

System řízení bezpečnosti informací v bankovníctví

Bc. Pavel Procházka

Diplomová práce
2016



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Pavel Procházka**
Osobní číslo: **A14378**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Systém řízení bezpečnosti informací v bankovníctví**
Téma anglicky: **Information Security Management System in Banking**

Zásady pro vypracování:

1. Zpracujete rešerši literatury a pramenů, které se vztahují ke zpracovávanému tématu.
2. Definujte základní pojmy systému řízení bezpečnosti informací
3. Zpracujte metodiku univerzální matice rizikové analýzy
4. Provedte analýzu rizik s využitím metody univerzální matice rizikové analýzy
5. V rámci analýzy rizik definujte charakteristické prvky systému řízení bezpečnosti informací v bankovníctví
6. Výstupy z analytické části kvalifikační práce aplikujte při zpracování návrhu opatření k eliminaci vybraných rizik.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. Čermák, Miroslav. Řízení informačních rizik v praxi. Brno : Tribun, 2009. 134 s. ISBN 978-80-7399-731-1.
2. Doucek, P.; Nedomová, L.: Nasazení integrovaného systému řízení pro získání konkurenční výhody. AT&P journal, , c. 12, 2004.
3. Smejkal, V.: Řízení rizik ve firmách a jiných organizacích. Grada, třetí vydání, 2010, ISBN 978-80-247- 051-6.
4. Šebesta a kol., Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005 Český normalizační institut, 2006, ISBN 80-7283-204-2.
5. Tichý, M.: Ovládání rizika. C.H. Beck, vyd. 1. vydání, 2006, ISBN 80-717-9415-5.

Vedoucí diplomové práce:

PhDr. Mgr. Stanislav Zelinka
Ústav bezpečnostního inženýrství

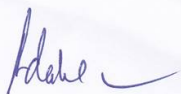
Datum zadání diplomové práce:

5. února 2016

Termín odevzdání diplomové práce:

16. května 2016

Ve Zlíně dne 5. února 2016



doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užit své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen přípouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor;
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

.....
podpis diplomanta

ABSTRAKT

V první (teoretické) části práce jsou definovány základní pojmy systému řízení bezpečnosti informací, řešerše normy ČSN ISO/IEC 27001:2014 a zákona 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, následuje popis managementu rizik včetně analýzy rizik a některých používaných metod. V druhé (praktické) části je popsána metodika praktické části, včetně metodiky univerzální matice rizikové analýzy, popis charakteristických prvků systému řízení bezpečnosti informací v bankovníctví, praktické provedení analýzy rizik (včetně definování aktiv a hrozeb), výsledky analýzy rizik a na jejich základě návrh opatření k ochraně neojohroženějších aktiv.

Klíčová slova: systémy řízení bezpečnosti informací, ISMS, analýza rizik, univerzální matice rizikové analýzy, UMRA, bankovníctví

ABSTRACT

The first part of the paper defines essential terms of information security management system; researches the ČSN EN/ISO 27001:2014 standard and the law on cyber security; and describes risk management including risk analysis and some of the commonly used methods.

The second part describes methodics, including universal matrix of risk analysis, description of typical elements of information security management system in finance, execution of risk analysis (including assets and threat definition), results of risk analysis and proposals for protection of the most endangered assets.

Keywords: information security management system, ISMS, risk analysis, universal matrix of risk analysis, UMRA, banking

Na tomto místě bych chtěl poděkovat PhDr. Mgr. Stanislavu Zelinkovi za cenné připomínky a rady při vedení diplomové práce, Ing. Petru Prokúpkovi za rady v oblasti managementu bezpečnosti informací a v neposlední řadě všem expertům, kteří vyplnili dotazník pro praktickou část této práce a bez kterých by tato práce nemohla vzniknout.

OBSAH

ABSTRAKT	5
ABSTRACT	5
ÚVOD	10
I TEORETICKÁ ČÁST	11
1 DEFINICE POJMŮ	12
1.1 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ.....	12
1.2 AKTIVUM.....	12
1.3 HROZBA.....	13
1.4 ZRANITELNOST.....	13
1.5 DOPAD, NÁSLEDEK.....	13
1.6 RIZIKO.....	13
1.7 OPATŘENÍ.....	13
2 NORMA ČSN ISO/IEC 27001:2014	15
2.1 KAPITOLY 0 AŽ 3 NORMY.....	15
2.2 KAPITOLA 4 NORMY <i>KONTEXT ORGANIZACE</i>	15
2.3 KAPITOLA 5 NORMY <i>VŮDČÍ ROLE</i>	16
2.4 KAPITOLA 6 NORMY <i>PLÁNOVÁNÍ</i>	16
2.5 KAPITOLA 7 NORMY <i>PODPORA</i>	16
2.6 KAPITOLA 8 NORMY <i>PROVOZOVÁNÍ</i>	18
2.7 KAPITOLA 9 NORMY <i>HODNOCENÍ VÝKONNOSTI</i>	18
2.8 KAPITOLA 10 NORMY <i>ZLEPŠOVÁNÍ</i>	19
2.9 NORMATIVNÍ PŘÍLOHA A.....	19
3 ZÁKON O KYBERNETICKÉ BEZPEČNOSTI	21
3.1 POJMY POUŽÍVANÉ ZÁKONEM O KYBERNETICKÉ BEZPEČNOSTI (HLAVA I).....	21
3.2 POROVNÁNÍ POJMŮ.....	22
3.3 DALŠÍ HLAVY A ČÁSTI ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI.....	24
3.3.1 Hlava II.....	24
3.3.2 Hlava III.....	25
3.3.3 Hlava IV.....	25
3.3.4 Hlava V.....	25
3.3.5 Hlava VI a další části ZKB.....	26
4 ANALÝZA RIZIK	27
4.1 IDENTIFIKACE AKTIV.....	28
4.2 OHODNOCENÍ AKTIV.....	28
4.3 IDENTIFIKACE PRÁVNÍCH A BUSSINESSOVÝCH POŽADAVKŮ.....	29

4.4	ODHAD HROZEB.....	29
4.5	IDENTIFIKACE EXISTUJÍCÍCH OCHRANNÝCH OPATŘENÍ.....	30
4.6	ODHAD ZRANITELNOSTI.....	30
4.7	IDENTIFIKACE NÁSLEDKŮ.....	31
4.8	ODHAD RIZIK.....	31
4.9	METODY ANALÝZY RIZIK.....	32
4.9.1	SWOT.....	33
4.9.2	FMEA.....	33
5	MANAGEMENT RIZIK.....	35
5.1	STANOVENÍ KONTEXTU.....	36
5.1.1	Určení základních kritérií.....	36
5.1.2	Rozsah a hranice.....	36
5.1.3	Organizační struktura.....	37
5.2	POSOUZENÍ RIZIK BEZPEČNOSTI INFORMACÍ.....	37
5.3	OŠETŘENÍ RIZIK.....	38
5.4	AKCEPTACE RIZIK.....	39
5.5	KOMUNIKACE RIZIK.....	39
5.6	MONITOROVÁNÍ A PŘEZKOUMÁNÍ RIZIK.....	40
II	PRAKTICKÁ ČÁST.....	41
6	METODIKA PRAKTICKÉ ČÁSTI.....	42
6.1	POUŽITÁ ANALÝZA.....	43
6.2	VÝBĚR RESPONDENTŮ.....	45
6.3	HW A SW VYBAVENÍ.....	45
7	POPIS CHARAKTERISTICKÝCH PRVKŮ ISMS V BANKOVNICTVÍ.....	47
8	ANALÝZA RIZIK.....	50
8.1	AKTIVA.....	50
8.2	HROZBY.....	53
8.3	SESTAVENÍ MATICE.....	56
9	VÝSLEDKY.....	63
10	OPATŘENÍ.....	75
10.1	VYZRAZENÍ.....	75
10.2	CHYBA V POUŽÍVÁNÍ.....	76
10.3	VZDÁLENÁ ŠPIONÁŽ.....	77
10.4	ODEPŘENÍ ČINNOSTI.....	78
10.5	ODPOSLECH.....	78
10.6	KRÁDEŽ MÉDIÍ NEBO ZAŘÍZENÍ.....	78

10.7	ZÁVAŽNÁ NEHODA.....	79
10.8	ZNIČENÍ ZAŘÍZENÍ.....	80
10.9	PŘETÍŽENÍ INFORMAČNÍHO SYSTÉMU.....	81
10.10	SELHÁNÍ ZAŘÍZENÍ.....	81
10.11	SELHÁNÍ KLIMATIZACE.....	82
	ZÁVĚR.....	83
	SEZNAM POUŽITÉ LITERATURY.....	84
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	86
	SEZNAM OBRÁZKŮ.....	88
	SEZNAM TABULEK.....	89
	SEZNAM PŘÍLOH.....	90

ÚVOD

Práci o managementu bezpečnosti informací v bankovníctví jsem si vybral ze dvou důvodů. Prvním z nich je, že bezpečnost informací je velmi aktuální téma. Bezpečnost informací se ve svém důsledku dotýká každého z nás. Dříve byl pojem bezpečnost informací chápán pouze jako synonymum k pojmu důvěrnost informací a řešení se obvykle omezovalo na technickou stránku (na zabránění nepovoleného přístupu k informacím). Současný přístup bere v úvahu nejen důvěrnost, ale především integritu, dostupnost a důvěryhodnost informací a zabývá se více organizační stránkou věci (managementem). Druhým důvodem je, že díky svému zaměstnání mám znalosti z prostředí bankovníctví, které mohu v této práci zúročit.

Banky bezpečnost informací řešily vždy, zejména kvůli zachování dobrého jména a image banky. Banka, která má dobré řešení bezpečnosti informací, je pro klienty důvěryhodná a ti ji snáze svěří své finance. Se zákonem 181/2014 Sb., o kybernetické bezpečnosti, pro banky nastaly některé nové povinnosti. Řešením se pro povinné instituce (nejen banky) může stát zavedení systému řízení bezpečnosti informací dle normy ČSN ISO/IEC 27001:2014 (dále i jen ISO 27001).

Cílem této diplomové práce je v první, rešeršní, části přiblížit informace o systému řízení bezpečnosti informací a zákonu o kybernetické bezpečnosti, včetně managementu rizik. Management rizik je proces, jehož cílem stanovit a vyhodnotit rizika. V případě systému řízení bezpečnosti informací se jedná o rizika působící na informační aktiva. Mezi základní kroky managementu rizik patří: identifikace rizik, hodnocení rizik a ošetření rizik (případně jejich akceptace). Součástí hodnocení rizik je analýza rizik, jejímž cílem je stanovení úrovně rizika.

Cílem druhé, praktické, části je popsání metodiky praktického postupu, včetně metodiky analýza rizik pomocí metody univerzální matice rizikové analýzy. Popsání specifík systému řízení bezpečnosti informací v bankovním prostředí, zpracování výsledků univerzální matice rizikové analýzy a na jejich základě stanovení nejohroženějších aktiv a nejzávažnějších hrozeb. Tyto hrozby pomocí obecných opatření ošetřím tak, abych snížil riziko působící na aktiva.

I. TEORETICKÁ ČÁST

1 DEFINICE POJMŮ

Stejně jako norma ISO 27001 využívám definice z normy ISO 27000 tam, kde je to možné. V případech, kdy slovník definice neuvádí nebo jsou pro tuto práci málo obsáhlé, jsem pro zpracování těchto pojmů využíval dalších norem pro systém managementu bezpečnosti informací, případně zákon o kybernetické bezpečnosti.

Níže uváděné pojmy jsou spolu propojeny, způsob propojení a vztahy mezi pojmy jsou znázorněny na obrázku 1.

1.1 Systém řízení bezpečnosti informací

Část celkového systému managementu organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. Systém managementu zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje [1].

1.2 Aktivum

Cokoli, co má pro organizaci nějakou hodnotu [1] nebo užitek (také pro její procesy byznysu a jejich kontinuitu). Aktiva potřebují ochranu, aby byly zajištěny korektní procesy byznysu a jejich kontinuita. Aktivum by mělo mít svého vlastníka¹, kterému by měla být přiřazena odpovědnost za udržování příslušných nástrojů řízení bezpečnosti [2, str 11].

Primární aktivum je informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém [3].

Podpůrnými aktivy se rozumí technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému [3].

¹ Pojem vlastník určuje jedince nebo entitu, která má potvrzenou manažerskou odpovědnost za řízení výroby, vývoje, udržování, používání a bezpečnost aktiv [2, str 11].

1.3 Hrozba

Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace [4]. Hrozba k poškození vyžaduje využití jedné nebo více zranitelností systémů, aplikací nebo služeb využívaných organizací. Může mít původ z prostřední uvnitř organizace, ale také z vnějšku [2].

1.4 Zranitelnost

Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami [4]. Zranitelnost sama o sobě nezpůsobuje poškození, jde pouze o okolnost nebo soubor okolností, které mohou umožnit hrozbě, aby se realizovala a zapříčinila poškození aktiv [2].

1.5 Dopad, následek

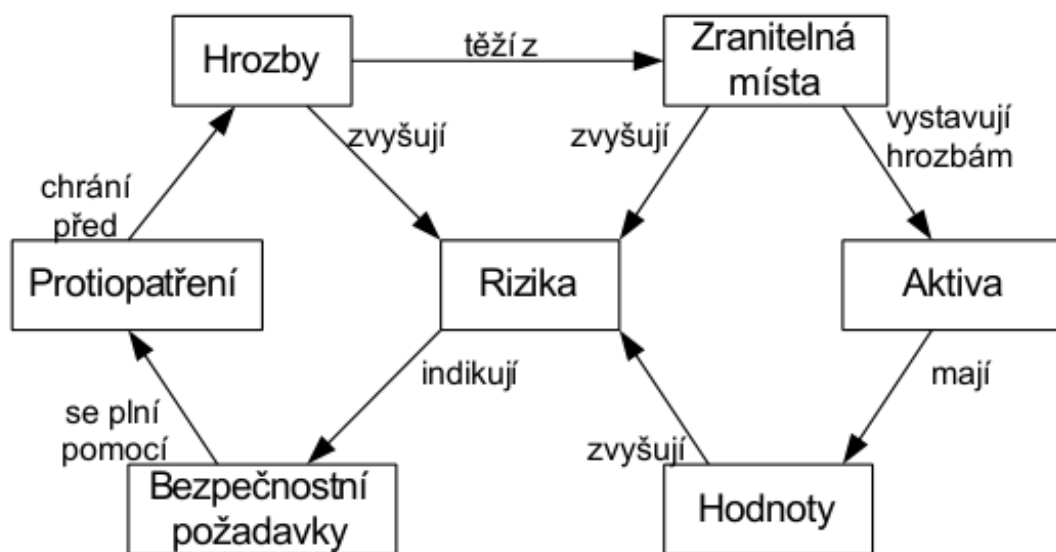
Výsledek události působící na cíle. Následek může být jistý nebo nejistý a v kontextu bezpečnosti informací je obvykle negativní. Jedna událost může vést k celé řadě následků. Ty mohou být vyjádřeny kvalitativně nebo kvantitativně. Počáteční následky se mohou stupňovat v důsledku lavinového efektu [4].

1.6 Riziko

Jedná se o účinek nejistoty na dosažení cílů. Je spojeno s možností, že hrozby využijí zranitelností informačního aktiva nebo skupiny informačních aktiv a způsobí tak organizaci škodu. Často je charakterizováno odkazem na potenciální události a následky nebo na jejich kombinaci. Riziko je často vyjádřeno jako kombinace následků události a s ní související pravděpodobnosti výskytu [4].

1.7 Opatření

Prostředek (řízení) [5] modifikující riziko, zahrnuje jakýkoli proces, politiku, zařízení, obvyklou metodu nebo jiné činnosti, které modifikují riziko [4]. Tato opatření mohou být povahy administrativní, technické, řídicí nebo legislativní [5]. Opatření nemusí vždy vyvolat zamýšlený nebo předpokládaný modifikující účinek [4].



Obr. 1: Vztahy při managementu rizik [6]

2 NORMA ČSN ISO/IEC 27001:2014

V této kapitole se budu zabývat popisem normy ČSN ISO/IEC 27001:2014. Tato norma stanovuje kritéria, podle kterých můžeme určit, zda byl nebo nebyl systém managementu bezpečnosti informací zaveden správně. Norma ČSN ISO/IEC 27001:2014 je rozdělena, včetně úvodu, do jedenácti částí a její nedílnou součástí je normativní příloha. Popisu těchto částí a příloze se věnuji v následujícím textu. Pro snazší orientaci v názvu podkapitol uvádím kurzívou odpovídající názvy kapitol normy ISO 27001.

2.1 Kapitoly 0 až 3 normy

V části 0 *Úvod* je vysvětlen důvod vzniku normy. Tím je poskytnutí požadavků na ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému managementu bezpečnosti informací (Information Security Management System, dále také jako ISMS). Je důležité, že ISMS je součástí procesů a celkové struktury řízení organizace a je do nich integrován [7].

V části 1 *Předmět normy* je definován předmět normy a jeho použití. Norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování ISMS v rámci kontextu organizace. Požadavky této normy je možné aplikovat ve všech organizacích, bez ohledu na jejich velikost, typ a povahu činnosti. Pokud chce organizace dosáhnout shody s touto normou, nelze vyloučit jakékoli požadavky z kapitol 4 – 10 [7].

V kapitole 2 *Citované dokumenty* je uveden odkaz na jedinou normu a to na ISO/IEC 27000 bez udání datace. Je tedy potřeba používat vždy nejnovější vydání tohoto dokumentu [7], což je nyní vydání z roku 2010.

V kapitole 3 *Termíny a definice* je konstatováno, že tato norma používá termíny a definice uvedené v ISO/IEC 27000 [7].

2.2 Kapitola 4 normy *Kontext organizace*

V této kapitole norma říká, že organizace musí určit externí a interní aspekt, který je významný pro záměry této organizace a který ovlivňuje její schopnost dosáhnout zamýšleného výstupu nebo výstupů ISMS. Organizace musí určit zainteresované strany (které mají vztah k ISMS) a požadavky těchto stran relevantní k bezpečnosti informací. Firma musí také stanovit rozsah, hranice a aplikovatelnost ISMS. Tento systém pak musí organizace ustavit, implementovat, udržovat a neustále zlepšovat (v souladu s požadavky

normy) [7].

2.3 Kapitola 5 normy *Vůdčí role*

Tato kapitola se vztahuje k vedení organizace, které musí zajistit stanovení politiky a cílů bezpečnosti informací tak, aby tyto byly slučitelné se strategickým směřováním organizace. Musí také zajistit integraci požadavků ISMS do procesů organizace (včetně zajištění potřebných zdrojů, podpory osob, přiřazení odpovědností a pravomocí apod.) [7]. Bez zapojení managementu organizace nemůže být implementace ISMS úspěšná [6], jedná se tedy o zásadní kapitolu.

2.4 Kapitola 6 normy *Plánování*

Aby bylo možné dosáhnout úspěšného zavedení ISMS, musí organizace plánovat opatření zaměřená na rizika a příležitosti a to, jak tato opatření integrovat, implementovat a vyhodnocovat. Proto musí organizace posuzovat a ošetřovat rizika bezpečnosti informací [7] (v zásadě se jedná o analýzu rizik, která je popsána v této práci v kapitole 4 *Analýza rizik*).

Organizace také musí stanovit cíle bezpečnosti informací a plánovat jejich dosažení. Tyto cíle by měly být v souladu s politikou bezpečnosti informací, brát v úvahu analýzu rizik a být dle potřeby aktualizovány. Pokud je to proveditelné, měly by tyto cíle být měřitelné. Při plánování dosažení těchto cílů musí organizace určit, jaké budou vyžadovány zdroje, kdo bude za plnění cílů odpovědný, do kdy mají být cíle splněny a jakým způsobem budou vyhodnoceny [7].

2.5 Kapitola 7 normy *Podpora*

Tato kapitola je (stejně jako kapitoly předchozí) rozčleněna na několik podbodů, které v rámci přehlednosti představím jednotlivě.

Zdroje

V rámci podpory ISMS musí vedení organizace určit a zajistit zdroje pro úspěšné fungování ISMS [7].

Kompetence

Organizace musí určit nezbytné kompetence osob vykonávajících pro organizaci práci, která má vliv na výkonnost bezpečnosti informací a zajistit, že tyto osoby jsou kompetentní na základě odpovídajícího vzdělání, školení nebo zkušeností (o této kompetenci uchovávat odpovídající dokumentované informace) a případně zajistit potřebná školení [7].

Povědomí

Osoby pracující pro organizaci si musejí být vědomy politiky bezpečnosti informací, svého přínosu k ISMS a důsledků nepřizpůsobení se požadavkům systému řízení bezpečnosti informací [7].

Komunikace

Organizace musí určit potřebu pro interní a externí komunikaci, ve které je zahrnuto o čem, s kým a kdy komunikovat, kdo má komunikovat a procesy, kterými musí být komunikace realizována [7].

Dokumentované informace

ISMS musí zahrnovat dokumentované informace požadované touto normou a takové dokumentované informace, které organizace považuje za nezbytné pro efektivnost systému řízení bezpečnosti informací. Rozsah dokumentovaných informací se tak může v jednotlivých organizacích lišit s ohledem na velikost organizace a typ její činnosti, složitost jejích procesů a kompetenci osob [7].

Nově vytvářené nebo aktualizované dokumentované informace musejí být jednoznačně identifikované a popsány (názvem, datem nebo jednacím číslem), musí být odpovídajícího formátu (grafika, jazyk) a na odpovídajícím médiu. Dokumentované informace musejí být přezkoumané a schválené [7].

Veškeré dokumentované informace vyžadované pro fungování ISMS musejí být řízeny, aby bylo zajištěno, že jsou dostupné pro použití kdykoli a kdekoli je to potřebné, a že jsou chráněné. V rámci řízení dokumentovaných informací je třeba věnovat pozornost distribuci, přístupu, vyhledávání a používání těchto informací, jejich zálohování, řízení změn (například řízením verzí), uchováváním a likvidací těchto informací. Pokud jsou některé dokumentované informace externího původu, i ty musejí být identifikovány a řízeny [7].

2.6 Kapitola 8 normy *Provozování*

Tato kapitola se týká provozování ISMS včetně posuzování a ošetřování rizik bezpečnosti informací. Jsou zde shrnuty požadavky předchozích kapitol, zvláště kapitoly 6. Je zdůrazněna nutnost uchovávat dokumentované informace v nezbytném rozsahu (včetně informací o výsledcích posuzování a ošetření rizik bezpečnosti informací) [7].

2.7 Kapitola 9 normy *Hodnocení výkonnosti*

Hodnocení výkonnosti ISMS se skládá za tří bodů, které jednotlivě popíší.

Monitorování, měření, analýza a hodnocení

Organizace dle této normy musí vyhodnocovat výkonnost bezpečnosti informací a efektivnost systému řízení bezpečnosti informací. Z toho důvodu je potřebu určit, co se bude monitorovat a měřit (včetně procesů a opatření bezpečnosti informací) a stanovit používané metody. Vedení organizace také stanovuje, kdy bude měření (monitorování) prováděno, kdo jej bude provádět, kdy budou vyhodnocovány a analyzovány výsledky a kdo toto vyhodnocení a analýzu bude provádět. O tomto procesu musejí být uchovávány dokumentované informace [7].

Interní audit

Interní audit je prováděn v plánovaných intervalech¹. Důvodem pro jeho provádění je získání informací o tom, zda systém řízení bezpečnosti informací vyhovuje (požadavkům organizace a zároveň požadavkům této normy) a zda je efektivně implementován a udržován. Interní audity musejí mít definovaná kritéria a rozsah, musí být naplánovány programy auditů (včetně četnosti, metod, odpovědností, plánování požadavků a podávání zpráv). Tyto programy musejí brát v úvahu význam příslušných procesů a také výsledky předchozích auditů. Vedení organizace vybírá auditory a zajišťuje provádění auditů tak, aby byly objektivní a nestranné. Výsledky auditů musejí být předloženy odpovídajícím vedoucím pracovníkům. O programu a výsledcích auditu musejí být uchovávány dokumentované informace [7].

Přezkoumání vedením organizace

Vrcholové vedení organizace musí v plánovaných intervalech² přezkoumávat ISMS pro zajištění jeho neustálé efektivnosti, přiměřenosti a vhodnosti. Přezkoumání musí brát

¹ Obvykle jedenkrát ročně

² Obvykle jsou intervaly shodné s intervaly interního auditu

v úvahu celou řadu vstupů, například:

- stav opatření z předchozích přezkoumání vedením organizace
- změny v externím a interním aspektu, které jsou relevantní pro ISMS
- zpětnou vazbu na výkonnost bezpečnosti informací, včetně
 - neshod a nápravných opatření
 - výsledků monitorování a měření
 - výsledků auditů¹
 - naplnění cílů bezpečnosti informací
- zpětnou vazbu od zainteresovaných stran²

Výstupy z přezkoumání vedením organizace musí zahrnovat rozhodnutí vztahující se k příležitostem neustálého zlepšování a k jakýmkoli potřebám pro změny v ISMS. O přezkoumání vedením musejí být uchovávané dokumentované informace [7].

2.8 Kapitola 10 normy *Zlepšování*

Organizace musí neustále zlepšovat vhodnost, přiměřenost a efektivnost systému řízení bezpečnosti informací. Jedním z prostředků jsou nápravná opatření. Při výskytu neshody na ni musí organizace reagovat a, pokud je to možné, přijmout opatření k jejímu řízení a nápravě (a také se zabývat následky). Je nutné vyhodnotit potřebu pro opatření k odstranění příčin neshody tak, aby se znovu nevyskytla. To se děje prostřednictvím přezkoumání neshody, určení jejích příčin a zjištění, zda existují obdobné neshody nebo zda by se mohly vyskytnout. Následně je potřeba implementovat příslušná opatření, přezkoumat jejich efektivnost a případně provést změny v systému řízení bezpečnosti informací. Nápravná opatření musejí být přiměřená dopadům neshod, kterým čelí. O neshodách a výsledcích nápravných opatření je potřeba uchovávat dokumentované informace [7].

2.9 Normativní příloha A

Cíle opatření a jednotlivá bezpečnostní opatření uvádí norma v přehledné tabulce. Konkrétní cíle a konkrétní opatření jsou vybírána v rámci procesu zavádění systému řízení bezpečnosti informací. Cíle opatření a jednotlivá opatření se zabývají těmito tématy: politikou

¹ Interních i externích

² Například zákaznické audity

bezpečnosti informací, organizací bezpečnosti informací, bezpečností lidských zdrojů, řízením aktiv, řízením přístupu, kryptografií, fyzickou bezpečností a bezpečností prostředí, bezpečností provozu, bezpečností komunikace, akvizicí, vývojem a údržbou systémů, dodavatelskými vztahy, řízením incidentů bezpečnosti informací, aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací a souladem s požadavky¹ [7].

1 Právními a smluvními

3 ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

Zákon 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, zkráceně zákon o kybernetické bezpečnosti (dále také jako ZKB), je platný od 1.1.2015 [3]. K tomuto zákonu se v základu vztahují tyto tři dokumenty:

- nařízení vlády 315/2014 Sb. z 8.12.2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury;
- vyhláška 316/2014 sbírky z 15.12.2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti);
- vyhláška 317/2014 sbírky z 15.12.2014 o významných informačních systémech a jejich určujících kritériích.

Z nařízení vlády 315/2014 sbírky části VII. Finanční trh a měna jednoznačně vyplývá, že se zákon o kybernetické bezpečnosti týká části bank, a to konkrétně tehdy, pokud přesahuje tržní podíl tohoto subjektu 10% z bilanční sumy bankovního sektoru, a v případě pojišťoven, pokud přesahuje tržní podíl tohoto subjektu měřený objemem předepsaného pojistného 25% [8]. Z pohledu tohoto nařízení je část tuzemských bank (Česká spořitelna, Komerční banka, ČSOB) součástí kritické infrastruktury.

3.1 Pojmy používané zákonem o kybernetické bezpečnosti (hlava I)

V této kapitole uvedu některé pojmy, které definuje ZKB. Pojmy, které jsou pro ISMS základní, jsou definovány v kapitole 1 *Pojmy*.

- *kybernetický prostor* – digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací
- *bezpečnost informací* - zajištění důvěrnosti, integrity a dostupnosti informací
- *bezpečnostní událost* - událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací
- *bezpečnostní incident* - narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických

komunikací v důsledku kybernetické bezpečnostní události

- *přijatelné riziko* - riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik
- *bezpečnostní politika* - soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv orgánem a osobou uvedenou v § 3 písm. c) až e) zákona
- *garant aktiva* - fyzická osoba pověřená orgánem nebo osobou uvedenou v § 3 písm. c) až e) zákona k zajištění rozvoje, použití a bezpečnosti aktiva
- *řízení rizik* - činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládnutí rizik, sdílení informací o riziku a sledování a přezkoumání rizik
- *hodnocení rizik* - proces, při němž je určována významnost rizik a jejich přijatelná úroveň,
- *kritická informační infrastruktura* – prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti,
- *významný informační systém* – informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci
- *správce informačního systému* – orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému
- *správce komunikačního systému* – orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování,
- *významná síť* – síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře

3.2 Porovnání pojmů

Pro porovnání používání základních pojmů (viz kapitola 1 Pojmy) normami ISMS a ZKB slouží tabulka 1.

<i>Název</i>	<i>Definice norem ISMS</i>	<i>Definice ZKB</i>
Systém řízení bezpečnosti informací	Část celkového systému managementu organizace založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. Systém managementu zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje [1].	Část systému řízení (povinných orgánů a osob dle ZKB) založená na přístupu k rizikům informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, která stanoví způsob ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací [3]
Aktivum	Cokoli, co má pro organizaci nějakou hodnotu [1] nebo užitek (také pro její procesy byznysu a jejich kontinuitu)[2, str. 11].	Primární aktivum a podpůrné aktivum [3]
Hrozba	Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace [4].	Potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva [3]
Zranitelnost	Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami [4].	Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami [3].

<i>Název</i>	<i>Definice norem ISMS</i>	<i>Definice ZKB</i>
Riziko	Jedná se o účinek nejistoty na dosažení cílů. Je spojeno s možností, že hrozby využijí zranitelností informačního aktiva nebo skupiny informačních aktiv a způsobí tak organizaci škodu [4].	Možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození aktiva [3]
Opatření	Prostředek (řízení) [5] modifikující riziko, zahrnuje jakýkoli proces, politiku, zařízení, obvyklou metodu nebo jiné činnosti, které modifikují riziko [4].	Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru [3].

Tabulka 1: Porovnání pojmů, zdroj: vlastní

3.3 Další hlavy a části zákona o kybernetické bezpečnosti

3.3.1 Hlava II

V hlavě II tohoto zákona jsou popsány systémové postupy pro zajištění kybernetické bezpečnosti a to pomocí bezpečnostních opatření, která jsou rozdělena na dvě skupiny: organizační a technická opatření. Mezi organizační opatření patří například systém řízení bezpečnosti informací, řízení aktiv, bezpečnost lidských zdrojů atd. Mezi technická opatření jsou zařazené například nástroje na ochranu integrity komunikačních sítí, nástroje pro řízení přístupových oprávnění nebo kryptografické prostředky [3].

Konkrétní obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace a rozsah bezpečnostních opatření stanovuje prováděcí předpis [3].

Dále se hlava II věnuje pojmům kybernetická bezpečnostní událost a kybernetický bezpečnostní incident, jejich hlášení, evidenci a opatřením. Opatření může být trojího typu:

varování, reaktivní opatření a ochranné opatření [3].

Hlava II definuje kontaktní údaje a specifikuje, kterým orgánům je nutné tyto údaje oznamovat. Vymezuje také fungování a činnosti národního CERTu včetně provozovatele (se kterým musí být uzavřena veřejnoprávní smlouva). Mezi činnosti národního CERTu patří například vyhodnocování kybernetických bezpečnostních incidentů, poskytování metodické podpory, přijímání hlášení o kybernetických bezpečnostních incidentech apod. Poslední část hlavy II se věnuje vládnímu CERTu jako součásti Národního bezpečnostního úřadu [3].

3.3.2 Hlava III

Hlava III definuje stav kybernetického nebezpečí jako stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Národního bezpečnostního úřadu a tato informace je zveřejněna pomocí rozhlasového a televizního vysílání. Tento stav je možné vyhlásit na dobu nejdéle sedmi dnů, lze ji však prodloužit, ne více než na 30 dní [3].

3.3.3 Hlava IV

Hlava IV se týká státní správy, kterou vykonává Národní bezpečnostní úřad, který například: stanovuje bezpečnostní opatření, vede evidence podle tohoto zákona, působí jako koordinační orgán ve stavu kybernetického nebezpečí, zajišťuje mezinárodní spolupráci, zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti apod. [3].

3.3.4 Hlava V

Hlava V se věnuje kontrole, nápravným opatřením a správním deliktům. Kontrolu v této oblasti vykonává Národní bezpečnostní úřad. Ten stanovuje nápravná opatření, může zakázat používání kritické informační infrastruktury nebo významných informačních systémů v případě, kdy jsou tyto přímo ohroženy (pro nedostatky) kybernetickým bezpečnostním incidentem, do té doby, než bude zjištěný nedostatek odstraněn. Dále jsou popisovány správní delikty, mezi které patří například: nesplnění za stavu kybernetického nebezpečí

povinností uložených Národním bezpečnostním úřadem, nesplnění povinností uložených nápravným opatřením, neohlášením kybernetického bezpečnostního incidentu apod. [3].

3.3.5 Hlava VI a další části ZKB

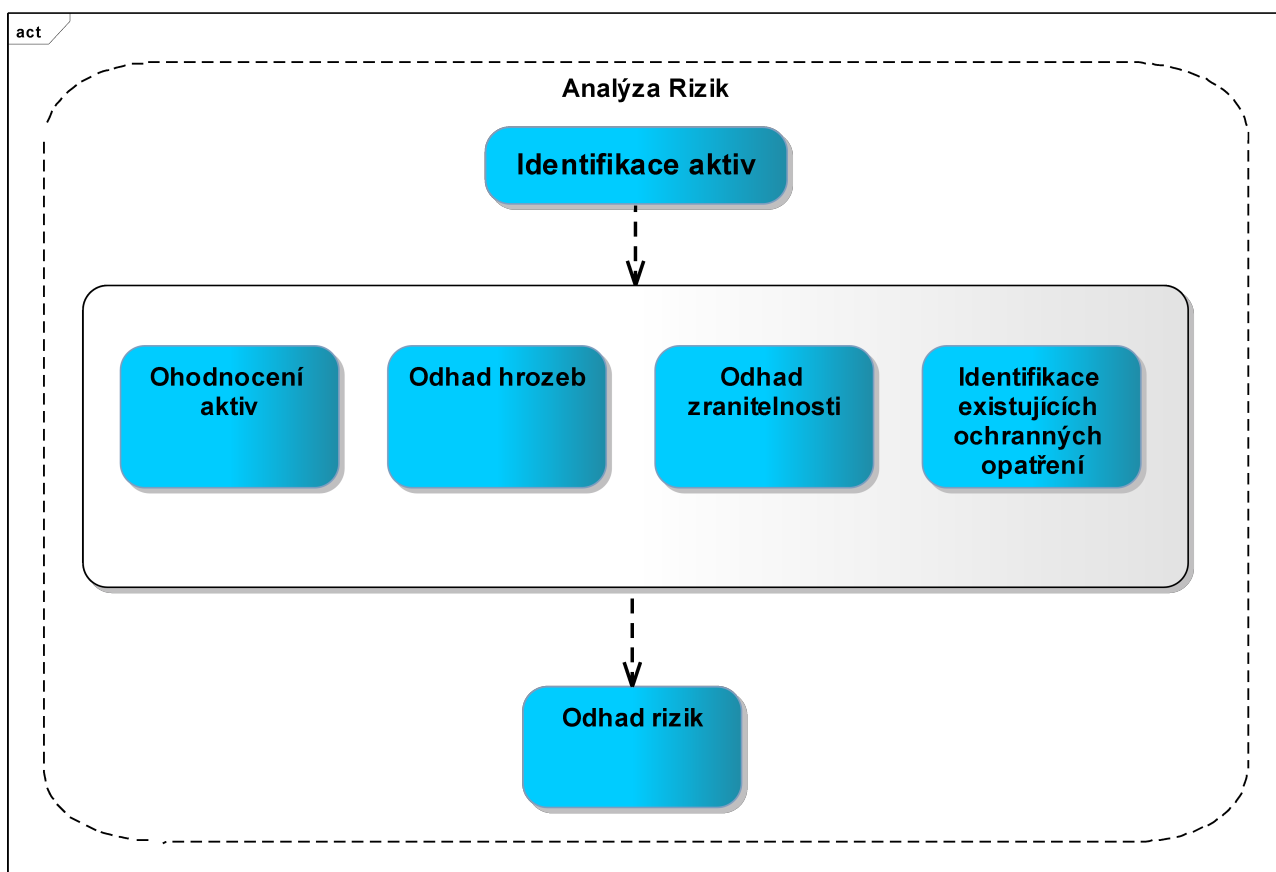
V hlavě VI jsou závěrečná ustanovení: zmocňovací, přechodná a společná [3].

V dalších částech zákona jsou změny zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, změna zákona o elektronických komunikacích, změna zákona o svobodném přístupu k informacím, změna zákona o provozování rozhlasového a televizního vysílání, a v poslední šesté části začátek účinnosti, který je 1. ledna 2015 [3].

4 ANALÝZA RIZIK

Je proces, který je součástí celkového managementu rizika (viz kapitola 5 *Management rizik*). Jde o „proces pochopení podstaty rizika a stanovení úrovně rizika. Analýza rizika poskytuje základ pro hodnocení rizik a pro rozhodnutí o ošetření rizika a zahrnuje také odhad rizika [5].“ Je nutnou podmínkou rozhodování o riziku [9, s. 119].

Analýza rizika by měla zahrnovat tyto kroky: identifikaci aktiv, identifikaci právních a businessových požadavků (významných pro identifikaci aktiv), ocenění aktiv, identifikaci významných hrozeb a zranitelností, posouzení pravděpodobnosti výskytu hrozeb a zranitelností [2]. V praxi se často využívá podobný model, který sestává z těchto kroků (obrázek 2): identifikace aktiv, ohodnocení aktiv, odhad hrozeb, odhad zranitelností, identifikace existujících ochranných opatření a odhad rizik [6]



Obr. 2: Kroky analýzy rizik [6]

4.1 Identifikace aktiv

Stanovení rozsahu

Pro správnou identifikaci aktiv je nejprve nutné stanovit rozsah řízení rizik a hranice řízení rizik [5]. Stanovení rozsahu jako takové patří do celkového managementu rizika, bylo by ale nesprávné tento krok opomenout, protože je nutnou vstupní podmínkou pro správnou a úplnou identifikaci aktiv, zranitelností, hrozeb a stávajících opatření.

Identifikace aktiv

Po stanovení rozsahu je nutné identifikovat všechna (informační) aktiva, která mají pro společnost nějakou hodnotu. Identifikace aktiv by měla být provedena na vhodném stupni podrobnosti. Zároveň by pro každé aktivum měl být identifikován jeho vlastník. Výstupem tohoto procesu je seznam aktiv, u kterých musí být zajištěno řízení rizik [5].

Jedním z nejdůležitějších a nejcennějších typů aktiva jsou informace. Ty je třeba chránit bez ohledu na to, jakou mají formu (databáze, datové soubory, systémová dokumentace, smlouvy, manuály, školicí materiály, směrnice, plány kontinuity, výsledky bussinessu). Mezi aktiva také zahrnujeme procesy a služby, software, fyzické položky (včetně hardware, technického vybavení a nábytku), a také lidí (zaměstnance, zákazníky) [2], dále například schopnost vytvářet a poskytovat produkty (know-how) nebo image firmy [6].

4.2 Ohodnocení aktiv

Hodnotu aktiv určujeme z hlediska jejich důležitosti pro klíčové procesy organizace, právních požadavků, požadavků prostředí byznysu a výsledných dopadů při ztrátě jejich důvěrnosti, integrity a dostupnosti [2].

Z předchozího kroku máme pro každé aktivum určeného vlastníka¹, který by měl být schopen posoudit důležitost daného aktiva. Vlastník aktiva by měl přezkoumávat, zda hodnota identifikovaného aktiva odpovídá jeho stávající hodnotě [2].

Je dobré určit hodnotu (a tedy potenciální dopad při ohrožení aktiva) pro každou vlastnost aktiva (důvěrnost, dostupnost, integrita a případně další) zvlášť, neboť tyto hodnoty jsou nezávislé a mohou se u každého aktiva lišit. Hodnoty aktiv se obvykle rozdělují do kategorií, například: nízká, střední a vysoká hodnota aktiva nebo zanedbatelná, nízká, střední, vysoká a velmi vysoká hodnota aktiva [2]. Hodnota aktiva se obvykle stává součástí sezna-

¹ Tento pojem určuje jedince/entitu, která má potvrzenou manažerskou odpovědnost [2]. Vlastník nemusí mít k aktivu vlastnická práva, ale má přiměřenou odpovědnost za jeho používání a bezpečnost [5]

mu aktiv, může být uváděna na škále a nebo vyjádřena např. v korunách [6].

4.3 Identifikace právních a bussinessových požadavků

Bezpečnostní požadavky v organizaci jsou, bez ohledu na její velikost, obvykle odvozené ze tří zdrojů:

- soubor hrozeb a zranitelností, který je jedinečný pro každou organizaci
- právní, zákonné a smluvní požadavky
- soubor zásad, cílů a požadavků na zpracování informací, který organizace vytvořila pro podporu své činnosti, je pro každou organizaci jedinečný

V procesu ocenění aktiv je nutné brát na tyto požadavky ohled a formulovat je ve smyslu požadavků na důvěrnost, integritu a dostupnost [2].

4.4 Odhad hrozeb

Pro každé aktivum je nutné identifikovat možné hrozby, často se vychází ze seznamů hrozeb, které jsou uvedeny například v ČSN 369790 (příloha C) nebo v ČSN ISO/IEC 27005 (příloha C).

Hrozba může způsobit nežádoucí incident, který může mít za následek poškození organizace a jejích aktiv. Hrozby mohou vzniknout jak z intencionálních, tak z neintencionálních příčin nebo událostí. Aby bylo poškozeno aktivum, musí hrozba využít jednu nebo více zranitelností aktiv. Hrozby mohou být interní i externí [2].

Vstupem pro identifikace hrozeb jsou informace o hrozbách získané z přezkoumání (bezpečnostních) incidentů, od vlastníků aktiv, od uživatelů a z jiných zdrojů (katalog hrozeb) [5]. Po identifikaci hrozeb (a zranitelností) je nutné posoudit pravděpodobnost, že dojde k jejich průniku a vytvoření rizika. Přitom bychom měli vzít v úvahu úmyslné hrozby, náhodné hrozby, minulé incidenty, nový vývoj a trendy [2].

Výstupem z tohoto procesu by měl být seznam hrozeb s identifikací jejich typu a zdroje hrozby [5], příklad viz tabulka 2.

Hrozba	Typ	Zdroj
Požár	Fyzické poškození	Náhodný, úmyslný, environmentální
Krádež zařízení	Ohrožení informací	úmyslný
Vyzrazení	Ohrožení informací	Náhodný, úmyslný
Přerušeni dodávky elektřiny	Ztráta základních služeb	Náhodný, úmyslný, environmentální
Nedostatek personálu	Ohrožení funkčnosti	Náhodný, úmyslný, environmentální
Chyba údržby	Technické selhání	Náhodný, úmyslný

Tabulka 2: Příklad seznamu hrozeb [5]

4.5 Identifikace existujících ochranných opatření

Identifikace stávajících opatření je důležitá, aby nedocházelo k duplikaci opatření, aby se odhalila stávající špatně fungující opatření¹ a aby byla odhalena opatření bez zranitelných míst [5].

Vstupem pro identifikaci stávajících opatření je jejich dokumentace a případně implementační plány ošetření rizik. V tomto kroku se kromě stávajících opatření identifikují i opatření plánovaná. V průběhu tohoto kroku se přezkoumávají dokumentované informace o stávajících opatřeních, probíhá kontrola s odpovědnými pracovníky a uživateli, dále také přezkoumání fyzických opatření na místě a případně přezkoumání výsledků interních auditů (pokud jsou již prováděny) [5].

Výsledkem tohoto procesu by měl být seznam existujících a plánovaných opatření, jejich zavedení a stav užívání těchto opatření [5].

4.6 Odhad zranitelnosti

Zranitelnost je slabé místo, které je spojené s aktivy organizace. Zranitelnost sama o sobě nezpůsobuje poškození. Identifikace zranitelností určuje slabá místa pro jednotlivá aktiva. [2].

Vstupem pro odhad zranitelností je seznam známých hrozeb, seznam aktiv a existujících opatření. V průběhu procesu by měly být identifikovány ty zranitelnosti, které mohou být zneužity hrozbami (a být tak způsobena škoda aktivům a organizaci) [5]. Příklady zrani-

¹ Nefungující bezpečnostní opatření může být zdrojem zranitelnosti [5].

telností a hrozeb, které je mohou využít, jsou uvedeny v tabulce 3.

Skupina	Příklad zranitelnosti	Příklad (pronikající) hrozby
Hardware	Citlivost na změny teploty	Meteorologický jev, požár
Software	Neprovádění logování událostí	Zneužití oprávnění
Zaměstnanci	Nedostatečná kontrola práce externích zaměstnanců/zaměstnanců zabezpečujících úklid	Krádež médií nebo dokumentů
Lokality	Poloha v zátopové oblasti	Povodeň
Sítě	Přenos odkrytých hesel	Vzdálená špionáž
Organizace	Nedostatečný formální postup při registraci a zrušení registrace uživatele	Zneužití oprávnění
Organizace	Nedostatky ve formální postupech pro autorizaci veřejně přístupných informací	Data pocházející z nedůvěryhodných zdrojů

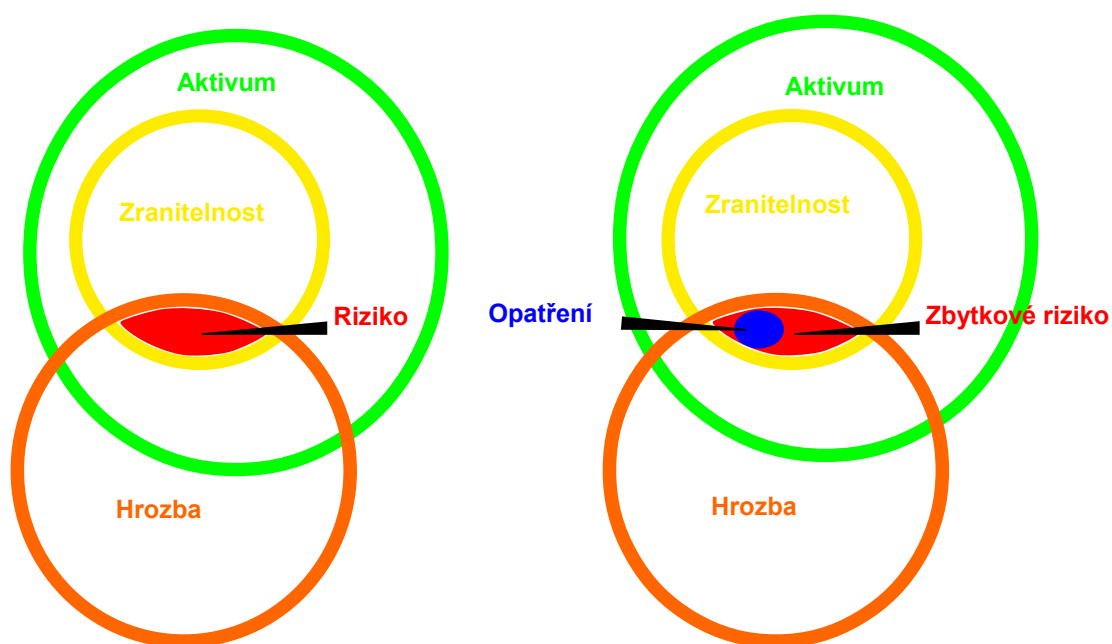
Tabulka 3: Příklad seznamu zranitelností [5]

4.7 Identifikace následků

Vstupem pro identifikaci následků je seznam aktiv, seznam procesů a seznam hrozeb a zranitelností. V průběhu této činnosti jsou identifikovány ty následky, které mohou pro aktivum znamenat ztrátu integrity, důvěrnosti nebo dostupnosti. Následkem může být například: ztráta pověsti, nepříznivé provozní podmínky, finanční ztráta apod [5].

4.8 Odhad rizik

Odhad rizika se provádí některou z metod analýzy rizik, viz kapitola 4.9 této práce. Riziko vznikne, pokud se hrozba setká se zranitelností, kterou může proniknout. I po ošetření zranitelností může zůstat zbytkové riziko, viz obrázek 3.



Obr. 3: Vztahy aktivum, hrozba, zranitelnost, riziko, opatření [10]

Praktickým příkladem situace vyobrazené na obrázku 3 je následující situace: Pro aktivum zaměstnance je jednou ze zranitelností možnost onemocnět chřipkou, hrozbou je nákaza a rizikem je nemoc pracovníka. Opatřením je očkování proti chřipce, zbytkovým rizikem je onemocnění jiným typem chřipky, než na kterou byl zaměstnanec očkovan.

4.9 Metody analýzy rizik

Při provádění analýzy rizik je důležité určit vhodnou metodu. Metody analýzy rizik jde rozdělit do dvou základních skupin: na kvalitativní a kvantitativní. U kvalitativních metod bývá míra rizika vyjádřena na určité škále nebo je hodnocena slovním popisem. Kvantitativní metody jsou založeny na matematickém výpočtu rizika [6] a jejich výsledkem je míra rizik vyjádřená číselně.

Expertní metody stojí na pomezí mezi kvalitativními a kvantitativními analýzami rizik. Vyjadřují verbální nebo numerický názor na analyzovaný problém. Mezi tyto metody patří například: analýza co – kdyby¹, FMEA, SWOT a UMRA [9]. V následujícím textu se budu věnovat analýzám SWOT a FMEA. Expertní metoda UMRA je popsána v praktické části této diplomové práce.

¹ Anglicky what – if analysis, hledá závěry, (co by se stalo) k předpokládaným rizikům (kdyby).

4.9.1 SWOT

Název je akronymem z anglických slov Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti), Threats (hrozby). Tato analýza pracuje s předpokladem, že riziko může být buď hrozbou, nebo příležitostí. Jejím cílem je získat přehled o možnosti, jak snížit pravděpodobnost hrozby a zvýšit pravděpodobnost příležitosti. Podmínkou je, aby experti, kteří tuto analýzu zpracovávají, měli podrobnou znalost dané problematiky. Výstupem této analýzy nejsou rizika, ale spíše možné postupy [9]. Příklad tabulky SWOT analýzy je uveden na obrázku 4.

		Interní analýza	
		S: Silné stránky	W: Slabé stránky
Externí analýza	O: Příležitosti	S-O strategie Vývoj nových metod, které jsou vhodné pro rozvoj silných stránek společnosti (projektu)	W-O strategie Odstranění slabín pro vznik nových příležitostí.
	T: Hrozby	S-T strategie Použití silných stránek pro zamezení hrozeb.	W-T strategie Vývoj strategií, díky nimž je možné omezit hrozby, ohrožující naše slabé stránky.

Obr. 4: SWOT analýza [10]

4.9.2 FMEA

Název je, stejně jako u metody SWOT, akronymem anglických slov Failure Mode and Effect Analysis (analýza možného výskytu a vlivu vad). Jde patrně o nejpoužívanější expertní metodu analýzy rizik. Probíhá ve dvou fázích. Ve verbální fázi se experti zaměřují na identifikaci možného vzniku poruch, možných způsobů poruch a možných následků poruch. V numerické fázi probíhá tříparametrický odhad rizika s využitím indexu RPN (Risk Priority Number). Ten lze spočítat dle vzorce (doplň vzorec) $RPN = C * PV * PO$ kde

- C = cena, význam, závažnost rizika
- PV = pravděpodobnost výskytu rizika

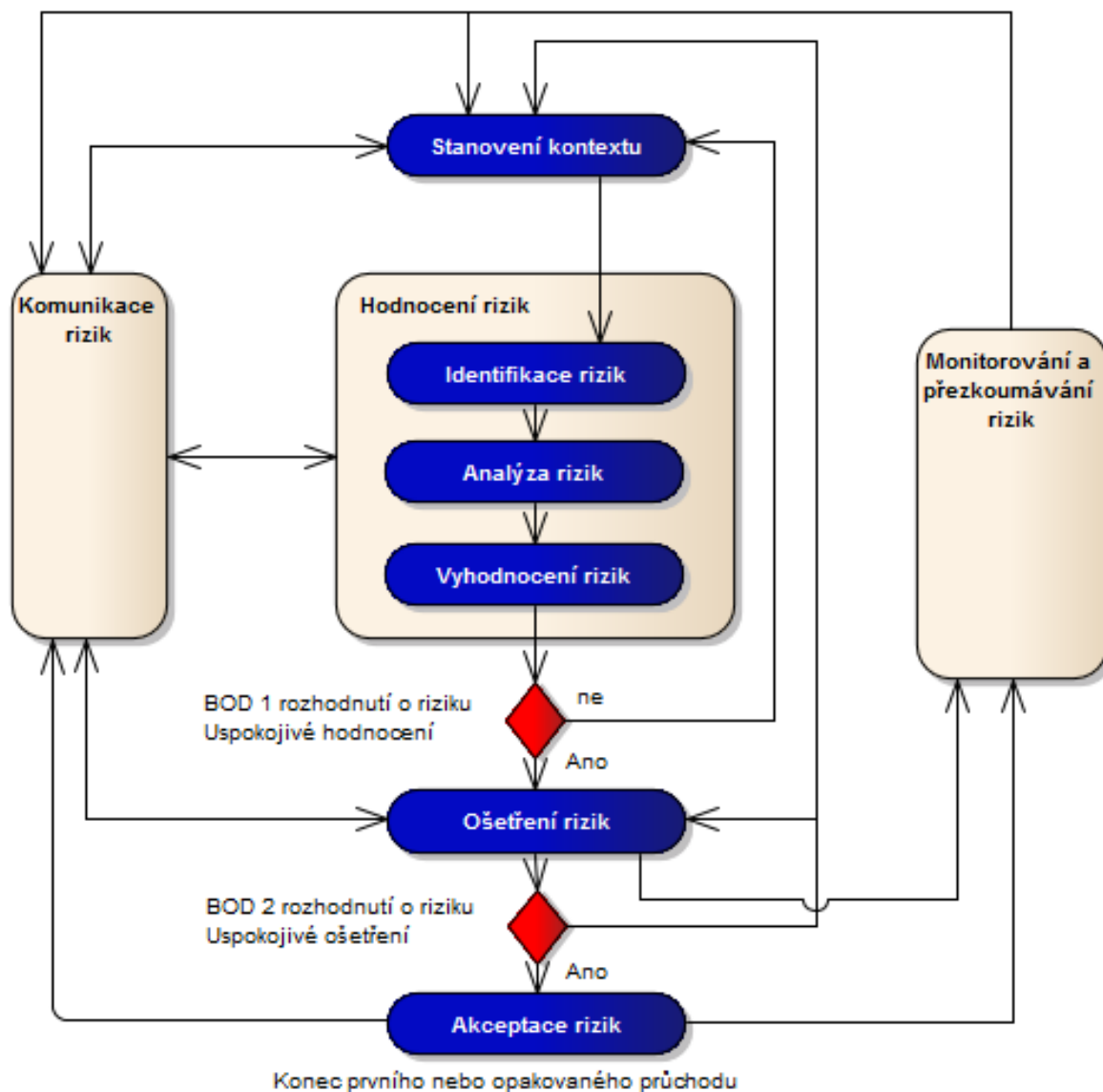
- PO = pravděpodobnost odhalení rizika

Pro každou z těchto kategorií je určena numerická stupnice významnosti, ve které nejpříznivější stav má nejnižší číselnou hodnotu, obvykle se využívá stupnice od 1 do 5. Nejnižší hodnotou nesmí být nikdy 0 [9]. Příklad této analýzy je tabulka 4. Analýza je provedena pro aktivum: operační systém linux. Čísla uvedená v tabulce pro výpočet RPN jsou v následujícím pořadí: hodnota aktiva, vyhodnocení opatření a závažnost hrozby. Zeleně označené položky splňují akceptační kritéria, červeně označené položky bylo nutné ošetřit a ke žlutě označeným se vyjádřil management organizace [10].

	Data z nedůvěryhodných zdrojů	Chyba údržby	Neoprávněné použití zařízení	Poškození dat	Chyba v používání	Zneužití oprávnění
Nesprávný pracovní postup	2*2*2=8	2*3*3=18	x	2*3*1=6	2*2*4=16	2*4*4=32
Znamé chyby SW	x	x	2*4*2=16	2*2*1=4	2*5*1=10	x
Chybné přiřazení přístupových práv	2*5*1=10	x	2*5*1=10	2*2*2=8	2*5*3=30	x
Neznámé chyby SW	x	x	2*5*1=10	2*5*3=10	2*5*1=10	x
Nespokojený pracovník	2*5*3=30	x	x	2*5*3=30	x	2*5*5=50
Neznámé chyby HW	x	x	x	2*5*1=10	x	x
Chybné nastavení zařízení	x	2*3*4=24	x	2*2*1=4	2*3*1=6	2*5*1=10
Chybné používání zřízení	x	x	x	2*2*2=8	x	x

Tabulka 4: Ukázka analýzy rizik metodou FMEA [10]

5 MANAGEMENT RIZIK



Obr. 5: Proces managementu rizik [5]

Celkový management rizika zahrnuje tyto kroky: stanovení kontextu, hodnocení rizik (součástí tohoto kroku je analýza rizik), komunikaci rizik, případné ošetření rizik, monitorování a přezkoumávání rizik a případnou akceptaci rizika [5]. Vztahy těchto kroků jsou ukázány na obrázku 1. Protože i v managementu rizik se (stejně jako v systémech managementu bezpečnosti informací) využívá PDCA cyklus, je možné průchod znázorněný na obrázku 5 opakovat tak, aby neustále docházelo ke snižování rizik, a tím ke zvyšování bezpečnosti.

5.1 Stanovení kontextu

Stanovení kontextu zahrnuje určení základních kritérií, definuje rozsah a hranice a stanovuje organizační strukturu [5].

5.1.1 Určení základních kritérií

Základní kritéria jsou následující:

- *Přístup k řízení rizik* – přístup k řízení rizik by měl být vybrán a vhodně přizpůsoben, zároveň by vedení organizace mělo zhodnotit, zda jsou k dispozici dostatečné zdroje [5].
- *Kritéria hodnocení rizik* – tato kritéria by měla zohledňovat strategické hodnoty procesu informací, kritičnost informačních aktiv, legislativní a jiné požadavky, důležitosti dostupnosti, důvěrnosti a integrity provozu a obchodních činností a očekávání a představy zainteresovaných stran [5].
- *Kritéria dopadu* – měla by být specifikována na základě stupně škod nebo ztrát organizace způsobených bezpečnostní událostí s ohledem na poškozené provozy, ztrátu činností organizace, finanční hodnoty, narušení bezpečnosti informací, úroveň klasifikace ovlivněného aktiva, poškození pověsti apod [5].
- *Kritéria akceptace rizik* – organizace by pro akceptaci rizik měla definovat své vlastní škály, včetně prahových úrovní. Pro různé třídy rizik mohou platit různá kritéria jejich akceptace [5].

5.1.2 Rozsah a hranice

Rozsah proce řízení rizik bezpečnosti informací musí být definován tak, aby bylo zajištěno, že při posouzení rizik jsou brána v úvahu všechna příslušná aktiva. Hranice určujeme, abychom byli schopni identifikovat rizika, která by mohla tyto hranice prolomit [5].

Vstupem pro stanovení rozsahu a hranic může být úvodní audit systému managementu bezpečnosti informací, dalšími vstupy jsou souhrn informačních aktiv [6], rozvaha vedení organizace a návrhy odborného konzultanta.

Při definování rozsahu a hranic by měla organizace přihlížet k těmto informacím:

- strategické obchodní cíle, strategie a politiky organizace,
- obchodní procesy,

- funkce a struktura organizace,
- právní, regulatorní a smluvní požadavky platné pro organizaci
- politika ISMS
- přístup organizace k řízení rizik
- informační aktiva
- sídlo organizace, geografické charakteristiky
- omezení ovlivňující organizaci
- sociální a kulturní prostředí a další [5]

Organizace by měla poskytnout odůvodnění pro všechna vyloučení z tohoto rozsahu. Příkladem rozsahu může být: aplikace, IT infrastruktura, obchodní proces, definovaná část organizace [5] nebo celá organizace.

5.1.3 Organizační struktura

Pro proces řízení rizik bezpečnosti informací by měla být stanovena a udržována organizace a odpovědnosti. Hlavními rolemi a odpovědnostmi jsou

- rozvoj procesu ISMS
- identifikace a analýza zainteresovaných stran
- definování rolí a odpovědností
- stanovení požadovaných vztahů apod [5].

Tato organizační struktura by měla být schválena příslušnými managery organizace. Lze ji chápat jako jeden ze zdrojů¹, které vyžaduje ISO 27001² [5].

5.2 Posouzení rizik bezpečnosti informací

Posouzení rizik sestává ze tří navazujících činností: identifikace rizik, analýza rizik a hodnocení rizik. První dva kroky popisují v kapitole 4 Analýza rizik, zde pro úplnost uvádím krátké shrnutí těchto kroků.

¹ Jedná se o zdroje nutné pro ustavení, zavedení, provozování, monitorování, přezkoumávání, udržování a zdokonalování ISMS [5].

² V normě ČSN ISO/IEC 27005:2011 je uvedena norma 27001:2005, shodné požadavky lze najít i v aktuální normě (ČSN ISO/IEC 27001:2014).

Identifikace rizik

Cílem identifikace rizik je určit, co by se mohlo stát, aby byla způsobena potenciální ztráta a zjistit, jak, kde a proč může ke ztrátě dojít. V této části probíhá identifikace aktiv, hrozeb, střetávajících opatření, zranitelností a následků.

Analýza rizik

V rámci tohoto probíhá analýza rizik vhodně zvolenou metodou. Obvykle se skládá z těchto činností (záleží ale na vybrané metodě): posouzení následků, určení pravděpodobnosti incidentu, určení úrovně rizik [5]. Tyto činnosti často neprobíhají samostatně, ale jako jeden celek v rámci vybrané metody analýzy rizik.

Hodnocení rizik

Při hodnocení rizik porovnáváme úroveň rizik s kritérii pro jejich hodnocení a s akceptačními kritérii. Pokud dojde k nahromadění většího množství nízkých nebo středních rizik, může se celkově zvýšit míra rizika. Při hodnocení rizik bychom měli zvažovat vlastnosti bezpečnosti informací (pokud například není důležitá ztráta důvěrnosti, pak rizika vyúsťující v její ztrátu nemusejí být důležitá) a důležitost procesu nebo aktiv ohrožených rizikem – méně důležitým procesům a aktivům je možné věnovat menší pozornost. Výsledkem hodnocení rizik by měl být seznam rizik se stanovenou prioritou [5].

5.3 Ošetření rizik

V rámci ošetření rizik by měla být vybrána opatření k redukci, akceptaci, vyhnutí se nebo sdílení rizik a měl by být zároveň definován plán ošetření rizik [5]. Činnost ošetření rizik je znázorněna v příloze 1.

Způsob ošetření rizik by se měl vybírat na základě výstupů z předchozích kroků, očekávaných nákladů na implementaci ošetření a očekávaných přínosech. Některé způsoby ošetření rizik mohou řešit více než jedno riziko. V rámci plánu na ošetření rizik by měly být stanoveny priority a jednotlivé způsoby ošetření rizik, včetně časového rámce. Někdy může být výhodné odstranit nadbytečná nebo zbytečná opatření (zejména pokud jsou vysokonákladová). Zároveň s plánem ošetření rizik by měla být určena zbytková rizika, to může vyžadovat opakované posouzení rizik. Pokud i přes ošetření zbytkové riziko nesplňuje kritéria nastavená managementem organizace pro akceptaci rizik, může být nutné zvážit další ošetření [5].

Norma ISO 27005 nabízí čtyři volby pro ošetření rizik:

- *Modifikace rizik* - vybírají se taková opatření/dochází k úpravě stávajících opatření tak, aby výsledné riziko bylo pro organizaci akceptovatelné. Může se jednat i o odstranění stávajícího opatření nebo nahrazení stávajícího opatření novým [5].
- *Podstoupení (akceptace) rizik* – pokud úroveň (míra) rizika splňuje akceptační kritéria, není nutné přijímat další opatření a riziko lze podstoupit. Podklady pro tento krok jsou získány analýzou rizik [5].
- *Vyhnutí se riziku* – tento způsob ošetření rizika se uplatňuje, pokud jsou identifikovaná rizika příliš vysoká nebo náklady na jiný způsob ošetření rizik převyšují přínosy. Organizace upustí od plánované nebo stávající činnosti nebo změní její podmínky tak, aby se riziku vyhnula [5].
- *Sdílení rizik* – jde o sdílení rizika s externími stranami. Tento způsob ošetření ale může vytvářet rizika nová. Příkladem může být pojištění, zajištění správy počítačové sítě odbornou firmou apod. Obvykle je možné sdílet odpovědnost za zvládnutí rizika, ale nikoli za jeho dopad – zákazníci posuzují nepříznivý dopad jako chybu organizace [5].

5.4 Akceptace rizik

Akceptace rizika je činnost, při které je posuzována hodnota aktiva, velikost zbytkového rizika, cena opatření a kritéria organizace pro akceptaci rizika. Při této činnosti by měla být zaznamenána rozhodnutí o této akceptaci spolu s odpovědností za tato rozhodnutí. Přestože úroveň zbytkového rizika nemusí vyhovovat akceptačním kritériím, je možné rizika přijmout – pokud jsou přínosy doprovázející rizika dostatečně atraktivní nebo pokud jsou náklady na modifikaci rizik velmi vysoké. Takto akceptovaná rizika by měla být řádně komentována odpovědnými osobami a za předpokladu, že se vyskytují častěji, by mělo dojít k přezkoumání kritérií pro akceptaci rizik [5].

5.5 Komunikace rizik

V průběhu této činnosti dochází k získání dohody (domluvy), jak rizika řídit pomocí sdílení nebo výměnou informací o těchto rizicích. Je velmi důležité, aby zainteresované strany sdílely informace o rizicích jako jsou existence, charakter, forma, pravděpodobnost, závažnost, ošetření a přijatelnost. Účinná komunikace zajistí, že všechny zainteresované

rozumějí podkladům, na jejichž základě jsou činěna rozhodnutí a také tomu, proč je nutné provést konkrétní akce. Měly by existovat plány komunikace jak pro běžné situace, tak pro situace nouzové [5].

5.6 Monitorování a přezkoumání rizik

Tento proces řízení rizik tvoří dvě činnosti: monitorování a přezkoumávání rizikových faktorů, a monitorování, přezkoumávání a zlepšování řízení rizik.

Monitorování a přezkoumávání rizikových faktorů

Rizika a jejich faktory, jsou jsou hodnota aktiv, dopady, hrozby a zranitelnosti, by měla být pravidelně monitorována a přezkoumávána tak, aby bylo možné co nejdříve identifikovat změny a udržovat přehled komplexního obrazu rizik. Rizika nejsou stálá, hrozby, zranitelnosti nebo následky se mohou měnit náhle, aktiva se mohou měnit například se změnami procesů. Je možné, že změny povedou ke zvýšení rizik původně hodnocených jako nízká. Výstup této činnosti může být vstupem pro podrobnější posouzení a ošetření rizik, která se provádí pravidelně a vždy, pokud dojde k větším změnám [5].

Monitorování, přezkoumávání a zlepšování řízení rizik

Cílem tohoto procesu je zajistit, že kontext, výstupy z posouzení a ošetření rizik a plán řízení jsou v souladu a odpovídají okolnostem. Je vhodné, aby byl brán v potaz např. právní kontext, přístup k posouzení rizik, hodnoty a kategorie aktiv, kritéria dopadu, kritéria vyhodnocení a akceptace rizik a nutné zdroje. Monitorování řízení rizik může vyústit v pozměnění nebo doplnění používaného přístupu, metodiky nebo nástrojů. Je tak zajištěna neustálá platnost procesu řízení rizik bezpečnosti informací [5].

II. PRAKTICKÁ ČÁST

6 METODIKA PRAKTICKÉ ČÁSTI

V této části popíši jednotlivé kroky praktické části tak, jak jsem je postupně prováděl. Podrobnosti k jednotlivým bodům jsou uvedeny v následujících kapitolách.

- 1. Výběr použité analýzy:** Při volbě vhodné metody analýzy rizik jsem se rozhodoval mezi expertními metodami SWOT, FMEA a UMRA. Analýzu SWOT jsem zavrhl z důvodu její výrazné časové náročnosti a pouze kvalitativních závěrů. Analýzu pomocí metody FMEA jsem nakonec vyloučil z důvodu, že jsem jí využíval při práci na svojí bakalářské práci a v diplomové práci jsem si chtěl rozšířit znalosti o práci s další metodou analýzy rizik. Metoda UMRA (podrobně kapitola 6.1 *Použitá analýza*) přináší také výhodu v tom, že určuje součinitel vnímání rizika jednotlivých expertů a v konečném zpracování dochází k úpravě vyplněných matic tak, aby všichni experti vnímali riziko obdobně (dojde tak k větší objektivitě).
- 2. Výběr expertů:** Experty jsem vybíral z okruhu osob, které se pohybují v problematice ISMS a bankovníctví. Podrobnosti výběru uvádím v kapitole 6.2 *Výběr respondentů*.
- 3. Analýza rizik:** V tomto kroku jsem určil specifika bankovního prostředí z hlediska ISMS a následně identifikoval příslušná aktiva a hrozby.
 - *Určení aktiv:* Z důvodu omezeného rozsahu jsem po konzultaci s experty vybral pouze ta aktiva, která jsou pro bankovní prostředí specifická nebo zajímavá.
 - *Určení hrozeb:* Při určování hrozeb jsem vycházel ze seznamů hrozeb.
 - *Zpracování matice pro analýzu UMRA:* Identifikovaná aktiva a hrozby jsem zpracoval do matice UMRA a odeslal expertům k vyhodnocení.
- 4. Zpracování výsledků z analýzy:** Po obdržení všech vyplněných matic jsem je dle metodiky popsané v kapitole 6.1 *Použitá analýza* zpracoval do výsledné matice (podrobnosti viz kapitola 9 *Výsledky*).
- 5. Určení nejohroženějších aktiv:** Nejohroženější aktiva jsem určil na základě zpracované výsledné matice UMRA.
- 6. Návrh obecných opatření k ochraně nejohroženějších aktiv:** Návrhy na opatření k ochraně ohrožených aktiv jsem zpracoval pouze v obecné rovině. Ke konkrétním řešením by bylo možné přistoupit pouze při spolupráci vysokého managementu některé z bank.

6.1 Použitá analýza

Zkratka UMRA znamená univerzální matice rizikové analýzy (z anglického Universal Matrix of Risk Analysis). Jedná se o expertní metodu, která ve dvou fázích kombinuje verbální a numerické odhady nebezpečí a rizik. V první, verbální fázi se experti zaměřují na identifikaci aktiv a hrozeb. Výsledkem této fáze je formulář výchozí matice, který se používá ve druhé, numerické fázi. Ta obsahuje odhad závažnosti rizika s využitím matice a následné rozdělení rizik dle předem zvolených hladin závažnosti [9].

Formulář matice rizik je dvojrozměrná mřížka, kterou v jednom směru tvoří aktiva a v druhém směru hrozby. Každý expert obdrží vlastní kopii a vyplní ji systémem, že u každého křížení aktivum – hrozba provede postupně tři zhodnocení [9]:

1. jsem schopen danou kombinaci aktiva a hrozby posoudit, pokud ne, nechám buňku prázdnou
2. může dané aktivum daná hrozba ohrozit nebo se zcela míjí; pokud buňka spadá do druhé kategorie nechává buňku prázdnou
3. expert se rozhodne, do jaké míry daná hrozba dané aktivum ohrožuje [9].

Po této části přichází samotné vyhodnocení rizik pro jednotlivá aktiva, které již probíhá v trojrozměrné matici, kde první dvě osy tvoří vyplňované mřížky a třetí osu tvoří jednotlivé vyplněné formuláře „naskládané“ na sebe. Pro jeho vyhodnocení je potřeba provést několik pomocných výpočtů [9]:

Nejprve získáme počty aktivních buněk:

- a) v expertních maticích k , značíme ${}^a N_k$
- b) v jednotlivých stozích C_{ab} , značíme ${}^a N_{ab}$
- c) v celém souboru expertních matic, značíme ${}^a N_t$ [11]

V rámci odstranění nevyváženosti expertních ratingů provedeme několik kroků:

1. Standardizace expertních matic

Expertní matice k se standardizuje součtem všech ratingů zapsaných do formuláře expertem (uplatňují se pouze aktivní buňky). Spočítáme jej dle vzorce [11]:

$${}^{st}Rt_{abk} = \frac{RtE_{abk}}{\sum_{ab} RtE_{abk}}, \quad (1)$$

kde $stRt_{abk}$ je standardizovaný expertní rating a RtE_{abk} expertní rating (zvolený hodnotou stupnicového ratingu zapsaný do buňky expertem) [11].

2. Modifikace expertního ratingu

Ratingy RtE_{abk} i jejich standardizované hodnoty $stRt_{abk}$ se liší od experta k expertovi díky rozdílnému vnímání rizika mezi jednotlivými experty. Pro výpočet modifikovaného expertního ratingu potřebujeme získat dva údaje [11]:

a) individuální součinitel vnímání impaktu Pc_k [11]

$$Pc_k = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k}, \quad (2)$$

kde RtS_{max} je nejvyšší stupnicová hodnota ratingu [11].

b) týmový součinitel vnímání impaktu Pc_t

$$Pc_t = \frac{\sum_{abk} RtE_{abk}}{RtS_{max} * {}^a N_t} \quad [11]. \quad (3)$$

Nyní s pomocí těchto údajů vypočítáme modifikovaný expertní rating $mdRt_{abk}$

$$mdRt_{abk} = \frac{stRt_{abk} * Pc_t}{Pc_k} \quad [11]. \quad (4)$$

3. Dále vypočítáme hrubý stohový rating $grRt_{ab}$

$$grRt_{ab} = \frac{\sum_k RtE_{abk}}{{}^a N_{ab}} \quad [11]. \quad (5)$$

4. Vypočítáme agregovaný stohový rating $agRt_{ab}$, což je průměr modifikovaných ratingů v aktivním stohu

$$agRt_{ab} = \frac{\sum_k mdRt_{abk}}{{}^a N_{ab}} \quad [11]. \quad (6)$$

5. Následně spočítáme destandardizovaný stohový rating $dsRt_{ab}$

$$dsRt_{ab} = agRt_{ab} * \sum_{ab} grRt_{ab} \quad [11]. \quad (7)$$

6. Pokud v jedné nebo více buňkách překročí destandardizovaný rating horní mez stupnice RtS , je nutné tyto ratingy upravit vyrovnávacím součinitelem ψ

$$\psi = \frac{RtS_{max}}{\max_{ab}(dsRt_{ab})} \quad (8)$$

kde ψ může být menší nebo rovno jedné [11].

Tento vzorec lze zjednodušit na hrubý stohový rating, pokud mají všichni experti o dané oblasti stejné znalosti a podobné vnímání rizika [11].

6.2 Výběr respondentů

S ohledem na zpracovávanou problematiku ISMS v bankovníctví jsem se rozhodl vybrat experty tak, aby byla co nejvíce zachována objektivita a zároveň tak, abych pokryl poměrně široké spektrum znalostí. Pro analýzu rizik expertními metodami je důležité, aby experti měli znalosti nejen ISMS, ale také aby znali specifika bankovního prostředí a na něj navázaných rizik.

Experty jsem vybíral podle dvou kritérií – jedna skupina zná (aktivně využívá v pracovním procesu, případně se podílí na konzultacích a auditech a prošla školením) systémy řízení managementu informací dle ISO 27001. Druhá část expertů je tvořena lidmi, kteří dlouhodobě pracují v oblasti informačních technologií v bankovníctví a mají výborné znalosti procesně řízených bankovních systémů. Třetí část expertů je kombinací obou předchozích skupin – pracuje v bankovníctví a zároveň se věnuje i ISMS. Experti z druhé skupiny obdrželi základní školení o ISMS a používané metodice, experti ISMS byli poučeni o specifikách bankovního prostředí.

6.3 HW a SW vybavení

Hardwarové vybavení

Jednotliví experti tabulku UMRA zpracovávali na svých osobních počítačích. Konečné zpracování proběhlo na běžném osobním počítači značky Hewlett Packard.

Softwarové vybavení

Software využívali experti dle své volby, tabulka jim byla zaslána buď ve formě Google dokumentu nebo ve formátu MS Excel. V okamžiku, kdy expert skončil se zpracováním, byla jeho tabulka uzamčena (ale neodevzdána) tak, aby jeho výsledky nemohly ovlivnit rozhodování dalších expertů. S výjimkou koordinátora nebylo ostatním expertům známo, kdo všechno se podílí na zpracování analýzy.

V praxi by vyplňování tabulky předcházelo stanovení aktiv a hrozeb v expertním týmu a tedy by bylo expertům známo, kdo se na analýze rizik podílí. Vzhledem k tomu, že v tomto případě se jednalo o zpracování v rámci diplomové práce, stanovil jsem aktiva

a hrozby samostatně a po jejich zpracování jsem je konzultoval se dvěma členy expertního týmu.

Samotné zpracování vypracovaných matic proběhlo v kancelářském balíku Libre Office.

7 POPIS CHARAKTERISTICKÝCH PRVKŮ ISMS

V BANKOVNICTVÍ

V následujícím textu přibližuji specifika bankovního odvětví. Při zavádění systémů řízení informační bezpečnosti je třeba brát na tato specifika ohled tak, aby systém byl funkční, nebyl zbytečně zatěžující pro organizaci a zároveň pokryl všechny potřebné oblasti.

- **Bankomaty:** jedná se o samoobslužná zařízení určená k vydávání peněžní hotovosti držitelům karet. V současné době bankomaty mohou poskytovat i další služby (zadání příkazu k úhradě, dobítí kreditu mobilního telefonu, „vkladomaty“¹). Mnoho z bankomatů není pod přímým dohledem banky, stojí samostatně (v průchodu metra, v obchodních centrech, na náměstích apod.), přitom uvnitř bankomatu jsou uloženy peníze a současně se musí SW bankomatu být schopen dostat do interní informační sítě banky tak, aby mohl ověřovat údaje o klientech a jejich produktech (účtech).
- **Peníze jako zboží:** v bankovníctví na rozdíl od jiných odvětví neexistuje žádný hmotný produkt, který by byl smyslem obchodu. Obchod se zaměřuje pouze na finanční operace, případně na obchod s cennými papíry, což může být lákadlem pro zloděje – cement za milion je obtížně zcizitelný (z důvodu váhy), zatímco zcizit milion v bankovkách není z tohoto pohledu příliš obtížné.
- **Velké finanční částky na koncových pobočkách:** souvisí s předchozím bodem (peníze jako zboží). Na pobočkách, na kterých dochází k většímu množství hotovostních transakcí, jsou uloženy značné finanční prostředky v hotovosti a je zde riziko zcizení.
- **Udržování bankovního tajemství:** mělo by být stejně neprolomitelné jako lékařské nebo advokátní tajemství. Pro banky je toto obtížné – k lékaři/advokátovi chodí člověk na jedno místo, banky mají pobočky po celé republice (a musí mít všude dostupné informace o klientovi) a zároveň klienti ovládají účty pomocí internetového bankovníctví, GSM bankovníctví a telefonních bankéřů – i na tyto úkony se vztahuje bankovní tajemství. Zároveň existuje povinnost některé typy transakcí hlásit České národní bance (ČNB) a (na vyžádání) poskytovat některé informace dalším subjektům, podrobněji viz integrovanost s ostatními bankami, platební terminály, platby kartou po internetu, reporty do ČNB a do registru dlužníků, externí

1 Bankomaty určené k vkládání hotovosti na účet

partneři.

- **Prointegrovanost s ostatními bankami a dodavateli služeb (VISA, MasterCard):** z povahy nabízených služeb se na banky klade nárok, aby jejich karty fungovaly u všech obchodníků a bankomatů bez ohledu na to, která banka nebo provozovatel karet je provozuje. Kvůli tomu musí banka spolupracovat s celou řadou externích subjektů a poskytovat jim data minimálně taková, aby bylo možné ověřit, zda na účtu konkrétního klienta jsou dostatečné prostředky pro danou transakci.
- **Platební terminály:** jsou elektronická zařízení určená k bezhotovostní platbě debetní nebo kreditní kartou. Mohou být stacionární nebo mobilní. Obvykle je využívají obchodníci a poskytovatelé služeb. Existují zde obdobné obtíže jako s bankomaty, má je mnoho obchodníků, musí se ověřovat informace o klientech a zároveň musí existovat důvěra obchodníkům, že údaje nezneužijí. Ke zřízení platebního terminálu uzavírá obchodník s bankou smlouvu o jeho provozování.
- **Internetové bankovníctví:** jedná se o možnost spravovat bankovní účet online, přes webové rozhraní. Souvisí s ním několik rizik:
 - *phishingové útoky* – jde o techniku určenou k získání citlivých údajů. Obvykle se jedná o odkaz zasláný do e-mailu, který vede na webovou stránku předstírající, že se jedná o stránky banky. Pokud uživatel zadá své přihlašovací údaje, získá je tím vlastník podvodné stránky. Přestože nejde o selhání banky, tak takovéto útoky podřívají důvěryhodnost banky a banky mohou přicházet o své dobré jméno. Určitou ochranou je autorizace přihlášení pomocí SMS kódu a autorizace odesílaných plateb pomocí SMS kódu – vlastník podvodné stránky získá přihlašovací údaje, ale nemůže je zneužít.
 - *závislost na klientech* - některá bezpečnostní opatření jsou závislá na zodpovědnosti klientů (nesdělování hesla, nenechat volně položený mobilní telefon) a zároveň může docházet k tomu, že některá bezpečnostní opatření klienty obtěžují (pravidelné přenastavování hesel, SMS validace přihlášení do internetového bankovníctví)
- **Platby kartou po internetu:** banka v dnešní době svým klientům musí umožnit platit i u obchodníků, kteří mají zřízenou internetovou platební bránu (i od jiného subjektu), což opět klade velké nároky na bezpečnost. V případě, že banka neposky-

tuje nebo klient nemá zřízený 3D secure, pak pro platbu stačí pouze údaje uvedené na platební kartě a její zneužití je tak poměrně snadné.

- **Reporty pro Českou národní banku:** pro ČNB jsou momentálně reportovány všechny úvěry, banka musí zajistit (kvůli dodržení bankovního tajemství) anonymizaci dat a to, že se k těmto datům nedostane nikdo kromě ČNB.
- **Reporty do registru dlužníků:** tyto reporty jsou obdobné jako reporty pro ČNB, s tím rozdílem, že se neposílají data anonymizovaná, ale konkrétní úvěr je přiřazen ke konkrétnímu klientovi (obvykle podle rodného čísla).
- **Externí partneři:** jedná se vlastně o outsourcing služeb (klient vnímá externí partnery jako součást banky). Banka na jednu stranu nechce externím partnerům poskytovat příliš mnoho informací o svých klientech, na druhou stranu někteří externí partneři mohou uzavírat jménem banky smlouvy a k údajům o klientech přístup potřebují.

8 ANALÝZA RIZIK

8.1 Aktiva

- **PC včetně vstupních a výstupních zařízení:** veškeré transakce dnes probíhají elektronickou formou a to včetně těch, které se zadávají papírově, poté je někdo zpracovává do digitální podoby.
- **Servery:** přes servery jde veškerý provoz banky, při jejich nedostupnosti dojde k omezení služeb poskytovaných bankou, tím může dojít ke ztrátě důvěryhodnosti a dobrého jména.
- **Bankomaty:** jsou typické pro bankovní sektor, nikdo jiný je nemá, obsahují potenciálně zranitelný SW a nemalé finanční částky. Jsou tedy zajímavé ze dvou hledisek: software je přístupný komukoli a jsou v nich uloženy peníze.
- **Routery:** sám o sobě je levný, ale zabraňuje výraznějším škodám, chrání důležitější aktiva, hlavní hodnotou routeru je jeho nastavení:
 - a) mohou oddělovat interní bankovní síť od vnějších nebezpečných sítí (je důležité jejich zabezpečení)
 - b) klient by neměl poznat, že dojde k výpadku serveru, routery tedy musí být schopné přeměrovat provoz jinam.
- **Vstupní karty zaměstnanců a externistů:** při neoprávněném získání vstupní karty se může její neoprávněný držitel pohybovat volně po budovách banky (dle oprávnění původního majitele).
- **Peníze:** mají hodnotu samy o sobě. V bance jsou využívány ve dvou podobách: jako fyzické peníze a jako virtuální peníze na účtech jednotlivých klientů.
- **Bankovní SW systémy pro pobočky:** jedná se o know-how banky, při nedostupnosti nelze uzavírat obchody, při narušení integrity může dojít k chybnému zpracování dat a neoprávněnému odmítnutí klienta, při narušení důvěrnosti může dojít k poškození dobrého jména banky.
- **Bankovní SW systémy pro backoffice:** jedná se o know-how banky, umožňuje generování smluv a šetří tak náklady na pracovníky, při jeho nefunkčnosti dojde k přetížení zaměstnanců – musejí ručně zpracovávat všechna data, včetně těch povinných ze zákona (exekuční rozhodnutí, insolvence).

- **Bankovní SW systémy využívané (potenciálními) klienty:** spadá sem internetové bankovníctví, je možné přes ně sjednávat i smlouvy, při narušení bezpečnosti může dojít ke sjednání úvěru nebo převodu finančních částek neoprávněnými osobami.
- **Informace o klientech:** je nutné dodržovat zákony (ochrana osobních údajů, bankovní tajemství) a současně musejí být banky schopné poskytnout údaje o klientech v nutném rozsahu:
 - orgánům činným v trestním řízení,
 - registru dlužníku
 - ČNB
 - externím partnerům
 - ostatním bankám
 - externím dodavatelům.

Z hlediska klientů únik těchto dat znamená výrazné narušení důvěryhodnosti banky a může vést k velkým finančním ztrátám.

- **Image organizace:** pro banku jde o zcela zásadní věc. Část klientů banka získává a udržuje si je díky dobrému jménu, klienti mohou dát přednost bance s vyššími poplatky, pokud jí více důvěřují.
- **Cloudové úložiště, elektronická pošta:** tyto služby jsou obvykle poskytovány dodavatelem, banky je nemají plně pod kontrolou. Pro fungování moderní banky jde o nepostradatelnou službu.
- **Datové schránky:** banky musejí mít datové schránky zřízené povinně. Dostávají informace například o exekučních příkazech, které musejí banky v poměrně krátké době zpracovat. Zpracování těchto informací ovlivňuje další osoby = klienty banky.
- **Zaměstnanci, servisní a provozní pracovníci, IT pracovníci (FullTime):** Zajišťují provoz technologií banky a nesou know-how infrastruktury banky. Přestože nezajišťují hlavní business banky, jsou nepostradatelní.
- **Zaměstnanci, servisní a provozní pracovníci, IT pracovníci (brigádníci):** podle pozice se mohou dostat i k velmi citlivým datům, přitom u brigádníků je obvykle menší ověřování jejich důvěryhodnosti, nemusejí se cítit příliš loajálně (na rozdíl od kmenových zaměstnanců).

- **Zaměstnanci, servisní a provozní pracovníci, IT pracovníci (bodyshop):** pracovníky neověřuje přímo banka, musí důvěřovat svému dodavateli. Obvykle mají přístup ke stejně citlivým údajům jako kmenoví zaměstnanci.
- **Outsourcing - externí partneři:** musí existovat důvěra externím partnerům, klient je chápe jako součást banky, přinášejí bance uzavření obchodů, hrozí, že při přechodu k jiné bance si s sebou externí partner odnese i své portfolio klientů.
- **Dodavatelé služeb – ostraha:** – obvykle se jedná o externího dodavatele, fyzické ostraze budov je obvykle nutné umožnit pohyb po celé budově, chrání ostatní aktiva a k části z nich má fyzický přístup.
- **Klienti:** z klientů pramení veškerý zisk banky. V bankovníctví v podstatě neexistují jednorázové nákupy, většina produktů je dlouhodobých – běžné účty, úvěry, spořicí účty apod.
- **Obchodní partneři (VISA, MasterCard):** řeší oblast karet, banka potřebuje tyto služby funkční – bez nich ztrácí pro klienta význam, nemůže se spolehnout na jednoho provozovatele (ten nepokryje celý svět).
- **Práce obchodníků (lidí na pobočkách):** zajišťují komunikaci s koncovým klientem, vytváří dobré jméno organizace – je tedy důležitý způsob jejich komunikace a vystupování. V případě osobních bankéřů se může stát, že portfolio svých klientů při odchodu z banky převede ke konkurenci (klienti jdou za svým bankéřem).
- **Práce backoffice:** zajišťují hladké fungování. V rámci obchodních aktivit se podílejí na řešení složitých situací: schvalují úvěry, vytvářejí znění smluv, u větších úvěrů zajišťují finance od partnerských finančních institucí.
- **Vývoj a testování SW – lidé:** vývojáři a testéři znají SW nejlépe, jsou schopni pomáhat aplikačním podporám. Při odchodu si odnášejí know-how vyvíjených softwarových aplikací.
- **Vývoj a testování SW - používaný SW:** pro vývoj se používají jak komerční řešení, tak frameworky vytvořené na míru pro danou banku (v kterých pak banka vyvíjí své vlastní aplikace).
- **Vývoj a testování SW – data:** banky dodavatelům nechtějí poskytovat originální data klientů (kvůli zachování bankovního tajemství a důvěry klientů), ale současně kvůli analýzám, vývoji a testování je nutná co nejpřesnější kopie produkčních dat,

což je náročné na jejich přípravu, aby splňovaly obě podmínky. Tedy aby data byla anonymní, ale současně struktura odpovídala produkčním datům.

- **Obchodní informace:** jsou důležité dvě skupiny obchodních informací (jedná se o informace nutné pro hlavní bussiness bank):
 - vztahy s ostatními finančními institucemi
 - data klientů
 - klientů jako fyzických osob
 - malých organizací a osob samostatně výdělečně činných
 - velkých organizací
 - VIP klienti ze všech tří výše uvedených segmentů.
- **Poskytování bankovních služeb:** jde o hlavní bussiness proces banky, to co bance přináší zisk.
- **Webové stránky:** v současnosti obvykle slouží jako primární komunikační médium a také většina klientů dnes spravuje své účty přes internet. Nedostupnost webových stránek, jejich neaktuálnost, chybovost (i pravopisné chyby) a nepřehlednost narušují důvěryhodnost a dobré jméno banky, mohou odradit klienty a tím může dojít k odlivu klientů a finančním ztrátám.
- **Zálohy dat:** jsou důležité pro banku stejně jako pro ostatní instituce. Pomáhají udržet kontinuitu provozu v případě výpadku primárních systémů.

8.2 Hrozby

- **Požár:** ohrožuje téměř všechna aktiva, včetně například: záloh dat, zaměstnanců, finanční hotovosti apod. „Možné zdroje: úmyslné, náhodné, environmentální [5].“
- **Poškození vodou:** může k němu dojít jak při živelných pohromách (tsunami, povodně), při menších nehodách (prasknutí potrubí, kondenzace páry), také při drobných incidentech (vylití kávy na notebook, špatně utažený kohoutek), tak k němu může dojít při řešení jiné hrozby (požáru). „Možné zdroje: úmyslné, náhodné, environmentální [5].“
- **Znečištění:** jedná se o souhrnné znečištění: špína i prach. U prachu může dojít například k přehřátí výpočetní techniky, vadí také např. skvrny na smlouvách.

„Možné zdroje: úmyslné, náhodné, environmentální [5].“

- **Závažná nehoda:** záleží na povaze nehody, může ohrozit většinu aktiv (a tím kontinuitu procesů). „Možné zdroje: úmyslné, náhodné, environmentální [5].“
- **Zničení zařízení nebo médií:** Rizikem není přímo finanční ztráta způsobená zničením zařízení nebo médií, ale ztráta dat způsobená zničením těchto zařízení. „Možné zdroje: úmyslné, náhodné, environmentální [5].“
- **Selhání klimatizace:** ohrožuje aktiva navázaná na výpočetní techniku (většinu obchodních procesů bank). „Možné zdroje: úmyslné, náhodné [5].“
- **Přerušování dodávky elektřiny:** stejně jako selhání klimatizace ohrožuje aktiva navázaná na výpočetní techniku a současně ohrožuje kontinuitu procesu na pobočkách. „Možné zdroje: úmyslné, náhodné, environmentální [5].“
- **Selhání telekomunikačních zařízení:** všechny pobočky banky potřebují spojení s centrálou, aby měly aktuální informace o klientech, při výpadku této komunikace dojde k omezení poskytovaných služeb na pobočkách. Pokud dojde k výpadku připojení telekomunikačního centra, ve kterém jsou servery obstarávající internetové bankovníctví, dojde logicky k přerušení této služby a banka tím přichází o peníze a případně i o klienty. „Možné zdroje: úmyslné, náhodné [5].“
- **Vzdálená špionáž:** mohou uniknout například informace o klientech nebo přístupové informace klientů. „Možné zdroje: úmyslné [5].“
- **Odposlech:** může dojít k odposlechnutí přímo na pobočce při jednání s klientem nebo se může jednat o telefonní odposlech, který je rizikový u telefonního bankovníctví. „Možné zdroje: úmyslné [5].“
- **Krádež médií nebo dokumentů, včetně vyřazených:** dochází k úniku citlivých údajů uložených na médiích nebo v dokumentech. „Možné zdroje: úmyslné [5].“
- **Vyzrazení:** může dojít k úniku citlivých údajů, případně k poškození dobrého jména banky (při úmyslném vyzrazení zaměstnancem banky, o kterém se dozví veřejnost). „Možné zdroje: úmyslné, náhodné [5].“
- **Falšování pomocí technického vybavení, falšování pomocí aplikačního programového vybavení:** může docházet k finančním podvodům. Pomocí této techniky se může pachatel pokoušet získat údaje o třetí osobě nebo společnosti.

„Možné zdroje: úmyslné, náhodné¹ [5].“

- **Selhání zařízení/chybné fungování zařízení:** v případě například platebních terminálů (a jejich častým výpadkům) může obchodník přejít k jiné bance, v případě bankomatů může přejít klient. „Možné zdroje: náhodné [5].“
- **Přetížení informačního systému:** dojde k nedostupnosti služeb. „Možné zdroje: úmyslné, náhodné [5].“
- **Chybné fungování programového vybavení nebo zařízení:** může způsobit finanční ztráty jak bance, tak klientům. „Možné zdroje: náhodné [5].“
- **Chyba údržby:** může dojít k fyzickému poškození zařízení, k vyvolání další hrozby (požár, poškození vodou). U softwaru může chyba údržby znamenat vznik zranitelnosti, například tím, že nedojde k nainstalování aktualizace opravující známé chyby softwaru. „Možné zdroje: úmyslné, náhodné [5].“
- **Neoprávněné použití zařízení:** Může dojít k neoprávněnému použití zařízení jak od zaměstnanců, tak od třetích osob. „Možné zdroje: úmyslné [5].“
- **Poškození dat/zařízení:** může dojít ke ztrátě dat důležitých pro udržení bussinessu. V případě poškození například bankomatu dojde k omezení dostupnosti služeb banky a finančním ztrátám (oprava bankomatu, zničení peněz uvnitř bankomatu). „Možné zdroje: úmyslné [5].“
- **Nezákonné zpracování dat:** banky zpracovávají velké množství dat, může dojít k situaci, že budou zpracovávat data, u kterých vypršel souhlas s jejich zpracováním. Tato hrozba je vyšší hlavně u bank, které nabízejí více služeb prostřednictvím dceřinných organizací (například běžné účty a stavební spoření). Tyto dceřinné organizace mají často společné programy na správu clientských dat (CRM - z anglického Customer relationship management). Může dojít k tomu, že klient dá souhlas se zpracováním osobních údajů organizaci poskytující stavební spoření a data bude zpracovávat i organizace poskytující běžný účet, případně může dojít k situaci, že v jedné organizaci již vyprší souhlas se zpracováním osobních údajů a ta je bude zpracovávat dál. Toto chybné zpracování může poškodit dobré jméno banky, hrozí právní postih a pokuty. „Možné zdroje: úmyslné [5],“ náhodné.

¹ K náhodnému falšování může dojít například při přihlašování do internetového bankovníctví na počítači, na kterém je uloženo přístupové heslo do tohoto bankovníctví nebo (nepravděpodobně) při zadání špatného (ale platného) přihlašovacího jména a souběhu hesel.

- **Chyba v používání:** Nedostatečně zaškolený pracovník může způsobit velké škody jak bance, tak klientům a tím poškodit dobré jméno banky. Ke škodě může dojít například opakovaným zápisem do registru dlužníků. K chybě v používání může také dojít ze strany klienta, například při práci s internetovým bankovníctvím. „Možné zdroje: náhodné [5].“
- **Zneužití oprávnění:** oprávnění mohou zneužít: dodavatelé softwaru, obchodníci na pobočkách nebo zaměstnanci. Může dojít k úniku klientských dat a tím poškození dobrého jména banky a poškození klientů. „Možné zdroje: úmyslné, náhodné [5].“
- **Odepření činností:** Tuto hrozbu je potřeba posuzovat jak z hlediska možnosti odepření jedním zaměstnancem (například z osobních důvodů), tak skupinou zaměstnanců (stávka). „Možné zdroje: úmyslné [5].“

8.3 Sestavení matice

Z výše uvedených aktiv a hrozeb jsem sestavil finální matici a zaslal ji vybraným expertům k vyplnění. Součástí této matice byly zároveň pokyny pro vyplňování v následujícím znění:

Pokyny pro vyplňování:

pro každé aktivum a pro každou hrozbu (možnost ohrožení aktiva), rozhodněte, do jaké míry je aktivum danou hrozbou v našich podmínkách ohroženo, podle následujícího klíče:

- 1 – žádné/malé ohrožení
- 2 – střední ohrožení
- 3 – velké ohrožení
- pokud se neumíte kvalifikovaně rozhodnout, vyplňte „x“
- pokud neexistuje logický souběh aktiva a hrozby, vyplňte „x“

Děkuji za čas, který vyplňováním strávíte.

V rámci zpracování výsledků byla všechna x nahrazena prázdným polem. V pokynech jsem volil výplň písmenem x aby bylo pro experty přehledné, která pole jsou již vyplněná, a která na vyplnění ještě čekají.

Kompletní sestavenou matici naleznete v elektronické příloze 2. Zde uvádím na sebe navazující části nevyplněné matice tak, aby čtenář získal představu o jejím vzhledu

(tabulky 5 až 10).

Hrozby Aktiva	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektřiny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení								
Servery								
Bankomaty								
Routery								
Vstupní karty zaměstnanců a externistů								
Peníze								
Bankovní SW systémy pro pobočky								
Bankovní SW systémy pro backoffice								
Bankovní SW využívaný klienty ¹								
Informace o klientech								
Image organizace								
Cloudová úložiště, elektronická pošta								
Datové schránky								
Zaměstnanci ² na plný úvazek								
Zaměstnanci ³ brigádníci								

Tabulka 5: Nevyplněná matice UMRA - část 1, zdroj: vlastní

1 I potencionálními

2 Servisní a provozní pracovníci, IT

3 Servisní a provozní pracovníci, IT

Hrozby Aktiva	Selhání telekomunikačních zařízení	Vzdálená špionáž	Odposlech	Krádež médií nebo dokumentů ¹	Vyřazení	Falšování ²	Selhání/chybné fungování zařízení	Přetížení informačního systému
PC včetně vstupních a výstupních zařízení								
Servery								
Bankomaty								
Routery								
Vstupní karty zaměstnanců a externistů								
Peníze								
Bankovní SW systémy pro pobočky								
Bankovní SW systémy pro backoffice								
Bankovní SW využívaný klienty ³								
Informace o klientech								
Image organizace								
Cloudová úložiště, elektronická pošta								
Datové schránky								
Zaměstnanci ⁴ na plný úvazek								
Zaměstnanci ⁵ brigádníci								

Tabulka 6: Nevyplněná matice UMRA - část 2, zdroj: vlastní

1 Včetně vyřazených

2 Pomocí technického vybavení nebo pomocí aplikačního programového vybavení

3 I potencionálními

4 Servisní a provozní pracovníci, IT

5 Servisní a provozní pracovníci, IT

Hrozby									
Aktiva	Přetížení informačního systému	Chybné fungování programového vybavení/zařízení	Chyba údržby	Neoprávněné použití zařízení	Poškození dat/zařízení	Nezákonné zpracování dat	Chyba v používání	Zneužití oprávnění	Odepření činností
PC včetně vstupních a výstupních zařízení									
Servery									
Bankomaty									
Routery									
Vstupní karty zaměstnanců a externistů									
Peníze									
Bankovní SW systémy pro pobočky									
Bankovní SW systémy pro backoffice									
Bankovní SW využívaný klienty ⁶									
Informace o klientech									
Image organizace									
Cloudová úložiště, elektronická pošta									
Datové schránky									
Zaměstnanci ⁷ na plný úvazek									
Zaměstnanci ⁸ brigádníci									

Tabulka 7: Nevyplněná matice UMRA - část 3, zdroj: vlastní

⁶ I potencionálními

⁷ Servisní a provozní pracovníci, IT

⁸ Servisní a provozní pracovníci, IT

Hrozby Aktiva	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektriny	Selhání telekomunikačních zařízení
Zaměstnanci ¹ brigádníci								
Zaměstnanci ² bodyshop								
Outsourcing – externí partneři								
Dodavatelé služeb - ostraha								
Klienti								
Obchodní partneři (VISA, MasterCard)								
Práce obchodníků (lidí na pobočkách)								
Práce backoffice								
Vývoj a testování SW - lidé								
Vývoj a testování SW – používaný SW								
Vývoj a testování SW - data								
Obchodní informace								
Poskytování bankovních služeb								
Webové stránky								
Zálohy dat								

Tabulka 8: Nevyplněná matice UMRA - část 4, zdroj: vlastní

1 Servisní a provozní pracovníci, IT

2 Servisní a provozní pracovníci, IT

Hrozby Aktiva	Selhání telekomunikačních zařízení	Vzdálená špionáž	Odposlech	Krádež médií nebo dokumentů ¹	Vyřazení	Falšování ²	Selhání/chybné fungování zařízení	Přetížení informačního systému
Zaměstnanci ³ brigádníci								
Zaměstnanci ⁴ bodyshop								
Outsourcing – externí partneři								
Dodavatelé služeb - ostraha								
Klienti								
Obchodní partneři (VISA, MasterCard)								
Práce obchodníků (lidí na pobočkách)								
Práce backoffice								
Vývoj a testování SW - lidé								
Vývoj a testování SW – používaný SW								
Vývoj a testování SW - data								
Obchodní informace								
Poskytování bankovních služeb								
Webové stránky								
Zálohy dat								

Tabulka 9: Nevyplněná matice UMRA - část 5, zdroj: vlastní

1 Včetně vyřazených

2 Pomocí technického vybavení nebo pomocí aplikačního programového vybavení

3 Servisní a provozní pracovníci, IT

4 Servisní a provozní pracovníci, IT

Hrozby									
Aktiva	Přetížení informačního systému	Chybné fungování programového vybavení/zařízení	Chyba údržby	Neoprávněné použití zařízení	Poškození dat/zařízení	Nezákonné zpracování dat	Chyba v používání	Zneužití oprávnění	Odepření činností
Zaměstnanci ⁵ brigádníci									
Zaměstnanci ⁶ bodyshop									
Outsourcing – externí partneři									
Dodavatelé služeb - ostraha									
Klienti									
Obchodní partneři (VISA, MasterCard)									
Práce obchodníků (lidí na pobočkách)									
Práce backoffice									
Vývoj a testování SW - lidé									
Vývoj a testování SW – používaný SW									
Vývoj a testování SW - data									
Obchodní informace									
Poskytování bankovních služeb									
Webové stránky									
Zálohy dat									

Tabulka 10: Nevyplněná matice UMRA - část 6, zdroj: vlastní

5 Servisní a provozní pracovníci, IT

6 Servisní a provozní pracovníci, IT

9 VÝSLEDKY

V tabulkách 11 a 12 uvádím ukázkou vyplněných matic experty 1 a 2.

Expert 1	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektriny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	2	3	2	1	3	1	3	3
Servery	2	3	1	1	3	3	3	3
Bankomaty	2	3	3	1	3	1	3	3
Routery	2	3	1	1	3	2	3	3
Vstupní karty zaměstnanců a externistů	1	1	2	1	3	1	1	1
Peníze	3	3	3	2	3	1	2	
Bankovní SW systémy pro pobočky	1	1	1	1	1	1	3	3
Bankovní SW systémy pro backoffice	1	1	1	1	1	1	3	2

Tabulka 11: Vyplněná tabulka - ukáзка, expert 1 (hrozba „selhání telekomunikačních zařízení“ s aktivem „peníze“ - expert buňku nevyplnil), zdroj: vlastní

Expert 2	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektriny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	1	1	1	1	3	1	2	1
Servery	1	1	1	1	1	2	1	1
Bankomaty	1	1	1	1	3	1	1	2
Routery	1	1	1	1	1	1	2	1
Vstupní karty zaměstnanců a externistů	1	1	1	1	3	1	1	1
Peníze	1	1	1	1	1	1	1	1
Bankovní SW systémy pro pobočky	1	1	1	1	1	1	1	1
Bankovní SW systémy pro backoffice	1	1	1	1	1	1	1	1

Tabulka 12: Vyplněná tabulka - ukázka, expert 2, zdroj: vlastní

Vyplněné matice jsem dále zpracovával dle výše uvedené metodiky. Nejprve jsem spočítal počty aktivních buněk:

- a) v expertních maticích ${}^a N_k$ (příloha 3, listy Expert 1 až Expert 9, buňky AB2)
- a) v jednotlivých stozích ${}^a N_{ab}$ (příloha 3, list Koeficienty, tabulka ${}^a N_{ab}$)
- b) v celém souboru expertních matic ${}^a N_t$ (příloha 3, list Koeficienty, buňka AB2)

Abych odstranil nevyváženost expertních ratingů, provedl jsem tyto výpočty:

Standardizovaný expertní rating dle vzorce:

$$stRt_{abk} = \frac{RtE_{abk}}{\sum_{ab} RtE_{abk}} \quad [11], \quad (9)$$

Ukázky¹ jsou uvedeny v tabulkách 13 a 14, celý výpočet v příloze 3, listy Expert 1 až Expert 9.

¹ Tam, kde je to vhodné pro přehlednost, jsem v ukázkách výsledky zaokrouhloval.

stRtabk	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektřiny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	0,00165	0,00247	0,00166	0,00082	0,00247	0,00082	0,00247	0,00247
Servery	0,00165	0,00247	0,00082	0,00082	0,00247	0,00247	0,00247	0,00247
Bankomaty	0,00165	0,00247	0,00247	0,00082	0,00247	0,00082	0,00247	0,00247
Routery	0,00165	0,00247	0,00082	0,00082	0,00247	0,00165	0,00247	0,00247
Vstupní karty zaměstnanců a externistů	0,00082	0,00082	0,00165	0,00082	0,00247	0,00082	0,00082	0,00082
Peníze	0,00247	0,00247	0,00247	0,00165	0,00247	0,00082	0,00165	
Bankovní SW systémy pro pobočky	0,00082	0,00082	0,00082	0,00082	0,00082	0,00082	0,00247	0,00247
Bankovní SW systémy pro backoffice	0,00082	0,00082	0,00082	0,00082	0,00082	0,00082	0,00247	0,00165

Tabulka 13: Standardizovaný expertní rating – ukázka, expert 1 (hrozba „selhání telekomunikačních zařízení“ s aktivem „peníze“ - expert buňku nevyplnil)

$stRt_{abk}$	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektřiny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	0,00125	0,00125	0,00125	0,00125	0,00376	0,00125	0,00251	0,00125
Servery	0,00125	0,00125	0,00125	0,00125	0,00125	0,00251	0,00125	0,00125
Bankomaty	0,00125	0,00125	0,00125	0,00125	0,00376	0,00125	0,00125	0,00251
Routery	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00251	0,00125
Vstupní karty zaměstnanců a externistů	0,00125	0,00125	0,00125	0,00125	0,00376	0,00125	0,00125	0,00125
Peníze	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125
Bankovní SW systémy pro pobočky	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125
Bankovní SW systémy pro backoffice	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125	0,00125

Tabulka 14: Standardizovaný expertní rating – ukázka, expert 2, zdroj: vlastní

Individuální součinitel vnímání impaktu P_{C_k} dle vzorce:

$$P_{C_k} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} *^a N_k} \quad [11] \tag{10}$$

Výsledky pro jednotlivé experty (P_{C_1} až P_{C_9}) uvádím níže (vzorce 11 až 19) a jsou uvedené také v příloze 3, Listy Expert 1 až Expert 9.

$$P_{C_1} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} *^a N_k} = \frac{1215}{1881} = 0,6459330144 \tag{11}$$

$$P_{C_2} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} *^a N_k} = \frac{798}{1800} = 0,4433333333 \tag{12}$$

$$P_{C_3} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} *^a N_k} = \frac{1330}{2001} = 0,6646676662 \tag{13}$$

$$P_{C_4} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k} = \frac{1126}{1986} = 0,5669687815 \quad (14)$$

$$P_{C_5} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k} = \frac{605}{1587} = 0,3812224323 \quad (15)$$

$$P_{C_6} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k} = \frac{300}{351} = 0,8547008547 \quad (16)$$

$$P_{C_7} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k} = \frac{394}{621} = 0,6344605475 \quad (17)$$

$$P_{C_8} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k} = \frac{1413}{1719} = 0,8219895288 \quad (18)$$

$$P_{C_9} = \frac{\sum_{ab} RtE_{abk}}{RtS_{max} * {}^a N_k} = \frac{523}{1308} = 0,3998470948 \quad (19)$$

Týmový součinitel vnímání impaktu P_{C_t} dle vzorce:

$$P_{C_t} = \frac{\sum_{abk} RtE_{abk}}{RtS_{max} * {}^a N_t} = \frac{7704}{13254} = 0,581258488 \quad [11] \quad (20)$$

Výsledek je také uveden v příloze 3, List Koeficienty, buňka AE2.

Modifikovaný expertní rating $mdRt_{abk}$ dle vzorce:

$$mdRt_{abk} = \frac{stRt_{abk} * P_{C_t}}{P_{C_k}} \quad [11]. \quad (21)$$

Ukázky výsledků uvádím v tabulkách 15 a 16, kompletní výsledky jsou v příloze 3, Listy Expert 1 až Expert 9, tabulka $mdRt_{abk}$.

mdR_{tabk}	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektřiny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	0,00148	0,00222	0,00148	0,00074	0,00222	0,00074	0,00222	0,00222
Servery	0,00148	0,00222	0,00074	0,00074	0,00222	0,00222	0,00222	0,00222
Bankomaty	0,00148	0,00222	0,00222	0,00074	0,00222	0,00074	0,00222	0,00222
Routery	0,00148	0,00222	0,00074	0,00074	0,00222	0,00148	0,00222	0,00222
Vstupní karty zaměstnanců a externistů	0,00074	0,00074	0,00148	0,00074	0,00222	0,00074	0,00074	0,00074
Peníze	0,00222	0,00222	0,00222	0,00148	0,00222	0,00074	0,00148	
Bankovní SW systémy pro pobočky	0,00074	0,00074	0,00074	0,00074	0,00074	0,00074	0,00222	0,00222
Bankovní SW systémy pro backoffice	0,00074	0,00074	0,00074	0,00074	0,00074	0,00074	0,00222	0,00148

Tabulka 15: Modifikovaný expertní rating – ukázka, expert 1 (hrozba „selhání telekomunikačních zařízení“ s aktivem „peníze“ - expert buňku nevyplnil), zdroj: vlastní

$mdRt_{abk}$	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektřiny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	0,00164	0,00164	0,00164	0,00164	0,00493	0,00164	0,00329	0,00164
Servery	0,00164	0,00164	0,00164	0,00164	0,00164	0,00329	0,00164	0,00164
Bankomaty	0,00164	0,00164	0,00164	0,00164	0,00493	0,00164	0,00164	0,00329
Routery	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00329	0,00164
Vstupní karty zaměstnanců a externistů	0,00164	0,00164	0,00164	0,00164	0,00493	0,00164	0,00164	0,00164
Peníze	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164
Bankovní SW systémy pro pobočky	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164
Bankovní SW systémy pro backoffice	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164	0,00164

Tabulka 16: Modifikovaný expertní rating - ukázka, expert 2, zdroj: vlastní

Hrubý stohový rating $grRt_{ab}$ dle vzorce:

$$grRt_{ab} = \frac{\sum_k RtE_{abk}}{N_{ab}} \quad [11]. \quad (22)$$

Kompletní výsledky jsou uvedeny v příloze 3, List koeficienty, tabulka $grRt_{ab}$, ukázka výsledku je uvedena v tabulce 17.

$grRt_{ab}$	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektriny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	1,66667	1,88889	1,55556	1,625	2,33333	1,125	2	1,5
Servery	1,875	2,25	1,75	1,71429	2,125	2,375	2,11111	1,5
Bankomaty	1,875	1,875	1,875	1,85714	2,44444	1	1,77778	1,71429
Routery	1,875	2,125	1,375	1,85714	2,25	1,57143	2,22222	1,625
Vstupní karty zaměstnanců a externistů	1,22222	1	1,125	1,16667	2,375	1,14286	1,25	1
Peníze	2	1,875	1,28571	1,33333	1,57143	1,14286	1,25	1
Bankovní SW systémy pro pobočky	1,33333	1,33333	1	1,2	1,5	1,66667	2,125	1,57143
Bankovní SW systémy pro backoffice	1,33333	1,33333	1	1,2	1,66667	1,33333	2	1,42857

Tabulka 17: Hrubý stohový rating – ukázka, zdroj: vlastní

Agregovaný stohový rating $agRt_{ab}$ dle vzorce:

$$agRt_{ab} = \frac{\sum_k m dRt_{abk}}{^a N_{ab}} \quad [11]. \quad (23)$$

Úplné výsledky jsou uvedeny v příloze 3, list koeficienty, tabulka $agRt_{ab}$. Ukázku výsledků uvádím v tabulce 18.

$agRt_{ab}$	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektřiny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	0,00237	0,00261	0,00275	0,00307	0,00324	0,00157	0,00296	0,00210
Servery	0,00245	0,00300	0,00269	0,00284	0,00266	0,00326	0,00292	0,00210
Bankomaty	0,00252	0,00232	0,00303	0,00324	0,00373	0,00154	0,00233	0,00256
Routery	0,00245	0,00272	0,00222	0,00324	0,00277	0,00179	0,00311	0,00216
Vstupní karty zaměstnanců a externistů	0,00170	0,00159	0,00160	0,00169	0,00291	0,00146	0,00186	0,00139
Peníze	0,00261	0,00209	0,00160	0,00209	0,00175	0,00146	0,00166	0,00150
Bankovní SW systémy pro pobočky	0,00137	0,00137	0,00121	0,00148	0,00148	0,00170	0,00269	0,00204
Bankovní SW systémy pro backoffice	0,00137	0,00137	0,00121	0,00148	0,00159	0,00144	0,00258	0,00193

Tabulka 18: Agregovaný stohový rating – ukázka, zdroj: vlastní

Destandardizovaný stohový rating $dsRt_{ab}$ dle vzorce

$$dsRt_{ab} = agRt_{ab} * \sum_{ab} grRt_{ab} \quad [11]. \quad (24)$$

Výsledky jsou uvedeny v příloze 3, List koeficienty, tabulka $dsRt_{ab}$, ukázku uvádím v tabulce 19.

$dsRt_{ab}$	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektriny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	2,74	3,02	3,17	3,55	3,75	1,82	3,42	2,43
Servery	2,83	3,47	3,11	3,28	3,07	3,77	3,38	2,43
Bankomaty	2,91	2,69	3,50	3,74	4,31	1,78	2,71	2,96
Routery	2,83	3,14	2,56	3,74	3,20	2,07	3,59	2,50
Vstupní karty zaměstnanců a externistů	1,97	1,84	1,85	1,96	3,37	1,69	2,15	1,61
Peníze	3,01	2,42	1,85	2,41	2,02	1,69	1,92	1,74
Bankovní SW systémy pro pobočky	1,59	1,59	1,39	1,71	1,71	1,97	3,11	2,36
Bankovní SW systémy pro backoffice	1,59	1,59	1,39	1,71	1,84	1,66	2,98	2,23

Tabulka 19: Destandardizovaný stohový rating – ukázka, zdroj: vlastní

Vzhledem k tomu, že destandardizované stohové ratingy překročily horní mez stupnice RtS (3), je nutné tyto ratingy upravit vyrovnávacím součinitelem ψ dle vzorce

$$\psi = \frac{RtS_{max}}{\max_{ab}(dsRt_{ab})} = \frac{3}{4,6596637721} = 0,6438232771 \quad (25)$$

Upravené destandardizované stohové ratingy jsou uvedeny v příloze 3, List Výsledná matice. Ukázka takto upravených destandardizovaných stohových ratingů je v tabulce 20.

Výsledná matice	Požár	Poškození vodou	Znečištění	Závažná nehoda	Zničení zařízení nebo médií	Selhání klimatizace	Přerušení dodávky elektriny	Selhání telekomunikačních zařízení
PC včetně vstupních a výstupních zařízení	1,76	1,94	2,04	2,29	2,41	1,17	2,20	1,56
Servery	1,82	2,24	2,00	2,11	1,98	2,43	2,18	1,56
Bankomaty	1,87	1,73	2,25	2,41	2,78	1,15	1,74	1,91
Routery	1,82	2,02	1,65	2,41	2,06	1,33	2,31	1,61
Vstupní karty zaměstnanců a externistů	1,27	1,19	1,19	1,26	2,17	1,09	1,39	1,04
Peníze	1,94	1,56	1,19	1,55	1,30	1,09	1,24	1,12
Bankovní SW systémy pro pobočky	1,02	1,02	0,90	1,10	1,10	1,27	2,00	1,52
Bankovní SW systémy pro backoffice	1,02	1,02	0,90	1,10	1,18	1,07	1,92	1,44

Tabulka 20: Destandardizovaný stohový rating upravený vyrovnávacím součinitelem – ukázka, zdroj: vlastní

Poté jsem stanovil ranking dle ratingu matice, kompletní výsledky jsou uvedeny v příloze 3 List Ranking. Zde na ukázkou uvádím výběr nejohroženějších aktiv a nejméně ohrožených hrozeb (tabulka 21).

Ranking	Nezákonné zpracování dat	Odposlech	Odepření činnosti	Neoprávněné použití zařízení	Vzdálená špionáž	Zneužití oprávnění	Chyba v používání	Vyzrazení
servery	1,25	2,06	1,45	2,21	2,03	1,84	2,06	1,76
Bankomaty	1,31	2,72	1,42	2,37	1,46	1,68	2,55	1,68
PC včetně vstupních a výstupních zařízení	1,52	2,06	1,70	1,93	1,63	2,10	2,01	2,20
Informace o klientech	2,34	1,75	1,68	2,28	2,60	2,28	2,01	3,00
routery	1,09	2,26	1,45	1,58	2,49	1,64	1,78	1,57
Bankovní SW systémy využívané klienty	1,91	1,36	2,34	2,20	1,85	1,90	2,62	1,43
Zálohy dat	1,54	1,44	1,58	2,15	2,08	1,89	1,63	1,61
Cloudové úložiště	1,95	1,95	1,98	1,46	1,97	1,83	1,65	1,69
Poskytování bankovních služeb	1,79	1,25	2,09	1,90	1,56	1,90	1,95	1,31
Image organizace	1,99	1,59	1,76	2,17	2,45	1,56	1,78	1,90
Bankovní SW systémy pro pobočky	1,57	1,53	2,42	1,89	1,62	1,89	2,16	1,84
Datové schránky	1,58	1,60	2,54	1,44	2,02	1,85	1,75	1,69
Vstupní karty zaměstnanců a externistů	1,89	1,86	1,23	1,86	1,57	2,17	1,63	2,47
Obchodní informace	1,74	1,85	1,30	1,85	1,98	1,97	1,61	2,93
Bankovní SW systémy pro backoffice	1,39	1,42	2,42	1,80	1,53	1,80	2,00	1,59

Tabulka 21: Nejohroženější aktiva, nejvážnější hrozby – ukázka, zdroj: vlastní

10 OPATŘENÍ

Dle rankingu jsem stanovil tato nejohroženější aktiva a nejpravděpodobněji na ně působící hrozby. V následujících podkapitolách jsou uvedeny hrozby a aktiva, která ohrožují. Pod skupinou aktiv je vždy uvedeno opatření proti dané hrozbě.

10.1 Vyzrazení

Ohrožená aktiva:

- informace o klientech
- vstupní karty
- obchodní informace
- zaměstnanci, servisní a provozní pracovníci, IT – brigádníci
- zaměstnanci, servisní a provozní pracovníci, IT – bodyshop

Opatření pro informace o klientech a obchodní informace

Opatření 1: Důsledné školení zaměstnanců o ISMS a jeho důležitosti.

***Zdůvodnění:** Toto opatření by mělo zabránit vyzrazení omylem od zaměstnanců (například při rozhovoru v restauraci nebo na teambuildingové akci).*

Opatření 2: Uzavírání smluv pouze s prověřenými a důvěryhodnými dodavateli (včetně bodyshopu).

***Zdůvodnění:** Tím bude zajištěno, že nebude docházet k vyzrazení ze strany dodavatelů.*

Opatření 3: Důsledné prověřování zaměstnanců před nástupem do zaměstnání.

***Zdůvodnění:** Toto opatření by mělo chránit před úmyslným vyzrazením.*

Opatření 4: Zavedení vhodné politiky přístupu zaměstnanců k informacím tak, aby se zaměstnanci dostali pouze k těm informacím, které potřebují pro výkon své práce.

***Zdůvodnění:** V případě úmyslného vyzrazení se zaměstnanec nedostane ke všem informacím. Dovoluje menší prověřování zaměstnanců na pozicích, ve kterých nepotřebují přístup k téměř žádným informacím.*

Opatření 5: Ve smlouvách se zaměstnanci i dodavateli (včetně bodyshopu) bude zavedena povinná mlčenlivost (se sankcemi).

***Zdůvodnění:** Motivování dodavatelů, aby pro banku pracovali pouze prověřeni a spolehliví pracovníci. Část interních zaměstnanců může hrozba sankce odradit od úmyslného vyzrazení.*

Opatření pro vstupní karty

Opatření 1: Oslovit jednotlivé experty a požádat je o upřesnění, resp. vyjasnění jejich vyjádření.

***Zdůvodnění:** Pravděpodobně došlo k záměně aktiva za zranitelnost. Neoprávněné užití karty může vést k úniku dat, únik dat pravděpodobně vstupní kartu neohrozí.*

Opatření pro zaměstnance

Opatření 1: Oslovit jednotlivé experty a požádat je o upřesnění, resp. vyjasnění jejich vyjádření.

***Zdůvodnění:** Pravděpodobně došlo k záměně aktiva za zranitelnost. Zaměstnanec může způsobit únik dat, únik dat pravděpodobně zaměstnance neohrozí.*

10.2 Chyba v používání

Ohrožená aktiva

- bankomaty
- bankovní SW využívaný (potenciálními) klienty

Opatření pro bankomaty

Opatření 1: Zavedení ochrany čtečky karet.

***Zdůvodnění:** K tomuto opatření bych přistoupil, aby nedocházelo k omylům při použití platební karty (místo platební karty omylem zasunutá jiná karta).*

Opatření 2: Důsledné testování SW. SW by měl být uživatelsky přívětivý, intuitivní a dostatečně robustní proti špatně zadaným údajům.

***Zdůvodnění:** Software musí být dostatečně intuitivní tak, aby jej byli schopni obsluhovat cizinci a osoby bez zkušeností s výpočetní technikou, aniž by došlo k poruše bankomatu.*

Opatření pro bankovní SW využívaný (potenciálními) klienty

Opatření 1: Zakázání ukládání hesel v prohlížečích.

Zdůvodnění: Aby nedocházelo k tomu, že si klient na veřejném PC uloží heslo a následně dojde k jeho zneužití (což na klienta může působit jako selhání banky).

Opatření 2: Důsledné testování SW. SW by měl být uživatelsky přívětivý, intuitivní a dostatečně robustní proti špatně zadaným údajům.

Zdůvodnění: Software musí být dostatečně intuitivní tak, aby jej byli schopni obsluhovat cizinci a osoby bez zkušeností s výpočetní technikou.

10.3 Vzdálená špionáž

Ohrožená aktiva

- informace o klientech
- routery
- image organizace

Opatření pro informace o klientech a routery

Opatření 1: Pravidelné skenování počítačové sítě pro zjištění programů využitelných pro vzdálenou špionáž.

Zdůvodnění: Zabráni provozu programů pro vzdálenou špionáž.

Opatření 2: Routery a servery nastavené tak, aby v případě přerušování spojení s koncovou stanicí (po ethernetu) došlo k automatickému odpojení portu a k obnovení komunikace došlo až po potvrzení od prověřeného pracovníka.

Zdůvodnění: Zabráni odpojení koncové stanice a připojení zařízení, přes které by bylo možné provádět vzdálenou špionáž.

Opatření pro image organizace

Opatření: Opatření nezavádím, jedná se o druhotné poškození. Opatření se zavádějí pro primárně ohrožená aktiva.

10.4 Odepření činnosti

Ohrožená aktiva

- bankovní SW pro pobočky
- datové schránky
- bankovní SW pro backoffice

Opatření pro všechna ohrožená aktiva

Opatření 1: Oslovit jednotlivé experty a požádat je o upřesnění, resp. vyjasnění jejich vyjádření, případně provést detailní analýzu rizik.

Zdůvodnění: Bez dalších informací nelze navrhnout adekvátní opatření..

10.5 Odposlech

Ohrožená aktiva

- bankomaty

Opatření pro bankomaty

Opatření 1: Oslovit jednotlivé experty a požádat je o upřesnění, resp. vyjasnění jejich vyjádření.

Zdůvodnění: Vzhledem k technickým vlastnostem bankomatů není jasné, jak by je mohl případný odposlech ohrozit. Pravděpodobně zde experti míní tzv. skimming, techniku v níž ovšem není ohrožen bankomat, ale finanční prostředky na účtu klienta a bankomat představuje nikoli ohrožené aktivum, ale zranitelnost.

10.6 Krádež médií nebo zařízení

Ohrožená aktiva:

- informace o klientech
- image organizace
- vstupní karty

Opatření pro informace o klientech

Opatření 1: Zaměstnancům, kteří nepotřebují ke své práci využívat přenosná média, mají zakázáno (pomocí politiky v operačním systému) na tato média nahrávat jakákoli data.

Zdůvodnění: Zabrání se tak vynesení dat o klientech.

Opatření 2: Pracovníci, kteří s přenosnými médii pracují, budou proškoleni ohledně skartace těchto zařízení a obecně o zásadách jejich používání.

Zdůvodnění: Zabrání se zcizení médií nebo funkčních zařízení s klientskými daty (například z komunálního odpadu).

Opatření pro image organizace

Opatření: Nezavádím.

Zdůvodnění: Image organizace je ohrožena druhotně, k její ochraně dojde zavedením opatření pro primárně ohrožená aktiva.

Opatření pro vstupní karty

Opatření 1: Při vstupu do budovy prokazování kromě vstupní karty dalším způsobem (biometrií, PINem).

Zdůvodnění: Nelze plně zabránit krádeži vstupní karty. Opatření směřuje k minimalizování dopadů při jejím odcizení.

10.7 Závažná nehoda

Ohrožená aktiva:

- bankomaty
- routery

Opatření pro bankomaty

Opatření 1: Bankomaty na veřejných místech budou mít velmi robustní provedení konstrukce.

Zdůvodnění: Zabrání se tak poškození bankomatu a jeho obsahu například při nabourání automobilu do bankomatu.

Opatření 2: V případě většího poškození bankomatu dojde k automatickému znehodnocení finančních prostředků uložených v bankomatu.

Zdůvodnění: V případě náhodného poškození nedojde k odcizení finanční hotovosti. Banka pak označené bankovky vymění v ČNB v kurzu 1:1.

Opatření 3: V případě většího poškození bankomatu dojde k jeho automatickému odpojení od sítě banky.

Zdůvodnění: Dojde k zabránění druhotným škodám, nedojde k narušení bankovní sítě.

Opatření pro routery

Opatření 1: Ochrana umístěním v racku nebo mimo dosah pracovníků a návštěvníků

Zdůvodnění: Vzhledem k malým rozměrům a nevelké mechanické pevnosti routerů je nejpravděpodobnější příčinou poškození nehodou náhodné poškození z důvodu nepozornosti (šlápnutí, náraz při stěhování apod.)

10.8 Zničení zařízení

Ohrožená aktiva:

- bankomat
- PC

Opatření pro bankomat

První tři opatření jsou shodná s opatřeními pro případ závažné nehody:

Opatření 1: Bankomaty na veřejných místech budou mít velmi robustní provedení konstrukce.

Opatření 2: V případě většího poškození bankomatu dojde k jeho automatickému znehodnocení finančních prostředků uložených v bankomatu.

Opatření 3: V případě většího poškození bankomatu dojde k jeho automatickému odpojení od sítě banky.

Opatření 4: Instalace elektronických zabezpečovacích systémů.

Zdůvodnění: Cílem je, aby byla banka varována při pokusu o zničení bankomatu.

Opatření pro PC

Opatření 1: Osobně bych tato aktiva nechránil před zničením.

***Zdůvodnění:** Z hlediska ISMS obvykle nedojde ke ztrátě důvěrnosti, dostupnosti nebo integrity. Cena těchto zařízení je z pohledu banky zanedbatelná. Ochranu si zaslouží především uložená data.*

Opatření 2: Pravidelné zálohování dat.

***Zdůvodnění:** Chrání se sekundárně postižená aktiva a minimalizují se tak důsledky zničení PC a periferií.*

10.9 Přetížení informačního systému

Ohrožená aktiva:

- bankovní SW využívané klienty

Opatření pro bankovní software využívaný klienty

Opatření 1: Provoz softwaru bude rozložen do více datových center a lokalit.

***Zdůvodnění:** Při přetížení jednoho datového centra bude možné dále využívat služby (pokryjí je další datová centra).*

Opatření 2: Software automaticky vyhodnotí a zablokuje útoky typu DOS¹ a DDOS².

***Zdůvodnění:** Zabrání přetížení na základě útoku.*

10.10 Selhání zařízení

Ohrožená aktiva:

- PC

Opatření pro PC včetně periferií

Opatření 1: Nákup PC a periferií od společností, které nabízejí opravu způsobem „next bussiness day“.

***Zdůvodnění:** Tímto opatřením dojde ke zmírnění dopadu v případě poruchy zařízení.*

Jako primární se opět jeví ochrana dat.

¹ Denial of Service, útok je veden z jednoho stroje.

² Distributed Denial of Service, útok je veden z více zařízení, cílem obou útoků je znepřístupnit službu (přehlcením, využitím chyby).

10.11 Selhání klimatizace

Ohrožená aktiva

- servery

Opatření pro servery

Opatření 1: Data centra budou mít více klimatizačních jednotek uspořádaných tak, aby v případě výpadku jedné klimatizační jednotky zůstal dostatečný chladicí výkon zbytku jednotek.

***Zdůvodnění:** Dostatečný chladicí výkon v případě výpadku klimatizační jednotky zabrání růstu teploty a tím poškození serverů.*

ZÁVĚR

Tato diplomová práce je rozdělena do dvou částí. První, rešeršní, část seznamuje se systémem řízení bezpečnosti informací (Information Security Management System - ISMS) tak, jak je chápán ve smyslu mezinárodní normy ISO/IEC 27001 vydané v ČR pod označením ČSN ISO/IEC 27001. A dále se zákonem 181/2014 Sb. o kybernetické bezpečnosti a změně souvisejících předpisů, který na rozdíl od normy ISO 27001, jejíž aplikace je dobrovolná, klade na vybrané organizace včetně řady bank povinnost zajistit řadu činností v oblasti informační bezpečnosti a stanoví i sankce za nedodržení těchto povinností. Rešeršní část se zabývá také managementem rizik včetně některých metod analýz rizik.

Druhá, praktická, část nejprve seznamuje s použitou technikou analýzy rizik, metodou univerzální matice rizikové analýzy (UMRA) a popisuje metodiku praktického postupu. Dále následuje popsání specifik systému řízení bezpečnosti informací v bankovním prostředí a vytvoření výchozí matice, která byla následně předložena expertům k vyplnění. Stěžejní částí je zpracování výsledků univerzální matice rizikové analýzy, tj. souhrnné zpracování tabulek vyplněných jednotlivými experty a na jejich základě stanovení nejohroženějších aktiv a nejvýznamnějších hrozeb. Kritériem pro zařazení mezi nejohroženější aktiva a nejvýznamnější hrozby bylo dosažení nebo překročení hodnoty $C_{abk} = 2,4$, tj. 80% maximálního rizika a více.

Nejohroženějšími aktivy na základě této analýzy jsou informace o klientech, vstupní karty, obchodní informace, zaměstnanci (servisní a provozní pracovníci, IT, brigádníci a pracovníci pronajatí v rámci bodyshoppingu), bankomaty, bankovní software (využívaný klienty, pro pobočky, pro backoffice), datové schránky, routery, PC a servery a druhotně i image organizace. Nejzávažnějšími hrozbami pak jsou vyzrazení, chyba v používání, vzdálená špionáž, odepření činnosti, odposlech, krádež médií nebo zařízení, závažná nehoda, zničení zařízení, přetížení informačního systému, selhání zařízení a selhání klimatizace. Pro tyto případy jsou v závěru druhé části navržena možná obecná opatření tak, aby bylo dosaženo snížení vlivu hrozeb na ohrožená aktiva, případně jsou identifikovány oblasti, které vyžadují podrobnější šetření.

Hlavním přínosem této práce je ověření možnosti využití postupů managementu a analýz rizik pro oblast ISMS v bankovním sektoru a identifikace hrozeb, jejichž nositelem může být i klient.

SEZNAM POUŽITÉ LITERATURY

- [1] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ: ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. 2005.
- [2] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ: ČSN 36 9790. *Systém managementu bezpečnosti informací – Směrnice pro management rizik bezpečnosti informací*. 2008.
- [3] ČESKÁ REPUBLIKA: *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: *Sbírka zákonů*. 23. 7. 2014.
- [4] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ: ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. 2010.
- [5] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ: ČSN ISO/IEC 27005- *Informační technologie – Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 2011.
- [6] ŠEBESTA, V.; ŠTVERKA, V.; STEINER, F.; aj.: *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*. Český normalizační institut, 2006, ISBN 80-7283-204-2.
- [7] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ: ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. 2014.
- [8] ČESKÁ REPUBLIKA: *nařízení vlády 315/2014 Sb. kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury*. In: *Sbírka zákonů*. 8.12.2014.
- [9] TICHÝ, MILÍK.: *Ovládání rizika*. C.H. Beck, vyd. 1. vydání, 2006, ISBN 80717-9415-5.
- [10] PROCHÁZKA, PAVEL. *Metodika zavádění ISMS do malých a středních firem*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2014.

[11] TICHÝ, MILÍK. Vysvětlivky k expertní analýze metodou UMRA. In: *Milík Tichý* [online]. [cit. 2016-04-21]. Dostupné z: http://tirisk.sweb.cz/umra_vysvetlivky_140127.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

$agRt_{ab}$	Agregovaný stohový rating
$^a N_{ab}$	Počet aktivních buněk ve stohu
$^a N_k$	Počet aktivních buněk v expertní matici
$^a N_t$	Počet aktivních buněk v celém souboru expertních matic
C	Cena, význam
C_{ab}	Stoh
CRM	System pro správu klientských dat, z anglického Customer Relationship Management
ČNB	Česká národní banka
ČSOB	Československá obchodní banka
DDOS	Typ útoku, z anglického Distributed Denial of Service
DOS	Typ útoku, z anglického Denial of Service
$dsRt_{ab}$	Destandardizovaný stohový rating
FMEA	Analýza možného výskytu a vlivu vad, z anglického Failure Mode and Effects Analysis,
FT	Zaměstnání na plný úvazek, z anglického Full Time
$grRt_{ab}$	Hrubý stohový rating
HW	Hardware
ISMS	System řízení bezpečnosti informací, z anglického information security management system
IT	Informační technologie
k	Expertní matice
$mdRt_{abk}$	Modifikovaný expertní rating
MS	Microsoft
PC	Počítač, z anglického Personal Computer
P_{C_k}	Individuální součinitel vnímání impaktu
P_{C_t}	Týmový součinitel vnímání impaktu
PDCA	Demingův cyklus, z anglického Plan, Do, Check, Act (plánuj, dělej, kontroluj, jednej)
PO	Pravděpodobnost odhalení rizika
PV	Pravděpodobnost výskytu rizika
RPN	Risk priority number
RtE_{abk}	Expertní rating
RtS_{max}	Nejvyšší stupnicová hodnota ratingu
Sb.	Sbírký, Sbírký zákonů
$stRt_{abk}$	Standardizovaný expertní rating

SW	Software
SWOT	Způsob analýzy rizik, z anglického Strengths, Weakness, Opportunities, Threats (silné stránky, slabené stránky, příležitosti, hrozby)
UMRA	Univerzální matice rizikové analýzy, Universal Matrix of Risk Analysis
ZKB	Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Sb.
Σ	Součet, suma
ψ	Vyrovňovací součinitel

SEZNAM OBRÁZKŮ

Obr. 1: Vztahy při managementu rizik [6].....	14
Obr. 2: Kroky analýzy rizik [6].....	27
Obr. 3: Vztahy aktivum, hrozba, zranitelnost, riziko, opatření [10].....	32
Obr. 4: SWOT analýza [10].....	33
Obr. 5: Proces managementu rizik [5].....	35

SEZNAM TABULEK

Tabulka 1: Porovnání pojmů, zdroj: vlastní.....	24
Tabulka 2: Příklad seznamu hrozeb [5].....	30
Tabulka 3: Příklad seznamu zranitelností [5].....	31
Tabulka 4: Ukázka analýzy rizik metodou FMEA [10].....	34
Tabulka 5: Nevyplněná matice UMRA - část 1, zdroj: vlastní.....	57
Tabulka 6: Nevyplněná matice UMRA - část 2, zdroj: vlastní.....	58
Tabulka 7: Nevyplněná matice UMRA - část 3, zdroj: vlastní.....	59
Tabulka 8: Nevyplněná matice UMRA - část 4, zdroj: vlastní.....	60
Tabulka 9: Nevyplněná matice UMRA - část 5, zdroj: vlastní.....	61
Tabulka 10: Nevyplněná matice UMRA - část 6, zdroj: vlastní.....	62
Tabulka 11: Vyplněná tabulka - ukázka, expert 1 (hrozba „selhání telekomunikačních zařízení“ s aktivem „peníze“ - expert buňku nevyplnil), zdroj: vlastní.....	63
Tabulka 12: Vyplněná tabulka - ukázka, expert 2, zdroj: vlastní.....	64
Tabulka 13: Standardizovaný expertní rating – ukázka, expert 1 (hrozba „selhání telekomunikačních zařízení“ s aktivem „peníze“ - expert buňku nevyplnil).....	65
Tabulka 14: Standardizovaný expertní rating – ukázka, expert 2, zdroj: vlastní.....	66
Tabulka 15: Modifikovaný expertní rating – ukázka, expert 1 (hrozba „selhání telekomunikačních zařízení“ s aktivem „peníze“ - expert buňku nevyplnil), zdroj: vlastní.....	68
Tabulka 16: Modifikovaný expertní rating - ukázka, expert 2, zdroj: vlastní.....	69
Tabulka 17: Hrubý stohový rating – ukázka, zdroj: vlastní.....	70
Tabulka 18: Agregovaný stohový rating – ukázka, zdroj: vlastní.....	71
Tabulka 19: Destandardizovaný stohový rating – ukázka, zdroj: vlastní.....	72
Tabulka 20: Destandardizovaný stohový rating upravený vyrovnávacím součinitelem – ukázka, zdroj: vlastní.....	73
Tabulka 21: Nejohroženější aktiva, nejvážnější hrozby – ukázka, zdroj: vlastní.....	74

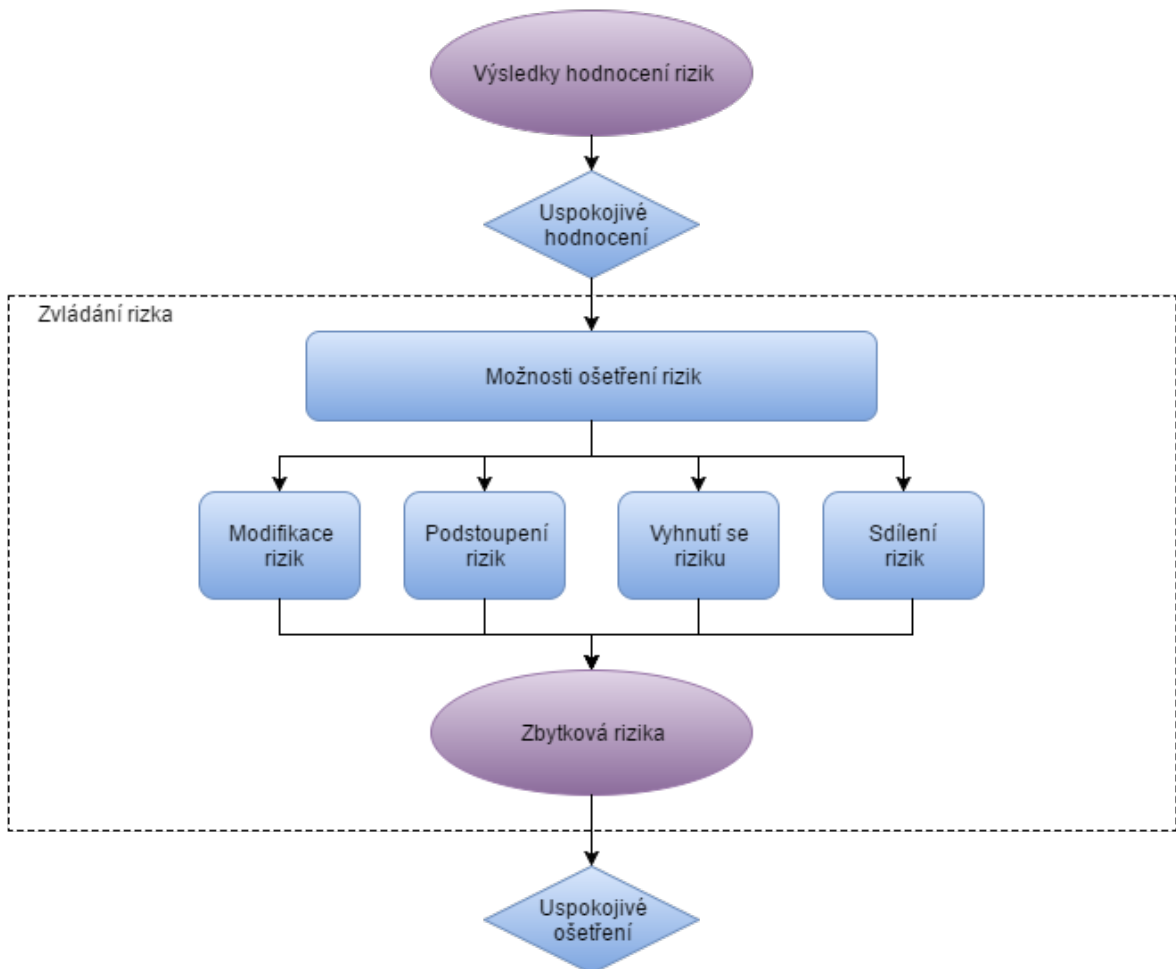
SEZNAM PŘÍLOH

Příloha P 1: Ošetření Rizik.

Příloha P 2: Umra dotazník.

Příloha P 3: Umra Výsledky.

PŘÍLOHA P 1: OŠETŘENÍ RIZIK.



Ilustrace 1: Příloha 1: Ošetření rizik [5]

PŘÍLOHA P 2: UMRA DOTAZNÍK.

Elektronická příloha na přiloženém CD, jako priloha2.xls.

PŘÍLOHA P 3: UMRA VÝSLEDKY.

Elektronická příloha na přiloženém CD, jako priloha3.xls.