VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

BAKALÁŘSKÁ PRÁCE

2012

MAGDA ČABALOVÁ

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

BAKALÁŘSKÁ PRÁCE

KOMUNIKACE A LIDSKÉ ZDROJE

Vysoká škola ekonomie a managementu

+420 841 133 166 / info@vsem.cz / www.vsem.cz

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

NÁZEV BAKALÁŘSKÉ PRÁCE
Bezpečnost a nakládání s elektronickými dokumenty v podniku

TERMÍN UKONČENÍ STUDIA A OBHAJOBA (MĚSÍC/ROK)
Leden 2012

JMÉNO A PŘÍJMENÍ / STUDIJNÍ SKUPINA
Magda Čabalová

JMÉNO VEDOUCÍHO BAKALÁŘSKÉ PRÁCE
Ing. Miroslav Lorenc

PROHLÁŠENÍ STUDENTA
Prohlašuji tímto, že jsem zadanou bakalářskou práci na uvedené téma vypracovala samostatně a že jsem ke zpracování této bakalářské práce použila pouze literární prameny v práci uvedené. Datum a místo: 28. 11. 2011 Praha _____ podpis studenta

PODĚKOVÁNÍ
Ráda bych tímto poděkovala vedoucímu bakalářské práce za metodické vedení a odborné konzultace, které mi poskytl při zpracování mé bakalářské práce

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

BEZPEČNOST A NAKLÁDÁNÍ S ELEKTRONICKÝMI DOKUMENTY V PODNIKU

Electronic documents maintaince and security in the company

Autor: Magda Čabalová

Souhrn

Tato bakalářská práce popisuje problematiku elektronických dokumentů a jejich zabezpečení při nakládání v podniku. Zdůrazňuje význam dokumentu, který je nositelem důležitých interních i externích informací uchovávaných pro důkazné účely a důležité pro rozhodování v podnikatelské činnosti. Práce je rozdělena do tří hlavních částí, ve kterých se pozornost zaměřuje na bezpečnostní opatření pro ochranu elektronických dokumentů. Úvodní kapitola stručně uvádí do popisované problematiky. Druhá kapitola, věnována teoretické části, charakterizuje dokument a popisuje jeho životní cyklus, zabývá se problémy bezpečnostních rizik elektronického dokumentu a představuje přehled základních přístupů k řešení tohoto problému. Ve třetí kapitole je analyzováno zabezpečení elektronických dokumentů ve velké finanční instituci. Kapitola rozebírá firemní dokumenty a jejich bezpečenost, všímá si především elektronické dokumenty. Poukazuje na význam požadavku zachování důvěrnosti informace a dokumentu, analyzuje nastavená bezpečnostní opatření a porovnává s obecně doporučovanými postupy. Nakonec na příkladu vybraného útvaru popisuje praxi při uchovávání útvarových dokumentů a nastiňuje možné přístupy ke zlepšení jejich zabezpečení.

Summary

The aim of this work is to serve comprehensive description of the electronic documents, their security and management in the company. In addition it puts stress on the documents that hold the important both internal and external information, indispensable for many decisions. The work is divided into the three parts, where I pay attention to the basic protection of the documents. The introduction handles the whole problem; the second part deals with the theory and the document characteristic. It also includes lists of risks and their subsequent solutions. The third part is dedicated to the analysis of the security in a big financial company. In addition it shows us how important it is to maintain confidential information and documents inside the company, analyses safety rules and furthermore, it compares recommended procedures. Finally to illustrate by an example of chosen department established practise to preserve of department of documents, it describes the particular problem and delineates potential solutions of improving their safety.

Klíčová slova:

Elektronický dokument, informace, integrita, důvěryhodnost, dostupnost, bezpečnostní opatření

Keywords:

Electronic document, information, intergrity, trustworthiness, usability, security provision

JEL Classification:

M15 – IT Management

M10 – Business Administration: General

O31 – Innovation and Invention: Processes and Incentives

Obsah

Seznam zkratek

CRAMM –CCTA	Risk Analysis and Management Methodology
DMS	Document management system
ERP	Enterprise resource planning
MoReq	Model Requirements for the management of electronic records
OAIS	Open archival information system
RSA	Rivest Shamir Adleman

Seznam tabulek

Seznam obrázků

1 Úvod

Tématem bakalářské práce je problematika zabezpečení elektronických dokumentů, které jsou v každém podniku nositelem více či méně důležitých informací. Používání dokumentů v elektronické podobě přináší podnikům vyšší efektivitu v řízení dokumentace, ale zároveň požaduje nutnost revidovat dosavadní podnikové procesy. Vůdčím segmentem v rozšíření elektronických dokumentů do běžné praxe se stává veřejný sektor, ve kterém již několik posledních let probíhá projekt elektronizace veřejné správy, tzv.eGovernment. Cílem projektu je elektronizace komunikace mezi úřady a občany, mezi úřady samotnými a elektronizace vnitřní agendy ve veřejné správě[1].

V souvislosti se zaváděním elektronizace dokumentů rostou i nároky na jejich ochranu. V každé organizaci tedy vyvstává otázka: jak chránit a zajistit důvěryhodnost významných elektronických dokumentů v podniku? Protože v sobě tyto dokumenty skrývají cenná aktiva, například informace pro řízení a rozhodování, měl by management firmy věnovat řešení otázky zabezpečení dokumentů mimořádnou pozornost. Zneužití a znehodnocení dokumentů nebo únik informace v nich obsažených by mohlo znamenat nedozírné důsledky pro konkurenceschopnost podniku. Soustavná analýza stávajících pravidel bezpečnosti je proto nevyhnutelná a je základem pro neustálé zlepšování a upevňování systému řízení rizik v oblasti elektronických dokumentů.

Cílem této práce je poskytnout ucelený pohled na problematiku elektronických dokumentů a zajištění jejich bezpečnosti v organizaci. Práce se zabývá potenciálními riziky a nastiňuje doporučené postupy, standardy a pravidla k zachování základních atributů dokumentu, tedy důvěrnosti, celistvosti a dostupnosti v rámci celého životního cyklu. Pro zpracování teoretické části bylo zvoleno studium a obsahová analýza odborné literatury, internetových zdrojů a relevantní legislativy. V praktické části jsou analyzovány hlavní bezpečnostní zásady při nakládání s elektronickými dokumenty v konkrétní organizaci. Předmětem zkoumání jsou opatření pro zajištění bezpečnosti

[1] MVCR.cz [online]. 2010 [cit. 2011-10-30]. Zákon o eGovernmentu.

elektronických dokumentů ve velké finanční instituci, která uchovává své podnikatelské informace v dokumentech v listinné formě, ale také v dokumentech elektronických. Výsledek zkoumání by měl potvrdit níže uvedené pracovní hypotézy:

- Proces řízení přístupů k citlivým dokumentům je efektivnější, když jsou přístupy uživatelů udělované podle pevně stanovených pravidel a standardů.
- K úmyslnému, ale i k neúmyslnému porušení integrity a důvěryhodnosti obsahu dokumentů nedochází při jejich správném zabezpečení v informačním systému.
- Pro snižování rizika ztráty nebo poškození elektronických dokumentů je vhodné zálohování pravidelné v přesně stanovených časových intervalech

V další kapitole jsou analyzovány vybrané interní dokumenty v útvaru Účetní kontrola a inventarizace a jejich zabezpečení. Na základě této analýzy jsou navrhnutá vhodná zlepšení.

2 Teoreticko-metodologická část práce

2.1 Dokument

Obecně lze dokument označit za zdroj a za nositele informací. V odborné literatuře najdeme několik definic pojmu dokument. Podle zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, v § 2, odst. d) je „dokumentem každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální, který vznikl z činnosti původce.“[2]. Standard MoReq (Model Requirements for the management of electronic records) specifikuje, že „dokument je vytvořený nebo přijatý osobou nebo organizací v průběhu činnosti a onou osobou nebo organizací uchovaný“[3]. Podle tohoto standardu klíčovou vlastností dokumentu je, že nemůže být měněn.

2.2 Základní rozdělení dokumentů

Základní rozdělení dokumentů se odvíjí od způsobu (formy) zaznamenání obsahu a od nosiče informací. Forma zaznamenání vymezuje dokument písemný, zvukový, obrazový, audiovizuální. Podle nosiče rozeznáváme dokumenty například přenášené energií, dokumenty listinné nebo dokumenty v elektronické podobě[4].

2.2.1 Listinné dokumenty

V mnohých organizacích, zejména ve firmách s menším počtem zaměstnanců, převládají v podnikové dokumentaci tištěné listiny. Jak již vyplývá z názvu, jedná se o papírové dokumenty, které jsou v podniku vytvořené a vytištěné, nebo do podniku přicházejí v papírové podobě, a které jsou rovněž ručně zpracovány a ukládány ve stejné podobě. Mohou to být přijaté a vystavené faktury, různé smlouvy s obchodními partnery, docházkové listy, účetní výkazy nebo podniková pravidla a směrnice. Manipulace s takovými dokumenty zvyšuje personální, časovou a nakonec i finanční náročnost. Určité řešení představuje konverze z listinné do elektronické podoby.

---

[2] *INKAM.cz* [online]. 2011 [cit. 2011-09-20]. Legislativa.

[3] EC.EUROPA.EU [online]. 2011 [cit. 2011-09-10]. Transparency..

[4] TKAČÍKOVÁ, Daniela. Jak pracovat s informacemi. In Obecné základy s informacemi [online]. 2010. [cit. 2011-09-20].

2.2.2 Elektronické dokumenty

Dokument zaznamenaný digitálním způsobem, zjednodušeně řečeno určitou posloupností nul a jedniček, na jiném než papírovém nosiči označujeme pojmem elektronický dokument. Obsah těchto dokumentů není závislý na materiálním nosiči, ale na technických prostředcích a programových nástrojích nezbytných pro zpřístupnění jejich obsahu[5]. Podle autorů Smejkal a Rais „je elektronický dokument datová zpráva zachycená na nosiči, který zaznamenává informace elektronicky, optoelektronicky nebo jiným obdobným způsobem“[6]. Elektronickou podobu může získat i listinný dokument, který změnil svou papírovou podobu na elektronickou naskenováním originálu, v tomto případě se tedy jedná o faksimile. Při vytvoření faksimile z papírového originálu je důležité vyřešit veškeré pochybnosti vůči pravosti a správnosti obsahu dokumentů. Může to být například připojení časového razítka k dokumentu, použití elektronického podpisu nebo elektronické značky a poté realizovat oběh dokumentů v podniku pouze ve faksimilní podobě[7]. Transformaci papírové podoby dokumentu do elektronické formy lze vymezit pojmem digitalizace dokumentu.

Součástí digitalizace dokumentu je také tvorba tzv. metadat. Jednoduchá definice metadat říká, že metadata jsou data o datech. Zajímavé je pojetí, které charakterizuje metadata jako „data sdružená s objekty, která zbavují jejich potencionální uživatele nutnosti jejich předběžné znalosti existence nebo charakteristik těchto objektů“[8]. V souvislosti s elektronickými dokumenty mají metadata kromě jiných funkcí především funkci popisnou a vyhledávácí . Aby metadata plnila svou úlohu, je nutné je nastavovat určitým způsobem, podle určitých obecných pravidel. Pro nastavení metadat dokumentů textových, obrazových, audiovizuálních i webových existuje mezinárodní norma ISO 15836 : 2003 Information and documentation – The Dublin Core metada

---

[5]TKAČÍKOVÁ, Daniela. Jak pracovat s informacemi. In Obecné základy s informacemi [online]. 2010. [cit. 2011-09-20].

[6]SMEJKAL, Vladimír; RAIS, Karel . Řízení rizik ve firmách a v jiných organizacích, GRADA Publishing a.s. 2006, str.259

[7]SMEJKAL, Vladimír; MATĚJKA, František. System Integration Conference Archive. In Elektronické dokumenty, podpisy, značky a veřejné listiny. : Praktické zkušenosti s převodem účetní dokumentace na digitální podobu[online], 2007 [cit. 2011-09-22].

[8]SKLENÁK , Vilém , et al. *Data, znalosti, informace a Internet*. Praha : C. H. Beck, str.333

element set, jež je výsledkem standardu Dublin Core z roku 1995. Cílem normy je specifikace jednotlivých elementů metadat. Základní sadu tvoří 15 prvků, které se vztahují k obsahu zdroje, k vlastnictví zdroje a ke zdroji jako instanci[9].

Druhým typem je dokument, který byl vytvořen jako datový soubor. Datový soubor lze charakterizovat jako množinu dat uspořádanou určitým způsobem, který vznikl v určitém programu[10]. Patří sem data z podnikových systémů, jakými jsou kupříkladu výstupní sestavy, strukturovaná data z jiných systémů, data doplněná do dokumentu, elektronické zprávy a stažené webové stránky [11].

2.3 Význam dokumentů v podniku

V každé organizaci najdeme řadu dokumentů, jejichž obsah zahrnuje informace různého charakteru. Pro podnik jsou tyto dokumenty tím významnější, čím důležitější informace jsou v nich obsaženy. Jsou důkazem o realizovaných činnostech v podniku a též poskytují informace v rozhodovacích procesech a v nastavení směrování obchodních aktivit. Podle místa vzniku lze rozdělit informace na interní a na externí. Interní informace vznikají přímo v organizaci v rámci její činnosti. Naproti tomu dokumenty obsahující externí informace vstupují do podniku z univerzálního vnějšího prostředí a z prostředí příslušného odvětví, v němž podnik působí[12]. O významu některých skupin podnikové dokumentace vypovídá i skutečnost, že podnik v souladu s platnou legislativou je povinen dodržovat pravidla při nakládání a uchovávání informací vztahující se k podnikatelské činnosti.

Interní informace

Interní informace vznikají přímo v podniku, jsou výsledkem její činnosti a vznikají záměrně nebo na základě legislativních požadavků. Nositeli těchto informací bývají strategické plány a záměry, smlouvy s obchodními partnery, finanční výkazy, výroční zprávy, projekty, došlé a vyšlé faktury, finanční analýzy, mzdové listy, personální záznamy, zápisy z porad nebo vnitřní předpisy.

---

[9] SKLENÁK , Vilém , et al. Data, znalosti, informace a Internet.. Praha : C. H. Beck, str.345

[10] Vydavatelství.vscht.cz [online]. 2011 [cit. 2011-10-30]. Datový soubor

[11] GÁLA, Libor; POUR, Jan; ŠEDIVÁ, Zuzana. Podniková informatika. Praha: GRADA Publishing,str.144

[12] VYMĚTAL, Jan; DIAČIKOVÁ, Anna ; VÁCHOVÁ, Miriam. Informační a znalostní mamagement v praxi. Praha 10 : LexisNexis CZ s.r.o, str.54,58

Externí informace

Z vnějšího prostředí se do podniku dostávají informace o jeho okolí, které mohou výrazně ovlivňovat konkurenceschopnost organizace. Do této kategorie lze zařadit legislativní dokumenty, marketingové analýzy, analýzy finančních trhů či rozhodnutí soudu[13].

2.4 Oběh elektronických dokumentů v podniku

Většina dokumentů bez ohledu na místo jejich vzniku vstupuje v průběhu své životnosti do určitých fází. Rozlišujeme čtyři základní etapy životního cyklu dokumentů, a to:

- pořízení dokumentů
- jejich zařazení do systému
- zpracování dokumentů
- archivace dokumentů[14]

Oběhem dokumentů určených původců[15] se zabývá Vyhláška č. 191/2009 o podrobnostech spisové služby, která popisuje podrobnosti a požadavky dílčích etap procesu nakládání s dokumentem. Součástí procesu spisové služby je příjem dokumentů a jejich evidence, rozdělování a oběh, vyřizování, vyhotovení, podepisování, odesílání a ukládání.

Pořízení dokumentů

Životní cyklus dokumentu začíná jeho vytvořením přímo v podniku nebo přijetím z vnějšího okolí podniku. Podoba dokumentu může být papírová, ale v současné době se často pořizují dokumenty v elektronické formě (příkladem mohou být elektronické faktury a datové zprávy zasílané prostřednictvím datových schránek) nebo jsou do této formy konvertovány v procesu digitalizace dokumentu, která spočívá v naskenování papírového originálu. Výsledkem je digitalizovaný dokument.

K podstatné změně vnímání elektronických dokumentů a k jejich rozšiřování do každodenní praxe přispěl Zákon č. 300/2008 Sb., o elektronických úkonech a

[13] VYMĚTAL, Jan; DIAČIKOVÁ, Anna ; VÁCHOVÁ, Miriam. Informační a znalostní mamagement v praxi. Praha 10: LexisNexis CZ s.r.o, str.58

[14] GÁLA, Libor; POUR, Jan; ŠEDIVÁ, Zuzana. Podniková informatika. Praha: GRADA Publishing,str.143

[15] INKAM.cz [online]. 2011 [cit. 2011-09-20]. Legislativa.

autorizované konverzi dokumentů a následně jeho doplnění vyhláškou č. 194/2009 Sb., o stanovení podrobnosti užívání a provozování informačních systémů a datových schránek. Podle tohoto zákona je datová schránka elektronické úložiště a je určena k doručování a k odesílání elektronických dokumentů. Takovou datovou schránku musí povinně podle platné legislativy vytvořit a využívat právnické osoby zřízené zákonem, například příspěvkové organizace, dále právnické osoby zapsané v obchodním rejstříku a orgány veřejné moci.

Zařazení dokumentu do informačního systému

Elektronický nebo digitalizovaný dokument má vlastnosti, které ho umožňují zařadit do určitého systému správy dokumentů a zefektivnit tím nakládání s dokumenty v podniku. Současné systémy pro správu dokumentů (DMS) nabízejí řadu možností, jak dokument opatřit metadaty, jednoznačnou identifikací, a zajistit jeho snadné vyhledávání, přeposílání či zpřístupňování pouze oprávněným uživatelům. Systémy automaticky doplní další informace o vkládaném dokumentu, jakými jsou jeho velikost a formát, datum vložení nebo profil uživatele, který dokument pořídil.

Zpracování dokumentu

Zařazením dokumentu do systému práce s dokumentem nekončí. Většina z nich je předmětem dalšího zpracovávání. Například vydaný firemní předpis je předložen vnitropodnikovým intranetem zaměstnancům a je od nich vyžadováno prostudování a potvrzení, že se řádně seznámili s novým předpisem. Dalším příkladem je přijatá naskenovaná a do systému vložená faktura, kterou předává účetní odpovědnému pracovníkovi k věcné kontrole a ke schválení úhrady částky. V rámci elektronického oběhu dokumentu, tzv. workflow, systém na základě předem nadefinovaných procesů a postupů automaticky zařídí, aby dokument dostal oprávněný uživatel[16]. O každé fázi oběhu je vytvořen protokol s informacemi o době zpracovávání, o provedených změnách a také o odeslání dokumentu dalšímu uživateli.

[16] KUNSTOVÁ, Renáta. Efektivní správa dokumentů. Praha 7 : GRADA Publishing a.s., 2009, str.80

Archivace

Po ukončení aktivní práce s dokumentem musí podnik některé z nich nadále uchovávat, a to zejména takové, které obsahují důležité informace. Podle požadavků platné legislativy je nutné archivovat vybrané dokumenty několik let, v případě mzdových listů pro účely důchodového pojištění až třicet let. Archivovat dokumenty lze i v elektronické podobě, je však důležité, aby byla informace v archivovaných dokumentech i o po letech dostupná, čitelná a dostatečně prokazatelná. Problém s uložením elektronických dokumentů se nezdá být složitým, otázkou však zůstává, zda bude po letech uložení dostupný a čitelný jejich obsah. Poměrně krátkodobá existence elektronických dokumentů nám zatím nedokáže uspokojivě odpovědět na otázku, zda se v budoucnosti nevyskytnou problémy při zobrazování validity dokumentu.

2.5 Identifikace bezpečnostních rizik elektronického dokumentu

Rozšíření a využívání elektronických dokumentů přináší organizacím a podnikům vyšší efektivitu v řízení dokumentů. Jejich efekty lze spatřovat ve zrychlení podnikových procesů, ve zkvalitnění vnitřní i vnější komunikace, v personálních a ve finančních úsporách. Na druhou stranu je však nutné si uvědomit, že to, co platí u listinných dokumentů z hlediska zabezpečení, platí u elektronických dokumentů dvojnásobně. Nastavení bezpečnostních opatření musí předcházet důkladná identifikace hrozeb, slabých míst a negativních dopadů možných incidentů vztahujících se k dokumentům. Vznik a existence dokumentu podmiňuje obvykle existence určité informace, která je v obsahu dokumentu vyjádřena. Když tedy chceme zjišťovat a identifikovat bezpečnostní rizika dokumentů, musíme se především zaměřit na analýzu bezpečnostních rizik informací v dokumentech obsažených. V souvislosti s analýzou rizika informace jsou níže vysvětlené pojmy hrozba, zranitelné místo, riziko a identifikace a ocenění informace.

Hrozba

Pravděpodobnost úniku informace, její poškození, ztráty nebo modifikace označujeme jako hrozbu, která využívá zranitelnost informace. Hrozby mohou pocházet od člověka nebo vzniknout přírodními silami nezávisle na vůli lidí. V případě hrozeb způsobených lidským faktorem lze hrozby rozdělit na úmyslné a neúmyslné.

Zranitelná místa

Hrozba se může naplnit, existuje-li určité slabé místo. Zranitelnost či slabina vystavují informace hrozbám a tak zvyšují její možná rizika[17].

Riziko

„Riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucím ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní“[18].

Identifikace a ocenění informací

Informace jsou v organizacích považovány za velmi cenná aktiva. Na rozdíl od jiných aktiv (hmotný majetek, cenné papíry, zásoby) není úplně jednoduché vést evidenci všech podnikových informací. Někteří odborníci na tuto problematiku doporučují rozdělit informace do informačních jednotek, které mají vztah ke konkrétní agendě. Například strategický plán, marketingová strategie, bezpečnostní dokumentace představují důvěrnou informační jednotku důležitou pro řízení společnosti. Ještě složitější úkol představuje ocenění informace. Metodologie CRAMM – CCTA Risk Analysis and Management Methodology doporučuje přistupovat k hodnocení informace z hlediska důvěrnosti, integrity a dostupnosti. Hodnota informace je podle tohoto přístupu odvozena od možného negativního dopadu pro společnost, který se může projevit ve formě finančních ztrát, poškození dobrého jména společnosti, porušení právních předpisů a předpisů a z toho plynoucích následků, vyzrazení osobních údajů osob, narušení veřejného pořádku únikem citlivých informací majících schopnost vyvolat protestní akce, ohrožení bezpečnosti zaměstnanců a osob společnosti[19]. Uveďme příklad úniku obsahu dokumentu výroční zprávy o hospodaření veřejně obchodovatelné společnosti. Finanční výsledky hospodaření jsou v tomto případě až do oficiálního zveřejnění důvěrnými interními informacemi, jejichž předčasné vyzrazení může způsobit společnosti určité finanční ztráty a poškození důvěryhodnosti.

---

[17] ŠEBESTA, Václav , et al. Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005. Praha : Český normalizační institut, 2006, str.58

[18] SMEJKAL, Vladimír; RAIS, Karel. Řízení rizik ve firmách a v jiných organizacích, GRADA Publishing a.s. 2006, str. 83

[19] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Brno: COMPUTER Press, a.s., 2006., str.21-22

2.5.1 Klasifikace informací

Stanovením klasifikačních stupňů informací se vytváří klasifikační model, který poskytuje určitý návod, jak zacházet s informacemi vyskytujícími se v podniku v různých podobách. Klasifikace se dotýká důvěrnosti, dostupnosti a integrity, přičemž prioritou tohoto modelu zůstává důvěrnost informace.

Důvěrnost informace

Z hlediska důvěrnosti se doporučuje stanovit tři až čtyři stupně, které informace klasifikují jako informace **veřejné, interní, důvěrné**, popřípadě **přísně důvěrné**. **Veřejné informace** obsahují dokumenty určené veřejnosti i zaměstnancům, přístup k nim tudíž není omezen. Mohou to být výroční zprávy, informační dokumenty o společnosti, nabídky služeb a výrobků. **Interní informace** se nacházejí v dokumentech, které vznikly přímo ve společnosti. Jsou určeny především pro zaměstnance, ale případné zpřístupnění těchto dokumentů externímu okolí by nepoškodilo společnost nebo její zaměstnance. Do této skupiny lze zařadit například základní obecné předpisy a nařízení. Auditní zprávy, havarijní plány, mzdové listy jsou dokumenty **s důvěrnými informacemi** o organizaci. Přístupné jsou pouze zaměstnancům, kteří informace obsažené v důvěrných dokumentech využívají pro svou práci. Malé procento dokumentů společnosti tvoří **přísně důvěrné dokumenty**, jejichž obsah je přístupný pouze omezenému počtu zaměstnanců, obvykle uvedených v seznamu osob s tímto oprávněním[20].

Integrita informací

Neporušenost, prokazatelnost a celistvost vytváří integritu informací. Podle tohoto hlediska je možné informace rozdělit na informace autentické, cenné a ostatní informace. Autentická informace vyžaduje zachování neporušenosti obsahu, celistvosti a prokazatelnosti. Cenné informace jsou informace důležité pro rozhodování nebo jsou též nositelem určitých hodnot[21].

[20] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Brno : COMPUTER Press, a.s., 2006., str.52

[21] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Brno : COMPUTER Press, a.s., 2006., str.54

Dostupnost informací

U některých informací je nezbytné zajistit, aby byly k dispozici v danou chvíli. Podle dostupnosti lze informace členit na kritické, například informace z finančních trhů při obchodování s finančními nástroji, dále na prioritní, kam patří klientské nebo mzdové informace, a nakonec na informace potřebné[22].

2.5.2 Bezpečnostní hrozby elektronického dokumentů

Klasifikace informací je východiskem pro nahlížení na dokumenty v podniku. Při analýze dokumentů elektronických či listinných je nutné zkoumat ohrožení důvěrnosti, neporušenosti a dostupnosti dokumentu. Při hledání možných hrozeb a slabých míst se musí rozlišovat forma dokumentu, která předurčuje přístup k implementaci vhodných bezpečnostních opatření. O jakých potencionálních hrozbách pro elektronické dokumenty lze tedy uvažovat? Vzhledem k formátu, způsobu a místa uložení těchto dokumentů nejčastěji hrozí:

- poškození dat
- modifikace obsahu
- úmyslné smazání dat
- neúmyslné smazání dat
- neoprávněný přístup k dokumentu
- nedostupnost dokumentu

Každá z těchto hrozeb znamená nebezpečí v jiném životním cyklu dokumentu. Například poškození, smazání nebo zneužití obsažených informací hrozí zejména při manipulaci s dokumentem, nedostupnost či ztráta dokumentu při dlouhodobém uchovávání[23].

2.6 Bezpečnostní opatření k zajištění rizik elektronických dokumentů

Výsledkem identifikace hrozeb, hledání zranitelných míst a stanovení míry rizika je implementace bezpečnostních opatření, tedy vhodné politiky, postupů, metod a programů, které sníží existující rizika na minimální míru nebo je také někdy úplně eliminuje. Pro zabezpečení požadovaných vlastností elektronických dokumentů

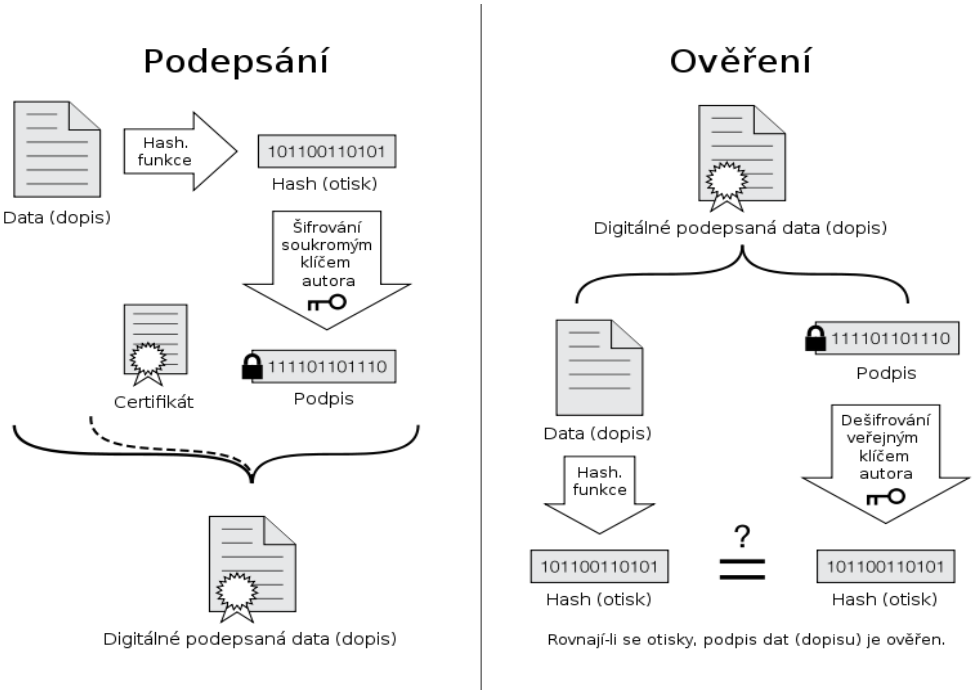
[22] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Brno : COMPUTER Press, a.s., 2006., str.55

[23] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Brno : COMPUTER Press, a.s., 2006., str.61

v průběhu celého životního cyklu, a to především autenticity a integrity, existuje řada doporučení a standardů. V komunikaci s úřady veřejné správy je základním nástrojem ověření autenticity zaručený elektronický podpis, elektronická značka a kvalifikované časové razítko. Bezpečnostní aspekty jsou také důležitou součástí systémů správy dokumentů, systémů pro spisovou službu a dlouhodobou archivaci elektronických dokumentů[24].

Elektronický podpis

Obrázek 1 Podepsání a ověření elektronického podpisu



Zdroj: wikipedia.org

Obdobou podpisu na listině je na elektronickém dokumentu elektronický podpis. Užití a vlastnosti elektronického podpisu stanovuje Zákon č.227/2002 Sb., o elektronickém podpisu a o změně některých zákonů. Při elektronické komunikaci s orgány veřejné správy lze využívat pouze tzv. zaručené elektronické podpisy.

Elektronický, tedy v technickém pojetí digitální podpis, je založen na šifrovací metodě RSA. Metoda RSA je šifrový systém založený na principu asymetrického šifrování. Zjednodušeně lze vysvětlit asymetrické šifrování jako algoritmus užívající pár klíčů,

[24] GOGELA, Robert . Důvěryhodný elektronický dokument. SystemOnline.cz dokument [online]. 2010, 3

jeden veřejný, druhý soukromý. Princip vytváření digitálního podpisu spočívá v tom, že se na podepisovaný text aplikuje hašovací funkce. Pomocí hašovací funkce se datům libovolné délky přiřadí hodnota pevné délky, vznikne otisk textu, tzv. haš. Vytvořený otisk odesílatel zašifruje svým soukromým klíčem. Tím je elektronický dokument podepsán digitálním podpisem. Součástí odeslaného zašifrovaného otisku je otevřený nezašifrovaný text. Při přijetí tohoto dokumentu příjemce pomocí hašovací funkce vypočte otisk otevřeného textu a zároveň odšifruje zašifrovaný text veřejným klíčem odesílatele, který dokument digitálně podepsal. Pokud je doručený otisk shodný s vypočteným otiskem, jedná se o autentický dokument. Pravost a platnost veřejných klíčů garantuje nezávislá autorita, která vydává potvrzení o pravosti veřejného klíče k danému subjektu, tzv. certifikáty[25]. Problematikou tvorby a fungování elektronického podpisu se zabývá kniha Jiřího Peterky „Báječný svět elektronického podpisu“, kterou lze doporučit všem, kteří chtějí lépe porozumět a využívat elektronický podpis.

Elektronická značka

Pro právnické osoby a organizační složky je určena elektronická značka. Po technické stránce je podobná elektronickému podpisu. Zákon č. 427/2000 o elektronickém podpisu, ve znění pozdějších předpisu § 2 odstavec c) říká, že „elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu
- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod kontrolou
- jsou k datové zprávě, ke které se vztahují, propojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat“.[26]

Dokumenty s elektronickou značkou jsou právoplatné dokumenty a lze je využívat v rámci elektronického oběhu dokumentů[27].

[25] MLÝNEK, Jaroslav. Zabezpečení obchodních informacíP. Brno : COMPUTER Press, a.s., 2006., str.94-95

[26] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů . In Sbírka zákonů, Česká republika. 2000

[27] KUNSTOVÁ, Renáta. Efektivní správa dokumentů. Praha 7 : GRADA Publishing a.s., 2009, str.116

Časové razítko

Spolu s elektronickým podpisem se používá časové razítko, které deklaruje, že elektronický podpis na dokumentu existoval v okamžiku, který je uveden na časovém razítku. Časová razítka poskytují autority časových razítek (Time Stamping Authority), jejichž činnost je řízena podle platné legislativy[28].

Certifikační autorita

Pravost a platnost veřejného klíče dokládá certifikát vydaným poskytovatelem certifikačních služeb, tedy certifikační autoritou. Především v oblasti veřejné správy, kde je nutné zajistit vysokou bezpečnost prostřednictvím zaručených elektronických podpisů, poskytují tyto služby společnosti, kterým Ministerstvo vnitra udělilo k této činnosti akreditaci. Akreditovaným poskytovatelem certifikačních služeb je v České republice První certifikační autorita, Česká pošta nebo společnost Eldentity a.s. Uznávané certifikační autority vydávají certifikáty splňující podmínky a požadavky standardu X. 509, který vydal Mezinárodní telekomunikační unií. Standard mimo jiné obsahuje i údaj o platnosti certifikátu[29]. Oproti tomu pro vnitrofiremní komunikaci postačí certifikát, který vydala certifikační autorita samotné firmy. Nejčastěji mají vlastní certifikační autority banky, které zajišťují certifikáty veřejných klíčů svým zaměstnancům a klientům banky.

2.7 Bezpečnostní opatření při oběhu elektronických dokumentů.

Neustále se zvyšující množství elektronických dokumentů a záznamů v podniku by nebylo možné efektivně řídit bez vhodných informačních systémů. Součástí informačních systémů pro správu elektronických dokumentů jsou sofistikované nástroje, které poskytují systémovou ochranu dokumentů. Zajišťují identitu dokumentů, řešení přístupových oprávnění k jednotlivým dokumentům, zaručují jeho autenticitu ve smyslu, že se jedná o pravý dokument, umožňují důvěryhodné uložení a bezpečné zlikvidování. Požadavky na informační systémy z hlediska kontroly a bezpečnosti elektronických dokumentů řeší například standard MoReq2, ze kterého vychází i národní standard pro elektronickou spisovou službu. Standard detailně specifikuje

[28] PETERKA, Jiří. Báječný svět elektronického podpisu [online]. Praha : CZ.NIC, 2011, str.55

[29] PETERKA, Jiří. Báječný svět elektronického podpisu [online]. Praha : CZ.NIC, 2011, str.17-26

možnosti nastavení bezpečnostních pravidel v systémech pro správu záznamů v elektronické podobě v souladu s platnou legislativou a zásadami organizace[30].

Řízení přístupů k dokumentům

K zachování důvěrnosti citlivých informací je nutné kontrolovat a řídit přístupy uživatelů k dokumentům organizace. Podle nastavení profilu a přiřazení oprávnění k tomuto profilu lze uživateli omezit přístup k vybraným souborům a dokumentům, znemožnit některé činnosti ve vztahu k dokumentům nebo odepřít přístup ke konkrétnímu datu. Nastavení přístupů a oprávnění by se nemělo vázat pouze na konkrétního uživatele, ale také na skupinu uživatelů konkrétního oddělení, popřípadě skupinu s různou úrovní přístupu. Při vyhledávání dokumentu, ke kterému nemá uživatel povolen přístup, může systém nabídnout podle úrovně bezpečnosti pouze částečné nebo žádné informace o existujícím záznamu[31].

Zajištění dostupnosti dokumentů

V důsledku technické závady informačního systému, poškození dokumentu nebo vymazání ze systému je nutné zajistit jeho rychlou obnovu. Podle standardu MoReq2 je proto důležité věnovat pozornost pravidelnému zálohování všech či vybraných věcných skupin, dokumentů a souborů, a rovněž administrativních vlastností úložiště informačního systému. Zálohování by mělo vycházet z automatických postupů, které mají přesně nastavenou frekvenci zálohování, skupinu zálohovaných dokumentů a místo pro tuto zálohu.

Zaručení autenticity podle standardu MoReq2

Autenticita a pravost jsou vlastností elektronických dokumentů. Pro dokazování pravosti a autenticity dokumentů lze využít již výše zmíněný elektronický podpis, elektronickou značku nebo časové razítko. Standard MoReq2 dále doporučuje systémové funkce, které dokážou odhalit přijetí dokumentů bez platného elektronického podpisu nebo jiných kontrolních nástrojů. Dále je nezbytné, aby systém znemožnil jakoukoliv modifikaci obsahu elektronického dokumentu.

[30] EC.EUROPA.EU [online]. 2011 [cit. 2011-09-10]. Transparency.

[31] EC.EUROPA.EU [online]. 2011 [cit. 2011-09-10]. Transparency.

Uchovávání elektronických dokumentů

Rozšíření elektronických dokumentů znamená vyřešit rovněž problémy jejich archivace. Současná platná legislativa nařizuje podnikům uchovávat některé dokumenty v delším časovém horizontu. Dlouhodobě lze uchovávat také dokumenty v elektronické podobě, je však nutné zajistit, aby byly čitelné a aby bylo možno garantovat jejich původ a neměnnost i po letech uložení. Podle Ladislava Cubra, autora studie k problémům dlouhodobé archivace elektronických dokumentů, můžeme rizika plynoucí z dlouhodobého uchovávání rozdělit na rizika:

- technologická, plynoucí z degradace nosičů a zastarávání hardwaru
- informační, plynoucí z ohrožení datových formátů
- systémová, plynoucí z nezvládnutí optimální správy enormního množství digitálních objektů, jejich přesné identifikace a také zajištění práva k jejich využívání
- institucionální, plynoucí z ukládání dokumentů do nevyhovujících digitálních archivů a z nedostatečného finančního a organizačního zajištění provozu[32].

V současnosti se doporučuje několik přístupů k dlouhodobému a bezpečnému archivování elektronických dokumentů. Jako příklad uveďme emulaci. Emulace je technologie, která umožňuje naprogramovat současnou počítačovou platformu na původní prostředí, ve kterém byl dokument vytvořen. Metodu emulace a její zásady charakterizoval ve své práci Jeff Rothenberg pro americkou nadvládní organizaci The Council on Library and Information Resources[33]. Vytvořením emulované aplikace je možné přistupovat z aktuálního operačního prostředí ke starším aplikacím v původním vzhledu a s původními funkcionalitami.

Dalším doporučovaným přístupem je migrace, která je založena na transformaci staršího formátu dokumentu do novějšího formátu[34]. Účelem migrace je zkonvertovat dokument do nové podoby, aby ho bylo možné zpřístupnit, zobrazit nebo případně i editovat aktuálním softwarem a na aktuálním hardwaru.

---

[32] BRATKOVÁ, Eva . Kvalitní studie k problémům dlouhodobé archivace digitálních dokumentů. Ikaros [online]. 2011, 15, 4

[33] ROTHENBERG, Jeff. A Report to the Council on Library and Information Resources. In Finding a Viable Technical Foundation for Digital Preservation [online]. Washington : 1999

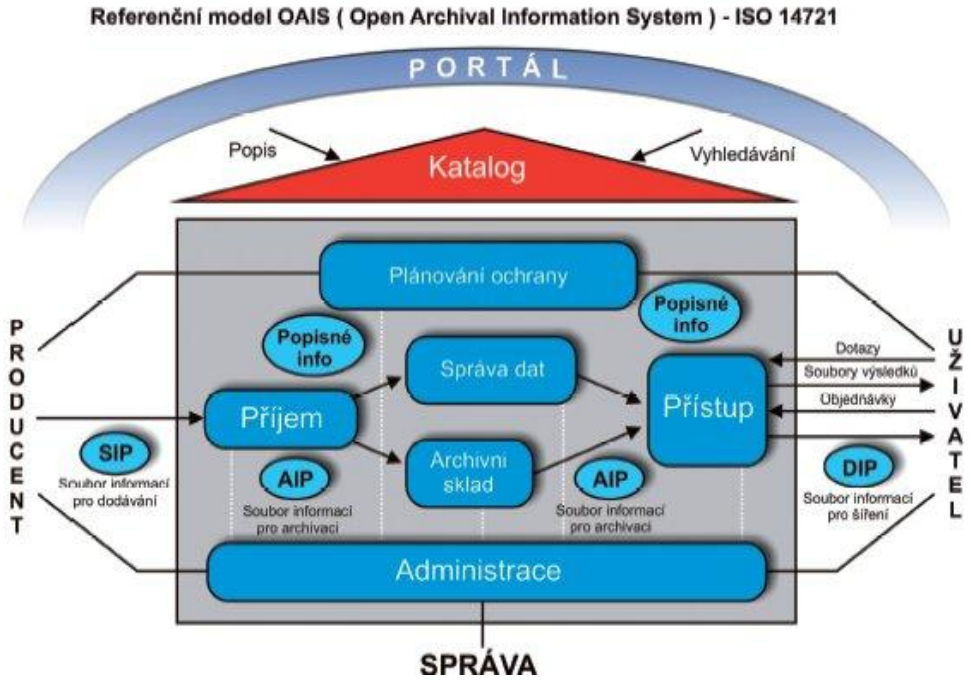
[34] LIDINSKÝ, Vít; ŠVARCOVÁ, Ivana. Securityworld.cz [online]. 2007 Dlouhodobé uchovávání elektronicky podepsaných elektronických dokumentů.

Otázkám bezpečného dlouhodobého uchovávání elektronického dokumentu se věnuje standard ISO 14721:2003 Space data and information transfer systems – Open archival information system – reference model. Jeho základem je referenční model Open Archival Information System, který popisuje základní principy tvorby digitálního archivu. Model OAIS popisuje proces od přípravy, uložení až po opětovné zobrazení archivovaného dokumentu:

- SIP (Submission Information Package) – informační balíček doručený do archivu
- AIP (Archival Information Package) – balíček dat v požadovaném archivním formátu
- DIP (Dissemination Information Package) – informační balíček pro uživatele jako odpověď na dotaz do archivu[35].

Následující obrázek popisuje základní koncept a vazeb podle modelu OAIS:

Obrázek 2 Referenční model OAIS



Zdroj: STOKLÁSKOVÁ, Bohdana . *Knihovna.nkp.cz* Perspektivy důvěryhodného digitálního úložiště v rámci Národní digitální knihovny

[35] KUNSTOVÁ, Renáta. Efektivní správa dokumentů GRADA Publishing a.s., 2009, str.130

3 Praktická část

Následující kapitola je věnována analytické části, která přináší pohled na řízení bezpečnosti elektronických dokumentů v konkrétní organizaci. Analýza bezpečnostních zásad vztahujících se k dokumentům je podkladem pro komparaci s obecně doporučovanými opatřeními. Praktická část zpracovává tuto problematiku ve finanční společnosti, která patří mezi největší svého druhu v České republice. Úspěšná a na trhu již několik desítek let působící bankovní instituce vytváří a pracuje s dokumenty různého charakteru. Dynamicky se rozvíjí elektronická komunikace mezi bankou a klientem, mezi bankou a jejím okolím a rovněž v rámci interní komunikace. Důsledkem je nepřetržitý tok nových elektronických dokumentů, které musí banka efektivně řídit a bezpečně chránit. Pro zjištění stavu elektronických dokumentů v bance a pro nastavení bezpečnostních procesů a kontrolních mechanismů nad dokumenty bylo zvoleno několik metod. Stěžejní metodou se stalo dotazování klíčových pracovníků odpovědných za řízení bezpečnostních rizik informací a dokumentů. Dalším zdrojem pro získání potřebných informací byly interní směrnice, pravidla a standardy a nakonec čerpala autorka práce, jakožto dlouholetý zaměstnance společnosti, i z vlastních zkušeností. Na základě získaných poznatků z rozhovorů a z firemních materiálů vznikl přehled platných bezpečnostních opatření, který je podkladem pro porovnání s obecně doporučenou bezpečnostní politikou v této oblasti. Druhá část se věnuje interním dokumentům v útvaru Účetní kontrola. Zde je pozornost zaměřena na důležité útvarové elektronické dokumenty a na jejich zabezpečení při uchovávání. Výsledkem analýzy je návrh pro zlepšení bezpečnějšího ukládání útvarových elektronických dokumentů.

3.1 Profil společnosti

Firma, kterou bakalářská práce zpracovává, je jednou z největších finančních institucí v tuzemsku. Vznikla ještě v šedesátých létech minulého století jako státní banka za účelem poskytování služeb v oblasti financování zahraničního obchodu. V současnosti je univerzální bankou nabízející služby všem klientským segmentům. Její majoritním vlastníkem je již několik let zahraniční banka, která sama je zároveň součástí velké finanční skupiny. Široké spektrum bankovních a finančních služeb zajišťuje téměř osm

tisíc zaměstnanců. Poskytování služeb probíhá prostřednictvím rozsáhlé pobočkové sítě rozmístěné po celé České republice.

Mezi hlavní předměty podnikatelské aktivity banky patří:

- přijímání vkladů od veřejnosti
- poskytování úvěrů fyzickým osobám, malým a středním podnikům, korporátní a institucionální klientele
- investování do cenných papírů na vlastní účet
- poskytování investičních služeb
- finanční pronájem (finanční leasing)
- platební styk a zúčtování
- vydávání a správa platebních prostředků
- poskytování záruk
- otevírání akreditivů
- směnárenská činnost
- poskytování bankovních informací

3.1.1 Dokumenty banky a jejich rozdělení

K plnění pracovních úkolů využívají zaměstnanci interní a externí informace, jež jsou obsaženy v nespočetném množství souborů, záznamů a dokumentů. Zároveň jsou záznamy a dokumenty výsledkem činností pracovního procesu. Některé dokumenty mají papírovou podobu, avšak již několik let jsou běžnou praxí elektronické dokumenty. Díky jejich rozšíření se zautomatizovaly a zefektivnily mnohé vnitrobankovní procesy.

Při širším pojetí definice elektronického dokumentu patří mezi elektronické dokumenty nejen digitalizované listinné dokumenty nebo elektronické dokumenty vytvořené kancelářskými aplikacemi, ale i výstupy z transakčních, manažerských a účetních systémů. Můžeme proto říct, že v bance existují skupiny různorodých elektronických dokumentů, které se vyskytují v každé kategorii písemností.

Podle platného standardu společnosti jsou všechny dokumenty bez ohledu na formu rozděleny do následujících kategorií:

- Kategorie projektové dokumentace, která vznikla k finálním projektům. Projektová dokumentace je obvykle vytvořena v papírové podobě. Pouze malá část má výhradně elektronickou formu.

- Kategorie dokumentů pro podporu uživatele zahrnuje uživatelské manuály, popisy pracovních procesů a popisy informačních systémů. V této kategorii převládají elektronické dokumenty nad dokumentací papírovou.
- Kategorie smluv obsahuje rámcové smlouvy s klienty na bankovní produkty, dodavatelské smlouvy, nájemné smlouvy, smlouvy o poskytování investičního poradenství a na služby při správě majetku. Originály dokumentů této skupiny mají papírovou podobu, některé z nich jsou převedeny naskenováním do digitální formy a evidované v systému správy dokumentů.
- Kategorie periodických zpráv je souborem dokumentů, jakým jsou například výroční zprávy, pravidelné finanční výkazy, finanční plány, zprávy o koordinaci vnitřní bezpečnosti. Vyskytují se v papírové i v elektronické formě.
- Kategorie zápisů ze strukturovaných porad vytvořené převážně v elektronické formě.
- Kategorie účetních dokumentů zastoupena došlými a vyšlými fakturami, účetními doklady. Jejich forma je elektronická i papírová, která je převedena do digitalizované formy. V případě došlých faktur se prosazuje elektronická fakturace.
- Kategorie právních listin zahrnuje stavební smlouvy, smlouvy o prodeji a nákupu majetku, plné moci, dokumenty o požární ochraně. Tyto dokumenty jsou převážně v papírové podobě. Některé jsou evidované v informačním systému v digitální podobě.
- Kategorie dokumentů z různých posudků, zprávy požární inspekce a geodetické posudky. Obvykle jsou originály v papírové podobě, případně bývají převedeny do digitalizované formy.
- Kategorie administrativních a ostatních dokumentů je skupinou různorodějších dokumentů, kam patří dokumenty obsahující informace o produktu, hodnocení dodavatelů, sledování trhu, personální informace, plánovací seznamy. Existují v papírové i v elektronické podobě.

Jak je z uvedeného přehledu patrné, téměř v každé skupině jsou zastoupeny elektronické dokumenty. Všechny poskytují informace nebo důkazy, proto je nutné dbát na jejich ochranu a na to, aby byla zajištěna jejich dostupnost, celistvost a důvěrnost. Ke splnění těchto požadavků přistupuje firma systematicky. Pravidelně vytváří, přehodnocuje a

aktualizuje pravidla bezpečnosti při nakládání s dokumenty. U papírových dokumentů existují postupy na ochranu prověřené v čase, u elektronických dokumentů je však situace poněkud jiná. Přestože elektronické dokumenty nabízejí řadu výhod v podobě efektivnějšího řízení, mají i své určité nevýhody. Jednou z nich je snadný únik citlivých informací nebo jejich nedostupnost v případě nedostatečného zabezpečení dokumentu.

3.1.2 Analýza opatření k zabezpečení elektronických dokumentů

Správa veškeré elektronické dokumentace vychází ze základních pravidel a standardů politiky informační bezpečnosti. Ochrana dokumentů se promítá ve dvou základních rovinách, a to v rovině procesní a v rovině systémové. **Procesní stránka** představuje implementaci nařízení a směrnic, jež vymezují bezpečné nakládání s dokumenty. Zahrnuje rovněž osvětu a školení zaměstnanců jak používat a chránit elektronické dokumenty a informace v nich obsažené před zneužitím nebo ztrátou. **Systémová ochrana**, jak sám název napovídá, znamená využití informačních systémů a jejich nástrojů pro ochranu samotného dokumentu. Nejen pro efektivní řízení dokumentů a jejich ukládání, ale i pro vhodné zabezpečení využívá banka informační systém pro správu dokumentů, který je integrován do celopodnikového ERP systému. Pro centrálně řízenou spisovou službu implementovala aplikaci spisových služeb a podle platné legislativy má zřízenou datovou schránku pro vyřizování komunikace s orgány veřejné moci.

Zachování důvěrnosti a integrity dokumentů

Bez ohledu na formu klasifikuje společnost své dokumenty podle důvěrnosti a důležitosti informačního obsahu, podle kterého se určují bezpečnostní opatření pro dokument. Dokumenty se v závislosti na klasifikačním stupni obsažené informace rozdělují na čtyři skupiny:

- Veřejné dokumenty
- Vnitřní dokumenty
- Důvěrné dokumenty
- Přísně důvěrné

Východiskem k zajištění důvěrnosti je model klasifikace informací a metodický pokyn pro zacházení s klasifikovanými informacemi. V souladu s firemním pokynem existuje

ke každému klasifikovanému dokumentu odpovědný vlastník a uživatel. **Vlastníkem** je obvykle vedoucí útvarů, který nese rozhodující odpovědnost za ochranu svěřených informací. Jeho povinností je vymezit klasifikační stupeň a na základě toho stanovit postupy pro řízení přístupů k dokumentům. **Uživatelem** je pracovník nebo jiná osoba, která pracují s informací uloženou v dokumentu. Všichni uživatele musí dodržovat pravidla vztahující se k zachování důvěrnosti dokumentu.

Při sdílení dokumentu se jednotlivé postupy a metody liší v závislosti na tom, komu a za jakým účelem je dokument předáván. V případě sdílení důvěrných nebo přísně důvěrných informací využívá vlastník nebo uživatel ve spolupráci s útvarem **Podpora vnitřního zákazníka** šifrovací nástroje. Pravidla předávání dokumentů jsou součástí modelu pro klasifikaci informace, které je každý zaměstnanec povinen znát a respektovat. Následující tabulka uvádí stručný přehled postupů při předávání dokumentů elektronickým přenosem prostřednictvím interní a externí sítě.

Tabulka 1 Pravidla při předávání elektronického dokumentu

	Přísně důvěrné	Důvěrné dokumenty	Vnitřní	Veřejné
Předávání prostřednictvím vnitřní sítě	Informace v dokumentu musí být zašifrovány	Doporučuje se informace v dokumentu šifrovat	Bez omezení	Bez omezení
	Přísně důvěrné	Důvěrné dokumenty	Vnitřní	Veřejné
Předávání prostřednictvím externí sítě	Informace v dokumentu musí být zašifrovány. Musí být připojeno standardní prohlášení[36]	Informace v dokumentu musí být zašifrovány. Do e-mailu musí být připojeno standardní prohlášení	Do e-mailu musí být připojeno standardní prohlášení	Bez omezení

Zdroj: Firemní materiál

Další hrozbou úniku důvěrných informací je nevhodné uchovávání dokumentů. Odpovědnost za uložení dokumentu nese jeho vlastník, který na základě klasifikačního

[36] Ve standardním prohlášení je deklarováno, že se jedná o důvěrné informace, které sou určené pouze uvedenému příjemci. Doporučuje postup v případě neoprávněného doručení dokumentu.

stupně zajišťuje vhodný způsob uchovávání. Model klasifikace informací, jehož základní principy jsou shrnuty v níže uvedené tabulce, doporučuje využít uzamykatelné skříně opatřené bezpečnostním klíčem nebo trezory s PIN kódem, šifrování informace, ochranu heslem a využívání systému řízených přístupů.

Tabulka 2 Uchovávání elektronických dokumentů

	Přísně důvěrné	Důvěrné	Vnitřní
Uchovávané na přenositelných médiích	Uzamčená skříň nebo místnost (klíčem, PIN kódem nebo jiným systémem řízení přístupu)	Uzamčená skříň nebo místnost (klíčem, PIN kódem nebo jiným systémem řízení přístupu	Bez omezení
Uchovávané na serverech a pracovních stanicích	Informace musí být zašifrovány. Používat systém řízení přístupu	Používat systém řízení přístupu	Bez omezení

Zdroj: Firemní materiál

Zabránění úniku citlivých informací z elektronických dokumentů napomáhá také systém pro správu dokumentů (DMS), který nedovoluje neoprávněným osobám dokument zobrazit nebo jinak s ním nakládat. Je součástí ERP systému SAP R/3 a znamená řešení pro správu došlých faktur a centrální evidenci některých právních dokumentů (nájemní smlouvy, dodavatelské smlouvy, licenční smlouvy, smlouvy o spolupráci, kupní smlouvy). Eviduje elektronické a digitální dokumenty, které vznikly naskenováním papírového originálu. Každý záznam má v systému jedinečný identifikátor v podobě čárového kódu, pod kterým skenovací aplikace uloží naskenovanou smlouvu nebo fakturu do systému správy dokumentů. Čárový kód zároveň poskytuje mimo funkce vyhledávácí také záruku autenticity elektronického obrazu listinného originálu. Pro zajištění důvěrnosti se dokumentům vloženým do DMS přidělí bezpečnostní znak, který je zkonstruován ze stupně utajení dokumentu, z účetního okruhu a ze skupiny nákupu. Oprávnění zároveň definuje okruh činností, které lze s dokumentem provádět.

Tabulka 3 Rozdělení oprávnění do skupin podle stupně utajení

První znak skupiny oprávnění	Oprávnění k přístupu podle stupně utajení
A	Bez utajení
D	Diskrétní
P	Přísně diskrétní
D	Vyhrazeno (skutečnost utajovaná z pohledu ohrožení státu

Tabulka 4 Rozdělení podle účetního kruhu

Druhý znak skupiny oprávnění	Oprávnění k přístupu podle účetního okruhu
C	První okruh
S	Druhý okruh
Y	Oba okruhy

Tabulka 5 Oprávnění podle skupiny nákupu

Konečné číslo skupiny oprávnění	Oprávnění k přístupu podle skupiny nákupu
1	IT a telekomunikace
2	Nemovitosti včetně investiční výstavby
3	Samostatné věci movité
4	Marketing
5	DHM a spotřební materiál
6	Vnitřní provozní služby
7	Personální a vzdělávání
8	Konzultační a poradenské služby
9	Elektronické bankovnictví
0	Právní

Zdroj: Firemní materiály

Bezpečnostní znak pro nájemní smlouvu je podle těchto pravidel AC6A a dovoluje manipulaci se smlouvou pouze uživateli, kterému byla přidělena role zahrnující oprávnění z této skupiny. Uživatel může dokument zobrazit a prohlížet, nemusí mít ale volbu pro jeho kopírování, tisk či ukládání mimo určené úložiště. Žádné oprávnění nedovolí koncovému uživateli naskenovaný záznam vymazat. Tato role je přidělena pouze gestorovi aplikace.

Pro došlé faktury je v rámci DMS vytvořena kniha faktur, ve které se evidují naskenované i elektronické faktury a ve které je možno filtrovat ty dokumenty, s nimiž chce uživatel pracovat. Podobně jako smlouvy jsou i faktury opatřeny bezpečnostním znakem.

Uživatel tak může podle svého oprávnění fakturu:

- nezobrazit, systém nabídne pouze základní metadata o dokumentu
- zobrazit a pouze prohlížet
- zobrazit a zpracovat
- zobrazit a přeposlat dál elektronicky jinému uživateli ke schválení

Každá změna, kterou oprávněný uživatel provede na dokumentech, je v systému zaprotokolovaná a tudíž kontrolovatelná.

Kromě klasických papírových daňových dokladů začala banka v nedávné době přijímat faktury v elektronické podobě. Řešení elektronické výměny faktur je založeno na formátu IDOC[37]. Všechny elektronické faktury přijaté do FCP[38] jsou na základě přesně nadefinovaných pravidel zkonvertovány do požadovaného formátu a předány do ERP SAP, kde se automaticky zpracovávají. Pro zajištění jednoznačnosti původu a neměnnosti obsahu, které vyžaduje platná legislativa, se ve FCP využívá elektronický podpis nebo elektronická značka. Systém tak automaticky ověří podpis či značku, neporušenost zprávy, věrohodnost certifikátu a v případě chyby pozastaví konverzi a další zpracování. Elektronický podpis nebo značka je součástí archivované elektronické faktury, a tak zaručuje její autenticitu, neporušenost jeho obsahu a čitelnost po celou dobu úschovy.

Tvorba, přijímání a evidence elektronických dokumentů je i předmětem Spisového řádu banky, jehož účelem je výkon spisové služby. Bez ohledu na formu se záznamy o doručených nebo odeslaných dokumentů evidují v informačním elektronickém systému AthenA. Elektronické dokumenty evidované v aplikaci AthenA vznikají jako pracovní dokumenty vnitrobankovní komunikace předávané prostřednictvím firemní sítě. Tyto dokumenty podléhají povinné evidenci a jejich originály v listinné podobě musí odpovědný pracovník autorizovat a datovat. Za shodu elektronické verze a papírové předlohy odpovídá odesílatel elektronického dokumentu. Pracovník spisové služby bezpečně umístí podepsaný originál v příručních spisovnách až do jejich odevzdání do ústřední spisovny nebo do archivu. Elektronické dokumenty uloží vlastník v archivu

[37] IDOC -Intermedia document (dočasný dokument) je standard pro elektronickou výměnu dat, který používá ERP SAP – zdroj: firemní materiál

[38] FCP zkratka pro Fakturační centrum podniku (aplikace Editel) – zdroj:firemní materiál

informačního systému, na sdílený disk či na fyzické médium, které musí zabezpečit v uzamykatelných skříních nebo v příručním trezoru organizačního útvaru po celou dobu skartační lhůty.

Elektronický systém AthenA také přijímá a ukládá datové zprávy z datové schránky. Na každou zprávu automaticky založí elektronický dokument a zaeviduje pod evidenčním číslem. Zprávu odešle vlastníkovi formou nového externího dokumentu, jehož součástí musí být i elektronický podpis a časové razítko, bylo-li součástí vložené přílohy datové zprávy. Vlastník po obdržení tohoto elektronického dokumentu do osobní emailové schránky pracuje s dokumentem obvyklým způsobem, tedy přidělí jednací číslo, vloží do spisu, zadá způsob vyřízení, předá dál jinému pracovníkovi nebo celé zpracování uzavře. Všechny dokumenty se rovněž automaticky ukládají v datovém úložišti připojenému k elektronickému systému spisové služby. Datová schránka se v bance v současnosti využívá pouze pro příjem datových zpráv, odesílání elektronických dokumentů jejím prostřednictvím není zatím povoleno.

Zachování dostupnosti dokumentů

S cílem zajistit dostupnost má každý dokument stanovenou minimální úroveň bezpečnosti při svém uchovávání, která vychází z důležitosti obsahující informace. Na základě provedené analýzy potenciálních rizik ze ztráty nebo nedostupnosti dokumentu, za kterou je vždy zodpovědný jeho majitel, se dokumenty rozdělují do skupiny:

- běžných dokumentů
- kriticky důležitých dokumentů
- dokumentů představující ekvivalent vysoké finanční hodnoty

Pro dokumenty existující pouze v elektronické podobě je hlavním bezpečnostním opatřením pro zajištění dostupnosti pravidelné zálohování, které na úrovni informačních systémů provádí útvar ICT. Řešení zálohy a obnovy kritických dokumentů je součástí pokynu představenstva o řízení kontinuity podnikání a jejich seznam obsahují havarijní plány. Kompletní seznam kritických dokumentů vede centrální databáze dokumentů celé finanční skupiny, do které banka patří. ICT také pravidelně zkoumá, zda je technické zařízení pro archivované dokumenty kompatibilní se záznamy na stávajících nosičích a zajišťuje jejich migraci na nové technické nosiče.

Zajistit pravidelné zálohování interních dokumentů uložených na sdílených útvarových discích je povinností každého útvaru banky. O jednorázové nebo o mimořádné zálohování dokumentů na fyzické nosiče CD/ DVD žádá útvar či uživatel prostřednictvím provozovatele ICT. Všechny nosiče jsou potom uloženy a archivovány v souladu s instrukcí o spisové službě a archivaci.

3.1.3 Výsledky šetření

Zkoumání dokumentů v této bance naznačuje, že existence pouze elektronických dokumentů jako originálů se vyskytuje v menší míře, než se předkládalo. Děje se tak pravděpodobně proto, že banky bývají obecně považovány za opatrnější a obezřetnější při zavádění nových technologií. Tato skutečnost se také promítá do používání elektronických dokumentů. Většinou se vedle nich uchovává dokument v listinné podobě. Opatření, která mají zajistit bezpečnost informací v elektronických dokumentech, jsou proto součástí celkové firemní politiky informační bezpečnosti. Politika informační bezpečnosti je důležitým pokynem představenstva a je závazná pro každého zaměstnance či externího pracovníka banky. Mimo jiné je pokyn také základem pro konkrétní opatření, jak zajistit bezpečnost informací, dokumentů, softwaru, hardwaru a dalších komunikačních technologií. Z provedené analýzy aplikovaných opatření týkající se zabezpečení elektronických dokumentů a z rozhovorů s odpovědnými osobami vyplývá, že největší důraz je kladen na ochranu důvěrných informací v dokumentech, na zabránění úniku citlivých dat do rukou neoprávněných osob. Pozornost se věnuje především zaměstnancům, uživatelům dokumentů, kteří bývají obecně nejslabším článkem bezpečnosti. Na jedné straně je tu systém pravidel a standardů, které je nutné dodržovat, na druhé straně uživatel, který by je měl dodržovat. Jedině tak lze účinně zajistit bezpečnost elektronických dokumentů. Z uvedeného důvodu firma průběžně na toto téma vzdělává své zaměstnance a rozšiřuje osvětu. Každý, kdo pracuje s firemní dokumentací, musí povinně absolvovat školení prostřednictvím e-learningu a složit závěrečný test. Informace o jeho absolvování je na osobní kartě zaměstnance. Nabádání k bezpodmínečnému dodržování zabezpečení informací a dokumentu se provádí nejen osvětou mezi zaměstnanci, ale i přísně udělovanými sankcemi, v těch v nekritičtějších případech přichází na řadu zrušení pracovního poměru.

Zvláštní pozornost se věnuje řízení přístupových práv k dokumentům. Hlavní znaky tohoto procesu se značně shodují s doporučovanými postupy mezinárodního standardu MoReq2 a zároveň vycházejí z obecného pokynu představenstva banky, který popisuje bezpečnostní politiku pro řízení logického přístupu uživatelů k transakcím, k aplikacím a k transformačním systémům. Přístupy k dokumentům uložených v informačním systému obdrží uživatel prostřednictvím schvalovacího procesu na základě oficiálních a schválených žádostí od liniového manažera a vlastníka aplikace, v níž se dokument nachází. Uživatel dostane pouze takové oprávnění, které se vztahuje k vykonávání jeho pracovní funkce. Všechny události spojené se správou s přístupovými oprávněními a se schvalovacím procesem se zaznamenávají v protokolu. Nestačí však oprávnění pouze přidělit, je nutné i kontrolovat jejich aktuálnost. Jednou ročně se proto provádí revize všech přístupů zaměstnanců, tedy i přístupů k elektronickým dokumentům. Takto nastavený proces přidělování přístupů se osvědčil jako velmi účinný a je zárukou eliminace neautorizovaným vstupům.

Dalším doporučovaným opatřením k zachovávání důvěrnosti, integrity a autenticity digitálního dokumentu je elektronický podpis a šifrování informace v obsahu dokumentu. Podíváme-li se na využívání těchto nástrojů zabezpečení, lze konstatovat, že jejich používání ve vnitřním prostředí firmy nepatří k běžné praxi. Elektronický podpis a šifrování je opatření především pro dokumenty s mimořádně citlivými informacemi nebo pro dokumenty důvěrné odesílané mimo firemní síť. V tomto případě předpisy přímo nařizují, aby byly odesílané dokumenty zašifrovány. Elektronický podpis je také zárukou autenticity elektronicky přijímaných faktur, kde spolu s časovým razítkem garantují jeho pravost a neporušenost. Kontrolní mechanismy jsou implementovány v aplikaci pro elektronickou fakturaci a kontrolují každý přijímaný dokument automaticky bez účasti uživatele, čímž zaručují jeho jednoznačnost a neměnnost.

3.2 Analýza útvarových dokumentů

Bezpečnostní pravidla a standardy pro nakládání s dokumenty, které banka implementovala, jsou automaticky závazné pro všechny organizační složky společnosti. Jednotlivé útvary mohou, některé vzhledem ke své specifické činnosti dokonce i musí, doplňovat tato opatření, ovšem pouze tak, aby nebyla v rozporu s obecnými standardy

nebo jejich účinnost nesnižovala. Na základě pečlivé analýzy rizik ze ztráty nebo úniku dat z pracovní dokumentace stanovuje bezpečnostní zásady i útvar Účetní kontrola a inventarizace.

3.2.1 Charakteristika a složení útvaru

Denně proběhne v bance tisíce obchodních operací, které více či méně ovlivňují finanční hospodaření společnosti. Všechny operace jsou zachyceny v podobě účetních záznamů, jež vytvářejí zaměstnanci s oprávněním tyto operace zaznamenávat v transakčních a účetních systémech. Vzhledem k jejich objemu je důležité, aby existoval a efektivně fungoval vnitřní kontrolní systém. Součástí rozsáhlého kontrolního systému je i útvar Účetní kontrola a inventarizace, jehož hlavním cílem je dbát o správnost účetních dat, která jsou základem pro finanční výkazy a zprávy o finančním hospodaření banky. Organizačně patří útvar Účetní kontrola a inventarizace do divize Finance. Celkem v něm působí dvanáct zaměstnanců včetně vedoucího. Útvar se dále člení do dvou skupin, které jsou zodpovědné za kontroly účtování různých obchodních činností. Do náplně práce útvaru náleží i metodická podpora koncových uživatelů transakčních a účetních systémů a systémů pro rekonciliace.

3.2.2 Hlavní činnosti pracovního procesu útvaru

Při využívání účetních a transakčních systémů hrozí riziko výskytu častých a opakujících pochybení ze strany uživatelů. K prevenci rizika a odstraňování příčin chyb je v bance zřízen interní kontrolní systém účetních procesů, který zahrnuje kontrolní prostředí, postupy kontrol, účetní a transakční systémy. Kontrolní prostředí tvoří organizační složky banky, srozumitelné vymezení kontrolovaných oblastí a vnitřní účetní pravidla. Kontrolní činnosti a postupy stanovují metody monitoringu sledovaných účtů, způsoby odstraňování zjištěných chyb, pořizování dokumentace o nalezených nesrovnalostech a hlášení o provedení pravidelných kontrol. Posledním prvkem kontrolního systému jsou účetní a transakční systémy. Představují zdroj informací pro analýzu hospodaření firmy a dalších rozhodnutí, proto musí pracovat zcela korektně. Je tedy důležité sledovat jejich fungování a odhalovat nespolehlivé zpracování dat nebo dokonce ztráty dat během zpracování samotného.

Úlohou útvaru Účetní kontrola a inventarizace je aktivně přispívat k zefektivňování vnitřního kontrolního systému. Jeho cílem není nahradit interní audit, ale pravidelně monitorovat omyly a nesrovnalost, a při účtování předcházet neúmyslným nebo úmyslným selháním.

Mezi hlavní činnosti pracovního procesu útvaru patří:

- pravidelné ověřování zůstatků účtů hlavní knihy
- kontrola oprávněnosti účtování vybraných operací
- koordinace a řízení procesu inventarizace
- přidělování odpovědnosti útvarům banky za správnost účtování na účty hlavní knihy podle obchodního produktu nebo účtovaného procesu
- kontrola nastavení parametrů účetních a transakčních systémů a jejich bezproblémový chod
- poskytování konzultační a poradenské služby správcům účtů při provádění kontroly

O provedení jednotlivých činností pracovních procesu se musí pořídit dokumentace v listinné nebo elektronické podobě sloužící pro vnitřní potřeby útvaru a také jiným oddělením, například internímu a externímu auditu nebo finančnímu výkaznictví. Do náplně útvaru patří také koordinování procesu inventarizace, jehož průběh a výsledek se podle zákona o účetnictví řádně zaznamenává v inventarizačních dokumentech.

3.2.3 Charakteristika dokumentů a popis stávajícího způsobu práce s dokumenty

Tato část kapitoly přináší seznam vybrané pracovní dokumentace a podrobněji popisuje vlastnosti, účel, význam a manipulaci s nimi v rámci pracovního procesu. Některé z dokumentů mají pouze elektronickou podobu, jiné se vyskytují současně v papírové i elektronické formě a patří k základním nástrojům činnosti útvaru. Většina dokumentů se uchovává několik let v souladu se základními pravidly banky nebo podle platné legislativy. V následující tabulce je přehled vybraných útvarových dokumentů, které tato kapitola blíže charakterizuje.

Tabulka 6 Přehled nejdůležitějších dokumentů v útvaru

Název dokumentu	Druh dokumentu	Použitý nosič	Důvěrnost dokumentu	Třída rizika dokumentu	Místo uložení
Zprávy o inventarizacích	Účetní dokumenty	Papír	důvěrný	Třída 3	pracoviště vlastníka
Ustanovení Koordinátorů, Inventurníků	Účetní dokumenty	Papír	důvěrný	Třída 3	pracoviště vlastníka
Inventarizační zápisy	Účetní dokumenty	Papír	důvěrný	Třída 3	pracoviště vlastníka
Inventurní soupisy, sestavy	Účetní dokumenty	Papír	důvěrný	Třída 3	pracoviště vlastníka
Měsíční reporty ke kontrolám	Účetní dokumenty	vzdálený disk	důvěrný	Třída 3	pracoviště vlastníka
Postupy kontrol účtů	Účetní dokumenty	vzdálený disk	vnitřní	Třída 1	pracoviště vlastníka
Nestandardní opravy	Účetní dokumenty	vzdálený disk	vnitřní	Třída 2	pracoviště vlastníka

Zdroj: Firemní materiál

Závěrečná zpráva o inventarizaci

Z ustanovení § 29 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů vyplývá pro účetní jednotky provádět inventarizaci k okamžiku, kdy sestavují řádnou nebo mimořádnou účetní závěrku. Prokázat provedení inventarizace majetku a závazku jsou povinny po dobu pěti let po jejím provedení. Ke splnění tohoto legislativního požadavku slouží veškerá dokumentace, jež je výsledkem inventarizačního procesu. Závěrečná zpráva je účetní dokument vznikající v útvaru Účetní kontrola. Jeho obsah tvoří informace o průběhu inventarizace, včetně příloh o odsouhlasení účetní evidence a inventurních soupisů. Součástí zprávy jsou navrhovaná opatření k vyřešení zjištěných nesrovnalostí. Zpráva slouží jako důkazný dokument o provedení inventarizace. Patří mezi kriticky důležité dokumenty do třídy 3 (celkem 6 tříd). V listinné podobě jako originál je opatřená podpisem odpovědné osoby a je uložena v uzamykatelné skříni po dobu jednoho roku po skončení inventarizace v příručním archivu útvaru. Následně po

předání do ústředního archivu se v souladu s firemním archivačním řádem uchovává deset let. Její elektronická kopie je uložena na útvarovém disku v určeném adresáři.

Stanovení koordinátorů inventarizace, inventurníků a správců účtu

Písemné jmenování odpovědných osob za jednotlivé fáze inventarizace má listinnou podobu a přesně vymezuje jejich povinnosti při zajišťování procesu. Dokument vytváří útvar Účetní kontrola. Patří mezi kriticky důležité dokumenty třídy 3 a v ústředním archivu se archivuje deset let. Jeho kopie má elektronickou podobu a rovněž jako závěrečnou zprávu, pravidla nařizují uchovávat tento dokument na útvarovém disku.

Inventarizační zápisy, inventurní soupisy, podpůrné kontrolní sestavy

Všechny dokumenty jsou charakterem považovány za účetní dokumenty a vznikají v útvaru, který je odpovědný za inventarizování účtu ve spolupráci s útvarem Účetní kontrola a inventarizace. Obsahují podrobné informace o provádění inventarizace jako číslo analytického účtu, jednoznačný popis majetku a závazků, datum provedení inventury, podpisy pracovníků pověřených provedením fyzické inventury nebo sestavy z transakčních systémů. Podobně jako ostatní dokumenty týkající se inventarizace patří mezi kritické důležité dokumenty ze třídy 3 a doba jejich archivace je deset let. Originály dokumentů jsou v papírové podobě, elektronické kopie se archivují na útvarovém disku po dobu dvou let od ukončení inventarizace.

Reporty o pravidelné kontrole zůstatku účtu

Report o pravidelné kontrole zůstatku účtu je formalizované písemné hlášení o výsledku provedení pravidelné kontroly. Report informuje o tom, zda byla provedena kontrola na všech přiřazených účtech a uvádí, zda je zůstatek věrohodný nebo zda existuje podezření o neoprávněnosti zůstatku. Odpovědnost za zpracování a odeslání hlášení má liniový vedoucí útvaru, ve kterém je kontrola prováděna. Report, všechny přílohy týkající se objevených nesrovnalostí a návrh na jejich vyřešení jsou předávány výlučně v elektronické formě. Pracovník útvaru Účetní kontrola ukládá tyto dokumenty rovněž v elektronické podobě ve sdíleném adresáři na útvarovém disku. Dokument náleží do skupiny vnitřních dokumentů do třídy 2, na které se vztahuje běžná úroveň bezpečnosti, tedy způsob zabezpečení dokumentu stanovuje majitel dokumentu na základě rizika případných ztrát v důsledku nedostupnosti dokumentu. Pro tento dokument stanovil vlastník dobu uchování na tři roky.

Postupy kontrol účtů

Dokument, který má výhradně elektronickou podobu, obsahuje závazná pravidla pro vykonávání kontroly na účtech a základní metody monitoringu účtů. Pravidelně aktualizovaný a na firemním intranetu zveřejňovaný dokument poskytuje návody a vhodné postupy logických kontrol zůstatků účtů, posouzení pravděpodobností, že operace nastala, nebo porovnávání zůstatku se zůstatkem ve srovnatelném období. Svým charakterem se zařazuje mezi vnitřní dokumenty ze třídy 1 a podle rozhodnutí útvaru se archivuje v elektronické podobě na sdíleném útvarovém disku po dobu dva roky.

Dokumenty vztahující se k nestandardním opravám v transakčním systému

Jak již bylo zmíněno výše, patří do náplně práce útvaru i kontrola bezproblémového chodu transakčních systémů a nastavování nových parametrů v systémech podle oprávněných požadavků. V těchto případech zajišťuje odpovědný pracovník ve spolupráci s útvarem ICT vyřešení problémů. K řešení požadavku a k odstraňování chyb se využívají žádosti o opravu, formuláře opravy a evidence opravy v elektronické či papírové formě.

Žádost o opravu nebo nastavení parametrů v systému

Všechny žádosti tohoto druhu zasílá pracovník do útvaru Účetní kontrola a inventarizace elektronicky prostřednictvím firemního emailu, ve kterém přesně specifikuje svůj požadavek a důvod. V současné době mají tyto žádosti podobu emailové zprávy nebo přílohy emailu, které nejsou šifrovány a ani podepsány elektronickým podpisem. Každá zpráva obsahuje nešifrovaný elektronický podpis ve smyslu uvedených informací o jménu a pracovní pozice odesílající osoby. Na základě zaslané žádosti pracovník útvaru Účetní kontrola a inventarizace připraví a odešle formulář opravy s popisem postupu opravy a uloží elektronickou žádost na útvarový disk do určeného adresáře po dobu pěti let.

Formulář opravy

Formulář uvádí postup opravy nebo nastavení parametrů v transakčním systému. Elektronická forma je odeslána emailem pracovníkovi ICT, který zajistí opravu. Každý elektronický formulář je zároveň převeden do listinné podoby, který podepisuje liniový

manažer útvaru. Elektronické formuláře se potom uchovává na útvarovém disku po dobu pěti let, jejich listinná forma rovněž pět let v příručním archivu útvaru.

Evidence provedených oprav

Jedna se o elektronický dokument, který je automaticky vygenerován z transakčního systému a slouží jako důkaz o provedení opravy v souladu s postupem uvedeným ve formuláři. Dokumenty jsou uloženy na útvarovém disku a archivovány podobně jako ostatní dokumenty vztahující se k opravám až pět let.

3.2.4 Analýza zabezpečení útvarových dokumentů a návrhy na jejich doplnění.

Přehled nejdůležitějších dokumentů, které ke své práci pracovníci útvaru využívají, ukazuje, že podobně jako v celé firmě jsou i zde zastoupeny elektronické dokumenty v menší míře než dokumenty listinné. Většinou jsou listinné dokumenty označené jako důvěrné ze třídy 3, které vyžadují podpis odpovědné osoby a liniového manažera. Práce s nimi a jejich archivování je řízeno podle prověřených pravidel pro dokumenty, jejichž nosičem je papír. V elektronické podobě jsou dokumenty v kategorii vnitřní dokument a patří do třídy 1 nebo 2, pro které platí běžná bezpečnostní pravidla. Dle posouzení důležitosti nebo prokazatelnosti dokumentů pro činnosti útvaru může vlastník nastavit vyšší stupeň zabezpečení, především při jejich dlouhodobějším uchovávání.

Elektronické dokumenty, tedy reporty o provedení kontroly, postupy kontrol účtů a záznamy o provedení nestandardních oprav mají jednotné úložiště pro dlouhodobější uchovávání na útvarovém disku v určených složkách. Pro útvarový disk je jmenován správce, který nastavuje a řídí přístupové oprávnění jednak zaměstnancům útvaru a také pracovníkům auditu. Jiným uživatelům může být přiděleno oprávnění na základě žádosti schválené manažerem a správcem disku. Řízení přístupových oprávnění zajišťuje aplikace, která zároveň poskytuje pohledy na aktuální nastavená oprávnění a reporty pro zpětnou kontrolu za posledních šest měsíců. Pracovníci ukládají dokumenty na společném útvarovém disku do jednotlivých adresářů, do nichž má přístup každý, kdo má oprávnění vstupu na útvarový disk. Reporty o provedení kontroly jsou doručovány jako přílohy emailu prostřednictvím poštovní schránky a rovněž ve formátu

aplikace Outlook uloženy na sílený disk. Uložení samotné zprávy a její přílohy poskytuje údaje o odesílateli a o datu přijetí zprávy. Podobný postup se aplikuje v případě ostatních pracovních dokumentů.

Na základě analýzy dokumentu a jejich stávajícího zabezpečení z hlediska důvěrnosti je vhodné doporučit vyšší stupeň bezpečnostních pravidel. Vzhledem k tomu, že reporty o kontrolách nebo formuláře oprav v informačním systému často obsahují citlivá data, jimiž jsou například osobní údaje klienta, klientské účty či informace o hospodaření banky, pouze řízení a kontrola přístupů k útvarovému disku není dostačující. V případě, že by neoprávněný uživatel získal přístup na útvarový disk, nic by mu nezabránilo, aby si zobrazil uložené dokumenty nebo si z nich pořídil kopii. Z tohoto důvodu je na místě navrhnout doplnění dalších postupů k zachování důvěrnosti. Prvním krokem by mělo být definování zásad, podle kterých se budou vybírat dokumenty podléhající důkladnějšímu zabezpečení. Dále je nutné přesně určit přístupová práva přímo k dokumentu, kupříkladu nastavit heslo pro jeho otevření, nadefinovat oprávněné uživatele, označit ho jako konečný nebo pouze ke čtení. Implementaci těchto a podobných kroků by jistě posunula zabezpečení útvarových dokumentů na kvalitativně vyšší úroveň.

Uložené dokumenty uchovávají informace o provedení kontroly, o zjištěných nesrovnalostech, o opravách chyb či bývají zdrojem informací o jiné činnosti pracovníků v útvaru. Proto by některé z nich měly být vždy dostupné a čitelné. Stávající pokyn archivování útvarových elektronických dokumentů stanoví jejich uchovávání v archivním adresáři na sdíleném disku útvaru, který pravidelně zálohuje útvar ICT. Zálohování útvarového disku však neřeší problém s dostupností dokumentů starších než šest měsíců. Na tuto skutečnost upozornil i interní audit ve své zprávě. Vzhledem k tomu, že je tady požadavek uchovávat vybrané dokumenty i několik let, je nutné doplnit opatření k zajištění dostupnosti, a to zálohováním vybraných dokumentů na fyzické médium. Dokumenty by se ukládaly do vyhrazeného archivního adresáře, ze kterého se jednou za měsíc pořídí plná záloha měsíčních dat na samostatný fyzický nosič (CD/DVD) pro případ ztráty z původního útvarového disku. Takto vytvořené kopie je možné uchovávat podle platné firemní instrukce o archivní službě.

4 Závěr

Prudký rozvoj informačních technologií a nástup elektronického prostředí do podniků přináší široké možností při využívání elektronických dokumentů v podnikatelské činnosti. Současná platná legislativa podporuje elektronizaci listinných dokumentů a vytváření elektronických originálů, které se mají stát při dodržení všech stanovených požadavků právoplatnými dokumenty nejen v podnikové sféře, ale i v životě běžných občanů. Jejich používání by mělo nejen omezit rutinní činnosti jako kopírování, přepisování obsahu dokumentu či hledání v nepřehledných archivech, nýbrž také přinést zrychlení pracovních procesů, odstranění chyb a efektivnější řízení podnikové dokumentace. Pokud se má elektronický dokument stát právoplatným originálem, je nutné zajistit jeho průkaznost, důvěrnost a celistvost nastavením vhodných bezpečnostních pravidel, jejichž přehledem a analýzou se zabývala tato bakalářská práce.

Hlavním přínosem této práce je vytvoření uceleného pohledu na zabezpečení elektronického dokumentu, jehož prostřednictvím je čtenář uveden do dané problematiky. Teoretická část prezentuje nejvhodnější postupy zabezpečení dokumentů a objasňuje význam a fungování některých důležitých nástrojů, kupříkladu princip elektronického podpisu a časového razítka. Obecné poznatky získané studiem odborné literatury a článků se dále aplikovaly v praktické části, která si kladla za cíl zmapovat opatření pro zajištění bezpečnosti při nakládání s elektronickými dokumenty ve finanční instituci a potvrdit názory vyjádřené v hypotézách na začátku práce. **V první hypotéze** se přepokládalo, že proces řízení přístupů k citlivým elektronickým dokumentům je efektivnější, když se přístupy uživatelům přidělují podle pevně stanovených pravidel. Tato hypotéza se potvrdila. Přidělování oprávněného přístupu k dokumentům probíhá podle předem nastaveného procesu. Schvalovací proces začíná podáním a posouzením žádosti, následuje schválení žádosti zodpovědným pracovníkem, pokračuje přidělením přístupů a nakonec zaprotokolováním událostí spojených se schvalovacím procesem a s uživatelským účtem. Všechny přístupy se přidělují tímto způsobem, který je zárukou vyloučení neautorizovaného přístupu a také efektivity řízení přístupů. **Druhá hypotéza** tvrdí, že k úmyslnému či neúmyslnému porušení integrity a důvěryhodnosti dokumentů nedochází v případě, jsou-li správně zabezpečené v informačním systému. Praxe

potvrdila hypotézu a ukázala, že pro zajištění těchto atributů je vhodné nejen přidělování přístupů k dokumentům, ale také nastavení bezpečnostního znaku na samotném záznamu dokumentu v informačním systému, který přesně vymezuje činnosti a znemožňuje odstranění záznamu dokumentu nebo nahrazení jiným záznamem. **Třetí hypotéza** přichází s názorem, že pro snižování ztráty nebo poškození elektronických dokumentů je vhodné pravidelné zálohování v přesně stanovených intervalech. Tuto hypotézu praxe opět potvrdila. Proces zálohování má definovaná pravidla, podle kterých probíhá zálohování automaticky a v pravidelných intervalech a v případě potřeby je možné obnovit i kriticky důležité dokumenty ve vhodném časové limitu. V závěru práce bylo navrhnuto doplnění postupů zabezpečení elektronických dokumentů ve vybraném útvaru, jejichž implementace by mohla zlepšit zabezpečení a zároveň vyhovět doporučení interního auditu. Dalším doporučením, které je však nad rámec této bakalářské práce, je věnovat větší podporu využití elektronického podpisu ve firemní elektronické dokumentaci předávané prostřednictvím vnitřní informační sítě.

Jak vyplývá z poznatků předkládaných v této bakalářské práci, problematika bezpečnosti elektronických dokumentů představuje velmi aktuální problém, jehož řešením se zabývá mnoho odborníků. Nelze předpokládat, že se podaří jednou provždy problematiku zcela vyřešit. Zajistíme-li dnes odhalená rizika, objeví se zítra nová hrozba. Proto i opatření, která jsou zmíněna v této práci, platí především pro současnost, v budoucnu se zcela jistě objeví potřeba nových a účinnějších metod ochrany elektronických dokument.

Literatura

Odborné knihy

GÁLA, Libor; POUR, Jan; ŠEDIVÁ, Zuzana. *Podniková informatika*. 2. vydání. Praha: GRADA Publishing, 2009. 469 s. ISBN 978 -80 -247 -2615-1.

KUNSTOVÁ, Renáta. *Efektivní správa dokumentů*. 1. vydání. Praha 7: GRADA Publishing a.s., 2009.208 s. ISBN 978-80-247-3257--2.

MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. 1. vydání. Brno: COMPUTER Press, a.s., 2006. 154 s. ISBN 978-80-251-1511-4.

PETERKA, Jiří. *Báječný svět elektronického podpisu* [online]. Praha: CZ.NIC, 2011, 2.4.2011 [cit. 2011-09-30]. Dostupné z WWW: <http://bajecnysvet.cz/index.php>.

SKLENÁK , Vilém , et al. *Data, znalosti, informace a Internet*. 1. vydání. Praha: C. H. Beck, 2001. 507 s. ISBN 80-7179-409-0.

SMEJKAL, Vladimír; RAIS, Karel. *Řízení rizik ve firmách a v jiných organizacích*. 2.rozšířené a aktualizované vydání. Praha 7 : GRADA Publishing a.s., 2006. 300 s. ISBN 80-247-1667-4.

ŠEBESTA, Václav , et al. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*. Praha : Český normalizační institut, 2006. 70 s. ISBN 80-7283-204-2.

VYMĚTAL, Jan; DIAČIKOVÁ, Anna ; VÁCHOVÁ, Miriam. *Informační a znalostní mamagement v praxi.* 1. vydání. Praha 10 : LexisNexis CZ s.r.o., 2006. 399 s. ISBN 80-86920-01-1.

Internetové zdroje

BRATKOVÁ, Eva . *Kvalitní studie k problémům dlouhodobé archivace digitálních dokumentů.* Ikaros [online]. 2011, 15, 4, [cit. 2011-10-30]. Dostupný z WWW: <http://www.ikaros.cz/node /6754>>. ISSN 1212-5075.

Česko. *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů*. In Sbírka zákonů, Česká republika. 2000, 68, s. 24. Dostupný také z WWW: <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

EC.EUROPA.EU [online]. 2011 [cit. 2011-09-10]. *Transparency.* Dostupné z WWW: <http://ec.europa.eu/transparency/archival_policy/moreq/doc/moreq_cs.pdf>.

GOGELA, Robert . *Důvěryhodný elektronický dokument.* SystemOnline.cz dokument [online]. 2010, 3, [cit. 2011-10-01]. Dostupný z WWW: <http://www.systemonline.cz/clanky/duveryhodny-elektronicky-dokument-1.htm>.

INKAM.cz [online]. 2011 [cit. 2011-09-20]. *Legislativa.* Dostupné z WWW: <http://www.inkam.cz/LEGISLATIVA/Uplne-zneni-zakona-c-499-2004-Sb-o-archivnictvi-a-spisove-sluzbe-v-platnem-zneni.html>.

LIDINSKÝ, Vít; ŠVARCOVÁ, Ivana. Securityworld.cz [online]. 2007 [cit. 2011-09-30]. *Dlouhodobé uchovávání elektronicky podepsaných elektronických dokumentů*. Dostupné z WWW: <http://securityworld.cz/securityworld/dlouhodobe-uchovavani-elektronicky-podepsanych-elektronickych-dokumentu-1025>.

MVCR.cz [online]. 2010 [cit. 2011-10-30]. *Zákon o eGovernmentu*. Dostupné z WWW: <http://www.mvcr.cz/clanek/ega-cili-zakon-o-egovernmentu.aspx>.

ROTHENBERG, Jeff. *A Report to the Council on Library and Information Resources. In Finding a Viable Technical Foundation for Digital Preservation* [online]. Washington : [s.n.], 1999 [cit. 2011-09-26]. Dostupné z WWW: <http://www.clir.org/pubs/reports/rothenberg/pub77.pdf>. ISBN 1-887334-63-7.

SMEJKAL, Vladimír ; MATĚJKA, František. System Integration Conference Archive. In *Elektronické dokumenty, podpisy, značky a veřejné listiny : Praktické zkušenosti s převodem účetní dokumentace na digitální podobu*[online]. 2007. [s.l.] : [s.n.], 2007 [cit. 2011-09-22]. Dostupné z WWW: <http://si.vse.cz/archive/index.asp?volume=2007>. ISBN 978-80-245-1196-2.

STOKLÁSKOVÁ, Bohdana . Knihovna.nkp.cz [online]. 2006 [cit. 2011-10-30]. *Perspektivy důvěryhodného digitálního úložiště v rámci Národní digitální knihovny*. Dostupné z WWW: <http://knihovna.nkp.cz/knihovna62/stoklas.htm>.

TKAČÍKOVÁ, Daniela . *Jak pracovat s informacemi*. In Obecné základy s informacemi [online]. 2010. [s.l.] : [s.n.], 2010 [cit. 2011-09-20]. Dostupné z WWW: < http://hdl.handle.net/10084/78274>. ISBN 978-80-248-2157-3.

Wikipedie [online]. 2011 [cit. 2011-09-22]. *Elekronický podpis*. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis>.

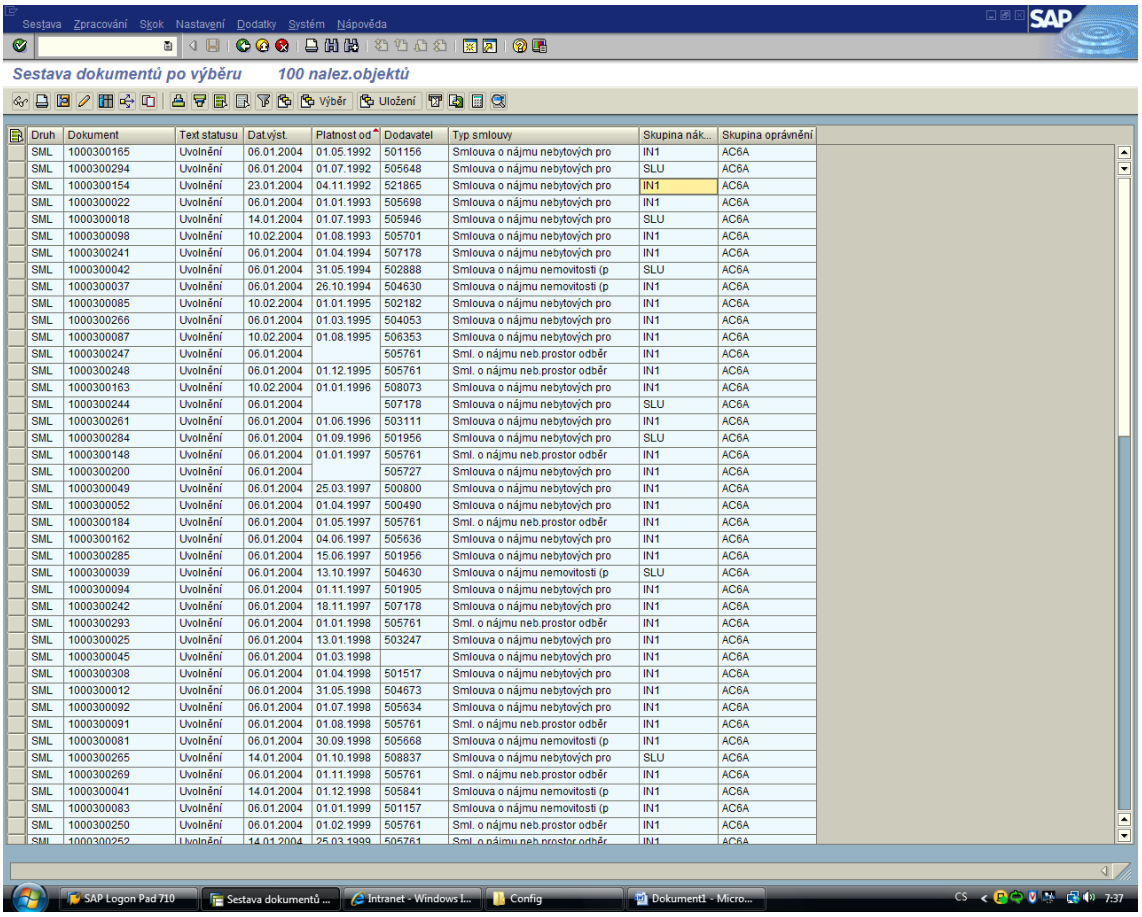
Vydavatelství.vscht.cz [online]. 2011 [cit. 2011-10-30]. *Datový soubor*. Dostupné z WWW: <http://vydavatelstvi.vscht.cz/knihy/uid_es-005/hesla/datovY_soubor.html>.

Ostatní zdroje

Firemní předpisy a instrukce

Přílohy

Příloha 1 Ukázka sestavy z informačního systému správy elektronických dokumentů



Zdroj: Firemní materiál