизировалось, и уже уверенные в своем статусе собственники хотели бы защитить себя от хищения активов со стороны наемных менеджеров и сотрудников. Общий термин таких хищений – корпоративные мошенничества – подразумевает под собой широкую совокупность форм и методов хищения и присвоения активов и имущества.

Российский законодатель не дал самостоятельного определения термина, необходимо исходить из его доктринального толкования или описывать несколькими присущими ему признаками. Эта одна из проблем, из-за которой возникает сложность привлечения к ответственности. Вторая сложность связана с тем, что издавна существующие в практике правоохранительных органов методы борьбы с понятными им приписками, хищениями, завышениями смет, оставшимися неизменными со времен СССР, оказываются неэффективными в ситуациях с искажением финансовой отчетности, дроблением бизнеса, выводом денег за рубеж и аналогичными технологичными и современными способами мошенничества. Советская школа позволяет выявлять существенное количество преступлений в области государственных финансов с их планированием и контролем, а вот для определения корпоративных мошенничеств с финансовой отчетностью иногда требуется обратиться к зарубежному опыту. В иностранной практике корпоративным мошенничеством признаются три вида нарушений:

искажение финансовой отчетности;

коррупция на корпоративном уровне;

хищение и вывод активов. Здесь могут инкриминироваться такие составы, как «мошенничество», «присвоение или растрата», «преднамеренное банкротство», «злоупотребление полномочиями».

В российской практике каждое из этих деяний будет иметь собственную уголовно-правовую квалификацию, а некоторые виды, например махинации с отчетностью, преследуются в уголовном порядке только в сфере финансовых организаций, банков.

Типичные характеристики корпоративного мошенничества

Следствие, имея уже определенный опыт выявления преступлений, имеющих признаки корпоративного мошенничества, выделяет следующие их типичные признаки:

объектом хищения становятся активы определенного корпоративного субъекта. Таким образом, потерпевшими являются не граждане вообще, а отдельные лица, вовлеченные в предпринимательский оборот. Это акционеры и собственники компаний, в ситуациях с коммерческими банками и финансовыми организациями – их клиенты и вкладчики;

лица, которые совершают преступление, имеют отношение к корпоративному субъекту с другой стороны, они его инсайдеры;

процесс совершения мошеннических действий практически всегда сопровождается внесением продуманных искажений в финансовую отчетность, в отчетность, составляемую для целей размещения акций на организованном рынке ценных бумаг;

способы совершения преступлений можно классифицировать по типам операций и уровню ответственности преступника.

Совокупность этих признаков характерна практически для каждого случая совершения корпоративного мошенничества. Его следует отличать от краж, которые практически никогда не несут в себе интеллектуальной составляющей.

Если исходить из классификации, предложенной ACFE, можно увидеть «конструктор мошенничества», совокупность обязательных элементов, из которых легко собирается любое сложное и организованное корпоративное мошенничество. Это:

все виды хищения и присвоения активов, примерами которых могут быть переоценка и вывод недвижимого имущества, создание фиктивной задолженности, выставление фиктивных счетов на компанию, растраты и т. д.;

самостоятельные коррупционные действия (взятки-откаты, взятки-благодарности, оплата за общее покровительство – все ситуации, в которых топ-менеджер бизнеса использует свое служебное положение вопреки интересам компании для влияния на финансово-хозяйственные операции с целью получения личной выгоды;

мошенничество с финансовой отчетностью – различные механизмы, позволяющие искажать финансовую отчетность в целях как ее улучшения, например, для указания большей выручки или большей стоимости активов, чтобы совершить обман инвестора, кредитора, покупателя бизнеса, так и ухудшения отдельных показателей и формирования убытка (налоговые преступления).

Субъекты корпоративного мошенничества

Каждое из определений корпоративного мошенничества в качестве его субъекта признает руководителя, должностное лицо или сотрудника компании. В некоторых корпоративных нормативных актах, например в «Политике противодействия коррупции и мошенничеству» ПАО «Газпром нефть», самостоятельными субъектами могут стать и юридические лица.

Можно составить следующую классификацию:

корпоративные субъекты – юридические лица или специализирующиеся на мошенничестве, или специально созданные в качестве орудий его совершения;

акционеры и собственники бизнеса, выводящие из него активы в ущерб другим собственникам;

руководители и топ-менеджеры, создающие схемы хищения имущества и причиняющие ущерб акционерам;

наемные сотрудники.

Часто различные субъекты создают устойчивые организованные группы, и их деятельность крайне сложно выявить и пресечь, так как опыта в подделке документов и сокрытии доказательств у них может быть намного больше, чем у аудиторов или следователей, которым поручено расследование дела.

Ущерб от корпоративного мошенничества

Не надо считать, что единственным видом ущерба от корпоративного мошенничества могут стать утраченные активы или денежные средства. Существуют и нематериальные потери, к которым относятся утраченная репутация, сложность с приемом на работу квалифицированных кадров и многое другое. Можно выделить следующие основные типы ущерба:

прямой вывод активов, их списание, вывод за рубеж;

снижение стоимости акций компаний в случае, если станет известно о том, что их стоимость была искусственно завышена;

потеря выгодных контрактов;

потеря средств при заключении контрактов на невыгодных условиях;

потеря клиентов;

потеря доли рынка.

Все эти последствия сопровождаются еще и упущенной выгодой. Как показывает практика, взыскание средств в порядке возмещения причиненного ущерба с корпоративных мошенников маловероятно, так как привлечь их к суду возможно в крайне редких случаях, особенно когда организатором схемы выступает сам собственник или топ-менеджер бизнеса.

Аудит и корпоративное мошенничество

В Европе и США аудиторские компании, специализирующиеся на выявлении ошибок и финансового мошенничества, создали особое направление аудиторской деятельности, так называемый fraud auditing. Это направление деятельности выработало стандарты и практики, призванные выявить типичные случаи мошенничества, а также найти и новые разработки, так как механика хищения средств постоянно совершенствуется. Ряд крупных мошенничеств, которые сотрясали зарубежные рынки в 1990–2000-х годах, потребовал серьезной перестройки корпоративного законодательства. Инициативный аудит махинаций стал краеугольным камнем, на котором держится система противодействия корпоративному мошенничеству. Он не исключает корпоративный контроль и обычный аудит, выявляющий достоверность отчетности, а является самостоятельной услугой, активно развивающейся в своем секторе рынка.

Но нельзя сказать, что даже этой отрасли удалось разработать общепризнанную методику выявления и предотвращения корпоративных мошенничеств. Используется комплекс мер, более или менее эффективных, некоторые из них уже прошли апробацию на российской почве. За координацию деятельности различных аудиторских компаний, отдельных исследователей, детективных агентств и других профессионалов отвечает Международная ассоциация сертифицированных специалистов по выявлению, расследованию и предупреждению корпоративных мошенничеств (ACFE – Association of Certified Fraud Examiners). Эта организация объединяет более 40 тысяч участников в большинстве стран мира, поставивших перед собой цель снизить роль так называемой «преступности белых воротничков». В России отделение ассоциации работает с 2007 года.

Собственных российских методических разработок в области противодействия корпоративному мошенничеству практически не существует, поэтому приходится ориентироваться или на традиционные методы расследования, принятые у правоохранительных органов, или на аудиторские стандарты.

Методы противодействия корпоративному мошенничеству

Практика выработала несколько групп методов противодействия корпоративному мошенничеству. Они делятся на три группы:

методы предупреждения;

методы выявления;

методы расследования.

В каждой из трех групп можно выделить организационные и технические методы, а также в качестве отдельного рассмотреть оперативный метод расследования.

Организационные

Наибольшую роль в выявлении и предотвращении мошенничеств в корпорациях играют организационные способы, основанные на развитой правовой и методической базе. В качестве организационных мер предупреждения выделяются:

принятие нормативно-правовой документации, описывающей все типы запрещенных деяний и меры ответственности за них, ознакомление персонала с этими документами;

создание в компании корпоративной культуры, полностью исключающей возможность совершения мошенничества;

широкая практика привлечения к ответственности, как дисциплинарной, так и уголовной, всех виновных лиц;

внесение в контракты сотрудников норм, позволяющих упростить их увольнение;

создание в компании подразделений, отвечающих за контроль: службы экономической безопасности и внутреннего аудита.

Помимо этого, необходимо в качестве мер выявления регулярно проводить отдельные и полные проверки деятельности компании, ревизии, инвентаризации. Привлечение независимой аудиторской компании позволит получить доказательственную базу, на основе которой правоохранительные органы смогут возбудить уголовное дело.

Технические

Технические способы можно разделить на программные и иные. К программным средствам относятся все программные продукты, позволяющие:

защищать информацию финансового характера от внесения в нее искажений;

предотвращать утечку информации из компании;

выявлять ошибки, несостыковки в отчетности и базах данных, указывающие на факт совершения мошенничества.

Защиту информационного периметра можно произвести путем установки программных продуктов, имеющих характеристики DLP-систем и SIEM-систем. Кроме того, необходимо контролировать уровни доступа сотрудников, использовать такие степени защиты финансовой информации и пароли, которые помогут выявить каждый факт несанкционированного вмешательства и своевременно информировать о нем службы безопасности.

При анализе отчетности и документации некоторые моменты поможет выявить программа Project Expert, аудиторы имеют собственные методики, позволяющие сравнивать показатели разных лет и находить пиковые искажения, которые могут свидетельствовать о совершении преступления и выводе активов.

Оперативные и следственные

Среди методов предотвращения корпоративных мошенничеств оперативные играют незаслуженно небольшую роль. Связано это с тем, что в крайне редких случаях компании принимают решение на стадии выявления деяния, имеющего признаки мошенничества, приглашать специалистов из правоохранительных органов. Самостоятельное же использование оперативных способов для служб безопасности компаний может стать поводом для нарушения законодательства. Тем не менее допустимы такие меры, как:

оборудование помещений системами видеоконтроля и звукозаписи;

проведение контрольных закупок;

не связанное с вторжением в частную жизнь изучение образа жизни сотрудника, заподозренного в мошенничестве.

Все эти способы помогают превратить подозрение в уверенность, но в большинстве случаев, в отличие от действий органов дознания, их результаты не смогут стать допустимыми доказательствами для суда в уголовном деле. Привлечение на самом раннем этапе органов дознания и следствия позволит использовать их наработанный аналитический аппарат, программные продукты, способы контроля сообщений СМС и переговоров в социальных сетях для того, чтобы собрать необходимые доказательства. Профессионалы в процессе проведения оперативных действий смогут выявить:

непосредственных виновников преступления и их пособников;

мотивы совершения преступления, не всегда ими бывает только обогащение, иногда существенными факторами становятся внешнее давление, угроза, запугивание;

механизм совершения преступления, характер и размер ущерба.

Важно, что правоохранительные органы могут работать в тесной связке с внутренними субъектами, отвечающими за защиту компании от мошенников. К ним могут относиться:

сотрудники служб безопасности;

ревизоры, аудиторы;

представители членов Совета директоров, осуществляющие корпоративный контроль.

Спецификой российского бизнеса становится частое использование в схемах фирм-однодневок. Их выявление возможно при работе в тесном контакте с налоговыми органами. Часто выявление одной частной схемы приводит к вскрытию развернутой сети, в рамках которой происходит обналичивание, отмывание денег, подкуп государственных служащих. Комплексная работа поможет очистить российский рынок от многих рудиментов 90-х годов.

Корпоративное мошенничество – серьезная общественная проблема. Методы его выявления и предотвращения должны исключить нанесение ущерба интересам общества и граждан, а это приведет к повышению инвестиционной привлекательности страны на мировой арене, большей налоговой дисциплине, существенному пополнению бюджета и препятствованию финансирования криминалитета.

Национальный опыт

Мошенничество зародилось в отношениях товарообмена, где злоумышленник мог рассчитывать на максимальное извлечение выгоды для себя. Вместе с ростом и развитием нашего государства росло и количество преступлений мошеннической направленности. Конечно же, правительство старалось реагировать на новые явления и предпринимать меры, направленные на борьбу с подобными деяниями. Увеличение количества норм, предусматривающих ответственность за преступления мошеннической направленности, может свидетельствовать об уровне распространенности и общественной опасности. На сегодняшний день актуальность противодействия настоящему деянию нисколько не уменьшилась, а наоборот, только увеличилась. Быстрые темпы развития экономики государства, института собственности, увеличение количества договорных отношений, конечно же, не оставили мошенников равнодушными. В связи с чем, привело к появлению новых видов мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Сегодня используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов и компьютеров. Постоянно появляются новые модели, программы и сервисы.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

В связи с чем, было принято Постановление Президента Республики Узбекистан № 4024 от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации и их защиты». Так как, внедрение в Узбекистане современных информационно коммуникационных систем в сфере государственного и общественного управления привело к мошенническим действиям, и сталкиваются с эти чуть ли не каждый второй житель. Наивно предполагать, что жертвами этих злоумышленников становятся только пожилые люди, это далеко не так. На удочку криминальных элементов может попасть абсолютно каждый.

В связи с чем, появляются новые виды мошенничества. Согласно статье 168 Уголовного кодекса Узбекистана, мошенничество – это завладение чужим имуществом или правом на чужое имущество путём обмана или злоупотребления доверием. Отличие мошенничества от других имущественных преступлений заключается в том, что при мошенничестве потерпевшие отдают мошеннику своё имущество и право на имущество по собственному желанию.

В статье 168 Уголовного кодекса мошенничество разделено на 5 частей. В 4 частях указано, при каких случаях применяется отягчающая квалификация. В пятой части изложены смягчающие обстоятельства. То есть, если после совершения преступления причинённый ущерб полностью возмещён, в отношении обвиняемого, подозреваемого или подсудимого может не применяться наказание в виде лишения свободы.

В настоящее время, под современное определение «мошенничество» попадают многие незаконные действия в самых различных сферах, в том числе и в сфере банковской деятельности, сотовой связи и современных информационных технологий. Несмотря на различия в технологии, все эти действия объединяет ряд общих признаков:

- Обманные действия; - Злоупотребление доверием;

-Умышленное искажение фактов или умолчание;

- Хищение чужой собственности;

- Незаконное приобретение прав на чужую собственность;

В большинстве случаев жертва мошенничества самостоятельно и добровольно передает преступникам свою собственность или права на нее. К примеру, мошеннические действия в банках можно условно разделить на несколько групп:

Мошенничество при кредитовании – зачисление сумм, предназначенных для погашения долга на другие счета, оформление кредитов на несуществующих заемщиков, оформление кредитов без ведома клиентов;

Мошенничество при рассчетно-кассовом обслуживании – несанкционированное списание сумм со счета, подмена купюр фальшивыми, вытягивание банкнот из пересчитанной пачки;

Мошенничество с депозитами – изъятие внесенных средств, преуменьшение сумм в документах, списание средств без ведома клиента.

Большинство банковских махинаций осуществляются в филиалах и отделениях банков, где меньше контроля, а не в крупных головных офисах. В таких условиях сотрудников меньше, но они вовлечены в большее количество бизнес-процессов, что открывает более широкие возможности для незаконной деятельности.

Например, разыгрывается звонок близкого родственника, попав В связи с активным ростом рынка электронных платежей и онлайн шопинга развиваются и новые современные формы мошенничества с использованием информационных технологий. Самыми распространенными видами мошенничества в интернете являются следующие махинации:

Фишинг – кража персональных данных (пароля, логина) с целью похищения средств с банковской карты. В основном для фишинга используют почтовую рассылку, содержащую ссылку на фальшивые сайты;

Мошенничество через электронную почту – так называемые «нигерийские письма». Они содержат в себе красивую легенду о наследстве от мифического родственника и просьбу перевести деньги на счет для получения оплаты услуг адвоката или выплаты комиссии;

Махинации с интернет-кошельками – чаще всего в таких случаях покупатель переводит предоплату продавцу на интернет-кошелек, но в итоге не получает ни товара, ни денег.

Мошенничество при помощи сотовой связи можно условно разделить на две группы. К первой следует отнести снятие денег непосредственно со счета владельца номера без его ведома. Такими махинациями могут заниматься как сами сотовые операторы, так и не имеющие отношения к их компаниям мошенники. Во вторую группу мошенничеств можно отнести случаи, в которых абонент сам перечисляет деньги на указанный счет, либо отдает их прямо в руки или оставляет в указанном мошенниками месте. В таких аферах

сотовая связь выступает лишь в качестве инструмента инсценировки шего в беду и срочно нуждающегося в деньгах.

Мошенничество с деньгами – это одна из самых обширных и всеобъемлющих групп, ведь практически любое мошенничество, так или иначе, подразумевает незаконное овладение чужими денежными средствами. Однако можно выделить несколько способов мошенничества, связанных косвенно или непосредственно с наличными купюрами. Эти способы могут практиковаться в магазинах, ларьках, обменных пунктах. Самым простым и распространенным является мошенничество путем замены настоящих купюр в пачке на фальшивые (в основном, сверху и снизу – настоящие, посередине – фальшивые или обычная бумага). Также практикуется «недостача» - из уже пересчитанной пачки купюр вытягивается несколько банкнот. Мошенничество может производиться также с помощью банкомата при попытке снять наличность, на котором устанавливается датчик, считывающий персональные данные.

«Ассортимент» разнообразных махинаций в наши дни существенно расширился, в основном благодаря приходу в повседневную жизнь современных технологий – таких, как интернет, сотовая связь, онлайн-шоппинг и банкинг. Однако традиционные виды мошенничеств также до сих пор развиваются. Среди них можно назвать уличных мошенников, предлагающих купить драгоценные изделия, подставных лиц, устраивающих аварии и предлагающих договориться на месте. Одним из самых крупных и вовлекающих одновременно большое количество человек видом аферы является финансовая пирамида.

ЗАКЛЮЧЕНИЕ

Все самые распространенные виды мошенничества были приведены выше, и они объединяются одним общим знаменателем – они осуществляются с учетом психологии потенциальных жертв аферистов. Аферы продумываются до мельчайших деталей и способны обмануть бдительность даже самых осторожных и внимательных людей. Именно поэтому необходимо помнить о том, что персональные данные, такие, как пароль, логин, номер банковского счета, кодовое слово, CVV2-код на банковской карте нельзя передавать в третьи руки.

Использованная литература:

1. Конституция Республики Узбекистан.

2. Постановление Пленума Верховного суда Республики Узбекистан от 11 октября 2017 года № 35 «О судебной практике по делам о мошенничестве».

3. Уголовный кодекс Республики Узбекистан.

4. Закон Республики Узбекистан от 14 мая 2014 года ЗРУ-371 «О профилактике правонарушений».

5. Постановление Президента Республики Узбекистан от 14 марта 2017 года №2833 «О мерах по дальнейшему совершенствованию системы профилактики правонарушений и борьбы с преступностью».

6. Постановление Президента Республики Узбекистан от 21 ноября 2018 года ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты».

7. Курс уголовного права Республики Узбекистан. Рустамбаев М.Х. Общая часть. Том 1. 2009. 8. Егорова Н.А.