VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
FAKULTA INFORMATIKY A STATISTIKY
KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

Studijní program:	**Aplikovaná informatika**
Obor:	**Informační systémy a technologie**

Diplomant:	Bc. Michal Frühauf
Vedoucí diplomové práce:	prof. Ing. Václav Řepa, CSc.
Oponent diplomové práce:	Mgr. Jan Pálka

Business Activity Monitoring

školní rok 2001/2010

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých jsem čerpal.

V Praze dne 14. 12. 2009

.....

podpis

Poděkování

Rád bych na tomto místě poděkoval panu prof. Ing. Václavu Řepovi, CSc., vedoucímu diplomové práce, za jeho vstřícnost, trpělivost, věcné připomínky, čas, pomoc a důvěru mi věnovanou, což vše bylo nutnými podmínkami vzniku mé práce.

Rád bych také poděkoval za spolupráci a odborné konzultace i názory pracovníkům compliance.

Dále bych chtěl poděkovat přítelkyni za trpělivost, pomoc a podporu.

Abstrakt

Hlavní těžiště diplomové práce leží v oblasti podpory rozhodování podnikového managementu nasazením a využitím IT/ICT. Konkrétní popisovanou technologií je Business Activity Monitoring. Přínos práce leží především ve dvou rovinách.

První rovinou je vytvoření pokud možno co nejucelenějšího pohledu o BAM. Poznatky jsou sbírány z různých směrů a oblastí. První směr je zaměřen na vývoj Business Intelligence a popis vzniku BAM jako trendu BI, popis průběhu vývoje, prognózy do budoucna. Druhý směr se orientuje především na detailní vymezení BAM, jeho definování, předpoklady nasazení, základní modely, způsob činnosti BAM a jeho přínosy pro podnikání. Třetí směr vymezuje zařazení BAM mezi jiné/podobné podnikové technologie a řešení – BI a BSM a hledání klíčových odlišností.

Druhou rovinou práce je zpracování návrhu podpory AML v prostředí banky pomocí BAM. Jedná se o praktickou ukázku možnosti využití BAM v praxi. Základ návrhu řešení leží v analýze rizik vyplývajících ze zákona a současného stavu řešení. Zmapováním bankovních procesů a vyhledáním míst vzniku rizik je pak možné na tato rizika nasadit BAM nástroje pro jejich řízení. Návrh podpory leží převážně v konceptuální rovině.

Klíčová slova

Business Activity Monitoring, Business Intelligence, Business Service Management, událostmi řízené systémy, dashboard, AML, řízení rizik, compliance, bankovní systémy, bankovnictví

Abstract

Main focus of the thesis lies in the corporate management decision support deploying and using IT / ICT. Specific technology described is Business Activity Monitoring. The contribution of the work lies primarily in two planes.

The first plane is to create as far as the most comprehensive view of the BAM. The findings are collected from different directions and areas. The first direction of research is focused on the development of Business Intelligence and description of BAM as a trend of BI, including the stages of development and projections into the future. The second direction focuses primarily on a detailed circumscribe of BAM. Its definition, deployment assumptions, basic models, the way how business can benefit from BAM usage. The third guideline shows the classification of BAM surrounded by the other / similar technologies and business solutions – BI and BSM, and the search key differences.

The second level of the work is to support the AML implementation in a specific environment of banks using BAM. This is a practical demonstration of the possibility of using BAM in practice. Basic design solution lies in the analysis of risks arising from the law and the current state of the solution. By mapping of banking processes and searching for points of risk it is then possible to deploy these risks BAM tools for their management. Motion of support lies mainly in conceptual terms.

Key words

Business Activity Monitoring, Business Intelligence, Business Service Management, Event Driven Systems, Dashboard, AML, Risk Management, Compliance, Banking Systems, Banking

Obsah

1 Úvod

Žijeme v turbulentní době plné nenadálých změn, vysokého pracovního i životního tempa a nasazení. Nové trendy, myšlenky i technologie neustále a dynamicky mění naše okolí, náš svět, ve kterém žijeme. Chceme-li uspět a prosadit se v tomto světě, musíme se v tomto prostředí dobře orientovat a dokonale se mu přizpůsobit.

Ruku v ruce s tím, jak jsou na lidi kladeny vyšší nároky, zvyšují se i nároky kladené na podniky. Konkurence se přiostřuje mimo jiné díky rychlé globalizaci celosvětové ekonomiky.

Žádný podnik si dnes nemůže být prakticky jistý, že v následující chvíli se neobjeví nový jiný podnik, který osloví a přebere jeho zákazníky, a takový podnik může být klidně z opačného konce světa, nebo třeba ze sousedovy garáže. Nebo jiná varianta, že dodavatel náhle neuzavře exkluzivní smlouvu s konkurencí. Další případy bychom jistě našli celkem rychle.

Nejen rostoucí tlak konkurence nabádá podniky k ostražitosti, ale i rostoucí vliv regulačních orgánů a zvyšující se počet regulací zvenku zasahujících trh jistě na klidném spaní vedení nepřidá.

Byrokracii je zřejmě zbytečné obviňovat, ta si žije svým vlastním životem a jen stěží lze odhadovat, co *nového* přinese, avšak mezi faktory rostoucího konkurenčního boje na globálním trhu lze hledat rostoucí vliv informačních a komunikačních technologií. Jednou jsme si je k sobě připustili, často je využíváme *hloupě*, proč se tedy nepokusit nabídnout jim příležitost, aby pomohly najít lepší příležitosti našemu podnikání a skutečnou konkurenční výhodu.

1.1 Volba tématu

IT/ICT už leccos dokázaly a s ledasčím nám lidem pomohly, přesto však mají ještě dostatečný potenciál pomoci více. Pro podniky je těžké neustále generovat zisk, musejí proto neustále hledat nové příležitosti na trhu, získávat nové zákazníky, stávající vhodně třídit a dobře se o ně starat.

Všechno tohle obnáší přijímat správná rozhodnutí. Jen správná rozhodnutí mohou zajistit přežití podniku. Aby mohlo vedení správně rozhodovat, potřebuje mít správné podklady k rozhodnutí. Většinu těchto podkladů podniky mají – bezpečně uložených v databázích, ale jen málokterý manažer je dokáže využívat.

Problematikou *správného* rozhodování se v IT zabývá především BI a BAM. Každý podnik potřebuje vytvářet nejen strategie na úrovni top managementu, ale potřebuje vidět i do chodu sebe samotného. Mnoho úspor (ve výsledku především finančních), optimalizací a redukování chyb chodu podnikání lze hledat uvnitř podniků. Stačí jen mít správné nástroje – BAM.

Obzvláště ve velkých podnicích může BAM přispět k lepšímu komunikačnímu propojení mezi nejnižší a nejvyšší vrstvou řízení, neboť každý běžný pracovník může prostřednictvím BAM jasně vidět svoji roli v rámci celého podniku a jasně chápat svůj přínos pro podnik. Řídit je potřeba jak nahoře, tak dole. Rozhodnutí jsou přijímána nejen top vedením, ale i nejnižšími zaměstnanci. Správná interakce mezi rozhodováním napříč podnikem je nezbytná pro přijímání správných rozhodnutí.

Osobně si myslím, že BAM svůj potenciál teprve ukáže. V rámci podniku může poskytnout mnoho cenných informací. Navíc může zpřehlednit vnitropodnikové prostředí a jasně podchytit vazby na okolí podniku (zákazníci, dodavatelé, regulátoři).

BAM je sice mladý, ale v rámci podnikové IT se může na rozdíl od jiných technologií snáze chlubit jasným vyčíslením přínosů pro podnik a minimálně tohle by mohlo nejedno vedení zajímat.

1.2 Cíle práce

V rámci vyhotovení diplomové práce si stanovuji naplnění následujících cílů:

- Shrnout pohledy na BAM od vzniku až po současnost, s případným odhadem budoucího vývoje.
- Umístit BAM mezi ostatní informační technologie v podniku.
- Detailní popis BAM (definice, model, reakce, výrobci, přínosy,omezení aj.).
- Navrhnout koncept reálného použití BAM v bankovním prostředí při implementaci AML.

1.3 Omezení práce

Elektronické dokumenty, které slouží jako zdrojová literatura, jsou čerpány z bezplatně dostupných veřejných zdrojů, novin, časopisů a elektronických zdrojů VŠE. Vzhledem k potenciálně ziskové technologii v budoucnu, je spousta aktuálních analýz a odborných publikací výrazně zpoplatněna, a proto lze čerpat spíše z článků starších.

Při práci na návrhu využití BAM v bankovním sektoru je omezující moje nezkušenost v návrhu podobného systému, nedostupnost a utajení bankovních vnitřních dokumentů.

1.4 Přínos

Shrnutí a uspořádání dostupných informací o BAM v rámci představení BAM v souhrnném pohledu – pokud možno v co nejkomplexnějším vysvětlení všeho, o čem BAM je, co obnáší, co s sebou přináší a co naopak odnáší.

Praktická ukázka návrhu pro použití BAM v konkrétním případě užití (implementace AML – zákona č. 253/2008 Sb.).

1.5 Komu je práce určena

Práce je určena čtenáři aspoň mírně seznámenému s problematikou podnikových IS/ICT, který chce získat ucelený přehled o možnostech BAM a jeho významu v rámci podniku.

Může být zajímavá pro kohokoliv, kdo má na starosti podnikové IS/ICT a rád by dosáhl dalších lepších výsledků business procesů.

Výrobcům a dodavatelům BAM řešení, kteří by si chtěli rozšířit obzor o možnost rozšíření svého portfolia řešených o oblast AML a jeho podpory pomocí BAM.

Pracovníkům bank na oddělení compliance, kteří by se chtěli seznámit s možnostmi eliminací rizik spojených s AML prostřednictvím IS/ICT – BAM. Práce obsahuje i popis řešení běžným neIT jazykem.

2 Na počátku

Píše se červenec roku 2001 a společnost Gartner[1] představuje nový pojem, nový trend, nový koncept – záleží na úhlu pohledu. Svět se poprvé seznamuje s *Business Activity Monitoring (BAM)*[2] (Gassman, 2003). Tento nový trend však nevzniká z čista jasna, nýbrž vchází a je dalším pokračováním tou dobou již známějšího a zaběhnutějšího konceptu, který se nazývá *Business Intelligence (BI)*.

Není zcela běžné psát o jednom tématu (BAM) a přitom práci zahájit tématem úplně jiným (BI). Oba systémy mají leccos společného, neboť BAM vychází z BI, je nepochybně vhodné se nejprve rychle seznámit s BI a teprve potom plynule přejít k samotnému podrobnějšímu popisu BAM.

Jak píši dále, BAM není vyloženě podmnožinou BI a rozkládá se napříč více oblastmi. Rozhodně nelze psát o BAM a BI vynechat. Podle mě BAM s BI sdílí především základní myšlenkové pojetí a podobnou filozofii – podpora rozhodování, analýza dat. Na BAM není možné nahlížet odděleně. Vzhledem ke spojitostem s BI pocházejícím z minulosti a nepochybně pokračujícím i do budoucna je začnu nejdříve se seznámením s BI a poté teprve přejdu k samotnému BAM.

Možná i nabudete dojmu, že BI zmiňuji příliš detailně, avšak dle mého názoru jsou BI a BAM natolik spjaty, že nelze dnes říci, že BAM se od BI odtrhne a bude mít *svůj vlastní život*. Uvedu průřez historií, současností i několika možnými dalšími trendy v BI, neboť jak později zjistíte, existují situace, kdy si BI a BAM jsou totožné. Pokud bych měl použít matematické terminologie, pak o BI říkám, že BAM ohraničuje neostře shora.

2.1 Business Intelligence

V posledních letech jsme svědky celosvětových trendů, v jejichž důsledku se mění mimo jiné i chování podniků a organizací. Ekonomiky jednotlivých států jsou navzájem stále více provázané, konkurence roste a stává se globální. V důsledku těchto změn je pro podnik stále složitější generovat zisk.

Pokud mají podniky v tomto novém prostředí přežít, musí změnit způsob, jakým přijímají důležitá rozhodnutí. Jinými slovy jejich rozhodování musí být mnohem *inteligentnější* než dřív. Musí si dokázat odpovědět na otázky jako například na *jaké zákazníky se zaměřit a kterých zákazníků je třeba se zbavit; které produkty je pro nás výhodné vyrábět; kolik zákazníků u nás utratí více než milion korun ročně*? K tomu, aby podniky mohly přijímat *správná* rozhodnutí, potřebují mít dostatek *informací*. Tyto informace jsou ukryty v datech, kterých je v dnešní době v okolí podniku a v něm samotném obrovské množství. Business Intelligence nabízí řešení, jak tato data zpracovat a na jejich základě poskytnout informace potřebné pro lepší rozhodování (Dokoupil, 2006).

2.1.1 BI – historie

V roce 1958 vydal *Hans Peter Lunch*, výzkumný pracovník laboratoří IBM, článek a *Business Intelligence System*, v němž užil termín *Business Intelligence*. BI definuje jako schopnost vnímat vzájemné vztahy prezentovaných faktů způsobem, aby se na jejich základě mohly provádět správné

[1] Gartner, Inc. – přední analytická a konzultační firma světa v oblasti informačních technologií založená v roce 1979 ve městě Stamford, Connecticut, USA.

[2] k definici a vysvětlení jednotlivých pojmů se dostanu dále v textu.

[3] Cituji pouze citovaný zdroj a k původnímu dokumentu jsem nezískal přístup, původní dokument je však možné koupit přímo od IBM, [on-line] https://www-

činnosti k dosažení cíle (Bus092)[3]. Po této události následuje odmlka a teprve koncem 80. let dochází k dalšímu posunu.

Znovu se s pojmem BI setkáváme konkrétně v roce 1989, kdy termín použil skutečný zakladatel *Howard J. Dresner* jako *množinu konceptů a metod určených pro zkvalitnění rozhodnutí firmy* (Dokoupil, 2006). Opět následuje určitá odmlka, avšak již v průběhu 90. let dochází již k významnějšímu rozšíření této myšlenky.

Spolu s postupným vývojem v oboru vznikaly i přesnější definice. Jednu takovou definici BI nabízí i Česká společnost pro systémovou integraci. *Business Intelligence je sada postupů, procesů a technologií, jejímž cílem je účinně a účelně podporovat rozhodovací procesy ve firmě. Představuje komplex aplikací IS/ICT, které podporují analytické a plánovací činnosti podniků a organizací a jsou postaveny na specifických, tzv. OLAP (On-Line Analytical Processing) technologiích a jejich modifikacích* (Dokoupil, 2006).

Trochu jinak zaměřené je vymezení od Václava Synáčka, který definuje BI jako ucelený pohled na specifickou část IS; lze tak označit specifické technologie a přístupy k vývoji této části IS, hotovou komponentu systému nebo přístup k získávání informací pro strategické řízení organizací (Synáček, 2007).

Nepochybně bych mohl uvést i další definice, ale nemyslím si, že by to bylo bezpodmínečně nutné. Pro základní objasnění a pochopení významu BI je předchozí definice dostačující.

Obecně se dá říci, že definice BI rozhodně neříká, jak mají vypadat datové sklady, nebo analytické nástroje nad nimi, nýbrž vymezuje prostor pro pohyb a naplnění hlavní myšlenky – podpora rozhodování a rozhodovacích procesů v rámci podniku.

BI obor se propracovával k současnému stavu po dobu více než 30 let. Teprve nyní je schopen poskytovat téměř *real-time*[4] data pro podporu strategického rozhodování. Mezi historicky prvotní potřeby pro podobně rychlou odezvu systému patří obory:

- finančního obchodování, včetně analýzy vývoje hodnot akcií a obchodování s nimi v reálném čase;
- vojenství a vojenského podnikání;
- přepravy, včetně leteckých systémů aerolinek, center pro letový provoz a řízení železnic;
- leteckých středisek NASA;
- logistických a přepravních služeb společnosti FedEx a UPS (Correia, a další, 2002).

2.1.2 BI – současnost

Obzvláště v období ekonomického útlumu přichází vhodná doba pro nástroje BI, kdy nejedno vedení podniku bude chtít analyzovat data o prodeji a zákaznících, aby bylo možné učinit kvalifikovaná rozhodnutí o další obchodní strategii. To pochopitelně zvyšuje poptávku po specialistech BI (Hoffmann, a další, 2/2009).

Podle informací společnosti Gartner zveřejněných v CIO BW[5] měly pro rok 2009 obchodní priority a IT priority podniků vypadat následovně.

---

[3] Cituji pouze citovaný zdroj a k původnímu dokumentu jsem nezískal přístup, původní dokument je však možné koupit přímo od IBM, [on-line] https://www-01.ibm.com/services/projects/wse/ww/epjd01.nsf/PEF_YourCart/56FF6B83E85264D00025767700609765?EditDocument&S_ActiveUserRole=8-Customer, přístup 23. 11. 2009.

[4] Vždy není zcela snadné překládat anglické termíny do češtiny a osobně si myslím, že mnohdy to není ani vhodné či žádoucí, proto budu na některých místech práce používat tyto nečeské výrazy, neboť jsou podle mého názoru *přesnější*.

Obchodní priority	IT priority
Zlepšování obchodních procesů	Business Intelligence
Snižování podnikových nákladů	Podnikové aplikace (ERP, CRM…)
Zlepšení efektivity pracovních sil	Modernizace starých aplikací
Získávání a udržení nových zákazníků	Technologie pro spolupráci
Lepší využití informací a analýz	Sítě, hlasová a datová komunikace
Vytváření nových produktů a služeb	Technická infrastruktura
Efektivnější cílení na trh a zákazníky	Bezpečnostní technologie
Řízení a zvládnutí změnových iniciativ	Aplikace a architektura SOA
Prohloubení existujících vztahů se zákazníky	Document management
Expanze na nové trhy a území	

Tabulka 1: Priority CIO pro rok 2009 (Erben, a další, 2/2009)

Společnost Gartner tedy staví BI na vrchol zájmu podnikových IT oddělení. Jako opačný názor uvádím část rozhovoru s Jaroslavem Prcházkou[6] z časopisu CIO BW, ze kterého jsou přinejmenším zřejmé mírně odlišné priority (Erben, 10/2009). Názor ředitele jedné konkrétní společnosti samozřejmě není zcela určující, avšak vychází z konkrétní zkušenosti.[7]

Redaktor: „Jak velký je zájem v současné době o řešení business intelligence, třeba kvůli modelování různých ekonomických scénářů a situací v podniku?“

J. Procházka: „Přestože mnoho našich zákazníků využívá ERP řešení, která poskytují vhodnou datovou základnu pro nasazení BI, nezaznamenáváme prozatím velký zájem, ani růst poptávky. Dokonce i v řadě velkých podniků se spokojují s funkcemi tradičních reportů ERP a o BI zatím neuvažují.“[8]

Hned o měsíc později zveřejnil CIO BW výsledky výzkumu o Business trendech. Výzkumu se zúčastnilo 797 IT profesionálů, kteří odpovídali na to, jaké vidí v současné době IT priority a do čeho podle nich půjdou v roce 2010 investice.

Odvětví IT	*považuje za IT prioritu*
Cloud Computing (CC)	60 %
Business Intelligence (BI)	51 %
Business Process Management (BPM)	51 %

Tabulka 2: Současné IT priority (Jirásko, 11/2009)

Odvětví	*zajímám se*	*aktivně zkoumám*	*právě implementuji*	*upgradujeme*	*nezajímá mě moc*
BI	35 %	16 %	16 %	14 %	19 %
BPM	32 %	19 %	17 %	12 %	20 %

Tabulka 3: Plány v IT (Jirásko, 11/2009)

[5] CIO BW – časopis *CIO Business World*

[6] Jaroslav Procházka – generální ředitel společnosti Infinity, a. s., která od roku 1992 podniká v oblasti IS/ICT.

[7] Proti analýzám společnosti Gartner samozřejmě nemám námitek, ale přijde mi vhodné jejich závěry konfrontovat, aspoň částečně, s realitou.

[8] Společnost Infinity uvádí jako své klienty podniky – *Volksbank, IDS Olomouc, Scania, Hyper-V, 2N Telekomunikace, AHORN CZ, Plzeňský prazdroj, DP města Brna aj.*

[on-line] http://www.infinity.cz/Stranka/reference-a-projekty, přístup 24. 11. 2009.

Je evidentní, že pokud výzkumy/respondenti nelžou, zájem o BI řešení je a bude. Avšak nepochybně je zde patrný rozdíl mezi tím, *považovat něco za prioritu* a *skutečně problém řešit*.

Správná podnikatelská rozhodnutí lze provádět jen na základě včasných a relevantních informací. Období ekonomický propadů často vede k opačnému efektu na trhu IT, neboť podniky jsou ochotny investovat do nových řešení, která jim budou schopna navyšovat efektivitu, zkracovat reakční dobu, popřípadě ukazovat možnosti dalšího růstu. Podniky často již mají implementován systém ERP, přičemž jeho rozšíření o BI základnu není nikterak drahé a přinese významné výsledky při sledování chování podniku. Podnik se pak může bez dodatečných nákladů významně posunout dále dopředu.

BI totiž může odhalit skryté rezervy v podnikových procesech a vyvolat včasnou reakci na odchylky od předpokládaných výkonových ukazatelů.[9]

2.1.3 BI – budoucnost

Je nezbytné uvést i výhled do budoucna. Následuje odborný odhad společnosti Gartner pro vývoj v oblasti Business Intelligence v nejbližších 3 letech (Wailgum, a další, 6/2009) – *5 předpovědí Gartneru pro BI*.

Výhled do roku 2012 říká:

1. více než 35 % velkých podniků nebude schopno činit informovaná rozhodnutí v souvislosti s významnými změnami na trhu či v oboru, a proto bude BI hodně poptáváno pro podporu správného a včasného rozhodnutí;
2. minimálně 40 % rozpočtů na BI bude v pravomoci obchodních jednotek či oddělení namísto jednotek IT, což bude způsobovat rostoucí výdaje na analytické balíčky CPM[10];
3. až 20 % podniků bude využívat oborové analytické aplikace formou *SaaS*[11];
4. ještě letos se objeví nástroje pro podporu společného či skupinového rozhodování; tyto nástroje představují spojení sociálních aplikací s BI platformami; sociální aplikace umožní uživatelům propojit nápady a myšlenky vznikající v procesu rozhodování s informacemi poskytovanými BI aplikacemi; toto pojetí by mělo znásobit možné přínosy BI pro podnik, poněvadž umožní propojení analytického pohledu s nápady obchodních oddělení;
5. do roku 2012 bude jedna třetina analytických aplikací dodávána prostřednictvím *hrubozrnných mashupů*; IT oddělení se odkloní od velkolepých vizí, jaké představuje například SOA, které předpokládají budování složených aplikací z pečlivě seskládaných služeb a portálů.

V současnosti podle Gartneru na poli BI vedou především tito výrobci a dodavatelé řešení: *IBM (Cognos)*, *Microsoft*, *Oracle*, *SAP*, *Information Builders*, *SAS* a *Micro Strategy*.

2.2 BAM jako trend BI

BI odvětví informatiky se ubírá různými směry, většinou podle soudobých trendů. Lze uvést příklady z článku pocházejícího z roku 2006 – Office-izing BI, integrace BI s procesním řízením, BI postavené na SOA a také vývoj BAM nástrojů (Smalltree, 2006). Citovaný dokument popisuje i myšlenku spojení BI a CPM[12] (BI-PM), kdy integrací těchto dvou konceptů mohou podniky snáze

[9] Myšlenky pocházejí z více článků - (Jirásko, 2/2009), (Jirásko, 7,8/2009) a (Erben, a další, 3/2009).

[10] CPM – Corporate Performance Management

[11] SaaS – Software as a Service

[12] CPM – Corporate Performance Management

propojovat analytický pohled na svá data na straně jedné se svými dlouhodobými cíli na straně druhé.

Jistě nepřekvapí, že je to právě koncept BAM, který představuje jeden z možných přístupů, které se snaží nabídnout řešení pro požadované propojení dat a cílů, a tím i poskytnout půdu pro podporu každodenního rozhodování.

V září roku 2003 vyšel článek *BAM and Business Intelligence* (White, 2003) a už tehdy autor začíná slovy v *těžkých časech soudobé ekonomiky…* Předpokládám, že ani netušil, co přijde o několik let později. Na zmíněný článek se tedy lze dívat na jako mírně nadčasový a v současnosti roku 2009 jej můžeme brát jako možný pohled a příležitost pro podniky.

V době ekonomické krize se podniky obracejí k BI řešením, aby jim pomáhala snižovat provozní náklady a zvýšit konkurence schopnost. Jedna z nových BI technologií slibovala, že něco podobného může podnikům nabídnout skrze real-time monitorování podnikového prostředí, konkrétně sledováním hodnot klíčových podnikových ukazatelů, což povede ke zvýšení rychlosti a kvality business procesů.

BAM umožňuje rozšířit působení BI systémů pod úroveň strategického a taktického podnikového řízení až na úroveň operačního managementu. Společnost Gartner v roce 2002 odhadovala významný vzestup této technologie do předních příček zájmu podniků, jež chtějí rychle a správně přijímat rozhodnutí.

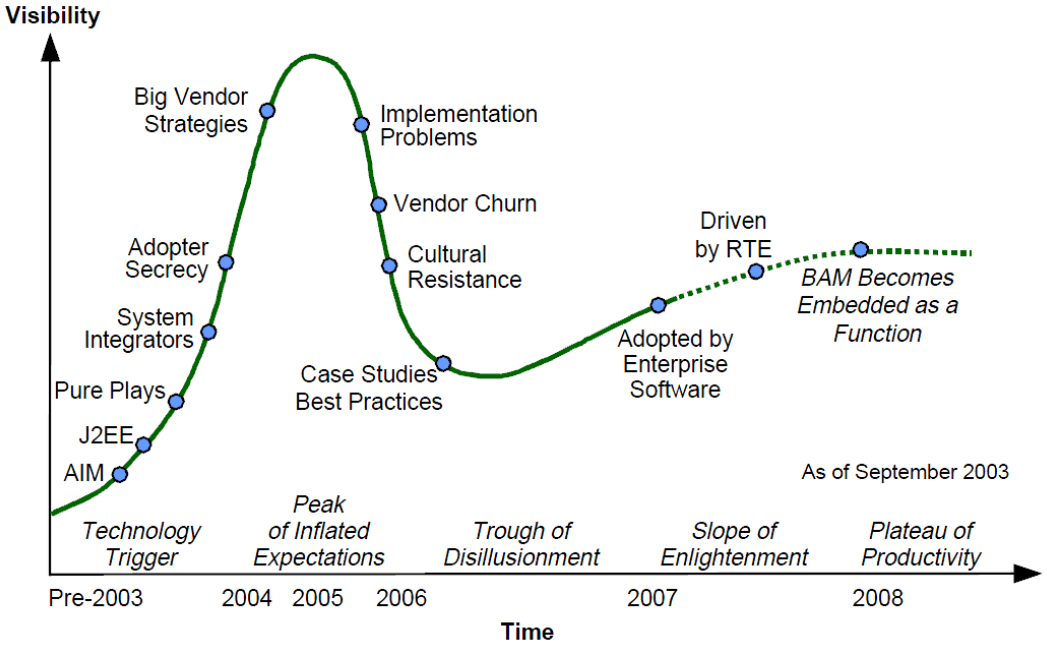
2.2.1 BAM – vize Gartnerů, BAM HC[13] 2003-2008

Podívejme se na původní pojetí a prognózy z analýzy společnosti Gartner ohledně BAM z roku 2003. Následující text je převážně čerpán právě ze zmíněné analýzy (Gassman, 2003).

Business Activity Monitoring definuje koncept poskytování přístupu ke klíčovým ukazatelům výkonu podniku v reálním čase tak, aby bylo zajištěno zvyšování rychlosti a efektivity business procesů. V roce 2002/2003 se BAM nachází v raných obdobích svého života a teprve pomalu se snaží získat si uznání a důvěru u průmyslu. Zatím se o BAM stále spíše jen ve větší míře hovoří, než že by se skutečně něco dělo, ale to se brzy změní. Potenciál BAM lze spatřit v horizontu delšího časového úseku, kdy si prodávající i kupující softwaru uvědomí jeho funkcionalitu a nabízené možnosti. Očekává se, že nejpozději v roce 2008 bude BAM představovat specifický trh, trh složený z překrývajících se několika rozličných trhů sub-řešení, na kterých BAM stojí a využívá je. Kolem roku 2003 BAM takovým trhem rozhodně není, zatím je spíše postaven nad odrazem zkušeností z poloviny 90. let, kdy se rozšiřovaly webově-orientované produkty, byly považovány za naprosto unikátní a v roce 2003 jsou již přijímány jako vestavěné funkce.

Následující obrázek Gartnerovské křivky ukazuje vývoj BAM v čase až do roku 2008.

[13] HC – Hype Cycle



Obrázek 1: BAM Hype Cycle, 2003 to 2008 (Gassman, 2003)

Technology trigger[14] *– vtrhnutí na svět, uveřejnění, zahájení života výrobku nebo jiné události, těší se značného zájmu ze strany tisku a průmyslu.*

Existuje snaha zachytit business události v momentě jejich vzniku, avšak jen málo podniků může říci, že by mělo implementováno BAM. Je velmi složité absorbovat všechny druhy událostí z velkého množství rozdílných zdrojů. Přesto však existují určité výjimky, kdy lze hovořit o prvních nasazeních skutečného BAM řešení, avšak zatím se jedná o velmi specializované aplikace, například pro detekci podvodů s kreditními kartami. Většina těchto aplikací představuje rychle se navracející investici a je tvořena s malou mírou flexibility.

Po BAM aplikacích roste poptávka vyvolaná především vlivem zvyšujícího se tempa podnikání, které nutí podniky zrychlovat své chování, především rychleji detekovat problémy i příležitosti. Nově přijatá nařízení, jakými jsou *Sarbanes-Oxley Act of 2002*[15] a *U. S. Health Insurance Portability and Accountability Act*[16], přináší požadavek na vyrovnání se s compliance rizikem. BAM v této situaci nabízí velmi příhodné a snadné řešení. BAM hraje do karet i čas jeho příchodu na svět, neboť technologie, které umožňují nasazení BAM jsou na trhu k dispozici již o dost dříve, přibližně od roku 2000. K významným a pro BAM příhodným změnám dochází v oblasti tvorby aplikací. Používání J2EE[17] a nasazování aplikačního *middlewaru*, který umožňuje posílat zprávy po systémové sběrnici, volá po použití monitorovacích technik, které mohou využívat externí aplikace jako je BAM, protože díky nim snáz *vidí* do systému.

[14] Fáze uvedení technologie

[15] *Sarbanes-Oxley Act of 2002*, zkráceně „SOX“ je kontrolní mechanismus firemních vnitropodnikových procesů. Jeho výstupy slouží jako podklady vlastníkům společností, k manažerským rozhodnutím a dále jako podklady k auditům (Microsoft).

[16] *U.S. Health Insurance Portability and Accountability Act*, zkráceně „HIPAA“ vyžaduje, aby byly prováděny správné kontroly zabezpečení informací a ochrany osobních dat za účelem ochrany záznamů pacientů (Microsoft).

[17] J2EE – Java 2 Enterprise Edition

Peak of Inflated Expectations[18] *– v průběhu této životní etapy se ochlazuje počáteční nadšení a přeceňovaná očekávání. Publikují se úspěšné projekty technologických lídrů v oblasti, avšak objevuje se i spousta selhání a neúspěchů, neboť technologie je zatlačena až na samou hranici svých možností. Nadšení mírně opadá a konference pořádají už jen podniky, které jsou schopny na dané technologii vydělávat.*

Kolem roku 2005 dochází k opadnutí všeobecného nadšení v oblasti BAM. Podniky, jež se rozhodly a stihly BAM implementovat, jej touto dobou nadále testují, nicméně celkový rozsah těchto projektů je velmi malý a zaměřený primárně pouze na několik málo specifických případů užití – omezené zdroje událostí a jednoduchá pravidla. Společnosti obecně odmítají svoji účast na projektech především ze dvou důvodů – buď se projekt zdařil a společnost si jej chce uchovat jako konkurenční výhodu, nebo se v průběhu projektu došlo k potížím a nezdarům, které si vedení společnosti raději nechá samo pro sebe a rozhodně se s nimi nevychloubá na veřejnosti.

Dalším ukazatelem, typickým pro toto období, je rostoucí počet dodavatelů zaměřených na BAM řešení. Až na pár světlých výjimek se dodavatelům příliš nedaří dosahovat významnějšího posunu v projektech. Vykazují sice zisk, avšak rozhodně nijak závratný. K *pískovišti* BAM se pomalu blíží systémoví integrátoři, což indikuje, že zájem o BAM stále je a že je také zájem na jeho dalším rozvoji.

Systémoví integrátoři mají na svědomí, že BAM se začíná integrovat jako funkcionalita do větších aplikačních systémů. Koncem roku 2004 se ozývají marketingová oddělení významnějších dodavatelů, že jejich společnost je schopna nabídnout kvalitní BAM řešení. Hlavními tahouny pro posun BAM do dalších životních období jsou rostoucí rozpočty marketingu, přísliby rychlé návratnosti investice a zdánlivý nadbytek možných řešení. V průběhu roku 2004 jsou spouštěny nové pilotní projekty a tím začínají pozvolna stoupat výdaje za BAM.

Pro ilustraci může sloužit počet odpovědí na dotaz *business activity monitoring* vyhledávače Google.com – v září roku 2003 nabídl 11 900 odkazů[19].

Trough of Disillusionment[20] *– technologii se nepodařilo naplnit vysoká očekávání z předchozích životních období, proto zájem medií o ni upadá a stává se nemoderní. Media se jí až na pár výjimek přestávají věnovat.*

Realita, jež ukazuje, jak skutečně obtížné je BAM nasadit, staví podnikům do cesty v jejich odhodlání spustit pilotní projekt BAM vysokou překážku. V rámci implementace se rychle objevují problémy s požadavky business uživatelů, kteří si přejí dostávat varovaní na události, které je velmi složité detekovat. Díky složitým pravidlům pro detekci událostí jsou často vyvolána falešná či mylná varování, která však prohlubují nedůvěru uživatelů v BAM technologii. Navzdory tomu, že existují úspěšné projekty se specifickým zaměřením, v celopodnikovém nasazení se širším polem působnosti, s většími požadavky na sběr události z různých podnikových zdrojů, rozmanitými potřebami zaměstnanců se nakonec jen některé podniky dostanou přes první generaci BAM. Ne každý podnik ze začátku disponuje potřebnou mírou disciplíny, kterou nasazení BAM do podniku vyžaduje.

Dříve, než je možné nasadit BAM nástroje, je nutné vyřešit otázky *change managementu* a *datové kvality* a *bezpečnosti*. V neposlední řadě také kulturní odpor mezi zaměstnanci může výrazně snížit nadšení okolo BAM. V podnicích, kde by díky BAM mohlo dojít k propouštění, narazí jeho zavádění nepochybně na odpor významný. Je více než zřejmé, že BAM díky automatizaci procesů může nahradit pracovníky, kteří dříve daný úkol plnili, a bude chvíli trvat, než pro toto bude nalezeno pochopení.

---

[18] Fáze přehnaných očekávání

[19] v listopadu 2009 je počet odkazů na dotaz „business activity monitoring“ na Google.cz – 36 300 000.

[20] Fáze vystřízlivění

Příliš optimistické plánování BAM dodávek ze strany dodavatelů rozšiřování technologie příliš neprospěje. Nerozhodnost a nepříliš vysoká důvěra podniků při zavádění BAM vede na straně dodavatelů k fúzování i bankrotům. Hráči očekávající rychlou návratnost investic se pokusí nasadit BAM již v průběhu těchto dodavatelských nepokojů, konzervativnější hráči vyčkají na zklidnění trhu a situaci, kdy bude trh dodavatelů a jejich produktů stabilnější a snáze čitelný.

Slope of Enlightenment[21] *– přestože tisk se víceméně vzdal tématu dané technologie, na trhu jsou stále firmy, které nadále experimentují a snaží se pochopit možné přínosy a praktické nasazení technologie.*

Jakmile BAM bublina splaskne, je čas na očistu a znovuobnovení zájmu. Objevují se první studie o dodavatelích, kteří přežili konsolidaci, a o podnicích, které odhalují, čeho všeho dosáhly díky použití BAM. Dodavatelé již mají k dispozici *best-practices*, díky nimž mohou snáze eliminovat potenciální neúspěchy při nasazování. V roce 2006 mají velcí hráči na trhu bezpečně integrovanou funkcionalitu BAM do svých produktů. Mohou tedy u svých zákazníků provádět upgrade. Přesně tohle významně oživuje povědomí o BAM a zároveň znesnadňuje další sledování života technologie. V momentě, kdy je BAM *pouhou* integrovanou funkcionalitou podnikových systémů, není na něj již snadno vidět. V tomto okamžiku BAM opouští svůj specifický trh a nadále je vnímán jako konkurenční funkce napříč produkty více trhů.

Plateau of Productivity[22] *– přínosy pro skutečný svět jsou známy a obecně přijímány. Dílčí nástroje a metodologie nabývají s každou další generací na stabilitě. Konečný rozměr využití je dán v závislosti na tom, zda technologie je schopna nabízet výhody pro velkou část trhu, nebo své uplatnění najde spíše jen na dílčích, okrajových trzích.*

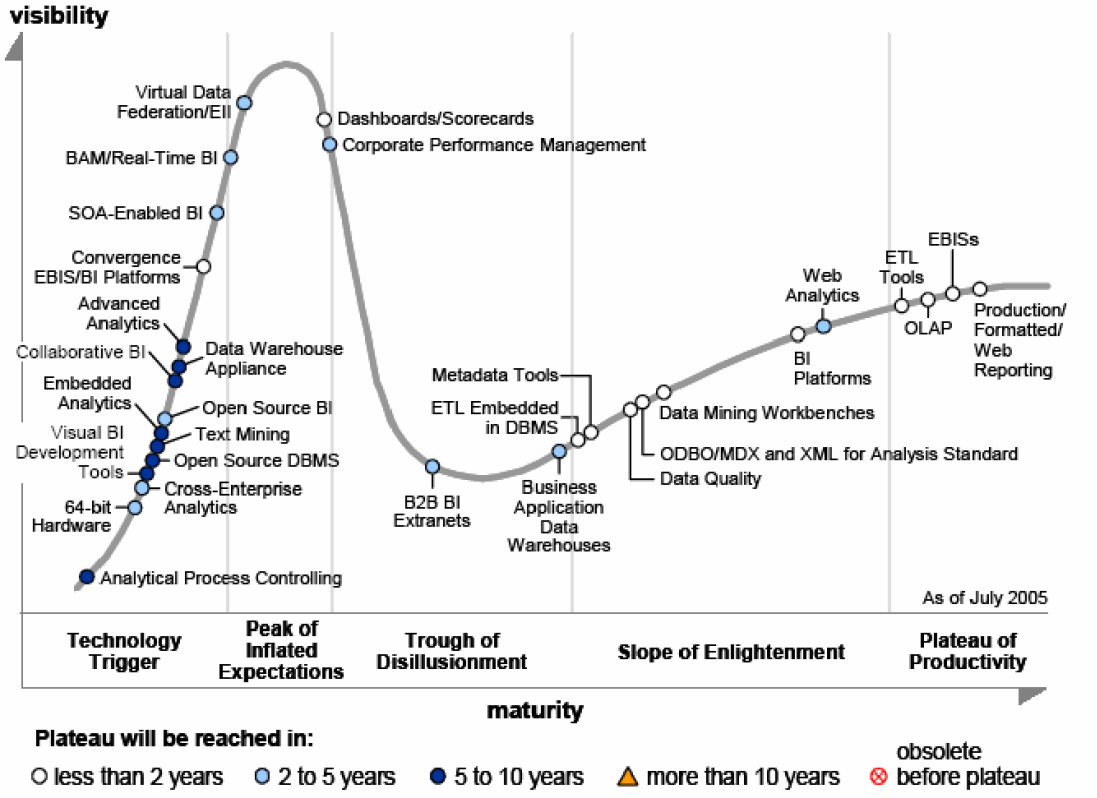
Kolem roku 2008 je BAM funkcionalita nabízena jakou součást podnikového softwaru a middlewaru. Podnikoví uživatelé mají jasno v síle nástroje, který poskytuje okamžitá varování na business události s podporou automatické reakce nebo rozhodování. BAM se plně přizpůsobuje požadavkům *real-time businessu*. Technologie na zpracování událostí již je propracovaná. Komplexní řízení událostí sice má ještě prostor pro vývoj, avšak již teď podnik zřetelně vidí a rozlišuje, co je možné a co je nezbytné. Funkcionalita varování je již na vyspělé úrovni a podnik se může plně zaměřit na jeho zautomatizování se systémy *business process managementu*. BAM sjednocuje nejen oddělení napříč podnikem, ale i za hranicemi podniku směrem k partnerům, regulátorům a zákazníkům. Jasným cílem je vytvoření standardů pro jejich propojení.

Bohužel žádná aktualizovaná HC pro BAM už nevyšla, nicméně společnost Gartner vydává svoje křivky i pro jiná odvětví IT, kde se BAM jako dílčí technologie často vyskytuje. Aspoň takto zprostředkovaně lze tedy i nadále sledovat životní vývoj BAM podle společnosti Gartner.

[21] Fáze osvícení

[22] Fáze produktivity

2.2.2 BAM – vize Gartnerů, HC for BI and DW, 2005



Obrázek 2: Hype Cycle for Business Intelligence and Data Warehousing, 2005 (Dokoupil, 2006)

Z porovnání tohoto odhadu s předchozím odhadem je zřejmé, že se příliš neliší. Je patrní jisté zpomalení ve vývoji. V roce 2005 měl BAM procházet *fází přehnaných očekávání*. Tato fáze se vyznačuje velkým zájmem o technologii ze strany odborné veřejnosti i ze strany výrobců, kteří BAM postupně integrují do svých podnikových řešení. Naproti tomu většina firem se zavedením dosud váhá, přestože technologie má potenciál výrazně zvýšit jejich příjmy a omezit náklady.

Na této křivce je BAM zařazen mezi *dospívající* technologii a v průběhu dalších 2 až 5 let bychom se mohli dočkat jeho dozrání do fáze produktivity, a tím i jejího rozšíření v podnikové informatice.

Funkcionalita BAM se začíná objevovat ve větších business aplikacích. Velcí dodavatelé software začínají prodávat BAM řešení, popřípadě je aktivně vyvíjejí.

Oblasti, do nichž BAM začíná pronikat a ovlivňovat je, jsou především *supply-chain mangement*, *event marketing*, *B2B sítě*, *compliance* či nástroje BPM[23].

Rozšíření na trhu se odhaduje mezi 1-5 %.

Mezi výrobce se řadí *Information Builders, Microsoft Terradata, Tibco, WebMethods*.[24]

2.2.3 BAM – současnost

Bohužel další analýzy společnosti Gartner zatím ještě nebyly uvolněny k *bezplatnému* užití[25], a je proto poněkud náročnější dopátrat se současného stavu. Současný stav tedy odhaduju ze zmínek

[23] BPM – Business Process Management

[24] Podobnost s dodavateli BI jistě není náhodná.

o jiných technologiích, které mají s BAM souvislost, a také z nahlédnutí a interpretací obsahu *zdarma* nedostupných zpráv[26].

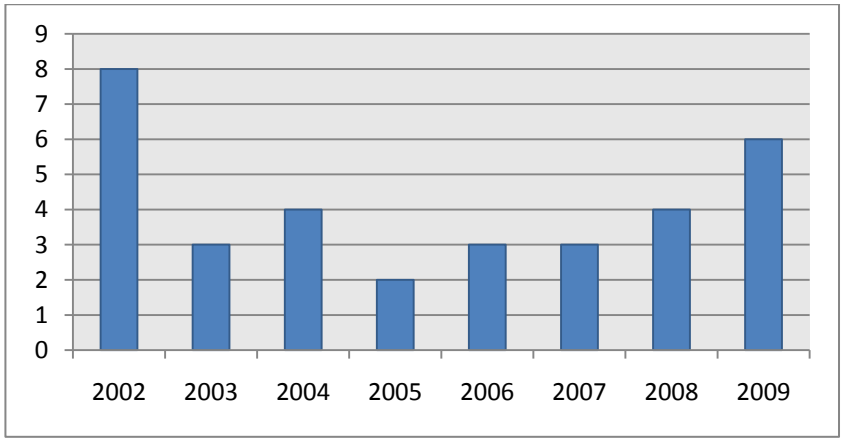
Nejprve je užitečné podívat se na rok vzniku odborných článků[27].

Největší počet článků je vydán v letech 2002-2003. Přeci jen došlo k prezentaci nové myšlenky a mnoho autorů mělo o čem psát.

Postupně počet článků klesá. Docela příhodné je, že z roku 2005 jsem našel pouze dva zdroje a jeden z nich je pojmenovaný *Is BAM Alive and Well* (White, 2005). Článek je od stejného autora, který o 2 roky dříve píše článek *BAM and Business Intelligence* (White, 2003). V té době vidí BAM jako výbornou příležitost pro podniky, o dva roky později se ptá, zdali ještě BAM existuje. V časovém odstupu těchto dvou článků je jasně čitelné, že BAM stále žije, nicméně neprožívá právě lehké časy, zmiňuje se spojení BAM se SOA[28] a někteří výrobci nabízející čisté BAM řešení Celequest a systémový integrátoři s BAM funkcionalitou IBM, TIBCO. Tohle může ukazovat přiblížení se k *fázi vystřízlivění*.

V analýze *Hype Cycle for Web and User Interaction Technologies, 2008* (Gartner) je v popisu současného stavu SOA zmínka o tom, že zvýšená poptávka po užívání BPM a BAM vede společnosti k zaměření se na SOA, neboť právě SOA nabízí snadnou a cenově přijatelnou implementaci BPM a BAM. Což lze interpretovat také tak, že technologie BAM přežila *fázi vystřízlivění*, technologicky se stabilizovala a mohla by se nacházet přibližně u *fáze osvícení*.

Nejčerstvější analýzy společnosti Gartner *Hype Cycle for BPM, 2009* (Gartner) přiřazují BAM na místo *Sliding Into the Trough*[29], stejně jako *Hype Cycle for BI and PM, 2009* (Gartner). Ta také zmiňuje BAM ve fázi *Sliding Into the Trough*. Je zřejmé, že Gartner nepatrně změnil názvosloví, i přesto je však nadevše jasné, že vývoj BAM sice poněkud přibrzdil, ale nachází se již blízko finální fáze produktivity a vzrůstající počet odborných článků může být toho důkazem.



Graf 1: Počet odborných článků v čase

[25] Obvyklou cenu, jež si společnost Gartner účtuje za zpřístupnění svých analýz je $ 1995. Zajímavých dokumentů (podle názvu, obsahu, klíčových slov) jsem našel hned několik… Nejen součet cen, ale i jedna samotná cena významně překračuje můj stanovený rozpočet na tvorbu diplomové práce. Bohužel pokus o emailovou komunikaci a poskytnutí materiálů Gartner k čistě akademickým účelům se nezdařil.

[26] Přestože celá analýza Gartnerů není zdarma, na jejich webu je k dispozici náhled na obsah analýzy. Poněvadž hype-cycle mají hodně podobný průběh, lze se z obsahu dovtípit, ve které části se sledovaná technologie nachází.

[27] Nejde o výsledek žádné přímo, na toto zaměřené studie, nýbrž o můj pohled na strukturu časového rozložení vzniku zdrojových odborných materiálů, které používám a cituji.

[28] SOA – Service Oriented Architecture

[29] Cesta k sedlu/obratu

3 Business Activity Monitoring

Gartner uvedl termín BAM již v červnu roku 2001 jako koncept pro zrychlování a zefektivňování business procesů v podniku prostřednictvím přímého přístupu ke klíčovým podnikovým ukazatelům v reálném čase. A výrobci jej přijali. Nicméně stále existují nejasnosti v tom, co za BAM označit a co ještě/už ne.

Podstatou monitorování podnikových aktivit a procesů v reálném čase je schopnost systému BAM zachycovat a zpracovávat události, které se odehrávají jak uvnitř, tak mimo hranice podniku. Každá z těchto událostí přitom v sobě obsahuje jistou informační hodnotu, která je pro podnik a průběh podnikových procesů často nezanedbatelná.

Události jsou charakteristické tím, že neprocházejí informačními systémy jedna za druhou. Existují mezi nimi složité vztahy – jedna vyvolává druhou, některé vznikají současně (i v různých časových zónách), jiné jsou navzájem nezávislé. Událostí může také v krátkém čase vzniknout velké množství.

V dnešní turbulentní době je více než kdy předtím potřeba pohotově využít příležitosti (která za hodinu již nemusí existovat) a na druhé straně rychle odhalit nebezpečí a reagovat na ně. Informace, které BAM poskytuje na základě zpracování událostí, by měly podniku takové chování umožnit.

Koncept monitorování činností v reálném čase byl známý mnohem dříve než BAM spatřil světlo světa. Tyto systémy se přesto od dnešního pojetí značně lišily – byly napojeny pouze na jediný zdroj dat a o tomto zdroji poskytovaly informace. Na rozdíl od nich zpracovává BAM informace z mnoha aplikací či zdrojů a umožňuje tak širší a sofistikovanější pohled na činnost podniku (Dokoupil, 2006).

3.1 Definice BAM

Definovat BAM není úplně snadné. Samozřejmě, jak už to nejen v IT bývá, různí autoři, či společnosti chápou často pojmy odlišně, a proto i samotné vyjádření se mírně liší. Nepochybně největší odlišnosti ve vysvětlení pojmu najdeme v samotném komerčním světě. Odchylky tam často způsobuje oddělení marketingu, která se snaží produkt *odlišit* od konkurence. Tady právě často vznikají odchylky v terminologii, které dávají více než k přesnému popisu použité technologie v produktu přednost tvorbě vhodné image firmy.[30]

3.1.1 Překlad

Nejsnazší vysvětlení termínu by mohl poskytnout obyčejný překlad. Volně by se BAM dal přeložit jako *sledování podnikových/business aktivit*. v podstatě není s čím nesouhlasit. Jak se dále v práci dozvíme, jedná se o relativně přesné vyjádření pojmu. Nicméně osobně budu nadále raději pracovat s původním anglickým označením namísto českého překladu, ať už je jeho kvalita jakákoliv.

3.1.2 Jan Kotek

Business Activity Monitoring neboli monitorování aktivit podniku, představuje nadstavbu a další přirozený rozvoj integrace podnikových procesů. Hlavním cílem BAM je dále zvyšovat efektivitu podnikových procesů pomocí poskytování včasných informací a zpětné vazby o aktuální situaci, ve které se podnik nachází. Informace o stavu a průběhu podnikových procesů pak umožňují managementu doslova držet ruku na tepu podniku a efektivně jej řídit na základě přesných informací (Kotek, 2004).

[30] Ukázkou práce marketingu může být například *4G internet* – rozhodně neběží na mobilní síti čtvrté generace a terminologicky *správně* by se měl nazývat *3G*.

3.1.3 MSDN

Business Activity Monitoring představuje soubor nástrojů na řízení datových agregací, varování a profilů ke sledování relevantních klíčových podnikových ukazatelů (Key Performance Indicators, KPI). Poskytuje ucelený přehled napříč celým podnikem i všemi business procesy, ukazuje data o aktuálním stavu a výsledcích podnikových transakcí, činností, procesů, takže je možné okamžitě odhalovat problematické oblasti a ihned se věnovat jejich řešením (Bus091).

3.1.4 Wikipedia

Pojem Business Activity Monitoring je původem z dílny analytiků společnosti Gartner. Odkazuje na agregaci dat a jejich následné analýzy a reportování v reálném čase. Primárním zaměřením jsou informace o zákazníkovi, činnostech zákazníka a organizace. Předmětem může být jeden konkrétní proces, software, ale častěji se jedná o spojení více procesů a činností, které procházejí napříč celým podnikem zahrnující více systémů a aplikací. Primárním zaměřením je poskytování informací o aktuálním chodu firmy pro operativní management (Bus09).

3.1.5 Gartner

Pojďme se podívat přímo ke zdroji, jak samotná společnost Gartner s termínem BAM nakládá. *Business Activity Monitoring – tento termín definuje, jak je možné zajistit přístup ke klíčovým podnikovým ukazatelům v reálném čase. Cílem zavedení takového systému je zvýšení rychlosti a efektivity podnikových operací* (McCoy, 2002).

3.2 Procesní integrace

Koncept BAM předpokládá procesní pohled na podnik. Pro zařazení na konkrétní pozici BAM v podniku ještě pár slov k problematice procesní integrace.

Integrace podnikových procesů tvoří základ, nad kterým je postaveno každé řešení pro monitorování aktivit podniku. Integrace podnikových procesů, business process integration (BPI), je založena na prostém faktu, že pouze ukončený výkon podnikových procesů procházejících skrze celý podnik je tím, co generuje příjmy podniku a tedy že efektivita podniku je přímo určována efektivitou těchto procesů.

Jinými slovy skutečné přínosy podniku nepřináší systém řízení výroby nebo aplikace pro správu dodavatelského řetězce, ale jejich prodejní, objednávkový či výrobní proces, který těmito aplikacemi prochází. Efektivní řízení výroby produktu samo o sobě nepřináší podniku příjmy, pokud nejsme schopni dodat přesné informace o skutečných požadavcích zákazníků nebo zajistit včasné dodání zboží, fakturaci a vymožení pohledávek. Řízení výroby tedy generuje příjmy pouze ve spojení s příjmem objednávek, fakturací, distribucí a dalšími aktivitami, které se podílí na (celo-) podnikovém procesu. A právě zlepšením, neboli hladkým, flexibilním a co možná nejvíce automatizovaným výkonem, takového podnikového procesu lze dosáhnout radikálních změn v efektivitě podnikání.

Mezi přínosy, které přináší změna a optimalizace podnikových procesů můžeme zahrnout zvýšení výkonnosti vlastního kapitálu díky zrychlení zpracování objednávek nebo snížením skladových zásob nebo celkové zvýšení úrovně služeb poskytovaných zákazníkům a obchodním partnerům, která se následně odráží ve zvýšení celkového objemu objednávek. Příkladem zde může společnost Dell, která prodává mezi 120 000 a 140 000 počítači každý den. V jejím případě se objednávky zákazníků (tj. první aktivita podnikového procesu) překládají do objednávek pro subdodavatele v reálném čase. Takto integrované podnikové procesy umožňují společnosti Dell dosáhnout nebývalé efektivity s více jak stonásobnou obrátkou zásob během roku. Výsledkem jsou pak nižší náklady, a tedy i nižší ceny než v případě konkurenčních společností se zřejmými důsledky.

V konečném důsledku není integrace podnikových procesů o ničem jiném, než o hladké a do maximální možné míry automatizované komunikaci uvnitř podniku a mezi podniky navzájem. Respektive mezi aplikacemi a informačními systémy uvnitř a vně podniku, které realizují jednotlivé

aktivity (příjem objednávky, naplánování výroby, zajištění logistiky…) podnikového procesu (Kotek, 2004).

3.3 Popis BAM

Následující text čerpá především z textu (Gassman, 2003) a (Govekar, a další, 2002).

BAM řešení je souhrnem nástrojů a funkcionalit, prostřednictvím nichž manažeři operační úrovně řízení podniku zlepšují, zefektivňují svá rozhodnutí. BAM pracuje s různými druhy varování, které pocházejí nejčastěji z real-time analýzy událostí probíhajících business procesů. Tyto události vznikají v různých nezávislých částech systému. Celý systém je postaven především na následujících třech základních kamenech:

1) absorpce událostí;
2) zpracování a filtrování událostí;
3) akce, doručení a zobrazení událostí.

BAM řešení může být postaveno na vrchol servisně-orientované architektury, přímo integrováno do business aplikací, nebo běžet jako samostatný program, aplikace. BAM sice vyžaduje ucelené řešení, ale může být napojen na jednotlivé komponenty, jakými jsou *message broker*, *database management system*, *rules engine*, *služby upozornění* nebo *reportovací nástroje BI*.

3.3.1 Definice real-time

Klíčovým přínosem BAM řešení je jeho práce ve *skutečném čase* – *real-time* nasazení. Ve světě BAM to značí, že příjemce zprávy je upozorněn na kritickou business událost téměř v okamžiku jejího vzniku; nicméně dosažení téměř okamžité reakce je velmi složité. Vhodnějším označením než *real-time* je termín *right-time*. Toto spojení se používá ve smyslu určitého kompromisu mezi faktory nákladů na vyvolání okamžitého varování, možností použité technologie a skutečné reakční doby uživatele. Přijde-li varování příliš pomalu, jeho potenciální užitná hodnota významně klesá. Podobně však přijde-li příliš rychle, může to vést přehnané reakci uživatele. Některé z prvních BAM řešení pracovaly v režimu jednodenního prodlení, nebo-li informace v nich byly nejméně jeden den staré. Od té doby se nároky na zpoždění přijetí varování o kritické business události mnohonásobně zpřísnily.

Vezměme si příklad, jednoho dne podnik extrahuje, transformuje a plní svůj datový sklad informacemi z více než dvanácti business aplikací. Během fáze transformování dat *rules engine* analyzuje data a snaží se najít ta, jež připadají na nespokojené zákazníky. Jakmile je objeví, odesílá zprávu s upozorněním pro příslušného vedoucího prodeje. Uživatelé jsou samozřejmě rádi, že už po jednom dni dochází k obratu – to přesně odpovídá jednodennímu prodlení, avšak mnohem raději by byli nespokojenosti informování ihned a měli tak příležitost zákazníka ještě přesvědčit. Úkol pro BAM.

Základ pro přístup k datům v reálném čase a integraci aplikací představují následující tři technologie

1) vysokorychlostní sítě;
2) internet a XML;
3) middleware – tj, aplikace, která se nachází mezi dvěma odlišnými business aplikacemi a zajišťuje přenos dat mezi nimi.

BAM nutí organizace, aby výrazně zlepšily kvalitu a typ informací, jež poskytují svým pracovníkům. Lidé obecně potřebují spíše méně než více informací, aby se zabránilo jejich informačnímu zahlcení. Softwarový BAM agenti jsou schopni v rámci neustálého reportování sledovat a vyhodnocovat anomálie v chování či nové trendy a na základě těchto svých zjištění vydávat varování často i s doporučením následujícího postupu vzhledem ke vzniklé situaci.

3.3.2 Přístup k různým zdrojům událostí

Hodnota BAM leží v rovině sledování celého širokého spektra nezávislých business aplikací, které dohromady umožňují chod jednotlivých business procesů podniku. Systémy BAM musejí přijímat zprávy o událostech ze všech těchto různých zdrojů, jakými jsou podpora vztahu se zákazníkem, dodavatelský řetězec a prodeje. Pokud tedy pravidla pro tvorbu varování mají obstát, musejí být napsána napříč všemi těmito aplikacemi – napříč, *end-to-end* business procesem. Dobrými zdroji pro sbírání událostí se jeví *webová rozhraní*, *integrační brokeři* a *integrované podnikové aplikace*.

3.3.3 Business události versus události procesů

Každá společnost potřebuje sledovat nejen činnosti business procesů, ale i základní techniku, jež business procesy podporuje. Funkcionalita BAM je striktně zaměřena na business procesy, zatímco podpora operačního IT, která monitoruje business služby, je zase zaměřena na základní technickou infrastrukturu a aplikace na ní. Řešení jsou shodná, avšak zdrojová data se liší, stejně jako pravidla a cílová skupina adresátů výsledků.

Varování generovaná systémem pro podporu operačního IT mohou být zaslána do systému BAM a vyvolat business varování (například pokles ve výkonu burzovního systému může vyvolat upozornění pro obchodníky, že zpomalení systému může mít vliv na rychlost obchodování).

3.3.4 Co je a co není BAM

BAM je jako koncept poskytování přístupu ke kriticky významným ukazatelům v business prostředí podniku v reálném čase, aby bylo možné dosahovat zlepšení efektivity a zvýšení rychlosti business operací. V nejširším pojetí představuje BAM konvergenci BI a aplikací pracujících v reálném čase zaměřených na dosahování podnikových cílů prostřednictvím výhod, jež poskytuje IT.

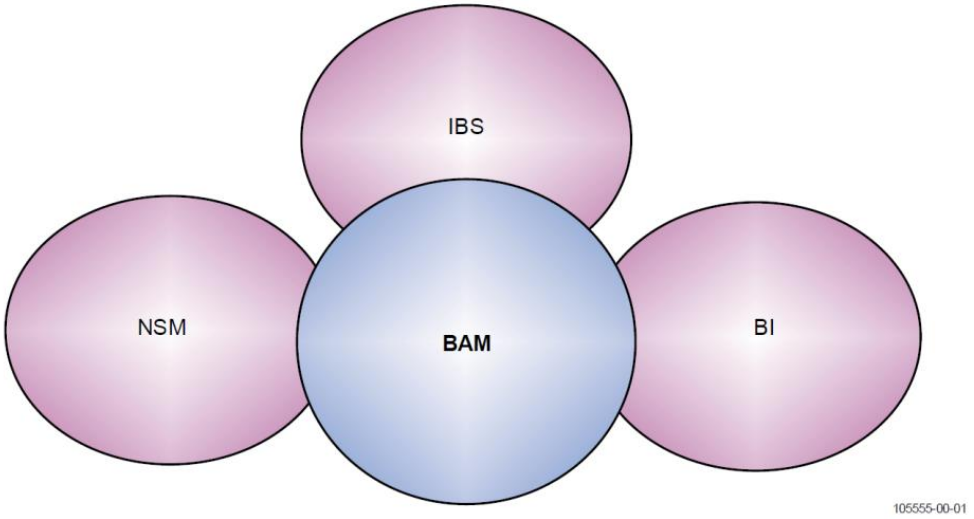
BAM poskytuje přístup ke kritickým ukazatelům business výkonu téměř v reálném čase, aby umožnil jejich zrychlení a zefektivnění v rámci business operací. Rozhodně se nejedná o *IT monitoring*.

BAM nástroje sledují obecně průběh klíčových procesů napříč celým podnikem a neomezují se pouze na určitá oddělení nebo specifickou technologii podniku. Rozsah BAM integrace zasahuje daleko za hranici oddělení nebo divize. Reálným časem potom nemusí být nutně čas v řádu nanosekund, nýbrž čas definovaný samotnou potřebou business procesu. BAM spojuje téměř skutečný/současný svět dat z datových skladů se světem *network and system managementu* a *sledováním business procesů* pomocí *integračních brokerů* a *sdílené sběrnice zpráv* (Correia, a další, 2002)[31].

3.3.5 Trh BAM

BAM nepředstavuje samostatný trh, nýbrž přesněji trh kombinovaný nebo i specifický. Specifičnost vychází z toho, že BAM zahrnuje několik dalších oblastí, které zaujímají samostatné trhy jiný technologií. Specifický trh představuje překryv těchto dílčích trhů. Nejvýrazněji do BAM zasahují *Business Intelligence*, *Network and System Management* a *Application Integration and Middleware*.

[31] Doufám, že je použitý text důvěryhodný. Přeci jen vyšel 1. dubna…



Obrázek 3: Kombinovaný trh BAM (Correia, a další, 2002)

3.3.6 Přínos BAM

Skutečný business přínos BAM leží na úrovní business strategií – umožňuje vznik nových strategií, snižování operačních nákladů, zvyšování výkonnosti business procesů a zdokonalování i jiných oblastí, jež stojí za pozornost managementu. Prvotní nasazení BAM v přepravě zboží a logistice jasně ukazují přínosy spojené s rychlejším přijímáním rozhodnutí.

Obecně zvyšující se tempo obchodování, vzrůstající požadavky na služby zákazníkům či požadavky na větší efektivitu a lepší návratnost investic nutí společnosti neustále zdokonalovat nastavení svých procesů a technologií, aby byly schopny lépe vyhovovat rostoucím obchodním požadavkům trhu. Všechny tyto faktory vytváří tlak na potřebu sáhnout po řešení typu BAM.

3.3.7 BAM a podnikání

Každý podnik bude dříve či později ovlivněn BAM – někteří jej budou potřebovat, aby vůbec přežili, jiní jej budou potřebovat jako nástroj konkurenční výhody nad ostatními. A to vše nastane díky prohlubování vztahu mezi IT podporou a business procesy.

Podniky musejí především pochopit, jaký vliv může mít BAM na jejich strukturu a činnosti, uvedu několik příkladů:

- ve skladech může být méně zásob a pracovníci mimo sklad mohou sledovat seznam a počet zboží, pohyb příjmů a výdejů zboží ve skladě, i na cestě do skladu;
- některá oddělení mohou zaniknout, zatímco jiná se mohou dále rozvíjet (například vymizení peněžních skrutátorů po zřízení a zavedení bankomatů);
- management již nemusí nadále shromažďovat informace, nýbrž rozhoduje o tom, které informace a v jaké podobě budou komu poskytnuty – lidé, kteří potřebují nejlepší informace, jsou umístění v centru business procesů;
- zaměstnanci se již nadále nemusejí zabývat nezpracovanými daty, ihned k dispozici mají grafické nebo textové výstupy reportů, upozornění na možné trendy či výchylky od plánů podle předem nadefinovaných kriterií (manažer přepravní společnosti je informován v momentě poklesu flotilou přepravované kapacity zboží pod stanovený práh, například SMS zprávou na mobilní telefon);
- ziskovost je pouze jedním z více ukazatelů, jež podniky sledují v reálném čase; dalšími sledovanými ukazateli může být spokojenost zákazníků, doručování zboží v čase, peníze v hotovosti na pokladnách aj;

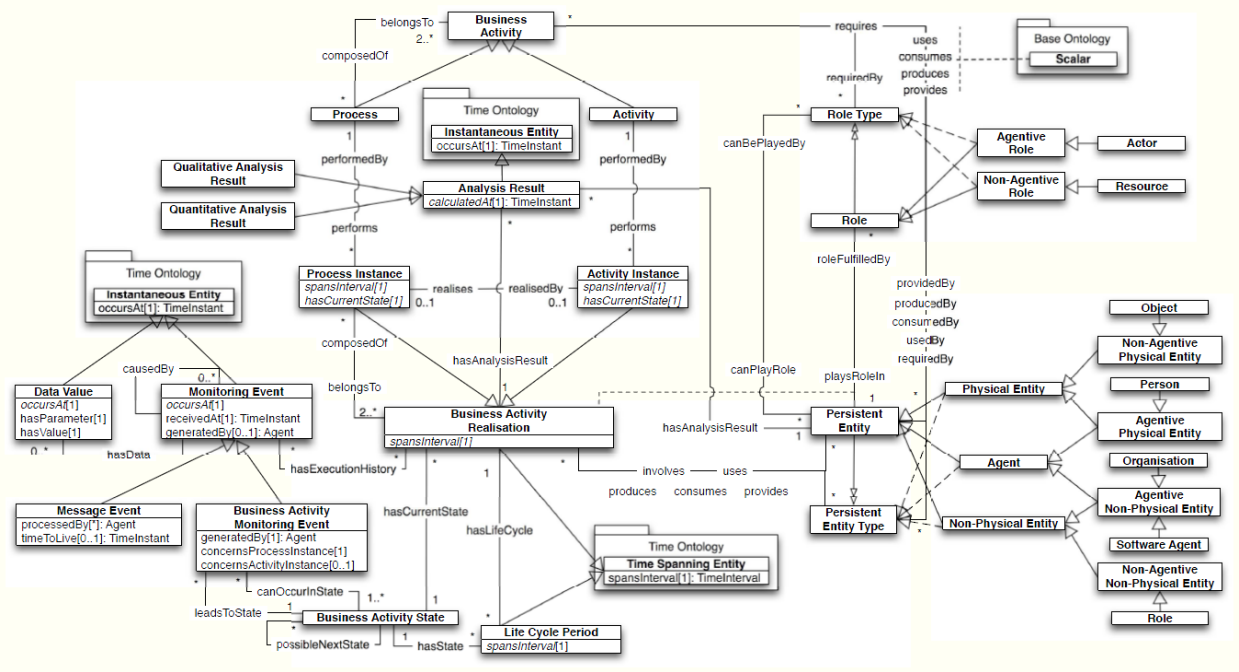
- business manažeři mohou vyvíjet složitější agregované ukazatele založené na korelaci chování při nakupování se zkušenostmi uživatelů.

Navzdory masovému rozšíření připojení vysokorychlostními sítěmi, rychlým počítačům i dostatečnému množství automatizovaných a on-line business procesů, BAM je stále jen koncept bez pěvně stanovených standardů a protokolů.

Některé z faktorů, které mohou bránit nasazování BAM:

- nedostatek zkušených pracovníků, kteří by dokázali pokračovat v podnikové integraci dále směrem k BAM;
- pochybnosti o výrobcích softwaru, že dokážou uspokojit poptávku po aplikacích, které nabídnou *real-time reporty* a *analýzy*.
- nedořešené otázky a problémy, které budou mít vliv na práci zaměstnanců v prostředí neustále se měnících pracovních postupů, úkolů a priorit;
- nezodpovězené otázky o použitelnosti a přínosech nasazení BAM;
- obavy odborových organizací z propouštění kvůli nasazování automatizovaných systémů na místo pracovníků.

3.4 Metamodel BAM



Obrázek 4: Metamodel BAM (Pedrinaci, a další, 2008)

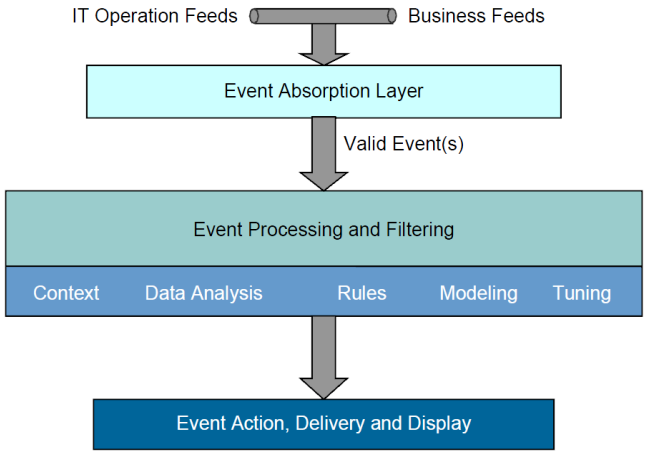
3.5 Logický model BAM architektury

BAM lze snadno pochopit jako koncept, to je ta snazší část. Podstatně složitější část je představit si, jak lze BAM začlenit do stávající architektury podniku. Následující schéma ukazuje, jak lze *událostmi* vyvolat *real-time reakci*. Model sice nemapuje úplný potenciál použitelných technologií pro BAM, avšak ukazuje dost, pro představu propojení jednotlivých částí oddělených systémů a jejich kooperaci na zachytávání, analýze a reakci na událost.

Základním archetypem BAM modelu je tradiční model používání v informatice *vstup-zpracování-výstup*. Činnost představuje rozpoznání smysluplné události, její analýza a následná komunikace s příjemcem výsledku. Následující obrázek ukazuje přeměnu vstupních událostí ve výstupní reakci systému BAM.

3.5.1 Tři základní kameny

Tři základní kameny (absorpce událostí; zpracování a filtrování událostí; akce, doručení a zobrazení událostí) jsou naprosto nezbytné pro jakékoliv BAM řešení. Podobně jako ve stavebnictví lze ze stavebního materiálu postavit *chatrč* nebo *palác*, mohou základní kameny BAM posloužit ke stavbě *dostačujícího* řešení nebo *skvělého* řešení. Existuje mnoho možností, jak BAM systém vystavět. Podniky by se měly vždy nejprve ujistit, že jejich základní požadavky na BAM jsou ve shodě se základními kameny, než se pustí do budování vyšších podpůrných funkcionalit jakými je automatizovaná tvorba pravidel nebo eskalace upozornění.



Obrázek 5: Logická architektura BAM, (Gassman, 2003)

Zdroje operačního IT

- selhání komponent infrastruktury;
- sniffování provozu integrační sběrnice;
- polling komponent infrastruktury;
- programová aplikační rozhraní;
- data z datových skladů.

Business zdroje

- finanční systémy (například změna ve výši úrokové míry);
- energetické systémy (například změny na vedení vysokého napětí vlivem napadeného sněhu);
- logistické systémy (například sledování poruch přepravních vozidel);
- systémy call-center (například zvyšování kapacity).

3.5.2 Absorpce událostí (VSTUP)

BAM nástroje využívají získávání událostí z více podnikových aplikací. Události mohou být získávány *pasivně* – pouhým přihlášením se k odběru zpráv procházejících skrz aplikační integrační broker; *aktivně* – pomocí *pollingu* nebo *screen scrapingu*.

Sledované události je možné roztřídit podle *místa jejich vzniku* a *informační hodnotě pro podnik*, typicky je lze definovat tři základní skupiny.

První skupina *– sledování událostí úzce souvisejících s částmi business procesů podniku:*

- *změny v klíčových podnikových ukazatelích (úroková míra);*
- *zavěšení hovoru s telefonním automatem;*
- *počet vrácených výrobků;*
- *varování generovaná samotným business procesem;*

- *agregované série událostí, které v souhrnu vykazují výkonnost celého systému (výkon call-centra).*

***Druhá skupina** – sledování událostí souvisejících s technickými, podpůrnými procesy podniku:*

- *selhání komponenty IT infrastruktury;*
- *události generované při chybě běhu aplikace;*
- *události z business procesů a aplikací.*

***Třetí skupina** – události ostatních technologických komponent a součástí IT infrastruktury, které spadají do sféry vlivu BAM:*

- *NSM nástroje pro monitorování provozu na síti, doby odezvy aplikací;*
- *nástroje BI, data miningu a datové analýzy;*
- *agenti;*
- *jiné aplikace (například od SAP nebo PeopleSoft).*

Faktorem pro vyhodnocení je úspěšnost správného ověření toků událostí, možnost jejich transformace na použitelný datový model a rozšíření o kontextové informace.

BAM aplikace *dostačujícího řešení* si vystačí sice se statickým datovým modelem, ale flexibilní BAM architektury vyžadují použití flexibilních datových modelů. *Skvělá řešení* by měla zahrnovat podporu pro široké spektrum adaptérů business aplikací, dočasné úložiště pro události k zamezení jejich případné ztráty, poskytovat distribuovanou množinu architektur a podporu filtrování formou před-analýzy.

3.5.3 Zpracování a filtrování událostí (ZPRACOVÁNÍ)

Tato vrstva je samotným srdcem celého BAM řešení. Primárním úkolem je hledat význam v záplavě přicházejících událostí ze vstupu. Rozhodně zde není prostor na prostoje či zdržení, je proto zajištění odpovídajícího výkonu představuje klíčový faktor. Vrstva zpracování a filtrování událostí musí především podle nastavených pravidel a kontextu odfiltrovat všechny události vyjma těch podstatných.

Zpracování zahrnuje hledání kontextu v událostech. Kontext může představovat analýza trendu (zkoumání významných datových bodů v DW a jejich porovnávání v čase, nebo normami, nebo dříve získanými šablonami) nebo sledování chování celého procesu (tyto aplikace sledují a vyhodnocují vliv události na zbytek business procesu s nímž je událost spojena).

Analýza business činnosti podle pravidel je podstatou pro přijetí správného rozhodnutí. Pravidla mohou být založena na *fuzzy logice* nebo *rozpoznávání vzorů*. Samotné zpracování událostí může běžet krom *real-time on-line režimu* také v pomalejším *off-line režimu* pro datové analýzy, modelování a ladění. Naposledy zmiňované je velmi podstatné, neboť platforma BAM je jednak systém varování a jednak systém analytický. Významná událost rozpoznaná jako významné ohrožení business procesu musí být automaticky vyhodnocena a co nejdříve předána jako varování pro zajištění následné odpovídající reakce. Analytické nástroje BAM pracují s velkými objemy dat, množstvím modelů a pravidel. Na jejich zpracování a analýzu lze použít *volný čas* systému, neboť obvykle nejsou kriticky závislé na okamžitém momentě zpracování.

Výsledkem zpracování událostí může být vygenerování *nových událostí*, které mohou být poslány zpět na vstup, *absorpční vrstvu*, nebo mohou vést k výsledkům, které jsou poslány na výstup, *vrstvu akce, doručení a zobrazení*. Pro přesné a rychlé fungování této vrstvy je tedy zapotřebí znalostí o technické a business konfiguraci. Obvykle je tato znalost již předpřipravená, avšak existují speciální případy, kdy ji lze vyvodit dle požadavků. Pro analýzu dat je vhodné použít nástroje BI, zatímco nástroje NSM se použijí pro zpracování dostupnosti a výkonnosti datové infrastruktury a pro účely procesu predikce, modelování a ladění. Nástroje aplikační integrace, BPM a business proces analýzy lze použít na rozbor událostí, plánování scénářů a ladění procesů.

Pravidla mohou být:

- *business pravidla (například risk management);*
- *technická pravidla (například různé algoritmy);*
- *datová analýza, modelování a ladění;*
- *nástroje z prostředí aplikační integrace, BI NSM, BPM a automatizace procesů.*

Produkty dosahující úrovně *dostačujícího řešení* obsahují obvykle pevně nastavená pravidla nebo jednoduchý editor pravidel a statický kontext. Jakmile událost zanalyzují, nejčastěji ji ihned zahodí. Produkty z kategorie *skvělých řešení* umožňují uživateli vytvářet komplexní pravidla a připojovat je na systémy business process managementu a nástroje business intelligence pro historické trendy. Všechny události jsou uloženy pro případnou post-analýzu k dalšímu zdokonalování pravidel. Tato vrstva nabízí spoustu prostoru pro invenci – hledání korelací a odhady vývoje, nebo jiné nabídky dodavatelů řešení. Dlouhodobé zkušenosti podniků s real-time správou událostí v IT infrastruktuře však naznačují, že nebude snadné stanovit a nadále udržovat spolehlivá a přesná business pravidla. Systém, kterému nelze bezpečně důvěřovat, nemá šanci uspět a být používán.

3.5.4 Akce, doručení a zobrazení událostí (VÝSTUP)

BAM nástroje potřebují mít k dispozici komunikační kanál, kterým mohou sdělit, co objevily. Jakmile je jednou událost zanalyzována, modelována a byla odhadnuta závažnost celé situace, je nezbytné informovat odpovídajícího příjemce.

Vrstva nutně potřebuje být nezávislá na koncovém zařízení, neboť je potřeba zajistit odeslání a správné zobrazení na velké množině potenciálních zařízení. Kvalita BAM řešení proto úzce souvisí s kvalitou varování – kontextem, podrobností a flexibilitou doručení. Cílový příjemce může být živá osoba, od které se očekává osobní zásah, nebo také automatizovaný systém, který provede jednoduchou reakci.

Dostačující řešení jednoduše zobrazí varování na přístrojové desce nebo odešlou e-mail do schránky příjemce. U *skvělých řešení* může být varování uživatelům posláno prostřednictvím *portálu* nebo *instant messagingu*. Na základě obdrženého varování si uživatelé mohou vyžádat další podrobná podkladová data, jež varování vyvolala, což může být zprostředkováno opět pomocí *přístrojové desky* nebo pomocí odkazu na webovém rozhraní. Navíc varování mohou být distribuována i dalším aplikací, a to buď přímo, nebo prostřednictvím *integračního brokeru*. Například je možné automaticky varováním spustit akci na upozornění zákazníka prostřednictvím BPM.

Požadavky na doručování:

- *nezávislost aplikací a zařízení;*
- *podpora mobilních zařízení, konzolí, kiosků, e-mailu, faxových přístrojů, papíru a tradičních počítačových zařízení.*

3.5.5 Reakce

Je nepochybné, že posledním krokem v tomto třístupňovém modelu je reakce, která může být poslána zpět do BAM systému, avšak v mnoha případech se skutečné místo reakce bude nacházet v systému mimo možnosti řízení BAM. BAM samozřejmě je možné rozšířit o doplňky nutné pro přímou reakci na podnikové události, většina uživatelů se však omezí na používání BAM na sběr dat, jejich interpretaci a generování varování. Lepší nastavení systému pomocí *kontrolních páček* je vždy spíše ponecháno na koncovém uživateli, aby se sám rozhodl, co potřebuje a co mu vyhovuje.

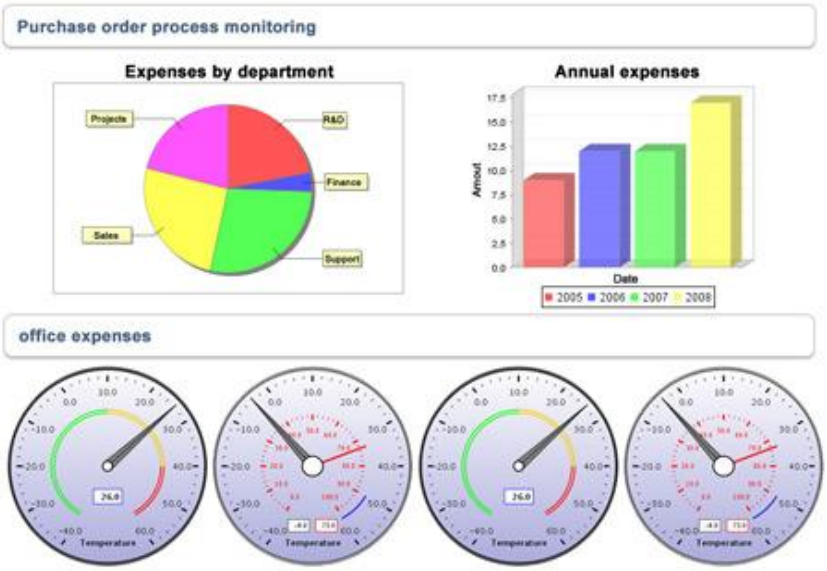
BAM řešení mohou být vytvořena tzv. *in-house* – vlastními silami, *sestavena systémovým integrátorem*, zakoupena jako *samostatná aplikace* nebo *integrovaná do podnikových aplikací*. Existuje řada rozšíření, která mohou BAM dílem doplňovat, ale aby se jednalo o skutečné BAM řešení,

musí zpracovávat události vzhledem k pravidlům a kontextu a zpracovávat je ve skutečném čase nad více aplikacemi, aby mohla dostát své požadované hodnotě.

3.6 Modely reakcí

Samotné *vyhlášení poplachu* je jen polovinou příběhu. Druhou polovinou je *reakce uživatelů* na tento poplach. Teprve vhodnou reakcí uživatele se dají měřit přínosy BAM. Podklady pro text tvoří článek (McCoy, a další, 2002).

Třívrstvou architekturu jsme si už představili a nyní se můžeme detailněji podívat na třetí vrstvu *akce, doručení a zobrazení událostí*. Někdy se této vrstvě metaforicky říká *dashboard*[32]. Původ je ve způsobu zobrazování dat uživateli, který je velmi podobný prezentaci výkonnostních dat řidiči automobilu prostřednictvím palubní přístrojové desky.



Obrázek 6: Ukázka BAM přístrojové desky (Polymita)

Přestože to zní velmi jednoduše, spousta přínosů se právě na tomto místě může získat nebo zahodit. Právě interakce mezi varováním nebo událostí systému BAM a cílovým uživatelem BAM je klíčová.

Celkově lze hovořit o pěti různých typech, každý je příhodný pro jiného odběratele, především v časování. Každý z nich má své přednosti, i nedostatky. Pořadí, ve kterém je budu níže popisovat, nemá nic společného s úrovní interakcí, složitosti či dospělostí daného přístupu. Navíc každý z těchto přístupů přináší jiné důsledky pro technologie, na kterých je dané BAM řešení postaveno – BI, NSM, middleware… Koneckonců BAM není řešení pro sledování na úrovni jedné aplikace, ačkoliv jím být může. BAM *dashboard* je agregujícím bodem zobrazujícím stav více různých aplikací.

3.6.1 BAM dashboard jako předpověď počasí

Kdykoliv sledujeme v televizi relaci o předpovědi počasí, sledujeme model jednosměrného přenosu informací – meteorolog nás informuje, varuje, kde zrovna řádí bouřka, kde je pro změnu jasné nebe a letní teploty a co můžeme v nejbližší době očekávat. Po zhlédnutí relace pak na základě obdržených informací přizpůsobíme své chování – vezmeme si deštník, nebo doma necháme teplé oblečení. Nepochybně je zbytečné snažit se jakkoliv manipulovat s televizí, abychom dosáhli změny

[32] Dashboard – přístrojová deska

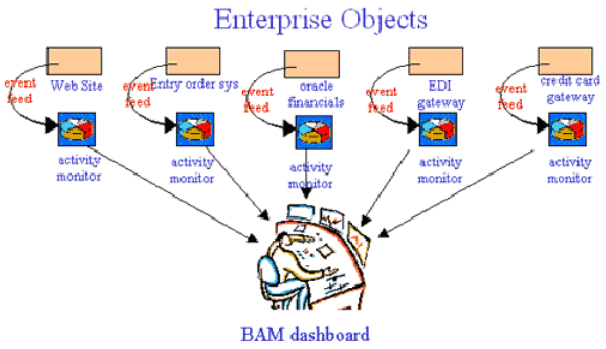
počasí. Všechno, co provedeme na základě informací z relace, se odehraje mimo prostředek přenosu informací, varování.

Jedná se o nejsnazší řešení a existuje jich spousta. Jsou tzv. *one-way push modely* pro doručování informací.

Jako příklad konkrétního podnikového nasazení lze uvést případovou studii společnosti Gartner (McCoy, 2002) – BAM dashboard měl na starost upozornit letového dispečera, pokud se chystalo odstartovat nákladní letadlo, které ještě nebylo plně vytížené. BAM systém nabízel varování typu *read-only*[33], dispečer musel po obdržení varování k vyřešení problému opustit prostředí systému BAM a využít jiné technické prostředky (např. osobně zajít, nebo zatelefonovat na nákladovou rampu apod.).

Tohle řešení je vhodné pro podniky, které začínají implementovat BAM. Nabízí jednoduchou konfiguraci a snadnou obsluhu, neboť není potřeba systémově řešit reakci, která probíhá vnějškem, mimo BAM systém.

Řešení může poskytovat první krůček ke složitějším řešením nebo také první a zároveň poslední krok celého řešení v případě, že výstraha systému vyžaduje určitý typ chování uživatele.



Obrázek 7: BAM dashboard a sběr událostí (Luckham, 2004)

Na obrázku sleduje BAM transakce systému. Šipky naznačují směr toku událostí v BAM, mezi BAM komponentami a BAM dashboardem. Je patrné, že BAM čte události generované činností sledovaného systému, ale do chodu samotného systému vůbec nezasahuje.

3.6.2 BAM dashboard jako manuální termostat

Je vidět, že prvnímu typu schází vnitřní mechanismus zpětné reakce v rámci systému kontrolovaného pomocí BAM. Všichni ti, co pracují v továrně nebo automatizovaném provozu, jednoduše prohlásí – doplňte dashboard o funkce, aby byl schopen pracovat nejen s varováním, ale navíc mohl i do systému, na který varuje, zasáhnout. Něco jako kontrolní panel jaderné elektrárny.

Příklad může být nastavení teploty pomocí termostatu na topení – systém ukazuje teplotu a nabízí mechanismus její úpravy.

1) Na termostatu je nastavena požadovaná teplota – význam lze snadno interpretovat; *je teplota vyšší nebo nižší, než bych si nyní přál*;
2) změna nastavené teploty na termostatu – povede ke změně výstupu systému; *termostat má nastaveno 25 °C, ale raději bych si dal jen 20 °C.*

[33] Read-only – pouze ke čtení

Tohle pojetí vyžaduje kromě dashboardu se zobrazením sledovaných hodnot navíc i zpětnou vazbu – mechanismus pro usměrnění řešení problému. Uživatelé BAM budou často sledovat *systém A* a prostřednictvím *systému B* reagovat na nežádoucí stavy *systému A*. Stejně jako v příkladu s topením – termostat ukazuje teplotu vzduchu v místnosti, ale samotnou změnu teploty má na starosti topení. Termostat i topení představují dva různé systémy.

V tomto typu není podstatné, kolik různých systémů je propojeno do zpětné vazby – jediným podstatným rysem je integrace systému informování a systému odpovědi na informaci.

Typickým pro tento přístup a zpětnou vazbou je:

- může být náročná na automatizaci;
- pravděpodobně zahrnuje i systémy mimo sledovanou oblast BAM;
- často se výrazně orientuje na interakci s člověkem.

Je lepší snažit se docílit tohoto stavu BAM řešení postupnými kroky, než hned mít od začátku 100 % reakcí spravováno přímo dashboardem. Zásadní rozdíl mezi příkladem s termostatem a skutečným BAM řešením je ve hloubce a šíři složitosti, inteligenci a znalostí BAM reakcí, které mohou pracovat s mnohem větším počtem nastavení a událostí.

3.6.3 BAM dashboard jako automatizovaný termostat

Příjemcem zprávy z BAM systému nemusí být vždy nutně jen člověk. Třeba dříve zmíněný centrální panel jaderné elektrárny – systémy v jaderných elektrárnách jsou výrazně automatizované, lidský zásah je vyžadován jen v minimu případů. BAM lze tedy použít jednak k automatickému varování pro lidské uživatele, ale stejně pro jiné další systémy, které jsou schopny lidskou činnost eliminovat.

Tentokráte vyměníme topení za klimatizaci, která obsahuje automatický termostat, který sleduje aktuální teplotu v místnosti a po dosažení konkrétní hodnoty vypne chlazení. Po dosažení jiné, stanovené teploty chlazení se později opět zapne. V průmyslu by se hodilo označení *stroj se zpětnou vazbou*. Samozřejmě BAM se zabývá business procesy namísto procesů mechanických. Využívá business pravidla, která definují, jak se má systém chovat při konkrétním rozpoložení hodnot sledovaných ukazatelů. Teoreticky je takto u dobře zmapovaných procesů snadné nahradit lidskou práci automatizovaným systémem.

Existují samozřejmě limity. Vždycky je potřeba umístit i mechanismy pro odstranění zacyklení. Například řídící jednotka motoru automobilu s tempomatem jej deaktivuje v momentě bezpečnostního lidského zásahu – řidič sešlápl brzdový pedál.

Tento přístup výrazně naráží na otázky přenesení odpovědnosti za rozhodování z lidí na automatizovaný systém. Současná generace lidí zřejmě takovému systému nikdy plně důvěřovat nebude, avšak současné děti, které vyrůstají ve společnosti počítačů, herních konzolí, chytrých telefonů aj., možná budou mít na tento přenos odpovědnosti BAM jiný názor a bude danému řešení přístupnější.

Tento přístup vystupuje sice jako plně automatizovaný, avšak stále v něm má uživatel, obvykle člověk, *právo veta*, tzv. *over-rule* na odstavení systému. Největším přínosem popisovaného typu reakcí tedy může být odfiltrování velkého množství *nezajímavých událostí*, které může systém řešit automaticky podle předpřipravených scénářů, a teprve *zajímavé události* přepošle k řešení uživateli. Díky tomu získá uživatel více prostoru pro řešení skutečně závažných situací a nemusí se rozptylovat rutinními, triviálními záležitostmi.

3.6.4 Řídící BAM

Cílem předchozího pojetí BAM je uvolnění rukou uživatelů BAM díky zabudovaným pravidlům pro vyhodnocování reakcí. Tento přístup se zaměřuje na tvorbu strategií pro BAM – poskytuje mnohem víc, než jen *odstřižení* člověka na spoluúčasti řízení, navíc nabízí flexibilní množinu

automatizovaných pokynů, které umožní člověku přijímat celkovou strategii pro reakce. Na každém uživateli pak leží volba konkrétního druh reakce – okamžitý zásah, eskalace problému nebo zjišťování dalších podrobností všechny, včetně odhadu rizika a případných dopadů na celý business.
Je to ukázkové manažerské paradigma, kdy manažer má k dispozici několik různých nástrojů a podle okolností, nebo vnitřních pocitů, nebo dřívějších zkušeností se rozhoduje, po kterém sáhne. Tento styl BAM reakce může poskytnout manažerovi před přijetím nezvratného rozhodnutí velmi přínosné informace. Reakční strategie avšak nezávisí jen na business pravidlech, nýbrž také na dalších hodnotách jakými jsou třeba morálka nebo etika.

Dojde-li k zobrazení varování na dashboardu, uživatel může spustit například přednastavený BPM tok, který jej provede sledem nejlepšího řešení dané situace. V závislosti na podmínkách může mít uživatel připravených těchto toků několik pro různé případy. Na rozdíl od předchozího přístupu, tento přístup vnáší do BAM odpovědi určitou míru vyvážení, neboť opět zapojuje člověka do procesu.

3.6.5 Adaptivní BAM

Předcházející 4 přístupy vypadají logicky a lze je vysvětlovat pomocí analogií o termostatech apod. Tento přístup jde ještě o kus dál, hlavně ve složitosti.

Adaptivní BAM se nespokojí jen s obyčejným generováním varování a vyvoláním automatické nebo lidské reakce podle předem daných pravidel, navrch přidává:

- učení se z minulých *zážitků*;
- implementací nových systémových pravidel;
- podporu uživatelů při řešení případů, kdy ještě žádná pravidla nejsou předem známa.

BAM se tak posunuje od čistě algoritmického modelu pracujícího s předdefinovanými procedurami kroku za krokem k modelu heuristickému se zaměřením na objevování, učení se a přizpůsobování se. Samotný systém je schopen tvořit vhodná řešení pro případy, které právě nově vznikly. Díky své složitosti se však jedná o vysoce exkluzivní produkt, určený převážně pro finanční instituce.

3.7 Funkcionalita BAM nástrojů

Pro snazší orientaci zákazníka mezi nabízenými BAM výrobky, rozděluje David Luckham jejich funkcionalitu do pěti kategorií (Luckham, 2005), překlad (Dokoupil, 2006):

1) ***Zpracování dat z událostí v reálném čase*** *(Real-Time Event Data Computation)* – nástroj s touto schopností umí zpracovávat události v reálném čase a agregovat je do metrik (KPI[34]). Tyto ukazatele poté zpřístupňuje uživateli v grafické formě nebo je poskytuje nějaké jiné aplikaci k dalšímu zpracování.
2) **Reakce na jednotlivé události** (Single Event Triggering) – nástroj dokáže reagovat na jednotlivé předdefinované události. Například při detekci kritické hodnoty KPI upozorní uživatele a poté provede akci podle předdefinovaného scénáře – např. poslání automaticky vygenerovaného e-mailu. Nástroj většinou uživateli umožňuje definovat pravidla pro reakci systému.
3) **Zpracování proudu událostí** (Event Stream Processing) – proud událostí je seřazenásekvence událostí. Tyto nástroje neumožňují kontrolovat pořadí, ve kterém nástroj události zachytí. Z proudu tedy nelze poznat vztahy mezi událostmi (které události vyvolaly jiné, které vznikly nezávisle) nebo čas jejich vzniku. Proto je nad událostmi možno provádět jen omezené operace (typicky logické operace *and* a *or*).

[34] KPI – Key Performance Indikator

4) ***Reakce na komplexní vzory událostí*** *(Complex Event Pattern Triggering)* – nástroje, které vyhovují tomuto zařazení, jsou schopné ve velkém množství událostí rozeznat složité vzory a reagovat na ně. Tyto vzory mohou obsahovat zároveň události vzájemně nějakým způsobem související i události nezávislé. (Systém může například zachytávat vzory aktivit konkurenta nebo dodavatele). Aby takové složité vzory mohly být použity, musí si nástroj u každé z událostí zapamatovat např. její příčinný vztah k jiné události, její nezávislost nebo čas jejího vzniku. Tato *genetická informace* události je poté klíčová při detekci vzorů.
5) ***Abstrakce vzorů událostí*** *(Event Pattern Abstraction)* – nástroje, které svou funkčností spadají do této kategorie, mohou jít ještě o kus dál. Mohou nabízet nástroje k tvorbě nových událostí, které vzniknou, kdykoliv nástroj zachytí nějaký konkrétní vzor. Nové události do své *genetické informace* mohou zapsat i údaje ze vzorů, kterými byly vyvolány, a mohou být dále zpracovány jako obyčejné události. Důležitá data se do nové *abstraktní* události zkopírují a nepodstatná vypustí. Nástroje s touto funkcionalitou by mohly nejvyššímu vedení podniku poskytovat cenné informace i o velmi složitých podnikových procesech.

3.8 Výrobci a dodavatelé BAM nástrojů

BAM řešení nabízí několik různých přístupů na pořízení, lze jej vyhotovit jako *in-house* řešení vlastními silami v rámci podniku, lze jej zakoupit jako samostatnou aplikaci, nebo jako součást většího balíků podnikových aplikací. Všichni výrobci, kteří nabízejí balíky BPM řešení, zahrnují i BAM funkcionalitu. Přesně tohle představuje nejběžnější zdroj BAM nástrojů pro podniky. Balíková řešení business aplikací stále častěji zahrnují i BAM funkcionalitu, ale mnoho z nich se omezuje pouze na sledování dat v rámci svého řešení. Kdykoliv není požadována nízká latence, BAM řešení lze vytvořit z platformy BI nástrojů pro vytvoření BAM aplikací.

Mezi dodavatele BPM řešení včetně BAM funkcionality patří – *IBM/WebSphere*, *Oracle*, *Microsoft*, *Software AG*, *Tibco and Vitra, IDS Sheer*.

Dodavateli BAM jako samostatné aplikace jsou *SL* a *Systar*.

Dalšími je skupina dodavatelů s výrobky se zaměřením na komplexní zpracování událostí. Tyto výrobky mohou být použity na vybudování BAM řešení. Dodavatelé jsou *Aleri*, *Event Zero*, *Progress / Apama*, *StreamBase* a *Truviso*.

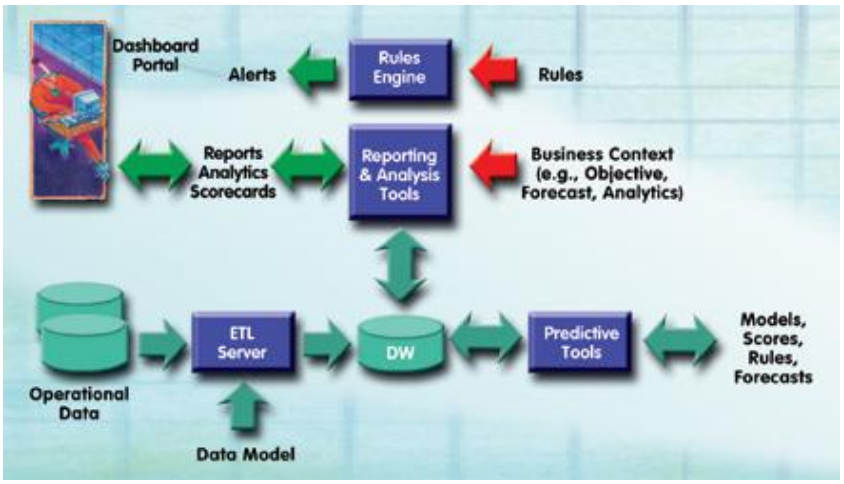
V poslední době také stoupá počet speciálních aplikací postavených na CEP[35] používajících BAM techniky pro bezpečnost, detekci podvodů, sledování okolí, analýzu clickstreamů aj.

[35] CEP – Complex Event Processing

4 Podobnosti a odlišnosti BAM & BI

Článek *BAM and Business Intelligence* (White, 2003) hezky popisuje základní rozdíly v chování systémů BI a BAM.

4.1 Business Intelligence



Obrázek 8: BI Framework (White, 2003)

Systémy BI jsou sestaveny z ETL[36] serveru a nástrojů pro tvorbu reportů (viz obrázek). ETL server sbírá data z transakčních systémů, transformuje je a ukládá do datových skladů (DW[37]). Reportovací nástroje si potom sahají na agregovaná data v DW a nechávají uživatele vytvářet parametrizované nebo ad hoc analýzy.

Tvůrci DW celkem brzy zjistili, že pokud chtějí data skutečně analyzovat, budou potřebovat něco více než jen obyčejné reportování a analýzy. Ve snaze zlepšit ROI[38] vznikly nástroje typu OLAP[39] pro práci s multidimenzionálně uloženými daty. Od doby, kdy byly BI nástroje doplněny o možnost zobrazování informací přes webové rozhraní, velmi se usnadnilo poskytování business reportů a analýz téměř komukoliv v personalizovaném podání.

K analytickým nástrojům BI byly časem přidány možnosti sledování a řízení výkonu. Uživatel může snadno porovnávat aktuální stav s požadovanými cíly. Vylepšením těchto nástrojů může být i automatické sledování stavů, jejich porovnávání s nastavenými prahy a automatické upozornění uživatele, který tak nemusí trávit čas ruční analýzou a snadněji může reagovat na potíže v business procesech. Tyto nástroje se v obrázku nazývají *predictive tools*. Jejich použití nabízí využití *data miningu* a předpovídání chování na základě modelů chování.

Obrázek *BI Framework* ukazuje možnosti nasazení BI na strategické a taktické úrovni řízení. Přestože by se mohlo zdát, že tento model lze užít i na každodenní monitorování operačního řízení podniku, není to úplně možné a je potřeba zajistit dodatečné kapacity a zdroje.

[36] ETL – Extract, Transform & Load

[37] DW – Data Warehouse

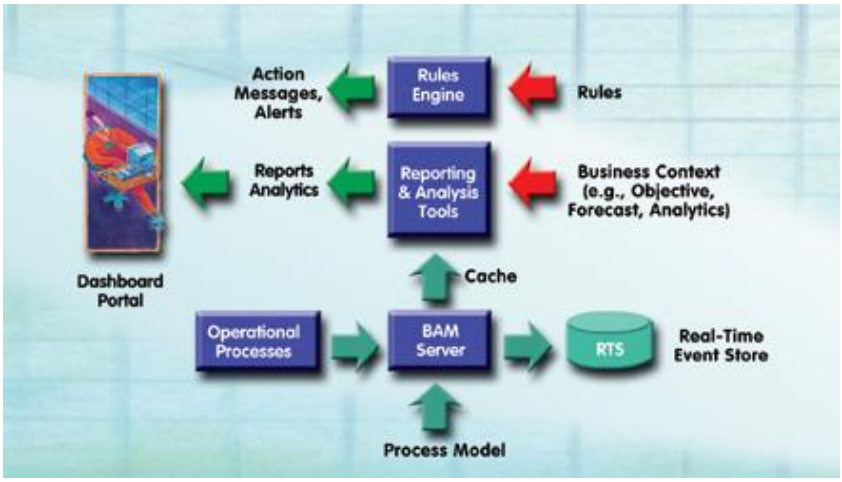
[38] ROI – Return on Investment

[39] OLAP – On-line Analytical Processing

Prvním krokem přiblížení BI nástrojů možnostem operačního řízení je nasazení úložišť dat s nízkou latencí - ODS[40]. Aktualizace těchto dat, samozřejmě závisí na nastavení, se pohybuje v řádu od dnů až po minuty. Právě rostoucí poptávka po přeměně datových úložišť v ODS vede také ke změnám v ETL, kde již nestačí obyčejné dávkové zpracování, ale je nutné data načítat co nejrychleji (sledování webových klikání, logování, messaging…).

4.2 Business Activity Monitoring

Z předchozího je zřejmé, že BI scházejí nástroje *performance managementu*. Nástroje BI nenabízejí dostatečnou kvalitu pro správu a řízení business procesů na operační úrovni, obzvláště pokud je vyžadována reakce v téměř reálném čase. BAM tohle umí.



Obrázek 9: BAM Framework (White, 2003)

Obrázek *BAM Framework* možná vypadá na první pohled hodně podobně, ne-li stejně, přesto se v něm jisté podstatné odlišnosti najdou. Nejviditelnější je zřejmě záměna ETL serveru BAM serverem, který sleduje a zachytává *události*, které se vážou na operační procesy. Tyto události je možné ukládat na RTS[41], který lze použít pro tvorbu DW.

Původ událostí je celkem pestrý. Mohou být shodné s těmi, jež zachytává ETL nebo integrační server; mohou být i hardwarového původu, kdy zdrojem je například ATM[42] nebo POS[43] terminál; mohou být z aplikací, kdy vznikají na základě transakcí atd.

BAM aplikace sledují každodenní business procesy, jakými jsou objednávky zákazníků, zajištění pohledávek či operace dodavatelského řetězce.

BAM nástroje jsou typicky řízeny na základě procesních modelů. Tohle představuje významnou odlišnost od datově řízeného ETL, které má buď velmi malé, ale spíše nemá žádné ponětí o business procesech. Jak BAM sleduje události z provozu, uchovává si tyto události ve vyrovnávací paměti, která se používá jako reportovací a analytický systém ve správě BAM serveru. Analytická část BAM může přistupovat k existujícím datům v BI a DW, aby je mohla nadále sledovat v rámci business procesu, dávat je do kontextu a generovat skóre výkonnosti operačních procesů. Některé BAM nástroje umožňují i detailně analyzovat a dolovat data z RTS.

---

[40] ODS – Operational Data Store

[41] RTS – Real-Time Store, podrobnosti lze najít v článku (LeHong, 2009)

[42] ATM – Automated Teller Machine, běžný bankomat

[43] POS – Point of Sale, pokladna

Výsledky analýz a reportů BAM obvykle zobrazuje na konzoli, přístrojové desce nebo portálu. Lze je také spojit s dalšími pravidly a prahovými hodnotami, a potom jsou schopny automaticky varovat při výskytu obtíží odpovědného business uživatele, nebo může vytvořit jinou zprávu, která upraví činnost business procesu, popřípadě spustí transakci. Veškeré BAM řízení a analýzy jsou prováděny v jediném integrovaném prostředí, které zajišťuje dostatečnou škálovatelnost, spolehlivost a vysokou výkonnost.

Klíčovým přínosem BAM prostředí pro podnik je možnost neustálého monitorování a téměř okamžité reakce procesního řízení na nově vyvstalou výjimku v běhu. Příklady nasazení a užití BAM aplikací ve skutečném business prostředí.

Finance	Výroba	Zdravotnictví	Obchod	Doprava
Řízení portfolia	Order Management	Real-time upozornění na stav pacienta	Single customer store	Ceny vstupenek
Detekce podvodů	Kontrola kvality	Varování na ohniska nákaz	Analýza zásob	Sledování výkonu letadel
Risk Management	Sledování pohybu just-in-time zásob	Varování mimořádných událostí	Real-time marketing	Detekce podvodů
Real-time Marketing	Odhady prodeje podle stavu výroby	Reklamace a podvody	Vracení výrobků	Sledování a trasování nákladních vozidel
Automatické schvalování úvěrů	Vracení výrobků			

Tabulka 4: Ukázky BAM nasazení (White, 2003)

4.3 Vztah BAM & BI

Systémy Business Intelligence postavené na technologii datových skladů mají se systémy BAM mnoho společného. Oba systémy jsou především určeny pro podporu manažerského rozhodování.

Doménou systémů BI je typicky práce s historickými daty a spouštění komplexních analýz na těchto datech. Výsledky této činnosti se používají jako podpora rozhodování převážně na strategické úrovni a slouží vrcholovému vedení podniku jako podklady k tvorbě globální dlouhodobé podnikové strategie. Jednoduše ukazují, co se dělo včera, děje dnes, a odhaduje, co by se mohlo dít zítra analýzou dat, odhalováním trendů, pochopením chování zákazníků, hledáním nových příležitostí pro byznys.

BI nástroje a systémy jsou zaměřeny především na analýzu trendů a businessu.

Na rozdíl od BI je BAM řízen událostmi a nepracuje s historickými daty, ale převážně s daty aktuálními.

Produkty BI jsou obvykle chápány jako nástroje pro zpracování historických dat posbíraných z datových skladů s nemožností jejich následné změny. BAM se oproti tomu liší ve třech podstatných věcech:

- BAM nástroje a systémy jsou řízeny *business událostmi*, data získávají přímo z OLTP transakčních systémů nebo nástrojů procesního managementu; výjimečně, spíše nikdy z databází;
- BAM nástroje a systémy zobrazují data v real-time zobrazení nezávisle na tom, zda uživatel obnovuje zobrazení nebo nastavuje automatickou aktualizaci;
- BAM nástroje a systémy jsou *procesně orientované*.

Orientován je primárně na podporu rozhodování vedoucích pracovníků na operativní úrovni podniku. Například vedoucí dílny potřebuje mít přehled o rychlosti výroby, aby v případě, že vyrábí pod plán, mohl zajistit dodatečné výrobní kapacity.

BAM nástroje a systémy jsou speciálně navrženy pro sledování automatických procesů systému a vyvolání akce na základě přednastavení nebo vzoru chování.

BAM a BI se mohou vzájemně doplňovat. Konkrétně – historická data z BI mohou být podkladem pro vytvoření prahů a pravidel varování nebo spouštění činností v BAM. Příkladem může být pozdržení odchozích nebo příchozích podezřelých plateb z nebo do nebezpečných oblastí. Pokud BAM zachytí pokus o transakci s chováním popsaným ve scénáři, automaticky ji pozastaví a informuje odpovědného pracovníka pro ruční akci, včetně dalšího sledování doby trvání od započatí transakce s možností generovat případně pro odpovědného pracovníka varování, že transakce je pozastavena a předána k ručnímu zpracování a do konce zákonné lhůty pro zpracování transakce zbývá kritický čas.

5 Podobnosti a odlišnosti BAM & BSM

Pokud jsem o BI hovořil jako o horní hranici, pak o BSM hovořím jako o spodní hranici. v nejobecnější rovině jsou si koncepty BAM a BSM rovny, avšak případy použití, zdroje dat, typy pravidel i cílová skupina uživatelů se liší (Gassman, a další, 2009).

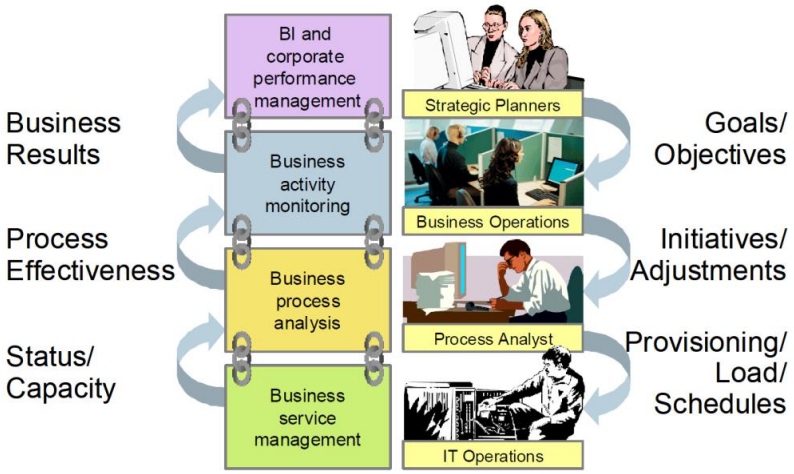
Obojí, business i oddělení operačního IT, mají požadavky na sledování důležitých ukazatelů výkonnosti podnikových procesů, avšak každé řeší odlišné problémy, a proto potřebují odlišné nástroje pro různá řešení. Zatím neexistuje produkt, jenž by uspokojil všechny potřeby business a operačního IT a hned tak zřejmě existovat nebude. Přesto technologie, které umožňují real-time monitorování, jsou shodné, jen dostupná řešení se liší.

BAM se zaměřuje na business procesy, business události, poskytuje business uživatelům přístup v reálném čase jak k reportům, tak k analýzám. BSM se zaměřuje na IT procesy a události pocházející ze základní IT infrastruktury podnikových komponent a aplikací. Poskytuje pracovníkům operačního IT přístup k IT indikátorům a analýzu vlivu businessu na IT v reálném čase.

Přestože BSM náleží do sféry vlivu operačního IT a BAM do businessu, obojí dohromady lze spojit ve větší celek, který zahrnuje řízení podnikových procesů a podnikové výkonnosti.

Obě disciplíny jsou ve většině podniků pečlivě odděleny, avšak využívají stejný technologický základ a sdílejí stejné potřeby pro analýzy související s *jedinou podnikovou pravdou* napříč všemi odděleními organizace. Tvůrci podnikových strategií pracují s nástroji pro řízení podnikové výkonnosti a modelují strategie na základě periodických obrázků business aktivit. Cíle a předpovědi vzniklé na strategické úrovni řízení propadají do nižší úrovně řízení – operační, kde se je organizace snaží naplnit konkrétními automatizovanými nebo lidskými procesy. BAM se stará o spojení mezi operačními business manažery a end-to-end business procesy, zajišťuje informace o efektivitě procesů a nabízí podporu při upravování procesů k naplnění aktuálních cílů podle aktuálních změn v business modelech. Operační business manažeři tedy nastavují procesy (ať už formálně, nebo ad hoc) a také je vykonávají. Procesní analytici mohou využít metrik, které jim BAM nabízí, avšak navíc potřebují ještě další specializované nástroje, kterými jim ohlídají technické ukazatele, jako je například délka fronty v procesním modelu. Navíc si musejí analytici hlídat aktuální vytížení a volné kapacity služeb business infrastruktury, která zajišťuje chod automatizovaných procesů.

BSM je část operačního IT provozu, která se zaměřuje na sledování výkonu aplikací a koncových komponent, které tvoří technické řešení pro business služby. Personál IT provozu stanovuje na základě metrik z BAM a řízení podnikových procesů priority na kapacity a řešení problémů.



Obrázek 10: Monitorování napříč podnikem (Gassman, a další, 2009)

Nástroje pro monitorování ve skutečném čase mají technologicky i technicky mnoho společného. Informace jsou ze sledovaného prostředí získávány prostřednictvím senzorů, toků událostí, či logovacích záznamů. Zpracováním těchto informací je zabezpečeno hlídání stálého provozu a zachytávání neobvyklých situací, vypočítávání metrik, vyhlašování varování v případě překročení stanovených limitů, či poskytování základních příčin a analýz dopadů. Výstup zprostředkovávají různé konzole, přístrojové desky, zprávy či varování. Rozdíly jsou především ve velikosti a složitosti toho, co je řízeno a v dovednostech a odpovědnostech koncových uživatelů a kupujících.

Snaží-li se prodejce dodat řešení oběma skupinám (koncovým uživatelům i kupujícím), nutně k tomu potřebuje odlišné marketingové a prodejní strategie. Někteří ze současných prodejců se o to již pokusili, avšak žádný z nich není lídrem obou trhů současně.

5.1 Business Service Management

5.1.1 Definice

Business Service Management je druh softwaru pro podporu provozu IT, který se snaží dynamicky propojovat kapacitu a výkon základní IT technologické infrastruktury podniku spolu s aplikačními komponentami business-orientovaných služeb k zajištění chodu business procesů. Aby mohl být produkt kvalifikovaný jako nástroj BSM kategorie, musí jednak vyhovovat výše popsané definici a dále uchovávat a vizualizovat topologii IT služeb pomocí objektového modelu a udržovat vztahy typu rodič-potomek a ostatní asociace napříč všemi zapojenými IT komponentami. BSM produkty musejí získávat real-time data o aktuálním stavu ze základních aplikací a komponent IT, a to buď přímo nebo prostřednictvím stanovených monitorovacích nástrojů, jakými jsou distribuované systémy nebo mainframe systémy pro korelaci a analýzu událostí (*event correlation and analysis*), plánování úkolů, a v některých případech použití nástrojů pro sledování výkonu. BSM nástroj potom takto získaná data porovnává vzhledem k objektovému modelu, vypočítává míru jeho *zdraví* a váží případné odchylky namísto toho, aby jen stroze informoval o stavu IT. Výsledky statutu business služeb potom obvykle zobrazuje v plně grafickém prostředí.

5.1.2 Typický uživatel

- *IT operations manager;*
- *IT service delivery manager;*
- *director of IT infrastructure and operations.*

5.1.3 Případ užití

Komponentní přístup v IT infrastruktuře a operačním managementu bývá jen málokdy sladěn s business jednotkami. IT infrastrukturu je potřeba řídit v souvislosti s dostupností a výkonností end-to-end IT business služeb, které infrastruktura zabezpečuje. Podle definice Garnterů a ITIL[44] musí být IT služba zaměřená na zákazníka, spadající do business služeb, které v podniku podporují business procesy.

Zaměření na zákazníka znamená jednak doslova zaměření na externí zákazníky, kteří přímo přinášejí podniku peníze, a jednak na interní zákazníky, kteří jsou důležití pro dosahování podnikových cílů. V závislosti na *maturity level*[45] čelí často IT organizace obtížím při popisování IT služeb, které poskytují. Často se chybně za IT služby označují *systémová administrace*, *VoIP*[46] nebo *záloha/obnova dat*. Přestože se jedná o důležité technické služby, žádná z nich nemůže být

[44] ITIL – IT Infrastructure Library

[45] Maturity level – vyspělost, vyzrálost procesů v podniku

[46] VoIP – Voice over IP, IP telefonie

považována za IT službu, neboť nevyhovuje definici – schází především výstup na zákazníka. Správným příkladem business IT služby zaměřené na zákazníka je *služba elektronického obchodování* nebo služba *quote-to-cash*[47], které se skládají z aplikací IT infrastruktury, lidí a procesů, které Q2C služby zahrnují. BSM nástroje mohou pomáhat IT pracovníkům při prezentování aktuálního stavu IT služeb přes business dashboard jak IT oddělením, tak business oddělením. BSM lze úspěšně nasadit do organizace s procesně vyzrálými IT službami.

BSM nutně potřebuje:

- předem definované business IT služby;
- dobré pochopení logických propojení mezi IT komponentami a IT službami, které jsou na komponentách provozovány;
- vyzrálé změnové řízení procesů pro aktualizaci služeb;
- dobré nástroje sledování IT komponent a IT služeb.

Spojení komponent IT infrastruktury a business IT služeb představuje klíčový prvek BSM. I když se toto spojení často provádí ručně pomocí *drag-and-drop*, *copy-and-paste* nebo jinými technikami *importování*, schopnost odhalit logické vazby a závislosti IT služeb a detekovat změny v těchto propojeních výrazně zlepšuje nasazení BSM. Existují také nástroje pro automatizované mapování závislostí IT služeb, nejsou však všelékem a stále se najde dost případů, kdy je vyžadována ruční konfigurace.

Budeme-li předpokládat vyzrálý základ, možné případy využití BSM zahrnují:

- identifikaci IT služeb ovlivněných poruchou IT komponenty – výsledkem je zlepšení dostupnosti služeb a snížení časů odstávek, protože podpora IT se může téměř okamžitě zaměřit na řešení *správných* business problémů vysoké priority; pokazí-li se více věcí, rozhodování o pořadí jejich řešení lze provést *inteligentněji s* lepší alokací zdrojů IT podpory;
- zkrácení MTTR[48] sledováním vizuální reprezentace závislostí od IT služeb k business aplikacím a komponentám IT infrastruktury (servery, úložiště, sítě, middleware, databáze) s cílem zjistit primární příčinu problémů IT služeb;
- prezentování business zobrazení toho, jak dobře si vedou IT služby na podporu klíčových business procesů – toto umožňuje zlepšení komunikace mezi IT a jejími business zákazníky, zvýšení spokojenosti zákazníka, zvýšení důvěryhodnosti IT jasným demonstrováním vlivu podpory IT služeb na podnikové business procesy a vytvoření základu pro odesílání kvalitních událostí s vlivem na business služby pro systémy BAM.

5.1.4 Dodavatelé

Ukázka několika dodavatelů BSM řešení – *ASG*; *BMC Software*; *CA*; *Compuware*; *HP*; *IBM Tivoli*; *Interlink Software*; *Nimsoft*; *Novell (Managed Objects)*; *Quest Software*; *Systar*; *Tango/04*; *USU*.

5.2 BAM

5.2.1 Definice

BAM je styl monitorování, který nabízí přímý přístup ke klíčovým ukazatelům business výkonnosti, statutu a aktuální situace, které jsou průběžně aktualizovány událostmi a dalšími artefakty vznikajícími v běžících business procesech. BAM se používá ke zvýšení rychlosti a účinnosti business procesů citlivých na čas prostřednictvím sledování toho, co se právě děje, a zkracováním

[47] Quote-to-Cash – Q2C, tvorba cenové nabídky pro zákazníka

[48] MTTR – Mean Time to Repair

času mezi vznikem nebezpečné události a přijetím jejího řešení prostřednictvím vyvoláním varování. Typicky je součástí BAM je dashboard, který zobrazuje aktuální stavy a porovnává jejich hodnoty s historickými nebo předpokládanými daty.

5.2.2 Typický uživatel

Typickým uživatel je buď vlastník business procesu, nebo jeho spolupracovník. Oba vyžadují neustálé sledování průběhu činností a stavů v business procesu a možnost rychle reagovat na riziko či příležitost. Každý zaměstnanec podniku, řidičem nákladního vozu počínaje, viceprezidentem operačního oddělení konče, může těžit při uvědomění si možností, které BAM nabízí, avšak pouze za předpokladu, že mají dashboard nastaven na míru požadavkům odpovídajícím jejich práci a roli. Informace z BAM nástrojů mohou být velmi přínosné pro pracovníky operačního IT, kteří díky nim mohou snáze pochopit význam různých úrovní IT služeb pro celkový business.

5.2.3 Případ užití

Typické je užití v logistickém dodavatelském řetězci, řízení vztahů se zákazníky, *event-based marketing*[49], řízení compliance rizika, či odhalování podvodů aj. Typická aplikace obsahuje zobrazení aktuálního stavu, detekci činností mimo sekvenci, vyhodnocení rizika scházejících termínů a nebo úrovně služeb, odhad potenciálních problémů se zásobami a kapacitami zdrojů.

5.2.4 Dodavatelé

Viz kapitola *Výrobci a dodavatelé BAM nástrojů*.

[49] Event-based marketing – cílený marketing, využívá příležitostí na straně klienta (např. narozeniny atd.)

6 Návrh řešení podpory AML[50] v prostředí banky pomocí BAM

Aby má práce nebyla zamřená jen teoreticky, rozhodl jsem se pokusit se o praktickou ukázku eliminace podnikového business rizika nasazením BAM. Jako velmi vhodné a zajímavé se mi jeví prostředí finančních institucí, konkrétně bank, které se musejí přizpůsobovat dohledu regulátorů a povinnostem vyplývajícím ze zákonů. Poslední rok byl pro české bankovní prostředí velmi výživný, neboť účinnost nabyly hned tři zákonné předpisy.

Nejvíce svoji pozornost zaměřím především na *zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu* (ČR, 2008) (AML). Dalšími dvěma zákony, které mají přímý vliv na chování bank a jsou spjaty s AML jsou *zákon č. 284/2009 Sb., o platebním styku* (ČR, 2009) a *zákon č. 40/2009 Sb., trestní zákoník* (ČR, 2009). Zmíněné zákony vymezují celkem přesný rámec chování i postihy a jejich naplnění ze strany bank poskytuje velmi vhodnou příležitost pro ukázku nasazení podpory BAM.

Každé podnikání s sebou přináší určitá rizika, která mohou být pro daný obor dána jednak samotným konkurenčním prostředím a jednak vnější regulací – zákony. Obzvláště pro banky existuje nezanedbatelný *compliance risk*, čili riziko nedodržení platné legislativy a případný postih regulátora i trhu. Regulátoři, v tomto případě Ministerstvo financí (MF ČR), Česká národní banka (ČNB) či Policie ČR (PČR), mají k dispozici hned několik účinných nástrojů pro sankcionování a rozhodně se je nebojí použít. Dalším postihem pro banku je pak ztráta dobré pověsti na trhu. Bankám tedy nezbývá než se snažit sladit své chování s požadovanými předpisy, aby všem svým povinnostem dostály a eliminovaly tím možnost postihu.

6.1 Postup práce

Rozpracování konceptuálního návrhu podpory *compliance managementu* s využitím BAM budu řešit v několika fázích.

1. **Identifikace zdrojů** – nejprve bude nutné identifikovat všechny potenciální zdroje podkladových materiálů. Velká část podstatných informací je v samotném zákoně, především AML[51], který obsahuje definice pojmů, popis žádaného chování a sankční část při porušení povinností ze zákona vyplývajících. Výhodou zákona je explicitní vyjádření a snaha zákonodárců o jednoznačný výklad[52], což by mohlo výrazně napomoci při hledání podstatného. Dále budu pracovat s popisem/odhadem současného řešení řízení rizik při aplikaci AML a s popisem požadovaného stavu (včetně podpory BAM) podle představ pracovníků compliance.[53]
2. **Identifikace rizik** – dále se pokusím identifikovat a popsat rizika vyplývající pro banky z AML a souvisejících zákonů, tato rizika poté konzultovat s *compliance officer (CO),* popřípadě je rozšířit o další jím definovaná rizika vycházející z jeho dalších poznatků a zkušeností. Další rizika bude třeba hledat v současném a požadovaném stavu řešení řízení rizik spojených s AML. U každého rizika bude nutné definovat jeho podstatu, ohodnotit jeho nebezpečnost, identifikovat dotčené bankovní procesy a identifikovat všechny aktéry.
   Bohužel bankovní business procesy spadají pod hned několik různých tajemství –

[50] AML – anti money laundering; zákon č. 253/2008 Sb. v platném znění

[51] Celé znění zákona AML je k dispozici v příloze.

[52] Čeština sice není diskrétní jazyk umožňující pouze jediné možné vysvětlení, avšak v případě AML lze v tomto směru hovořit o úspěchu. Zákon je přehledný, srozumitelný a těžko se v něm hledá *další* výklad.

[53] Oba popisy (současný i požadovaný stav) jsou k dispozici v příloze.

obchodní, bankovní, v neposlední řadě pak povinnost mlčenlivosti vyplývající z AML, a proto bude nástin průběhu procesů nastaven obecně. Ostatně chci-li se držet obecné roviny návrhu podpory, je tento přístup vhodnější.

3. **Návrh detekce rizik** – zákony obsahují demonstrativní výčet typického chování při pokusu o legalizaci výnosů z trestné činnosti, proto se pokusím navrhnout vhodnou formu jejich detekce.
4. **Modely** – procesní modely rizikových oblastí.
5. **Návrh BAM** – poslední fází je návrh dashboardu pro oddělení compliance.

Řešit daný problém budu pouze v rovině bank[54], tj. peněžních operacích – *hotovostní* a *bezhotovostní transakce* a *vznik nových obchodních vztahů* – otevření účtu; nebudu se zabývat jinými finančními institucemi (pojišťovny, penzijní fondy, stavebními spořitelnami atd.) ani jinými produkty či službami. Primárně se budu orientovat na fyzické osoby. Odlišnosti uplatňování AML u fyzických osob a právnických osob jsou nepatrné, přesto jsou, avšak nebudou v textu zmíněny. Důvodem je snaha udržet míru podrobnosti, přehlednosti a srozumitelnosti.

6.2 Identifikace zdrojů

Nejbohatším zdrojem informací je nepochybně AML, ke kterému je BAM podpora směřována. Avšak v širších souvislostech je nutné zmínit část zákona o platebním styku, který nabyl účinnosti dnem 1. 11. 2009, konkrétně mám na mysli povinnost banky provádět peněžní transakce ve stanoveném časovém limitu. Druhým zákonem je nový trestní zákoník, který nabude účinnosti dnem 1. 1. 2010 a ke všem potenciálním sankcím definovaným v AML přidává navíc i osobní odpovědnost zaměstnance a možnost zbavení ho svobody na základě naplnění skutkové podstaty nedbalostního trestného činu, který se v zákoně objevuje nově.

Mnohá rizika bude možné jistě hledat i v současném pojetí řízení rizik spojených s AML bankami. Netvrdím, že se jedná o přesný popis, to rozhodně ne. Jedná se spíše o odhad, neboť přesný popis žádná banka nezveřejní – jednak z důvodu ochrany svého know-how a jednak i z důvodu prevence pokusů o trestnou činnost – obcházet či prolamovat bezpečnostní mechanismy lze snáze, pokud víme, jak vnitřně pracují.

Jedna věc je samotný zákon AML a jeho požadavky na banku a jiná věc je skutečně vhodná podpora ze strany BAM a IT. Proto důležitý podklad pro práci představují představy CO a mé, jak by se měl výsledný systém chovat – funkcionalita a prezentace informací. Podstatný pro mou práci bude i dokument o požadovaném stavu.

6.3 Identifikace rizik

6.3.1 §43 Porušení povinnosti mlčenlivosti

§38 odst. 1 *Nestanoví-li tento zákon jinak, jsou povinné osoby a jejich zaměstnanci, zaměstnanci ministerstva, zaměstnanci ostatních dozorčích úřadů a fyzické osoby, které jsou pro povinnou osobu, ministerstvo nebo jiný dozorčí úřad činné na základě jiné než pracovní smlouvy, povinny zachovávat mlčenlivost o skutečnostech, týkajících se oznámení a šetření podezřelého obchodu, úkonů učiněných ministerstvem nebo plnění informační povinnosti stanovené v §24.*

Podstata rizika:

- žádná osoba, vyjma relevantních zaměstnanců banky, zejména klient, se nesmí dozvědět, jak je který klient posuzován bankou
  (*běžný klient* vs *potenciálně problémový klient*)

[54] §2 odst. 1 písm. a) bod 1.

- žádná osoba, vyjma relevantních zaměstnanců banky, zejména klient, se nesmí dozvědět, že na klienta bylo podáno oznámení na FAÚ[55] a je vyšetřován

Nebezpečnost:

- uložení pokuty v rozmezí 200 000 – 1 000 000 Kč
- reputační riziko pro banku

Dotčené bankovní procesy:

- hotovostní transakce
- bezhotovostní transakce
- vznik obchodního vztahu

Aktéři:

- pracovníci front-office
- někteří pracovníci back-office
- pracovníci compliance

Řízení rizika:[56]

- neinformovat klienta
- neinformovat pracovníky o jakémkoliv vývoji hlášení
- pouze v případě nezbytnosti informovat relevantního pracovníka
- systémově zabezpečit komunikaci o hlášeních a oznámeních v souvislosti s AML
- pravidelně školit pracovníky v dané oblasti

6.3.2 §44 Nesplnění povinností při identifikaci a kontrole klienta

§7 odst. 1 *Jestliže je povinná osoba účastníkem obchodu v hodnotě převyšující částku € 1 000, před jeho uskutečněním vždy identifikuje klienta, pokud tento zákon dále nestanoví jinak.*

§7 odst. 2 *Bez ohledu na limit stanovený v odstavci 1 identifikuje povinná osoba klienta rovněž vždy, pokud jde o*

a) podezřelý obchod,

b) vznik obchodního vztahu,

§16 odst. 1 *Identifikační údaje získané podle § 8 odst. 1 a 2 nebo na základě přímo použitelného předpisu Evropských společenství, kterým se stanoví povinnost doprovázet převody peněžních prostředků informacemi o plátci, kopie dokladů předložených k identifikaci, byly-li pořizovány, údaj o tom, kdo a kdy provedl první identifikaci klienta, dokumenty odůvodňující výjimku z identifikace a kontroly klienta podle § 13, a v případě zastupování originál nebo ověřenou kopii plné moci, uchovává povinná osoba po dobu 10 let od ukončení obchodního vztahu s klientem.*

§16 odst. 2 *Údaje a doklady o obchodech spojených s povinností identifikace uchovává povinná osoba nejméně 10 let po uskutečnění obchodu nebo ukončení obchodního vztahu.*

§16 odst. 4 *Lhůta podle odstavců 1 až 3 začíná běžet prvním dnem kalendářního roku následujícího po roce, ve kterém byl uskutečněn poslední úkon obchodu známý povinné osobě.*

---

[55] FAÚ – finančně-analytický útvar Ministerstva financí ČR; má na starosti řešení oznámení od bank a jiných povinných osob.

[56] *Ten, kdo chce zachovat tajemství, musí zachovat tajemství, že má tajemství k zachování.* (Lynn, a další, 2003)

Podstata rizika:

- zákonem jsou definována přesná pravidla, kdy je potřeba provést identifikaci/kontrolu klienta (přesná znění identifikace je v §8, kontroly v §9)
- v závislosti na výsledku identifikace a kontroly je vyžadováno další chování ze strany banky (§15)
- je přesně stanovena lhůta, po kterou je nutné uchovávat identifikační údaje o klientovi a jeho obchodech

Nebezpečnost:

- uložení pokuty v rozmezí 1 000 000 – 50 000 000 Kč
- reputační riziko pro banku
- nedbalostní trestní čin

Dotčené bankovní procesy:

- hotovostní transakce
- bezhotovostní transakce
- vznik obchodního vztahu

Aktéři:

- pracovníci front-office
- někteří pracovníci back-office

Řízení rizika:

- nastavit práh citlivosti v systému pro obchody nad € 1 000 a zároveň zkoumat chování klienta z hlediska podezřelých obchodů
- automatická kontrola klienta před vznikem vztahu/provedení transakce proti databázím WorldCheck a black-listům
- odmítnutí provedení transakce na základě nesoučinnosti klienta či podezření
- stanovení akceptovaných důvěryhodných dokladů pro ověření totožnosti klienta
- proškolení zaměstnanců
- nastavení mandatorních polí v systému zpracovávajícím transakci
- nastavení časového zámku/prodlevy při transakci

6.3.3 §45 Nesplnění informační povinnosti

§24 *Povinná osoba na žádost sdělí ministerstvu v jím stanovené lhůtě údaje o obchodech souvisejících s povinností identifikace nebo ohledně nichž ministerstvo provádí šetření, předloží doklady o těchto obchodech nebo k nim umožní přístup pověřeným zaměstnancům ministerstva při prověřování oznámení a poskytne informace o osobách, které se jakýmkoliv způsobem účastnily takových obchodů.*

Podstata rizika:

- banka musí poskytnout součinnost FAÚ při řešení oznámení (i z jiné banky nebo jiného orgánu)[57]

Nebezpečnost:

- uložení pokuty v rozmezí 1 000 000 – 50 000 000 Kč
- reputační riziko pro banku

[57] Banka samozřejmě musí poskytnout součinnost i PČR, exekutorům, notářům a dalším, kterým toto právo poskytuje jiný zákon než AML.

Dotčené bankovní procesy:

- *žádný*

Aktéři:

- compliance

Řízení rizika:

- umožnit CO generovat reporty o historii chování klienta
- v rámci zachování mlčenlivosti nechat součinnost co nejvíce na CO

6.3.4 §46 Nesplnění oznamovací povinnosti

§46 odst. 1 Povinná osoba se dopustí správního deliktu tím, že neoznámí ministerstvu podezřelý obchod.

Podstata rizika:

- banka musí povinně oznamovat všechny podezřelé obchody

Nebezpečnost:

- uložení pokuty v rozmezí 5 000 000 – 50 000 000 Kč
- reputační riziko pro banku
- nedbalostní trestní čin

Dotčené bankovní procesy:

- hotovostní transakce
- bezhotovostní transakce
- vznik obchodních vztahů

Aktéři:

- pracovníci front-office
- někteří pracovníci back-office
- compliance

Řízení rizika:

- školení pracovníků
- aktivní automatizovaná detekce chování klienta podle zákonem definovaných modelů

6.3.5 §47 Nesplnění povinnosti odložit příkaz klienta

§20 odst. 1 *Pokud hrozí nebezpečí, že bezodkladným splněním příkazu klienta by mohlo být zmařeno nebo podstatně ztíženo zajištění výnosu z trestné činnosti nebo prostředků určených k financování terorismu, povinná osoba může splnit příkaz klienta týkající se podezřelého obchodu nejdříve po uplynutí 24 hodin od přijetí oznámení podezřelého obchodu ministerstvem. Majetek, jehož se příkaz klienta týká, vhodným způsobem zajistí proti manipulaci, která by byla v rozporu s účelem tohoto zákona. Na odklad splnění příkazu klienta upozorní povinná osoba ministerstvo v oznámení o podezřelém obchodě.*

Podstata rizika:

- má-li banka pochybnosti o konkrétní transakci (například účel, příjemce), musí to oznámit FAÚ a současně zablokovat provedení transakce

Nebezpečnost:

- uložení pokuty v rozmezí 1 000 000 – 50 000 000 Kč
- reputační riziko pro banku
- nedbalostní trestní čin

Dotčené bankovní procesy:

- hotovostní transakce
- bezhotovostní transakce

Aktéři:

- pracovníci front-office
- někteří pracovníci back-office
- compliance

Řízení rizika:

- školení pracovníků
- včasné upozornění CO na nově vzniklé hlášení v bance
- rychlá obousměrná zabezpečená komunikace s FAÚ
- automatizace odeslání pokynu k zablokování transakce při podání oznámení

6.3.6 §48 Nesplnění povinnosti k prevenci

§48 odst. 3 *Povinná osoba se dopustí správního deliktu tím, že nezajistí pravidelné proškolení zaměstnanců podle § 23.*

Podstata rizika:

- banka musí mít vypracovaný systém vnitřních zásad
- vnitřní zásady musí schválit MF ČR
- banka musí zajistit pravidelné školení zaměstnanců

Nebezpečnost:

- uložení pokuty v rozmezí 1 000 000 – 50 000 000 Kč
- reputační riziko pro banku

Dotčené bankovní procesy:

- školení

Aktéři:

- zaměstnanci
- compliance

Řízení rizika:

- automatizovaný e-learningový program pro školení zaměstnanců
- elektronické sledování docházky a vystavování certifikátů
- systém upozornění CO na termíny školení jednotlivých zaměstnanců

6.3.7 §49 Povinnosti při převodech peněžních prostředků

Podstata rizika:

- veškeré převody peněžních prostředků musí mít vyplněná povinná pole dle zákona
- banka musí mít mechanismy pro zjištění obsahu těchto povinných polí
- banka musí informace z těchto polí na vyžádání poskytovat i ostatním bankám

Nebezpečnost:

- uložení pokuty v rozmezí 10 000 000 – 50 000 000 Kč
- reputační riziko pro banku

Dotčené bankovní procesy:

- hotovostní transakce
- bezhotovostní transakce

Aktéři:

- pracovníci front-office
- někteří pracovníci back-office
- compliance

Řízení rizika:

- pro každou transakci nutně požadovat název a číslo účtu odesílatele, název a číslo účtu plátce, stanovení účelu transakce, popřípadě další identifikaci plátce
- účinná spolupráce s ostatními bankami

6.3.8 Shrnutí rizik vyplývajících přímo ze zákona AML

Při významném porušení zákona AML může dojít i k odebrání *oprávnění k provozování bankovní činnosti na území České republiky* vydávané ČNB, což představuje významnou překážku podnikání a toto riziko je označováno za velmi výrazné.

Dalšími riziky, avšak ne v pravém slova smyslu, jsou v případě prohřešku proti zákonu určité druhy nepříjemností – interní audit, externí audit, dohlídka ČNB, vynucené personální změny aj. Osobně bych tuto oblast nazval jako nevyslovená rizika. Rozhodně je třeba je zahrnout.

	rizika			činnosti					aktéři			
	pokuta (v milionech Kč)	reputace	nedbalostní trestní čin	hotovostní	bezhotovostní	vznik obchodního vztahu	školení	externí spolupráce	front-office	back-office	compliance	zaměstnanci (obecně)
mlčenlivost	0,2-1	x		x	x	x			x	x	x	(x)
identifikace/kontrola[58]	1-50	x	x	x	x	x			x	x		
informační	1-50	x						x			x	
oznamovací	5-50	x	x	x	x	x			x	x	x	
odklad příkazu	1-50	x	x	x	x				x	x	x	
prevence	1-50	x					x				x	x
převod	10-50	x		x	x				x	x	x	

Tabulka 5: Přehled rizik AML

[58] *Identifikace* a *kontrola* jsou v podstatě totožné činnosti, obsah je stejný, jen okamžik použití je jiný; identifikace se provádí při prvním kontaktu, kontrola při každém dalším.

Dlouho jsem přemýšlel, jak ohodnotit výše popsaná rizika. Když to shrnu – všechny výrazné prohřešky mohou vést ke ztrátě licence a ke ztrátě dobrého jména banky. Obojí představuje pro banku velkého strašáka. Jemné odlišnosti jsou ve výši pokut a od nového roku přibývá možnost trestního stíhání konkrétního zaměstnance. Rizika tedy nejde snadno oddělit, a proto je potřeba se zabývat eliminací jich všech.

Podařilo se mi identifikovat rizika ze zákona a nyní je potřeba ještě vyhledat a identifikovat rizika vzhledem k aktuálnímu stavu řešení situace s AML.

6.3.9 Identifikace rizik v současném stavu řešení vzhledem k rizikům AML

Rizika v ***Hlášení podezřelého obchodu***

- nesystémové řešení vzniku a další práce s hlášením (*.doc* soubor, který je poslán na CO, kde je jako soubor *někde* uložen)
  → MLČENLIVOST
- nezabezpečený komunikační kanál (soubor je odeslán emailem, u CO je chráněn pouze *znalostí místa uložení* a *heslem do OS pracovní stanice*)
  → MLČENLIVOST
- CO nemůže sám aktivně vyhledat dodatečné podklady pro ohodnocení hlášení, musí *zainteresovat* dalšího pracovníka banky
  → MLČENLIVOST

Rizika v ***Komunikace s FAÚ***

- CO vytvoří oznámení, které posílá faxem nebo prostřednictvím služby *MoneyWeb* na FAÚ
  → MLČENLIVOST při použití faxu
- ruční poznámka o čase a datu podání oznámení na FAÚ, zainteresování dalšího pracovníka banky při zadání pokynu pro blokování transakce; ruční hlídání uplynuté lhůty, ruční požadavek na odblokování transakce
  → nesystémové řešení, které klade zbytečné požadavky na CO z hlediska dodržování lhůt a řízení blokování & MLČENLIVOST

Rizika v ***Mlčenlivost***

- *převážně viz výše*
- nesystémové užívání nezabezpečených technologií k přenosu samotného hlášení a varování o vzniku hlášení (hlášení je posíláno emailem, telefonicky je upozorněn CO, ale co když je na obědě, jednání… a není u emailu, ani telefonu v kanceláři)
  → ODKLAD & OZNAMOVACÍ P.

Rizika v ***Aktivní hledání podezřelého chování***

- CO musí aktivně hledat a ručně analyzovat chování na účtech klientů
  → OZNAMOVACÍ P. & PŘEVOD

Rizika v ***Detekování politicky exponované osoby*** *(PEO)*

- PEO je potřeba přiřadit zvláštní – přísnější režim kontroly
  → IDENTIFIKACE/KONTROLA

Riziko v ***Detekování potenciálně problémového klienta*** *(PPK)*

- cíl celého AML směřuje k tomu, neobchodovat s PPK a jejich snahy o obchod ihned oznamovat, zjistí-li regulátor uskutečněný obchod s PPK, je to vždy velký problém
- ruční kontrola klientů proti různým seznamům a databázím
  → IDENTIFIKACE/KONTROLA

Riziko v ***Školení zaměstnanců***

- ruční evidence CO o tom, kdo byl a kdy proškolen
  → PREVENCE

Riziko v ***Archivace***

- nesystémová práce se soubory, papírovými seznamy s podpisy
  → MLČENLIVOST, OZNAMOVACÍ P., INFORMAČNÍ P. & PREVENCE

Eliminace těchto rizik je popsána již výše v rámci popisu jednotlivých rizik vyplývajících ze zákona AML.

6.3.10 Mapování rizik v rámci bankovních procesů

V této části bych rád identifikoval, kde se jednotlivá rizika nacházejí v rámci konkrétního bankovního procesu.

6.3.10.1 Otevření účtu v bance

Cíl	Rozdělení klientů při otevírání účtu – běžný klient, PEO, PPK
Rizika	identifikace, mlčenlivost, oznamovací povinnost
Aktéři	neklient, klient (běžný, PEO), PPK, osobní bankéř

Na pobočku osobně přichází neklient, setkává se s osobním bankéřem (front-office) a chce otevřít účet (vznik nového obchodního vztahu). Pro banku jsou v tento moment primární tři úkoly:

1) ověřit skutečnou totožnost neklienta (pochybnosti → odmítnutí a oznámení),
2) detekovat, zda se nejedná o PEO (zařazení klienta jako *běžného* nebo *PEO*),
3) detekovat, zda se nejedná o PPK (pozitivní nález →odmítnutí a oznámení).

Klient není **NIKDY** pravdivě informován o skutečném důvodu odmítnutí, nebo o jeho zařazení do PEO a tím i přísnějšího režimu kontrolu, nebo o podání oznámení na něj.

Seznam činností:

1) neklient musí předložit doklad vydaný státním orgánem;
2) pracovník banky porovná skutečnou podobu neklienta a fotografii, případně si vyžádá další doklad totožnosti;
3) ověří doklad v databázi zneplatněných dokladů MV ČR[59];
4) pořídí si fotokopii dokladu;
5) opíše identifikační údaje podle §5 AML;
6) dotáže se neklienta, zda je PEO;
7) neklient podepisuje návrh smlouvy;[60]
8) probíhá detekce na PEO;
9) probíhá detekce na PPK;
10) neklient se stává klientem, nebo je odmítnut.[61]

[59] MV ČR – Ministerstvo vnitra České republiky

[60] Princip oferty a akceptace

[61] Mezi podpisem neklienta a podpisem banky je časové prodleva, která umožňuje zkoumat neklienta.

PEO	PPK	Výsledek
NE	NE	účet otevřen, běžný klient
ANO	NE	účet otevřen, PEO klient
ANO	ANO	účet neotevřen, oznámení
NE	ANO	účet neotevřen, oznámení

Tabulka 6: Žádost o otevření účtu

6.3.10.2 Průběžná kontrola klienta

Cíl	Kontrola správného zařazení klienta
Rizika	identifikace, mlčenlivost, oznamovací povinnost
Aktéři	klient (běžný, PEO), PPK, CO, systém[62]

Všechny klienty je potřeba neustále kontrolovat, jestli nedošlo ke změně v jejich zařazení. Rozhodující je tedy aktualizace databází a automatizovaná kontrola. Změna zařazení klienta může vzniknout dvěma způsoby:

1) chyba banky při první identifikaci;
2) skutečná změna postavení klienta.

Původní zařazení	Nové zařazení	Akce banky
klient	PEO	změna zařazení klienta, přísnější kontrola chování klienta
PEO	klient	změna zařazení klienta, standardní kontrola chování klienta
klient	PPK	okamžité zmrazení účtu, oznámení
PEO	PPK	okamžité zmrazení účtu, oznámení
PPK	x	(PPK nebyl NIKDY veden jako klient)

Tabulka 7: Změny v zařazení klienta

Největší riziko představuje oznámení špatného zařazení klienta (neodhalení PPK) regulátorem. Menší riziko pak oznámení regulátora o nezařazení klienta mezi PEO.

6.3.10.3 Uzavření účtu v bance

Primárně se o rizikovou činnost nejedná, je potřeba spíše zkoumat v souvislostech s předchozím chováním klienta.

6.3.10.4 Osobní hotovostní transakce - vklad

Cíl	Eliminovat riziko legalizace hotovosti pokladnou
Rizika	Identifikace, kontrola, mlčenlivost, oznamovací p., převod, odklad, informační p.
Aktéři	klient, neklient, osobní bankéř, zpracování plateb

Primárně je podezřelý **vklad**. Nejrizikovější situaci představuje moment, kdy je hotovost posílána na účet neklienta.

Nadměrné vklady musí vkladatel vždy oznamovat s předstihem a banka má možnost jejich přijetí odmítnout (bez udání důvodu).[63]

[62] Systém – mám tím na mysli částečně zautomatizovanou kontrolu proti seznamům.

[63] Rozhodne-li se někdo přinést do banky například 5 000 000 Kč v hotovosti a banka jej odmítne, může to samozřejmě zkusit třeba v pěti dnech po 1 000 000 Kč, což už banka přijmout může, nicméně tak či tak si v obou případech může být jist, že bude ze strany banky zkoumán původ a účel prostředků a v případě sebemenší pochybnosti bude jeho transakce oznámena.

Vkladatel	Příjemce	Činnost banky
neklient	neklient	Identifikace neklienta
klient	neklient	Kontrola klienta
neklient	klient	Identifikace neklienta
klient	klient	Kontrola klienta

Tabulka 8: Osobní hotovostní transakce - vklad

Seznam činností:

1) vkladatel musí předložit doklad vydaný státním orgánem;
2) pracovník banky porovná skutečnou podobu neklienta a fotografii, případně si vyžádá další doklad totožnosti;
3) ověří doklad v databázi zneplatněných dokladů MV ČR;
4) pořídí si fotokopii dokladu;
5) opíše (identifikace)/ porovná (kontrola) identifikační údaje podle §5 AML;
6) vkladatel vyplní formulář (název a číslo účtu příjemce, suma, původ prostředků, podpis vkladatele);
7) přijetí hotovosti a předání požadavku na zpracování plateb
8) kontrola vkladatele (PEO, PPK);
9) kontrola příjemce (PEO, PPK);
10) provedení, nebo zablokování a ohlášení transakce.

Pokud existuje pochybnost, nebo klient odmítá kompletně vyplnit formulář, osobní bankéř může odmítnout přijetí a oznámí klientovo podezřelé chování.

V případě, že vkladatel je PEO – je to považováno za podezřelejší transakci a je kladen důraz na původ prostředků.

Podle §7 odst. 1 není potřeba identifikovat klienta při obchodu menším než je € 1 000. Osobně si myslím, že je vhodnější identifikovat/kontrolovat klienta i při nižších objemech obchodu.[64]

6.3.10.5 Osobní hotovostní transakce - výběr

Cíl	Eliminovat riziko legalizace hotovosti pokladnou
Rizika	kontrola, mlčenlivost, oznamovací p., převod, odklad, informační p.
Aktéři	klient, osobní bankéř

Výběr hotovosti je obecně podezřelý po předchozím podezřelém chování na účtu klienta. Výběr nadměrné hotovosti je opět potřeba hlásit předem. Větší pozornost vzbuzuje výběr hotovosti PEO.

Seznam činností:

1) klient musí předložit doklad vydaný státním orgánem;
2) pracovník banky porovná skutečnou podobu neklienta a fotografii, případně si vyžádá další doklad totožnosti;
3) ověří doklad v databázi zneplatněných dokladů MV ČR;
4) pořídí si fotokopii dokladu;
5) porovná identifikační údaje podle §5 AML;
6) klient vyplní formulář (název a číslo svého účtu, suma, účel výběru prostředků, podpis klienta);

Přijetí velké hotovosti představuje pro banku jednak riziko AML a jednak i velké náklady na samotné zpracování hotovosti.

[64] Už třeba z důvodu pokusu o udání padělaných peněz. € 1 000 = CZK ±25 000, a to není malá částka.

7) přijetí, nebo pozdější přijetí z důvodů nedostatku peněz transakce osobním bankéřem.

Jakékoliv podezření je důvodem k oznámení.

6.3.10.6 Bezhotovostní transakce – převody

Cíl	Eliminovat riziko legalizace peněžních prostředků
Rizika	kontrola, mlčenlivost, oznamovací p., převod, odklad, informační p.
Aktéři	klient, telefonický bankéř[65], zpracování plateb, systém

Bezhotovostní transakce může provádět pouze klient banky a má obvykle k dispozici čtyři různé způsoby:

1) osobní návštěva pobočky a vyplnění papírového platebního příkazu;
2) telefonickým bankovnictvím;
3) internetovým bankovnictvím;
4) platbou prostřednictvím platební karty.

V prvním případě klient vyplní formulář[66] (název a číslo účtu odesílatele, název a číslo účtu příjemce, částka, datum splatnosti, účel platby[67], podpis podle podpisového vzoru). Formulář se dostává na zpracování plateb, které informace na formuláři zkontroluje a zadá do systému.

U telefonního bankovnictví je klient identifikován na základě kontrolních otázek[68] a dále *vyplní formulář* (název a číslo účtu příjemce, částka, datum splatnosti, účel platby) s telefonickým bankéřem. Požadavek potom směřuje na zpracování plateb.

Prostřednictvím internetu je klient identifikován na základě přihlašovacích údajů (číslo, heslo, certifikát, token apod.) a ručně zadává (název a číslo účtu příjemce, částka, datum splatnosti, účel platby). Požadavek odchází na zpracování plateb.

Poslední variantou je převod prostředků prostřednictvím platební karty. Identifikace klienta je provedena obvykle podpisem nebo zadáním PIN.[69] Požadavek opět putuje na zpracování plateb.

V rámci převodů mezi klienty jedné banky není potřeba provádět dodatečnou kontrolu na PPK. Pokud jsou prostředky poslány z jiné banky, klientovi *naší* banky, odpovědnost za odesílatele nese druhá banka. Pokud klient *naší* banky posílá prostředky jiné bance, je potřeba provést detekci na PEO a PPK.

Poslední tři zmíněné způsoby poskytují dostatečnou spolehlivost na správnou kontrolu klienta. Slabým místem je první způsob, kdy *někdo* vyplní papír a pokusí se o neautorizované provedení transakce. V případě pochybností/neúplnosti/chyby v údajích na formuláři, může zpracování plateb předat příkaz k ověření přes telefonického bankéře, který se s klientem spojí a zadání platebního příkazu proběhne podle scénáře telefonického bankovnictví.

---

[65] Jsem v rozpacích, jestli je vhodné používat *telefonní* nebo *telefonický bankéř*, určitě ne *bankéř na telefonu*. Věřím, že i přes slabší český výraz si rozumíme, o koho jde.

[66] Papírový platební příkaz je přežitek z historie, který nabízí relativně malou formu zabezpečení (pouze podpisový vzor) a jistou míru nespolehlivosti při nesprávném vyplnění.

[67] Účel platby se často zjišťuje dodatečně až v případě naplňování informační povinnosti.

[68] Přijatelnou míru spolehlivosti zajistí aspoň otázky na informace, které není možné vyčíst z dokladů.

[69] Od 1. 11. 2009 se od podpisu ustupuje z důvodu odpovědnosti banky za uskutečněné autorizované transakce v případě odcizení karty. Podpis nenabízí dostatečnou spolehlivost a záruky.

6.3.10.7 Preventivní školení

Cíl	Pravidelné školení zaměstnanců
Rizika	prevence
Aktéři	CO, zaměstnanci

Podle §23 musí banka zajistit proškolení všech zaměstnanců, kteří se mohou setkat s podezřelým obchodem při výkonu své funkce. Školení připravují CO a sledují účast.

Školení probíhá prostřednictvím e-learningu nebo osobní prezentací CO školeným.

Kontrola plnění je v kompetenci CO. Každý nově příchozí zaměstnanec musí být proškolen nejpozději do tří měsíců od nástupu. Všichni zaměstnanci musejí být opakovaně školeni nejméně jednou za dvanáct měsíců.

6.4 Detekce rizik

AML bankám jasně předepisuje požadované chování a dává jim do rukou nástroje pro jeho naplnění. Základní povinností bank je *oznamovací povinnost*, od ní se teprve odvíjejí povinnosti další. Oznamovací povinnost ukládá bance oznámit podezřelý obchod.

Podezřelý obchod je jednak přesně vymezen v zákoně:

§6 odst. 1 *Podezřelým obchodem se pro účely tohoto zákona rozumí obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu, anebo jiná skutečnost, která by mohla takovému podezření nasvědčovat.*

Pokud je zjištěna některá z následujících skutečností, jedná se o podezřelý obchod a musí být **vždy** oznámen.

§6 odst. 2 *Podezřelým je obchod vždy, pokud*

a) klientem nebo skutečným majitelem je osoba, vůči níž Česká republika uplatňuje mezinárodní sankce podle zákona o provádění mezinárodních sankcí[70]*,*

b) předmětem obchodu je nebo má být zboží nebo služby, vůči nimž Česká republika uplatňuje sankce podle zákona o provádění mezinárodních sankcí, nebo

c) klient se odmítá podrobit kontrole nebo odmítá uvést identifikační údaje osoby, za kterou jedná.

Body *a* a *b* je potřeba detekovat v rámci detekce PPK nebo kontroly původu či účelu prostředků. Bod *c* je potřeba detekovat v rámci identifikace/kontroly.

Pokud je zjištěna některá z následujících skutečností, jedná se velmi pravděpodobně o podezřelý obchod, nebo by minimálně mělo vzniknout podezření:

§6 odst. 1

a) klient provádí výběry nebo převody na jiné účty bezprostředně po hotovostních vkladech,

b) během jednoho dne nebo ve dnech bezprostředně následujících uskuteční klient nápadně více peněžních operací, než je pro jeho činnost obvyklé,

c) počet účtů zřizovaných klientem je ve zjevném nepoměru k předmětu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,

d) klient provádí převody majetku, které zjevně nemají ekonomický důvod,

[70] §2 zákona č. 69/2006 Sb., o provádění mezinárodních sankcí

e) prostředky, s nimiž klient nakládá, zjevně neodpovídají povaze nebo rozsahu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,

f) účet je využíván v rozporu s účelem, pro který byl zřízen,

g) klient vykonává činnosti, které mohou napomáhat zastření jeho totožnosti nebo zastření totožnosti skutečného majitele,

h) klientem nebo skutečným majitelem je osoba ze státu, který nedostatečně nebo vůbec neuplatňuje opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, nebo

i) povinná osoba má pochybnosti o pravdivosti získaných identifikačních údajů o klientovi.

Navíc ještě každá banka musí mít povinně vypracovaný systém vnitřních zásad (§21 odst. 1, 2 a 5) pro uplatňování AML, který je povinně schválen MF ČR. Jedná se o závazný předpis, kde si každá banka sama stanovuje své postupy při naplňování AML. Nepochybně tento dokument patří k velmi pečlivě střeženým dokumentům v bance. Systém vnitřních zásad definuje i další znaky podezřelých obchodů, avšak vzhledem k tajemstvím a nutnosti nezveřejňovat charakteristiky aplikace AML se jimi nebudu moci podrobněji zabývat.

6.4.1 Místa vzniku rizik

Banka se musí pokusit všemi svými prostředky zajistit veškeré potřebné informace o prováděném obchodu, Má-li pochybnost musí tuto skutečnost oznámit. Navrhuji dvoustupňové řešení, neboť v rámci chodu banky mohou vznikat falešné poplachy a pravomoc pro odeslání oznámení má pouze compliance. V prvním stupni vznikne *pouze* hlášení, které je doručeno na compliance a teprve CO rozhodne o dalším osudu hlášení – buď uloží v systému pouze jako hlášení, bez další akce, anebo jej připojí k oznámení pro FAÚ a odešle jej. Snadno se tím zaručí rozdělení pravomocí, odfiltrování falešných oznámení.

Kde všude mohou hlášení vzniknout, co hlásí a jakou mají závažnost.

Činnost	Odpovědný pracovník	Skutečnosti podezřelého obchodu
Otevření účtu	Osobní bankéř	Pochybnosti o totožnosti (1)
		Shoda na seznamu PPK (1)
		Větší počet současně otevřených účtů (2)
Kontrola zařazení klienta	CO	Shoda na seznamu PPK (1)
	Systém	
Osobní hotovostní transakce - vklad	Osobní bankéř	Pochybnosti o totožnosti (1)
		Shoda na seznamu PPK (1) [vkladatel]
	Zpracování plateb	Podezřelé chování na účtu (2)
	Systém	
Osobní hotovostní transakce - výběr	Osobní bankéř	Pochybnosti o totožnosti (1)
	Zpracování plateb	Podezřelé chování na účtu (2)
Bezhotovostní transakce - převod	Zpracování plateb	Pochybnosti o totožnosti příjemce mimo banku (2)
		Shoda na seznamu PPK (1) [příjemce]
		Pochybnosti o totožnosti (1)
	Systém	Shoda na seznamu PPK (1)
		Podezřelé chování na účtu (2)

Tabulka 9: Místa pro vznik hlášení

Skupina (1) představuje hlášení, které je možné rozšířit na oznámení a přeposlat na FAÚ bez dalšího hlubšího zkoumání, neboť vyhovují §6 odst. 2. Závažná hlášení.

Skupina (2) představuje hlášení, která mohou a nemusí nutně znamenat podezřelý obchod, a proto je vhodné na ně upozornit a nechat rozhodnutí na CO.

6.4.1.1 Pochybnosti o totožnosti

Při identifikaci nebo kontrole totožnosti klienta by mělo vzbudit podezření:

- neochota klienta poskytnout součinnost při identifikaci/kontrole
  →odmítnutí obchodu[71]
- výrazná neshoda mezi skutečnou podobou a fotkou na dokladu[72]
  →okopírování dokladu, odmítnutí obchodu, hlášení
- doklad je neplatný podle databáze MV ČR
  →okopírování dokladu, odmítnutí obchodu, hlášení
- neúspěšná hlasová identifikace při telefonickém bankovnictví
  →předání do pravomoci osobního bankéře, který zjistí, zda se jedná o podvod (hlášení) nebo náhodu

Řízení:

- školení zaměstnanců
- elektronický formulář pro identifikaci/kontrolu[73] klienta s
  - povinným textovým polem číslo OP (číslo pasu), který je na pozadí systémově zkontrolován se seznamem zneplatněných průkazů MV ČR, při pozitivním nálezu zobrazí text neplatný doklad a znemožní odsouhlasit identifikaci/kontrolu
  - polem pro připojení fotokopie průkazu
  - tlačítkem *Vytvořit hlášení*
- samotný nález shody čísla dokladu posílá upozornění na CO dashboard

6.4.1.2 Shoda na seznamu PPK

Před akceptací obchodu nebo vznikem nového obchodního vztahu je zkoumána shoda jména klienta s obsahem několika různých databází

- seznam sankcionovaných osob[74];
- seznam sankcionovaných zemí[75];
- seznam známých teroristů a osob s nimi spojených;
- seznam osob spojených s kategorií nebezpečné podnikání;
- seznam osob v majetkovém vztahu se společnostmi kategorie nebezpečné podnikání;

Řízení:

- interní seznamy je potřeba automaticky aktualizovat;
- shodu může odhalit
  - *systém* při automatické aktualizaci dat o stávajících klientech
    → generuje hlášení pro CO;
  - osobní bankéř při ručním spuštění kontroly údajů o neklientovi, který chce otevřít účet
    →neotevření účtu, kopie dokladů, hlášení;

---

[71] Bohužel není co hlásit, vzhledem k tomu, že ani nevíme, kdo stojí před námi.

[72] Před pracovníkem front-office stojí černoch s fotkou opáleného bělocha…

[73] Viz příloha *Okno identifikace & kontrola*

[74] Jeden druh vydává FATF (Financial Action Task Force), který je závazný ze zákona, druhý druh seznamů vydává EU a třetí druh seznamů si vytváří každá banka sama.

[75] Stejně jako předchozí poznámka.

    - osobní bankéř při ručním spuštění kontroly údajů o vkladateli, který chce vložit osobně hotovost, nebo o příjemci této hotovosti →odmítnutí transakce, kopie dokladů, hlášení;
    - zpracování plateb při kontrole příjemce příkazu k úhradě →neprovedení transakce, hlášení
- samotný nález shody PPK posílá upozornění na CO dashboard

6.4.1.3 Větší počet současně otevřených účtů

Chce-li si klient otevřít další účet, je na osobním bankéři, shledá-li tuto skutečnost podezřelou, vzhledem k majetku či oboru podnikání klienta. Podle svého nejlepšího vědomí a svědomí poté tuto skutečnost může ohlásit na CO, které rozhodne o dalším osudu hlášení.

Řízení:

- sledovat počet otevřených účtů nepředstavuje výrazný problém
- CO stanoví limitní prahy pro maximální obvyklý počet současně otevřených účtů v závislosti na majetku, typu podnikání a PEO
    - do tohoto limitu může podat hlášení osobní bankéř
    - nad tento limit je při otevření nového účtu odesláno upozornění na CO dashboard

6.4.1.4 Podezřelé chování na účtu klienta

Detekovat podezřelé chování na účtu patří k nejsložitějším, neboť je potřeba sbírat a vyhodnocovat data z různých zdrojů. Lze na toto nasadit automaty, které budou hledat typické chování, avšak nepochybně výsledky jejich analýz budou sloužit jako podkladová data pro přijetí rozhodnutí.

Systém monitorování plateb (Payment Screening) – automatizovaný systém, který v reálném čase detekuje platby, které jsou spojeny se jmény na black-listech.

Před provedením platby jsou všechna pole transakce automatických předmětem kontrol proti seznamům. Při pozitivním nálezu je transakce zablokována a je informováno CO. Při chybné detekci lze transakci manuálně povolit. Při korektní detekci je podáno oznámení na FAÚ a běží lhůta pro odklad platby.

Systém monitorování plateb z/do zemí nebezpečných zemí (Non-cooperative Countries Payment Screening) – každá banka má celý svět rozdělený do několika zón, podle stupně uplatňování prevence AML. Monitorují se platby v závislosti na zemi příchozí či odchozí platby. Vysoké riziko představují platby z/do zemí jako jsou Nigérie, Írán, Severní Korea aj. Při pozitivní detekci je transakce zablokována a ohlášena CO, který o ní dále rozhodne (oznámení, odblokování).

Monitorování hotovostních transakcí (Cash Screening) – monitorování účtů klientů, kde došlo k hotovostním transakcím. CO nastavuje práh pro citlivost tohoto systému.

Monitorování obratů na účtech (Abnormal Money Usage) – systém sleduje a vyhodnocuje odchylky od obvyklého počtu transakcí v čase a od obvyklého objemu transakcí. Umožňuje snadno detekovat tzv. *mrtvé/spící účty*[76]. Při významné odchylce od běžného stavu je transakce zablokována a ohlášena CO.

Řízení:

[76] Mrtvý/spící účet – typicky je pouze založen, ale velmi dlouho se na něm neuskuteční žádná transakce, až jednoho dne se přes něj najednou někdo pokusí přeposlat 10 000 000 Kč.

- výstupy těchto systémů je potřeba zpřístupnit CO, aby mohl bez účasti dalších zaměstnanců
    - získávat podklady při hodnocení rizika podezřelého obchodu
    - doplnit oznámení o detaily, nebo nově požadované podklady
    - sám analyzovat chování klientů
    - spolehlivěji zabezpečit mlčenlivost
- výstupy je vhodné ukládat do DW (nebo RTS), aby je mohl analyzovat systém
    - podle předdefinovaných pravidel
    - za účelem získání nových pravidel

Analýzou výstupů z těchto systémů a porovnáním s předdefinovanými modely chování lze úspěšně detekovat skutečnosti *§6 odst. 1 písm. a, b, c, e,* a *f*.

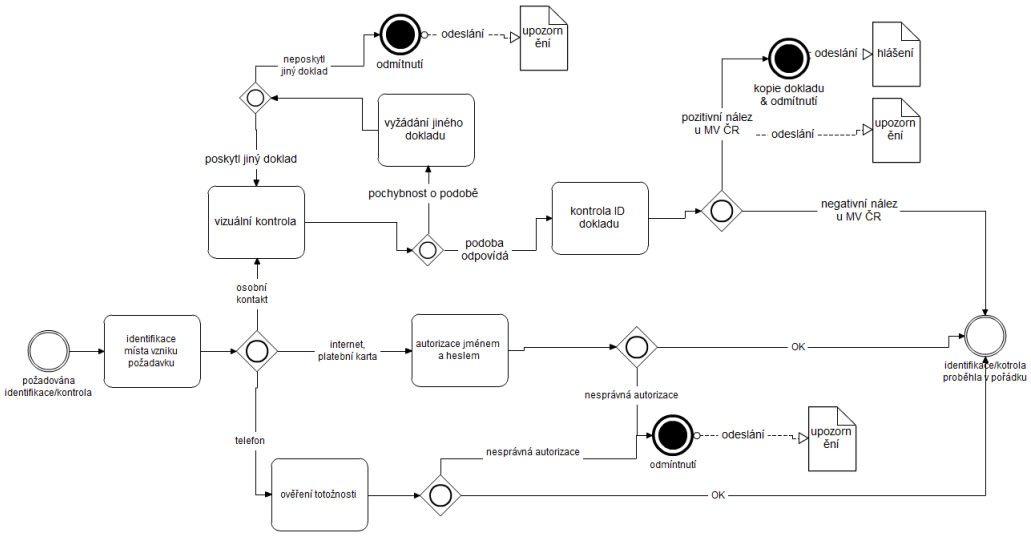
6.4.2 Modely procesů[77]

Určitě je potřeba doplnit grafické vyjádření výše popsaného. Nejsem si jist, že mnou použití nástroj pro modelování odpovídá specifikace BPMN[78], proto pro jistotu přikládám legendu.

Symbol	Vysvětlení	Symbol	Vysvětlení
	začátek procesu; konec procesu		zpráva zdroj dat
	rizikový konec procesu		OR rozhodování v procesu
	činnost; skupina činností		směr průběhu procesu
	dílčí proces		vznik zprávy čerpání dat ze zdroje

Tabulka 10: Legenda k modelům procesů

6.4.2.1 *Identifikace/kontrola*

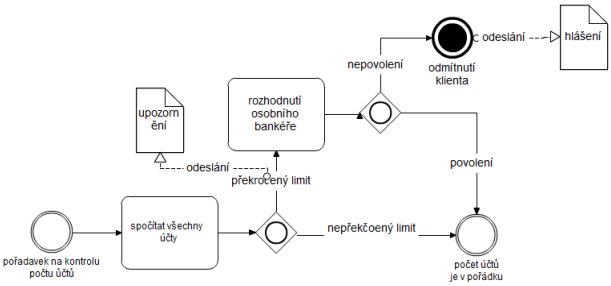


Obrázek 11: Proces Identifikace/kontrola

[77] Pro tvorbu všech modelů používám nástroje webové služby www.gliffy.com.

[78] BPMN – Business Process Modeling Notation

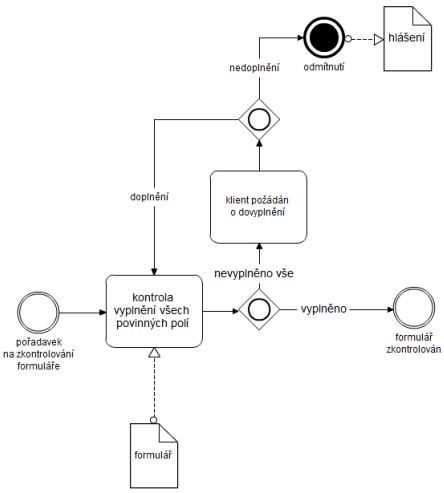
6.4.2.2 Kontrola počtu účtů



Obrázek 12: Proces kontrola počtu účtů

Nastavení prahového limitu je v kompetenci CO, popřípadě lze časem vyžít výsledků analýzy chování.

6.4.2.3 Kontrola formuláře



Obrázek 13: Proces kontrola formuláře

V rámci tohoto procesu je potřeba klást velký důraz na šablonu formuláře a přesné vymezení *povinných polí* podle potřeb zákona a souboru vnitřních předpisů.

Povinná pole *vkladového formuláře*:

- identifikace vkladatele
  - jméno, druhé jméno, příjmení
  - rodné číslo (pokud má[79])
- identifikační doklad
  - typ dokladu (pas, občanský průkaz, průkaz EU, průkaz o povolení k trvalému pobytu),
  - ID dokladu
- Identifikace platby
  - číslo účtu, na který je vkládána částka
  - částka rozepsaná na konkrétní bankovky a počet bankovek jednotlivých nominálních hodnot[80], měna

[79] Cizinci nemusejí mít RČ přidělené, potom není povinné.

    - původ vkládaných prostředků (například mzda, renta, úspory, prodej domu, pronájem, podnikání…)
    - účel vkladu (například koupě fondů, vklad na termínovaný účet…)
- podpis klienta
- podpis za banku (osobní bankéř, razítko – jméno, číslo, podpis)
- datum

Povinná pole *výběrového formuláře*:

- identifikace klienta
    - jméno, druhé jméno, příjmení
    - rodné číslo (pokud má)
- Identifikační doklad
    - typ dokladu (pas, občanský průkaz, průkaz EU, průkaz o povolení k trvalému pobytu)
    - číslo dokladu
- Identifikace výběru
    - číslo účtu, ze kterého je částka vybírána
    - částka rozepsaná na konkrétní bankovky a počet bankovek jednotlivých nominálních hodnot, měna
    - účel výběru (např. koupě fondů, vklad na termínovaný účet…)
- podpis klienta
- podpis za banku (osobní bankéř, razítko – jméno, číslo, podpis)
- datum

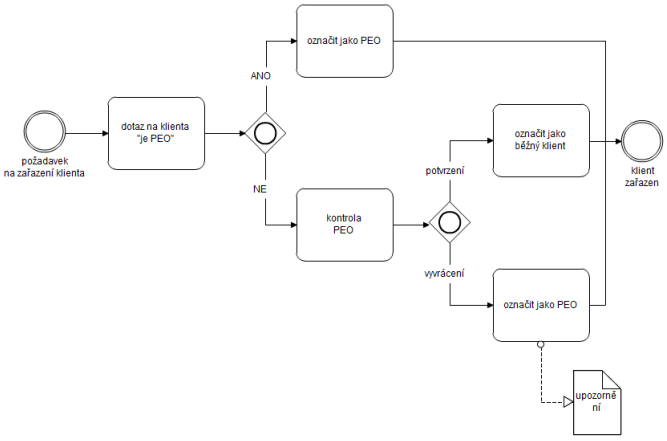
Povinná pole *platebního příkazu (převodu)*[81]

- identifikace klienta
    - jméno, druhé jméno, příjmení
    - rodné číslo (pokud má)
- identifikace převodu
    - číslo účtu, z něhož má být proveden příkaz
    - typ příkazu
    - jednorázový, trvalý, inkasní
    - frekvence, pokud se jedná o trvalý nebo inkasní
    - částka (limit inkasa, jde-li o inkasní příkaz)
    - měna
    - účel transakce (např. platba nájemného, výživné, splátka hypotéky, platba za telefon, apod.)
- podpis klienta (podle podpisového vzoru)
- datum

[80] Údaj o tom, zda jsou bankovky opatřeny páskou jiné banky, nebo jsou volně, může být důležitý a dává se většinou do hlášení; na vkladovém formuláři ale není.

[81] Ukázka příkazu k převodu viz příloha – Příkaz přes zahraniční platební styk

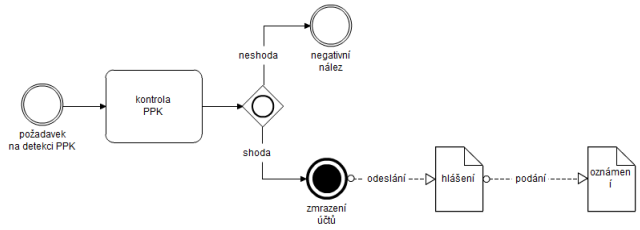
6.4.2.4 Detekce PEO



Obrázek 14: Proces detekce PEO

Při osobním kontaktu je činnost „dotaz na klienta…“ myšlena, jako skutečný dotaz (ústní, nebo součást formuláře). Při systémové kontrole je tato činnost myšlena jako dotaz na hodnotu atributu klienta.

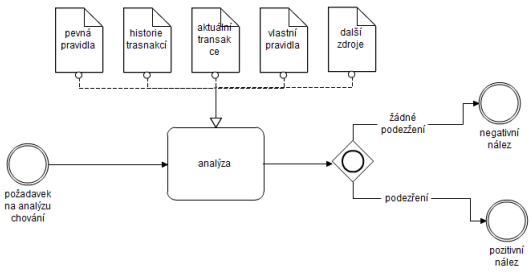
6.4.2.5 Detekce PPK



Obrázek 15: Proces detekce PPK

V případě pozitivního nálezu je účet ihned *zmražen*, aby náhodou ani omylem nemohlo dojít k provedení jakékoliv transakce.

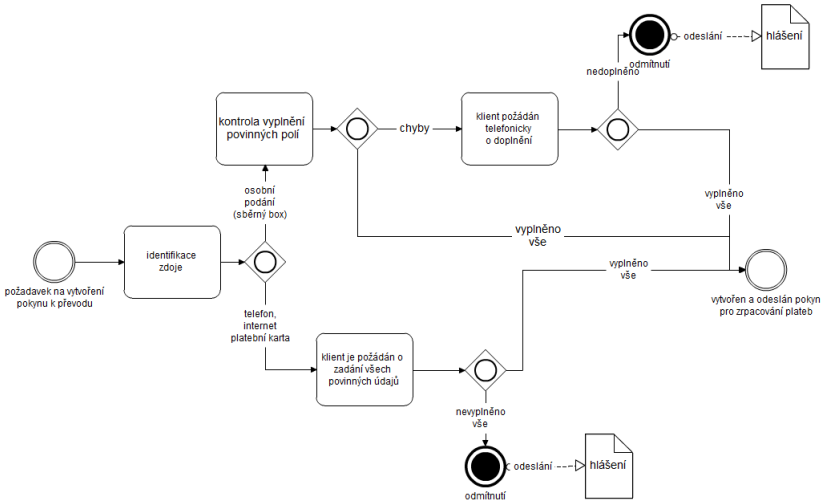
6.4.2.6 Analýza chování



Obrázek 16: Proces analýza chování

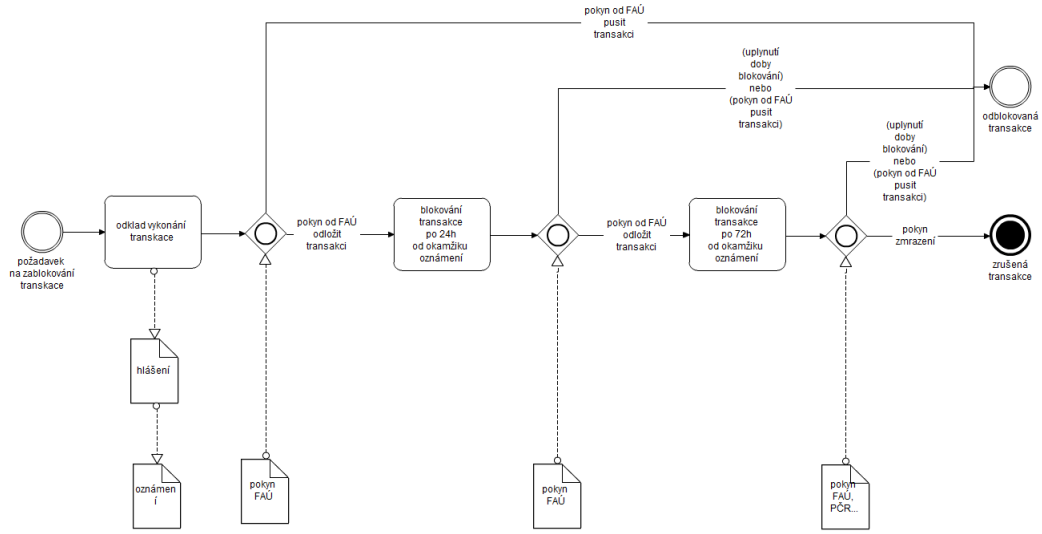
Neodesílá upozornění ani hlášení, neboť tento proces je součástí větších procesů a o notifikaci se starají související procesy.

6.4.2.7 Vytvoření pokynu k provedení platby



Obrázek 17: Proces vytvoření pokynu k provedení platby

6.4.2.8 Zablokování transakce

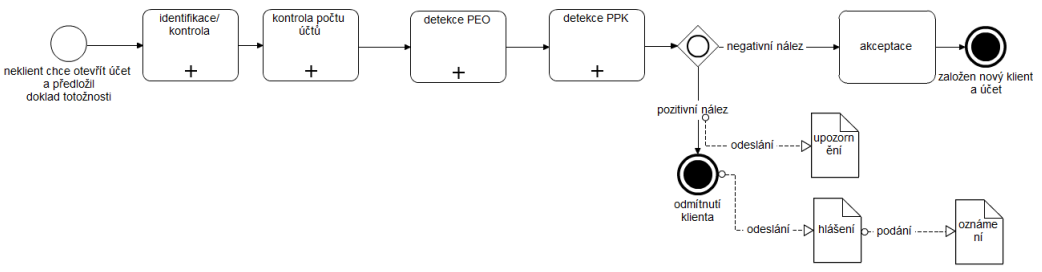


Obrázek 18: Proces zablokování transakce

V případě pochybnosti o transakci je vždy podáno oznámení – *banka si kryje záda*.

V tomto modelu procesu nejsou podchycené možné kolize AML se zákonem o platebním styku. Konkrétně se k nim vyjádřím u dalších modelů.

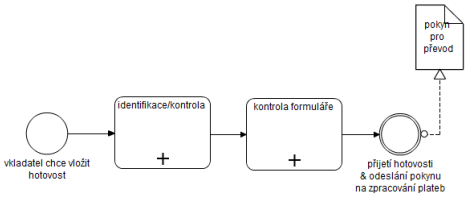
6.4.2.9 Otevření účtu



Obrázek 19: Proces otevření účtu

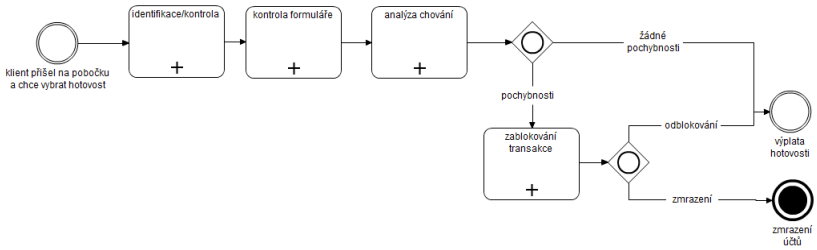
Otevření účtu je konkrétním typem vzniku obchodního vztahu. Uzavření dohody je podmíněno smluvní volností, tzn. nikdo nemůže nikoho nutit do uzavření smlouvy. Při pozitivní detekci PPK je banka oprávněna odmítnout vznik smlouvy, bez udání důvodu. V tomto případě skutečný důvod nesmí zmínit.

6.4.2.10 Vklad hotovosti



Obrázek 20: Proces vklad hotovosti

6.4.2.11 Výběr hotovosti

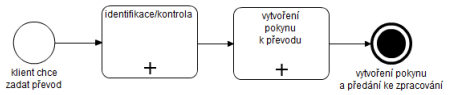


Obrázek 21: Proces výběr hotovosti

V případě na výběr velké hotovosti, což je ostatně často podezřelé, jsou klienti nuceni tuto skutečnost oznámit pár dní předem, tudíž nevzniká zřejmá potíž při zablokování.

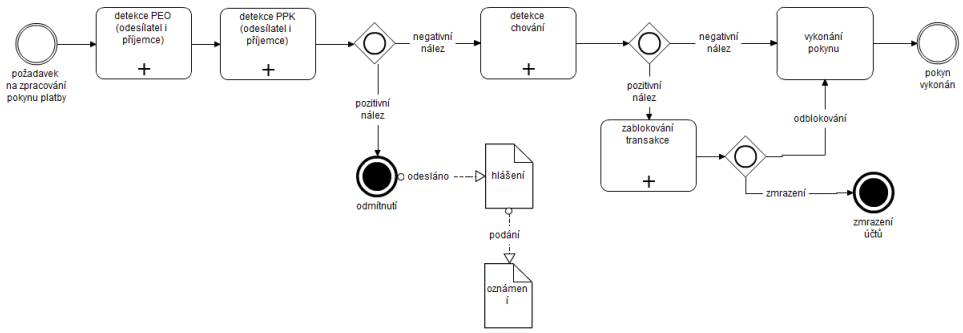
V případě částky, kterou banka může vyplatit, ale došlo k zablokování musí být pracovník banky *herec*, neboť nesmí klientovi naznačit podání oznámení a vzhledem k zablokování transakce nesmí ani nic vydat, čili mu nezbývá něž zahrát například *technické potíže, nedostatek hotovosti aj.* podle jeho fantazie. Klient je v silnější pozici, kdy banka má jeho peníze a tudíž se nemůže sama rozhodnout peníze nevydat.

6.4.2.12 Převod



Obrázek 22: Proces převod

6.4.2.13 Zpracování platebního pokynu



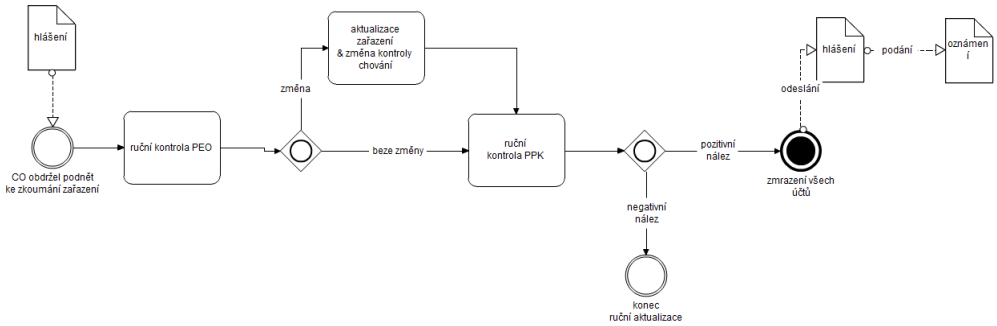
Obrázek 23: Proces zpracování platebního příkazu

Opět je zde potíž odloženého provedení.

Příklad: Klient převádí peníze na jiného klienta, téže banky. Zákon o platebním styku říká, že transakce musí být provedena během jednoho dne (24h). AML říká, že banka musí umožnit odklad transakce až o 72h. FAÚ skutečně nařídí odklad, ale nakonec nic nezjistí, tzn. že klientovi může vzniknout ztráta. Otázka pro právní experty (nebo soud), kdo tuto ztrátu nese?

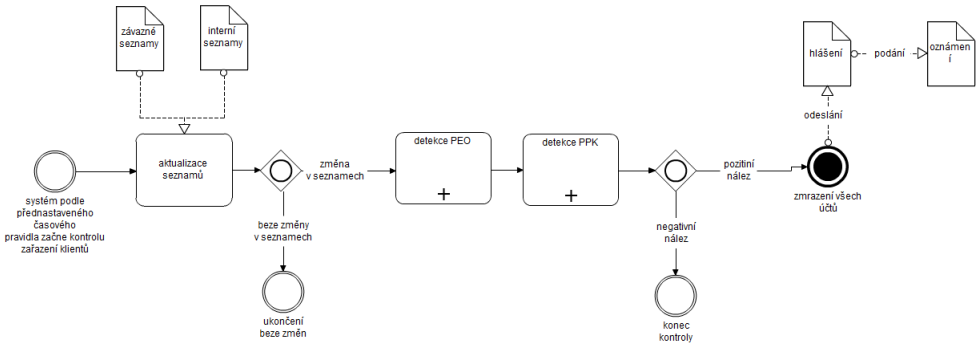
Každopádně pro banku představuje větší riziko postih ze strany regulátora, než *vzteklý* klient, proto dá přednost AML. Bude-li se klient ptát, musí jeho osobní bankéř opět předvést něco ze svých hereckých dovedností.

6.4.2.14 Ruční kontrola CO zařazení klientů



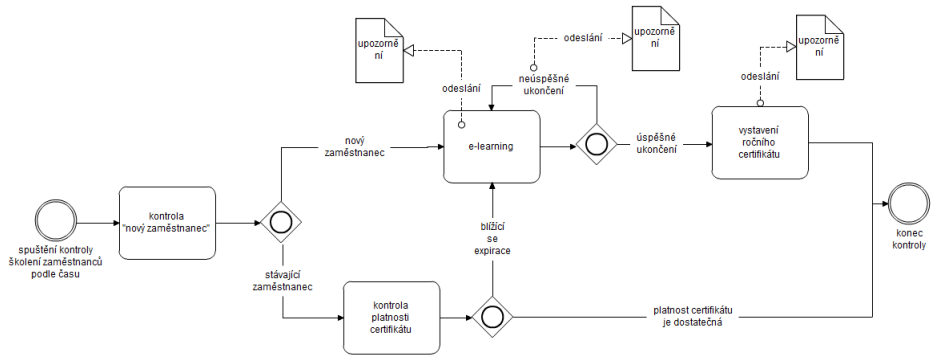
Obrázek 24: Proces ruční kontrola CO zařazení klientů

6.4.2.15 Systémová kontrola zařazení klientů



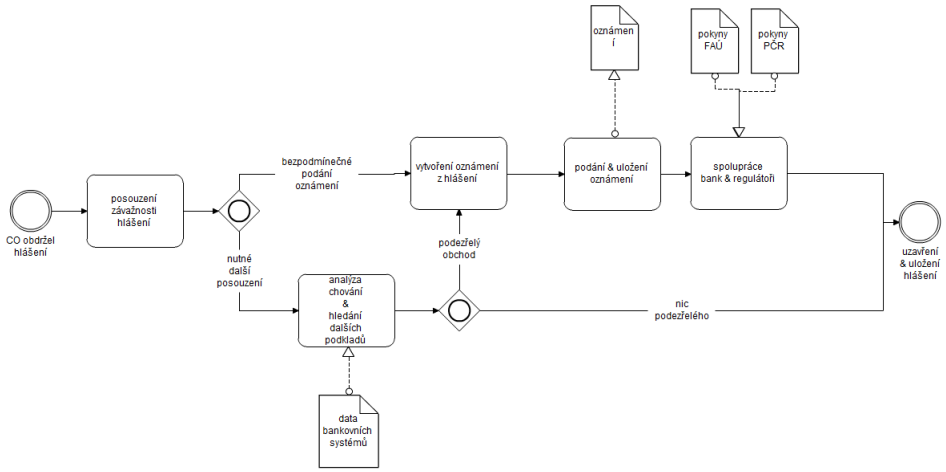
Obrázek 25: Proces systémová kontrola zařazení klientů

6.4.2.16 Školení



Obrázek 26: Proces školení

6.4.2.17 Hlášení



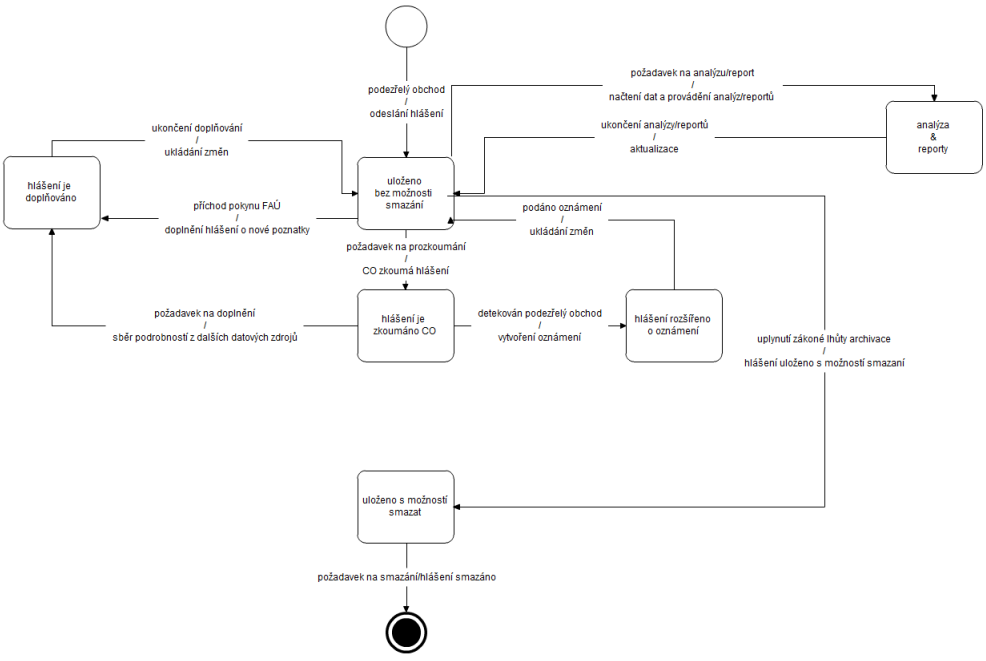
Obrázek 27: Proces hlášení

6.4.2.18 Obecná pochybnost

Každý zaměstnanec může podat hlášení i mimo konkrétní proces. Stačí když se přihlásí k systému a vyplní k tomu určený formulář. Tento způsob vytvoření hlášení je velmi výrazně závislý na odhadu a zkušenostech zaměstnance. Důvodem je i možnost vzniku *podezřelého obchodu* i v naprosto *nepodezřelého obchodu*. Pro snazší pochopení uvedu příklad.

Na pobočku přijde klient banky a provádí vklad hotovosti. Podle nastavených procesů není detekována žádná podezřelá skutečnost. Jen osobní bankéř si všimne, že vklad hotovosti klienta z povzdálí *kontroluje* jiný člověk, který s klientem přišel. Tento *kontrolor* se snaží o legalizaci skrze někoho jiného. Systémově se tento postup velmi těžce, pokud vůbec *odchytává*, avšak *zkušený* osobní bankéř může získat pochybnost.

6.4.3 Model životního cyklu hlášení



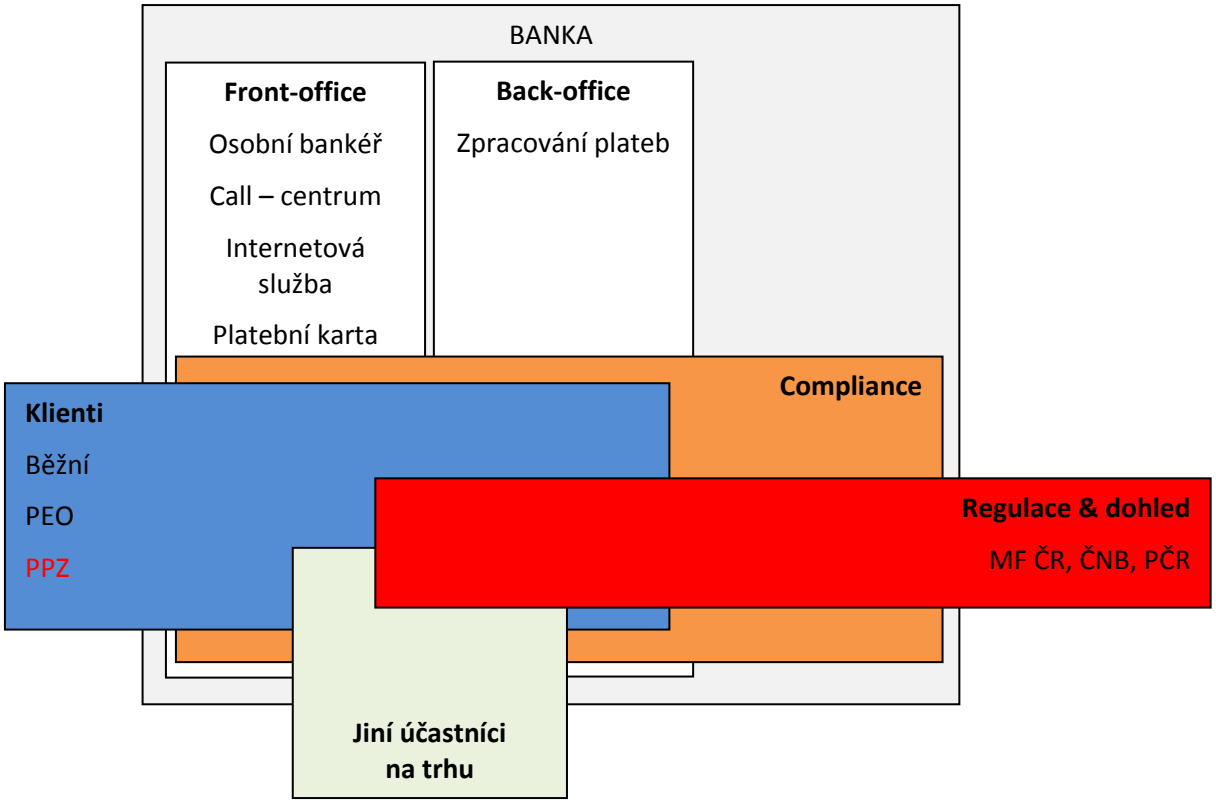
Obrázek 28: Životní cyklus hlášení

Symbol	Vysvětlení	Symbol	Vysvětlení
○	začátek	◉	konec
▭	stav	→	směr přechodu mezi stavy
popis / **popis**	událost způsobující změnu stavu / akce při změně stavu		

Tabulka 11: Legenda k modelu životního cyklu

Kvůli zachování přehlednosti modelu jsem znovu nenavazoval změny stavů a aktivity pro přechodu do stavu *uložení s možností smazat*.

6.4.4 Model prostředí banky



Obrázek 29: Model prostředí banky

Náhled na vztahy a účastníky řešených v AML.

6.5 Návrh BAM podpory

BAM jsou systémy řízené událostmi na podporu zlepšení business procesů. V tomto případě jsou událostmi skutečnosti poukazující na podezřelý obchod. Zlepšení business procesů je zde hlavně v omezení možnosti postihu ze strany regulátora.

Při činnostech banky vznikají různé situace, na které je potřeba správně reagovat. Obecně je podle AML potřeba podezřelou transakci oznámit nejpozději do pěti dnů od jejího vzniku, avšak je-li to možné, je potřeba nebezpečným transakcím předcházet. Zabránit provedení nebezpečné transakce lze jen v případě včasného odhalení její nebezpečnosti.

Každý proces má svůj identifikátor, podle kterého je možné dohledat jeho propojení na klienta, zaměstnance, hlášení, oznámení.

Návrh by měl sbírat tyto druhy dat

1) odeslaná upozornění,
2) odeslaná hlášení,

Nemyslím si, že je podstatné podrobně popisovat funkcionalitu jednotlivých *návrhů*. S trochou zkušeností a představivosti je snadné dovtípit se funkcionality z názvu a kontextu prvku v rámci ukázky okna. Ještě doplním, že nemám zkušenosti s návrhem GUI u aplikací, proto berte tuto stránku problému trochu s nadhledem.

6.5.1 Upozornění

Je generována systémová zpráva, která pouze upozorňuje, že došlo ke sledované skutečnosti. Slouží pouze pro ke sledování systému, ze strany CO nevyžaduje žádnou další akci. Upozornění jsou ukládána a mohou být dále analyzována pro tvorbu pravidel detekce odchylek chování analytických nástrojů, generování reportů apod.

Vznikají na konkrétních místech v procesech a jejich odeslání je řešeno systémově bez účasti ručního zásahu (*viz. Obrázek BAM dashboard a sběr událostí*).

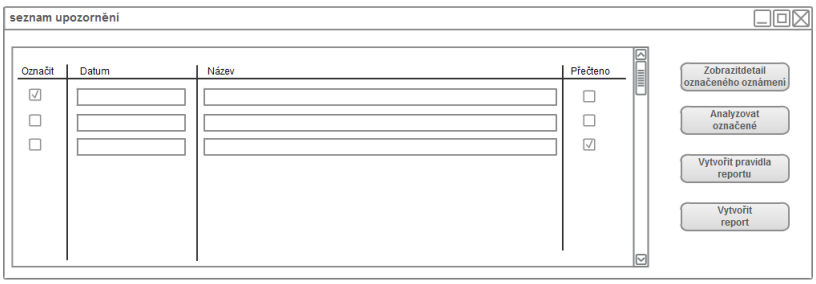
CO je na příchod nových událostí upozorněn prostřednictvím emailu, sám si nastaví frekvenci posílání těchto mailů, minimálně však 1x měsíčně, aby bylo zajištěn odpovídající průběh preventivního školení zaměstnanců.

Seznam generovaných upozornění

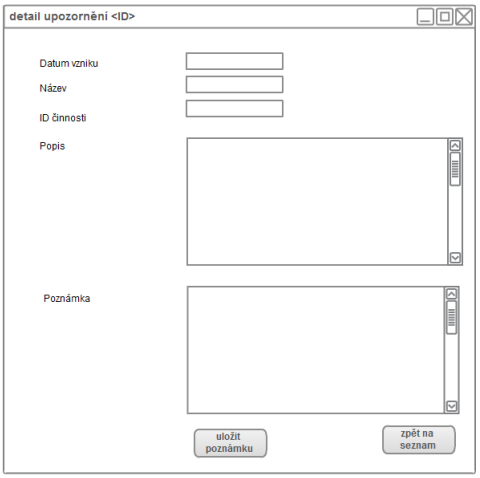
- transakční procesy
  - pozitivní nález detekce neplatného dokladu totožnosti,
  - pochybnosti o dokladu,
  - nezdařený pokus o autorizaci,
  - změna v zařazení klienta (zařazení do PEO),
  - pozitivní nález PPK,
- proces školení
  - spuštění e-learningu zaměstnancem,
  - neúspěšné zakončení e-learningu,
  - vystavení certifikátu zaměstnanci.

6.5.1.1 Upozornění z transakčních procesů

Sleduje se *datum vzniku*, *název*, *popis*, *id činnosti vzniku, poznámka*.



Obrázek 30: Okno seznam upozornění



Obrázek 31: Okno detail upozornění

6.5.1.2 *Upozornění z procesu školení*

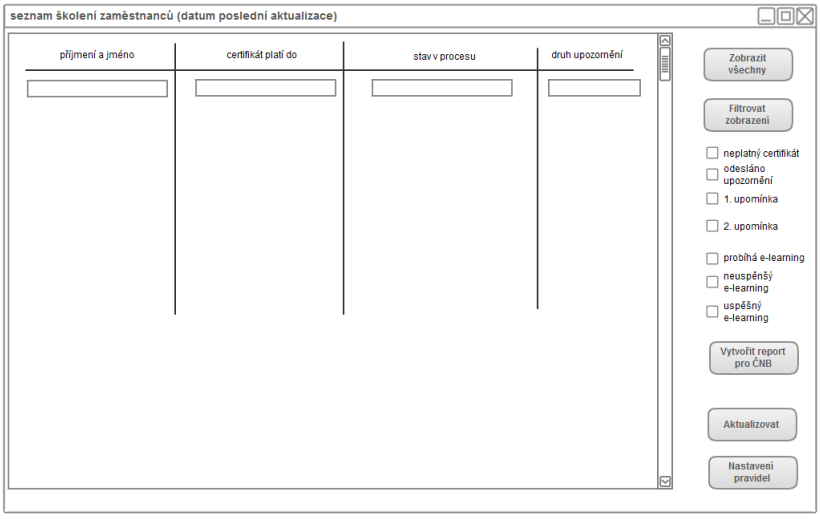
Tento proces nejen sbírá a ukazuje upozornění o školení, ale navíc ještě notifikuje emailem zaměstnance. Proces se pouští automaticky k prvnímu dni kalendářního měsíce nebo ručně CO. CO musí nastavit limity:

- zbývající čas před koncem platnosti certifikátu
  → sytém pak upozorňuje zaměstnance na nutnost nového proškolení,
- čas první upomínky
  → automatické vygenerování a odeslání emailu o nutnosti proškolení,
- čas druhé upomínky
  → automatické vygenerování a odeslání emailu o nutnosti proškolení,
- doba platnosti certifikátu
  → možnost přizpůsobení při změně zákona nebo vnitřních zásad.

Až na nutnost ručního zadání pravidel pracuje systém opět bez dalšího ručního zásahu. V případě netečnosti zaměstnance na upomínky ohledně získání nového certifikátu, použije CO externí systém (telefon, email, osobní návštěvu…) pro zjištění příčin a vyřešení.

V případě kontroly regulátorem lze snadno vygenerovat aktuální stav preventivního školení zaměstnanců.

Sleduje se *jméno zaměstnance, konec platnosti certifikátu, upomínky, stav školení.*



Obrázek 32: Okno seznam školení

6.5.2 Hlášení

Hlášení představuje komplexnější upozornění, může být vytvořeno konkrétním zaměstnancem nebo systémem na konkrétních místech činností. Hlášení je podklad pro případné podání oznámení na FAÚ a soubor hlášení může být zajímavým zdrojem pro analyzování chování klientů a tvorbu nových pravidel detekce podezřelých obchodů.

Všechna hlášení je potřeba ukládat z důvodu jejich užití v analýzách nového chování a reportech (například poměr hlášení a oznámení, počtu transakcí a hlášení…). Mimo to AML ukládá povinnost archivace hlášení, ze kterých bylo podáno oznámení, po dobu nejméně 10 let od okamžiku detekování podezřelého obchodu (lhůta začíná běžet dne 1. 1. následujícího roku po podání oznámení).

Hlášení od zaměstnanců a systému vznikají v předem stanoveném formátu a struktuře

1) Obecné náležitosti – fyzická osoba, klient
   - jméno, druhé jméno, příjmení,
   - datum narození, rodné číslo, místo narození
   - bydliště (trvalé i přechodné, v ČR i v zahraničí), státní příslušnost, pohlaví
   - údaje o průkazu totožnosti – typ (OP, pas, apod.), číslo dokladu, instituce, která vydala doklad, datum vydání, datum ukončení platnosti dokladu
   - telefonní, faxové číslo

2) Údaje o zmocněnci[82],[83]
   - jméno, druhé jméno, příjmení,
   - datum narození, rodné číslo, místo narození
   - bydliště (trvalé i přechodné, v ČR i v zahraničí), státní příslušnost, pohlaví
   - údaje o průkazu totožnosti – typ (OP, pas, apod.), číslo dokladu, instituce, která vydala doklad, datum vydání, datum ukončení platnosti dokladu
   - telefonní, faxové číslo

3) Informace k podezřelému obchodu
   - předmět obchodu (např. vklad/výběr vysoké částky v hotovosti, neobvykle vysoká příchozí/odchozí transakce, opakovaný vklad/výběr vysoké částky v hotovosti, podezřelý příjemce transakce, transakce příjemci/od odesílatele, který je příslušníkem rizikové země, apod.)
   - účel transakce uváděný klientem (pokud je k dispozici)
   - měna
   - čísla účtů, k nimž se transakce vztahuje, jejich identifikace (odesílatel/příjemce; u vkladu a výběru údaje o jednom účtu)
   - částka transakce
   - časové údaje (datum, hodina)
   - u hotovostní transakce (vklad/výběr) – popis použité hotovosti, informace o tom, zda měla hotovost bankovní pásky
   - podezřelé okolnosti obchodu – slovy popsat, co konkrétně bylo na transakci podezřelé, vložit co nejvíce informací: popis chování účastníka, informace o dopravních prostředcích, informace o historii klienta, apod.

[82] Zmocněnec – osoba, která má podpisové oprávnění nebo plnou moc k účtu klienta.

[83] Vyplňuje se pouze tehdy, pokud taková osoba existuje, ne každý účet má zmocněnce.

4) Informace o zaměstnanci,

- kontakt na zaměstnance[84]
- datum oznámení

CO musí být o hlášeních informován, co nejdříve, proto nestačí použití emailu, ale

- je-li aktivně přihlášen ke svému pracovnímu PC, zobrazit okno s upozorněním na příchod nového hlášení,
- není-li u PC, odeslat SMS zprávu na služební mobil.

Seznam možných hlášení

- skrývání pravé totožnosti (lze nahlásit pouze neplatný doklad),
- překročení limitu počtu současně otevřených účtů,
- odmítnutí uvedení všech požadovaných údajů,
- podezřelé chování,
- obecná pochybnost,
- odklad podezřelé transakce (podání oznámení),
- pozitivní nález PPK (podání oznámení).

U hlášení, které zrovna generují oznámení, CO pouze zkontroluje a ručně povolí podání oznámení. U ostatních hlášení je CO povinen rozhodnout, jestli se jedná o podezřelý obchod.

Oznámení je automatické vyplnění polí hlášení do formuláře na zabezpečené webové službě MoneyWeb pro kontakt s FAÚ. V případě technických potíží s připojení či službou je oznámení odesláno faxem.

Při podání oznámení o blokování transakce jsou současně systémově automaticky odebrána zaměstnancům veškerá práva přístupu k hlášené transakci kromě čtení – zobrazuje se status *technické potíže*[85] a je udělána časová značka, aby bylo možné sledovat zákonné lhůty pro odblokování. Všechna práva zůstávají pouze CO. Po dobu šetření FAÚ může být požadováno doplnění dalších informací. Pouze v kompetenci CO je doplnit hlášení o požadovaná další data na pokyn FAÚ[86]. Výsledkem je spolupráce s FAÚ může být požadavek zmrazení nebo odblokování. Při odblokování CO dá pokyn odblokovat a systém provede spuštění transakce a obnoví zaměstnancům odebraná práva. FAÚ taky nemusí poslat žádný pokyn, ten po uplynutí lhůty způsobí odblokování transakce podle popisu výše.

Při pozitivním nálezu PPK je podáno oznámení zmraženy účty a zaměstnancům odebrána všechna práva.

U ostatních hlášení je podání oznámení v kompetenci CO, který veškerá hlášení zkoumá a podle svého uvážení potom rozhoduje o dalším vývoji.

Tato část systému je velmi blízko reakcím typu *automatizovaný termostat*, kdy systém sleduje, částečně automaticky reaguje a nabízí i prostředky k dalším úkonům.

Doplněním o sady pravidel chování a reakcí na ně by se mohl tento systém posunout ještě dál do roviny *řídícího BAM*, možná i k *adaptivnímu BAM*, pokud by se užil podle svých minulých

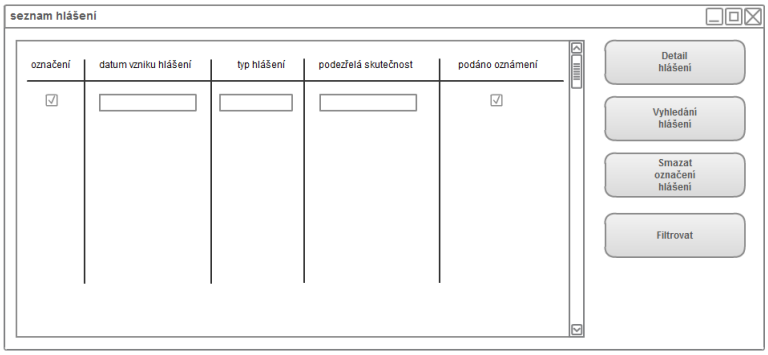
---

[84] Pokud je hlášení generováno systémem, je jako zaměstnanec uveden CO, který hlášení zkoumá.

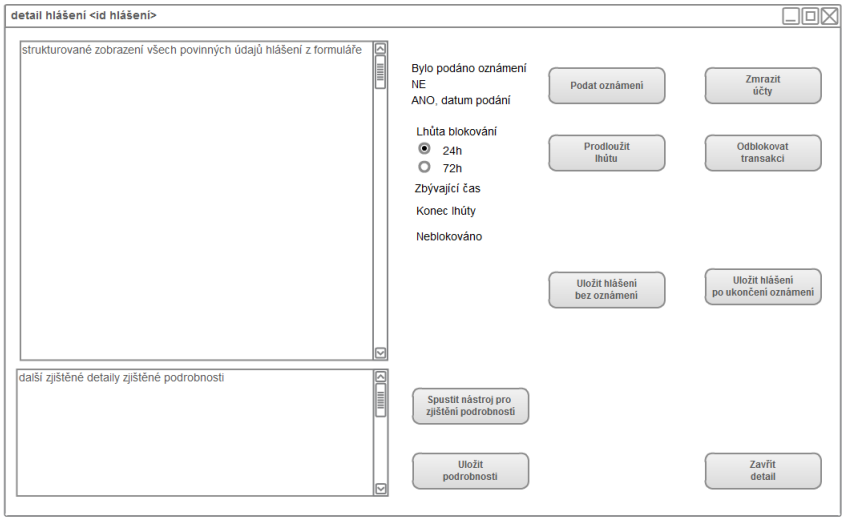
[85] Zobrazovat se může v podstatě cokoliv. Pro jednoduší naplnění povinnosti mlčenlivosti je lepší neinformovat ani zaměstnance. Samozřejmě zaměstnanec není *blbec*, a když se zamyslí nad sledem událostí *podal hlášení a nastaly technické potíže*, zřejmě ho, jako správně proškoleného v AML, *něco* napadne, avšak jedná se pouze jeho domněnku, nikoliv jistotu.

[86] Systém správy hlášení musí CO umožňovat tvorbu reportů, spouštění analýz a pokud možno i přístup ke všem relevantním transakčním systémům banky.

zkušeností, avšak pravdou je, že zřejmě nepřekonatelné bariéry postoupení do této fáze jsou především v osobní zodpovědnosti CO za oznámení a nedostatečně dlouhé transakční historii – málokomu projde na jednom účtu několik pokusů o legalizaci výnosů. Pokus o legalizaci obvykle nemá dlouhý časový průběh, jedná spíše o nárazovou akci v krátkém časovém úseku[87].



Obrázek 33: Okno seznam hlášení



Obrázek 34: Okno detail hlášení

6.5.3 Oznámení

Oznámení je v podstatě hlášení, kde je však místo identifikačních údajů zaměstnance, který hlášení vytvořil a odeslal, nahrazeno značkou[88] zaměstnance CO, který oznámení podal a datem podání.

6.5.4 Analýza a reporty podezřelého chování

Část systému, která má za úkol rychle a přesně podporovat rozhodování CO hledáním shody mezi známými pravidly průběhu legalizace a detekovaným chováním.

[87] Nervozita a pravděpodobnost odhalení je přímo úměrná časové délce pokusu o trestný čin.

[88] Pro identifikaci CO je použit pouze smluvený kód, seznam kódů a identifikačních údajů všech CO mají banka a FAÚ uložen bezpečně u sebe v trezoru. Důvodem je ochrana CO v případě podání trestního oznámení – spis je přístupný žalované straně a možnost získání identifikace CO podezřelým by mohla nepříjemně ovlivnit vyšetřování, anebo majetek a zdraví CO.

Pro správný chod potřebuje tato část systému dostatek známých pravidel. Pravidla lze vytvořit buď ručně, nebo nasadit analytické nástroje BAM pro jejich vytvoření nad skutečnými daty. Vhodné je propojení pevných algoritmů a heuristiky.

Některé poklady pravidel lze vyčíst přímo ze zákona, jiné vycházejí ze zkušenosti banky nabyté v průběhu jejího *života*, další z konferencí české bankovní asociace apod. Konkrétní nastavení pravidel (limitů a prahů sledování, posloupností činností atd.) nejsou volně dostupná, neboť banky si je pečlivě chrání, aby co možná nejvíce znesnadnily prolomení či obcházení pravidel detekce vycházejícího ze znalosti podstaty kontroly.

CO potřebuje vytvářet také reporty pro vedení, ČNB apod., proto by měla tato část systému umožňovat nastavení konkrétních sledovaných ukazatelů (počet hotovostní transakcí, průměrný objem vkladu,aj.), jejich agregace, volbu grafického výstupu, nastavení výstupu do externího souboru apod.

Součástí detekce je hledání shody polí z transakce a seznamy podezřelých osob. Seznamy jsou dvojího typu – interní a externí. Interní aktualizuje CO, externí jsou systémově aktualizovány v přednastavených časových intervalech.

6.5.5 Dashboard

Kdo se těšil na otáčkoměry, bude nejspíš zklamaný, neboť centrální panel obsluhy pro CO je složen z dílčích pouze z následujících prvků:

- podokna
  - seznam upozornění,
  - seznam hlášení,
  - seznam školení,
- tlačítka
  - tvorba reportů,
  - analýza,
  - vytvořit hlášení,
  - aktualizace seznamů a black-listů,
  - aktualizace zařazení klienta.

6.5.6 Konkrétní řešení

Bohužel nejsem obeznámen s konkrétními systémy v bankách a jejich vzájemným propojením, a výstupy k uživatelům.

Nepochybně systémy mají, používají a dost za ně zaplatily nebo stále platí a cesta vytvoření řešení na zelené louce nepřichází v úvahu.

Jako vhodné mi přijde řešení typu BAM/BI. Velké objemy historických transakcí a trendy v nich jsou zpracovávány pomocí BI, zatímco detekování a varování na aktuální činnosti má na starosti BAM. Možná by šlo uvažovat i o nasazení i databázové řešení doplněné BAM nástroje. Tato řešení lze umístit vedle stávajících a užitím middlewaru pro zajištění komunikace mezi jednotlivými systémy pak vše provozovat. Ale jedná se pouze o můj osobní názor, skutečnost může být jiná. Jedná se o specifický problém svázaný s konkrétním prostředím banky a jím danými možnostmi/omezeními integrace BAM řešení – mimo rozsah mé práce.

Volba pořízení řešení vlastními silami nebo externím dodavatelem je na zvážení. Oba přístupy nabízejí určité výhody a nevýhody. V rámci této práce se jimi nechci zabývat.

7 Závěr

Motivaci pro zpracování daného tématu byl původní záměr pokusit se nalézt uplatnění pro BAM při monitorování obchodních aktivit mimo/vně podniku. Při bližším seznamování se s tématem došlo k přehodnocení tohoto záměru a přiklonění se méně ambiciózním cílům, které jsou prezentovány v úvodu.

Prvním vytýčeným cílem bylo shrnutí pohledů na BAM od vzniku až po současnost, s případným odhadem budoucího vývoje. V průběhu sběru a vyhodnocování dat se projevila očekávaná omezení i jiné obtíže. V době uvedení BAM na svět byla BAM často vysvětlována jako samostatná technologie, o které se bohatě psalo a nebylo obtížné ji sledovat. Postupem času však technologie začala prorůstat jinými oblastmi a tudíž přestala být snadno viditelná a sběr dat se zkomplikoval, neboť se musely procházet zdroje tematicky příbuzné k BAM. Je patrné, že technologie má potenciál k dalšímu růstu a rozvoji, což plyne z vysokých cen analýz společnosti Gartner, která BAM vymyslela a pravidelně o ní publikuje články. Několik zdrojů pro nalezení přesnějších dat o jejím současném stavu zůstalo za hranicí vysoké pořizovací ceny, avšak tuto překážku se podařilo částečně odstranit odhady a zkoumáním a výkladem metadat nedostupných dokumentů. Veskrze hodnotím výsledek o popsání vývoje BAM jako úspěšně podchycené a popsané i přes horší dostupnost aktuálních materiálů. Samozřejmě získáním a zapracováním *nedostupných* materiálů by nepochybně došlo ke zpřesnění.

Dalším cílem bylo detailně popsat BAM. Celkově se jsem se držel spíše úrovně myšlenek a konceptuálního řešení. Jako hlavní smysl jsem si vytýčil seznámit čtenáře s fungováním BAM na úrovni vyšší míry obecnosti. Rozhodně nebylo mojí snahou řešit nižší úrovně fungování – konkrétní řešení a použitelné technologie pro předávání zpráv, či propojení jednotlivých aplikací. Zde nechávám příležitost pro navázání a podrobné zmapování na případných zájemcích o rozšíření.

Tato část je rozdělena na více oblastí, které dohromady podávají ucelený pohled. Uvádím několik definic, lišících se typicky podle zaměření autora (vývojář, integrátor apod.). Významnou část věnuji podrobnému popisu modelu fungování a popisu možných reakcí, které může BAM poskytovat, či vyvolávat.

Můj názor je, že se podařilo vytvořit text, popisující nejen samotné fungování ,ale i zahrnutí dalších aspektů neležících přímo v IT, které mají na BAM vliv.

Předposledním cílem bylo zařadit a vymezit pozici BAM mezi jinými podnikovými aplikacemi. Jako nejdůležitější jsem shledal vymezení BAM shora a zespodu. Zespodu omezují BAM systémy BSM, které primárně slouží ke sledování informatických zdrojů. Shora BAM omezují, ale mohou se společně prolínat, systémy BI, které jsou zaměřeny na podporu rozhodování na vyšší úrovni než má BAM.

Při získávání podkladů jsem narazil i na další technologie, například BPM, který BAM využívá, avšak z hlediska vymezení myslím, že by mohl spíše být na podobné úrovni. Nicméně propojení těchto dvou technologií v práci nenajdete. Opět si myslím, že se jedná o zajímavé a obsáhlejší téma, které lze rozpracovat v samostatné práci. Podobně jako třeba využití SOA při BAM řešeních.

Posledním a nejtěžším cílem byl návrh konceptu reálného použití BAM v bankovním prostředí při implementaci AML. K dispozici jsem měl znění zákona, názory a zkušenosti compliance. K vytvoření návrhu jsem nepoužil žádnou metodiku, vycházel jsem ze své intuice. Snažil jsem se navrhnout výslednou podobu nástroje, který pracovníkům compliance poskytne možnost centralizované správy činností spojených s AML a přitom přispěje k řízení rizik, které se v souvislosti s AML objevují.

Klíčovým pro návrh podpory je identifikace rizik. Rizika jsem identifikoval přímo ze zákona. Poté jsem se snažil najít v současném stavu řešení a navrhl k nim způsoby jejich řízení. Rizika tedy byla známa a bylo nutné je připojit ke konkrétním bankovním procesů.

Pro podporu jsou podstatné dva pojmy – upozornění a hlášení. Hlášení je naprosto elementárním prvkem, neboť se jedná o řídící událost, která je pro správnou podporu BAM potřebná.

V rámci řešení jsem se omezil na návrh, který neřeší konkrétní technické řešení a pro oblast zájmu jsem vybral pouze banky a jejich transakce ovlivněné AML. Neřeším ani konkrétně algoritmy pro detekci určitého podezřelého chování. Samozřejmě část systému s algoritmy je součástí modelování, ale přesný obsah jsem neřešil. Důvody jsou dva – 1) jedná se o střežená tajemství z hlediska bank i bankovnictví, 2) jejich podrobnější návrh by si zasloužil vlastní zpracování.

Výsledkem mého snažení je základní kámen/kamínek, o který je možné se opřít při vypracovávání dalších podrobností a směrů v dané problematice. Dalšími směry pro navázání mohou být již zmíněné algoritmy/systémy pro odhalování podezřelého chování; zamyšlení nad možnosti pořízení takového systému; popis nižších úrovní řešení (technologie pro komunikaci mezi bankovními systémy a BAM – middleware); rozšíření návrhu o další instituce, pro které je AML závazný.

Dle mého názoru bude v budoucnu růst potřeba nalézání a detekce určitých konkrétních dat, na která bude nezbytné rychle reagovat, ať už z důvodu tlaku konkurence nebo tlaku regulátora trhu. BAM jistě může výrazně přispět a návrh použití BAM jako podpory při řízení rizik spojených s AML jasně ukazuje potenciál a možnosti, které IT/ICT podnikání mohou poskytnout.

8 Terminologický slovník

Termín	Zkratka	Význam
Anti-Money Laundering	AML	Anti-Money Laundering, soubor pravidel v oblastech práva a bankovnictví pro prevenci legalizace výnosů trestní činnost a terorismu; základ představuje zákon č. 253/2008 Sb.
Back-office		Oddělení banky, na kterých nedochází k přímému kontaktu s klientem
Busienss Service Management	BSM	Nástroje pro sledování a měření výkonnost IT služeb z business perspektivy (Bus093)
Business Activity Monitoring	BAM	Termín definuje, jak je možné zajistit přístup ke klíčovým podnikovým ukazatelům v reálném čase. Cílem zavedení takového systému je zvýšení rychlosti a efektivity podnikových operací (McCoy, 2002)
Business Inteligence	BI	Sada procesů, aplikací a technologií, jejichž cílem je účinně a účelně podporovat rozhodovací procesy ve firmě. Podporují analytické a plánovací činnosti podniků a organizací a jsou postaveny na principech multidimenzionálních pohledů na podniková data. (Novotný, a další, 2005)
Business Process Modeling Notation	BPMN	Notace používaná pro modelování business procesů
Compliance		Oddělení banky, které ma starosti usměrňovat chování banky podle platných zákonů a předpisů
Compliance Officer	CO	Pracovník banky oddělení compliance.
Dashboard		Metaforický název pro třetí vrstvu modelu BAM, vrstva "akce, doručení a zobrazení událostí"; někdy se používá termín kokpit nebo palubní deska vzhledem k podobnostem s autem
Event-based marketing		Marketing založený na využívání významných událostí na straně klienta (např. narozeniny)
Extract Transform Load	ETL	Systémy extrakce, transformace a přenos dat (Novotný, a další, 2005)
Finančně-analytický útvar	FAÚ	Odbor Ministerstva financí, který má na starosti přezkoumávání oznámení o podezřelých obchodech dle AML.
Front-office		Oddělení banky, na kterých dochází k přímému kontaktu s klientem
Gartner		Přední analytická a konzultační firma světa v oblasti informačních technologií založená v roce 1979 ve městě Stamford, Connecticut, USA
Hlášení		Interní dokument, který upozorňuje CO na podezřelý obchod
Information Technology Infrastructure Library	ITIL	Mezinárodně uznávaný standard pro řízení IT služeb (ITI09)
Klient		Osoba, která je v obchodním vztahu s bankou

Maturity level		Vyzrálost podnikových procesů, celkem je definována 5 úrovní (ad hoc, repeatable, defined, managed, optimized) (Cap09)
Middleware		Druh softwaru, který spojuje jiné softwarové komponenty a aplikace mezi sebou (Mid09)
Ministerstvo financní ČR	MF ČR	jeden z regulátorů českého bankovního trhu.
Neklient		Osoba, která není v obchodním vztahu s bankou
Operational data store	ODS	Databáze navržená speciálně pro integraci dat z různých datových zdrojů za účelem usnadnění analýz a reportování.
Oznámení pro FAÚ		Hlášení, ve kterém CO identifikoval možnost podezřelého obchodu a odeslal jej na FAÚ
Politicky exponovaná osoba	PEO	Osoby, kterým jsou svěřeny významné veřejné funkce, jejich nejbližší rodinní příslušníci nebo osoby známé jako blízcí společníci takových osob (ČR, 2008)
Potenciálně problémový klient	PPK	Termín používaný v této práci pro označení osoby, která se nachází na některém ze seznamů sankcionovaných osob podle AML
Real-Time Store	RTS	Databáze pro ukládání události v systémech BAM (LeHong, 2009)
Regulátor		V českém právní prostředí - Ministerstvo financí ČR a ČNB
Reputační riziko		Možnost ztráty dobrého jména banky na trhu.
Trestní zákoník		Zákon č. 40/2009 Sb. (ČR, 2009)
Voice over IP	VoIP	Technologie, umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů UDP/TCP/IP prostřednictvím počítačové sítě nebo jiného média, prostupného pro protokol IP. Využívá se pro telefonování prostřednictvím Internetu, intranetu nebo jakéhokoliv jiného datového spojení (Voi09)
WorldCheck		Veřejně přístupná světová databáze politicky exponovaných osob, www.worldcheck.com
Zákon o platebním styku		Zákon č. 284/2009 Sb. (ČR, 2009)

9 Citovaná literatura

Business Activity Monitoring [Online] // Wikipedia. - 23. 11 2009. - http://en.wikipedia.org/wiki/Business_activity_monitoring.

Business intelligence [Online] // Wikipedia. - 10. 11 2009. - http://en.wikipedia.org/wiki/Business_intelligence.

Business Service Management [Online] // Wikipedia. - 13. 12 2009. - http://en.wikipedia.org/wiki/Business_service_management.

Capability Maturity Model [Online] // Wikipedia. - 13. 12 2009. - http://en.wikipedia.org/wiki/Capability_Maturity_Model.

Correia Joanne a Schroder Norma BAM: A Composite Market View [Online] // Siventures. - 1. 4 2002. - 3. 11 2009. - http://www.siventures.com/portfolio/pdf/070202/BAM.pdf.

ČR Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti [Online] // Portál veřejné správy České republiky. - 5. 6 2008. - 3. 12 2009. - http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=253/2008&PC_8411_l=253/2008&PC_8411_ps=10#10821.

ČR Zákon č. 284/2009 Sb., o platebním styku [Online] // Portál veřejné správy České republiky. - 1. 11 2009. - 2. 12 2009. - http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_name=o%20platebn%C3%ADm%20styku&PC_8411_l=284/2009&PC_8411_ps=10#10821.

ČR Zákon č. 40/2009 Sb., trestní zákoník [Online] // Ministerstvo vnitra. - 9. 2 2009. - 3. 12 2009. - www.mvcr.cz/soubor/sb011-09-pdf.aspx.

ČS a.s. Příkaz přes zahraniční platební styk [Online]. - 13. 12 2009. - 13. 12 2009. - www.servis24.cz.

Dokoupil Otakar Business Inteligence [Online] // isis.vse.cz. - 2006. - 1. 11 2009. - https://isis.vse.cz/auth/lide/clovek.pl?zalozka=7;id=14916;studium=4809;download_prace=1.

Erben Lukáš a Gruman Galen Priority CIO pro rok 2009 [Článek] // CIO Business World. - 2/2009. - str. 12.

Erben Lukáš a Jirásko Tomáš Vytěžování ERP [Článek] // CIO Business World. - 3/2009. - str. 14.

Erben Lukáš IT jako konkurenční výhoda [Článek] // CIO Business World. - 10/2009. - str. 31.

Gartner [Online] // Near-Time.net. - 2. 11 2009. - http://www.near-time.org/pdf/hype_cycle.pdf.

Gartner Hype Cycle for Business Intelligence and Performance Management, 2009 [Online] // Gartner. - 10. 11 2009. - http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&id=1094612&ref=.

Gartner Hype Cycle for Business Process Management, 2009 [Online] // Gartner. - 10. 11 2009. - http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&docCode=167464&ref=docDisplay.

Gassman B. Clarifying the Definition of Business Activity Monitoring [Online] // Google docs. - 4. 6 2003. - 24. 11 2009. -

http://docs.google.com/viewer?a=v&q=cache:fYjbnNrQCfoJ:www.bus.umich.edu/KresgePublic/Journals/Gartner/research/115300/115355/115355.pdf+Clarifying+the+Definition+of+Business+ActivityMonitoring&hl=cs&gl=cz&pid=bl&srcid=ADGEESjLFM89kmiGVjGjZ_ACzkEPL93Miv9X.

Gassman B. Hype Cycle for Business Activity Monitoring, 2003 [Online] // Michigan Ross School of Business. - 22. 9 2003. - 15. 11 2009. - http://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/117400/117446/117446.pdf.

Gassman Bill a Curtis Debra Business Activity Monitoring and Business Service Management Are Different [Online] // Gartner. - 9. 10 2009. - 20. 11 2009. - http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&resId=1203613&ref=QuickSearch&sthkw=business+activity+monitoring.

Govekar Milind [a další] Turning the Theory of BAM Into a Working Reality [Online]. - 18. 3 2002. - 13. 11 2009. - https://ekms.ultimatix.net/Gartnernewone/research/105100/105190/105190.html.

Hoffmann Thomas a Erben Tomáš Devět IT specializací pro rok 2009 [Článek] // CIO Business World. - 2/2009. - stránky 10-11.

ITIL [Online] // Wikipedia. - 13. 12 2009. - http://cs.wikipedia.org/wiki/Information_Technology_Infrastructure_Library.

Jirásko Tomáš BI a knowledge management [Článek] // CIO Business World. - 2/2009. - str. 30.

Jirásko Tomáš Business trendy [Článek] // CIO Business World. - 11/2009. - str. 6.

Jirásko Tomáš Business Trendy: IT krize je i příležitostí [Článek] // CIO Business World. - 7,8/2009. - str. 6.

Kotek Jan Business Activity Monitoring - monitorování aktivit podniku [Online] // si.vse.cz. - 2004. - 15. 11 2009. - http://si.vse.cz/archive/proceedings/2004/business-activity-monitoring-monitorovani-aktivit-podniku.pdf.

LeHong Hung The Real-Time Store Monitoring Platform [Online] // BVI Networks. - 26. 8 2009. - 11. 11 2009. - http://www.bvinetworks.com/library/the_realtime_store_monitoring.pdf.

Luckham David Bringing Order to the Business Activity Monitoring [Online] // ebizQ. - 19. 6 2005. - 3. 11 2009. - http://www.ebizq.net/topics/operational_bi/features/6044.html.

Luckham David The Beginnings of IT Insight: Business Activity [Online] // ebizq.net. - 21. 6 2004. - 5. 11 2009. - http://www.ebizq.net/topics/bam/features/4689.html.

Lynn Jonathan a Jay Anthony Jistě pane ministře. [Kniha]. - Praha : Aurora, 2003. - Sv. II. část. - 80-7299-060-8.

McCoy David a Govekar Milind Evolving Interaction Styles in Business Activity Monitoring [Online]. - 22. 8 2002. - 5. 11 2009. - https://ekms.ultimatix.net/Gartnernewone/research/109300/109363/109363.html.

McCoy David Business Activity Monitoring: The Merchant's Tale [Online]. - 26. 8 2002. - 10. 11 2009. - https://ekms.ultimatix.net/Gartnernewone/research/106400/106406/106406.html.

McCoy David W. Business Activity Monitoring: Calm Before the Storm [Online] // Gartner. - 4 2002. - 2. 11 2009. - http://www.gartner.com/resources/105500/105562/105562.pdf.

Microsoft Zlepšení dodržování předpisů [Online]. - 14. 11 2009. - http://www.microsoft.com.nsatc.net/cze/business/peopleready/compliance/strategic_analysis.mspx.

Middleware [Online] // Wikipedia. - 13. 12 2009. - http://en.wikipedia.org/wiki/Middleware.

Novotný Ota, Pour Jan a Slánský David Business Intelligence [Kniha]. - Praha : Grada, 2005. - 80-247-1094-3.

Operational Data Store [Online] // Wikipedia. - 13. 12 2009. - http://en.wikipedia.org/wiki/Operational_data_store.

Pedrinaci Carlos [a další] SENTINEL: A Semantic Business Process Monitoring Tool [Online] // ACM Portal. - 2008. - 6. 11 2009. - http://portal.acm.org.ezproxy.vse.cz/citation.cfm?id=1452567.1452568&coll=ACM&dl=ACM&CFID=61563650&CFTOKEN=21499194.

Polymita Business Activity Monitoring [Online] // Polymita - Empowering Business Productivity. - 10. 11 2009. - http://www.polymita.com/portal/bpm/Performance_Indicators.

Smalltree Hannah Gartner sees BI, CPM together for the long haul [Online] // SearchSAP.com. - 07. 03 2006. - 4. 11 2009. - http://searchsap.techtarget.com/news/article/0,289142,sid21_gci1171651,00.html.

Synáček Václav Metodika vývoje IS [Online] // ISIS. - 2007. - 1. 11 2009. - https://isis.vse.cz/auth/lide/clovek.pl?id=7392;zalozka=7;studium=46167.

Voice over IP [Online] // Wikipedia. - 13. 12 2009. - http://cs.wikipedia.org/wiki/Voice_over_Internet_Protocol.

Wailgum Thomas, Brož Robert a Erben Lukáš Data ≠ informace [Článek] // CIO Business World. - 6/2009. - stránky 14, 15.

What Is BAM? [Online] // MSDN Library. - Microsoft. - 5. 11 2009. - http://msdn.microsoft.com/en-us/library/aa560139(BTS.10).aspx.

White Colin BAM and Business Intelligence [Online] // Information Management. - 9 2003. - 2. 11 2009. - http://www.information-management.com/issues/20030901/7304-1.html.

White Colin Is BAM well and Alive? [Online] // Information Management. - 9 2005. - 2. 11 2009. - http://www.information-management.com/issues/20050901/1035618-1.html.

10 Seznamy

10.1 Seznam obrázků

10.2 Seznam grafů

10.3 Seznam tabulek

11 Přílohy

11.1 AML, zákon č. 253/2008 Sb., v platném znění

Systém ASPI - stav k 7.12.2009 do částky 136/2009 Sb. a 46/2009 Sb. m. s.
Obsah a text 253/2008 Sb. - poslední stav textu nabývá účinnost až od 1. 1. 2011

253/2008 Sb.

ZÁKON
ze dne 5. června 2008

o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

Změna: 285/2009 Sb.
Změna: 227/2009 Sb.
Změna: 281/2009 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Předmět úpravy

Tento zákon zapracovává příslušné předpisy Evropských společenství 1), zároveň navazuje na přímo použitelné předpisy Evropských společenství 2) a upravuje

a) některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu,

b) některá práva a povinnosti fyzických a právnických osob při uplatňování opatření proti legalizaci výnosů z trestné činnosti a financování terorismu,

a to za účelem zabránění zneužívání finančního systému k legalizaci výnosů z trestné činnosti a k financování terorismu a vytvoření podmínek pro odhalování takového jednání.

§ 2

Povinné osoby

(1) Povinnou osobou se pro účely tohoto zákona rozumí

a) úvěrová instituce, kterou je
1. banka,
2. spořitelní a úvěrní družstvo,
3. instituce elektronických peněz,
4. vydavatel elektronických peněz malého rozsahu 3),
5. platební instituce, poskytovatel platebních služeb malého rozsahu 3),

b) finanční instituce, kterou, pokud není úvěrovou institucí, je
1. centrální depozitář, osoba vedoucí evidenci navazující na centrální evidenci cenných papírů vedenou centrálním depozitářem, osoba vedoucí samostatnou evidenci investičních nástrojů, osoba vedoucí evidenci navazující na samostatnou evidenci investičních nástrojů 4),
2. organizátor trhu s investičními nástroji,
3. osoba s povolením k poskytování investičních služeb 5) s výjimkou investičního zprostředkovatele 6),
4. investiční společnost, investiční fond a penzijní fond,
5. osoba oprávněná k vydávání nebo správě bezhotovostních platebních prostředků,
6. osoba oprávněná k poskytování leasingu, záruk, úvěrů nebo peněžních půjček anebo k obchodování s nimi,
7. osoba oprávněná ke zprostředkování spoření, leasingu, úvěrů nebo peněžních půjček,
8. pojišťovna, zajišťovna, pojišťovací zprostředkovatel a samostatný likvidátor pojistných událostí při výkonu činností souvisejících s provozováním životního pojištění 7), s výjimkou pojišťovacího zprostředkovatele, u něhož pojišťovna nese odpovědnost za škodu způsobenou jeho činností,
9. osoba, která vykupuje dluhy a pohledávky a obchoduje s nimi,
10. osoba oprávněná ke směnárenské činnosti podle devizového zákona,
11. osoba neuvedená v bodech 1 až 10, oprávněná k provádění nebo zprostředkování platebních služeb nebo poštovních služeb, jejichž účelem je dodání poukázané peněžní částky,

12. osoba oprávněná k poradenské činnosti pro podnikatele ve věcech kapitálové struktury, průmyslové strategie nebo k poradenství a službám v oblasti fúzí a koupě podniků,
13. osoba poskytující služby peněžního makléřství,
14. osoba poskytující služby úschovy cenností,

c) držitel povolení k provozování sázkových her v kasinu podle zákona o loteriích a jiných podobných hrách,

d) osoba oprávněná k obchodování s nemovitostmi nebo ke zprostředkování obchodu s nimi,

e) auditor, daňový poradce a účetní,

f) soudní exekutor při provádění další činnosti exekutora podle exekučního řádu a při úschově peněz, cenných papírů nebo jiného majetku,

g) notář při úkonech v rámci notářské úschovy 8) anebo advokát nebo notář při úschově peněz, cenných papírů nebo jiného majetku svého klienta, anebo jestliže klientem požadované služby mají spočívat nebo spočívají v jednání jménem klienta nebo na jeho účet při
1. obstarávání koupě nebo prodeje nemovitosti nebo podniku 9) anebo jeho části,
2. správě peněz, cenných papírů, obchodních podílů nebo jiného majetku svého klienta, včetně jednání jménem klienta nebo na jeho účet v souvislosti se zřízením účtu u úvěrové instituce nebo zahraniční úvěrové instituce anebo účtu cenných papírů a správou takového účtu,
3. zakládání, řízení nebo provozování obchodní společnosti, podnikatelského seskupení nebo jiného obdobného útvaru, a to bez ohledu na to, zda se jedná o právnickou osobu či nikoliv, jakož i získávání a shromažďovaní peněžních prostředků nebo jiných penězi ocenitelných hodnot za účelem založení, řízení nebo ovládání takového subjektu, nebo
4. inkasu, platbách, převodech, vkladech nebo výběrech prováděných při bezhotovostním i hotovostním platebním styku, anebo jakémkoli jiném jednání, které směřuje k pohybu peněz nebo jej přímo vyvolá,

h) osoba nenaplňující znaky podle písmen a) až g), poskytující jiné osobě služby, které spočívají v
1. zakládání právnických osob,
2. jednání jako statutární orgán nebo jeho člen, další osoba, která je oprávněna jménem nebo za právnickou osobu jednat, anebo jiná osoba v obdobném postavení, pokud výkon této služby je pouze dočasný a souvisí se založením a správou právnické osoby,
3. poskytování sídla, adresy, popřípadě i dalších s tím souvisejících služeb pro jinou právnickou osobu,
4. jednání jako pověřený akcionář pro jinou osobu, pokud tato není společností, jejíž cenné papíry jsou přijaty k obchodování na regulovaném trhu a která podléhá požadavkům na zveřejnění informací rovnocenným požadavkům práva Evropských společenství, nebo
5. jednání jejím jménem nebo na její účet při činnostech uvedených v písmenu g),

i) osoba, která poskytuje služby uvedené v písmenu h) v rámci svěřeneckého vztahu nebo jiného obdobného smluvního vztahu podle cizího právního řádu,

j) osoba oprávněná k obchodování s kulturními památkami 10) nebo s předměty kulturní hodnoty 11) nebo ke zprostředkování takových obchodů,

k) osoba oprávněná k obchodování s použitým zbožím nebo ke zprostředkování takových obchodů nebo k přijímání věcí do zástavy.

(2) Povinnou osobou je rovněž

a) zahraniční právnická nebo fyzická osoba uvedená v odstavci 1, která na území České republiky působí prostřednictvím své pobočky, organizační složky nebo provozovny, a to v rozsahu činnosti touto pobočkou, organizační složkou nebo provozovnou vykonávané,

b) na území České republiky působící zahraniční osoba, pokud jako podnikatel vykonává činnosti uvedené v odstavci 1,

c) Středisko cenných papírů,

d) podnikatel, který není uveden v odstavci 1, jestliže přijímá platbu v hotovosti v hodnotě 15 000 EUR nebo vyšší,

e) právnická osoba, která není podnikatelem, pokud je oprávněna poskytovat jako službu některou z činností uvedených v odstavci 1, nebo pokud přijímá platbu v hotovosti v hodnotě 15 000 EUR nebo vyšší.

(3) Povinnou osobou není, s výjimkou osoby uvedené v odstavci 2 písm. d) a e), osoba, která činnosti uvedené v odstavci 1 nevykonává jako předmět svého podnikání.

§ 3

Základní pojmy

(1) Legalizací výnosů z trestné činnosti se pro účely tohoto zákona rozumí jednání sledující zakrytí nezákonného původu jakékoliv ekonomické výhody vyplývající z trestné činnosti s cílem vzbudit zdání, že jde o majetkový prospěch nabytý v souladu se zákonem; uvedené jednání spočívá například

a) v přeměně nebo převodu majetku s vědomím, že pochází z trestné činnosti, za účelem jeho utajení nebo zastření jeho původu nebo za účelem napomáhání osobě, která se účastní páchání takové činnosti, aby unikla právním důsledkům svého jednání,

b) v utajení nebo zastření skutečné povahy, zdroje, umístění, pohybu majetku nebo nakládání s ním nebo změny práv vztahujících se k majetku s vědomím, že tento majetek pochází z trestné činnosti,

c) v nabytí, držení, použití majetku nebo nakládání s ním s vědomím, že pochází z trestné činnosti, nebo

d) ve zločinném spolčení osob nebo jiné formě součinnosti za účelem jednání uvedeného pod písmeny a), b) nebo c).

(2) Financováním terorismu je

a) shromažďování nebo poskytnutí peněžních prostředků nebo jiného majetku s vědomím, že bude, byť i jen zčásti, použit ke spáchání trestného činu teroru 12), teroristického útoku 13) nebo trestného činu, který má umožnit nebo napomoci spáchání takového trestného činu 14), nebo k podpoře osoby nebo skupiny osob připravujících se ke spáchání takového trestného činu, nebo

b) jednání vedoucí k poskytnutí odměny nebo odškodnění pachatele trestného činu teroru, teroristického útoku nebo trestného činu, který má umožnit nebo napomoci spáchání takového trestného činu 14), nebo osoby pachateli blízké ve smyslu trestního zákona 15), nebo sbírání prostředků na takovou odměnu nebo na odškodnění.

(3) Pro účely tohoto zákona není rozhodující, zda k jednání uvedenému v odstavci 1 nebo 2 nebo ke spáchání trestného činu došlo nebo má dojít zcela nebo zčásti na území České republiky nebo v cizině.

§ 4

Další pojmy

(1) Obchodem se pro účely tohoto zákona rozumí každé jednání povinné osoby s jinou osobou, pokud takové jednání směřuje k nakládání s majetkem této jiné osoby nebo k poskytnutí služby této jiné osobě.

(2) Obchodním vztahem se pro účely tohoto zákona rozumí smluvní vztah mezi povinnou osobou a jinou osobou, jehož účelem je nakládání s majetkem této jiné osoby nebo poskytování služeb této jiné osobě, jestliže je při vzniku smluvního vztahu s přihlédnutím ke všem okolnostem zřejmé, že bude obsahovat opakující se plnění.

(3) Příkazem klienta se pro účely tohoto zákona rozumí každý jeho úkon, na jehož základě má povinná osoba nakládat s majetkem.

(4) Skutečným majitelem se pro účely tohoto zákona rozumí

a) u podnikatele
1. fyzická osoba, která fakticky nebo právně vykonává přímo nebo nepřímo rozhodující vliv na řízení nebo provozování podniku tohoto podnikatele; nepřímým vlivem se rozumí vliv vykonávaný prostřednictvím jiné osoby nebo jiných osob,
2. fyzická osoba, která sama nebo na základě dohody s jiným společníkem nebo společníky disponuje více než 25 % hlasovacích práv tohoto podnikatele; disponováním s hlasovacími právy se rozumí možnost vykonávat hlasovací práva na základě vlastního uvážení bez ohledu na to, zda a na základě jakého právního důvodu jsou vykonávána, popřípadě možnost ovlivňovat výkon hlasovacích práv jinou osobou,
3. fyzické osoby jednající ve shodě, které disponují více než 25 % hlasovacích práv tohoto podnikatele, nebo
4. fyzická osoba, která je na základě jiné skutečnosti příjemcem výnosů z činnosti tohoto podnikatele,

b) u nadace nebo nadačního fondu
1. fyzická osoba, která má být příjemcem alespoň 25 % z rozdělovaných prostředků, nebo
2. nebylo-li rozhodnuto, kdo bude příjemcem výnosů nadace nebo nadačního fondu, fyzická osoba nebo okruh osob, v jejichž zájmu byly založeny, nebo v jejichž zájmu působí,

c) u sdružení podle jiného právního předpisu 16), obecně prospěšné společnosti anebo jiné obdobné osoby a v případě svěřeneckého vztahu nebo jiného obdobného vztahu podle cizího právního řádu fyzická osoba,
1. která disponuje více než 25%jejich hlasovacích práv nebo majetku,
2. která má být příjemcem alespoň 25 % z rozdělovaných prostředků, nebo
3. v jejímž zájmu byly založeny nebo v jejímž zájmu působí, nebylo-li rozhodnuto, kdo bude příjemcem jejich výnosů.

(5) Politicky exponovanou osobou se pro účely tohoto zákona rozumí

a) fyzická osoba, která je ve významné veřejné funkci s celostátní působností, jako je například hlava státu nebo předseda vlády, ministr, náměstek nebo asistent ministra, člen parlamentu, člen nejvyššího soudu, ústavního soudu nebo jiného vyššího soudního orgánu, proti jehož rozhodnutí obecně až na výjimky nelze použít opravné prostředky, člen účetního dvora, člen vrcholného orgánu centrální banky, vysoký důstojník v ozbrojených silách nebo sborech, člen správního, řídicího nebo kontrolního orgánu podniku ve vlastnictví státu, velvyslanec nebo chargé d'affaires, nebo fyzická osoba, která obdobné funkce vykonává v orgánech Evropské unie nebo jiných mezinárodních organizací, a to po dobu výkonu této funkce a dále po dobu jednoho roku po ukončení výkonu této funkce, a která
1. má bydliště mimo Českou republiku, nebo
2. takovou významnou veřejnou funkci vykonává mimo Českou republiku,

b) fyzická osoba, která
1. je k osobě uvedené v písmenu a) ve vztahu manželském, partnerském anebo v jiném obdobném vztahu nebo ve vztahu rodičovském,
2. je k osobě uvedené v písmenu a) ve vztahu syna nebo dcery nebo je k synovi nebo dceři osoby uvedené v písmenu a) osobou ve vztahu manželském (zeťové, snachy), partnerském nebo v jiném obdobném vztahu,
3. je společníkem nebo skutečným majitelem stejné právnické osoby, popřípadě svěřenectví nebo jiného obdobného právního uspořádání podle cizího právního řádu, jako osoba uvedená v písmenu a), nebo je o ní povinné osobě známo, že je v jakémkoli jiném blízkém podnikatelském vztahu s osobou uvedenou v písmenu a), nebo
4. je skutečným majitelem právnické osoby, popřípadě svěřenectví nebo jiného obdobného právního uspořádání podle cizího právního řádu, o kterém je známo, že bylo vytvořeno ve prospěch osoby uvedené v písmenu a).

(6) Průkazem totožnosti se pro účely tohoto zákona rozumí doklad vydaný orgánem veřejné správy, v němž je uvedeno jméno a příjmení, datum narození a z něhož je patrná podoba, popřípadě i jiný údaj umožňující identifikovat osobu, která doklad předkládá, jako jeho oprávněného držitele.

(7) Korespondenčním bankovním vztahem se pro účely tohoto zákona rozumí smluvní vztah mezi úvě- rovou institucí nebo zahraniční úvěrovou institucí, působící prostřednictvím své pobočky na území České republiky, a úvěrovou nebo obdobnou institucí v zahraničí, který úvěrové instituci, zahraniční úvěrové instituci, působící prostřednictvím své pobočky na území České republiky, anebo úvěrové nebo obdobné instituci v zahraničí umožňuje provádět platby do zahraničí, nebo přijímat platby ze zahraničí prostřednictvím druhé smluvní strany.

§ 5

Identifikační údaje

Pro účely tohoto zákona se identifikačními údaji rozumí

a) u fyzické osoby všechna jména a příjmení, rodné číslo, a nebylo-li přiděleno, datum narození, místo narození, pohlaví, trvalý nebo jiný pobyt a státní občanství; jde-li o podnikající fyzickou osobu, též její obchodní firma, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo osoby,

b) u právnické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, sídlo, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí; u osob, které jsou jejím statutárním orgánem nebo jeho členem, údaje podle písmene a).

§ 6

Podezřelý obchod

(1) Podezřelým obchodem se pro účely tohoto zákona rozumí obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu, anebo jiná skutečnost, která by mohla takovému podezření nasvědčovat, a to pokud například

a) klient provádí výběry nebo převody na jiné účty bezprostředně po hotovostních vkladech,

b) během jednoho dne nebo ve dnech bezprostředně následujících uskuteční klient nápadně více peněžních operací, než je pro jeho činnost obvyklé,

c) počet účtů zřizovaných klientem je ve zjevném nepoměru k předmětu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,

d) klient provádí převody majetku, které zjevně nemají ekonomický důvod,

e) prostředky, s nimiž klient nakládá, zjevně neodpovídají povaze nebo rozsahu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,

f) účet je využíván v rozporu s účelem, pro který byl zřízen,

g) klient vykonává činnosti, které mohou napomáhat zastření jeho totožnosti nebo zastření totožnosti skutečného majitele,

h) klientem nebo skutečným majitelem je osoba ze státu, který nedostatečně nebo vůbec neuplatňuje opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, nebo

i) povinná osoba má pochybnosti o pravdivosti získaných identifikačních údajů o klientovi.

(2) Podezřelým je obchod vždy, pokud

a) klientem nebo skutečným majitelem je osoba, vůči níž Česká republika uplatňuje mezinárodní sankce podle zákona o provádění mezinárodních sankcí 17),

b) předmětem obchodu je nebo má být zboží nebo služby, vůči nimž Česká republika uplatňuje sankce podle zákona o provádění mezinárodních sankcí 17), nebo

c) klient se odmítá podrobit kontrole nebo odmítá uvést identifikační údaje osoby, za kterou jedná.

ČÁST DRUHÁ

ZÁKLADNÍ POVINNOSTI POVINNÝCH OSOB

HLAVA I

IDENTIFIKACE A KONTROLA KLIENTA

§ 7

Povinnost identifikace

(1) Jestliže je povinná osoba účastníkem obchodu v hodnotě převyšující částku 1 000 EUR, před jeho uskutečněním vždy identifikuje klienta, pokud tento zákon dále nestanoví jinak.

(2) Bez ohledu na limit stanovený v odstavci 1 identifikuje povinná osoba klienta rovněž vždy, pokud jde o

a) podezřelý obchod,

b) vznik obchodního vztahu,

c) uzavření smlouvy o účtu, vkladu na vkladní knížce nebo vkladním listu nebo sjednání jiné formy vkladu,

d) uzavření smlouvy o nájmu bezpečnostní schránky nebo smlouvy o úschově,

e) uzavření smlouvy o životním pojištění, má-li klient právo jednostranně hradit další pojistné nad sjednaný rámec plateb jednorázového nebo běžně placeného pojistného,

f) nákup nebo přijetí kulturních památek, předmětů kulturní hodnoty, použitého zboží nebo zboží bez dokladu o jeho nabytí ke zprostředkování jejich prodeje anebo přijímání věcí do zástavy, nebo

g) výplatu zůstatku zrušeného vkladu z vkladní knížky na doručitele.

(3) Povinná osoba identifikuje osobu, která má právo na plnění ze životního pojištění, nejpozději v době vyplacení pojistného plnění.

§ 8

Provádění identifikace

(1) První identifikaci klienta, který je fyzickou osobou, a každé fyzické osoby jednající jménem klienta, který je právnickou osobou, provede povinná osoba za fyzické

přítomnosti identifikovaného, pokud není v tomto zákoně stanoveno jinak.

(2) Při identifikaci klienta, který je

a) fyzickou osobou, povinná osoba identifikační údaje zaznamená a ověří z průkazu totožnosti, jsou-li v něm uvedeny, a dále zaznamená druh a číslo průkazu totožnosti, stát, popřípadě orgán, který jej vydal, a dobu jeho platnosti; současně ověří shodu podoby s vyobrazením v průkazu totožnosti,

b) právnickou osobou, povinná osoba identifikační údaje zaznamená a ověří z dokladu o existenci právnické osoby a v rozsahu podle písmene a) provede identifikaci fyzické osoby, která jejím jménem jedná v daném obchodu; je-li statutárním orgánem, jeho členem nebo ovládající osobou této právnické osoby jiná právnická osoba, zaznamená i její identifikační údaje.

(3) Je-li klient zastoupen na základě plné moci, provádí se identifikace zmocněnce podle odstavce 2 a dále předložením plné moci; tato plná moc se nevyžaduje, jestliže osoba, která jinak nebyla zmocněna k nakládání s peněžními prostředky na účtu, ukládá na účet hotovost a současně doručuje povinné osobě již vyplněné a oprávněnou osobou podepsané doklady, nebo pouze doručuje doklady, na základě kterých má být uskutečněna dispozice s peněžními prostředky na účtu.

(4) Je-li klient zastoupen zákonným zástupcem, provádí se identifikace zákonného zástupce podle odstavce 2. Zákonný zástupce doloží identifikační údaje zastoupeného.

(5) Při dalších obchodech s klientem, který byl již identifikován podle odstavce 2, ověří povinná osoba vhodným způsobem totožnost konkrétní jednající fyzické osoby. Toto ověření lze provést i bez fyzické přítomnosti klienta, který je fyzickou osobou, nebo fyzické osoby jednající jménem klienta, který je právnickou osobou.

(6) V době trvání obchodního vztahu nebo při dalších obchodech povinná osoba kontroluje platnost a úplnost identifikačních údajů klienta, informací získaných v rámci kontroly klienta (§ 9) nebo důvodnost výjimky z kontroly klienta (§ 13) a zaznamenává jejich změny.

(7) Jestliže povinná osoba při uzavírání obchodu má podezření, že klient nejedná svým jménem nebo že zastírá, že jedná za třetí osobu, vyzve klienta, aby doložil plnou moc podle odstavce 3. Každý je povinen této výzvě vyhovět, pokud jiný právní předpis nestanoví jinak; advokát nebo notář může tuto povinnost vůči povinné osobě splnit též předáním kopií příslušných částí dokladů, z nichž identifikační údaje zjistil.

(8) Klient poskytne povinné osobě informace, které jsou k provedení identifikace nezbytné, včetně předložení příslušných dokladů. Povinná osoba může pro účely tohoto zákona pořizovat kopie nebo výpisy z předložených dokladů a zpracovávat takto získané informace k naplnění účelu tohoto zákona.

§ 9

Kontrola klienta

(1) Povinná osoba před uskutečněním jednotlivého obchodu v hodnotě 15 000 EUR nebo vyšší, obchodu, na který se vztahuje povinnost identifikace podle § 7 odst. 2 písm. a) až d), obchodu s politicky exponovanou osobou a dále v době trvání obchodního vztahu provádí také kontrolu klienta. Klient poskytne povinné osobě informace, které jsou k provedení kontroly nezbytné, včetně předložení příslušných dokladů. Povinná osoba může pro účely tohoto zákona pořizovat kopie nebo výpisy z předložených dokladů a zpracovávat takto získané informace k naplnění účelu tohoto zákona.

(2) Kontrola klienta zahrnuje

a) získání informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu,

b) zjišťování skutečného majitele, pokud klientem je právnická osoba,

c) získání informací potřebných pro provádění průběžného sledování obchodního vztahu včetně přezkoumávání obchodů prováděných v průběhu daného vztahu za účelem zjištění, zda uskutečňované obchody jsou v souladu s tím, co povinná osoba ví o klientovi a jeho podnikatelském a rizikovém profilu,

d) přezkoumávání zdrojů peněžních prostředků.

(3) Povinná osoba provádí kontrolu klienta podle odstavce 2 v rozsahu potřebném k posouzení možného rizika legalizace výnosů z trestné činnosti a financování terorismu v závislosti na typu klienta, obchodního vztahu, produktu nebo obchodu. Osobám oprávněným k provádění kontroly plnění povinností podle tohoto zákona (§ 35) povinná osoba odůvodní přiměřenost rozsahu kontroly klienta nebo ověření splnění podmínek pro výjimku z identifikace a kontroly klienta podle § 13, a to s ohledem na výše uvedená rizika.

§ 10

Identifikace klienta provedená notářem, krajským úřadem nebo obecním úřadem

(1) Jestliže provedení první identifikace klienta povinnou osobou podle § 8 odst. 1 brání vážné důvody, na základě žádosti klienta nebo povinné osoby může takovou identifikaci provést notář anebo v přenesené působnosti krajský úřad nebo obecní úřad obce s rozšířenou působností.

(2) Notář nebo úřad uvedený v odstavci 1 sepíše o identifikaci listinu, která je veřejnou listinou, v níž uvede

a) kdo, na čí žádost a pro jaký účel identifikaci provedl,

b) identifikační údaje klienta,

c) osvědčení prohlášení identifikované fyzické osoby, osoby jednající jménem identifikované právnické osoby nebo zástupce identifikované osoby o účelu provedené identifikace a o potvrzení správnosti identifikace, popřípadě o výhradách k provedené identifikaci,

d) místo a datum sepsání listiny, popřípadě místo a datum, kde a kdy k identifikaci došlo, jsou-li odlišná od místa nebo data sepsání,

e) podpis toho, kdo provedl identifikaci, otisk jeho úředního razítka a pořadové číslo evidence listin o identifikaci.

(3) Přílohou listiny o identifikaci jsou kopie těch částí dokladů, použitých k identifikaci, z nichž lze zjistit identifikační údaje a dále druh a číslo průkazu totožnosti, stát, popřípadě orgán, který jej vydal, a dobu jeho platnosti, a kopie žádosti, byla-li podána písemně. Je-li tímto způsobem prováděna identifikace zmocněnce, je přílohou i originál plné moci nebo její ověřená kopie. Uvedené přílohy se pevně spojí do svazku k listině o identifikaci.

(4) Kopie dokladů musí být pořízeny takovým způsobem, aby příslušné údaje byly čitelné a byla zajištěna možnost jejich uchování po dobu stanovenou v § 16, a musí obsahovat i kopii vyobrazení identifikované fyzické osoby v průkazu totožnosti v takové kvalitě, aby umožňovala ověření shody podoby.

(5) Notář a úřad uvedený v odstavci 1 vede samostatnou evidenci listin o identifikaci, která obsahuje

a) pořadové číslo a datum sepsání,

b) údaje o identifikované osobě
1. jméno, příjmení, trvalý nebo jiný pobyt, rodné číslo nebo datum narození identifikované fyzické osoby nebo fyzické osoby jednající za identifikovanou právnickou osobu,
2. v případě identifikace právnické osoby její obchodní firmu nebo název včetně odlišujícího dodatku nebo dalšího označení, identifikační číslo osoby a sídlo,

c) účel identifikace.

(6) Evidence listin o identifikaci se vede po dobu kalendářního roku. Po jejím uzavření je uložena po dobu 10 let.

§ 11

Převzetí identifikace

(1) Povinná osoba nemusí provést identifikaci klienta, zjištění informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu podle § 9 odst. 2 písm. a) a zjištění skutečného majitele podle § 9 odst. 2 písm. b), pokud tyto úkony byly provedeny

a) úvěrovou nebo finanční institucí, s výjimkou osoby oprávněné ke směnárenské činnosti podle devizového zákona, držitele poštovní licence podle zákona upravujícího poštovní služby, platební instituce, jejíž činnost spočívá převážně v poskytování platebních služeb, při nichž dochází k převodům peněžních prostředků, kdy plátce ani příjemce nevyužívají účet u poskytovatele platebních služeb plátce, a poskytovatele platebních služeb malého rozsahu podle zákona upravujícího platební styk, nebo

b) zahraniční úvěrovou nebo finanční institucí, s výjimkou zahraniční osoby oprávněné ke směnárenské činnosti, zahraniční platební instituce, jejíž činnost spočívá převážně v poukazování peněz, nebo zahraničního poskytovatele platebních služeb s obdobným postavením, jako má poskytovatel platebních služeb malého rozsahu podle zákona upravujícího platební styk, jestliže působí na území státu, který jí ukládá srovnatelným způsobem povinnost identifikace, kontroly klienta a uchování záznamů, podléhá v tomto státu zákonné povinné profesní registraci

a je nad ním vykonáván dohled, zahrnující kontrolu plnění těchto povinností, včetně možnosti kontroly jednotlivých obchodů a kontroly na místě.

(2) Povinná osoba, která postupuje podle odstavce 1, musí mít zajištěno poskytnutí informací, včetně kopií příslušných dokladů o identifikaci klienta, účelu a zamýšlené povaze obchodního vztahu a totožnosti skutečného majitele od úvěrové nebo finanční instituce, popřípadě od zahraniční úvěrové nebo finanční instituce, která identifikaci nebo zjištění příslušných údajů provedla. Úvěrová nebo finanční instituce se souhlasem identifikované osoby na vyžádání neprodleně poskytne informace včetně kopií příslušných dokladů podle věty první jiné povinné osobě, pokud tato na ni při identifikaci klienta nebo zjištění příslušných údajů spoléhá.

(3) Povinná osoba nepřevezme informace o identifikaci klienta, informace o účelu a zamýšlené povaze obchodu nebo obchodního vztahu nebo zjištění skutečného majitele podle odstavců 1 a 2, vzniká-li pochybnost o správnosti nebo úplnosti těchto informací.

(4) V případě smlouvy o finančních službách uzavírané na dálku podle občanského zákoníku provede povinná osoba identifikaci klienta tak, že

a) první platba z této smlouvy bude uskutečněna prostřednictvím účtu vedeného na jméno klienta u úvěrové instituce nebo u zahraniční úvěrové instituce působící na území členského státu Evropské unie nebo Evropského hospodářského prostoru,

b) klient zašle povinné osobě kopii dokladu, potvrzujícího existenci účtu podle písmene a), kopie příslušných částí průkazu totožnosti a nejméně jednoho dalšího podpůrného dokladu, z nichž lze zjistit identifikační údaje a dále druh a číslo průkazu totožnosti, stát, popřípadě orgán, který jej vydal, a dobu jeho platnosti; kopie musí být pořízeny způsobem uvedeným v § 10 odst. 4.

(5) Úvěrová nebo finanční instituce nemusí provést identifikaci klienta, zjištění informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu podle § 9 odst. 2 písm. a) a zjištění skutečného majitele podle § 9 odst. 2 písm. b), pokud tyto úkony byly před uskutečněním obchodu provedeny osobou, která jedná jejím jménem a na její účet a je vázána jejími vnitřními předpisy, a jestliže úvěrová nebo finanční instituce nese odpovědnost za škodu způsobenou činností této osoby. Informace včetně kopií příslušných dokladů podle věty první, pokud byly pořizovány, se ukládají u povinné osoby.

(6) Úvěrová nebo finanční instituce při poskytování investičních služeb nemusí provést identifikaci klienta, zjištění informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu podle § 9 odst. 2 písm. a) a zjištění skutečného majitele podle § 9 odst. 2 písm. b), pokud tyto úkony byly provedeny investičním zprostředkovatelem v souladu s tímto zákonem a jejími vnitřními předpisy. Povinná osoba za provedení těchto úkonů odpovídá, jako by je provedla sama.

(7) V případech uvedených v odstavcích 1 a 4 až 6 povinná osoba ověří, zda jsou splněny uvedené podmínky a zda podle informací, které má povinná osoba k dispozici, nepředstavuje některý z klientů, některý z produktů nebo některý konkrétní obchod zvýšené riziko zneužití pro legalizaci výnosů z trestné činnosti nebo financování terorismu. V případě pochybnosti se výjimka neuplatní.

§ 12

Společné ustanovení k identifikaci podle § 10 a 11

Byla-li provedena identifikace a další úkony podle § 10 nebo podle § 11 odst. 4 a 6, identifikační údaje a další informace a doklady tam uvedené musí být uloženy u povinné osoby před uskutečněním obchodu.

§ 13

Výjimky z povinnosti identifikace a kontroly klienta

(1) Povinná osoba nemusí provádět identifikaci a kontrolu klienta, pokud je klient

a) úvěrovou nebo finanční institucí,

b) zahraniční úvěrovou nebo finanční institucí působící na území státu, který ukládá této instituci v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu povinnosti rovnocenné požadavkům práva Evropských společenství 1), a s ohledem na plnění těchto povinností je nad ní vykonáván dohled,

c) společností, jejíž cenné papíry jsou přijaty k obchodování na regulovaném trhu, a která podléhá požadavkům na zveřejnění informací rovnocenným požadavkům práva Evropských společenství,

d) skutečným majitelem peněžních prostředků uložených na účtu úschov notáře, advokáta,

soudního exekutora nebo soudu,

e) ústředním orgánem státní správy České republiky, Českou národní bankou nebo vyšším územním samosprávným celkem, nebo

f) klientem,
1. kterému byly svěřeny významné veřejné funkce podle předpisů Evropských společenství a Evropské unie,
2. jehož identifikační údaje jsou veřejně dostupné a není důvod pochybovat o jejich správnosti,
3. jehož činnosti jsou průhledné,
4. jehož účetnictví podává věrný a poctivý obraz předmětu účetnictví a finanční situace,
5. který je odpovědný buď orgánu Evropské unie nebo orgánům členského státu Evropské unie nebo Evropského hospodářského prostoru, anebo u něhož existují jiné vhodné kontrolní postupy zajišťující kontrolu jeho činnosti.

(2) Povinnost identifikovat a kontrolovat klienta není třeba plnit u

a) smlouvy o životním pojištění nebo o penzijním připojištění se státním příspěvkem, jestliže jednorázové pojistné nebo vklad nepřesahuje částku 2 500 EUR, nebo pokud běžné pojistné nebo souhrn pravidelných vkladů v jednom kalendářním roce nepřesahuje částku 1 000 EUR,

b) systémů zaměstnaneckého penzijního pojištění, provozovaných na území České republiky institucemi z členských států Evropské unie nebo států Evropského hospodářského prostoru podle jiného právního předpisu 18), pokud jsou příspěvky placeny srážkou ze mzdy a pravidla systému nedovolují postoupení členského podílu v rámci příslušného systému,

c) elektronických peněz podle jiného právního předpisu 19), pokud nejvyšší částka uložená na elektronickém peněžním prostředku, který nelze dobíjet, nepřekročí 150 EUR, nebo, pokud lze elektronický peněžní prostředek dobíjet, je pro kalendářní rok stanoven celkový limit ve výši 2 500 EUR, s výjimkou případů, kdy majitel v témže kalendářním roce zpětně vymění celkem 1 000 EUR nebo více, nebo

d) dalších produktů, pokud představují nízké riziko zneužití k legalizaci výnosů z trestné činnosti nebo financování terorismu a splňují současně následující podmínky:
1. smlouva o poskytnutí produktu má vždy písemnou formu,
2. platby v rámci tohoto produktu se provádějí pouze prostřednictvím účtu vedeného na jméno klienta u úvěrové instituce nebo zahraniční úvěrové instituce, působící na území členského státu Evropské unie nebo Evropského hospodářského prostoru, nebo působící na území státu, který jí ukládá v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu povinnosti rovnocenné požadavkům práva Evropských společenství 1) a s ohledem na plnění těchto povinností je nad ní vykonáván dohled,
3. daný produkt ani jednotlivé platby nejsou anonymní a jejich povaha je taková, že umožňují rozpoznání podezřelého obchodu,
4. daný produkt má předem stanovený limit maximální hodnoty obchodu, který nepřekročí částku 15 000 EUR, a v případě spořících produktů nepřekročí jednorázový vklad částku 2 500 EUR nebo součet pravidelných vkladů v kalendářním roce nepřekročí částku 1 000 EUR,
5. plnění z daného produktu nelze uskutečnit ve prospěch třetích stran, kromě případů úmrtí, invalidity, překročení předem určeného pokročilého věku nebo podobných událostí,
6. u produktů umožňujících investovat prostředky do finančního majetku nebo pohledávek, včetně pojištění nebo jiného druhu podmíněných pohledávek, jsou plnění z tohoto produktu uskutečnitelná pouze v dlouhých časových lhůtách, daný produkt nemůže být použit jako zajištění a neprovádí se žádné zrychlené platby, nejsou využita ustanovení o odstoupení a v průběhu obchodního vztahu není učiněn úkon k jeho předčasnému ukončení.

(3) V případech uvedených v odstavcích 1 a 2 povinná osoba ověří, zda jsou splněny uvedené podmínky a zda podle informací, které má povinná osoba k dispozici, nepředstavuje některý z klientů, některý z produktů nebo některý konkrétní obchod zvýšené riziko zneužití pro legalizaci výnosů z trestné činnosti nebo financování terorismu. V případě pochybnosti se výjimka podle odstavců 1 a 2 neuplatní.

(4) Výjimka podle odstavce 2 se nepoužije u klienta, který je politicky exponovanou osobou.

§ 14

Výjimka z povinnosti uvádět informace o plátci při převodech peněžních prostředků

Povinnosti podle přímo použitelného předpisu Evropských společenství, kterým se stanoví povinnost doprovázet převody peněžních prostředků informacemi o plátci 20), se nevztahují na převody peněžních prostředků nebo peněžní služby, jimiž se provádí platba za poskytování zboží a služeb, pokud

a) se převod uskuteční v České republice,

b) poskytovatel platebních služeb příjemce je prostřednictvím příjemce platby vždy schopen

určit konkrétního plátce a účel platby,

c) převáděná částka nepřekročí částku 1 000 EUR.

§ 15

Neuskutečnění obchodu

(1) Povinná osoba odmítne uskutečnění obchodu nebo uzavření obchodního vztahu v případě, že je dána identifikační povinnost podle § 7 odst. 1 nebo 2 a klient se odmítne podrobit identifikaci anebo odmítne doložit plnou moc podle § 8 odst. 3, neposkytne potřebnou součinnost při kontrole podle § 9, nebo z jiného důvodu nelze provést identifikaci anebo kontrolu klienta, anebo má-li osoba provádějící identifikaci nebo kontrolu pochybnosti o pravdivosti informací poskytnutých klientem nebo o pravosti předložených dokladů.

(2) Povinná osoba neuskuteční obchod s politicky exponovanou osobou, pokud jí není znám původ majetku užitého v obchodu.

(3) Zaměstnanec povinné osoby neuskuteční obchod s politicky exponovanou osobou bez souhlasu bezprostředního nadřízeného nebo statutárního orgánu této povinné osoby.

HLAVA II

UCHOVÁVÁNÍ INFORMACÍ

§ 16

Uchovávání údajů povinnou osobou

(1) Identifikační údaje získané podle § 8 odst. 1 a 2 nebo na základě přímo použitelného předpisu Evropských společenství, kterým se stanoví povinnost doprovázet převody peněžních prostředků informacemi o plátci 20), kopie dokladů předložených k identifikaci, byly-li pořizovány, údaj o tom, kdo a kdy provedl první identifikaci klienta, dokumenty odůvodňující výjimku z identifikace a kontroly klienta podle § 13, a v případě zastupování originál nebo ověřenou kopii plné moci, uchovává povinná osoba po dobu 10 let od ukončení obchodního vztahu s klientem.

(2) Údaje a doklady o obchodech spojených s povinností identifikace uchovává povinná osoba nejméně 10 let po uskutečnění obchodu nebo ukončení obchodního vztahu.

(3) Povinná osoba uvedená v § 2 odst. 1 písm. j) a k) uchovává údaje a doklady po dobu nejméně 10 let po ukončení obchodu nebo obchodního vztahu, byla-li hodnota obchodu 10 000 EUR nebo vyšší; v ostatních případech 5 let po ukončení obchodu.

(4) Lhůta podle odstavců 1 až 3 začíná běžet prvním dnem kalendářního roku následujícího po roce, ve kterém byl uskutečněn poslední úkon obchodu známý povinné osobě.

§ 17

Spolupráce při uchovávání údajů

Jestliže se na konkrétním obchodu s týmž klientem podílí více povinných osob, mohou být údaje podle § 16 uchovávány pouze u některé z nich za předpokladu, že ostatní zúčastněné povinné osoby mají zajištěno poskytování potřebných informací včetně kopií příslušných dokladů bez zbytečného odkladu.

HLAVA III

POSTUP PŘI PODEZŘELÉM OBCHODU

§ 18

Oznámení podezřelého obchodu

(1) Zjistí-li povinná osoba v souvislosti se svou činností podezřelý obchod, oznámí to Ministerstvu financí (dále jen „ministerstvo“) bez zbytečného odkladu, nejpozději do 5 kalendářních dnů ode dne zjištění podezřelého obchodu. Vyžadují-li to okolnosti případu, zejména hrozí-li nebezpečí z prodlení, oznámí povinná osoba podezřelý obchod neprodleně po jeho zjištění.

(2) V oznámení podezřelého obchodu uvede povinná osoba identifikační údaje toho, koho se oznámení týká, identifikační údaje všech dalších účastníků obchodu, které má v době podání oznámení k dispozici, informace o podstatných okolnostech obchodu a jakékoli další informace, které by mohly s podezřelým obchodem souviset a jsou významné pro jeho posouzení z hlediska opatření proti legalizaci výnosů z trestné činnosti nebo financování terorismu.

(3) V oznámení se neuvádí údaje o zaměstnanci povinné osoby nebo osobě v obdobném pracovněprávním vztahu, která podezřelý obchod zjistila.

(4) Oznámení podezřelého obchodu přijímá ministerstvo prostřednictvím Finančního analytického útvaru, který je jeho součástí. Způsobem umožňujícím dálkový přístup zveřejní ministerstvo adresu pro doručování a další možnosti spojení pro podávání oznámení podezřelého obchodu.

(5) Jestliže se oznámení podle odstavce 2 týká rovněž majetku, na který se vztahuje mezinárodní sankce vyhlášená za účelem udržení nebo obnovení mezinárodního míru a bezpečnosti, ochrany základních lidských práv nebo boje proti terorismu, povinná osoba na to v oznámení upozorní. V oznámení uvede dále i stručný popis tohoto majetku, údaje o jeho umístění a jeho vlastníkovi, pokud je oznamovateli znám, a informaci, zda hrozí bezprostřední nebezpečí poškození, znehodnocení nebo užití tohoto majetku v rozporu se zákonem.

(6) Oznamovatel současně sdělí ministerstvu jméno, příjmení a pracovní zařazení kontaktní osoby (§ 22) nebo osoby, která za povinnou osobu zpracovávala oznámení podezřelého obchodu, a možnosti telefonického, popřípadě elektronického spojení s touto osobou, pokud tyto informace nemá ministerstvo k dispozici.

(7) Zjistí-li v souvislosti se svou činností podezřelý obchod více povinných osob společně, na základě sdílení informací podle § 39 odst. 2, je splněna povinnost oznámit podezřelý obchod podle odstavců 2 až 4 všemi povinnými osobami, pokud oznámení podá alespoň jedna z nich, a v oznámení uvede, za které další povinné osoby oznámení podává.

§ 19

Oznámení podezřelého obchodu se podává písemně doporučeným dopisem nebo ústně do protokolu v místě určeném po předchozí domluvě. Za písemné oznámení se považuje též oznámení podané elektronicky technickými prostředky zajišťujícími zvláštní ochranu přenášených údajů.

§ 20

Odklad splnění příkazu klienta

(1) Pokud hrozí nebezpečí, že bezodkladným splněním příkazu klienta by mohlo být zmařeno nebo podstatně ztíženo zajištění výnosu z trestné činnosti nebo prostředků určených k financování terorismu, povinná osoba může splnit příkaz klienta týkající se podezřelého obchodu nejdříve po uplynutí 24 hodin od přijetí oznámení podezřelého obchodu ministerstvem. Majetek, jehož se příkaz klienta týká, vhodným způsobem zajistí proti manipulaci, která by byla v rozporu s účelem tohoto zákona. Na odklad splnění příkazu klienta upozorní povinná osoba ministerstvo v oznámení o podezřelém obchodě.

(2) Podle odstavce 1 se nepostupuje v případě, kdy odložení splnění příkazu klienta není možné, zejména u operací prováděných elektronickými platebními prostředky, nebo kdy je povinné osobě známo, že by takové odložení mohlo zmařit nebo jinak ohrozit šetření podezřelého obchodu; o splnění příkazu klienta povinná osoba ihned informuje ministerstvo. povinná osoba ihned informuje ministerstvo.

(3) Jestliže hrozí nebezpečí podle odstavce 1 a šetření podezřelého obchodu si pro složitost vyžaduje delší dobu, ministerstvo rozhodne

a) o prodloužení doby, na kterou se odkládá splnění příkazu klienta, nejdéle však na dobu 72 hodin od přijetí oznámení podezřelého obchodu ministerstvem, nebo

b) o odložení splnění příkazu klienta nebo o zajištění majetku, který má být předmětem podezřelého obchodu, u povinné osoby, u níž se tento majetek nachází, až na dobu 72 hodin.

(4) Rozhodnutí o odkladu splnění příkazu klienta nebo o zajištění majetku podle odstavce 3 nabývá právní moci jeho vyhlášením. Vyhlášení může být provedeno ústně, telefonicky, telefaxem nebo elektronicky; vždy se však následně doručuje stejnopis písemného vyhotovení. Proti rozhodnutí o odkladu splnění příkazu klienta nebo o zajištění majetku není přípustný rozklad. Při rozhodování o tomto opatření je účastníkem řízení pouze povinná osoba, která podala oznámení podezřelého obchodu, nebo u níž se nachází majetek, který má být předmětem podezřelého obchodu.

(5) Povinná osoba obratem sdělí ministerstvu vykonání rozhodnutí podle odstavce 3 písm. b) a potvrdí čas, od něhož se počítá běh lhůty podle odstavce 3 písm. b). Ministerstvu dále průběžně podává informace o všech podstatných skutečnostech týkajících se majetku uvedeného v rozhodnutí.

(6) Jestliže ministerstvo do konce lhůty stanovené v odstavci 3 povinné osobě nesdělí, že podalo trestní oznámení, povinná osoba příkaz klienta provede.

(7) Podá-li ministerstvo ve lhůtě stanovené v odstavci 1 nebo 3 oznámení orgánu činnému

v trestním řízení podle § 32 odst. 1, povinná osoba provede příkaz klienta po uplynutí 3 kalendářních dnů ode dne podání trestního oznámení, pokud orgán činný v trestním řízení do konce této lhůty nerozhodne o odnětí nebo zajištění předmětu podezřelého obchodu. O podání trestního oznámení informuje ministerstvo povinnou osobu před uplynutím lhůty podle odstavce 1 nebo 3.

HLAVA IV

DALŠÍ POVINNOSTI POVINNÝCH OSOB

§ 21

Systém vnitřních zásad

(1) Povinná osoba zavede a uplatňuje odpovídající postupy vnitřní kontroly a komunikace za účelem naplnění povinností stanovených tímto zákonem.

(2) Povinná osoba uvedená v § 2 odst. 1 písm. a) až d), h) a i) vypracuje v rozsahu, ve kterém provádí činnosti podléhající působnosti tohoto zákona, písemně systém vnitřních zásad, postupů a kontrolních opatření k naplnění povinností stanovených tímto zákonem (dále jen „systém vnitřních zásad").

(3) Povinná osoba uvedená v § 2 odst. 1 písm. b) až d), h) a i) nemusí vypracovat systém vnitřních zásad písemně, jestliže v oblastech činnosti podléhajících působnosti tohoto zákona nezaměstnává další osoby, nebo pro ni nepracují další osoby na základě jiného vztahu.

(4) Povinná osoba uvedená v § 2 odst. 1 písm. b) až d), h) a i), která smluvně vykonává činnost podléhající působnosti tohoto zákona pouze pro jednu jinou povinnou osobu, nemusí vypracovat vlastní systém vnitřních zásad, pokud se řídí systémem vnitřních zásad této jiné povinné osoby, v němž je její činnost dostatečně popsána.

(5) Systém vnitřních zásad podle odstavce 2 zahrnuje

a) podrobný demonstrativní výčet znaků podezřelých obchodů, které se mohou vyskytovat při činnosti konkrétní povinné osoby,

b) způsob identifikace klienta, zahrnující opatření k rozpoznání politicky exponovaných osob a subjektů, vůči nimž Česká republika uplatňuje mezinárodní sankce podle zákona o provádění mezinárodních sankcí,

c) postupy pro provádění kontroly klienta a stanovování rozsahu kontroly klienta odpovídající riziku legalizace výnosů z trestné činnosti a financování terorismu v závislosti na typu klienta, obchodního vztahu, produktu nebo obchodu,

d) přiměřené a vhodné metody a postupy pro posuzování rizik, řízení rizik, vnitřní kontrolu a zajišťování kontroly nad dodržováním povinností stanovených tímto zákonem,

e) postup pro zpřístupnění údajů uchovávaných podle části druhé hlavy II příslušným orgánům,

f) postup povinné osoby od zjištění podezřelého obchodu do okamžiku doručení oznámení ministerstvu tak, aby byla dodržena lhůta stanovená v § 18 odst. 1, jakož i pravidla pro zpracování podezřelého obchodu a určení osob, které podezřelý obchod vyhodnocují,

g) pravidla a postupy, kterými se při nabízení služeb nebo produktů povinné osoby řídí třetí osoby jednající jménem nebo na účet povinné osoby,

h) opatření, která vyloučí zmaření nebo podstatné ztížení zajištění výnosu z trestné činnosti bezodkladným splněním příkazu klienta,

i) technická a personální opatření, která zajistí provedení odkladu splnění příkazu klienta podle § 20, a ve stanovené lhůtě splnění povinností podle § 24,

j) v případech uvedených v § 25 odst. 4 popis doplňkových opatření k účinnému zvládání rizika legalizace výnosů z trestné činnosti nebo financování terorismu.

(6) Úvěrová instituce, finanční instituce uvedená v § 2 odst. 1 písm. b) bodech 5, 6, 10 a 11 a povinná osoba uvedená v § 2 odst. 1 písm. c) doručí ministerstvu systém vnitřních zásad do 60 dnů ode dne, kdy se stala povinnou osobou; oznámení o změnách v systému vnitřních zásad doručí do 30 dnů ode dne jejich přijetí. Povinná osoba uvedená v § 2 odst. 1 písm. b) bodech 1 až 4 má povinnosti podle věty první vůči České národní bance.

(7) Zahraniční úvěrová nebo finanční instituce, která na území České republiky působí prostřednictvím své pobočky, organizační složky nebo provozovny, nemusí pro jejich činnost vypracovat zvláštní systém vnitřních zásad, pokud je jejich činnost upravena obdobným vnitřním předpisem této zahraniční úvěrové nebo finanční instituce a tento vnitřní předpis splňuje požadavky alespoň rovnocenné požadavkům tohoto zákona. Uvedený vnitřní předpis musí být k

dispozici v českém jazyce.

(8) Zjistí-li ministerstvo nebo Česká národní banka nedostatky v systému vnitřních zásad, který jim byl zaslán podle odstavce 6, stanoví termín k jejich odstranění. Povinná osoba ve stanoveném termínu podá písemnou informaci o způsobu odstranění zjištěných nedostatků.

(9) Prováděcí právní předpis stanoví v mezích stanovených odstavcem 5 písm. c) a d) požadavky na zavedení a uplatňování systému vnitřních zásad některými povinnými osobami, vůči nimž Česká národní banka vykonává dohled 21).

§ 22

Kontaktní osoba

(1) Povinná osoba určí konkrétního zaměstnance k plnění oznamovací povinnosti podle § 18 a k zajišťování průběžného styku s ministerstvem, pokud tyto činnosti nebude zajišťovat přímo statutární orgán. O určení této osoby a o případných následných změnách informuje úvěrová nebo finanční instituce neprodleně ministerstvo s uvedením jména, příjmení, pracovního zařazení a údajů pro spojení včetně telefonického a elektronického.

(2) Člen statutárního orgánu úvěrové nebo finanční instituce nesmí být kontaktní osobou, ledaže by to bylo nezbytné s ohledem na velikost instituce, způsob řízení či počet zaměstnanců.

(3) Kontaktní osobou úvěrové nebo finanční instituce nesmí být zaměstnanec, který je odpovědný za uzavírání nebo vypořádávání jejích obchodů, anebo je osobou podílející se na výkonu vnitřního auditu.

(4) Nezajišťuje-li činnosti kontaktní osoby přímo statutární orgán, povinná osoba zajistí kontaktní osobě možnost přímé komunikace se statutárním a dozorčím orgánem povinné osoby.

§ 23

Školení zaměstnanců

(1) Povinná osoba zajistí nejméně jedenkrát v průběhu 12 kalendářních měsíců proškolení zaměstnanců, kteří se mohou při výkonu své pracovní činnosti setkat s podezřelými obchody, a proškolení všech zaměstnanců před zařazením na takováto pracovní místa.

(2) Školení podle odstavce 1 povinná osoba zajistí také pro osoby, které se na předmětu činnosti povinné osoby podílejí na základě jiné než pracovní smlouvy, pokud se tyto osoby mohou při výkonu své činnosti setkat s podezřelými obchody.

(3) Obsahem školení je zejména typologie a znaky podezřelých obchodů a postupy při zjištění podezřelého obchodu. Povinná osoba obsah školení průběžně doplňuje a aktualizuje.

(4) Povinná osoba vede evidenci o účasti a obsahu školení, a to nejméně po dobu 5 let od jejich konání.

§ 24

Informační povinnost

Povinná osoba na žádost sdělí ministerstvu v jím stanovené lhůtě údaje o obchodech souvisejících s povinností identifikace nebo ohledně nichž ministerstvo provádí šetření, předloží doklady o těchto obchodech nebo k nim umožní přístup pověřeným zaměstnancům ministerstva při prověřování oznámení a poskytne informace o osobách, které se jakýmkoliv způsobem účastnily takových obchodů.

HLAVA V

ZVLÁŠTNÍ USTANOVENÍ O NĚKTERÝCH POVINNÝCH OSOBÁCH

§ 25

Zvláštní ustanovení o úvěrových a finančních institucích

(1) Úvěrová instituce nesmí vstoupit do korespondenčního bankovního vztahu se zahraniční úvěrovou nebo obdobnou institucí (dále jen „respondenční instituce“),

a) která je zapsána do obchodního nebo obdobného rejstříku v zemi, v níž není fyzicky přítomna ani se zde nenachází její skutečné vedení, a která není přičleněna k žádné regulované finanční skupině,

b) o níž je jí známo, že umožňuje využívání svých účtů institucí uvedenou v písmenu a), nebo

c) která neuplatňuje opatření proti legalizaci výnosů z trestné činnosti a financování terorismu alespoň rovnocenná požadavkům práva Evropských společenství 1), a pokud již do takového vztahu vstoupila, musí jej ukončit v době co nejkratší.

(2) Úvěrová instituce před navázáním korespondenčního bankovního vztahu s respondenční institucí

a) shromáždí dostatek informací o respondenční instituci a povaze jejího podnikání,

b) z veřejně dostupných informací zjistí, jaká je kvalita dohledu, kterému respondenční instituce podléhá,

c) zhodnotí opatření prováděná respondenční institucí proti legalizaci výnosů z trestné činnosti a financování terorismu.

(3) K navázání korespondenčního bankovního vztahu musí vydat souhlas statutární orgán úvěrové instituce nebo vedoucí pobočky zahraniční úvěrové instituce působící na území České republiky.

(4) Úvěrová a finanční instituce ve svých pobočkách a většinově vlastněných dceřiných společnostech, nacházejících se ve státech, které nejsou členskými státy Evropské unie nebo Evropského hospodářského prostoru, uplatňuje opatření pro kontrolu klienta a uchovávání záznamů, která jsou alespoň rovnocenná požadavkům práva Evropských společenství 1). Za tím účelem jim předává relevantní informace o uplatňovaných metodách a postupech. Pokud právní předpisy takové země nedovolují uplatňování rovnocenných opatření, informuje o tom ministerstvo; v takovém případě přijme povinná osoba odpovídající doplňková opatření k účinnému zvládání rizika zneužití pro legalizaci výnosů z trestné činnosti nebo financování terorismu a zabránění přenosu těchto rizik na území České republiky a dalších členských států Evropské unie nebo Evropského hospodářského prostoru.

(5) Systém vnitřních zásad úvěrové nebo finanční instituce schvaluje její statutární orgán.

(6) Úvěrová nebo finanční instituce na žádost ministerstva v jím stanovené lhůtě sdělí informaci, zda udržuje nebo v předchozích 10 letech udržovala obchodní vztah s konkrétní fyzickou nebo právnickou osobou, vůči níž měla povinnost identifikace, a o povaze tohoto vztahu. K tomuto účelu zavede úvěrová nebo finanční instituce účinný systém, odpovídající velikosti instituce a povaze její podnikatelské činnosti.

(7) Práva a povinnosti, které tento zákon stanoví pro úvěrové instituce, se vztahují i na Českou národní banku při vedení účtů a poskytování dalších bankovních služeb.

§ 26

Zvláštní ustanovení o auditorech, účetních, soudních exekutorech a daňových poradcích

(1) Ustanovení § 18 odst. 1 a § 24 se nevztahují na auditora, účetního, soudního exekutora nebo daňového poradce, pokud jde o informace, které získá od svého klienta nebo které získá o svém klientovi během zjišťování jeho právního postavení, během jeho zastupování v soudním řízení anebo v souvislosti s takovým řízením, včetně poradenství ohledně zahájení takového řízení nebo vyhnutí se takovému řízení, bez ohledu na to, zda jsou takové informace získány před tímto řízením, během něj nebo po něm.

(2) Má-li auditor, účetní, soudní exekutor nebo daňový poradce za to, že klient žádá o právní poradenství za účelem legalizace výnosů z trestné činnosti nebo za účelem financování terorismu, odstavec 1 se nepoužije.

(3) Oznámení podle § 18 učiní

a) auditor Komoře auditorů České republiky,

b) soudní exekutor Exekutorské komoře České republiky,

c) daňový poradce Komoře daňových poradců České republiky.

(4) Příslušná profesní komora oznámení přijaté podle odstavce 3 přezkoumá z hlediska, zda není v rozporu s odstavcem 1 nebo s § 18 odst. 1 a zda má všechny náležitosti stanovené tímto zákonem. Pokud oznámení náležitosti stanovené tímto zákonem nemá, komora na to oznamovatele upozorní. Splňuje-li oznámení podmínky uvedené ve větě první, komora postupuje tak, aby je předala ministerstvu bez zbytečného odkladu, nejpozději do 7 kalendářních dnů ode dne zjištění podezřelého obchodu.

§ 27

Zvláštní ustanovení o advokátech a notářích

(1) Ustanovení § 9, § 18 odst. 1 a § 24 se nepoužijí u advokáta, pokud jde o informace o klientovi, které získal od klienta nebo jakýmkoliv jiným způsobem během nebo v souvislosti s

a) poskytováním právních porad nebo následným ověřováním právního postavení klienta,

b) obhajobou klienta v trestním řízení,

c) zastupováním klienta v řízení před soudy, nebo

d) poskytováním jakýchkoliv právních porad týkajících se řízení uvedených v písmenech b) a c), a to bez ohledu na to, zda tato řízení již byla zahájena či nikoliv nebo zda již byla ukončena.

(2) Ustanovení § 9, § 18 odst. 1 a § 24 se nepoužijí u notáře, pokud jde o informace o klientovi, které získal od klienta nebo jakýmkoliv jiným způsobem během nebo v souvislosti s

a) poskytováním právních porad nebo následným ověřováním právního postavení klienta 22),

b) zastupováním klienta v řízení před soudy v rozsahu svého oprávnění stanoveného jiným právním předpisem 23), nebo

c) poskytováním jakýchkoliv právních porad týkajících se řízení uvedených v písmenu b), a to bez ohledu na to, zda tato řízení již byla zahájena či nikoliv nebo zda již byla ukončena.

(3) Oznámení podle § 18 učiní advokát České advokátní komoře a notář Notářské komoře České republiky. Česká advokátní komora nebo Notářská komora České republiky (dále jen „komora") oznámení advokáta nebo notáře přezkoumá z hlediska, zda není v rozporu s odstavcem 1 nebo 2, § 2 odst. 1 písm. g) anebo § 18 odst. 1 a zda má všechny náležitosti stanovené tímto zákonem. Pokud oznámení advokáta nebo notáře náležitosti stanovené tímto zákonem nemá, komora na to advokáta nebo notáře upozorní. Splňuje-li oznámení advokáta nebo notáře podmínky uvedené ve větě první, komora postupuje tak, aby je předala ministerstvu bez zbytečného odkladu, nejpozději do 7 kalendářních dnů ode dne zjištění podezřelého obchodu.

(4) Sdělení údajů, předložení dokladů nebo poskytnutí informací podle § 24 vyžaduje ministerstvo po advokátovi nebo notáři prostřednictvím komory. Advokát nebo notář sdělí ministerstvu ve lhůtě jím stanovené požadované údaje, předloží doklady nebo mu poskytne požadované informace prostřednictvím komory.

(5) Advokátem se pro účely tohoto zákona rozumí i evropský advokát podle zákona o advokacii.

§ 28

Zvláštní ustanovení o osobách přijímajících hotovost 15 000 EUR nebo vyšší

Podnikatel a právnická osoba uvedená v § 2 odst. 2 písm. e), pokud se povinnou osobou stává pouze tehdy, jestliže přijímá platbu v hotovosti ve výši 15 000 EUR nebo vyšší, má v rámci tohoto jednotlivého obchodu povinnost

a) provést identifikaci klienta podle § 8, popřípadě ji nahradit identifikací podle § 10 nebo 11, pokud se na tento obchod nebo na klienta nevztahuje výjimka podle § 13,

b) odmítnout uskutečnění obchodu, jestliže má pochybnosti o pravdivosti získaných identifikačních údajů o klientovi, jestliže se klient odmítne podrobit identifikaci nebo odmítne doložit plnou moc podle § 8 odst. 3; o této skutečnosti současně informuje ministerstvo,

c) provádět kontrolu klienta podle § 9 odst. 2,

d) uchovávat informace podle § 16 odst. 1 a 2,

e) podávat oznámení podezřelého obchodu podle § 18,

f) informační podle § 24,

g) mlčenlivosti podle § 38.

§ 29

Zvláštní ustanovení o provozování peněžních poštovních služeb

(1) Vykonávat činnost na základě poštovní smlouvy a za podmínek stanovených zákonem o

poštovních službách, jejímž účelem je dodání poukázané peněžní částky, může pouze osoba, která je držitelem osvědčení o způsobilosti vydaného ministerstvem. Osvědčení se vydává na žádost osoby, která hodlá tuto činnost vykonávat.

(2) Ministerstvo vydá osvědčení podle odstavce 1, pokud žadatel, osoba, která je společníkem žadatele, statutárním orgánem žadatele, členem statutárního orgánu žadatele, osoba, která bude řídit podnikání žadatele, a skutečný majitel žadatele jsou osobami bezúhonnými.

(3) Za bezúhonnou se pro účely tohoto zákona považuje osoba, která nebyla pravomocně odsouzena pro trestný čin spáchaný

a) úmyslně, nebo

b) z nedbalosti, jehož skutková podstata souvisí s předmětem podnikání,
pokud se na ni nehledí, jako by nebyla odsouzena.

(4) Bezúhonnost se prokazuje u fyzické osoby s místem trvalého nebo jiného pobytu

a) na území České republiky výpisem z evidence Rejstříku trestů, ne starším než 1 měsíc; to neplatí v případě, kdy si může tento výpis vyžádat ministerstvo podle jiného právního předpisu,

b) mimo území České republiky a u osoby, která se v posledních 5 letech nepřetržitě zdržovala mimo území České republiky po dobu delší než 6 měsíců, dokladem obdobným výpisu z evidence Rejstříku trestů, vydaným k tomu oprávněným orgánem státu trvalého nebo jiného pobytu této osoby a států, ve kterých se tato osoba v posledních 5 letech nepřetržitě zdržovala po dobu delší než 6 měsíců; pokud stát trvalého nebo jiného pobytu této osoby není totožný se státem, jehož je tato osoba občanem, též dokladem vydaným státem, jehož je občanem.

ČÁST TŘETÍ

ČINNOST MINISTERSTVA A DALŠÍCH ORGÁNŮ

HLAVA I

ČINNOST MINISTERSTVA A DALŠÍCH ORGÁNŮ

§ 30

Získávání informací

(1) Ministerstvo může vyžadovat informace nezbytné pro plnění povinností podle tohoto zákona od Policie České republiky, zpravodajských služeb a orgánů veřejné moci.

(2) Při šetření podezřelého obchodu může ministerstvo v souladu se zákonem upravujícím správu daní, vyžadovat od orgánů věcně příslušných podle jiných právních předpisů ke správě daní informace získané při správě daní; tyto orgány informují bezodkladně ministerstvo o podezření, že daňový subjekt zneužívá systém správy daní k legalizaci výnosů z trestné činnosti nebo k financování terorismu.

(3) Ministerstvu jsou poskytovány pro výkon působnosti podle tohoto zákona

a) referenční údaje ze základního registru obyvatel,

b) z agendového informačního systému evidence obyvatel údaje o obyvatelích,

c) z informačního systému cizinců údaje o cizincích,

d) z registru rodných čísel údaje o fyzických osobách, kterým bylo přiděleno rodné číslo, avšak nejsou uvedeny v písmenu b) nebo c).

(4) Pokud to umožňuje technický stav, poskytuje Ministerstvo vnitra ministerstvu údaje uvedené v odstavci 3 pouze v elektronické podobě způsobem umožňujícím dálkový přístup.

(5) Z poskytovaných údajů lze v konkrétním případě použít vždy jen takové údaje, jejichž použití je v daném případě nezbytné.

(6) Na základě oznámení zpravodajské služby o zjištění skutečností nasvědčujících podezřelému obchodu zahájí ministerstvo šetření podezřelého obchodu; o výsledku tohoto šetření informuje zpravodajskou službu.

§ 31

Zpracování informací

(1) Ministerstvo soustřeďuje a analyzuje údaje získané při své činnosti podle tohoto zákona. Je oprávněno vést údaje získané při plnění úkolů podle tohoto zákona v informačním systému za podmínek, které stanoví zákon o ochraně osobních údajů. K tomu účelu je oprávněno sdružovat informace a informační systémy sloužící k rozdílným účelům.

(2) Ministerstvo neposkytuje podle zákona o ochraně osobních údajů na požádání dotčené osobě zprávu o informacích, které jsou o ní uchovávány v informačním systému vedeném podle tohoto zákona.

(3) Ministerstvo uchovává údaje a doklady o přijatých oznámeních a o vlastním šetření po dobu 10 let od konce roku, v němž bylo šetření ukončeno. Přijetím nového oznámení nebo obnovením šetření v téže věci nebo vůči stejnému subjektu se běh lhůty podle věty první přerušuje do ukončení nového šetření.

(4) Ministerstvo vede a nejméně jednou ročně uveřejňuje na internetových stránkách statistické přehledy o účinnosti a výsledcích opatření proti legalizaci výnosů z trestné činnosti a financování terorismu. Orgány činné v trestním řízení poskytují ministerstvu průběžně zobecněné informace o řízeních ve věcech souvisejících s legalizací výnosů z trestné činnosti nebo financováním terorismu.

(5) Finanční analytický útvar je technicky oddělen od jiných pracovišť ministerstva a jsou v něm uplatňována taková organizační, personální a jiná opatření, která zaručují, že s informacemi získanými při provádění tohoto zákona nepřijde do styku nepovolaná osoba.

§ 32

Nakládání s výsledky šetření

(1) Zjistí-li ministerstvo skutečnosti nasvědčující tomu, že byl spáchán trestný čin, podá oznámení podle trestního řádu a současně orgánu činnému v trestním řízení poskytne všechny související informace z výsledků vlastního šetření.

(2) Zjistí-li ministerstvo skutečnosti, které jsou významné pro výkon činnosti územních finančních orgánů nebo celních orgánů, informuje o těchto zjištěních příslušné finanční ředitelství nebo Generální ředitelství cel a poskytne mu všechny související informace z výsledků vlastního šetření, pokud poskytnutí takových informací není v rozporu s účelem tohoto zákona nebo pokud nepostupovalo podle odstavce 1.

§ 33

Mezinárodní spolupráce

(1) V rozsahu stanoveném mezinárodní smlouvou, kterou je Česká republika vázána, nebo na základě vzájemnosti ministerstvo spolupracuje se zahraničními orgány a mezinárodními organizacemi se stejnou věcnou působností, zejména při předávání a získávání údajů sloužících k dosažení účelu stanoveného tímto zákonem.

(2) Za podmínek, že informace budou užity pouze k dosažení účelu tohoto zákona a budou požívat ochrany alespoň v rozsahu tímto zákonem stanoveném, může ministerstvo spolupracovat i s dalšími mezinárodními organizacemi.

§ 34

Povolování výjimek

(1) Ministerstvo na základě žádosti rozhodne, že povinná osoba, která některou z činností uvedených v § 2 odst. 1 vykonává pouze příležitostně nebo ve velmi omezené míře a takovým způsobem, že je vyloučeno nebo značně omezeno její zneužití k legalizaci výnosů z trestné činnosti nebo financování terorismu, nebude v souvislosti s touto činností považována za povinnou osobu podle tohoto zákona.

(2) Výjimka podle odstavce 1 se udělí, pokud

a) vykonávaná činnost je pouze doplňkovou činností, která přímo souvisí s hlavní činností povinné osoby, která jinak s výjimkou činnosti uvedené v § 2 odst. 2 písm. d) není povinnou osobou podle tohoto zákona, a je poskytována pouze v souvislosti s hlavní činností povinné osoby,

b) celkový roční obrat z této činnosti nepřesahuje 5 % z celkového ročního obratu povinné osoby a současně nepřekročí částku, kterou ministerstvo v rozhodnutí stanoví s ohledem na druh činnosti,

c) je zajištěno, že hodnota jednotlivého obchodu nebo více obchodů v rámci činnosti uvedené v písmenu a) uskutečněných v průběhu 30 po sobě jdoucích dnů s týmž klientem nepřekročí částku 1 000 EUR.

(3) K žádosti podle odstavce 1 povinná osoba písemně doloží splnění podmínek v odstavcích 1 a 2.

(4) Výjimku podle odstavce 1 lze udělit i na dobu určitou. V rozhodnutí stanoví ministerstvo případné další povinnosti v rozsahu povinností povinných osob za účelem zabránění zneužití výjimky pro legalizaci výnosů z trestné činnosti nebo financování terorismu.

(5) Ministerstvo výjimku udělí pouze tehdy, je-li při výkonu činnosti povinné osoby vyloučeno nebo značně omezeno nebezpečí jejího zneužití k legalizaci výnosů z trestné činnosti nebo financování terorismu.

(6) Povinná osoba umožní dozorčímu úřadu (§ 35 odst. 1) v době trvání výjimky podle odstavce 1 kontrolu plnění stanovených podmínek a kontrolu, zda tato výjimka není zneužívána k činnostem, které by usnadňovaly legalizaci výnosů z trestné činnosti nebo financování terorismu. Dozorčí úřady mají stejná oprávnění jako při provádění kontroly povinné osoby.

(7) Povinnost povinné osoby stanovená v § 18 a postup ministerstva vůči povinné osobě podle § 24 při provádění šetření podezřelého obchodu nejsou rozhodnutím o výjimce podle odstavce 1 dotčeny.

(8) Výjimku podle odstavce 1 ministerstvo rozhodnutím odejme, jestliže

a) se významně změnilo hodnocení rizikovosti příslušné činnosti z hlediska možnosti zneužití k legalizaci výnosů z trestné činnosti nebo financování terorismu, nebo

b) ten, komu byla udělena výjimka, porušil stanovené podmínky.

(9) Rozklad proti rozhodnutí podle odstavce 8 nemá odkladný účinek.

HLAVA II

SPRÁVNÍ DOZOR

§ 35

Výkon správního dozoru

(1) Dozorčím úřadem pro správní dozor nad plněním povinností stanovených tímto zákonem povinnými osobami je ministerstvo, které současně kontroluje, zda nedochází k legalizaci výnosů z trestné činnosti nebo financování terorismu povinnými osobami. Kontrolu plnění povinností stanovených tímto zákonem dále provádí

a) Česká národní banka u povinných osob, vůči nimž vykonává dohled 21),

b) správní úřady s působností nad dodržováním zákona o loteriích a jiných podobných hrách u držitelů povolení k provozování sázkových her uvedených v § 2 odst. 1 písm. c),

c) Česká obchodní inspekce u povinných osob uvedených v § 2 odst. 1 písm. j) a k).

(2) Ministerstvo dále vykonává kontrolu plnění povinností podle přímo použitelného předpisu Evropských společenství, kterým se stanoví povinnost doprovázet převody peněžních prostředků informacemi o plátci 20); Česká národní banka vykonává kontrolu plnění povinností podle uvedeného předpisu u povinných osob, vůči nimž vykonává dohled 21).

(3) Ministerstvo poskytuje ostatním dozorčím úřadům informace z vlastní činnosti potřebné pro výkon správního dozoru nebo dohledu.

(4) Ostatní dozorčí úřady poskytnou ministerstvu na vyžádání písemná stanoviska nebo jinou požadovanou součinnost.

(5) Pokud dozorčí úřad uvedený v odstavci 1 písm. a) až c) zjistí skutečnosti, které by mohly souviset s legalizací výnosů z trestné činnosti nebo financováním terorismu, bez odkladu o tom informuje ministerstvo a sdělí mu současně všechny informace v rozsahu uvedeném v § 18 odst. 2.

§ 36

Podnět k odnětí oprávnění k podnikatelské nebo jiné samostatné výdělečné činnosti

Zjistí-li ministerstvo, že právnická nebo fyzická osoba mající příjmy z podnikatelské nebo jiné samostatné výdělečné činnosti zvlášť závažným způsobem nebo opětovně porušuje některou z povinností stanovených v tomto zákoně nebo uložených rozhodnutím vydaným podle

tohoto zákona, předloží podnět ke zrušení nebo odnětí oprávnění k podnikatelské nebo jiné samostatné výdělečné činnosti orgánu, který je podle jiného právního předpisu oprávněn o jeho odnětí rozhodnout. Tento orgán je povinen do 30 dnů ode dne doručení podnětu ministerstvo vyrozumět o svých opatřeních a o způsobu jeho vyřízení.

§ 37

Zvláštní ustanovení o správním dozoru u advokáta, notáře, auditora, soudního exekutora nebo daňového poradce

(1) Ustanovení této hlavy se na advokáty, notáře, auditory, soudní exekutory a daňové poradce nevztahují.

(2) Příslušná komora je povinna provést na základě písemného podnětu ministerstva kontrolu dodržování povinností vyplývajících z tohoto zákona advokátem, notářem, auditorem, soudním exekutorem nebo daňovým poradcem a uvědomit písemně ministerstvo o jejím výsledku v jím stanovené lhůtě.

ČÁST ČTVRTÁ

MLČENLIVOST

§ 38

Povinnost mlčenlivosti

(1) Nestanoví-li tento zákon jinak, jsou povinné osoby a jejich zaměstnanci, zaměstnanci ministerstva, zaměstnanci ostatních dozorčích úřadů a fyzické osoby, které jsou pro povinnou osobu, ministerstvo nebo jiný dozorčí úřad činné na základě jiné než pracovní smlouvy, povinny zachovávat mlčenlivost o skutečnostech, týkajících se oznámení a šetření podezřelého obchodu, úkonů učiněných ministerstvem nebo plnění informační povinnosti stanovené v § 24.

(2) Převedením osob uvedených v odstavci 1 na jinou práci, skončením jejich pracovněprávního nebo jiného smluvního vztahu k povinné osobě, ministerstvu nebo jinému dozorčímu úřadu ani tím, že povinná osoba přestala vykonávat činnosti uvedené v § 2, povinnost mlčenlivosti nezaniká.

(3) O skutečnostech uvedených v odstavci 1 je povinen zachovávat mlčenlivost každý, kdo se o nich dozví.

§ 39

Výjimky z mlčenlivosti

(1) Povinnosti zachovávat mlčenlivost stanovené v § 38 se nelze dovolávat vůči

a) orgánu činnému v trestním řízení, pokud provádí řízení o trestném činu souvisejícím s legalizací výnosu z trestné činnosti nebo financováním terorismu, anebo jedná-li se o splnění oznamovací povinnosti vztahující se k takovému trestnému činu,

b) specializovaným policejním složkám pro vyhledávání legalizace výnosů z trestné činnosti a financování terorismu, pokud jde o informace získané podle § 42 odst. 3,

c) zahraničnímu orgánu uvedenému v § 33 při předávání údajů sloužících k dosažení účelu stanoveného tímto zákonem, pokud to jiný právní předpis nezakazuje,

d) příslušnému finančnímu ředitelství nebo Generálnímu ředitelství cel, pokud jde o skutečnosti, které jsou součástí informace uvedené v § 32 odst. 2,

e) dozorčím úřadům uvedeným v § 35 odst. 1 a příslušným orgánům profesních komor advokátů, notářů, auditorů, soudních exekutorů nebo daňových poradců,

f) správnímu orgánu, který plní úkoly v systému certifikace surových diamantů podle jiného právního předpisu,

g) správnímu orgánu oprávněnému vykonávat státní kontrolu nebo vést sankční správní řízení podle zákona o provádění mezinárodních sankcí,

h) orgánu oprávněnému podle jiného právního předpisu rozhodovat o odnětí oprávnění k podnikatelské nebo jiné samostatné výdělečné činnosti v případě, že ministerstvo předloží podnět k odnětí takového oprávnění,

i) finančnímu arbitrovi rozhodujícímu podle jiného právního předpisu ve sporu navrhovatele proti instituci,

j) osobě, která by mohla uplatnit nárok na náhradu škody způsobené postupem podle tohoto zákona, jde-li o následné oznámení skutečností rozhodných pro uplatnění takového nároku; povinná osoba může v tomto případě sdělit klientovi, že bylo jednáno podle tohoto zákona, až po dni, ve kterém bylo vykonáno rozhodnutí orgánu činného v trestním řízení o odnětí nebo zajištění předmětu podezřelého obchodu nebo ve kterém skončila lhůta stanovená v § 20 odst. 7; v ostatních případech až po předchozím písemném souhlasu ministerstva,

k) soudu rozhodujícímu v občanském soudním řízení spory týkající se podezřelého obchodu nebo nároku na náhradu škody vzniklé v důsledku splnění povinnosti podle tohoto zákona,

l) Národnímu bezpečnostnímu úřadu, Ministerstvu vnitra nebo zpravodajské službě při provádění bezpečnostního řízení podle jiného právního předpisu 24),

m) příslušné zpravodajské službě, jedná-li se o informace, které jsou významné pro plnění jejích úkolů v oblastech působnosti vymezených zákonem upravujícím zpravodajské služby.

(2) Povinnosti zachovávat mlčenlivost stanovené v § 38 se, za předpokladu, že sdělené informace se použijí výhradně pro účely předcházení legalizaci výnosů z trestné činnosti a financování terorismu, nelze dovolávat při sdělování informací mezi

a) úvěrovými nebo finančními institucemi, včetně zahraničních úvěrových a finančních institucí, jestliže působí na území státu, který jim ukládá v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu povinnosti rovnocenné požadavkům práva Evropských společenství, a pokud náleží do stejné skupiny ve smyslu zákona o finančních konglomerátech 25),

b) povinnými osobami uvedenými v § 2 odst. 1 písm. e) a f) nebo osobami stejného typu působícími na území státu, který jim ukládá v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu povinnosti rovnocenné požadavkům práva Evropských společenství, pokud vykonávají svou profesní činnost jako zaměstnanci nebo v obdobném pracovněprávním vztahu, v rámci téže právnické osoby a mezi právnickými osobami, které jsou spolu smluvně nebo personálně propojeny, nebo

c) úvěrovými nebo finančními institucemi, nebo mezi povinnými osobami uvedenými v § 2 odst. 1 písm. e) a f), nebo osobami stejného typu působícími na území státu, který jim ukládá v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu povinnosti rovnocenné požadavkům práva Evropských společenství, a to v případech, které se týkají stejného klienta a stejného obchodu, a na nichž se podílí dvě nebo více osob, pokud jsou ze stejné profesní kategorie a vztahují se na ně rovnocenné povinnosti o zachování profesního tajemství a ochrany osobních údajů.

(3) Povinnosti mlčenlivosti se nelze dovolávat v řízení podle zákona o provádění mezinárodních sankcí.

§ 40

Zvláštní ustanovení o mlčenlivosti advokáta, notáře, auditora, soudního exekutora nebo daňového poradce

(1) Ustanovení této části se na advokáty a notáře nevztahují.

(2) Ustanovení této části se s výjimkou § 39 odst. 2 na auditory, soudní exekutory a daňové poradce nevztahují.

(3) Advokát, notář, auditor, soudní exekutor a daňový poradce je však i ve vztahu ke klientovi povinen zachovávat mlčenlivost o skutečnostech uvedených v § 38 odst. 1; to neplatí, pokud mají být tyto skutečnosti klientovi sděleny ve snaze odradit ho od zapojení se do nedovolené činnosti.

(4) Odstavce 1 až 3 se použijí i u jiných osob, na které se podle jiných právních předpisů vztahuje povinnost mlčenlivosti uložená advokátům, notářům, auditorům, soudním exekutorům a daňovým poradcům.

ČÁST PÁTÁ

PŘESHRANIČNÍ PŘEVOZY

§ 41

Oznamovací povinnost při přeshraničních převozech

(1) Fyzická osoba při vstupu do České republiky z oblasti mimo území Evropských společenství a při výstupu z České republiky do takové oblasti je povinna písemně oznámit celnímu orgánu dovoz a vývoz platných platidel v české nebo cizí měně, cestovních šeků nebo

peněžních poukázek směnitelných za hotové peníze, cenných papírů na doručitele nebo na řad, jakož i dalších investičních nástrojů, které jsou podepsané, ale neobsahují jméno příjemce, anebo vysoce hodnotných komodit, jako jsou zejména drahé kovy nebo drahé kameny, v úhrnné hodnotě 10 000 EUR nebo vyšší.

(2) Povinnost uvedenou v odstavci 1 má rovněž právnická osoba, která věci uvedené v odstavci 1 dováží nebo vyváží. Tuto povinnost za právnickou osobu plní fyzická osoba, která má tyto věci při sobě při překročení hranice území Evropských společenství.

(3) Osoba odesílající z České republiky mimo území Evropských společenství nebo přijímající odtud poštovní nebo jinou zásilku, která obsahuje věci uvedené v odstavci 1 v úhrnné hodnotě 10 000 EUR nebo vyšší, je povinna oznámit celnímu orgánu tuto zásilku a zajistit, aby mu byla zásilka předložena ke kontrole.

(4) Oznamovací povinnost podle odstavců 1 až 3 má osoba i tehdy, pokud na území Evropských společenství dováží nebo z něj vyváží anebo v zásilce přijímá nebo odesílá v průběhu 12 po sobě jdoucích měsíců věci uvedené v odstavci 1 v úhrnné hodnotě 10 000 EUR nebo vyšší. Oznamovací povinnost vzniká v době, kdy je osobě známo, že stanovené hranice bude dosaženo.

(5) V oznámení podle odstavců 1 až 4 se uvedou identifikační údaje oznamovatele, identifikační údaje vlastníka a zamýšleného příjemce přepravované věci, jsou-li oznamovateli známy, popis přepravované věci, údaje o původu věci a účelu dovozu nebo vývozu a trasa a způsob přepravy.

(6) Oznámení se podává na tiskopise, jehož vzor je uveden v příloze k tomuto zákonu. Tiskopis je k dispozici u celního úřadu; ministerstvo jej rovněž zveřejní způsobem umožňujícím dálkový přístup. Osoba, která oznámení podává, odpovídá za správnost a úplnost v něm vyplněných údajů.

(7) Pro přepočet jiné měny na euro podle odstavců 1, 3 nebo 4 se použije po celý kalendářní měsíc kurz vyhlášený Českou národní bankou a platný předposlední středu předchozího kalendářního měsíce. Celní úřad sdělí osobám na základě ústní žádosti výši kurzů pro účely plnění oznamovací povinnosti podle odstavců 1 až 4. Hodnotou cenných papírů a vysoce hodnotných komodit se rozumí jejich aktuální tržní cena, popřípadě cena stanovená podle kurzů na oficiálních trzích.

§ 42

Činnost celních orgánů

(1) Celní orgány kontrolují plnění oznamovací povinnosti stanovené v § 41.

(2) Celní orgány zaznamenávají a zpracovávají oznámení uvedená v § 41 včetně osobních údajů v nich uvedených. Za účelem výkonu kontroly podle odstavce 1 mohou zaznamenávat a zpracovávat i informace o převozu nebo zaslání věci, uvedené v § 41 odst. 1, v hodnotě nižší než 10 000 EUR.

(3) Celní úřady neprodleně zasílají ministerstvu údaje o plnění oznamovací povinnosti stanovené v § 41 včetně případů, kdy došlo k porušení této povinnosti.

(4) Celní úřad může při zjištění porušení povinností stanovených v § 41 odst. 1 až 4 zajistit věci, kterých se porušení povinnosti týká. Proti rozhodnutí celního úřadu o zajištění věci není přípustné odvolání a je vykonatelné okamžikem jeho ústního vyhlášení tomu, kdo má věci u sebe. Písemné vyhotovení rozhodnutí se doručuje tomu, u koho byly věci zajištěny; o zajištění se dále vyrozumí stejnopisem rozhodnutí ten, kdo věci dováží nebo vyváží, a jejich majitel, pokud jsou tyto osoby rozdílné od toho, u koho byly věci zajištěny, a jsou-li celnímu úřadu známy.

(5) Osoba, které bylo rozhodnutí o zajištění věci podle odstavce 4 oznámeno, vydá věci celnímu úřadu. Nejsou-li zajištěné věci na výzvu celnímu úřadu vydány, mohou být tomu, kdo je má u sebe, odňaty. Osobě, která věci vydala nebo jíž byly odňaty, vystaví celní úřad o této skutečnosti potvrzení.

(6) Nebudou-li zajištěné věci k dalšímu řízení potřebné, nebude-li rozhodnuto o jejich propadnutí nebo zabrání a nepřichází-li v úvahu jejich použití na úhradu pokuty, nákladů řízení nebo exekuce, vrátí je celní úřad bez zbytečného odkladu osobě, která je vydala nebo jíž byly odňaty.

ČÁST ŠESTÁ
SPRÁVNÍ DELIKTY

§ 43

Porušení povinnosti mlčenlivosti

(1) Zaměstnanec povinné osoby, zaměstnanec ministerstva nebo jiného dozorčího úřadu, anebo fyzická osoba, která je pro povinnou osobu, ministerstvo nebo jiný dozorčí úřad činná na základě jiné než pracovní smlouvy, se dopustí přestupku tím, že poruší povinnost mlčenlivosti stanovenou v § 38 odst. 1 nebo 2.

(2) Fyzická osoba neuvedená v odstavci 1 se dopustí přestupku tím, že poruší povinnost mlčenlivosti podle § 38 odst. 3.

(3) Povinná osoba se dopustí správního deliktu tím, že poruší povinnost mlčenlivosti podle § 38 odst. 1 nebo 2.

(4) Za přestupek podle odstavců 1 a 2 lze uložit pokutu do 200 000 Kč a za správní delikt podle odstavce 3 se uloží pokuta do 200 000 Kč.

(5) Za přestupek podle odstavce 1 lze uložit pokutu do 1 000 000 Kč a za správní delikt podle odstavce 3 se uloží pokuta do 1 000 000 Kč, jestliže tímto jednáním bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu.

§ 44

Neplnění povinností při identifikaci a kontrole klienta

(1) Povinná osoba se dopustí správního deliktu tím, že

a) nesplní povinnost identifikace klienta podle § 7,

b) opakovaně nesplní povinnost kontroly klienta podle § 9,

c) uskuteční obchod nebo uzavře obchodní vztah v rozporu se zákazem uvedeným v § 15, nebo

d) nesplní povinnost uchovávat údaje podle § 16.

(2) Za správní delikt podle odstavce 1 písm. a) a b) se uloží pokuta do 1 000 000 Kč.

(3) Za správní delikt podle odstavce 1 písm. c) a d) se uloží pokuta do 10 000 000 Kč.

(4) Jestliže jednáním podle odstavce 1 písm. a), b) nebo d) bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu, uloží se pokuta do 50 000 000 Kč.

§ 45

Nesplnění informační povinnosti

(1) Povinná osoba se dopustí správního deliktu tím, že

a) nesplní informační povinnost podle § 24, nebo

b) v případě uvedeném v § 25 odst. 4 nepřijme odpovídající doplňková opatření k účinnému zvládání rizika zneužití pro legalizaci výnosů z trestné činnosti nebo financování terorismu a zabránění přenosu těchto rizik na území České republiky a dalších států Evropské unie nebo Evropského hospodářského prostoru.

(2) Úvěrová nebo finanční instituce se dopustí správního deliktu tím, že

a) v rozporu s § 25 odst. 4 nepředá relevantní informaci své pobočce nebo většinově vlastněné dceřiné společnosti nacházející se ve státě, který není členem Evropské unie nebo Evropského hospodářského prostoru, o uplatňovaných metodách a postupech kontroly klienta a uchovávání záznamů v těchto zemích, nebo

b) nesdělí informaci podle § 25 odst. 6.

(3) Za správní delikt podle odstavců 1 a 2 se uloží pokuta do 10 000 000 Kč.

(4) Jestliže jednáním podle odstavce 1 bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu, uloží se pokuta do 50 000 000 Kč.

§ 46

Nesplnění oznamovací povinnosti

(1) Povinná osoba se dopustí správního deliktu tím, že neoznámí ministerstvu podezřelý obchod.

(2) Za správní delikt podle odstavce 1 se uloží pokuta do 5 000 000 Kč.

(3) Jestliže jednáním podle odstavce 1 bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu, uloží se pokuta do 50 000 000 Kč.

§ 47

Nesplnění povinnosti odložit příkaz klienta

(1) Povinná osoba se dopustí správního deliktu tím, že poruší povinnost odložit splnění příkazu klienta podle § 20 odst. 1.

(2) Povinná osoba se dopustí správního deliktu tím, že nesplní povinnost odložit splnění příkazu klienta nebo zajistit majetek na základě rozhodnutí vydaného ministerstvem podle § 20 odst. 3.

(3) Za správní delikt podle odstavce 1 se uloží pokuta do 1 000 000 Kč.

(4) Za správní delikt podle odstavce 2 se uloží pokuta do 10 000 000 Kč.

(5) Jestliže jednáním podle odstavce 1 bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu, uloží se pokuta do 50 000 000 Kč.

§ 48

Nesplnění povinností k prevenci

(1) Povinná osoba uvedená v § 2 odst. 1 písm. a) až d), h) a i) se dopustí správního deliktu tím, že nevypracuje systém vnitřních zásad podle § 21 odst. 2 až 5.

(2) Povinná osoba uvedená v § 2 odst. 1 písm. a), b) bodech 1 až 6, 10, 11 a písm. c) se dopustí správního deliktu tím, že systém vnitřních zásad nebo jeho změny nedoručí podle § 21 odst. 6 nebo nepodá písemnou informaci o způsobu odstranění zjištěných nedostatků podle § 21 odst. 8.

(3) Povinná osoba se dopustí správního deliktu tím, že nezajistí pravidelné proškolení zaměstnanců podle § 23.

(4) Úvěrová instituce se dopustí správního deliktu tím, že poruší povinnosti stanovené pro navazování korespondenčního bankovního vztahu podle § 25 odst. 1, 2 nebo 3.

(5) Povinná osoba uvedená v § 29 odst. 1 se dopustí správního deliktu tím, že vykonává činnost na základě poštovní smlouvy a za podmínek stanovených zákonem o poštovních službách, jejímž účelem je dodání poukázané peněžní částky, bez osvědčení o způsobilosti podle § 29.

(6) Za správní delikt podle odstavců 1 až 3 se uloží pokuta do 1 000 000 Kč.

(7) Za správní delikt podle odstavce 4 nebo 5 se uloží pokuta do 5 000 000 Kč.

(8) Jestliže jednáním podle odstavce 4 bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu, uloží se pokuta do 50 000 000 Kč.

§ 49

Porušení povinností při převodech peněžních prostředků

(1) Povinná osoba jako poskytovatel platebních služeb nebo jako zprostředkující poskytovatel platebních služeb se při převodu peněžních prostředků dopustí správního deliktu tím, že v rozporu s přímo použitelným předpisem Evropských společenství, který určuje obsah informací, doprovázejících takové převody 20),

a) nezajistí, aby převod peněžních prostředků doprovázely informace o plátci,

b) nemá zavedeny efektivní postupy pro identifikaci chybějících nebo neúplných informací o plátci,

c) nepřijme odpovídající opatření vůči poskytovateli platebních služeb plátce, který při převodu peněžních prostředků nezajistí, aby platba byla doprovázena informací o plátci, nebo

d) nezpřístupní na vyžádání poskytovateli platebních služeb příjemce úplné informace o plátci v případech, kdy převod není doprovázen úplnou informací o plátci.

(2) Za správní delikt podle odstavce 1 se uloží pokuta do 10 000 000 Kč.

(3) Jestliže jednáním podle odstavce 1 bylo znemožněno nebo ztíženo zajištění nebo odčerpání výnosu z trestné činnosti nebo umožněno financování terorismu, uloží se pokuta do 50 000 000 Kč.

§ 50

Neplnění oznamovací povinnosti při přeshraničních převozech

(1) Fyzická osoba se dopustí přestupku tím, že

a) nesplní oznamovací povinnost při vstupu do České republiky z oblasti mimo území Evropských společenství nebo při výstupu z České republiky do takové oblasti podle § 41 odst. 1 nebo 4, nebo

b) nesplní oznamovací povinnost při odeslání poštovní nebo jiné zásilky z České republiky mimo území Evropských společenství nebo přijetí takové zásilky z oblasti mimo území Evropských společenství podle § 41 odst. 3 nebo 4.

(2) Právnická osoba se dopustí správního deliktu tím, že

a) nesplní oznamovací povinnost při vstupu do České republiky z oblasti mimo území Evropských společenství nebo při výstupu z České republiky do takové oblasti podle § 41 odst. 2 nebo 4, nebo

b) nesplní oznamovací povinnost při odeslání poštovní nebo jiné zásilky z České republiky mimo území Evropských společenství nebo přijetí takové zásilky z oblasti mimo území Evropských společenství podle § 41 odst. 3 nebo 4.

(3) Za přestupek podle odstavce 1 lze uložit pokutu do 10 000 000 Kč nebo propadnutí věci.

(4) Za správní delikt podle odstavce 2 se uloží pokuta do 10 000 000 Kč nebo propadnutí věci.

Společná ustanovení o správních deliktech

§ 51

(1) Propadnutí věci lze uložit, jestliže věc náleží pachateli a byla

a) ke spáchání správního deliktu užita, nebo

b) správním deliktem získána nebo nabyta za věc tímto deliktem získanou.

(2) Nebylo-li uloženo propadnutí věci uvedené v odstavci 1 písm. a) nebo b), rozhodne se o jejím zabrání, jestliže

a) náleží pachateli, kterého nelze za správní delikt stíhat,

b) nenáleží pachateli správního deliktu nebo mu nenáleží zcela, nebo

c) vlastník není znám.

(3) Propadnutí věci nelze uložit a věc nelze zabrat, je-li hodnota věci v nápadném nepoměru k povaze správního deliktu.

(4) Vlastníkem propadlé nebo zabrané věci se stává stát.

§ 52

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při určení výměry pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 2 let ode dne, kdy se o něm dozvěděl, nejpozději však do 10 let ode dne, kdy byl spáchán.

(4) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby nebo v přímé souvislosti s ním, se vztahují ustanovení tohoto zákona o odpovědnosti a postihu právnické osoby.

(5) Správní delikty podle tohoto zákona, s výjimkou správních deliktů spáchaných povinnou osobou uvedenou v § 2 odst. 1 písm. j) a k) a správních deliktů podle § 50, v prvním stupni projednává ministerstvo.

(6) Správní delikty spáchané povinnou osobou uvedenou v § 2 odst. 1 písm. j) a k) projednává v prvním stupni dozorčí úřad.

(7) Správní delikty podle § 50 projednává celní úřad. Přestupek podle § 50 odst. 1 může příslušný celní úřad postoupit k projednání celnímu úřadu, v jehož územním obvodu má pachatel přestupku trvalý pobyt.

(8) Pokuty a náhrady nákladů řízení vybírá správní orgán, který je uložil. Pokuty a náhrady nákladů řízení jsou splatné do 30 dnů ode dne nabytí právní moci rozhodnutí. Příjem z pokut a z náhrad nákladů řízení je příjmem státního rozpočtu.

(9) Není-li ve lhůtě splatnosti pokuta zaplacena, celní úřad může na její úhradu použít zajištěné věci uvedené v § 41 odst. 1, 3 a 4, pokud je zajistil; postupuje přitom podle ustanovení o celním zástavním právu podle celního zákona.

§ 53

Podle jiného právního předpisu 26) se projedná jednání, které má znaky správního deliktu podle § 43 až 48, dopustí-li se jej advokát, notář, auditor, soudní exekutor nebo daňový poradce jako povinná osoba. Dozorčí úřad uvedený v § 35 odst. 1 bezodkladně odevzdá věc k projednání orgánu příslušnému podle takového jiného právního předpisu a na jeho žádost učiní nezbytná šetření k zajištění důkazních prostředků.

ČÁST SEDMÁ

SPOLEČNÁ A ZÁVĚREČNÁ USTANOVENÍ

§ 54

(1) Povinnosti, které tento zákon ukládá povinným osobám, se vztahují pouze k činnostem, které jsou předmětem jejich podnikání nebo jimi poskytovaných služeb.

(2) Není-li v tomto zákoně stanoveno jinak, mají povinné osoby uvedené v § 2 odst. 2 písm. a) a b) práva a povinnosti, které tento zákon stanoví pro příslušný typ povinné osoby uvedené v § 2 odst. 1.

(3) Částkou uvedenou v eurech, nestanoví-li tento zákon jinak (§ 41 odst. 7), se pro účely tohoto zákona rozumí odpovídající hodnota v jakékoliv měně stanovená podle kurzu vyhlášeného Českou národní bankou a platného pro den, ve kterém je plněna povinnost podle tohoto zákona; pokud tento kurz ještě není v tomto dni k dispozici, použije se kurz platný pro předchozí den. Je-li platba rozdělena na několik samostatných plnění, je hodnotou obchodu nebo platby jejich součet, jestliže spolu tyto platby souvisí.

(4) Platba vysoce hodnotnými komoditami, jako jsou zejména drahé kovy nebo drahé kameny, se považuje za platbu v hotovosti.

(5) Povinná osoba, jejímž jménem nebo na jejíž účet nabízejí její produkty nebo služby třetí osoby, zajistí, aby tyto osoby uplatňovaly postupy k předcházení legalizaci výnosů z trestné činnosti a financování terorismu ve stejném rozsahu jako tato povinná osoba.

§ 55

(1) Řízení vedené podle tohoto zákona je vždy neveřejné.

(2) Na základě přijatého oznámení podezřelého obchodu nebo jiného podnětu provádí ministerstvo šetření, ve kterém postupuje bez zbytečných průtahů.

(3) Po ukončení šetření ministerstvo bez zbytečného odkladu vhodným způsobem vyrozumí o této skutečnosti toho, kdo podal oznámení podezřelého obchodu. Jiná osoba se o šetření a jeho ukončení nevyrozumívá.

(4) Pověření zaměstnanci ministerstva se při výkonu činností podle tohoto zákona prokazují služebním průkazem, vydaným na základě zákona o provádění mezinárodních sankcí.

§ 56

Zmocňovací ustanovení

Česká národní banka vydá vyhlášku k provedení § 21 odst. 9.

§ 57

Přechodná ustanovení

(1) Řízení zahájená přede dnem nabytí účinnosti tohoto zákona se dokončí podle tohoto zákona, s výjimkou řízení o přestupku nebo jiném správním deliktu, spáchaném přede dnem nabytí účinnosti tohoto zákona, pokud je předchozí právní úprava pro obviněného příznivější.

(2) Osoba, která ke dni nabytí účinnosti tohoto zákona vykonává činnost na základě poštovní smlouvy a za podmínek stanovených zákonem o poštovních službách, jejímž účelem je dodání poukázané peněžní částky, může v této činnost bez osvědčení o způsobilosti podle § 29 pokračovat nejdéle po dobu 6 měsíců ode dne nabytí účinnosti tohoto zákona.

(3) Povinná osoba uvedená v § 2 odst. 1 písm. a) až d), h) a i), která má vypracovaný systém vnitřních zásad, postupů a kontrolních opatření podle dosavadních právních předpisů, vypracuje do 60 dnů ode dne nabytí účinnosti tohoto zákona systém vnitřních zásad, postupů a kontrolních opatření ve smyslu § 21 odst. 2.

(4) Úvěrová instituce, finanční instituce uvedená v § 2 odst. 1 písm. b) bodech 5, 6, 10 a 11 a povinná osoba uvedená v § 2 odst. 1 písm. c), která má vypracovaný systém vnitřních zásad, postupů a kontrolních opatření podle dosavadních právních předpisů, doručí do 60 dnů ode dne nabytí účinnosti tohoto zákona ministerstvu systém vnitřních zásad, postupů a kontrolních opatření vypracovaný ve smyslu § 21 odst. 2.

§ 58

Zrušovací ustanovení

Zrušují se:

1. Zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů.

2. Vyhláška č. 343/2004 Sb., kterou se stanoví vzor tiskopisu podle § 5 odst. 5 zákona č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů.

3. Vyhláška č. 344/2004 Sb., o plnění oznamovací povinnosti podle zákona č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů.

4. Vyhláška č. 283/2006 Sb., kterou se mění vyhláška č. 344/2004 Sb., o plnění oznamovací povinnosti podle zákona č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů.

§ 59

Účinnost

Tento zákon nabývá účinnosti prvním dnem druhého kalendářního měsíce následujícího po dni jeho vyhlášení.

Vlček v. r.

Klaus v. r.

Topolánek v. r.

Příloha
OZNÁMENÍ/DECLARATION

1) Směrnice Evropského parlamentu a Rady 2005/60/ES ze dne 26. října 2005 o předcházení zneužití finančního systému k praní peněz a financování terorismu.
Směrnice Komise 2006/70/ES ze dne 1. srpna 2006, kterou se stanoví prováděcí opatření ke směrnici Evropského parlamentu a Rady 2005/60/ES, pokud se jedná o definici „politicky exponovaných osob" a technická kritéria pro zjednodušené postupy hloubkové kontroly klienta a pro výjimku na základě finanční činnosti vykonávané příležitostně nebo ve velmi omezené míře.

2) Nařízení Evropského parlamentu a Rady (ES) č. 1889/2005 ze dne 26. října 2005 o kontrolách peněžní

hotovosti vstupující do Společenství nebo je opouštějící.
Nařízení Evropského parlamentu a Rady (ES) č. 1781/2006 ze dne 15. listopadu 2006 o informacích o plátci doprovázejících převody peněžních prostředků.

3) Zákon č. 284/2009 Sb., o platebním styku.

4) § 91 až 115 zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů.

5) § 4 zákona č. 256/2004 Sb., ve znění pozdějších předpisů.

6) § 29 zákona č. 256/2004 Sb., ve znění zákona č. 56/2006 Sb.

7) § 2 odst. 1 písm. v) zákona č. 363/1999 Sb., o pojišťovnictví, ve znění pozdějších předpisů.

8) § 81 a násl. zákona č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů.

9) § 5 obchodního zákoníku.

10) § 2 zákona č. 20/1987 Sb., o státní památkové péči.

11) § 1 odst. 1 zákona č. 71/1994 Sb., o prodeji a vývozu předmětů kulturní hodnoty, ve znění zákona č. 80/2004 Sb.

12) § 93 trestního zákona.

13) § 95 trestního zákona.

14) Čl. 1 až 4 rámcového rozhodnutí Rady ze dne 13. června 2002 o boji proti terorismu (2002/475/SVV).

15) § 89 odst. 8 trestního zákona.

16) § 20f a násl. občanského zákoníku.
Zákon č. 83/1990 Sb., o sdružování občanů, ve znění pozdějších předpisů.

17) § 2 zákona č. 69/2006 Sb., o provádění mezinárodních sankcí.

18) Zákon č. 340/2006 Sb., o činnosti institucí zaměstnaneckého penzijního pojištění z členských států Evropské unie na území České republiky a o změně zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů.

19) Zákon č. 124/2002 Sb., ve znění pozdějších předpisů.

20) Nařízení Evropského parlamentu a Rady (ES) č. 1781/2006.

21) § 44 zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.

22) § 3 odst. 1 písm. a) zákona č. 358/1992 Sb.

23) § 3 odst. 1 písm. b) zákona č. 358/1992 Sb.

24) Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

25) Zákon č. 377/2005 Sb., o doplňkovém dozoru nad bankami, spořitelními a úvěrními družstvy, institucemi elektronických peněz, pojišťovnami a obchodníky s cennými papíry ve finančních konglomerátech a o změně některých dalších zákonů (zákon o finančních konglomerátech), ve znění pozdějších předpisů.

26) Zákon č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů.
Zákon č. 358/1992 Sb., ve znění pozdějších předpisů.

Zákon č. 254/2000 Sb., o auditorech a o změně zákona č. 165/1998 Sb., ve znění pozdějších předpisů.

Zákon č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů, ve znění pozdějších předpisů.

Zákon č. 523/1992 Sb., o daňovém poradenství a Komoře daňových poradců České republiky, ve znění pozdějších předpisů.

11.2 Vybraná část ze zákona č. 284/2009 Sb. o platebním styku, v platném znění

Oddíl 2

Lhůty pro provádění platebních transakcí

§ 108

(1) Poskytovatel provede platební transakci ve lhůtách dohodnutých s uživatelem v souladu s ustanoveními tohoto oddílu, nestanoví-li jiný právní předpis možnost lhůtu prodloužit.

(2) Připadne-li okamžik přijetí peněžních pro- středků od uživatele nebo okamžik připsání částky platební transakce na účet poskytovatele příjemce na dobu, která není provozní

dobou poskytovatele, platí, že k přijetí nebo připsání došlo na začátku následující pro- vozní doby poskytovatele.

§ 109

Lhůta pro připsání peněžních prostředků na účet poskytovatele příjemce

(1) Poskytovatel plátce zajistí, aby peněžní pro- středky byly připsány na účet poskytovatele příjemce nejpozději do konce následujícího pracovního dne po okamžiku přijetí platebního příkazu.

(2) V případě papírového platebního příkazu se plátce a jeho poskytovatel mohou dohodnout na lhůtě o 1 pracovní den delší, než je lhůta uvedená v odstavci 1.

(3) V případě platebních transakcí

a) v měně euro, nebo

b) na území České republiky v české měně,

které zahrnují nanejvýš jednu směnu měn mezi měnou euro a měnou členského státu, na jehož území ke směně měn dochází, si uživatel a jeho poskytovatel mohou dohodnout pouze lhůtu kratší, než je lhůta uvedená v odstavcích 1 a 2.

(4) V případě jiných platebních transakcí, než které jsou uvedeny v odstavci 3, si uživatel a jeho poskytovatel mohou dohodnout lhůtu odlišnou, než jaká je uvedena v odstavcích 1 a 2, nejvýše však 4 pracovní

(5) Odstavce 2 a 4 se nepoužijí v případě platebních transakcí na území České republiky v české měně; pokud taková platební transakce zahrnuje směnu měn jinou než mezi měnou euro a českou měnou, mohou se plátce a jeho poskytovatel dohodnout na lhůtě o 1 pracovní den delší, než je lhůta uvedená v odstavci 1.

(6) Lhůty uvedené v odstavcích 2 až 5 počínají běžet dnem následujícím po dni, kdy nastal okamžik přijetí platebního příkazu, není-li mezi plátcem a jeho poskytovatelem dohodnuto, že lhůta počíná běžet dříve.

§ 110

Lhůta pro připsání peněžních prostředků na platební účet příjemce

Poskytovatel příjemce

a) připíše částku platební transakce na platební účet

b) nevede-li příjemci platební účet, dá příjemci částku platební transakce k dispozici

neprodleně poté, kdy byla připsána na účet poskytovatele příjemce, nebo jedná-li se o platební transakci v měně jiného než členského státu nebo o platební účet vedený v měně jiného než členského státu, do konce pracovního dne následujícího po dni, kdy byla připsána na účet poskytovatele příjemce.

§ 111

Lhůta platební transakce v rámci jednoho poskytovatele v české měně

Ustanovení § 109 a 110 se nepoužijí v případě platební transakce v rámci téhož poskytovatele na území České republiky v české měně. V tomto případě musí být peněžní prostředky připsány na platební účet příjemce, nebo nevede-li poskytovatel příjemci platební účet, dány příjemci k dispozici nejpozději na konci dne, v němž nastal okamžik přijetí příkazu. Pokud ta- ková platební transakce zahrnuje směnu měn, mohou se plátce a jeho poskytovatel dohodnout na lhůtě o 1 pracovní den delší.

§ 112

Lhůta pro připsání peněžních prostředků vložených na platební účet

(1) Ustanovení § 109 až 111 se nepoužijí, vloží-li spotřebitel nebo drobný podnikatel na účet hotovost v měně členského státu, ve které je platební účet veden. V takovém případě poskytovatel peněžní prostředky připíše na platební účet příjemce neprodleně po oka- mžiku přijetí peněžních prostředků od spotřebitele nebo drobného podnikatele. V témže okamžiku nastává i den valuty a peněžní prostředky musí být uživateli k dispozici.

(2) Ustanovení § 109 a 110 se nepoužijí,

a) vloží-li spotřebitel nebo drobný podnikatel na platební účet hotovost v měně jiného než členského státu, ve které je platební účet veden, nebo

b) vloží-li uživatel, který není spotřebitelem ani drobným podnikatelem, na platební účet hotovost v měně, ve které je platební účet veden.

(3) V případech uvedených v odstavci 2 připíše poskytovatel peněžní prostředky na platební účet příjemce nejpozději následující pracovní den po dni přijetí peněžních prostředků od uživatele. V témže okamžiku nastává i den valuty a peněžní prostředky musí být uživateli k dispozici.

§ 113

Lhůta pro předání platebního příkazu v případě platební transakce z podnětu příjemce

(1) V případě platební transakce z podnětu příjemce, k níž byl dán souhlas za použití platebního pro- středku, předá poskytovatel příjemce platební příkaz poskytovateli plátce ve lhůtě dohodnuté mezi příjemcem a jeho poskytovatelem.

(2) V případě inkasa předá poskytovatel příjemce platební příkaz poskytovateli plátce ve lhůtě dohodnuté mezi příjemcem a jeho poskytovatelem tak, aby bylo umožněno dodržení okamžiku přijetí platebního příkazu dohodnutého mezi plátcem a příjemcem.

§ 114

Den valuty peněžních prostředků

(1) Den valuty peněžních prostředků odepsaných z platebního účtu plátce nastává nejdříve okamžikem přijetí platebního příkazu.

(2) Den valuty peněžních prostředků připsaných na platební účet příjemce nastává nejpozději okamžikem, kdy jsou peněžní prostředky připsány na účet příjemce; § 112, 117 a 118 tím nejsou dotčeny.

(3) Okamžikem připsání peněžních prostředků na platební účet příjemce musí být tyto peněžní prostředky k dispozici příjemci.

11.3 Vybraná část ze zákona č. 40/2009 Sb., trestní zákon, v platném znění

§ 214

Podílnictví

1) Kdo ukryje, na sebe nebo jiného převede anebo užívá

a) věc nebo jinou majetkovou hodnotu, která byla získána trestným činem spáchaným na území České republiky nebo v cizině jinou osobou, nebo jako odměna za něj, nebo

b) věc nebo jinou majetkovou hodnotu, která byla opatřena za věc nebo jinou majetkovou hodnotu uvedenou v písmenu a),

bude potrestán odnětím svobody až na čtyři léta, peněžitým trestem, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty; spáchá-li však čin ve vztahu k věci, která pochází z trestného činu, na který zákon stanoví trest mírnější, bude potrestán tímto trestem mírnějším.

(2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 ve vztahu k věci nebo jiné majetkové hodnotě, která má větší hodnotu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného větší prospěch.

(3) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin ve vztahu k věci nebo jiné majetkové hodnotě pocházející ze zvlášť závažného zločinu,

c) spáchá-li takový čin ve vztahu k věci nebo jiné majetkové hodnotě, která má značnou hodnotu, nebo

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 ve vztahu k věci nebo jiné majetkové hodnotě, která má hodnotu velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 215

Podílnictví z nedbalosti

(1) Kdo ukryje nebo na sebe nebo jiného převede z nedbalosti věc nebo jinou majetkovou hodnotu nikoli malé hodnoty, která byla získána trestným činem spáchaným na území České republiky nebo v cizině jinou osobou, nebo jako odměna za něj, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 proto, že porušil důležitou povinnost vyplývající z jeho zaměstnání, povolání, postavení nebo funkce nebo uloženou mu podle zákona, nebo

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 ve vztahu k věci nebo jiné majetkové hodnotě pocházející ze zvlášť závažného zločinu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 216

Legalizace výnosů z trestné činnosti

(1) Kdo zastírá původ nebo jinak usiluje, aby bylo podstatně ztíženo nebo znemožněno zjištění původu

a) věci nebo jiné majetkové hodnoty, která byla získána trestným činem spáchaným na území České republiky nebo v cizině, nebo jako odměna za něj, nebo

b) věci nebo jiné majetkové hodnoty, která byla opatřena za věc nebo jinou majetkovou hodnotu uvedenou v písmenu a), nebo kdo jinému spáchání takového činu umožní,

bude potrestán odnětím svobody až na čtyři léta, peněžitým trestem, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty; spáchá-li však takový čin ve vztahu k věci nebo jiné majetkové hodnotě, která pochází z trestného činu, na který zákon stanoví trest mírnější, bude potrestán tímto trestem mírnějším.

(2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 ve vztahu k věci nebo jiné majetkové hodnotě ve větší hodnotě, nebo

b) získá-li takovým činem pro sebe nebo pro jiného větší prospěch.

(3) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin ve vztahu k věci nebo jiné majetkové hodnotě pocházející ze zvlášť závažného zločinu,

c) spáchá-li takový čin ve vztahu k věci nebo jiné majetkové hodnotě ve značné hodnotě,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) zneužije-li ke spáchání takového činu svého postavení v zaměstnání nebo své funkce.

(4) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 ve spojení s organizovanou skupinou působící ve více státech,

b) spáchá-li takový čin ve vztahu k věci nebo jiné majetkové hodnotě v hodnotě velkého rozsahu, nebo

c) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 217

Legalizace výnosů z trestné činnosti z nedbalosti

(1) Kdo jinému z nedbalosti umožní zastřít původ nebo zjištění původu věci nebo jiné majetkové hodnoty ve větší hodnotě, která byla získána trestným činem spáchaným na území České republiky nebo v cizině, nebo jako odměna za něj, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 proto, že porušil důležitou povinnost vyplývající z jeho zaměstnání, povolání, postavení nebo funkce nebo uloženou mu podle zákona, nebo

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 ve vztahu k věci nebo jiné majetkové hodnotě pocházející ze zvlášť závažného zločinu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

11.4 Popis současného stavu řešení řízení rizik spojených s AML

11.4.1 Hlášení podezřelého obchodu/klienta

Pracovník banky vyplní formulář (dokument ve Wordu), který následně zašle elektronickou poštou na odpovědného pracovníka compliance, v případě nutnosti navíc oznámí tuto skutečnost telefonicky. Podezření pro vznik hlášení může vzniknout ve front-office i back-office. Poslat jej může libovolný pracovník, který má podezření.

V případě dohledávání dalších podrobností k přijatému hlášení se musí CO obrátit znovu na pracovníka, který hlášení poslal, nebo na jiného pracovníka banky, aby vyhledal další potřebné informace. Je pouze v kompetenci CO rozhodnout, zdali hlášení bude sloužit jako podklad pro vznik a odeslání oznámení dle AML příslušnému dohledovému orgánu státní správy (FAÚ) nebo bude odloženo bez žádných dalších akcí.

11.4.2 Komunikace s FAÚ

Uzná-li CO náležitosti pro podání oznámení, činí to obvykle faxem a telefonátem na příslušný orgán nebo prostřednictvím portálu Moneyweb. Ručně si zapisuje datum a čas odeslání oznámení, v případě nutnosti volá odpovědnému pracovníkovi banky, aby zablokoval provedení transakce. Právo opět transakci odblokovat má pouze CO. Děje se to v případě uplynutí zákonem stanovené doby pro zablokování transakce, kdy regulátor nenařídil další blokaci, nebo pokud regulátor sdělí, že transakci je možné odblokovat ještě před uplynutím zákonné doby. Hlídání uplynutí času je na CO a jeho písemné poznámce. Odblokování se děje opět telefonátem na příslušeného pracovníka banky.

11.4.3 Mlčenlivost

Zachování mlčenlivosti je řízeno pokud možno jednosměrným komunikačním kanálem směrem k oddělení compliance, které zpětně neinformuje o dalším nakládání s hlášením. CO nesděluje ostatním pracovníkům banky, proč potřebuje dodatečné materiály, či z jakého důvodu je transakce blokována. Odůvodnění blokace přichází v úvahu pouze ve specifických případech (konkrétně v momentě, kdy se klient snaží zjistit, proč jeho transakce doposud nebyla provedena), kdy je vysvětlení podáno pouze interně v maximálně stručné míře sdělení s důrazem na to, že klient se o tomto nesmí dozvědět.

11.4.4 Aktivní hledání podezřelého chování

Compliance z vlastní iniciativy kontroluje a hledá podezřelé chování na účtech klientů. Většina této činnosti je prováděna ručně porovnáváním výstupů z různých bankovních systémů a hledáním odchylek od *běžného* chování. Na základě získaných dat může podat oznámení příslušnému orgánu.

11.4.5 Detekování politicky exponované osoby

Při vzniku nového obchodního vztahu je součástí procesu i dotaz na klienta, zda-li je politicky exponovanou osobou. V případě kladné odpovědi, jsou po něm vyžadovány další osobní údaje.

Ať už nový klient odpoví jakkoliv, je ručně zkontrolován ve veřejné databázi WorldCheck[89]. Stávající klienti jsou dále ručně kontrolováni v pravidelných intervalech v průběhu trvání obchodního vztahu a jejich stav je případně aktualizován.

[89] www.world-check.com

11.4.6 Detekování potenciálně problémového klienta

Zvláštní kategorii klientů tvoří potenciálně *problémoví* klienti, jedná se o osoby, které mají riziková zaměstnání; např. chemický, zbrojní, loterijní, či výherní průmysl, nebo jsou majetkově s tímto průmyslem spjati.

Dále se jedná o klienty s původem v nebezpečných zemích; např. Írán, Afghánistán.

Problémoví klienti mohou být již na *black-listu*, tzn. že existuje záznam o jejich dřívějším prohřešku.

V rámci řízení rizika spojeného s platebními transakcemi těchto klientů je vhodné držet jejich podíl na únosné/řiditelné míře. Práh není stanoven předpisem a banka si jej určuje sama.

11.4.7 Školení zaměstnanců

Všichni zaměstnanci musejí být minimálně jednou za rok proškoleni v oblasti AML. Důkaz o proškolení je velmi podstatný při kontrole od regulátorů. Školení probíhají osobně v rámci větší skupiny zaměstnanců pod vedením CO, či prostřednictvím e-learningu. Docházka se uchovává na papíře (datum, jméno, podpis).

11.4.8 Archivace dokumentů

Archivování veškerých dokumentů je ve většině případů v papírové podobě, či uložených *.doc* souborů v síťových složkách CO.

11.5 Popis požadovaného stavu řízení rizik spojených s AML

11.5.1 Hlášení podezřelého obchodu/klienta

V případě pochybností pracovník banky vyplní předpřipravený webový formulář *hlášení* na bankovním intranetu (identifikuje klienta, popíše příčiny svých pochybností, identifikuje transakci, zvolí odpovídají prioritu, identifikuje sebe) a potvrdí uložení hlášení. Hlášení je ihned uloženo do databáze a je upozorněn CO o vzniku nového hlášení.

CO si u sebe otevře nově došlé hlášení, v případě potřeby si nechá systémově analyzovat historii klienta, posoudí jeho závažnost a buď z něj nechá vytvořit oznámení pro FAÚ nebo jej označí jako nepodezřelé.

11.5.2 Komunikace s FAÚ

Vygenerované oznámení se odesílá prostřednictvím speciálního zabezpečeného webového rozhraní regulátora (MoneyWeb), v případě technických potíží je na druhém místě fax, na třetím osobní telefonát.

Současně s odesláním oznámení je jeho elektronická kopie uložena v databázi banky a je automaticky (případně ručně) vložen čas a datum odeslání oznámení a zároveň je odeslán pokyn pro zablokování provedení transakce identifikované v hlášení.

CO vidí na svém dashboardu seznam oznámení včetně jejich časového vývoje (tzn. běží základní doba blokování 24h, běží prodloužená doba blokování 72h). Odblokování transakce může provést opět jen CO a to na základě obdržení zprávy z FAÚ, že je to možné, nebo v případě neobdržení žádné zprávy v době trvání lhůty blokování transakce.

Pokud lhůta blokování transakce vyprší bez odezvy FAÚ, je CO upozorněn systémem, že je potřeba provést odblokování transakce, po schválení CO je odeslán příkaz pro odblokování provedení transakce.

Jedná-li se pouze o oznámení ex-post, kdy není vyžadováno zablokování transakcí, je pouze toto oznámení odesláno, kopie s časem odeslání uložena v databázi a není potřeba spolupráce s jiným pracovištěm banky.

11.5.3 Mlčenlivost

Zaměstnanci mají možnost pouze vytvořit a odeslat hlášení, k odeslanému hlášení nemají možnost se vracet či jej jakkoliv upravovat. O dalším vývoji hlášení nejsou žádným způsobem informováni, není-li k tomu nezbytný důvod. O vývoji hlášení má informace pouze CO.

Žádný další pracovník banky není činnostem CO účasten.

Veškeré dokumenty jsou *uzavřené* v systému pro hlášení a oznámení, nejsou již odesílány emailem a ukládány ve složkách na síťových discích. Přístup k nim je pouze přes systémové rozhraní.

11.5.4 Aktivní hledání podezřelého chování

CO má k dispozici analýzy z výstupu různých bankovních systémů, je-li v nich automaticky detekováno podezřelé chování, je vygenerováno hlášení, které je odesláno CO. Systém má přednastavené modely chování, pomocí kterých se snaží odhalovat podezřelé chování. Analýzy jsou prováděny neustále bez nutnosti aktivní účasti CO.

CO může nadále sledovat a analyzovat výstupy systémů ručně a generovat si sám hlášení.

11.5.5 Detekování politicky exponované osoby

Detekce se provádí ve dvou rovinách – první je při vzniku nového obchodního vztahu je klient dotázán a podle odpovědi je na něj nahlíženo; druhá v průběhu trvání smluvního vztahu je potřeba informaci o ne/zařazení klienta do kategorie politicky exponovaných osob pravidelně aktualizovat.

Automatickou aktualizaci podle přednastavených časových intervalů provádí systém vůči databázi WorldCheck. CO má možnost ručně údaj aktualizovat v případě užití jiného důvěryhodného zdroje.

11.5.6 Detekování potenciálně problémového klienta

Před vznikem nového obchodního vztahu je klient prověřen automaticky vůči databázím s potenciálně nebezpečnými zeměmi původu, zaměstnáními, sankcionovanými subjekty, známými teroristy a dalším black-listům.

Všichni klienti jsou pravidelně automaticky podrobeni zkoumáním ne/příslušnosti k některým z vyjmenovaných skupin. CO má možnost ručně údaj aktualizovat v případě užití jiného důvěryhodného zdroje.

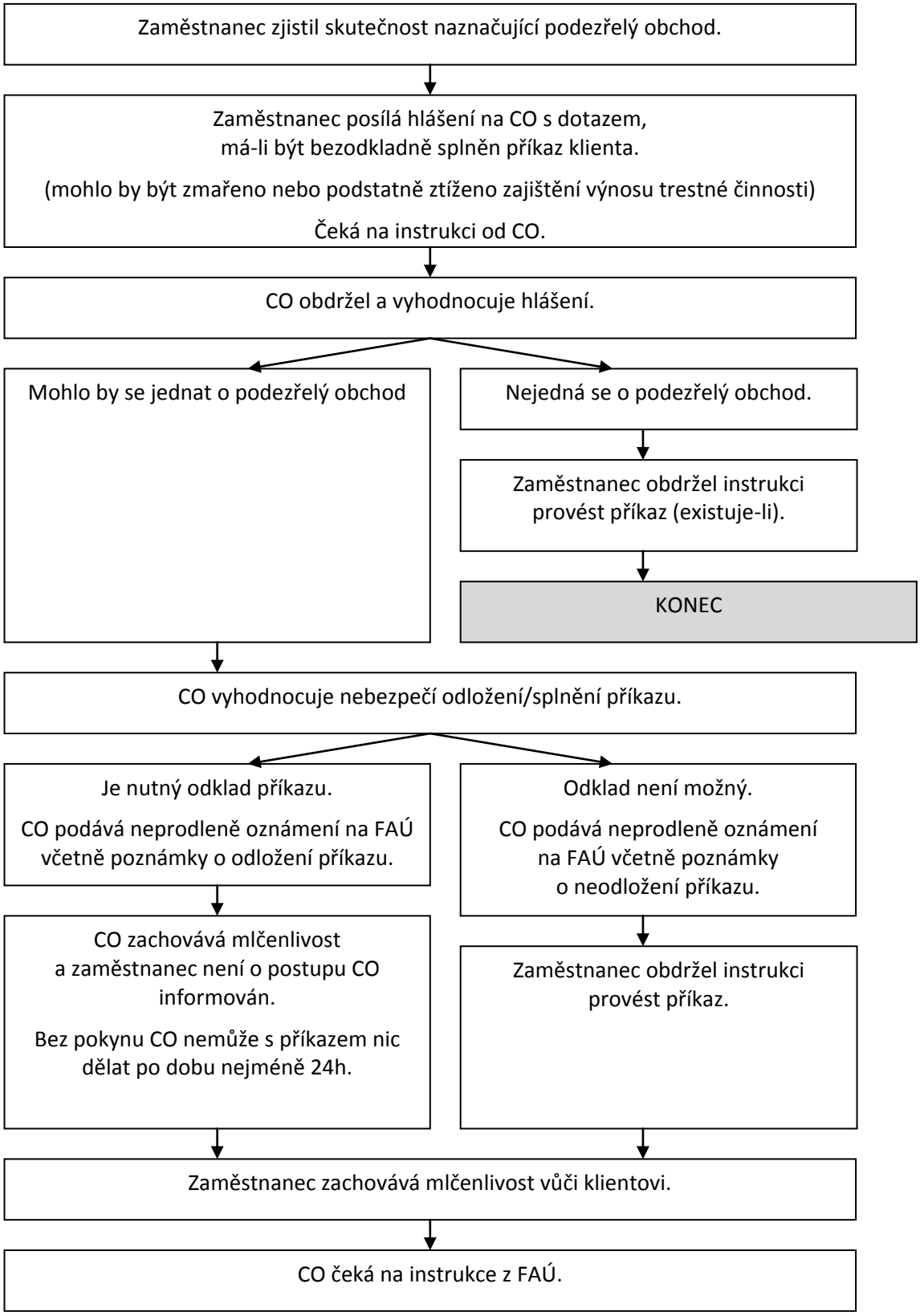
11.5.7 Školení zaměstnanců

Školení zaměstnanců v maximální míře probíhá prostřednictvím intranetového e-learningu. CO má k dispozici seznam, který sleduje jednotlivé zaměstnance a certifikáty z jejich proškolení. Při přiblížení termínu konce platnosti certifikátu systém automaticky upozorní zaměstnance e-mailem a uloží datum a poznámku o odeslaném upozornění ke jménu zaměstnance na seznamu CO.

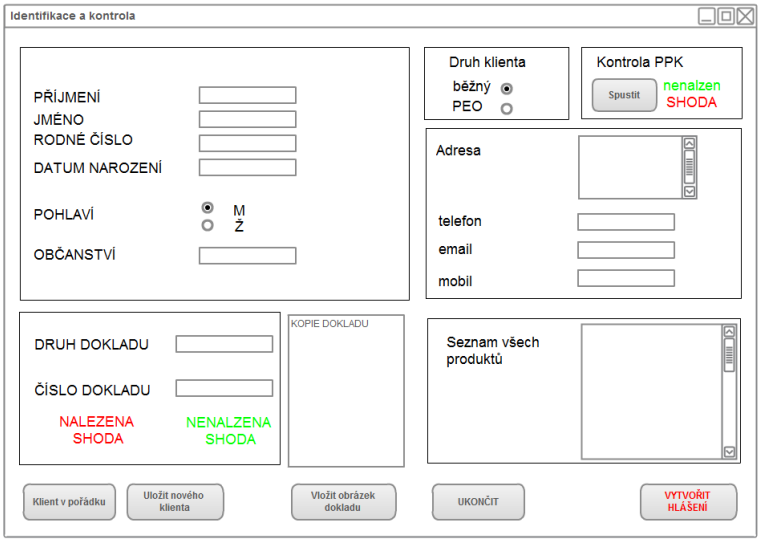
11.5.8 Archivace dokumentů

Hlášení a oznámení jsou systémem centrálně ukládána v databázi. Žádné dokumenty nechodí prostřednictvím nezabezpečených komunikačních kanálů.

11.6 Manuál pro zaměstnance

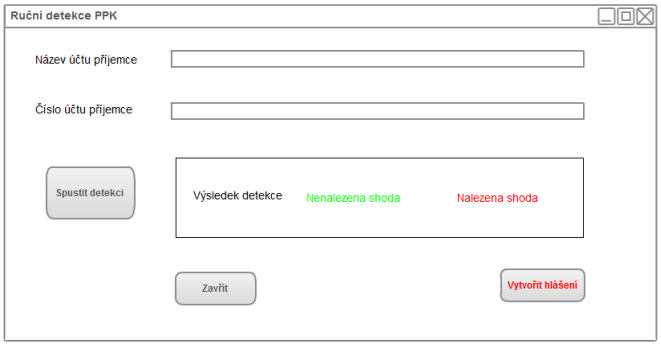


11.7 Návrh okna *Identifikace & kontrola*



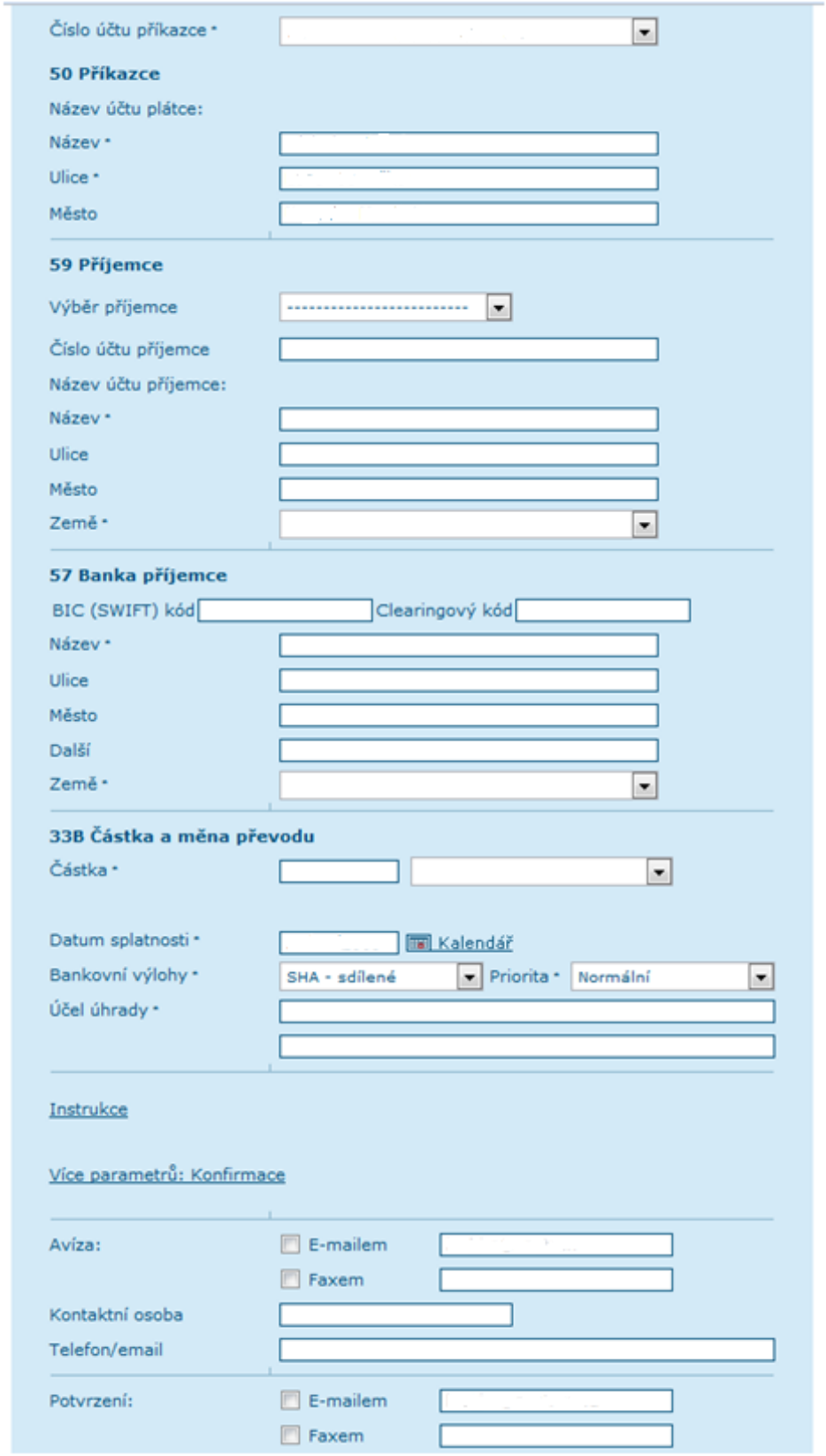
Obrázek 35: Okno identifikace a kontrola

11.8 Návrh okna *Ruční detekce PPK*



Obrázek 36: Okno ruční detekce PPK

11.9 Příkaz přes zahraniční platební styk



Obrázek 37: Příkaz přes zahraniční platební styk (ČS, 2009)