"MONEY AND BANKS" COURSE
Topic -12: MODERN MONEY CIRCULATION RISK MANAGEMENT

«PUL VA BANKLAR» FANI
Mavzu - 12: ZAMONAVIY PUL MUOMALASI RISKLARINI BOSHQARISH

Reja:

12.1. Raqamlashtirish sharoitida axborot xafsizligi va uning axamiyati

Axborot xavfsizligi - bu ma'lumotlarga ruxsatsiz kirish, foydalanish, oshkor qilish, noto'g'ri taqdim etish, o'zgartirish, tekshirish, yozib olish yoki yo'q qilishning oldini olish amaliyotidir (Wikipedia). U uchta maxfiylik, yaxlitlik va ma'lumotlarning mavjudligi tamoyillariga rioya qilish uchun javobgardir.

Axborot xavfsizligining asosiy vazifasi - ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini muvozanatli himoya qilish. Bunga asosiy va nomoddiy aktivlarni, tahdidlar manbalarini, zaifliklarni, potentsial ta'sirlarni va risklarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli risklarni boshqarish jarayoni orqali erishiladi.

Maxfiylik ma'lumotlarga faqat vakolatli shaxslar, ya'ni bunday qilish huquqiga ega bo'lganlar kirishini ta'minlaydi.

Axborotning yaxlitligi barcha ma'lumotlarning to'liq va o'zgartirilmagan holda saqlanishini anglatadi.

Olish imkoni mavjudligi ma'lum ma'lumotlarga kirish huquqiga ega bo'lganlar har doim undan foydalanishi mumkinligini anglatadi.

Raqamli xavf - bu xavf samaradorligi va samaradorligini oshiradigan barcha raqamli imkoniyatlarni, xususan, jarayonlarni avtomatlashtirish, qaror qabul qilishni avtomatlashtirish, raqamli monitoring va erta ogohlantirishni o'z ichiga olgan atama. Yondashuvda ish jarayonini avtomatlashtirish, belgilarni optik aniqlash, ilg‘or tahlil (jumladan, mashinani o‘rganish va sun’iy intellekt) va yangi ma’lumotlar manbalari, shuningdek, robototexnikani jarayonlar va interfeyslarga qo‘llash qo‘llaniladi. Asosan, raqamli xavf jarayonlarni, ma'lumotlarni, tahliliy va IT-ni va umumiy tashkiliy tuzilmani, shu jumladan iste'dod va madaniyatni kelishilgan sozlashni nazarda tutadi.

Axborot xavfsizligining asosi axborotni himoya qilish faoliyati - uning maxfiyligi, mavjudligi va yaxlitligini ta'minlash, shuningdek, tanqidiy vaziyatda har qanday murosaga yo'l qo'ymaslikdir [5]. Bunday holatlarga tabiiy, texnogen va ijtimoiy ofatlar, kompyuterning ishdan chiqishi, jismoniy o'g'irlash va boshqalar kiradi.

Axborot xavfsizligi tarmoq va tegishli infratuzilma xavfsizligini, dasturiy ta'minot va ma'lumotlar bazasini himoya qilishni, axborot tizimlari auditini, biznesning uzluksizligini rejalashtirishni, elektron yozuvlarni aniqlash va kompyuter kriminalistikasi kabi ko'plab professional ixtisosliklarni yaratdi.

Axborot xavfsizligiga tahdidlar turli shakllarda bo'lishi mumkin. 2018 yil uchun eng jiddiylari "xizmat sifatida jinoyat " (ingliz. Crime-as-a-Service), narsalar Interneti, ta'minot

Bu Ta'minot zanjirlariga tahdid shundaki, tashkilotlar o'z etkazib beruvchilari bilan turli xil qimmatli va nozik ma'lumotlarni almashishga moyil bo'lib, ular ustidan bevosita nazoratni yo'qotadilar. Shunday qilib, ushbu ma'lumotlarning maxfiyligi, yaxlitligi yoki mavjudligini buzish xavfi sezilarli darajada oshadi. Regulyatorlarning tobora ko'proq yangi talablari tashkilotlarning hayotiy axborot aktivlarini boshqarishni sezilarli darajada murakkablashtiradi. Misol uchun, 2018 yilda Yevropa Ittifoqida qabul qilingan Ma'lumotlarni himoya qilish bo'yicha umumiy reglament har qanday tashkilotdan istalgan vaqtda o'z faoliyati yoki ta'minot zanjirining istalgan qismida qanday shaxsiy ma'lumotlar va u erda qanday maqsadlar uchun mavjudligini ko'rsatishni talab qiladi, ular qayta ishlanadi, saqlanadi va himoyalanadi. Bundan tashqari, ushbu ma'lumotlar nafaqat vakolatli organlar tomonidan tekshirish paytida, balki ushbu ma'lumotlar egasining birinchi talabiga binoan ham taqdim etilishi kerak. Bunday muvofiqlikka rioya qilish muhim byudjet mablag'lari va resurslarini tashkilotning boshqa axborot xavfsizligi vazifalaridan chetlashtirishni talab qiladi. Shaxsiy ma'lumotlarni qayta ishlashni soddalashtirish uzoq muddatli istiqbolda axborot xavfsizligini yaxshilashni nazarda tutsa ham, qisqa muddatda tashkilotning xavflari sezilarli darajada oshadi.

Aksariyat odamlar u yoki bu tarzda axborot xavfsizligi tahdidlariga duchor bo'lishadi. Masalan, ular zararli dasturlar (viruslar va qurtlar, troyanlar, ransomware), fishing yoki identifikatorni o'g'irlash qurboni bo'lishadi.

Fishing — maxfiy ma’lumotlarni (masalan, hisob, parol yoki kredit karta ma’lumotlari) olishga qaratilgan firibgarlik urinishi. Odatda, ular internet foydalanuvchisini har qanday tashkilotning (bank, internet-do‘kon, ijtimoiy tarmoq va h.k.) asl veb-saytidan ajratib bo‘lmaydigan soxta veb-saytga jalb qilishga harakat qiladilar. Qoidaga ko'ra, bunday urinishlar, go'yoki tashkilotning o'zi nomidan, soxta saytlarga havolalarni o'z ichiga olgan soxta elektron pochta xabarlarini ommaviy yuborish orqali amalga oshiriladi. Brauzerda bunday havolani ochib, bexabar foydalanuvchi firibgarlarning mulkiga aylangan o'z hisob ma'lumotlarini kiritadi. Ingliz tilidan «Identity Theft» atamasi. — "identifikatsiya o'g'irligi" 1964 yilda ingliz tilida paydo bo'lgan, bunda kimningdir shaxsiy ma'lumotlari (masalan, ism, bank hisobi yoki kredit karta raqami, ko'pincha fishing orqali olingan) firibgarlik va boshqa jinoyatlarni sodir etish uchun foydalaniladi. Axborot xavfsizligi shaxsiy hayotga bevosita ta'sir qiladi, bu turli madaniyatlarda turlicha ta'riflanishi mumkin.

- Tokenlar va raqamli huquqlar (tokenlashtirilgan aksiyalar, robotlar, mobil banking, aqlli shartnomalar)
- Kriptovalyuta (raqamli valyuta)
- Raqamli moliyaviy aktivlar
- Virtual mulk
- Personal ma’lumotlar va katta ma’lumotlar (Big date)
- Intelektual faoliyati natijalari raqamli shaklda.

Tasniflashda tartibga soluvchi raqamli texnologiyalarni ajratish mumkin:

a) moliya institutlari tomonidan qo'llaniladigan muvofiqlik texnologiyalari bo'yicha korporativ risklarni boshqarish

b) tartibga soluvchi (RegTech). Ishtirokchilarning risklarini tartibga solishda moliya bozorini tartibga soluvchi organlar tomonidan qo’llash mumkin.

Raqamli muvofiqlik texnologiyalari oqim samaradorligini oshirishga yordam beradi jarayonlarni kuzatish va boshqarish (masalan, kompyuter yordamida biznes-tahlil bo'yicha trening), bilan bog'liq muvofiqlik jarayonlarini avtomatlashtirish regulyatorning me'yoriy talablariga muvofiqligi, hisobot boshqaruvi, tranzaktsiyalarning ichki monitoringi, mijozlarni identifikatsiya qilish.

Raqamli ob'ektlar (asboblar) o'rtasidagi asosiy farqlar. Klassik bozorga nisbatan moliyaviy bozor: an'anaviy bozorni almashtirish raqamli moliyaviy vositalar (kriptovalyuta (to'lov belgilari), foydali tokenlar, tokenlashtirilgan aksiyalar (inglizcha xavfsizlik tokenidan), robotlar, mobil banking, aqlli shartnomalar), to'lov xavfsizligini oshirdi aqlli shartnomalar orqali operatsiyalar, ochiq dasturlash imkoniyati, operatsiyalarni optimallashtirish va yaxlitligi, uzoq muddatli xotira (to'liq bitimlar tarixi), bozor ehtiyojlariga moslashish.

Xalqaro amaliyotda moliyaviy risklarni boshqarishni modellashtirishga turlicha yondashuvlar mavjud. Masalan, moliyaviy risklarni boshqarish (Moliyaviy risklarni boshqarish) - bu qabul qilingan moliyaviy risklar qiymmatini baholash va iqtisodiy faoliyat natijasida olingan risklar uchun adolatli kompensatsiyani nazorat qilish jarayoni. Moliyaviy vositalardan foydalangan holda, ta'sir ko'rsatish boshqariladi, shu jumladan quyidagi risklar: operatsion risk, kredit riski, bozor riski, valyuta riski, o'zgaruvchanlik riski, likvidlik riski, biznes riski, yuridik risk, obro'-e'tibor xavfi, tarmoq riski va boshqalar.

Moliyaviy risklarni boshqarish tushunchalari xalqaro miqyosda tez va sezilarli o'zgarishlarga duchor bo'ladi. Ushbu muammolarni bartaraf etishda transmilliy korporatsiyalar turli to'siqlarga duch kelishadi. Ko'pgina mamlakatlarda ishlayotgan kompaniyalar e'tiborga olishlari kerak bo'lgan xatarlarni o'rganish o'tkazildi.

12.2. Raqamlashtirish sharoitida banklarning moliyaviy jinoyatlar xavfiga qarshi kurashish strategiyasi

To'lov xizmatlari uzoq vaqtdan beri kompaniyalar va jismoniy shaxslarga banklar tomonidan taklif qilingan, ammo so'nggi 20 yil ichida maxsus va ixtisoslashgan provayderlar bozorni sezilarli darajada kengaytirdilar. 2020 yilda global to'lovlar daromadi 1,9 trillion dollarga yetdi. So'nggi o'n yil ichida jismoniy shaxslar va elektron tijorat savdogarlari to'lov xizmatlaridan tobora ko'proq foydalanmoqda. So'nggi o'sishning yarmiga yaqini iste'molchidan biznesga va biznesdan iste'molchiga to'lovlarda bo'ldi. Shimoliy Amerika va Evropada elektron to'lovlar juda tez kengaymoqda, bu mintaqalarda YaIM o'sish sur'atlaridan ikki baravar ko'p; Osiyoda kengayish yanada tezlashmoqda. Elektron tranzaktsiyalar sonining portlashi elektron tijorat va m-tijorat bumlarining bir qismi va naqd to'lovlardan voz kechishdir. Raqamli to'lov mexanizmlari kartalarni, shuningdek, raqamli hamyonlar kabi so'nggi to'lov yangiliklarini ham o'z ichiga oladi. Raqamli to'lovlarga o'tish davom etishi kutilmoqda.

To'lov xizmatlarini ko'rsatuvchi provayderlar (PSP) muvaffaqiyatining muqarrar o'lchovlaridan biri bu moliyaviy jinoyatlar xavfining oshishi hisoblanadi. Elektron to'lov platformalari tomonidan qo'llaniladigan nazoratning zaif tomonlari regulyatorlarning e'tiborini tortadi. Bundan tashqari, banklar o'z tarmog'ining bir qismini tashkil etuvchi PSP'lardan pul yuvishga qarshi (AML) va firibgarlikka qarshi kuchli nazoratga ega bo'lishini tobora ko'proq kutishmoqda. Yangi tartibga solishni kutish o'rniga, PSPlar o'zlarining ilg'or texnologik ko'nikmalaridan foydalangan holda banklar tajribasidan saboqlarni o'z ichiga olgan holda faol harakat qilishlari mumkin. Ushbu munozarada PSP mijozlar tajribasini saqlab qolish va yaxshilashda moliyaviy jinoyatlar tahdidiga qarshi turishda o'z foydalari uchun foydalanishi mumkin bo'lgan strategiyani ishlab chiqishning asosiy tamoyillari bayon etilgan.

Moliyaviy jinoyatlar xavfi ortib borayotgani tartibga soluvchi e'tiborni kuchaytirdi. Birlashgan Millatlar Tashkilotining Giyohvand moddalar va jinoyatchilik bo'yicha boshqarmasining xabar berishicha, pul yuvish qiymatini hisoblash juda qiyin, ammo bu miqdorlar juda katta va o'sib borayotganini ta'kidlaydi, bu esa jahon yalpi ichki

mahsulotining 5 foiziga yoki yiliga 800 milliard dollardan 2 trillion dollargacha yetadi (Mikkelsen, Rajdev & Stergiou, 2022).

Taqiqlangan va noqonuniy giyohvand moddalar savdosi, soliq to'lashdan qochish sxemalari, pul yuvish va iste'molchilarning firibgarliklari kabi noqonuniy faoliyatlar raqamli to'lov kanallaridan tobora ko'proq foydalanmoqda va bu vositalar orqali pul yuvish xavfini oshirmoqda.

Barcha so'nggi nuqtalarni himoya qilish echimlari yoki antiviruslar, masalan, elektron pochta bilan bog'liq tahdidlardan himoya qilmaydi. Oddiy qilib aytganda, tashkilot o'z aktivlarini himoya qilish uchun faqat bitta yondashuvga tayanishi mumkin emas, unga chuqurlikdagi mudofaa (DiD **-** Defense in Depth) deb nomlanuvchi qatlamli yondashuv kerak.

DiD strategiyasi xavfsizlikning bir qatlamidan kiberhujumlarga qarshi yagona qarshi chora sifatida foydalanilmasligini nazarda tutadi. Agar ushbu bitta qatlam tarmoqni himoya qila olmasa, u holda hamma narsa (aktivlar) xakerlar tomonidan buzib kirishi uchun ochiq bo'ladi. DiD barcha aktivlarni har xil turdagi kiberhujumlardan himoya qilish uchun qatlamli yondashuvni amalga oshiradi, bunda agar bir qatlam aktivni himoya qila olmasa, xavfsizlikni ta'minlash uchun boshqa qatlam mavjud.

Chuqur mudofaa kontseptsiyasi infratuzilma mudofaa tashkilotini uchta boshqariladigan qismga ajratadi:

Jismoniy: Bu ruxsatsiz shaxslar tomonidan AT infratuzilmasiga jismoniy kirishni cheklash bo'yicha barcha choralarni o'z ichiga oladi. Masalan, ofis qo'riqchisi, kirishni boshqarish tizimlari, CCTV kameralari, signalizatsiya, qulflangan telekommunikatsiya kabinetlari va boshqalar.

Texnik: bu axborot tizimi ob'ektlariga tarmoq kirishini boshqarish uchun mo'ljallangan barcha apparat va dasturiy ta'minot axborot xavfsizligi vositalarini, xavfsizlik devori, ish stantsiyalari, proksi-serverlar, autentifikatsiya va avtorizatsiya tizimlari uchun virusga qarshi himoya vositalarini o'z ichiga oladi.

Ma'muriy: Bu tashkilot tomonidan qabul qilingan barcha axborot xavfsizligi siyosati va protseduralarini o'z ichiga oladi. Ushbu hujjatlar himoyani boshqarish, muhim ma'lumotlarni tarqatish va qayta ishlash, kompaniyada dasturiy va texnik vositalardan foydalanishni, shuningdek, xodimlarning axborot tizimi, uchinchi tomon tashkilotlari va boshqa tashqi sub'ektlar bilan o'zaro munosabatlarini tartibga solish uchun mo'ljallangan. Tashkilot o'z aktivlarini himoya qilish uchun faqat bitta yondashuvga tayanishi mumkin emas, unga chuqurlikdagi mudofaa (DiD) deb nomlanuvchi qatlamli yondashuvi kerak.

DiD strategiyasi xavfsizlikning bir qatlamidan kiberhujumlarga qarshi yagona qarshi chora sifatida foydalanilmasligini nazarda tutadi. Agar ushbu bitta qatlam tarmoqni himoya qila olmasa, u holda hamma narsa (aktivlar) xakerlar tomonidan buzib kirishi uchun ochiq bo'ladi. DiD barcha aktivlarni har xil turdagi kiberhujumlardan himoya qilish uchun qatlamli yondashuvni amalga oshiradi, bunda agar bir qatlam aktivni himoya qila olmasa, xavfsizlikni ta'minlash uchun boshqa qatlam mavjud.

Bank sektoridagi xatarlarni boshqarishning raqamli strategiyalari jarayonlarni avtomatlashtirish, qarorlarni avtomatlashtirish va raqamli monitoring va erta ogohlantirishni o'z ichiga oladi. Ushbu strategiyalarda ish oqimini avtomatlashtirish, optik belgilarni aniqlash, ilg'or tahlillar (shu jumladan mashinani o'rganish va sun'iy intellekt) va yangi ma'lumotlar manbalari, shuningdek, jarayonlar va interfeyslarga robototexnika qo'llanilishi .

Raqamlashtirish bank strategiyasiga chuqur singib ketdi, so'nggi o'n yil ichida xarajatlarning sezilarli oshishini ko'rgan xavf funktsiyasi bundan mustasno bo'lmasligi kerak. Darhaqiqat, tavakkalchilikdagi raqamli o'zgarishlarni samaradorlik va tavakkalchilik qarorlarining sifatini oshirish orqali haqiqiy biznes qiymatini yaratish mumkin. Raqamli

xavf funktsiyasi, shuningdek, yaxshiroq monitoring va nazoratni va tartibga solishning yanada samarali muvofiqligini ta'minlaydi.

12.3. Raqamli to‘lovlar sohasida moliyaviy jinoyatlar xavflarini boshqarish usullari

Moliyaviy jinoyatlar bo‘yicha xalqaro standartlarni belgilovchi yetakchi organ – Moliyaviy harakatlar bo’icha xakqaroishchi quruh (Financial Action Task Force) ma’lumotlariga ko‘ra, butun pandemiya davrida moliyaviy jinoyatlar va muvaffaqiyatsizliklar ko‘payib borgan. Ayniqsa, iste'molchilar sohasida, firibgarlik salohiyati ham COVID-19 pandemiyasi paydo bo'lishi bilan oshdi. Buni engish uchun ko'plab PSPlar tranzaksiya monitoringi kabi boshqaruvlarini kuchaytirdilar, regulyatorlar esa masofaviy ishga tushirish va mijozlarni doimiy tekshirishga oid talablarni yangiladilar. Aksariyat platformalarda mijozni bilish (KYC - Know Your Customer) talablari (masalan, shaxsni tekshirish) va tranzaksiyalarni doimiy monitoring qilish bo'lsa-da, boshqalari hisob ochish va yuritish uchun kamroq tafsilotlarni talab qiladi. Qanday bo'lmasin, moliyaviy jinoyatlarga qarshi qiymat zanjiri bo'ylab mavjud nazoratning zaifliklari moliyaviy jinoyatlar bilan shug'ullanuvchilar uchun maqsaddir. Eng muhimi, raqamli va kontaktsiz to'lovlar, shuningdek, masofaviy ulanish ko'plab mijozlar tomonidan ma'qullangan imkoniyatlardir. O'sib borayotgan hajmlar kompaniyalarning salohiyatini va mijozlar tajribasiga salbiy ta'sir ko'rsatmasdan tegishli operatsion risklarni aniqlash va boshqarish qobiliyatini kengaytiradi.

Agar nazorat qilinmasa, moliyaviy jinoyatlar PSPlar uchun ekzistensial xavf tug'dirishi mumkin. Misol uchun, keng miqyosda ekvayring xizmatlarini taklif qiluvchi PSP'lar noqonuniy manbalardan olingan daromadlarni yuvish uchun ushbu xizmatlardan foydalanish uchun maxsus tuzilgan firibgar tashkilotlarga duch kelishi mumkin. Bortga kirish va undan keyin ishonchli, uzluksiz KYC jarayonlarining etishmasligi pul yuvish vositalarini jalb qilishi va provayderning obro'si va tartibga soluvchi obro'siga putur etkazishi mumkin. Xuddi shunday, PSPlar turli tashkilotlarga va ulardan pul mablag'larini o'tkazishni osonlashtirgani uchun, ular sanktsiyalangan sub'ektlar emasligini va ruxsat etilgan yakuniy-benefisiar egasiga tegishli emasligini ta'minlashi kerak. Mijozlarni monitoring qilish, tranzaktsiyalarni kuzatish va skrining dasturlari asosiy boshqaruv vositalaridir. Bundan tashqari, PSP-larning virtual aktivlar birjalariga (VASP) va undan keladigan to'lov xizmatlarini ko'rsatishi ushbu birjalar bilan bog'liq bo'lgan muayyan faoliyat va mijozlardan kelib chiqadigan obro' va moliyaviy jinoyat xavfiga duchor bo'ladi. Tahdidga qarshi turish uchun PSPlar ushbu birjalarning moliyaviy jinoyatlarga qarshi kurash tizimini tushunishlari kerak.

Raqamli to'lov platformalarini boshqarishdagi zaif tomonlar tartibga solishning kuchayishiga olib kelishi mumkin. Bu sanoatda yaxshi tan olingan namunadir, chunki moliya institutlari odatda yangi tartibga solishni kutish o'rniga munosabatda bo'lishadi. Masalan, Yevropa Ittifoqi 2015-yilda qayta ko‘rib chiqilgan to‘lov xizmatlari bo‘yicha Direktivani (PSD2) qabul qildi. Qoida Yevropa Ittifoqi va Yevropa iqtisodiy hududidagi PSP landshaftida iste’molchilar huquqlarini himoya qilishni uyg‘unlashtirish va kuchaytirishga qaratilgan edi. Bu firibgarlikka qarshi nazoratga yangi e'tiborni taqdim etdi. Endi firmalar PSP2 ga ko'proq yoki kamroq mos kelishi kutilmoqda, bu tez orada har tomonlama ko'rib chiqilishi va firibgarlik va mijozlarni himoya qilishga e'tiborni kuchaytirishi mumkin. Xuddi shunday, PSPlar to'lov qiymat zanjirining bir qismini tashkil qilganligi sababli, tartibga soluvchilar PSPlar nomidan to'lovlarni osonlashtiradigan banklarni o'zlarining mijozlari va hamkorlari tarmog'i bo'ylab moliyaviy jinoyatlarga qarshi nazorati etarliligini tasdiqlash uchun ogohlantirmoqda.

Moliyaviy jinoyatlarga qarshi kurash samaradorligi haqidagi xavotir ortib borayotganini hisobga olib, Yevropa Ittifoqi ham maxsus tartibga soluvchi organni tashkil qilmoqchi va PSPlar bu masalalar bo'yicha kuchaytirilgan tekshiruvni ko'rishlari mumkin. 2021-yil iyul oyida Yevropa Komissiyasi (EK) jinoiy daromadlarni legallashtirish va terrorizmni moliyalashtirishga qarshi kurashish bo‘yicha yangi Yevropa Ittifoqi vakolatini yaratish rejasini e’lon qildi. Evropa Ittifoqi darajasidagi Pul yuvishga qarshi kurash boshqarmasi (AMLA) shubhali faoliyatni aniqlashni kuchaytirish va moliyaviy tizimni jinoiy noto'g'ri foydalanishdan yaxshiroq izolyatsiya qilish uchun mo'ljallangan yangi qonunchilik choralari bilan qo'llab-quvvatlanadi. EC e'lonida aytilishicha, AML texnologik innovatsiyalar bilan bog'liq yangi va paydo bo'layotgan muammolarni hisobga olgan holda moliyaviy jinoyatlar bo'yicha mavjud Evropa Ittifoqi tizimini "katta yaxshilaydi". Bularga virtual valyutalar, yagona bozorda yanada integratsiyalashgan moliyaviy oqimlar va ayrim taqiqlangan tashkilotlarning global ta'sir doirasi kiradi. Ushbu takliflar jinoiy faoliyatdan olingan daromadlarni legallashtirishga va terrorizmni moliyalashtirishga qarshi kurashish qoidalariga rioya qilishni operatorlar, ayniqsa, chegaralar orqali faol bo'lganlar uchun osonlashtiradigan ancha izchil asos yaratishga yordam beradi.

Qo'shma Shtatlarda joriy tartibga soluvchi asosiy e'tibor litsenziyalangan pul o'tkazgichlariga qaratilgan, ammo PSP'lar ushbu sohalardagi boshqa provayderlarga o'xshash standartlar qo'llanilmaydi deb taxmin qila olmaydi. Moliyaviy jinoyatlarga rioya qilish yukini faqat banklar o'z zimmasiga oladi, deb ham taxmin qilish mumkin emas. Moliyaviy jinoyatlarga qarshi kurash tarmog'i (FinCEN) va depozitlarni sug'urtalash bo'yicha federal korporatsiya (FDIC) moliyaviy institutlarga PSPlar tomonidan yuzaga keladigan yuqori xavflarni tan olishga yordam berish uchun ko'rsatmalar berdi. Natijada, AQSh moliya institutlari endi o'z tarmog'ining bir qismini tashkil etuvchi PSP'lardan AML, sanktsiyalar va firibgarlikka qarshi kuchli nazoratga ega bo'lishini kutmoqda. Ushbu nazoratlar savdogarning tegishli tekshiruvi va shubhali faoliyat monitoringi, shuningdek, PSPlar moliyaviy institutlarni qo'shimcha xavf ostiga qo'ymasligini ta'minlash uchun boshqa jarayonlarni (xavfni baholash kabi) o'z ichiga oladi.

Yevropa va boshqa yurisdiksiyalardagi moliya institutlari AQSH dollarida biznes yuritganligi sababli, bu chora-tadbirlarning barchasiga ta'sir qiladi. Firibgarlik va pul yuvish holatlari ko'payganligi sababli, Qo'shma Shtatlar va boshqa yurisdiktsiyalar to'lov provayderlari uchun talablarga rioya qilishni kuchaytirishi mumkin. Yevropa Ittifoqi doirasida PSD2 ga taklif qilinayotgan yaxshilanishlar firibgarlik, moliyaviy jinoyatlar va mijozlar xavfsizligiga ko‘proq e’tibor qaratishi kutilmoqda. Mijoz identifikatori va autentifikatsiyasiga oid texnik talablar kuchaytirilishi va to‘lovni to‘lovni to‘lovni qaytarish tartib-qoidalari orqali to‘lovchining himoyasi kiritilishi kutilmoqda.

Banklar tajribasidan kelib chiqadigan bo'lsak, PSPlar bunday risklarni to'g'ri boshqara olmasligi tufayli obro'ga katta zarar yetkazishi mumkin. Normativ e'tiborga qo'shimcha ravishda, to'lov platformalaridagi faoliyat moliyaviy jinoyatlardan tashqari sabablarga ko'ra kuzatuvchi tashkilotlarning e'tiborini tortdi va bu obro'ga xavfni samarali boshqarishning ahamiyatini oshirdi. Masalan, Strategik muloqot instituti va janubiy qashshoqlik huquqi markazi xabar berishicha, irqchi guruhlar mablag' yig'ish uchun asosiy to'lov platformalaridan foydalanishda davom etmoqda. Bunday faoliyatlar haqidagi matbuot xabarlari keng jamoatchilik tomonidan faollarning javoblariga sabab bo'lishi mumkin, hatto ijtimoiy mas'uliyatni bajarmagan brendlar va kompaniyalarni boykot qilishi mumkin.3 Ba'zi noto'g'ri foydalanish holatlari texnik jihatdan qonun doirasida bo'lishi mumkin, ammo brend va ishonchga jiddiy zarar etkazishi mumkin. Shunday bo'lsa-da, mijozlar.

Shunday qilib, moliyaviy-jinoyat risklarini boshqarishning nazorat mexanizmlari biznes modeli, mijozlar va PSPl.arning ichki operatsiyalariga ta'sir qiladi. Ta'sirlar

boshqaruv elementlari qanday o'rnatilgani bilan belgilanadi. Ushbu muammolarni hal qilish uchun mo''jizaviy texnologik yechim mavjud emas yoki tez orada ishlab chiqilmaydi. Aksariyat hollarda banklar va PSPlar o'zlarining ichki jarayonlarini barqaror, yaxshiroq tuzilgan va integratsiyalashgan qilish uchun doimiy ravishda baholaydilar. Ushbu jarayonda ular qabul qilgan vositalar, platformalar va tizimlar shunchaki yordam beradi. Ushbu maqolada PSP mijozlar tajribasini saqlab qolish va yaxshilashda moliyaviy-jinoyat risklarini boshqarishda o'z foydasiga foydalanishi mumkin bo'lgan strategiyani ishlab chiqishning asosiy tamoyillari bayon etilgan.

Xavf ta’sirini belgilaydigan xavfni yakka tartibda baholash.

Xavfga aniq shakllantirilgan tabitni ta’minlash uchun biznes-modelni qo‘llash natijasida yuzaga keladigan xavflarni yakka tartibda baholash zarur. PSP va iste’molchilar va savdoschilar uchun boshqa xizmatlar etkazib beruvchilar uchun ular uchun muayyan salohiyatli xavflarni aniqlashi va o‘z biznesini himoya qilish uchun tegishli ichki infratuzilma yaratishi kerak. Har bir PSP o‘zining biznes-modellari tushadigan moliyaviy xavflar turli tipologiyasi va stsenariylarini ko‘rib chiqishi lozim. Elektron tijorat platformasi, masalan, noqonuniy mablag‘larni o‘tkazish uchun mijozlar bilan fuqarolik qilayotgan firibgarlik savdolarini jalb etishi mumkin. Transchegaraviy to‘lovlarni ta’minlovchi platformalar boshqa muassasalar tomonidan ko‘rilgan nazorat chora-tadbirlarini bartaraf etish uchun foydalanishi mumkin.

Moliyaviy-jinoyat xavfini boshqarish uchun PSPlar moliyaviy jinoyatlarni boshqarish bo'yicha o'z yondashuvlarini qayta ko'rib chiqar ekan, ular **uchta asosiy dizayn** tamoyilini qo'llashlari mumkin.

1.*Proportsional ramka yaratish*. Nazorat tizimi umumiy biznes modeliga mutanosib bo'lishi kerak. Tashkilotlar o'zlarining xavf ishtahalaridan tashqarida bo'lgan xavf-xatarlarni qabul qilishga tayyor ekanliklarini hal qilishlari kerak. Misol uchun, ba'zi AML va KYC muammolari to'lov biznes modelining muhim afzalligi bilan bog'liq: soddalashtirilgan mijozlar tajribasi, jumladan, tezkor ishga tushirish, tekshirish va tranzaktsiyalar.

2.*An'anaviy nazorat muhitiga o’zgartirish.* PSPlar an'anaviy banklarning boshqaruv muhiti va tizimlarining samaradorligini shubha ostiga qo'yishi mumkin. Ko'proq nazorat PSPlar uchun moliyaviy jinoyatlardan yaxshiroq himoya qilishni anglatmaydi. Ushbu keskinlikni aniqlab, PSP'lar tartibga soluvchi talablarni qondirish va mijozlar tajribasi maqsadlarini qo'llab-quvvatlash uchun yanada ijodiy fikrlash va faol ravishda echimlarni ishlab chiqish imkoniyatiga ega bo'ladi.

3.*Ta'sir qilishda doimo faol bo'lish.* PSPlar tartibga solish talablariga va regulyatorlarning e'tiboriga javob berishdan ko'proq narsani qilishlari kerak. Ularning ta'siriga samarali javob berish uchun PSPlar xavflarni oldindan bilishlari va asosiy xizmatlar va mahsulotlarni loyihalashda himoya vositalarini yaratishlari kerak. Shuningdek, ular o'z yondashuvlarini doimiy ravishda yangilashlari, masalan, firibgarlik tahdidi manzarasini hal qilish uchun o'zlarining muntazam va maxsus dasturiy ta'minot relizlarini tezda sozlashlari kerak. Oxir oqibat, ushbu strategiya PSPlarga moliyaviy jinoyatlarga qarshi kurashish uchun keyingi avlod mexanizmlarini ishlab chiqishda yordam beradi.

Xatarlarni samarali identifikatsiya qilish yuqori darajadagi ta'riflar va xavflarni nazariy baholashdan ko'ra ko'proq narsani o'z ichiga oladi. U savdogarlarning to'lov qiymati zanjiridagi roli, ularning portfelidagi mijozlar turlari va segmentlari, ularning biznes modellari va mahsulot takliflari, shuningdek hajm va turlar bo'yicha tranzaksiya oqimlarining batafsil, ma'lumotlarga asoslangan tahlillarini o'z ichiga olishi kerak. Keyinchalik tahlil xavf ishtahasi va unga bog'liq bardoshlik chegaralarini belgilash, doimiy ravishda monitoring qilish uchun ishlatilishi mumkin. Ushbu ma'lumotlarning barchasi doimiy ravishda to'planishi va yangilanishi kerak, bunda xavf ishtahasidan farqlar

aniqlanganda, boshqaruv elementlariga kiritilgan triggerlar mavjud.

Tegishli riskga asoslangan yondashuvning g'oyasi shundaki, PSPlar potentsial xavfli operatsiyalar va mijozlarning kichik foiziga ko'proq e'tibor qaratishlari kerak. Buning uchun muassasalar maqsadli aniqlash va mijozlar va tranzaktsiyalarni eng past riskdan eng yuqori xavfga qadar aniq tartiblash imkonini beradigan real vaqt rejimida, dolzarb ma'lumotlarga asoslangan yanada nozik segmentatsiya modellarini ishlab chiqishi kerak. Bunday model nafaqat tarixiy tranzaksiya ma'lumotlarini va KYC fayllaridagi mijozlarning statik yozuvlarini, balki istiqbolli ma'lumotlar nuqtalarini va yomon aktyorlar haqidagi tashqi ma'lumotlarni ham hisobga oladi.

O'z sa'y-harakatlarini boshlashda, PSPlar samarasiz yondashuvlarga resurslarni isrof qilmaslik uchun ushbu tajribadan saboq olishlari mumkin:

Jarayonlar va qarorlar ichiga boshqaruv elementlarini kiriting. Ko'pgina PSPlar toza varaqdan boshlanadi va muhim ilg'or texnologik tajribaga ega. Shuning uchun ular bir nechta ma'lumotlar yoki tizim cheklovlari bilan mos keladigan dizayn jarayonlarini yaratish uchun yaxshi holatda.

Biznes modeliga mutanosib ravishda dizayn boshqaruvi. Ko'pincha, nazorat vositalarining narxi oshishi va ularga e'tibor qaratish PSPlar tomonidan tanlangan biznes modelining bevosita funktsiyasidir, masalan, kripto yoki raqamli aktivlar platformalari kabi yuqori xavfli sektorlarga xizmat ko'rsatish. Bunday hollarda, yanada samaraliroq va samarali boshqaruv va tizimlarga sarmoya kiritish bozorning yuqori xavfli qismlariga xizmat ko'rsatishning zaruriy shartidir.

12.4. Moliya muassasalarining xavf-xatarlarni boshqarish modellarini ishlab chiqishning jaxon tajribasi

XXI asrda jahon iqtisodiyoti yangi raqamli shaklni ola boshladi. Innovatsion biznes yo‘nalishlari, bozor imkoniyatlari va yuqori texnologiyali innovatsion loyihalar paydo bo‘ldi. Ularning paydo bo'lishi moliyaviy risklarni baholashning klassik modellari eskirgan va manfaatdor foydalanuvchilarga ob'ektiv ma'lumot bera olmasligiga olib keldi.

Har qanday xo‘jalik yurituvchi subyekt, xoh davlat, xoh uy xo‘jaligi, xoh tashkilot, o‘z xarajatlarini minimallashtirish, ulkan loyihalarni moliyalashtirish va amalga oshirishdan, qo‘shimcha moliyaviy resurslar yoki foyda olishdan manfaatdor. Qayta ishlab chiqarish jarayonida xo'jalik yurituvchi sub'ekt turli moliyaviy risklar bilan bog'liq muammolar va imkoniyatlarga duch keladi. Har qanday moliyaviy tavakkalchilikni noto'g'ri baholash moliyaviy resurslarning katta qismini yo'qotishga, qiymati eksponent ravishda tushib ketadigan moliyaviy vositalarni sotib olishga yoki aniq foyda keltirmaydigan loyihalarni amalga oshirishga olib kelishi mumkin.

Moliyaviy risklarni boshqarish (Moliyaviy risklarni boshqarish) - bu qabul qilingan moliyaviy risklarning narxini aniqlash va iqtisodiy faoliyat natijasida olingan risklar uchun adolatli kompensatsiyani nazorat qilish jarayoni. Moliyaviy vositalardan foydalangan holda, ta'sir ko'rsatish boshqariladi, shu jumladan quyidagi risklar: operatsion risk, kredit riski, bozor riski, valyuta riski, o'zgaruvchanlik riski, likvidlik riski, biznes riski, yuridik risk, obro' - e'tibor xavfi, tarmoq riski va boshqalar.

Xorijiy amaliyotda moliya institutlarida moliyaviy risklarni boshqarishning turli standartlari mavjud. Masalan, xalqaro faol banklar odatda operativ, kredit va bozor risklarini kuzatish, hisobot berish va aniqlash uchun Bazel kelishuvlariga tayanadilar.

Qo'shma Shtatlarda moliyaviy xizmatlar sektorida kiberxavfsizlikni kuchaytirish uchun bir qancha chora-tadbirlar mavjud. Masalan, Axborot xavfsizligi standartlarini belgilash bo'yicha idoralararo yo'riqnomada bank tashkilotlariga mijozlar ma'lumotlarining xavfsizligi, maxfiyligi va yaxlitligini ta'minlash uchun ma'muriy, texnik va jismoniy himoya

choralarini ishlab chiqish va amalga oshirish talablari qo'yiladi.

Federal zaxira tizimi, shuningdek, kiberxavfsizlik va moliyaviy tizimning barqarorligi to'g'risidagi hisobotga ega bo'lib, unda moliyaviy xizmatlar sektorida kiberxavfsizlikni kuchaytirish va Kengashning tartibga soluvchi sifatidagi funksiyalariga nisbatan ko'rilgan chora-tadbirlar tavsiflanadi.

Bundan tashqari, moliya institutlari va moliya sektorini ortib borayotgan kiberxavfsizlik xatarlaridan yumshatish va himoya qilish orqali moliya tizimining xavfsizligi, mustahkamligi va barqarorligini oshirishga qaratilgan “Moliyaviy xizmatlar sektoriga xos kiberxavfsizlik profili” mavjud.

Moliyaviy xizmatlar sektoriga xos kiberxavfsizlik "profili" moliya sektori uchun va ular tomonidan kiberxavfni baholash uchun asosdir. U Kiberxavfsizlik asosiga asoslanadi va tartibga soluvchilarning muhim boshqaruv va uchinchi tomon muammolariga e'tiborini qaratish uchun moliya sanoati uchun kengaytirilgan.

Profil diagnostik bayonotlar deb ataladigan 277 nazorat maqsadlariga 2400 dan ortiq tartibga soluvchi taxminlarni uyg'unlashtiradi. U rivojlanayotgan kiberxavfsizlikni tartibga solish landshaftini aks ettirish uchun muntazam yangilanadi [5].

Profilning maqsadi moliyaviy institutlar va moliya sektorini kiberxavfsizlikning ortib borayotgan xavflaridan yumshatish va himoya qilish orqali moliya tizimining xavfsizligi, mustahkamligi va mustahkamligini oshirishdan iborat [5].

Tahdid va zaiflikni baholash metodologiyasini va OCTAVE axborot risklarini boshqarish yondashuvini va Britaniya CRAMM metodologiyasi mavjud [6].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) va CRAMM (CCTA Risk Analysis and Management Method) axborot xavfsizligi xavflarini baholash metodologiyasi hisoblanadi. Ular tashkilotlarda axborot xavfsizligi xatarlarini tahlil qilish va boshqarish uchun ishlatiladi.

OCTAVE modelining mohiyati shundan iboratki, xavfni tahlil qilish jarayoni tashqi tashkilotlar maslahatchilari yordamisiz faqat korxona xodimlari tomonidan amalga oshiriladi. Buning uchun ham texnik mutaxassislar, ham barcha darajadagi menejerlarni o'z ichiga olgan aralash guruh yaratish kerak. Bu axborot xavfsizligi bilan bog‘liq yuzaga kelishi mumkin bo‘lgan hodisalar tufayli biznes uchun barcha oqibatlarni har tomonlama baholash, shuningdek, qarshi choralarni ishlab chiqish imkonini beradi.

CRAMM axborot xavfsizligi sohasidagi xavflarni tahlil qilishning birinchi usullaridan biridir. U ustida ish 80-yillarning o'rtalarida Buyuk Britaniyaning Markaziy Kompyuter va Telekommunikatsiyalar Agentligi (CCTA) tomonidan boshlangan.

Xabar qabul qilindi. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) va CRAMM (CCTA Risk Analysis and Management Method) axborot xavfsizligi xavflarini baholash metodologiyasi hisoblanadi. Ular tashkilotlarda axborot xavfsizligi xatarlarini tahlil qilish va boshqarish uchun ishlatiladi. OCTAVE modelining mohiyati shundan iboratki, xavfni tahlil qilish jarayoni tashqi tashkilotlar maslahatchilari yordamisiz faqat korxona xodimlari tomonidan amalga oshiriladi. Buning uchun ham texnik mutaxassislar, ham barcha darajadagi menejerlarni o'z ichiga olgan aralash guruh yaratish kerak. Bu axborot xavfsizligi bo‘yicha yuzaga kelishi mumkin bo‘lgan hodisalar tufayli biznes uchun barcha oqibatlarni har tomonlama baholash, shuningdek, ularga qarshi choralar ishlab chiqish imkonini beradi. CRAMM axborot xavfsizligi sohasidagi xavflarni tahlil qilishning birinchi usullaridan biridir. U ustida ish 80-yillarning o'rtalarida Buyuk Britaniyaning Markaziy Kompyuter va Telekommunikatsiyalar Agentligi (CCTA) tomonidan boshlangan.

OCTAVE metodologiyasi AQShda Karnegi Mellon dasturiy ta'minot institutida ishlab chiqilgan. CRAMM metodologiyasi Buyuk Britaniyada Markaziy Kompyuter va Telekommunikatsiyalar Agentligi (CCTA)12 tomonidan ishlab chiqilgan.

Ushbu metodologiyalar dunyoning ko'plab mamlakatlarida tashkilotlarda axborot xavfsizligi xavflarini baholash uchun qo'llaniladi. Biroq, men ushbu metodologiyalardan foydalanadigan muayyan mamlakatlar haqida ma'lumot topa olmadim.

OCTAVE xavf modeli. Ushbu modelning mohiyati shundan iboratki, xavflarni tahlil qilish jarayoni tashqi tashkilotlar maslahatchilari yordamisiz faqat korxona xodimlari tomonidan amalga oshiriladi. Buning uchun ham texnik mutaxassislar, ham barcha darajadagi menejerlarni o'z ichiga olgan aralash guruh yaratish kerak. Bu axborot xavfsizligi bo‘yicha yuzaga kelishi mumkin bo‘lgan hodisalar tufayli biznes uchun barcha oqibatlarni har tomonlama baholash, shuningdek, ularga qarshi choralar ishlab chiqish imkonini beradi. Ushbu usul tahlilning 3 bosqichini taklif qiladi:

1) aktiv bilan bog'liq bo'lgan tahdidlar profilini ishlab chiqish;
2) infratuzilmaning zaif tomonlarini aniqlash;
3) xavfsizlik strategiyasi va rejalarini ishlab chiqish.

CRAMM xavf modeli. Ushbu model tahlilning sifat va miqdoriy usullarini o'zida mujassam etgan xavfni baholashning kompleks yondashuviga asoslanadi. Ushbu model ko'p qirrali va yirik va kichik korxonalar, davlat va tijorat sektorlari uchun mos keladi. CRAMM dasturiy ta'minot mahsulotlarining versiyalari turli turdagi korxonalarga mo'ljallangan va ularning bilim bazalari bilan farqlanadi. Ushbu model yordamida tizimlarning axborot xavfsizligini tahlil qilish uch bosqichda amalga oshiriladi.

Dasturiy ta'minot va ma'lumotlarning qiymati quyidagi holatlarda aniqlanadi:

1) istalgan vaqt davomida resursning mavjud emasligi;
2) oxirgi zaxira nusxasidan keyin olingan ma'lumotlarning yo'qolishi yoki to'liq yo'q qilinishi;
3) ruxsatsiz shaxslar yoki xodimlar tomonidan ruxsatsiz kirish vaqtida maxfiylikni buzish;
4) modifikatsiya (ma'lumot kiritish bilan bog'liq kichik xatolar, dasturiy ta'minotdagi xatolar uchun ko'rib chiqiladi)
5) ma'lumotni uzatish bilan bog'liq xatolar (bu etkazib berishni rad etish, noto'g'ri adresatga etkazib berish, ma'lumotni etkazib bermaslik).

Tayanch iboralar:

Axborot xavfsizligi, raqamli xavf, risk, moliyaviy risk, raqamli ob’ektlar, raqamlashtirish riski, risk menejment, riskni baholash, baholash metodlari, CRAMM usuli, OCTAVE usuli.

Nazorat va muxokama uchun savollar

1. Axborot xafsizligi tushunchasi
2. Raqamlashtirish sharoitida axborot xafsizligi va uning axamiyati
3. Raqamli xavf va uni boshqarish
4. Raqamlashtirish sharoitida banklarning moliyaviy jinoyatlar xavfiga qarshi kurashish strategiyasi
5. Raqamli to‘lovlar sohasida moliyaviy jinoyatlar xavflarini boshqarish usullari
6. **Axborot tizimi sharoitida tartibga soluvchi raqamli texnologiyalar**
7. Raqamli ob’ektlarga nimalar kiradi.
8. Moliya sohasida xavf-xatarlarni boshqarishning jaxon tajribasi.
9. OCTAVE axborot xavfsizligi sohasidagi xavflarni tahlil etishning mohiyati
10. CRAMM xavfni boshqarish modeli.

Foydalanilgan adabiyotlar

1. Абдурахманова, М. М. (2021). Деньги и банки. [Darslik] Иктисодиёт.
2. Мардонова, А. Т. (2021). Пул ва банклар. [O'quv qo'llanma] СамДУ Нашри.

Internet saitlar

3. Mikkelsen, D., Rajdev, S., & Stergiou, V. (2022). Financial crime risk management in digital payments. McKinsey. [28.05.2023] Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments
4. Ganguly, S., Harreis, H., Margolis, B., & Rowshankish, K. (2017). Digital risk: Transforming risk management for the 2020s. [29.05.2023]. From https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s
5. Cybersecurity and Financial System Resilience Report. Report To Congress. September, 2021. [31.05.2023] from https://www.federalreserve.gov/publications/files/cybersecurity-report-202109.pdf
6. Разумников, С. (2014). Современные проблемы науки и образования. [31.05.2023] from https://science-education.ru/ru/article/view?id=12197