MUNI
ECON

Nelegální činnosti v bankovnictví, praní špinavých peněz

Obsah

- Nelegální činnosti v bankovnictví
  - Pachatel mimo banku
  - Pachatel uvnitř banky
  - Kyberkriminalita
  - Počítačové bankovní krádeže
  - Insider trading
- Praní špinavých peněz
- Mezinárodní spolupráce

Nelegální činnosti v bankovnictví

- Změna postavení bank na trhu
- Změna způsobu získávání klientů
- Forma komunikace bank s klienty
- Rostoucí podíl mimobilančních aktivit bank
- Rozvoj elektronického bankovnictví

→ zpronevěry, loupeže, krádeže, podvody, korupce, insider trading a praní špinavých peněz.

Charakteristika finančních podvodníků

- Velcí finanční podvodníci – neustále na cestách, zpravidla pocházejí z angloamerického světa, většina bezstrestní občané, muži ve věku 50 – 60 let.
- Sídlo – kanceláře v nejvyšších patrech mrakodrapů, luxusní hotely.
- Účastní se různých setkání za účelem dojednání velkých bankovních transakcí (trustů).

Pachatel je mimo banku :

- **Podvodné žádosti o úvěr**
- Klient-podvodník žádá o úvěr a snaží se zastřít svoji finanční historii, používá falešné či pozměněné údaje o sobě, aby nebylo možné zjistit jeho nesplacené úvěry u jiných bank. Následné poskytnutí úvěru a předlužení pak vede k nevyhnutelnému bankrotu podniku či platební neschopnosti klienta.
- **Převody peněz na základě falešných dokumentů**
- Předložením falešného příkazu k úhradě z účtu bez tušení klienta odejde platba do vzdálené banky ve vzdálené zemi, kde jsou peníze vybrány, účet uzavřen a pachatelé zmizí.
- **Falešné směnky, falešné bankovní garance**

Pachatel je mimo banku :

- **Mezinárodní podvody – zneužití jména banky a banky bez licence**
- Krátkodobě existující banky, které nemají bankovní licenci a snaží se předstírat, že jsou renomovanou bankovní institucí.
- Například v roce 2002 se v USA objevil subjekt s názvem Chase Trust Bank, jehož název se snažil napodobovat tehdy existující velkou banku Chase Manhattan Bank. Tato banka bez licence pak podnikala za hranicí zákona.
- **Vylákání údajů o klientovi přímo od klienta**
- prostřednictvím podvodných e-mailů, tvářících se jako e-maily a zobrazení stránky banky nebo jiné instituce (tzv. phishing)

Pachatel je mimo banku :

- **Podvody s investováním**
  - Nabídka výhodného investování, alokace finančních prostředků. Jde o falešné nabídky neuvěřitelně výhodného zhodnocení peněz, které nikdo jiný nenabízí. Může jít o varianty pyramidových her nebo jiná schémata.
  - Investiční hry
- **Nabídka daňových úniků, neúměrného zhodnocení nebo zúročení kapitálu**
- **Fiktivní převody FP**
- **Nabídka koupě CP, výhodné burzovní spekulace, finanční účasti**
- **Útok hrubou silou**

Příklad phisingu

MUNI ECON

Průvodní e-mail

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s fraudem. Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu.

Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.

V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.

Průvodní e-mail

V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti. Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.
Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred fraudem.

Závěr

- Nikdy nesdělujte osobní údaje, hesla či kódy PIN formou e-mailu.
- Banka od klientů nikdy nevyžaduje sdělení údajů touto formou!
- Banka nezasílá nevyžádané e-maily s odkazy na internetové adresy.
- V případě dalších otázek se můžete kdykoli obrátit, popř. můžete kontaktovat informační linku banky.

Podvody s platebními kartami

Oblast zahrnuje mnoho kriminálních aktivit:

- krádež platebních karet,
- kopírování karet tajným zařízením připojeným k bankomatu,
- krádež údajů na kartě a zaplacení cizí kartou na internetu.

Libanonská – ukrajinská smyčka

MUNI
ECON

Libanonská – ukrajinská smyčka

Způsob a technika realizace

- Kamera
- Magnetofonový pásek
- Tepelná folie pokrývající klávesnici
- Odezírání
- „Dobrá rada“

Libanonská – ukrajinská smyčka

- Podvodníci do štěrbiny, kam se zasouvá karta, nainstalovali čtečku.

- Pro zjištění PIN kódu nepoužili jako obvykle mikrokameru, ale klávesnici bankomatu polepili tepelnou fólií, která zaznamenávala dotyky prstů.

V neděli 14. května 2006 do bankomatu v pražské centrále ČSOB bylo instalováno zařízení, jež dokáže kopírovat platební karty. Takzvaný skimming trval téměř po celý den.

Pachatel uvnitř

Podvodné úvěry

- zapojeni zaměstnanci banky, kteří poskytnou či napomohou poskytnutí úvěru spřízněné společnosti, nebo jednotlivci
- dotyčná společnost nedlouho poté vyhlásí bankrot
- banka přijde o půjčené peníze a podvodník zevnitř banky i jeho komplicové zvenku se podělí o kořist

Nadměrně rizikové obchody – krytí ztrát

- Obchodník-zaměstnanec překračuje limity banky pro spekulativní obchody. Jakmile prodělá a hrozí mu odhalení, dělá další a další podobné nepovolené transakce jménem banky, kterými se snaží ztrátu nahradit.

Pachatel uvnitř

Padělání dokumentů po krádeži

- Krádež finančních prostředků v bance by mohla být odhalena při kontrole účetnictví.
- Pachatel zevnitř nebo vně banky padělá dokumenty, které dají účetní stránku zmizelých peněz naoko "do pořádku".
- Krádež pak vypadá, jakoby peníze byly poskytnuty někomu ve formě úvěru, vybrány vkladatelem nebo převedeny či investovány.

Krádeže identity

- Zaměstnanci banky prodají nebo předají osobám zvenčí údaje o klientech banky, jejich účtech a dalších údajích.

Padělání bankovek a mincí (legálních platidel)

Prevence podvodů vlastních pracovníků

- Vytvoření bezpečnostního prostředí banky
- Školení bezpečnostní politiky banky a vzdělávání zaměstnanců
- Bezpečnostní politika banky
- Vytvoření a udržování firemní kultury

Kyberkriminalita

- soubor trestných činů, které jsou páchané prostřednictvím počítačů nebo jejichž cílem jsou počítače.
- Nejedná se o nové trestné činy, které by výpočetní technika přinášela, ale jedná se o nový způsob jejich provedení, pomocí informačních technologií. Zejména jde o sabotáže, krádeže, neoprávněné užití cizí věci, vydírání a špionáž.
- **Prolomení systému**
- S digitalizací veškerých dat a veškerých postupů je možné získáním nadvlády nad systémem udělat téměř cokoliv. Prolomení systému může probíhat různými postupy

Kyberkriminalita

- **Útok hrubou silou**
- Neznamená útok pomocí kladiva, nýbrž pomocí speciálně navrženého softwaru, který se snaží na základě zkoušení všech možných kombinací uhodnout heslo k danému systému. Útok hrubou silou je limitován sílou hesla k danému systému, což znamená při současném výkonu počítačů, že heslo musí mít minimálně 8 znaků.
- **Slovníkový útok**
- Zde se jedná o útok na heslo, způsobem kdy se použijí slovníky všech dostupných jazyků a zkouší se jednotlivá slova, tak aby došlo k prolomení hesla.

Kyberkriminalita

- **Odposlech síťové komunikace**
- software sledující vaší práci s počítačem a v okamžiku, kdy se přihlašujete do zabezpečeného systému tak čte znaky, které vyťukáváte do klávesnice. Příkladným způsobem jak tento druh získání vašeho hesla omezit je využívání zabezpečených stránek, které jsou šifrovány a jejichž napadení je složitější.
- **Využití neukončeného spojení**
- Neodhlášení se např. z internetového bankovnictví. K této na první pohled malicherné chybě může dojít i v souvislosti s bankovním systémem. Jedná se o zcela zásadní pochybení, kterého mohou pachatele využít. Některé stránky mají ochranu formou automatického ukončování při nečinnosti, což bývá zpravidla 15 minut.

Kyberkriminalita

- **Zadní vrátka**
- Pro hackera není problém napsat program, který mu umožní vstup do daného systému, pomocí tzv. zadních vrátek, díky kterým nepotřebuje ani uživatelské jméno ani heslo. Tento program pak do počítače uživatele dostane pomocí viru, zpravidla jím bývá trojský kůň nebo počítačový červ.

Počítačové bankovní krádeže

- **Phishing**
- **Pharming**
- Jedná se o specifický způsob získávání citlivých údajů, kterému předchází napadení DNS a přepsání IP adresy počítače uživatele. Což způsobí, že při zadání webové stránky pro přihlášení do internetbanky je přepsána URL a uživatel je přesměrován na falešnou stránku vytvořenou pachatelem. Jedná se o téměř identické stránky, které jsou k nerozeznání od skutečných stránek dané banky.

Insider trading

- Termín „insider obchody“ je velice frekventovaný a je většinou znám všem ekonomům i subjektům spojeným s bankovní a obecně s podnikatelskou činností.
- Obchody a smlouvy, při kterých jsou využívány (resp. zneužity) ostatním subjektům nedostupné informace, kdy dochází k manipulování trhem či k nedostatečné ochraně investorů.
- **Insider obchody jsou téměř výlučně spojeny s nákupem a prodejem cenných papírů.**
- Jen výjimečně k nim dochází i při jiných finančních a bankovních, resp. smluvních aktivitách, např. při poskytování úvěrů v bankách nebo při úniku důvěrných informací z vládních zdrojů či institucí veřejné správy.
- Zářným příkladem zneužití neveřejných informací je nakoupení cenných papírů při nízkém kurzu následované markantním nárůstem kurzu, který vzroste na základě zveřejnění důležité informace nebo opačně.

Praní špinavých peněz

- Nebo-li legalizace výnosů z trestné činnosti - úmyslné jednání, které zakrývá nezákonný původ jakéhokoli výnosu z trestné činnosti a které se současně snaží vzbudit zdání, že se jedná o příjem nebo o majetek, získaný v souladu s platnými zákony.

Legislativa

- **Zákon č. 253/2008 o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu**
  - Zákon zapracovává příslušné předpisy Evropských společenství a upravuje oblast problematiky legalizace výnosů z trestné činnosti a financování terorismu. Účelem je zabránění zneužití finančního systému k praní špinavých peněz. Zákon vstoupil v účinnost dne 01.09.2008.
- **Zákon č. 69/2006 Sb. o provádění mezinárodních sankcí**
  - Tento zákon upravuje některé povinnosti fyzických a právnických osob, při uskutečňování mezinárodních sankcí za účelem udržení nebo obnovení mezinárodního míru a bezpečnosti, ochrany základních lidských práv a boje proti terorismu.
- **Vyhláška ČNB č. 281/2008 Sb. o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu**

Zdroje výnosů z trestné činnosti

- obchod s nelegálními zbraněmi všeho druhu,
- obchod s drogami,
- obchod s „bílým masem“ a lidskými orgány,
- pašování a obchod s kradeným zbožím,
- padělání a obchod se značkovým zbožím,
- provozování nelegálních skládek odpadu,
- porušování autorských práv,
- padělání osobních dokladů a zkreslování účetnictví,
- daňové podvody a celní úniky,
- padělání bankovek, mincí, cenin, šeků a cestovních šeků,
- podvody s bankovními produkty a finančními instrumenty,
- insider trading a pojišťovací podvody,
- lichva a hospodářská kriminalita,
- počítačová trestná činnost,
- hazardní hry, sázky,
- únosy atp.

Fáze praní špinavých peněz

- **Placement – umístění**
- Cíl: Dostat peníze do místního finančního systému (platby na konta, využívání finančních tržních instrumentů).
- **Layering - rozdrobení peněz**
- Zametání stop, umísťování peněz kriminálně získaných do finančních systémů po celém světě.
- **Integration**
- navrácení kriminálně získaného a nyní již vypraného jmění zpět do normálního ekonomického oběhu

Metody praní špinavých peněz

- utajování neboli ukrývání výnosů z trestné činnosti uvnitř legálních obchodních struktur,
- zneužívání legitimních obchodů,
- používání falešné totožnosti (neboli falešných nebo odcizených osobních dokladů), resp. nastrčených osob (tzv. „bílých koní“),
- využívání různých právních řádů v různých zemích a/nebo
- používání anonymního majetku.

Boj bank proti legalizaci výnosů z trestné činnosti

Systém vnitřních zásad

- v kompetenci nejvyššího vedení banky, jejím úkolem je definování potencionálních rizik a odhad ztrát z nich vznikajících. Jedná se o rizika související se zneužitím produktů a služeb banky teroristickými a zločineckými skupinami.
- V reálu to znamená shromažďování veškerých informací o jednotlivých klientech a jejich transakcích, kde je archivována i jejich četnost a objemy.

Boj bank proti legalizaci výnosů z trestné činnosti

Poznej svého klienta

- U každého klienta musí být provedena legitimace, tedy kontrola klienta fyzicky s jeho doklady totožnosti, jejich zanesení do spisu klienta a samozřejmě nutnost vytvoření podpisového vzoru.
- Klient je sledován a jeho návyky a veškeré transakce, včetně jednotlivých produktů, které využívá, jsou pečlivě zaznamenány a případné odchylky od normálu jsou brány jako podezřelé a následně jsou i prověřeny.

Jak poznat podezřelého klienta – právnické osoby

- Především subjekty obchodující se zeměmi třetího světa, zejména se zeměmi, na něž jsou uvaleny mezinárodní sankce,
- subjekty s nepřehlednou vlastnickou strukturou, kde jsou vlastníky společnosti třeba i jiné právnické osoby,
- nejasný původ finančních prostředků,
- podezřelost sídla společnosti,
- neseriózност statutárního zástupce/ů,
- podezřelost obchodů prováděných společníky,
- zmocňování třetích osob k jednání s bankou,
- podezřelé názvy subjektu (lehce zaměnitelné za lukrativní společnosti a značky),
- negativní reklama v médiích,
- obranné chování při konkrétním dotazování na obchodní aktivity.

Jak poznat podezřelého klienta – fyzické osoby

- občan odmítá svou identifikaci,
- figurují ve výkonných orgánech mnoha PO,
- nejasný původ finančních prostředků,
- předkládají falešné dokumenty nebo informace,
- snaha o uplácení bankovních úředníků,
- snaha o urychlení bankovního procesu,
- jsou ovládáni třetí osobou,
- objemné transakce brzy po uzavření smlouvy.

Podezřelé obchody

Podezřelým je obchod vždy, pokud:

- klientem nebo skutečným majitelem je osoba, vůči které Česká republika uplatňuje mezinárodní sankce podle zvláštního zákona,
- předmětem obchodu je nebo má být zboží nebo služby, vůči nimž Česká republika uplatňuje sankce podle zvláštního zákona,
- klient se odmítá podrobit kontrole nebo odmítá uvést identifikační údaje osoby, za kterou jedná.

Za podezřelý obchod se považuje vždy obchod, u kterého je detekován některý z rizikových faktorů, nebo v případech, kdy klient předkládá v rámci požadovaného obchodu nebo poskytnutí služby podklady popř. sděluje informace, obsahující skutečnosti, které by mohly nasvědčovat podezřelému obchodu (např. proplacení faktury v ekvivalentu přesahujícím v přepočtu aktuálního kurzu české koruny částku 15.000 EUR), nebo pokud finanční instituce obdrží informaci o rizikovém faktoru od jiné banky nebo finanční instituce nebo z obecně dostupných informačních zdrojů.

Monitorování a vyhodnocení podezřelých obchodů

– Podezřelé obchody jsou identifikovány na základě výběru systémového a systematického monitorování znaků podezřelých obchodů.

Interní oznámení o možném podezřelém obchodu

– zaměstnanec, který na základě zjištění či jiné informace identifikuje znak podezřelého obchodu či jakoukoliv jinou skutečnost, která by mohla nasvědčovat podezřelému obchodu, zašle neprodleně kontaktní osobě interní oznámení podezřelého obchodu, a to písemně prostřednictvím vyplněného formuláře „Interní hlášení podezřelého obchodu“ nebo formou e-mailu.

Monitorování a vyhodnocení podezřelých obchodů

Obsah interního oznámení

- přesné a úplné identifikační údaje týkající se účastníků obchodu,
- úplné vylíčení skutkového děje, ve kterém je spatřován podezřelý obchod,
- vyjádření, zda byl obchod proveden nebo odložen,
- přehled dalších účtů klienta vedených ve finanční instituci, případně u jiných bank, pokud jsou tyto skutečnosti zaměstnanci známy,
- veškeré další údaje a skutečnosti, které mohou jakkoliv přispět k posouzení věci,
- popis všech možných vazeb a dalších relevantních údajů, které jsou k dispozici.

Monitorování a vyhodnocení podezřelých obchodů

Postup při oznámení podezřelého obchodu

- posouzení znaků podezřelého obchodu,
- odeslání interního oznámení podezřelého obchodu kontaktní osobě,
- shromáždění veškerých relevantních a písemných podkladů k oznámení podezřelého obchodu, které v případě vyžádání odešle kontaktní osobě, případně na základě výzvy kontaktní osoby poskytne k věci doplňující informace nebo podklady.
- Kontaktní osoba na základě obdrženého oznámení o podezřelém obchodu, popřípadě na základě dalších vyžádaných informací rozhodne o tom, zda se jedná o podezřelý obchod podléhající oznámení MF.

Vyhodnocení podezřelých obchodů

Oznámení podezřelého obchodu MF

- Kontaktní osoba je v případě vyhodnocení obchodu jako podezřelého povinna učinit oznámení MF bez zbytečného odkladu, nejpozději do 3 pracovních dnů od zjištění obchodu. Hrozí-li nebezpečí z prodlení, či vyžadují-li to okolnosti případu, oznámí kontaktní osoba podezřelý obchod neprodleně po jeho zjištění.
- Odklad splnění příkazu klienta
- Odklad splnění příkazu klienta je nástrojem, jehož cílem je zabránit, aby výnos z trestné činnosti unikl mimo dosah orgánů činných v trestním řízení. O odkladu splnění příkazu klienta rozhoduje kontaktní osoba, a to v rámci pravidel stanovených zákonem.

Vyhodnocení podezřelých obchodů

Neuskutečnění obchodu – shrnutí

- Finanční instituce neuskuteční obchod za následujících podmínek:
- klient je pro finanční instituci nepřijatelným klientem dle Pravidel přijatelnosti,
- klient se odmítne podrobit identifikaci
- klient neposkytne požadovanou či potřebnou součinnost při kontrole, resp. neposkytne informace, které jsou k provedení kontroly nezbytné
- Finanční instituce nemůže z dalších důvodů provést identifikaci či kontrolu klienta
- příslušný zaměstnanec má pochybnosti o pravdivosti klientem poskytnutých informací nebo o pravosti předložených dokladů,
- klientem je politicky exponovaná osoba, přičemž kontaktní osoba neschválila obchod nebo finanční instituci není znám původ majetku užitého v obchodu.

Podezřelé obchody – depozitní účty

Podezření by mělo vyvolat následující ukazatele:

- více účtů zřizovaných pro jednoho klienta,
- převody, jejichž objem neodpovídá finanční situaci klienta,
- problémy s identifikací klienta,
- podezřelé transakce,
- jednání vysoce odlišné od jednání běžných klientů,
- omezovaní dispozičních práv společníků,
- udělení dispozičních práv osobám, které logicky nesouvisí s klientem,
- náhlé zaktivování nevyužívaného účtu vysokými transakcemi,
- klient obchoduje se zeměmi, které podporují terorismus,
- klient obchoduje se zeměmi, které nemají opatření proti praní špinavých peněz,
- klient je doprovázen třetí osobou.

Podezřelé obchody – bezhotovostní platební styk

- převody z/do daňových rájů,
- prokazatelné odůvodnění neobvyklé transakce,
- velké množství transakcí v krátkém časovém horizontu,
- převody částek neodpovídajících ekonomické situaci klienta,
- převody z/do zahraničí, jejichž účelem je dar, nebo úvěr,
- významné změny v zůstatku v krátkém čase,
- kulantně zaokrouhlené částky s předmětem „platba za zboží/služby“,
- netypické transakce a
- převody autorizované zmocněnou osobou.

Podezřelé obchody – hotovostní platební styk

- opakované vklady těsně pod úrovní limitu stanoveného zákonem č. 252/2004 Sb.,
- vklady z různých poboček bank na jeden účet klienta,
- počet hotovostních vkladů je neobvyklý danému klientovi,
- časté vklady v cizí měně a výběry v domácí,
- velké množství malých vkladů oproti malému množství velkých výběrů,
- transakce v neobvyklých měnách a neobvyklých objemech,
- vklady a následné převody vysokých částek do zahraničí.

Podezřelé obchody – bezpečnostní schránky

- pronajímání většího množství schránek,
- dispoziční práva k více schránkám,
- nevyužití jiných služeb banky,
- podezřelý (neupravený) vzhled klienta.

Podezřelé obchody – šeky a cestovní šeky

- pronajímání většího množství schránek,
- dispoziční práva k více schránkám,
- nevyužití jiných služeb banky,
- podezřelý (neupravený) vzhled klienta.

Podezřelé obchody – bankovní úvěry

- místěpříslušnost klienta k pobočce,
- přítomnost třetích osob při žádosti o úvěr,
- pozměněné nebo falešné podklady pro žádost o úvěr,
- ručitelský závazek osob nespjatých s klientem (bez prokazatelné motivace),
- předčasné splacení úvěru třetí osobou,
- záruka, jejíž původ je pochybný,
- splácení úvěru prostředky, u nichž může být podezření, že pochází z trestné činnosti,
- opakované nabírání a předčasné splácení úvěrů,
- využití prostředků v rozporu s účelem úvěru.

Podezřelé obchody – cenné papíry

- neobvyklé množství nebo druh CP,
- nezvyklé vypořádání obchodu na klientovu žádost,
- odlišnost cen obchodovaných cenných papírů oproti jejich cenám na běžném trhu,
- nákupy velkého množství CP nově emitovaných, nebo emitovaných společnostmi z daňových rájů,
- obchodování s CP, které jsou v seznamu odcizených nebo ztracených,
- neobvykle vysoké smluvní pokuty u opčních smluv,
- obchody, jejichž zprostředkovatelé jsou společnosti sídlící v daňových rájích.

Mezinárodní spolupráce

- harmonizace legislativy, pravidel a koordinace postupů v této oblasti napříč zeměmi.
- **Vídeňská úmluva 1988** - Úmluva OSN proti nelegálnímu obchodování s drogami a psychotropními látkami.
- Tato úmluva je „základním kamenem“ spolupráce mezi státy v této oblasti.
- **Deklarace principů Basilejského výboru 1988**, která bankám doporučuje dodržovat 4 základní procedury.
- Znát svého zákazníka
- Soulad s právním řádem,
- Spolupracovat se soudními orgány
- Dodržování Deklarace

Mezinárodní spolupráce

- **Financial Action Task Force (FATF)**
- „Skupina pro finanční úkoly“ je nezávislou skupinou devětadvaceti států a dvou organizací, která byla založena na ekonomickém summitu zemí skupiny G7 v roce 1989 v Paříži právě za účelem boje proti praní špinavých peněz.
- **Štrasburská úmluva**
- Štrasburská úmluva z roku 1990 vstoupila v platnost pro Českou republiku dne 1. března 1997. Tato úmluva má za úkol zlepšit opatření mezinárodní spolupráce proti mezinárodní organizované kriminalitě jako celku.
- Jeden z cílů úmluvy je usnadnit mezinárodní spolupráci ve vyšetřování, vyhledávání, zabavení a konfiskaci příjmů ze všech typů kriminality, zvláště ze závažné trestné činnosti jako prodej drog, obchodování se zbraněmi, obchodování s dětmi a mladými ženami a terorismus a další trestné činy, které vytvářejí velký zisk.