COURSE :
MONEY AND BANKS

FAN:
PUL VA BANKLAR

LECTURE №12

MA’RUZA №12

MODERN MONEY CIRCULATION RISK MANAGEMENT

ZAMONAVIY PUL MUOMALASIDA RISKLARNI BOSHQARISH

Lecturer: PhD Kh. Rakhimova

Maruzachi: PhD Kh. Rakhimova

REJA:

01

ITEM 01

Raqamlashtirish sharoitida axborot xafsizligi va uning axamiyati.

02

ITEM 02

Raqamlashgan sharoitida banklarning moliyaviy jinoyatlar xavfiga qarshi kurashish strategiyasi.

03

ITEM 03

Raqamli to‘lovlar sohasida moliyaviy jinoyatlar xavflarini boshqarish usullari.

04

ITEM 04

Moliya sohasida xavf-xatarlarni boshqarishning jaxon tajribasi

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 VA UNI BOSHKARISH TAMOYILLARI

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, ilg‘or tahlil (jumladan, mashinani o‘rganish va sun’iy intellekt), shuningdek, robototexnikani interfeyslarga qo‘llash qo‘llaniladi. Asosan, raqamli xavf jarayonlarni, ma'lumotlarni, tahliliy va IT-ni hamda umumiy tashkiliy tuzilmani ma’lum talablarga muvofik sozlashni nazarda tutadi.

Axborot xavfsizligining asosi axborotni himoya qilish faoliyati - uning maxfiyligi, saqlangan holda foydalanish hamda yaxlitligini ta'minlash.
Salbiy vaziyatda murosaga yo'l qo'ymaslik muximdir [5]. Bunday holatlarga tabiiy, texnogen va ijtimoiy ofatlar, kompyuterning ishdan chiqishi, jismoniy o'g'irlash va boshqalar kiradi.

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

Axborot Xavfsizligini axamiyati

- 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.

- 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.

AXBOROT HAFSIZLIGINI NOMOYON BO’LISHI

Axborot xavfsizligiga tahdid etish ko’rinishlari

- Zararli dasturlar (viruslar, troyanlar va boshkalar);
- Fishing;
- Identifikatorni o'g'irlanishi;
- Tisimlarni buzish orqali axborotlarni o’qirlash.

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.

TARTIBGA SOLUVCHI RAQAMLI TEXNOLOGIYALAR

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

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.

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

Raqamli ob'ektlar

- **Moliyaviy**
- **Nomoliyaviy**

Raqamli ob'ektlar

- **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**

Source:ID 131299032
© Taras Gavryliuk | Dreamstime.com

- aqlli shartnomalar orqali to'lov xavfsizligini ta’minlanadi;
- operatsiyalarni optimallashtirish va yaxlitligi ochiq dasturlash orqali amalga oshiriladi;
- uzoq muddatli munosabatlar xotira bazasi (to'liq bitimlar tarixi);

12.2. Raqamlashgan sharoitida banklarning moliyaviy jinoyatlar xavfiga qarshi kurashish strategiyasi

So'nggi o'n yil ichida jismoniy elektron tijorat savdogarlarini kenqaib borishi. Shimoliy Amerika va Evropada elektron to'lovlar juda tez kengaymoqda, bu esa, mintaqalarda YaIMni o'sishiga ta'sir etmoqda.

Osiyoda bu tendensiya yanada tezroq. Elektron tranzaktsiyalar sonining oshishi elektron tijorat va mobil-tijorat evasiga naqd to'lovlardan voz kechishiga undamoqda.

Raqamli to'lov mexanizmlari | raqamli kartalar, raqamli hamyonlar va boshka to'lov tizim va vositalar

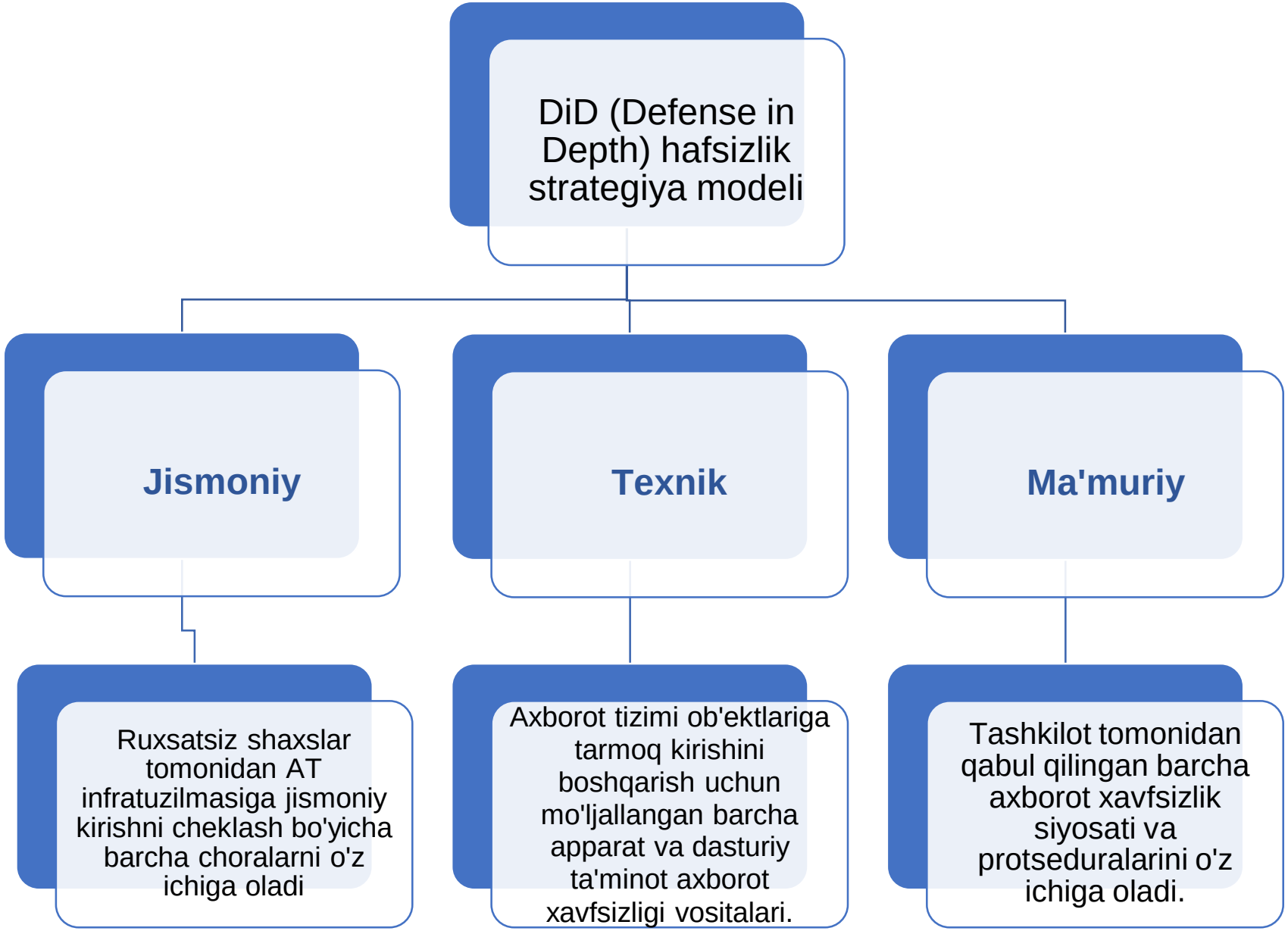
Birlashgan Millatlar Tashkilotining Giyohvand moddalar va jinoyatchilik bo'yicha boshqarmasining xabar berishicha, pul yuvish qiymatini hisoblash juda qiyin, ammo bu miqdorlar juda katta va o'sib borayotganini ta'kidlaydi, bu esa jahon yalpi ichki mahsulotining 5 foiziga yoki yiliga 800 milliard dollardan 2 trillion dollargacha yetadi (Mikkelsen, Rajdev & Stergiou, 2022).

To'lov xizmatlarini ko'rsatuvchi provayderlar (PSP) moliyaviy jinoyatlar xavfining oshishiga sabab bolmoqda. 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.

Banklar **DiD (Defense in Depth)** xavfsizlik modelidan foydalanishini kuzatish mumkin.

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,Texnik, Ma'muriy.**



DiD chuqur mudofaa kontseptsiyasi infratuzilma mudofaa tashkilotini uchta boshqariladigan qismga ajratdik va ular **quidagi qo’rinishda namoyon bo’ladi**:

Jismoniy: Masalan, ofis qo'riqchisi, kirishni boshqarish tizimlari, CCTV kameralari, signalizatsiya, qulflangan telekommunikatsiya kabinetlari va boshqalar.

Texnik: 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: 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.

Xatarlarni boshqarishning raqamli strategiyaning mohiyati

Bank sektoridagi xatarlarni boshqarishning raqamli strategiyasi jarayonlarni avtomatlashtirish, qarorlarni avtomatlashtirish va raqamli monitoring va erta ogohlantirishni o’z ichiga oladi.

Ushbu strategiyada 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 oshishi xavf funktsiyasiga ham e’tiborni oshishiga asos bo’ldi. Raqamli iqtisodiyot sharoitida tavakkalchilikdagi raqamli o'zgarishlarni samaradorlik va tavakkalchilik qarorlarining sifatini oshirish orqali haqiqiy biznesni yaratish mumkin bo’ladi.

Biznesda 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 havflarini boshqarishning ahamiyatini o’sib bo’rishi

Moliyaviy jinoyatlar bo‘yicha xalqaro standartlarni belgilovchi yetakchi organ – Moliyaviy harakatlar bo’icha xalqaro ishchi 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 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) talablari (masalan, shaxsni tekshirish) va tranzaksiyalarni doimiy monitoring qilish. Moliyaviy jinoyatlarga qarshi 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. Shu bilan birga o'sib borayotgan kompaniyalarning salohiyati va mijozlar tajribasi operatsion risklarni aniqlash va boshqarish qobiliyatini kengaytiradi.

Moliyaviy jinoyatlar havflarini boshqarishning ahamiyatini o’sib bo’rishi

Moliyaviy jinoyatlar PSPlar uchun katta xavf tug’diradi. Keng miqyosda ekvayring xizmatlarini taklif qiluvchi PSP'lar noqonuniy manbalardan olingan daromadlarni yuvish uchun ushbu xizmatlardan jinoyatchilar foydalanishi mumkin.

Uzluksiz KYC jarayonlarining etarli tashkil etilmaganligi pul yuvish vositalarini jalb qilishi provayderning obro'siga putur etkazishi mumkin.

Xuddi shunday, PSPlar turli tashkilotlarga va ulardan pul mablag'larini o'tkazishni osonlashtirgani uchun, ular sanktsiydagi 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’ yoki moliyaviy jinoyat xavfiga duchor bo'ladi.

Tahdidga qarshi turish uchun PSPlar ushbu birjalarning moliyaviy jinoyatlarga qarshi kurash tizimini tushunishlari kerak.

Moliyaviy jinoyatlar havflarini boshqarishda jahon tajribasi

Raqamli to'lov platformalarini boshqarishdagi zaif tomonlar tartibga solishning kuchayishiga olib kelishi mumkin. Bu sohada yaxshi tan olingan 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 PSP har tomonlama firibgarlik va mijozlarni himoya qilishga e'tiborni kuchaytirdi.

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 tasdiqlashini ko’zda tutadi.

Moliyaviy jinoyatlar havflarini boshqarishda jahon tajribasi

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.

Yevropa Ittifoqi darajasidagi Pul yuvishga qarshi kurashish 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.

Moliyaviy jinoyatlar havflarini boshqarishda jahon tajribasi

AMLA texnologik innovatsiyalar bilan bog'liq yangi va paydo bo'layotgan muammolarni hisobga olgan holda moliyaviy jinoyatlar bo'yicha mavjud Yevropa Ittifoqi tizimini "yaxshilaydi".

Yevropa Ittifoqi tizimlari

- virtual valyutalar
- yagona bozorda yanada integratsiyalashgan moliyaviy oqimlar
- ayrim taqiqlangan tashkilotlarning global ta'sir doirasi

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.

Moliyaviy jinoyatlar havflarini boshqarishda jahon tajribasi

Qo'shma Shtatlarda joriy tartibga soluvchi asosiy e'tibor litsenziyalangan pul o'tkazgichlariga qaratilgan.

Moliyaviy jinoyatlarga rioya qilish yukini faqat banklar o'z zimmasiga olmaydi, balki Moliyaviy jinoyatlarga qarshi kurash tarmog'i (FinCEN) va depozitlarni sug'urtalash bo'yicha federal korporatsiya (FDIC) ham oladi

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'lish imkonini kiritdi.

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.

Moliyaviy jinoyatlar havflarini boshqarishda jahon tajribasi

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 PSP 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.

Source : https://ru.depositphotos.com/279993104/stock-illustration-hacker-typography-banner.htm

Moliyaviy-jinoyat risklarini boshqarishning nazorat mexanizmlari biznes modeli, mijozlar va PSPl.arning ichki operatsiyalariga ta'sir qiladi.

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. 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.

Source: https://ru.freepik.com/free-photos-vectors/cyber-attacks/8

Source: https://www.linkedin.com/pulse/protect-your-business-from-social-engineering-schemes-matt/

To‘lov xizmati provayderlari (PSP) moliyaviy jinoyatlar xavfini boshqarishda uchta asosiy dizayn tamoyilini qo‘llashi mumkin:

moliyaviy jinoyatlar xavfini boshqarishda uchta asosiy dizayn

- mutanosib asos yaratish,
- an’anaviy nazorat muhitiga moslashish
- proaktiv ta’sir ko‘rsatish

Source: https://uzsoft.uz/moshennichestvo-novyj-vitok/

Moliyaviy jinoyatlar xavfini boshqarishda uchta asosiy dizayn

1. ***Mutanosib asos 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 moslashish.***

. 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. ***Proaktiv ta’sir ko‘rsatish.*** PSPlar tartibga solish talablariga 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.

To'lov vositachilari bilan ishlashda xavflarni baholash

To'lov vositachilari bilan ishlashda xavflarni baholash

Bu ularning roli, mijozlari va biznes modellari va tranzaktsiyalarini tahlil qilishni o'z ichiga oladi.

Ushbu ma'lumotlar xavf darajasini aniqlashga yordam beradi.

Ushbu ma'lumotni yangilab turish muhimdir.

To'lov vositachilari potentsial xavfli operatsiyalar va mijozlarga ko'proq e'tibor berishlari kerak.

Buning uchun siz zamonaviy ma'lumotlardan foydalanishingiz va segmentatsiya modellarini ishlab chiqishingiz kerak.

Bu samarasiz yondashuvlardan qochish va xavflarni yaxshiroq boshqarishga yordam beradi.

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

Moliyaviy risklarni boshqarish

- Moliyaviy risklarni baholashning an'anaviy modellari eskirgan
- Qabul qilingan moliyaviy risklarning qiymatini aniqlash va adolatli kompensatsiyani nazorat qilish
- Chet el amaliyotida moliyaviy risklarni boshqarishning turli standartlari
- Xalqaro banklar Bazel kelishuvlariga amal qiladilar
- kiberxavfsizlikni kuchaytirish bo'yicha chora-tadbirlar
- Moliyaviy xizmatlar sektori uchun "Kiberxavfsizlik profili"

Moliyaviy risklarni boshqarish

Moliyaviy risklarni boshqarish qabul qilingan moliyaviy risklar qiymatini aniqlash va iqtisodiy faoliyat natijasida yuzaga kelgan risklar uchun adolatli kompensatsiyani nazorat qilishni o'z ichiga oladi.

- Jahon iqtisodiyoti XXI asrda yangi raqamli shaklga ega bo‘ldi
- Innovatsion biznes yo'nalishlari va yuqori texnologiyali innovatsion loyihalarning paydo bo'lishi
- Qabul qilingan moliyaviy tavakkalchiliklar narxini aniqlash va adolatli kompensatsiyani nazorat qilish
- xorijiy amaliyotda moliyaviy risklarni boshqarishning turli standartlari
- Xalqaro faol banklar Bazel kelishuvlariga amal qiladilar

Tahdidlar va zaifliklarni baholash metodologiyalari

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation - Operatsion jihatdan muhim tahdid, aktiv va zaiflikni baholash);

- CRAMM (CCTA Risk Analysis and Management Method - risklarni tahlil qilish va boshqarish usuli)
- Tashkilotlarda axborot risklarini tahlil qilish va boshqarish uchun foydalaniladi

- OCTAVE: xavf tahlili faqat kompaniya xodimlari tomonidan tashqi maslahatchilar yordamisiz amalga oshiriladi

- CRAMM: axborot xavfini tahlil qilishning birinchi usullaridan biri

OCTAVE (Operatsion jihatdan muhim tahdid, aktiv va zaiflikni baholash)

OCTAVE

- AQShdagi Karnegi Mellon dasturiy ta'minot institutida ishlab chiqilgan
- Xatarlarni tahlil qilish faqat kompaniya xodimlari tomonidan tashqi maslahatchilar yordamisiz amalga oshiriladi
- Barcha darajadagi texnik mutaxassislar va menejerlarning aralash jamoasini yaratish talab etiladi
- Axborot risklari bilan bog'liq biznes uchun barcha oqibatlarni har tomonlama baholash imkonini beradi
- Qarshi choralarni ishlab chiqishga imkon beradi

CRAMM (CCTA risklarni tahlil qilish va boshqarish usuli)

CRAMM

- Axborot xavfini tahlil qilishning birinchi usullaridan biri
- 1980-yillarning o'rtalarida Buyuk Britaniya Markaziy Kompyuter va Telekommunikatsiya tizimlari agentligi (CCTA) tomonidan ishlab chiqilgan.
- Tashkilotlarda axborot risklarini tahlil qilish uchun foydalaniladi
- Axborot xavfini baholashga kompleks yondashuv asosida
- Katta va kichik kompaniyalar, davlat va tijorat sektorlari uchun javob beradi

XAVF TAHLILINING BOSQICHLARI

OCTAVE
xavf tahlilining
3 bosqichi

- Obyektga tahdid profilini yaratish
- Infratuzilmaning zaif tomonlarini aniqlash
- Xavfsizlik strategiyasi va rejalarini ishlab chiqish

CRAMM:
xavf tahlilining
3 bosqichi

- Dasturiy ta'minot va ma'lumotlarning qiymatini aniqlash
- Axborot xavfsizligi tahdidlarini baholash
- Xavfsizlik strategiyasi va rejalarini ishlab chiqish

Source: https://www.pngwing.com/ru/free-png-bhioz

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.
3. **Internet saitlar**
4. 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
5. 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
6. 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
7. Разумников, С. (2014). Современные проблемы науки и образования. [31.05.2023] from https://science-education.ru/ru/article/view?id=12197

E’TIBORINGIZ UCHUN RAXMAT!!!